المملكة العربية السعودية

مدينة الملك عبدالعزيز
للعلوم والتقنية KACST

أمن المعلومات

تأليف
د. ذيب بن عايض القحطاني

الرياض
١٤٣٦هـ - ٢٠١٥م

المملكة العربية السعودية

مدينة الملك عبدالعزيز
للعلوم والتقنية KACST

أمن المعلومات

تأليف

د. ذيب بن عايض القحطاني

الرياض

١٤٣٦هـ - ٢٠١٥م

ح مدينة الملك عبدالعزيز للعلوم والتقنية، ١٤٣٦هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

القحطاني، ذيب بن عايض

أمن المعلومات. / ذيب بن عايض القحطاني .- الرياض ، ١٤٣٦هـ

.. ص ؛ .. سم

ردمك: ٨-٧٧-٨٠٤٩-٦٠٣-٩٧٨

١- أمن المعلومات أ. العنوان

ديوي ٨, ٠٠٥ ١٤٣٦/٥٣٣١

رقم الإيداع: ١٤٣٦/٥٣٣١

ردمك: ٨-٧٧-٨٠٤٩-٦٠٣-٩٧٨

مدينة الملك عبدالعزيز للعلوم والتقنية

ص.ب. ٦٠٨٦ الرياض ١١٤٤٢

المملكة العربية السعودية

هاتف: ٠١١ ٤٨٨٣٤٤٤ - ٠١١ ٤٨٨٣٥٥٥ فاكس: ٠١١ ٤٨٨٣٧٥٦

الموقع الالكتروني: www.kacst.edu.sa

إصدارات المدينة: publications.kacst.edu.sa

البريد الالكتروني: awareness@kacst.edu.sa

المحتويات

تقديم

يتميز هذا العصر بالتقدم العلمي الهائل والمتسارع في شتى جوانب المعرفة، وكذلك في عدد الاكتشافات والمخترعات في مختلف الجوانب والتطبيقات. وقد أحدث ما شهدته الحضارة الإنسانية من قفزات وطفرات علمية تغييرًا جذريًّا شمل معظم نواحي الحياة البشرية.

ولأسباب تتعلق بهذا التراكم الكبير من العلوم وتطبيقاتها، وبسياق يستهدف تنمية الإنسان علميًّا من أجل تنميته الذاتية، أخذت مفاهيم، مثل: الوعي العلمي، والتنوير العلمي، والتثقيف العلمي تشق طريقها؛ لتسهم في زيادة الوعي بالعلوم ومنتجاتها، والمعارف وتطوراتها، بل شملت نواتج التطور في بعض العلوم وآثارها، واستخداماتها الرديئة.

ولهذه الأسباب وغيرها برزت أهمية الاهتمام بما يعرف بالثقافة العلمية، حيث ظهر هذا المصطلح على الساحة الثقافية العامة، وأصبح يفرض نفسه كضرورة ملحة؛ لتكوين المواطن الواعي بالمجريات العلمية التي من حوله، وخاصة بعد التفجر المعرفي الهائل الذي غيّر كثيرًا من الأنماط الفكرية والسلوكية للإنسان، وذلك بعد دخول العلم بنظرياته وتقنياته في مختلف مجالات النشاط الإنساني.

وقد جاءت السياسة الوطنية للعلوم والتقنية والابتكار في المملكة العربية السعودية مؤكّدة على أهمية نشر الوعي العلمي، والثقافة العلمية في المجتمع السعودي؛ لربط المجتمع العريض بتطورات العلوم، ونشر مفاهيمها الأساسة، ومن ثمّ بناء ثقافة علمية تستجيب للتوجهات الحثيثة نحو البحث العلمي، والتطوير التقني في المملكة.

وقد حرصت مدينة الملك عبدالعزيز للعلوم والتقنية منذ إنشائها على الاهتمام بالتوعية العلمية، ونشر الثقافة العلمية، حيث دأبت على متابعة إصدار المطبوعات العلمية من مجلات، وكتيّبات، وكتب علمية، وغيرها من الإصدارات الموجهة إلى عموم القرّاء والمستفيدين من أوعية النشر المتعددة، وكذلك نشاطاتها الأخرى: كأسبوع العلوم والتقنية، والمحاضرات، والندوات، والمؤتمرات؛ وذلك للإسهام في تثقيف أفراد المجتمع، وتنمية معارفهم العلمية، بالإضافة إلى إثراء المكتبة العربية، والمحتوى العربي في أوعية المعلومات الحديثة؛ لتعمّ الفائدة، وتتسع آثارها.

ويأتي هذا الإصدار كأحد الإصدارات العلمية الموجهة إلى عموم القرّاء الكرام. وستتبعه- بإذن الله تعالى- إصدارات عدة تشكّل سلسلة ممتدة من المعارف والعلوم والتطبيقات العلمية في مجالات كثيرة.

أسأل الله التوفيق؛ للمضي قدمًا في سعينا إلى إثراء المكتبة العربية بإصدارات علمية متنوعة، حيث نرجو أن تحقق أثرًا حميدًا يدفعنا جميعًا نحو مجتمع معرفي، يحثّ الخطى صوب التقدم والتطور.

رئيس مدينة الملك عبدالعزيز للعلوم والتقنية

د. تركي بن سعود بن محمد آل سعود

المقدّمة

الحمد لله رب العالمين والصلاة والسلام على رسوله الأمين، وبعد:

بدأ علم أمن المعلومات وتطوَّر مع بداية تقنية المعلومات وتطوّرها. فعندما بدأت الحاسبات الآليّة باحتـواء معلومات مهمّة، بدأ القلق علـى أمن هذه المعلومات والأجهـزة التي تعالجها وتخزّنها وتنقلها؛ فبدأ التفكير في تأمين مواقع هذه الأجهزة والمعلومات التي فيها وحمايتها، وزاد الأمر تعقيدًا ارتباط أجهزة الحاسب الآلي حول الكرَة الأرضيّة بشبكة واحدة هي شبكة الإنترنت، واعتماد كثير من الناس عليها في أداء أعمالهم، وتنمية تجارتهم، وزيادة تحصيلهم العلمي، وتواصلهم الاجتماعي، وإنهاء إجراءاتهم الحكوميّة.

لو أنّ تلك الحلول والخدمات الإلكترونيّة خالية من التهديدات وآمنة طوال الأوقات، لكان الأمر في منتهى الروعة والجمال، ولزاد التوسع في تقـديم المزيد من الخدمات الإلكترونيّة، ولاتّسعت رقعة الإقبال عليها. لكن ما يحدث هو أنّ تلك الحلول والخدمات تتعامل مع معلومات حسّاسة وبالغة الأهميّة، وفي الوقت نفسه تتعرّض لكثير من التهديدات، بل أثبتت الدراسات الحديثة نجاح اختراقات كثيرة لتلك الأنظمة وتعطيلها، أو التعدّي على معلوماتها.

أضحى علم أمن المعلومات أحد أهـم العلوم في هذا العصر، نتيجة للطلب المتزايد عليه، ولحاجة المنشآت إلى بناء أنظمة حماية جيّدة، وليس هذا فحسب، فبعد أن أصبحت المعلومات تشكّل ثروة هائلة لتلك المنشآت ومواردًا أساسيًّا مـن مواردها صارت تستحقّ بموجبه توجيه الأموال الطائلة والجهود المُضنية للحفاظ على أمنها واستمراريّة تدفقها.

بطبيعة الحال فـإنّ الصراع المستمرّ بـين أنظمة الحماية وتقنياتهـا وآلياتها من جانب، والتهديدات والأخطار والمخترقين والمهاجمين من جانب آخر، يجعل أمن المعلومات عمليّة لا تنتهي ولا تتوقّف عند حدّ معيّن، طالما استمر هذا الصـراع في تزايد، وطالما استمرت تقنية المعلومات في تطوّر تصاعديّ.

من هذا المنطلَق، رأيت تأليف هذا الكتاب ليكون مرجعًا رئيسًا لأمن المعلومات، يستهدف المبتدئين والمتخصّصين؛ فيجد المبتدئ فيه ما يساعده على البدء في دراسة علم أمن المعلومات،

ويجد المتخصّص فيه ما يشرح له أساس مفاهيم وموضوعات أمن المعلومات، وعلاقتها ببعضها بعضًا ليتسنّى له البحث فيهـا وتطويرها. يحوي هذا الكتاب بين دفّتيه عشرة فصول، تغطّي علم أمن المعلومات من عشرة جوانب، على النحو الآتي:

الفصـل الأول: مقدّمة لأمن المعلومات، وهو يوفر مقدّمة مختصرة عن أمن المعلومات تحتوي تعريفًا وشرحًـا للمفاهيم والمصطلحات الأساسيّة التي يحتـاج إليها دارس علم أمن المعلومات بالقدر الـكافٍ لهذا الغرض، دون التوسّع في علوم الحاسـب الآلي وطريقة عمله التفصيليّة كعلم مستقل. ويحتوي هذا الفصل أيضًا تعريف أنظمة المعلومات وشرح مكوّناتها الرئيسة: المكوّنات الماديّة، والبرامج، والبيانات، والمستخدمين، والإجراءات، وشبكات الحاسب الآلي.

الفصل الثاني: لماذا أمن المعلومات؟ وهو يقدم الإجابة عن السؤال الكبير: «لماذا أمن المعلومات؟» من خلال التعريف بعلم أمن المعلومات، والمحاور التي يشملها، والأسباب الرئيسة وراء الحاجـة الملحّة لأمن المعلومات، ثـمّ يوضّح أهميّة أصول المعلومـات الحرجة التي يجب حمايتها، وما تشكّله من قيم ماديّة أو معنويّة أو خدميّة، ويستعرض التهديدات المحيطة بها، وأنواع الهجمات التي يجب التصدي لها.

الفصـل الثالث: عناصر أمن المعلومات، وهو يستعرض عناصر أمن المعلومات السبعة الرئيسة: التحقّق من الهُويّة، والتحكّم بالوصول، والسِّريّة، وسلامة المعلومة وتكاملها، وعدم الإنكار، وتوافر المعلومة، والتدقيق.

الفصل الرابع: وسائل تحقيق عناصر أمن المعلومات، وهو يوضح الوسائل التي يمكن من خلالها تحقيق عناصر أمن المعلومات، فيقدّم ثلاث وسائل رئيسة يمكن استخدامها كوحدات بناء أساسيّة لتحقيـق أغلب هذه العناصر، وهي: التشفير بنوعيـه: المتناظر وغير المتناظر، والتّصديق الرقمي، والبصمة الرقميّة.

الفصـل الخامس: سياسات أمن المعلومـات. فمن المعروف أنّه كلمـا كانت إجراءات الأمن أكثر تفصيـلًا ودقة كان معرفة من يخالف؟ وأين؟ ومتى؟ تقـع المخالفة أسهل. وكلما

كانت القواعد مكتوبة كان فرضها أسهل. لذا يجب أن يشتمل برنامج أمن المعلومات على: السياسات الأمنيّة(Information Security Policies) وبرامج التدريب والتوعية (Awareness and Training) المنظِّمة لأمن المعلومات؛ وهو ما يقدّمه هذا الفصل.

الفصل السادس: أمن الحاسبات والبرمجيات والملفّات، وهو يحتوي: أمن أجهزة الحاسب الآلي(كعتاد صلد) وأمن البرمجيّات، مثل: أمن أنظمة التشغيل والبرامج التطبيقية، وأمن الملفّات الخازنة للمعلومات، مثل: ملفّات معالجة النصوص، والجداول الإلكترونيّة، وقواعد البيانات، ورسائل البريد الإلكتروني، وأمن نظام الملفّات(File System)، الذي يتحكّم بإدارة جميع الملفّات.

الفصل السابع: أمن شبكات الحاسب الآلي، وهو يوضح أشهر التهديدات الرقميّة لشبكات الحاسب الآلي، ثم يستعرض المتطلّبات الأساسيّة لأمن الشبكات، والتقنيات والآليات اللازمة لذلك.

الفصل الثامن: إدارة المخاطر المعلوماتيّة، حيث يتناول هذا الفصل التعريف بالمصطلحات والمفاهيم الأساسية في إدارة المخاطر المعلوماتيّة، ثم ينتقل إلى عمليّة تحليل المخاطر المعلوماتيّة، والطّرق المتّبعة لإجراء التحليل، وكيفية الاستفادة من نتائجه، ثمّ يستعرض الإجراءات الاحترازيّة لمواجهة المخاطر، المعلوماتيّة ومعالجة الأخطار والكوارث المعلوماتيّة بعد وقوعها.

الفصل التاسع: الحماية الماديّة، حيث يتناول هذا الفصل الحماية الماديّة لمراكز البيانات(Data Center) ومواقع مصادر المعلومات المهمة. كما يوضح متطلبات الحماية الماديّة الإداريّة والتقنية، التي يُعدُّ كلٌّ منهما مكملًا للآخر للوصول إلى حماية جيّدة. يتضمن هذا الفصل أيضًا، نظام التغذية بالطاقة الكهربائيّة، وما يجب أن تكون عليه، سواءً أكانت تغذية رئيسة معتادة، أم تغذية في حالات الطوارئ.

الفصل العاشر: أمن المعلومات والأدلة الرقميّة، حيث يستعرض هذا الفصل جرائم المعلوماتيّة، من حيث: التعريف بها وأهدافها وخصائصها، ثمّ ينتقل إلى التعريف بعلم حديث لكنّه انتشر في الآونة الأخيرة بشكل كبير، وأصبح يدرَّس كتخصّص مستقلّ في الجامعات

العالميّة، وهو علم التحقيق الجنائي للحاسب الآلي(Computer Forensics) الذي يهدف بالدرجة الأولى إلى الحصـول على أدلة رقميّة جيّدة دون إبطـال فاعليّتها أمام القضاء، أو تدميرها بعملية الحصول نفسها؛ فيوضح هذا الفصل تعريف هذا العلم الحديث والإجراءات التحضيريّة لإجراء عمليّة التحقيق، ثم يوضح المقصود بالأدلّـة الرقميّة ومواصفات الدليل الرقمي الجيد، وكيفية الحصول عليه، ثم يستعرض عملية مهمّة جدًا، وهي فحص الأجهزة ووسائط التخزين المختلفة وتحليلها من أجل استخراج الأدلـة الرقميّة منها، وأخيرًا يوضح هذا الفصل العلاقة بين أمن المعلومات وجرائم المعلوماتيّة والأدلة الرقميّة.

أسأل الله العليّ القدير أن ينفع بهذا الكتاب، والحمد لله أولًا وأخيرًا.

المؤلّف

الثلاثاء ١٤٣٣/٩/١٩ هـ

الموفق ٢٠١٢/٨/٧ م

الفصل الأول

مقدّمة لأمن المعلومات

أهداف الفصل:

- التعرّف إلى البيانات والمعلومات.
- التعرّف إلى أنظمة المعلومات ومكوّناتها.
- التعرّف إلى شبكات الحاسب الآلي وأنواعها واستخداماتها.
- التعرّف إلى شبكات الإنترنت والإنترانت والإكسترانت والبروتوكولات المستخدمة فيها، وطُرق الاتّصال بها، والبرامج والأدوات التي تتعامل معها.

ما ستتعلمه في هذا الفصل:

- تعريف المعلومات والبيانات.
- المكوّنات الرئيسة لأنظمة المعلومات: المكوّنات الماديّة (Hardware)، والبرامج (Software)، والبيانات، والمستخدمون، والإجراءات، والشبكات.
- نظام التشغيل، والبيانات، وقواعد البيانات، والملفّات، والبرامج التطبيقيّة؛ كأهداف رئيسة لأمن المعلومات.
- مفهوم البيانات الرقميّة، وماذا تعني؟ وكيفية تمثيلها في الحاسب الآلي.
- وحدات القياس المستخدمة لقياس سعات مكوّنات أنظمة المعلومات وسرعاتها.
- تعريف شبكات الحاسب الآلي وأهدافها الرئيسة.
- بنيات (طبوغرافيا) شبكات الحاسب الآلي ومميّزات كلٍّ منها وعيوبها.
- أنواع شبكات الحاسب الآلي، من حيث المساحة الجغرافية، ومن حيث المركزيّة.
- تعريف شبكات الإنترنت والإنترانت والإكسترانت، وطبقاتها، والبروتوكولات المستخدمة فيها، والخدمات التي تقدّمها، والفروق فيما بينها.

مقدّمة لأمن المعلومات

١-١ مقدّمة

انتشرت الأنظمة والأجهـزة الرقميّة في عصرنا الحاضر بشكل كبـير، ويُقصد بالنظام الرقمي، النظام الثنائي الذي يعتمد على تمثيل البيانات فيه وفق النظام الثنائي للعدّ، الذي يتكوّن من رقمين فقط، هما: الصفر والواحد. ويمكن تمثيل أيّ رقم أو حرف أو رمز من خلال النظام الثنائي، كما هي الحال في نظام (كـود) الآسكي (ASCII Code). إذاً يمكن القول إنّ البيانات هي مجموعة الأرقام الثنائيّة، سواءً أكانت تمثّل أرقامًا أم حروفًا أم رموزًا أم أيّ خليط منها، ومن الأمثلة على البيانات ما يرسل عبر الشبكات من أرقام ثنائيّة على شكل سيل من البيانات (صفر، واحد) تتعامل معها الأجهزة فقط، ولا يستطيع أن يتعامل معها الإنسان. مثال آخر للبيانات هو ما يُخزّن على أقراص التخزين المختلفة على شكل أرقام ثنائية (صفر و واحد) فقط، وتشكّل البيانات المادّة الخام للمعلومات. فالمعلومات هي البيانات بعد معالجتها و وضعها في شكل مفهوم ذي معنى، تغيّرت من خلاله الحالـة المعرفيّة لدى الإنسان، ومثال ذلك هو الحروف والكلمات والجُمل العربيّة، وجميع ما يُشكّل ويُركّب منها.

قد يُستخدم لفظ البيانات للدلالة على المعلومات، والعكس صحيح، وفي كلا الحالتين فإنّ علم أمن المعلومات هو المعنيّ بالمحافظة على المعلومات، سواءً أكانت في شكلها المعرفي المكوّن من حروف وكلمات وجُمل، أو كانت على شكل بيانات رقميّة ثنائيّة ثابتة أو متنقلة. والأسئلة التي تتبادر إلى الذهن هي: كيف تُمثّل البيانات داخل الأجهزة؟ وما المقصود بأنظمة المعلومات؟ وما مكوّناتها؟ وكيف تعمل هذه المكوّنات مع بعضها بعضًا؟ وما نظام التشغيل؟ وما الشبكات التي يجب المحافظة عليها؟ وما أنواعها؟ إلـى غير ذلك من الاستفسارات الأساسيّة في علم أمن المعلومات، والهدف من هذا الفصل هو الإجابة عن هذه الأسئلة كمدخل لهذا الكتاب.

لقد روعي في هذا الفصل أن تُعرّف المفاهيم والمصطلحات الأساسيّة التي يحتاجها دارس علم أمن المعلومات وتُشرح بالقدر الكافي لهذا الغرض، دون التوسع في علوم الحاسب الآلي، وطريقة عمله التفصيلية كعلم مستقل بذاته. فنبدأ بتعريف أنظمة المعلومات، وشرح مكوّناتها

الرئيسة: المكوّنات الماديّة، والبرامج، والبيانات، والمستخدمون، والإجراءات، وشبكات الحاسب الآلي، ويشمل ذلك تعريف نظام التشغيل والمهام الأساسيّة التي يؤدّيها، وشرح طُرُق تمثيل البيانات داخل الحاسب الآلي، والتعرّف إلى وحدات القياس الأساسيّة المُستخدمة في قياس السرعات: (سرعة المعالج المركزي (الأداء)، وسرعة إرسال البيانات)، وقياس سعات وحدات التخزين. كما يقدّم هذا الفصل مدخلًا إلى شبكات الحاسب الآلي، يشمل: تعريف شبكات الحاسب الآلي، وأهدافها، وبُنياتها (طبوغرافيا الشبكات)، وأنواعها من حيث: المساحة الجغرافية، و المركزيّة. يلي ذلك موضوع مهمّ، وهو تعريف شبكات الإنترنت والإنترانت والإكسترانت، وطُرُق الاتصال بها، والخدمات الأساسيّة التي تقدّمها، وطرق تصفحها، والبروتوكولات المُستخدَمة فيها، والنطاقات التي تنظّم مواقعها وتحدد صفحاتها.

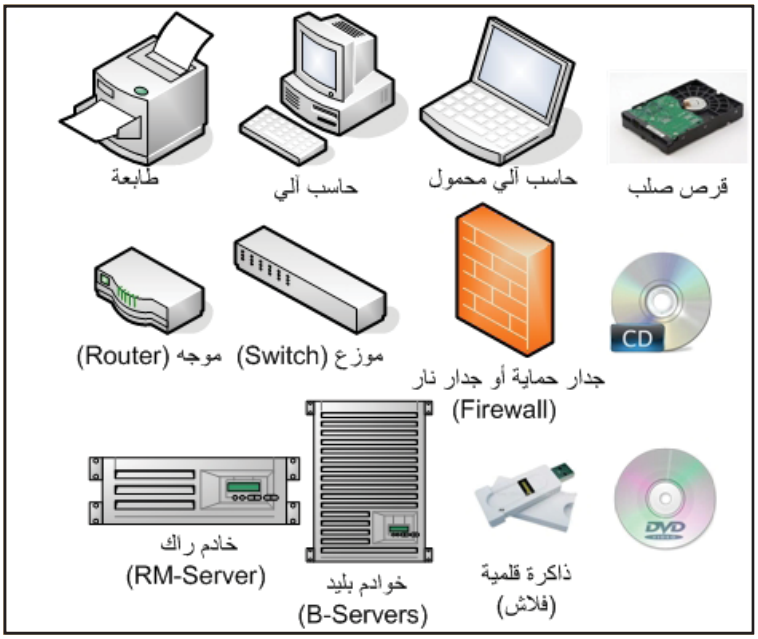
١-٢ مكوّنات أنظمة المعلومات

يجري التعامل مع المعلومات من خلال منظومة من المكوّنات الرئيسة التي تتولّى تخزين المعلومات ومعالجتها ونقلها بأشكالها كافة، وهذه المكوّنات هي: المكوّنات الماديّة (أو العتاد الصلد) (Hardware)، والبرامج (Software)، والبيانات (Data)، والمستخدمون (أو الناس) (People)، والشبكات (Networks)، والإجراءات (Procedures). وتتعامل هذه المكوّنات مع المعلومات كموردٍ رئيس من موارد المنشأة يجب المحافظة عليه، وتأمينه ضدّ التعامل الخاطئ أو التعدّي المتعمّد.

١-٢-١ المكوّنات الماديّة (Hardware)

يُقصد بالمكوّنات الماديّة (أو العتاد الصلد) الأجهزة والمعدات التقنية التي تحتوي البرامج وتشغّلها، وتحتفظ بالمعلومات وتعالجها وترسلها، مثل: أجهزة الخوادم الرئيسة (Servers)، والحاسبات الآلية بشتّى أنواعها، وأجهزة تخزين المعلومات، مثل: الأقراص الصلبة أو أجهزة التخزين (Storage Area Network-SAN)، وأجهزة الشبكة، مثل: الموجهات (Routers)، والموزِّعات (Switches)، وأجهزة الحماية، مثل: جدران الحماية (أو جدران النار) (Firewalls)، إلى غير ذلك من التجهيزات الماديّة المحسوسة التي تؤدي أيّ عملية من

العمليّات الأساسيّة للمعلومات، مثل: التخزين، والمعالجة، والإرسال، انظر الشكل(١-١).



الشكل ١-١: بعض المكوّنات الماديّة لأنظمة المعلومات

من أهم أهداف أمن المعلومات المحافظة على المكوّنات الماديّة من جميع الأضرار التي قد تلحق بها، وكذلك توفير الحماية الماديّة لها ضد التلف أو الفقد أو السرقة، كما سيأتي معنا في الفصل التاسع: الحماية الماديّة.

١-٢-٢ المكوّنات البرمجيّة (Software)

لا تستطيع المكوّنات الماديّة أن تعمل دون المكوّنات البرمجيّة، حتى ولو اكتملت جميع المكوّنات الماديّة. فالحاسب الآلي(كمكوّن مادي) ما هو إلا آلة ودوائر إلكترونيّة لا يمكن أن تستقبل الأوامر من المستخدم وتتعرف إليها ثم تنفّذها كخطوات ونتائج لها معنى لدى المستخدم، دون المكوّنات البرمجيّة، وتتألف المكوّنات البرمجيّة من مكوّنين رئيسين هما: نظام التشغيل والبرامج التطبيقيّة.

نظام التشغيل (Operating System (OS)

هو البرنامج الأساس الذي يتحكّم بالمكوّن المادي، ويسيطر عليه، ويجعل منه آلة تستجيب

للأوامر، ويحوّلها إلى هيئة معروفة من قبل المستخدم، وقد يكون نظام التشغيل خاصًّا بمكوّن ماديّ محدّد لا يصلح لغيره(Special Purpose) تنتجه الشّركة المتخصّصة في إنتاج المكوّن المادي نفسه، مثل أنظمة تشغيل أجهزة الربط، كالموزِّعات والموجِّهات، وقد يكون نظام تشغيل عام(General Purpose)، مثل أنظمة تشغيل الحاسبات الآلية. ومن أشهر أنظمة تشغيل الحاسبات الآلية نظام النوافذ(ويندوز) من شركة مايكروسوفت(MS Windows)، ونظام يونكس(Unix)، ونظام لينكس(Linux)، ونظام الماكنتوش(Macintosh).

وعادة ما يقوم نظام التشغيل أيًّا كان نوعه بالعمليّات الأساسيّة الآتية:

١. إدارة جميع أجزاء المكوّن المادي من أجهزة وبرامج، مثل: الذاكرة، والقرص الصّلب، والشاشة، والأجهزة الطرفيّة، ومنافذ الربط،...إلخ.

٢. إدارة العمليّات(Process Management) ومن ذلك تشغيل البرامج التطبيقيّة، وترتيب أولوية التعامل معها، وتحميلها إلى الذاكرة.

٣. إدارة الذاكرة(Memory Management)

٤. إدارة عمليات الدخل والخرج(I/O Management).

٥. التحكم في إرسال البيانات إلى المكوّن المادي واستقبالها منه.

٦. إدارة الملفّات والبيانات، أو ما يسمّى نظام الملفّات(File System).

البرامج التطبيقيّة(Application Programs)

هي مجموعة البرامج التي تنفِّذ الأعمال المختلفة التي يحتاج إليها المستخدم، كتحرير الوثائق والخطابات وجداول الحسابات الإلكترونيّة وقواعد البيانات وتنسيقها، وتصفّح شبكة الإنترنت، ويمكن القول إنّ البرامج التطبيقيّة هي جميع البرامج العاملة والمخزنة على المكوّن المادّي، خلاف نظام التشغيل، ومن البرامج التطبيقيّة المشهورة على الحاسب الآلي(كمكوّن مادي): برنامج معالجة الكلمات(وورد«Word")، وبرنامج الجداول الإلكترونيّة(اكسل(Excel))، وبرنامج قواعد البيانات(أكسس(Access))، وبرنامج البريد

الإلكتروني (آوتلوك (Outlook))، وبرنامج العروض التقديمية (بوربوينت (PowerPoint))، وبرنامج متصفح الإنترنت (اكسبلورر (Explorer))، وبرنامج مشغل الصوتيات والفيديو (ريال بلييـر (Real Player))، وبرنامج الرسام (بينت (Paint)) وكذلك فإنّ البرامج المستخدمة لكتابة البرامـج التطبيقيّة الأخرى (لغات البرمجة، مثل: فيجـول بيسك دوت نيت (Visual Basic (VB.Net))، وأيّ برامج يجري تطويرها باستخدام هذه اللغات لأغراض محدّدة خاصة بالمستخدم، كالبرامج الصحية، وبرامج الجامعات والمكتبات، وبرامج الأعمال الحكومية، هي جميعًا برامج تطبيقيّة.

تجدر الإشارة إلى أنّ حماية المكوّنات البرمجيّة هـي المهمّة الأكثر صعوبة من بين حماية المكوّنـات الأخرى لأنظمـة المعلومات؛ لأنهـا أكثر المكوّنـات عرضة للهجمـات وأضعفها كما سيأتي معنا في الفصـول: الثـاني والسادس والسابع. فالثغـرات الأمنيّة، ونقـاط الضعف، والأخطاء (Bugs)، والمشكلات المتعلّقة بأمن المعلومات، تأتي غالبًا من البرامج، سواءً أكانت أنظمة تشغيل أو برامج تطبيقيّـة، وإن كانت في أنظمة التشغيل أقـوى وأخطر، ويزيد الأمر تعقيدًا أنّ تطوير البرامج يحـدث في أوقات محدّدة، وتحت ضغوط ماليّة وتنافسيّة قوية، ولا تُدمج فيها آليات الحماية من البداية أولًا بأول، وإنّما يجري معالجة ما يخصّ أمن المعلومات بعد الانتهاء من تطويرها، وهذا يشكّل عبئًا أكبر ومهام أصعب لحماية هذه البرامج.

١-٢-٣ البيانات

كما مرَّ معنا، فإنّ البيانات هي المادة الأساسيّـة للمعلومات، ويطلق على البيانات عندما تكون في شكل مفهوم ومقروء وذات معنى: «المعلومات» وما يُعالج ويُخزّن ويُرسل عبر المكوّنات الأخرى لأنظمة المعلومات هي البيانات في شكلها الثنائي الرقمي (Digital) وقد تكون البيانات هيكليّة (Structured Data) مقسّمة إلى حقول تُخزّن في قواعد بيانات (Databases)، وقد تكون غير هيكليّة (Non-structured Data) تُخزّن في ملفات (File Systems) وفيما يلي نتعرف إلى كلّ قسم من هذه الأقسام.

١-٢-٣-١ قواعد البيانات

يمكن تعريف قاعدة البيانات بأنها: «مجموعة من الجداول» يحتوي كل جدول منها مجموعة من الأعمدة والصفوف التي تحوي بيانات متجانسة فيما بينها، و يحتوي كلّ عمود حقلًا واحدًا من المعلومات، وكل صف سجّلًا كاملًا يحتوي قيمة واحدة من كلّ حقل من الحقول. فمثلًا قد تحتوي قاعدة بيانات الموظفين جدولين: الأول يحتوي المعلومات الشخصية للموظف، والثاني يحتوي المهام الموكلة لكلّ موظف، ويربط بينهما رابط واحد وهو رقم الموظف. فقد يحتوي الجدول الأول ثلاثة أعمدة (حقول) هي: الاسم، ورقم الموظف، وجنسيته، ويحتوي صفوفًا (سجلّات) بعدد موظفي المنشأة، بحيث يكون هناك سجّل لكل موظف يحتوي اسمه ورقمه وجنسيته، وكذلك الحال في الجدول الثاني، فقد يحتوي أربعة أعمدة (حقول) هي: رقم الموظف، والمهمّة الموكلة إليه، وتاريخ بدايتها، ومدّتها، و صفوفًا (سجلّات) بعدد جميع المهام الموكلة لجميع الموظفين.

تجدر الإشارة إلى أنّ تطبيق أنظمة أمن المعلومات على قواعد البيانات هي أسهل بكثير منها في حالة البيانات غير الهيكلية، والسبب في ذلك هو هيكليّة البيانات وتقسيمها إلى جداول، ثمّ إلى حقول وسجلّات داخل كلّ جدول، ما يجعل السيطرة عليها والتحكّم في الصّلاحيّات والعمليّات عليها، كالحذف والإضافة والتغيير أقوى وأسهل، وكذلك فإنّ إجراء عمليّات المتابعة على قواعد البيانات، ومعرفة من قام بأي عمليّة، وعلى أيّ حقل أو سجّل، وتاريخ ذلك و وقته، وما إذا كان لديه الصلاحية أم لا هو أمر أدقّ وأسهل وأسرع في حال قواعد البيانات من غيرها. من جهة أخرى، يمكن الاستفادة من أنظمة أمن المعلومات التي تردُ وفق قواعد البيانات التي تُطورها الشركات المنتجة لقواعد البيانات مثل: (قواعد بيانات أوراكل و إس كيو إل (SQL)) ؛ لتوفير الحماية اللازمة للبيانات داخل تلك القواعد (كتشفير حقل أو عدّة حقول معيّنة)، والسيطرة على مستخدميها، والصلاحيّات الممنوحة لهم، وتعقّب جميع العمليّات التي تتم عليها وتسجيلها، وليس هذا فحسب، بل يمكن الاستفادة من أنظمة الحماية التي توفّرها تلك الأنظمة في حال تصدير البيانات (Export) خارج قواعدها.

١-٢-٣-٢ الملفّات

الملف عبارة عن كميّة (كتلة) من البيانات التي تحفظ في مساحة محدّدة ومعروفة من قبل نظام التشغيل على أيّ وسط تخزين، وتحمل اسمًا محدّدًا. وقد تكون هذه البيانات نصوصًا، أو صورًا، أو مقاطع فيديو، أو صوتًا، أو برامج تنفيذيّة، أو أيّ خليط منها، ويمكن من خلال نظام التشغيل إجراء العمليّات الأساسيّة على الملفّات، ومنها: الحذف، والإضافة، والتعديل، والنّسخ، وتغيير الاسم، وتغيير الخصائص، والإخفاء، والطباعة.

يوجد لكلّ ملف اسم وحيد، ونوع، وخصائص تميّزه من غيره من الملفّات. ويتكوّن اسم الملف من جزئين تفصل بينهما نقطة ".". الجزء الأول هو اسم الملف والجزء الثاني هو نوع الملف، ويطلق عليه "الامتداد". فمثلًا اسم الملف(doc.تجربة) يعني أن اسم الملف الذي حدّده المستخدم هو(تجربة)، ونوعه هو(doc)، أي أنّه ملّف نصّي(وثيقة) لبرنامج معالجة الكلمات(وورد) وعلى الرغم من أنّ هذه هي الطريقة الأساسيّة لتسمية الملفّات، إلّا أنّ أنظمة التّشغيل الحديثة لا تعرض امتداد الملفّات إلا عند طلب المستخدم، وبدلًا من ذلك، أصبحت هناك رموز لكل نوع من أنواع الملفّات تُعرض للمستخدم لتسهيل معرفة نوع الملف، بحيث يمكن التعرّف إلى الملف والبرنامج اللازم لفتحه مباشرة من خلال هذه الرموز.

من أهم خصائص الملفّ، تاريخ آخر تعديل تم عليه و وقته، و نوعه، و حجمه(يقاس بالبايت) وعند استخدام طريقة العرض "تفاصيل"(في نظام التشغيل ويندوز) فإنّ هذه الخصائص تُعرض بشكل تلقائي، وهناك خصائص إضافيّة يمكن عرضها عند الحاجة لذلك، مثل: مالك الملف، وعنوانه، وعدد صفحاته، وتاريخ الإنشاء، وتاريخ آخر حفظ، وتاريخ آخر وصول(فتح).

إنّ لهذه المعلومات عن الملفّات أهميّة بالغة لأمن المعلومات، فيمكن تصنيف الملفّات حسب أنواعها، ويمكن تتبّع حدثٍ ما من خلال تاريخ حدوثه و وقته. كما تؤدي أنواع الملفّات ومعرفة محتوياتها دورًا بارزًا في مكافحة الفيروسات و الديدان و برامج التجسّس، و كذلك فإنّ لها أهميّة بالغة في معالجة الأدلة الرقميّة و جرائم المعلوماتيّة، كما سيأتي معنا في الفصل العاشر.

عادةً ما يحدّد نوع الملفّ طبيعة البيانات التي يحتويها. فملفات الصّور تحتوي صورًا، والملفّات النصّية تحتوي نصوصًا، وفي حالاتٍ أخرى، يمكن أن يحتوي الملف بداخله نصوصًا،

أو صورًا، أو خليطًا من أيّ نـوع من أنواع البيانات، حتى لو كانـت تختلف عن نوعه الأصلي.

الجدول(١-١) يوضح بعض أشهر أنواع الملفّات وامتداداتها[١].

امتداد الملف	نوع البيانات التي يحتويها
bmp. jpeg. jpg. gif. pcx. wmp. pdf. tiff. png. psd. wmf. cdr	الصور
mpeg. mpg. 3gp. 3gpp. wmv. aps. ass. asx. asf. avi. mmm. mov. mp4. divx. flv. rm. vob	الأفلام، والفيديو، والوسائط المتعددة
ra. ram. da. dfm. mp3. mpa. wav. wma. pcm	الصوت
txt	نصوص من دون أيّ تنسيق
doc. xls. ppt. mdb	ملفات أوفيس ٢٠٠٣
docx. xlsx. pptx. accdb	ملفات أوفيس ٢٠٠٧
zip. rar. arj. z. dmg	الملفّات المضغوطة(وقد تكون مجلدات مضغوطة)
pgp. pgd. asc. axx. bex. bfa. docenx. docxenx. pptenx. pptxenx. xlsxenx. htmlenx. pde.	الملفّات المشفرة، والمرمزة، وذات العلاقة بكلمات المرور والصلاحيّات
eml. emlx. maildb. mbox msg. nws. vfb. edb. dbx. pst	ملفات البريد الإلكتروني، والملفّات ذات العلاقة به
exe. com. bat	البرامج التنفيذية
sys. ss. dll. dat. log. str. spl. ocx. key. ini. inf. ins. dev	ملفات خاصة بنظام التشغيل وتعريف الأجهزة

الجدول(١-١): بعض أشهر أنواع الملفّات وامتداداتها

١-٢-٣-٣ تمثيل البيانات

البيانات هي المعلومات التي تكون بصيغة ثنائيّة(صفر ، ١) ويمكن التعرف إليها ومعالجتها من قبل الحاسب الآلي، وقد تكون هذه البيانات عبارة عـن نصوص، أو صوت، أو فيديو، أو

١- مكتبة امتدادات الملفات على موقع المنظمة(File Extensions Organization): www.file-extensions.org

بيانات تحكم، أو برامج تنفيذية، وغير ذلك.

يتم تمثيل البيانات في الحاسب الآلي بالصيغة الثنائية(صفر و ١) أو ما يطلق عليه أيضًا النظام الثنائي الرقمي(Binary Digital System). والنظام الثنائي هو نظام عدّ يتكوّن من رقمين فقط هما: (صفر و ١)، (لاحظ أنّ النظام العشري يتكوّن من عشرة أرقام: من صفر إلى ٩). يُطلَق على الخانة الواحدة في النظام الثنائي التي يمكن أن تحتوي إمّا صفرًا أو(١) اسمًا: "بت" (Bit) وكلّ ثماني خانات(بتات) يُطلَق عليها حرفًا أو بايتًا(Byte) وكل(١٠٢٤) حرفًا تكوّن كيلو بايت واحدًا.

يُمثّل كلّ حرف من حروف اللغة العربيّة ببايت واحد . فيمثل الحرف "أ" في النظام الثنائي، طبقًا لكود الآسكي، بالبايت "١٠١٠٠٠٠١". لاحظ أنّ هذا البايت يتكوّن من ثماني خانات "بتات"، ويمكن أيضًا تمثيل البيانات بالنظام الست عشري(Hexadecimal) وهو نظام عدّ يتكوّن من ١٦ رقمًا: من صفر إلى ١٥، تسمّى في بعض الأحيان رموزًا ستّ عشريّة، وتُمثّل الأرقام من ١٠ إلى ١٥ في هذا النظام بالأحرف من A إلى F على الترتيب. الجدول(١-٢) يوضّح أرقام النظام العشري من صفر إلى ١٥، وما يقابلها في النظامين الثنائي والستّ عشري.

الرقم العشري(المعتاد)	الرقم الثنائي	الرقم الست عشري
٠	٠٠٠٠	٠
١	٠٠٠١	١
٢	٠٠١٠	٢
٣	٠٠١١	٣
٤	٠١٠٠	٤
٥	٠١٠١	٥
٦	٠١١٠	٦
٧	٠١١١	٧

الرقم العشري(المعتاد)	الرقم الثنائي	الرقم الست عشري
٨	١٠٠٠	٨
٩	١٠٠١	٩
١٠	١٠١٠	A
١١	١٠١١	B
١٢	١١٠٠	C
١٣	١١٠١	D
١٤	١١١٠	E
١٥	١١١١	F

الجدول(١-٢): أرقام النظام العشري من صفر إلى ١٥، وما يقابلها في النظام الثنائي والنظام الست عشري.

من أهم ما يميز النظـام الست عشري هو إمكانية تمثيل البايت(الحرف) برقمين فقط بدلًا من ثمانية بتات. فمثلًا، يمكن تمثيل الحرف «أ» بالرقمين "A5" في النظام الست عشري بدلًا من "١٠١٠٠١٠١" كما هي الحال في النظام الثنائي. وهذا أمر يسهل القدرة على فهم محتويات البيانـات عند الحاجة إلى عرضها في شكلها الحقيقـي السِّت عشري، كما سيأتي معنا في معالجة الأدلة الرقميّة.

١-٢-٣-٤ وحدات القياس المتعلِّقة بالبيانات

هناك وحدات قياس أساسيّة في الحاسب الآلي هي: وحـدة قياس السعة، و وحدة قياس سرعة المعالج المركـزي، و وحدة قياس سرعة إرسال البيانات. أمّـا وحدة قياس السّعة فهي الحرف أو البايت(Byte)، و وحدة قياس سرعة المعالج المركزي هي الهيرتز(Hertz-Hz)، و وحدة قياس سرعة البيانات هي البتّ لكلّ ثانية(Bit Per Second-bps).

يستخدم البايـت لقياس سعـة الذاكـرة العشوائيّـة(Random Access Memory-RAM)، والذاكـرة القرائيّة فقـط(Read Only Memory-ROM)، والذاكرة المخبأة أو الكاشـ(Cache Memory)، وأقراص التخزين على اختـلاف أنواعها واستخداماتها. الجدول(١-٣) يوضح بعض السّعات المستخدمة حاليًّا والأكثر انتشارًا.

السعة = عدد البايتات	المسمى باللغة العربيّة	المسمى باللغة الإنجليزية
١	بايت(حرف)	Byte
$٢^{١٠}$ = ١٠٢٤	كيلو بايت	Kilo Byte(KB)
$٢^{٢٠}$ = ١٠٤٨٥٧٦	ميجا بايت	Mega Byte(MB)
$٢^{٣٠}$ = ١٠٧٣٧٤١٨٢٤	جيجا بايت	Giga Byte(GB)
$٢^{٤٠}$ = ١٠٩٩٥١١٦٢٧٧٧٦	تيرا بايت	Tera Byte(TB)

الجدول(١-٣): بعض مكوّنات وحدة قياس السعة

الهيرتز هو عـدد النبضات(الـدورات) الموجيّة في الثانيـة الواحدة، ويستخـدم لقياس سرعة المعالج المركـزي، وهو وحدة القياس نفسها المستخدمـة في البث الإذاعي والفضائي. الجدول(١-٤) يوضح بعض السرعات المستخدمة حاليًّا والأكثر انتشارًا.

السرعة = عدد النبضات في الثانية	المسمى باللغة العربيّة	المسمى باللغة الإنجليزية
١	هيرتز	Hertz
١٠٠٠	كيلو هيرتز	Kilo Hertz(Khz)
١٠٠٠،٠٠٠	ميجا هيرتز	Mega Hertz(Mhz)
١٠٠٠،٠٠٠،٠٠٠	جيجا هيرتز	Giga Hertz(Ghz)

الجدول(١-٤): بعض مكوّنات وحدة قياس سرعة المعالج المركزي

عـدد البتّات(الخانـات) في الثانيـة الواحدة هو وحـدة قياس سرعـة إرسـال البيانات، ويستخدم لقياس سرعة الإرسال في شبكات الحاسب الآلي وخطوط الاتصال بشبكة الإنترنت. الجدول(١-٥) يوضح بعض السرعات المستخدمة حاليًّا والأكثر انتشارًا.

السرعة = عدد البتات/ ثانية	المسمى باللغة العربيّة	المسمى باللغة الإنجليزية
١	بت/ثانية	Bit Per Second(bps)
$٢^{١٠}$ = ١٠٢٤	كيلوبت/ثانية	Kilo Bit Per Second(Kbps)
$٢^{٢٠}$ = ١٠٤٨٥٧٦	ميجابت/ثانية	Mega Bit Per Second(Mbps)
$٢^{٣٠}$ = ١٠٧٣٧٤١٨٢٤	جيجابت/ثانية	Giga Bit Per Second(Gbps)

جدول(١-٥):بعض مكوّنات وحدة قياس سرعة إرسال البيانات الرقميّة(الثنائية)

١-٢-٤ المستخدمون

المستخدمون هم من يعمل على المكوّنات الماديّة، ويتعامل مع البرامج، ويُدخل المعلومات،

ويطبع التقارير، وينفّذ الإجـراءات، ويتواصل من خلال الشبكات. يمكن وصف المستخدمين بأنّهم المحرّك الحقيقي في منظومة أنظمة المعلومات والمستهدفين بالجزء الأكبر من أنظمة الحماية التابعة لها، ولا يمكن أن تستمرّ أيّ منشأة في أداء أعمالها بأيّ حال من الأحوال دون وجود المستخدمين المدرَّبين والمؤهلين والموثوق بهم، الذين لديهم العلم والثقافة الكفيلين بأداء أعمالهم وفق سياسات المنشأة عامةً، و وفق السياسات الأمنيّة للمعلومات خاصةً.

يبقى المستخدمـون والناس المتعاملون مع مكوّنات أنظمة المعلومـات هم التهديد المستمر المستعد لإلحاق الأذى والضرر بالمعلومات أو الكشف عنها، والتعدي على أنظمة حمايتها، إمّا عمدًا أو عن طريق الخطأ، ويُعدُّ المستخدمون الحلقة الأضعف في برنامج أمن المعلومات، بسبب قابليتهم للنسيان والخطأ، وحاجتهم الماسة إلى التدريـب والتأهيل المستمرِّين، وما تفرضه عليهم حاجة المهام والأعمال الموكلـة إليهم من التنقل والحركـة باستمرار. هناك كثير من الهجمات الإلكترونيّة التي تركّز علـى استغلال نقاط الضعف لدى المستخدمين، والنفاذ من خلالها، أو الإيقاع بهـم للإفصاح عن المعلومات السِّريّة، كما سيأتي معنا في الفصل الثاني: هجمات الهندسة الاجتماعيّة؛ وهو ما يحتّم ضرورة حماية المستخدمين ضدّ هذه الهجمات، وكذلك حماية المكوّنات الأخرى من أخطاء المستخدمين أو أضرارهم المتعمّدة، وكشف ذلك والتعامل معه كما سنرى في الفصول: السادس والسابع والتاسع.

١-٢-٥ الإجراءات (Procedures)

الإجراءات المقصودة هنا كمكوّن من مكوّنات أنظمة المعلومات هي الأوامر المكتوبة لتنفيذ مهام محدّدة. تُعدُّ الإجراءات هي الرابط بين المستخدمين والمكوّنات الماديّة والبرمجيّة، فهي التي تحدّد طريقة العمل الذي ينفّذ من خلال تلك المكوّنات، ولضبط أمن المعلومات في المنشأة، فإنّه يلزم تحديد الإجراءات المطلوب من كل مستخدم أداءها، وتحديد الأجهزة والبرامج التي يجب عليه أن يستخدمها، وعليه، فإنّ قيام أيّ مستخدم بمهمة ليست من اختصاصه، واطّلاعه على إجراءاتها ومعلوماتها يُعدُّ خرقًا لأمن المعلومات. فمثلًا قد يكون لدى أحد البنوك مستشار مالي يتطلـب عمله أن يعرف آلية تحويل الأموال بين الحسابـات البنكية والأجهزة والبرامج

المستخدمة لذلك من أجل تطويرها، وبوجـود ثغرة أمنيّة في أنظمة الحماية في البنك حيث، لا يُطبّق على هذا المستشار عنصر التحقّق من الهُويّة لدى دخوله إلى قواعد البيانات(انظر الفصل الثالـث)، فإنّه يمكنـه أن يحوّل أموالًا بطريقـة غير شرعيّة، نتيجـة معرفته التامّة بإجراءات التحويل، وقدرته على تغيير قيم حقول قواعد البيانات، ويزداد الأمر خطورة إذا كانت الإجراءات غير الآمنة هي إجراءات الحماية وأمن المعلومات نفسها. فمثلًا قد يعرّض ضعف إجراءات الحماية الماديّة(انظر الفصـل التاسع) للنُسخ الاحتياطية لمعلومات المنشأة التي تُحفظ خارج مقر المنشأة تلك، النُسخ لخطر السرقة أو الفقد أو الاعتداء عليها وأخذها بالقوة، نتيجة معرفة إجراءات النّسخ والنقل والحفظ من قبل أشخاص غير مصرّح لهم.

لذلك فإنّ المحافظة على أمن الإجراءات وسريّتها وحصرها في الأشخاص المصرّح لهم فقط على أساس «المعرفة بقدر الحاجة»(need-to-know) هو أمر أساسي في أمن المعلومات، لاسيما إذا كانت تلك الإجراءات تعالج معلومات حساسة ومهمة.

١-٢-٦ شبكات الحاسب الآلي

تُعدُّ شبكات الحاسب الآلي(أو شبكات المعلومات) العصب الناقل المهم في عصرنا الحاضر، الذي تستخدمه شرائح كبيرة من الناس، من أجـل نقل المعلومات وتبادلها والحصول عليها بكل يسر وسهولة، وإذا ما قيل إنّ العالم أصبح أشبه ما يكون بقرية صغيرة، فإن ذلك أصبح حقيقة ملموسة نعايشها يوميًّا.

من أعظم ما يؤرّق المتخصّصين في تقنية المعلومات وأصحاب المنشآت الحكوميّة والخاصة على اختلاف أحجامها هو أمن هذه الشبكات المهمة، ولا بدّ لأي باحث في هذا المجال أن يتعرف أوّلًا إلى شبكات المعلومات وأنواعها، والمهام التي تؤدّيها قبل الولوج في تفاصيل حمايتها.

يمكن تعريف شبكة الحاسب الآلي بأنّها: «منظومة مـن أجهزة الحاسب الآلي والبرامج وأجهزة الربط المتّصلة فيما بينها بأحد وسائط نقل البيانات» وقد انتشرت شبكات الحاسب الآلي بشكل كبير في العصر الحاضر، فلا تكاد تخلو منشأة مهما كانت طبيعة عملها من شبكة حاسب آلي، بل تعدّى الأمر ذلك بوصول شبكات الحاسب الآلي إلى المنازل أيضًا.

أهداف شبكات الحاسب الآلي

تحقّق شبكات الحاسب الآلي الأهداف الآتية :

١. تبادل البيانات والمعلومات بين الجهات والأجهزة في مواقع مختلفة بسرعة وكفاءة.

٢. مشاركة مستخدمي الشبكة في مصادر المنشأة الموحّدة، كقواعد البيانات الموحّدة والأجهزة والطابعات المركزيّة.

٣. تقليل تكلفة الحصول على برامج معالجة البيانات وأجهزتها، من خلال الاستخدام المركزي والموحّد لموارد المنشأة عالية الكلفة.

٤. تحكّم مركزي في الأجهزة، والمعلومات، والمستخدمين.

١-٢-٦-١ بُنية (طبوغرافيا) شبكات الحاسب الآلي

بُنية الشبكة هي هيكليّة الشبكة التي تنتج عن الطريقة التي تربط بها الأجهزة، باستخدام الوسط الناقل (كالكابلات). فمن الممكن ربط أجهزة الحاسب الآلي بعدّة أشكال (طبوغرافية) حسب الحاجة، وحسب أدوات الربط والكابلات المتوافرة، ويعتمد اختيار بُنية شبكة الحاسب الآلي علي معايير مهمّة تتلخّص فيما يلي:

- نوع أجهزة الربط والكابلات المتوافرة، التي تحتاج إليها الشبكة.
- خصائص هذه الأجهزة والكابلات، من حيث السرعة والمسافة التي تغطّيها دون الحاجة إلى إعادة الإرسال.
- نموّ الشبكة في المستقبل.
- أدوات إدارة الشبكة المستخدمة.

وهناك أنواع رئيسة من بُنيات شبكات الحاسب، وهي:

١. البُنية الخطيّة (Bus Topology).

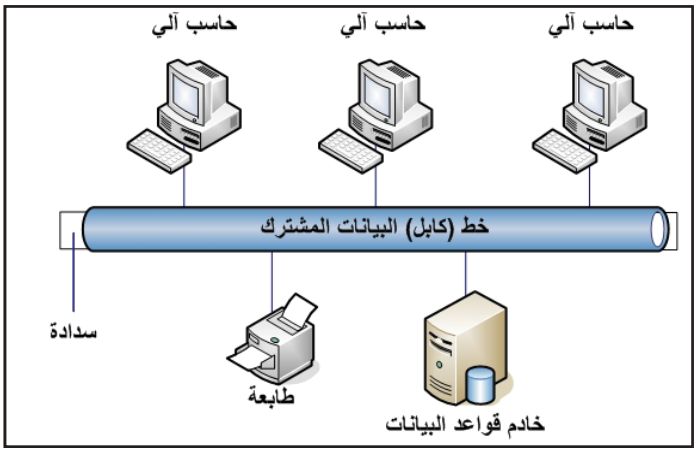
٢. البُنية النجميّة (Star Topology).

٣. البُنية الحلقيّة (Ring Topology).

٤. البُنية النجميّة الشجريّة(Star-Tree Topology).

١. البُنية الخطيّة(Bus Topology)

في هذه البُنية، تربط جميع الأجهزة بخط(كابل) نقل واحد(ومن هنا جاءت التّسمية: الخطيّة) باستخدام أداة ربط خاصّة تكون على شكل حرف(T) تسمّى(T-Connector)، انظر الشكل(١-٢). عادة ما يكون الكابل ذا نهايتين مفتوحتين، لذا يجب استخدام سدّادتين(Terminators) ذاتَيْ مقاومة عالية عند طرفي الكابل لإبطال مفعول الإشارة التي تصل إلى هناك لتلافي حدوث التصادم (Collusion).



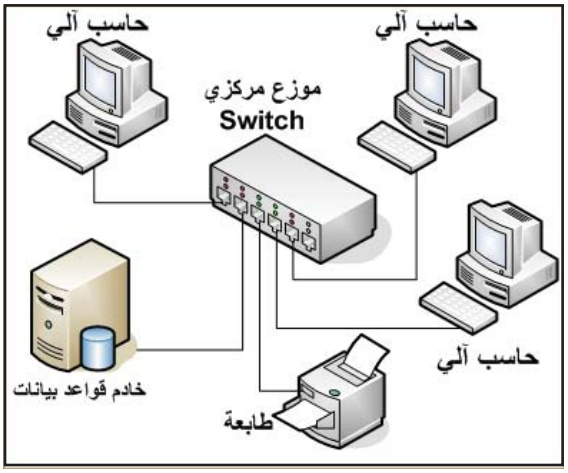
الشكل(١-٢): البُنية الخطية للشبكات

وطريقة عملها، هو أن يبثّ الجهاز المرسل البيانات ويضعها على الكابل المشترك لتنتشر في كلا الاتجاهين، وكلّ جهاز يُرسل البيانات إلى الجهاز الذي يليه، وهكذا حتى وصولها إلى الجهاز الهدف(المرسل إليه) أو إلى السدّادتين في طرفي الكابل، وإذا كانت البيانات التي على الكابل لا تخصّ الجهاز فإنّه ببساطه يهملها.

٢. البُنية النجميّة (Star Topology)

في هذه البُنية، تربط جميع الأجهزة بموزع مركزي(Switch) ، بحيث يتّصل كل جهاز على الشبكة بكابل منفصل بالموزّع المركزي، انظر الشكل(١-٣). ويمكن استخدام أنواع مختلفة من الكابلات والموزعات المركزيّة حسب حجم الشبك، و طريقة عملها هو أن يرسل الجهاز

المرسل بياناته إلى المجمّع المركزي، الذي يبثّها لجميع الأجهزة المرتبطة به، فيستلمها الجهاز المرسل إليه فقط ، بناءً على عنوان المرسل إليه. أمّا الأجهزة الأخرى فتتجاهل هذه البيانات.

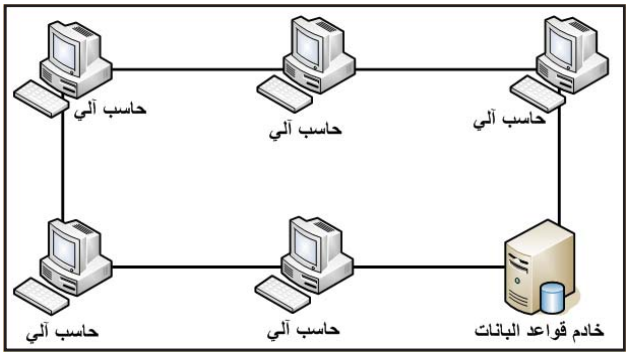


الشكل(١-٣): البُنية النجمية للشبكات

٣. البُنية الحلقية (Ring Topology)

في هذه البُنية، يُربط كل جهاز بالذي يليه بوساطة كابل واحد مشترك، ثمّ يربط الجهاز الأخير بالجهاز الأول لتشكيل حلقة من الأجهزة(ومن هنا جاءت التسمية: الحلقيّة) ، انظر الشكل(١-٤) . تشبه البُنية الحلقية في تركيبها البُنية الخطية، من حيث ربط الأجهزة على كابل واحد، لكن الفرق أنّ طرَفي الكابل في الحلقيّة مرتبطان مع بعضهما بعضًا؛ أي أنّه لا توجد نهايات للكابل، ولا تحتاج إلى سدّادات، لأنّ الكابل متّصل على شكل حلقة تسمح للإشارات المتولدة من الأجهزة بأن تمرَّ عبر الحلقة بجميع الأجهزة الأخرى إلى أن تعود مرّةً أخرى إلى مكان انطلاقها.

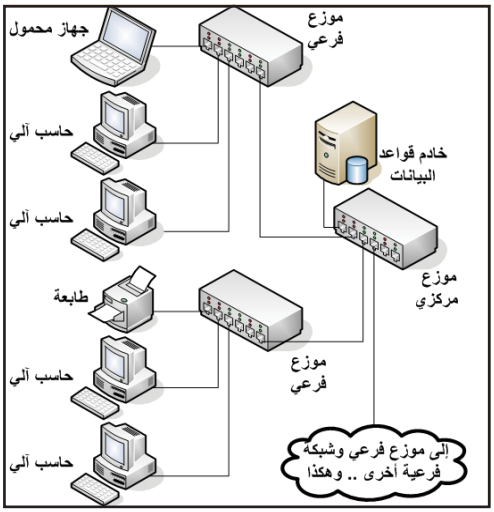
وطريقة عملها هو أن يمرِّر كلّ جهاز البيانات إلى الجهاز الذي يليه في الحلقة، الذي بدوره يقوي هذه الإشارة ويمرّرها إلى الجهاز التالي، وهكذا...، حتّى تصل البيانات إلى الجهاز المستهدف، ويعمل كل جهاز متّصل بهذه البُنية كمكرّر للإشارة التي تصله إن لم تكن تعنيه.



الشكل(١-٤): البُنية الحلقيّة للشبكات

٤. البُنية النجميّة الشجريّة (Star-Tree Topology)

في هذه البُنية، تجمع الأجهزة في مجموعات من البنيات النجميّة، ثم تربط هذه البُنيات النجميّة على شكل شجرة، انظر الشكل(١-٥). ويكون في هذه الحالة هنالك موزّع(Switch) مركزيّ مرتبط بموزّعات فرعيّة تربط فروع الشبكة، وهكذا لتشكل شجرة كبيرة من الشبكات الفرعيّة. وهـذه البُنية أكثر البُنيات انتشـارًا وأحدثها استخدامًـا. إذا تعطّل أحد الموزّعات الفرعيّة، فإنّه ينحصر أثره في الشجرة الفرعيّة المرتبطة به فقط، ولا يكون له تأثير في بقية الشّبكات الفرعيّة، ولتلافي مشكلة تعطّل الموزّع المركزي، يمكن استخدام موزّع مركزي رديف له يحلّ محلّه في حالة تعطلّه.



الشكل(١-٥): البُنية النجميّة الشجريّة للشبكات

وكمقارنة بين بُنيات شبكات الحاسب الآلي السابقة، يوضح الجدول(١-٦) مميزات وعيوب كل بُنية، التي بناءً عليها يمكن الاختيار من بين هذه البُنيات، وإن كان بعضها قد قلّ استخدامه كثيرًا حتى ليكاد أن يكون معدومًا، مثل البُنيات الخطيّة والحلقيّة، بينما اتسع انتشار بعضها، كالبُنيات النجميّة الشجريّة.

١-٢-٦-٢ أنواع شبكات الحاسب الآلي من حيث المساحة الجغرافيّة

تنقسم شبكات الحاسب الآلي من حيث المساحة الجغرافية التي تغطيها إلى نوعين رئيسين هما:

- شبكات الحاسب الآلي المحليّة (Local Area Network-LAN).

وهي منظومة من الحاسبات الآلية وأجهزة الربط الأخرى التي يجمعها مكان محدود كشركة أو مؤسسة، بحيث تتم عملية الربط والتواصل دون خطوط اتّصال خارجيّة، سواءً من شركة اتصالات هاتفية أو من الإنترنت.

- شبكات الحاسب الآلي الواسعة(Wide Area Network-WAN).

وهي منظومة من الحاسبات الآلية وأجهزة الربط الأخرى التي تتوزع على نطاق واسع(على مستوى المدينة أو الدولة أو العالم)، بحيث تستخدم في عملية الربط والتواصل خطوط اتصال خارجية، سواءً من شركة اتصالات هاتفية أو من الإنترنت. وقد تتكون الشبكات الواسعة من شبكات محليّة مرتبطة فيما بينها بخطوط اتصال خارجيّة.

١-٢-٦-٣ أنواع شبكات الحاسب الآلي من حيث المركزيّة

تنقسم شبكات الحاسب الآلي من حيث المركزيّة في الاتصال إلى نوعين رئيسين هما:

- شبكة الخادم والعميل(Client/Server).

تتكوّن من جهاز مركزي(Server) يقدّم مجموعة من الخدمات عبر الشبكة لحواسيب – عملاء – أخرى(Clients). فالخادم هو الذي يقدم الخدمة للعميل، أمّا العميل فهو الذي يطلب الخدمة من الخادم. ومن الأمثلة على الخوادم: خادم الملفّات (File Server)، وخادم الطباعة(Print Server)، وخادم الويب(Web Server).

- شبكة الند للند (Peer-to-Peer).

تكون الأجهزة في هذا النوع من الشبكات متكافئة، وبإمكان أيّ جهاز أن يكون خادمًا وعميلًا في الوقت نفسه.

البُنية	مميزاتها	عيوبها
الخطية	• انخفاض التكلفة • سهولة التركيب	• عطل أي جهاز على هذه الشبكة يعطل الشبكة كاملة. • قطع الكابل الرئيسي للشبكة يؤدي إلى تعطل الشبكة بالكامل. • صعوبة تحديد مكان العطل، بسبب ربط كل جهاز بالكابل المشترك مباشرة.
النجمية	• عطل جهاز أو أكثر لا يؤثر على باقي الأجهزة . • عطل كابل أو أكثر يؤدي إلى تعطيل الجهاز المتصل به فقط، ولا يؤثر على باقي الشبكة. • يمثل الموزع المركزي نقطة تحكم مركزية يتم من خلالها التحكم بالشبكة وإدارتها. • سهولة التوسع المستقبلي للشبكة. فلإضافة حاسب آلي جديد، فإننا نحتاج فقط إلى منفذ خالٍ في الموزع المركزي، وكابل من الجهاز الجديد إلى الموزع المركزي.	• التكلفة العالية مقارنة بالبنية الخطية لحاجتها إلى كابلات أكثر. • عطل الموزع المركزي يسبب تعطل الشبكة كاملة.
الحلقية	• تحتاج إلى كمية أقل من الكابلات مقارنة مع البُنية النجمية.	• في حالة حصول قطع في الكابل تتوقف الشبكة عن العمل. • في حالة حصول عطل في أحد الأجهزة، تتوقف الشبكة عن العمل. • لا تتوفر بسرعات عالية.
النجمية الشجرية	• عطل جهاز أو أكثر لا يؤثر في باقي الأجهزة . • عطل كابل أو أكثر يؤدي إلى تعطيل الجهاز المتصل به فقط، ولا يؤثر على باقي الشبكة. • يمثل الموزع المركزي نقطة تحكم مركزية، ويتم من خلالها التحكم في الشبكة وإدارتها. • سهولة التوسع المستقبلي للشبكة. • سهولة التركيب مقارنة بالنجمية.	• التكلفة العالية مقارنة بالبنية الخطية لحاجتها إلى كمية كابلات أكثر. • عطل الموزع المركزي يسبب تعطل كامل الشبكة.

الجدول(١-٦): مقارنة بين بنيات شبكات الحاسب الآلي.

١-٢-٦-٤ الإنترنت(Internet)

اصطلاح «الإنترنت»(Internet) هو اختصار للعبارة(International Network)، أي "الشبكة الدولية"[١]، وهي شبكـة ضخمة تضمّ الحواسيب المرتبطـة حول العالم. تتبادل هذه الحواسيب البيانات فيما بينها بواسطة تبديل رزم(حزم) البيانات(Packets)، باتباع بروتوكول الإنترنت الموحد(Internet Protocol-IP). ولتحديد الأجهزة المرتبطة بهذه الشبكة العملاقة، فإنّ كلّ جهاز موصول بها مباشرة يكون له عنوان خاصّ يسمّى عنوان الإنترنت(IP Address) وهذا العنوان عبارة عن رقم خاص يتكوّن من ٤ خانات، وكلّ خانة يمكن أن تكون أيّ رقم في المدى من الصفر إلى ٢٥٥(من (٠٠٠٠٠٠٠٠) إلى (١١١١١١١١) بنظام العد الثنائي)، وتكتب بهذه الطريقة(مثلًا)(١٠٤, ١٦١, ٢٣٣, ٦٤). وتقدّم الإنترنت كثيرًا من الخدمات، من أشهرها:

- خدمة مواقع الشبكة العنكبوتية العالمية(الويب World Wide Web-WWW)[٢].
- خدمات البريد الإلكتروني.
- خدمات نقل الملفّات(File Transfer Protocol – FTP).
- خدمات التخاطب أو المحادثة الآنية، وتشمل: المحادثة الكتابية(Chatting)، والمحادثة الصوتيّة، والمحادثة الفوريّة بالصوت والصورة(محادثات الفيديو).
- الخدمات الإلكترونيّة عن بعد، مثل خدمات الحكومة الإلكترونيّة، وخدمات التعليم عن بعد.
- خدمات التجارة الإلكترونيّة، وتشمل خدمات البيع والشراء إلكترونيًّا، والخدمات البنكيّة الإلكترونيّة.

تمثّل الإنترنت اليوم ظاهرة لهـا تأثيرها الاجتماعي والثقافي في جميع بقاع العالم، حيث أدّت إلى تغيير المفاهيم التقليديّة لعدّة مجالات، مثل: الاتصال، والتعليم، والتجارة، وإلى بروز شكل آخر للمجتمعات يسمّى المجتمع المعلوماتي.

١ إبراهيم، خالد ممدوح(٢٠٠٨)، «أمن المعلومات الإلكترونية»، ص ١٥.

٢ يقصد بالشبكة العنكبوتية شبكة الإنترنت، وإنما أطلق عليها هذا الاسم إشارة إلى خدمة المواقع(WWW).

طُرُق الاتصال بشبكة الإنترنت

للاتصال بشبكة الإنترنت، فإنّه يلزم توفير التجهيزات الخاصّة بذلك، وكذلك يلزم الاشتراك مع مزوّد خدمة الإنترنت(Internet Service Provider-ISP) المحلّي الذي سيعطي المشترك أولًا عنوان الإنترنت(IP Address)، الذي سيكون عنوانًا فريدًا يميّز المشترك من باقي المستخدمين لشبكة الإنترنت على مستوى العالم، ثمّ يوصل المشترك بشبكة الإنترنت العالميّة. هناك عدّة طُرُق يمكن من خلالها الاتصال بشبكة الإنترنت[1]، ولكلٍّ منها ميّزاته وعيوبه الخاصة به، وهي:

١. الاتصال عن طريق الاتصال(الطلب) الهاتفي(Dial-up): ويتم ذلك عن طريق الاتصال الهاتفي المباشر بمزوّد خدمة الإنترنت من خلال رقم هاتفي محدّد. وكلّ ما يحتاج إليه المستخدم في هذه الحالة هو خط تليفون عادي وجهاز حاسب آلي مزوّد بمنفذ للاتصال الهاتفي (RJ41) (مودم داخلي) وفي حال عدم توافر منفذ الاتصال الهاتفي في جهاز الحاسب الآلي، فإنّه يلزم استخدام جهاز مودم(Modem)[2] خارجي لتحويل بيانات الحاسب الآلي الرقميّة إلى إشارة تماثلية(Analog) يمكن نقلها على خط الهاتف، كما لو كانت إشارة صوت، وكذلك إجراء العملية العكسيّة للتحويل(من إشارة تماثلية إلى رقميّة). وغالبًا ما تقدّم شركات الاتصالات هذه الخدمة لكلّ المشتركين مباشرة، دون الحاجة إلى طلب الاشتراك من قبل المستخدم؛ لأنّها أصبحت خدمة أساسيّة، ويمكن للشركة احتساب تكاليفها مع فاتورة الهاتف مباشرة. وهذه الطريقة هي الأسهل والأقدم من بين كل الطرق، كما يسهل الحصول عليها، لكنّها تُعدُّ أبطأ الطرق سرعةً، حيث لا تتجاوز سرعة الاتصال فيها (٥٦) كيلوبت في الثانية. ومن عيوب هذه الطريقة أنّه لا يمكن استقبال أو إجراء مكالمة هاتفية أثناء الاتصال بالإنترنت، ويلزم في هذه الحالة قطع الاتصال بالإنترنت.

---

١ الغثبر، خالد بن سليمان و القحطاني، محمد بن عبد الله(٢٠٠٩)، «أمن المعلومات بلغة ميسرة»، ص ١٩.

٢ هذه التسمية هي اختصار لكلمتي التضمين(أو التحميل)(Modulation) وفك التضمين(Demodulation) باللغة الإنجليزية لتصبح(Modem) وتستخدم هذه العبارات كذلك للتعبير عن تحميل إشارة الصوت على الموجات الحاملة ثم فصلها عنها لدى المستقبل(المذياع) في البث الإذاعي.

٢. الاتصال عن طريق خطوط الاتصال الرقميّة(Digital Subscriber Line-DSL): ويتم ذلك عن طريق خطّ هاتفي رقمي(وليس عاديًّا تماثليًّا(Analog)) وجهاز موجّه صغير(Router) خارجي خاص بذلك. ويمكن أن يكون جهاز الموجّه لاسلكيًّا، كما أنّه يمكن أن يكون سلكيًّا(أو سلكيًّا/لاسلكيًّا في الوقت نفسه) يوصل بالحاسب الآلي من خلال منفذ الشبكات(RJ45). ويمكن ربط أكثر من جهاز حاسب آلي على الموجّه نفسه والخط نفسه في آنٍ واحدٍ معًا، وكذلك يمكن إجراء المكالمات الهاتفيّة وتصفّح الإنترنت على الخط نفسه في وقت واحد معًا، دون الحاجة إلى قطع الاتصال. تتوافر خدمة الإنترنت فور إيصال الموّجه بخط الهاتف الرقمي، دون الحاجة إلى القيام بأيّ عمليّة اتصال هاتفي، حيث إنّ جهاز الحاسب الآلي يكون على اتّصال مستمر مع مزوّد الخدمة، وتُوفَّر هذه الطريقة عن طريق مزوّدي خدمة الإنترنت، ويلزم الاشتراك في تلك الخدمة من قبل المستخدم، ويمكن الاشتراك بسرعات عالية من خلال هذه الطريقة تبدأ من(٦٤) كيلوبت لكل ثانية، وقد تصل إلى عدد من الميجابت لكل ثانية. تتميّز هذه الطريقة بتوفير السرعات العالية، إلّا أنّها تتطلّب الاشتراك لدى أحد مزودي خدمة الإنترنت، وتكاليفها أعلى من طريقة الطلب الهاتفي.

٣. الاتصال اللاسلكي عن طريق شرائح(كروت) الربط مع شبكات الهاتف الجوال: ويتمّ ذلك عن طريق بطاقة(كرت) خاصة مزوَّدة بشريحة هاتف جوال من الجيل الثالث(فأعلى) ويوصل مباشرة بالحاسب الآلي عن طريق أحد منافذ(USB). وتتميّز هذه الطريقة بسرعة الاتصال، حيث تصل في بعض الأحيان إلى ٧,٢ ميجابت لكل ثانية(في الوقت الراهن)، إلّا أنها تُعدُّ عالية التكلفة، ولا يمكن إجراء المكالمات الهاتفية من خلالها.

٤. الاتصال عن طريق الشبكة المحلية(LAN): ويتم ذلك عن طريق توفير خدمة الإنترنت مركزيًّا، وبثّ هذه الخدمة من خلال شبكة الحاسب الآلي المحلية، وعند دخول المستخدم للشبكة المحليّة يكون بإمكانه تصفّح شبكة الإنترنت مباشرة، دون أن يكون لديه أيّ تجهيزات أو خطوط خاصّة بذلك. وتطبّق هذه الطريقة -عادة- لدى

الشركات والجهات الحكوميّة التي لديها شبكات حاسب آلي محليّة، ولديها عدد كبير من مستخدمي الإنترنت، وتشترك الشركة أو الجهة الحكوميّة مع أحد مزودي خدمة الإنترنت، وغالبًا ما تكون بطريقة خطوط الاتصال الرقميّة(DSL)، وبسرعات عالية تستطيع تلبية حاجة موظفيها. تتميّز هذه الطريقة بسهولة حصول الموظّف عليها ، إلّا أنّها عالية التكلفة، وتحتاج إلى عمليّات إدارة معقّدة من الشركة أو الجهة الحكوميّة، وقد يوجد في هذه الطريقة بعض التقييد للموظف؛ إذ قد لا يكون بمقدوره تصفّح جميع المواقع، وقد لا تتوافر له خدمة الإنترنت في جميع الأوقات، بحسب السياسة الأمنيّة لاستخدام الإنترنت المطبّقة لدى الشركة أو الجهة الحكوميّة.

٥. الاتصال عن طريق الأقمار الصناعية: ويتم ذلك عن طريق طبق استقبال(دش) مزوّد برأس خاصّ بهذه الخدمة، وموجّه إلى القمر الصناعي المراد الاتصال عن طريقه، وكرت استقبال يوصل بالحاسب الآلي، ونظام تشغيل يدعم استقبال الإنترنت عن طريق الطبق. وتتميّز هذه الطريقة بسرعة الاتصال، إلّا أنّها عالية التكلفة، وتعدُّ أقل أمانًا من الطّرق الأخرى.

المتصفّحات(Browsers)

هي برامج معدّة خصيصًا لتصفّح الإنترنت، بحيث تعطي إمكانيّة إدخال عنوان الصفحة(URL)، ومن ثم تعرض محتوياتها، ويسمح المتصفح للمستخدم باستعراض النصوص والصور والملفّات، وأيّ محتويات أخرى مختلفة في أيّ موقع، طالما أنّها تتبع اللغة القياسيّة العالميّة(Hyper Text Markup Language-HTML). ويتيح المتصفّح للمستخدم الوصول إلى المعلومات الموجودة في مواقع الإنترنت بسهولة وسرعة عن طريق تتبع الروابط(Links)، سواءً أكانت في الموقع نفسه أو في مواقع أخرى. وهناك العديد من المتصفّحات المشهورة مثل متصفح إكسبلورر(Explorer)، ونيتسكيب(Netscape)، وأوبيرا(Opera)، وفايرفوكس(Firefox).

تجدر الإشارة إلى احتماليّة وجود ثغرات أمنيّة إمّا في المتصفحات نفسها أو في أنظمة

التشغيل، تجعل الدخلاء يتمكّنون من الوصول إلى المعلومات الشخصيّة، أثناء تصفّح المستخدم للإنترنت وهو لا يشعر، ولا يكتشفها المتصفّح.

بروتوكول النص الفائق(HTTP)

بروتوكول النص الفائق(HTTP- Hypertext Transfer Protocol)، هو البروتوكول المستخدم لنقل مكوّنات صفحات الإنترنت وتبادلها(نصوص، وصور، وأفلام، وروابط، ... إلخ) باستخدام لغة HTML، ويتميّز بقدرته على نقل هذه المكوّنات بسرعة كبيرة، وهذا يعني تصفّحًا أسرع للإنترنت. ويمكّن بروتوكول النص الفائق مواقع الإنترنت والمتصفّح من الاتّصال وتبادل الوثائق والصور والصوت والمكوّنات الأخرى، إلّا أنّه تجدر الإشارة إلى أنّ هناك بعض الجوانب في بروتوكول النص الفائق، تجعل من الممكن تتبّع نشاطات المستخدم أثناء تصفّحه الإنترنت بدون علمه.

النطاق(Domain)

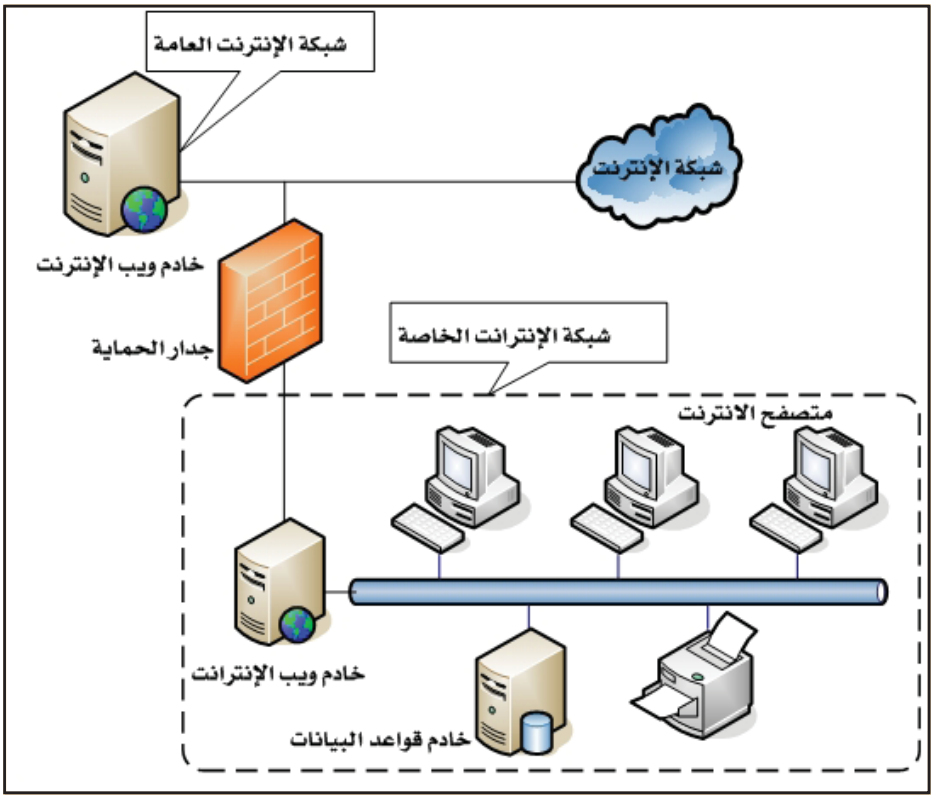
اسم النطاق(Domain Name)، هو اسم النص المصاحب لعنوان بروتوكول الإنترنت(IP) لأي موقع على الإنترنت. ويوجد لكل موقع على الإنترنت اسم نطاق خاص به لا يتكرر. فمثلًا، اسم النطاق(www.google.com) هو موقع محرك البحث الشهير جوجل، ويقابله عنوان الإنترنت(١٠٤ , ١٦١ , ٢٣٣ , ٦٤) الخاص به. وسواءً كتبت اسم النطاق أو عنوان الإنترنت في خانة العنوان في المتصفّح، فسوف تحصل على الصفحة نفسها.

يُعدُّ نظام اسم النطاق مفيدًا لعدّة أسباب، أكثرها وضوحًا أنّه يجعل من الممكن استبدال عناوين(IP) الصعبة التّذكر، مثل(١٠٤ , ١٦١ , ٢٣٣ , ٦٤)، بأسماء نطاقات سهلة التذكر، مثل(www.google.com) وهذا يسهّل على المستخدمين التّعامل مع عناوين الإنترنت وعناوين البريد الإلكتروني. كما أنّ النظام يسمح بإنشاء أسماء معترف بها ويمكن الوصول إليها بسهولة، والمصطلح الفني لعنوان صفحة ما في أي موقع على شبكة الإنترنت هو ما يعرف "بالرابط"، ويعبَّر عنه في اللغة الإنجليزية بـ(URL-Uniform Resource Location) فمثلًا (http://www.google.com.sa/advanced__search?hl=ar) هو الرابط أو(URL)

لصفحة البحث المتقدّم في موقع جوجل.

١-٢-٦-٥ الإنترانت(Intranet)

هي شبكة حاسب آلي محليّة خاصّة بالمنشأة، لكنها تستخدم بروتوكول الإنترنت(Internet protocol) وتقنيات الإنترنت كخوادم وبرامج الويب، لتقديم خدماتها وبرامجها الداخليّة الخاصّة بالمنشأة. وقد تكون الإنترانت غير مرتبطة بالإنترنت نهائيًّا، لكن في حالة الارتباط بها يجب أن يفصل بينهما جدار حماية(Firewall)، انظر الشكل(١-٦). وعلى ذلك، فإنّ الإنترانت هي شبكة غير ظاهـرة أو غير ممكن الوصول إليها بالنسبة للعالم الخارجي، غير أنّه يمكـن عدُّها شبكة إنترنت خاصّـة بالمنشأة؛ للتشابه الكبير بينهـا وبين شبكة الإنترنت، واستخدامها للتقنيات نفسها، لكن على مستوى محلّي مغلق على المنشأة.



الشكل(١-٦): شبكة الإنترانت

يمكن أن تحتوي شبكة الإنترانت موقعًا أو بوابة داخلية للمنشأة، كما يمكن تقديم برامج وخدمات(ويب) من خلالها، مطابقة تمامًا لتلك الموجودة على شبكة الإنترنت العالمية، مثل[1]:

- خدمات تصفّح الصفحات والمواقع والبوابات الداخليّة.
- البريد الإلكتروني الداخلي.
- نظام نقل الملفّات(FTP) الداخلي.

أنظمة المحادثات الصوتيّة والمرئيّة والكتابيّة داخل المنشأة.

١-٢-٦-٦ الإكسترانت(Extranet)

في حال السّماح للمستخدمين من شبكات أخرى خارج المنشأة بالدخول إلى شبكة الإنترانت الداخليّة للمنشأة؛ فإنّها تصبح بذلك شبكة إكسترانت، فالإكسترانت ما هي إلا شبكات إنترانت مرتبطة مع بعضها بعضًا باستخدام تقنية الشبكات الخاصّة الافتراضيّة(VPN) عبر شبكة الإنترنت، انظر الشكل(١-٧). وتبقى شبكات الإنترانت في شبكة الإكسترانت محمية بجار الحماية(Firewall)، الذي يمكن من خلاله التحكم بوصول المستخدمين من شبكة الإكسترانت إلى موارد الإنترانت الداخليّة.

وقد أتاحت شبكة الإكسترا نت للمنشآت أن تتشارك في أنظمتها وشبكاتها المحلية، وإن كانت متباعدة جغرافيًا، وبأقل تكلفة ماديّة ممكنة. كما أتاحت كذلك التعامل والتواصل الجيد مع مورّدي الأنظمة والخدمات بشكل ممتاز، لكن كل ذلك مقرون ببعض المخاطرة بأمن المعلومات[2].

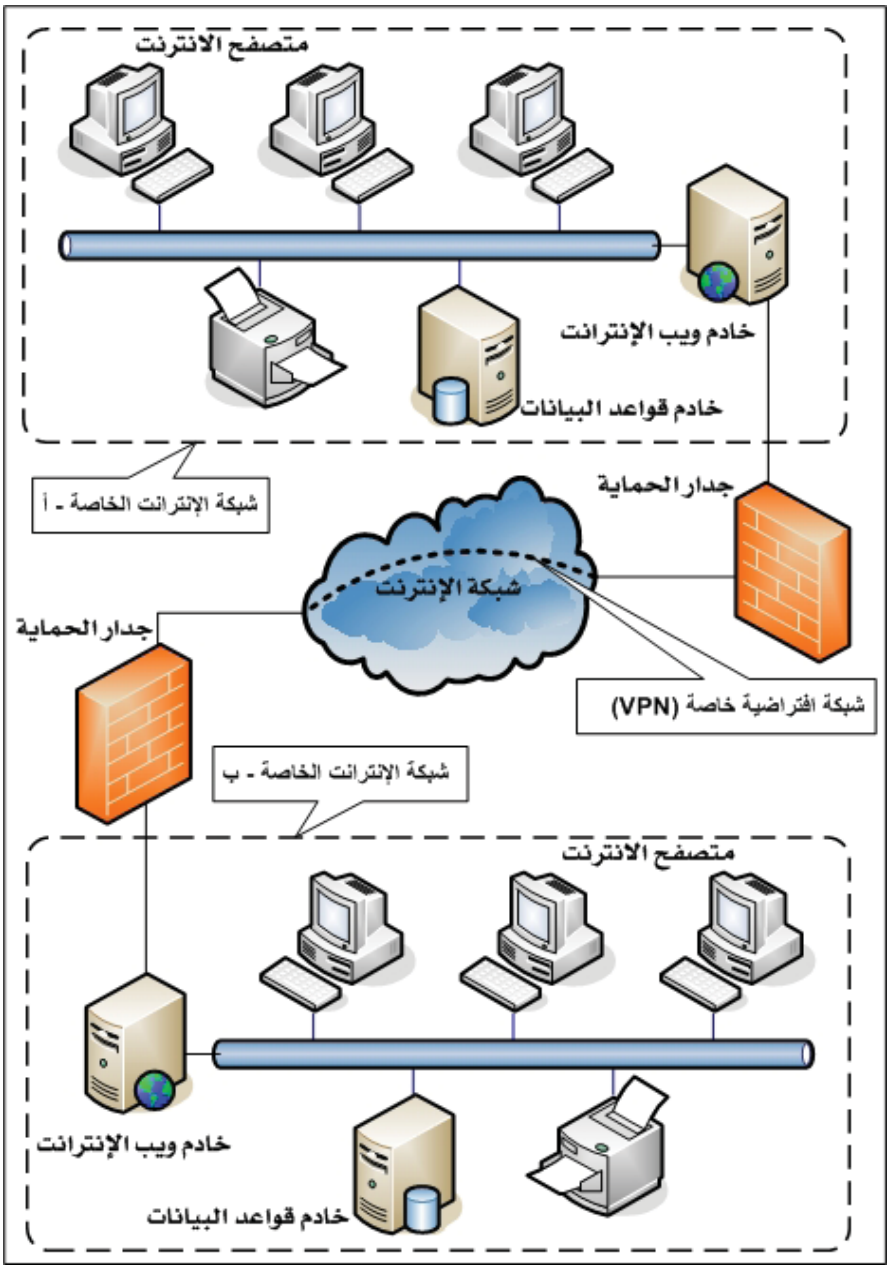
١-٢-٦-٧ الحوسبة السحابية(Cloud Computing)

كثير منّا يحتاج إلى تركيب أنظمة التشغيل والبرامج التطبيقيّة على جهازه الخاص لاستخدامها في أعمالة اليوميّة الرقميّة، كإعداد الوثائق، وكتابة الخطابات، وإرسال البريد الإلكتروني واستقباله ، وتصفّح الإنترنت، والتواصل مع الآخرين. والسؤال المطروح هنا: لماذا

---

١ داود، حسن طاهر(٢٠٠٤ب)، «أمن شبكات المعلومات»، ص ٣٦-٣٧.

٢- داود، حسن طاهر(٢٠٠٤ب)، «أمن شبكات المعلومات»، ص ٨٤



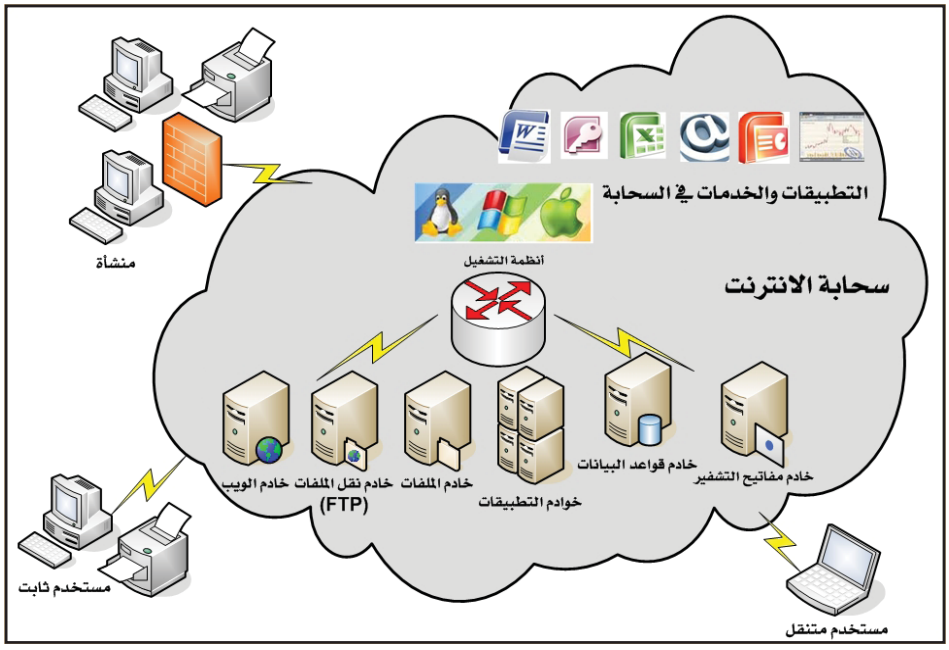
الشكل (١-٧): شبكة الإكسترانت

يضطر المستخدم إلى شراء هذه الأنظمة والبرامج والخدمات وتملّكها بشكل دائم وتحديثها وصيانتها على الرغم من أنه لا يحتاج إليها كلّ الأوقات، بل قد لا يحتاج إلى كثير من أجزائها وإمكانياتها المتقدّمة التي يدفع ثمنها ولا يستخدمها؟ والجواب عن هذا السؤال هو استخدام

تقنية الحوسبة السحابيّة. ففي الحوسبة السحابيّة، تُشبَّـه الإنترنت بأنها سحابة توجد بها جميع تلك الأنظمة والبرامج والخدمات، وكل ما يحتاج إليه المستخدم هو الأخذ منها بالقدر الذي يحتاج إليه فقط، تاركًا مهمّة التّطوير والتحديث والصيانة للسحابة.

بشكل عام يمكن تعريف الحوسبة السحابية بأنهـا: «تقديم الأنظمة والبرامج والعمليّات الرقميّة المختلفة كخدمات(Services) عبر الإنترنت، وليس كمنتجات(Products) مستقلّة يلزم وجودها لدى المستخدم" انظر الشكل(١-٨). يمكن تشبيه خدمات الحوسبة السحابيّة بخدمات تقديم الطاقة الكهربائيّة، حيث يمكن للمستفيد الحصول على الطاقة مباشرة دون الاكتراث بطريقة توليدها، ومن أين تأتي؟ ومن يديرها ويقوم على صيانتها؟

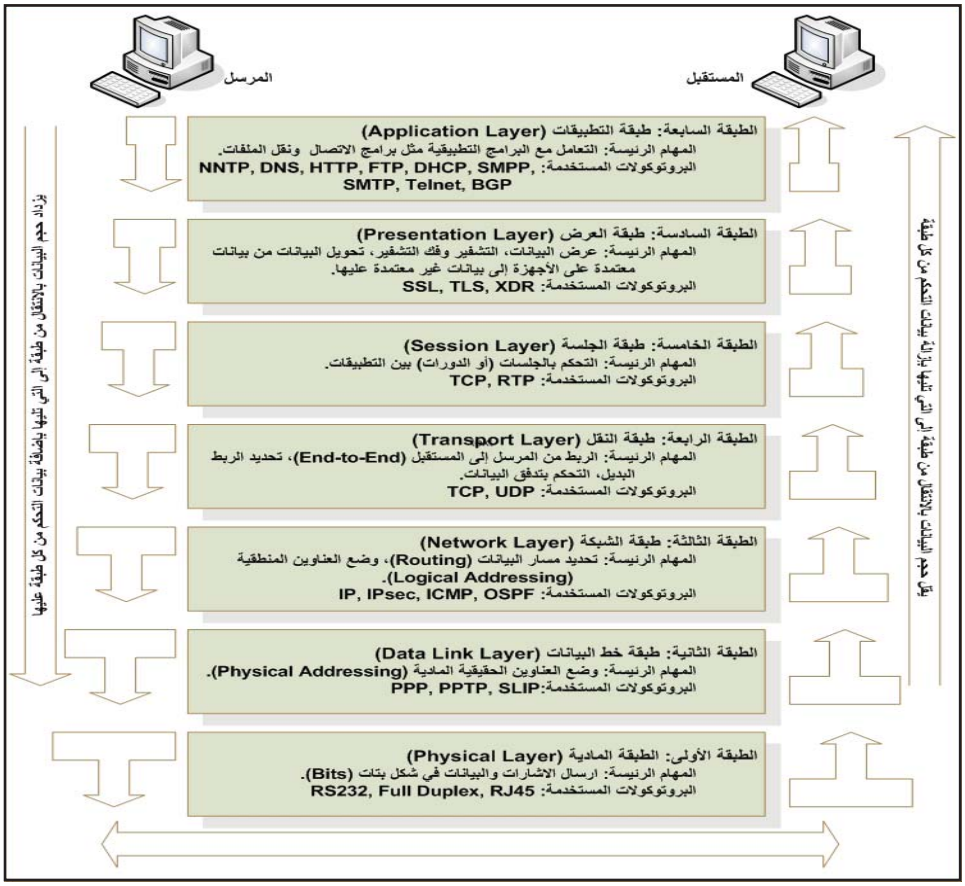
تدعم تقنية الحوسبة السحابيّة حرّية التنقّل للمستخدم(حول العالم)، مع استمراره في أداء أعماله الإلكترونيّة من أيّ مكان، في ظلّ وجـود جميع ما يحتاج إليه من أجهزة وأنظمة وبرامج وخدمات في السحابة، كما أنّها طريقة مثلى للتخلص من إدارة تلك المكوّنات وصيانتها والتركيز على عمله الأساسي.



الشكل(١-٨): الحوسبة السحابية.

١-٢-٦-٨ طبقات الشبكات (Network Layers)

استحدثت المنظمة العالمية للقياس (International Organization for Standardization-IOS) نظام الربط البيني المفتوح (Open System Interconnection-OSI- Model)[١]، وهو نظام قياسيّ عالميّ لتنظيم عمل شبكات الحاسب الآلي، وفق طبقات من البروتوكولات، يتم من خلالها التوافق والتفاهم بين الشبكات لدى ارتباطها ببعضها بعضًا. ويتكوّن نظام الربط البيني المفتوح (OSI) من سبع طبقات (لدى كلّ من المرسِل والمستقبِل) تتعامل كل طبقة مع التي فوقها، والتي أسفل منها، وتدفع كلّ طبقة البيانات إلى التي أسفل منها في حالة الإرسال، وإلى التي أعلى منها في حالة الاستقبال، انظر الشكل (١-٩).



الشكل (١-٩): الطبقات السبع في نظام الربط البيني المفتوح (OSI).

١- Shon Harris (2008) "All-in-One CISSP Exam Guide", Fourth Edition, p 483.

وتختص كل طبقة بمهام محدّدة، وتستخدم بروتوكـولات مخصّصة لتنفيذ هذه المهام، كما هو موضّح في كل طبقة في الشكل (١-٩).

عند مرور حزم البيانات (Packets) من الطبقة السابعة إلى الطبقة الأولى لدى المرسِل تُضاف بيانات التحكّم الخاصّة بكلّ طبقة إلى تلك الحزم في خانة الرأس (Header)، ومن ثَمَّ يزداد حجمها، وعند مرور هذه الحُزم من الطبقة الأولى إلى الطبقة السابعة لدى المستقبل تُزال بيانات التحكّم بـكّل طبقة لدى مرور الحُزمة بالطبقة، حتّـى وصولها إلى المستقبِل في شكلها الأصلي الذي كانت عليه لدى المرسِل.

تؤدي طبقات الشبكات وفق هذا النظام دورًا بارزًا في تحديد أجهزة وبرامج أمن المعلومات المناسبة لكل طبقة، بحيث أصبح هناك أجهزة وبرامج مخصّصة لكلّ طبقة، كما سيأتي معنا في الفصلين: الثاني، والسابع.

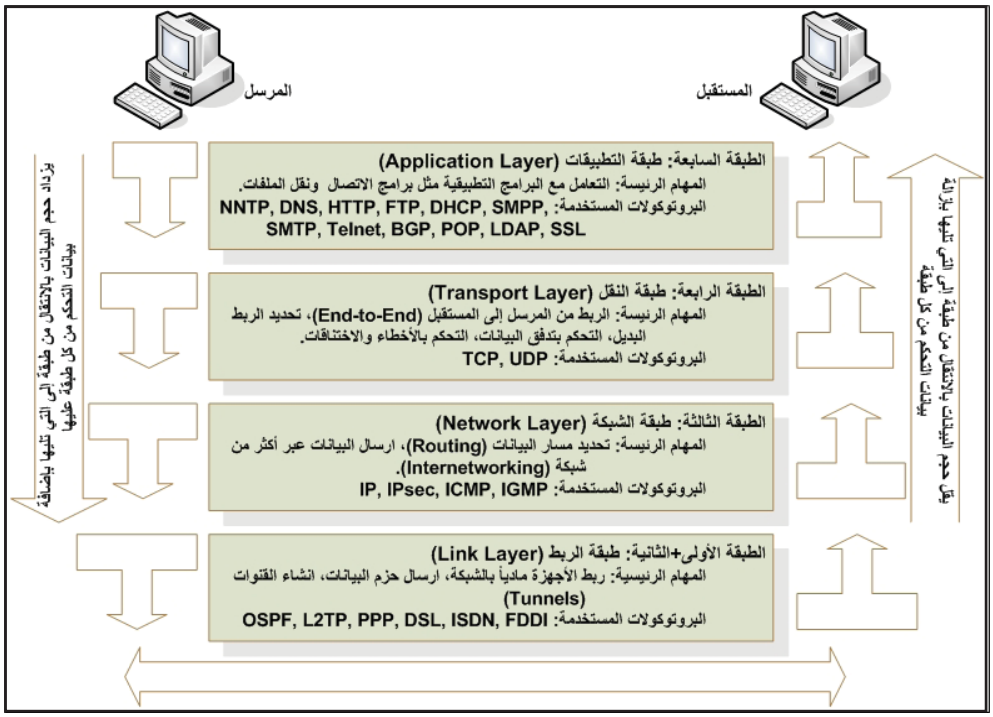
بروتوكول التحكم بالنقل (Transport Control Protocol/Internet Protocol-TCP/IP)

هو حزمة مـن البروتوكولات التـي تتحكّم بنقل البيانـات في شبكة الإنترنـت والشبكات المشابهة لها مثل: شبكات الإنترانت والاكسترانت. وهذه الحزمة كافية للتحكّم بنقل البيانات من المُرسِل إلى المُستقبِل بشكل كامل عبر شبكة الإنترنت والشبكات المشابهة لها، وتستخدم هذه الحُزمة أربع طبقات من طبقات نظام الربط البينـي المفتوح (OSI) مع بعض التعديل البسيط، حيث دُمجت الطبقة الماديّة (Physical Layer) مع طبقة خط البيانات (Data Link Layer) في طبقة واحدة، أطلق عليها اسم طبقة الربط (Link Layer)، و غُيّر اسم طبقة الشبكة (Network Layer) إلى طبقة الإنترنت (Internet Layer)، انظر الشكل (١-١٠)[١].

ملخص الفصل

يُعدُّ هذا الفصل مقدّمة لعلم أمن المعلومات، حيث يحتوي المصطلحات والمفاهيم الأساسيّة المتعلّقة بالمعلومات، ومكوّنات أنظمة المعلومات التي تقوم بمعالجة المعلومات وإجراء العمليّات الرئيسة عليها، وهي: الحفظ، والمعالجة، والإرسال.

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition, 503.



الشكل(١-١٠): طبقات الإنترنت الأربع وبروتوكول التحكم بالنقل TCP/IP.

فجرى تعريف البيانات والمعلومات والفرق بينهما، وحُدّدت مكوّنات أنظمة المعلومات الرئيسة: المكوّنات الماديّة، والبرامج، والبيانات، والمستخدمين، والإجراءات، وشبكات المعلومات، التي تُعدُّ أهدافًا رئيسة لأمن المعلومات، وقد شُرحت هذه المفاهيم والمكوّنات بالقدر الكافي لبناء الخلفيّة النظريّة التي يمكن بعدها البدء في البحث في علم أمن المعلومات وطرق تطبيقه وآلياته. فمّما تضمّنه هذا الفصل تعريف نظام التشغيل والمهام الأساسيّة التي يؤدّيها، وشرح طُرُق تمثيل البيانات داخل الحاسب الآلي، والتعرّف إلى وحدات القياس الأساسيّة المستخدمة في قياس السرعات، وقياس سعات وحدات التخزين المختلفة. كما قـدّم هذا الفصل مدخلًا لشبكات الحاسب الآلي، وأهدافها، وبنياتها، وأنواعها، وطرق الاتصال بها، والخدمات الأساسيّة التي تقدمها، وطبقاتها، والبروتوكولات المستخدمة فيها.

مسائل

١. عرف البيانات والمعلومات. وما الفروق بينهما؟

٢. رتّب مكوّنات أنظمة المعلومات حسب أولوية كل منها لتطبيق أمن المعلومات عليه، موضحًا السبب في هذا الترتيب لكلّ مكوّن.

٣. ما المكوّن المادي الذي يؤثر تأثيرًا مباشرًا في سرعة الحاسب الآلي؟ وما المكوّن المادي الذي يؤثر تأثيرًا مباشرًا في قدرة الحاسب الآلي على تشغيل أكثر من برنامج تطبيقي في الوقت نفسه؟ اشرح كيف يكون ذلك.

٤. ما الفرق بين الذاكرة العشوائية(RAM)، والذاكرة القرائيّة فقط(ROM)، والذاكرة القلميّة(Flash)؟ أيها أكثر عرضة لتهديدات أمن المعلومات؟ ولماذا؟

٥. ما الفرق بين الذاكرة العشوائيّة والقرص الصلب من حيث: السّعة والسرعة والاستخدام؟

٦. يتم تمثيل جميع البيانات داخل الحاسب الآلي باستخدام النظام الثنائي. فما هذا النظام؟ وما الفرق بينه وبين النظام السِّت عشري؟

٧. ما الهيرتز؟ ولماذا لا تقاس سرعة إرسال البيانات بالهيرتز؟

٨. عرّف نظام التشغيل، ثم عدد المهام الرئيسة التي يقوم بها.

٩. ما الفرق بين الملف والمجلّد؟ ولماذا تختلف أنواع الملفّات، بينما هناك نوع واحد من المجلدات؟

١٠. ما البرامج التطبيقيّة؟ أعط أمثلة لها.

١١. أيهما أخطر: الهجوم على نظام التشغيل أم على برنامج تطبيقي؟ ولماذا؟

١٢. عرّف شبكات الحاسب الآلي، ثم عدد البُنيات الرئيسة لها. ما أحدث هذه البُنيات؟ ولماذا؟

١٣. قارن بين بُنيات شبكات الحاسب الآلي من حيث مميزات وعيوب كلّ منها، ثم رتّبها

حسب صلاحيّة كل منها لمنشأة كبيرة الحجم.

١٤. ما عنوان الإنترنت؟ ولماذا يكون عنوانًا فريدًا؟ أعط خمسة أمثلة لعناوين حقيقية داخل المملكة العربيّة السعودية وخارجها.

١٥. عدّد طُرُق الاتصال بشبكة الإنترنت، ثم قارن بينها من حيث سهولة الحصول عليها وسرعتها وتكاليفها ومناسبتها من حيث أمن المعلومات.

١٦. ما الخدمات التي يقدّمها كلّ من: شبكة الإنترنت، والإنترانت، والإكسترانت؟ ثم عدّد الفروق بين تلك الشبكات.

الفصل الثاني

لماذا أمن المعلومات؟

أهداف الفصل:

- التعريف بأمن المعلومات.
- توضيح الحاجة إلى أمن المعلومات، وأنّها ضرورة ملحّة، وليست حلولًا اختياريّة.
- التعرّف إلى تهديدات أنظمة أمن المعلومات، كأحد الأسباب الرئيسة للحاجة إلى أمن المعلومات.
- التعرّف إلى الهجمات الإلكترونيّة وخطورتها على المعلومات والأنظمة المعالجة لها، مع إبراز الحاجة إلى أمن المعلومات لمجابهتها.

ما ستتعلمه في هذا الفصل

- تعريف أمن المعلومات.
- المحاور الرئيسة لمفهوم أمن المعلومات.
- الأسباب الرئيسة(الخمسة) وراء الحاجة إلى أمن المعلومات.
- تهديدات أمن المعلومات والأنظمة المعالجة لها: تهديدات فنية، وتهديدات بشرية، وتهديدات طبيعيّة.
- الهجمات الإلكترونيّة والحاجة للحماية منها.
- خطورة الهجمات الإلكترونيّة ليس فقط على معلومات المنشآت بل على بقاء بعضها واستمراره(قد تكون سببًا لانهيار المنشأة أو اختفائها).

لماذا أمن المعلومات

٢-١ مقدّمة

تـزداد الاعتماديّة على حلـول تقنية المعلومـات يومًا بعد يـوم في تسيير أعمـال المنشآت الخاصة والعامّة على حدٍّ سواء، بـل تعدّى الأمر ذلك إلى المستوى الفردي، فأصبح كثير من الناس يمتلك جهازه الخاصـ به(محمولًا أو مكتبيًّا أو كفّيًّـا) لأداء أعماله المختلفة وتصفّح شبكة الإنترنت. ويمكن أخذ الحكومة الإلكترونيّة وما تقدّمه من خدمات للمواطنين والمقيمين والهيئات والمنظمات الداخليّة والخارجية كمثـال للاعتماديّة العالية على تقنية المعلومات في تقديم هذه الخدمات من جهة، والاستفادة منها من جهة أخرى. فمقدّمو الخدمات الحكوميّة الإلكترونيّـة يحتاجون إلى مراكز البيانـات(Data Centers) الكبيرة المتكاملة من خوادم وأجهزة تخزين وربط بالشبكات المحلية(WAN) والواسعة(LAN) والإنترنت، والمستفيدون يحتاجون إلى أجهزة الدخـول إلى مواقع الخدمة، ويحتاجون إلى وسائل الارتباط بالإنترنت للحصول على تلك الخدمات.

لو أنّ تلك الحلول والخدمات الإلكترونيّة خالية من التهديدات وآمنة طوال الأوقات لكان الأمر في منتهى الروعة والجمال، ولزاد التوسّع في تقـديم المزيد من الخدمات الإلكترونيّة، ولاتّسعت رقعة الإقبال عليها من جميع الأوساط، وقبل هذا لأمكن توجيه الأموال الطائلة التي تُصرف في توفير وسائل الحمايـة إلى توفير خدمات إضافيّة وزيـادة مساحة التغطية بتلك الخدمات. لكن ما يحدث هـو أنّ تلك الحلول والخدمات تتعامل مع معلومات حسّاسة وبالغة الأهميّة، وفي الوقت نفسه تكـون معرّضة لكثير من التهديدات، بل أثبتت الدراسات الحديثة نجاح اختراقات كثيرة لتلك الأنظمة وتعطيلها، أو التعدّي على معلوماتها.

إذاً فأمـن المعلومات ضرورة ملحّة، وليست حلًا اختياريًّا، بـل يمكن القول إنّ أيّ مشروع يتضمن حلًا تقنيًّا لا بدّ أن يرافقه مشروع توأم لأمن المعلومات، أو أن يشتمل على التجهيزات اللازمة لحماية المعلومات التي يجري التعامل معها ومعالجتها ونقلها من خلال ذلك المشروع.

يقدّم هـذا الفصل الإجابة عن السؤال الكبير: "لماذا أمـن المعلومات؟" أو "ما الحاجة

إلى أمن المعلومات؟". فيجيب مـن خلال التعريف بأمن المعلومات والمحاور التي يشملها، ثم توضيح أهميّة أصول المعلومات الحرجة التي يجب حمايتها، وما تشكّله من قيم ماديّة أو معنويّة أو خدميّة، ثم استعراض التهديدات المحيطة بها، وأنواع الهجمات التي يجب التصدي لها.

٢-٢ التعريف بأمن المعلومات

إنّ علم أمن المعلومات هو العلم الذي يُعنى بحماية المعلومات من المخاطر التي قد تتعرّض لها. ويمكـن تعريف أمن المعلومات بشكل مختصر بأنه: «حمايـة المعلومات من الوصول غير المسموح به». ويمكن تعريفه بتفصيل أكثر بأنه: «المفاهيم والتقنيات والتدابير التقنية والإداريّة المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمدًا أو سهوًا أو حيازتها أو الإضرار بها، أو كشفها، أو التلاعب بها، أو تعديلها، أو فقدها أو إساءة استخدامها»[١]. تعرّف لجنة أنظمة الأمن القومي الأمريكية(Committee on National Security Systems-CNSS)[٢] أمن المعلومات بأنه: «حماية المعلومـات وعناصرها المهمة(الحرجة) بما في ذلك الأنظمة والأجهزة التي تَستخدِم هذه المعلومات وتخزنهـا وترسلها»[٣]. ويُعدُّ هذا التعريف هو التعريف الأنسب؛ لشموليته للمعلومات بأشكالهـا وعناصرها كافة، التي من أهمّها الأجهزة والأنظمة(البرامج) التي تخزّن هذه المعلومات وتعالجهـا وترسلها، وبهذا يتّسع مفهوم أمن المعلومات ليشمل المحاور الآتية:

- حماية المعلومات من الضرر بأشكاله كافة، سواءً أكان مصدره أشخاص(كالمخترقين)، أم برامج(كفيروسات الحاسب الآلي)، وسواءً أكان متعمّدًا أم عن طريق الخطأ.
- حماية المعلومات من الوصول غير المصرّح به، أو السرقة، أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستخدام.
- حماية قدرة المنشأة على الاستمرار وأداء أعمالها على أحسن وجه.
- تمكين أنظمة تقنيّة المعلومات والبرامج التطبيقيّة لدى المنشأة من العمل بشكل آمن.

---

١ McDaniel, George(1994), "IBM Dictionary of Computing".

٢ كان يطلق عليها اسم لجنة الأمن القومي لأمن الاتصالات وأنظمة المعلومات(National Security Telecommunications and Information Systems Committee(NSTISSC)).

٣ Withman, M. and Mattord, H.(2005), "Principles of Information Security".

٢-٣ الحاجة لأمن المعلومات

كما أوضحنا سابقًا، فإنّ أمن المعلومـات ليست ترفًا ولا حلولًا وإجراءات اختياريّة، وإنّما ضرورة مُلحّة ظهرت الحاجة إليها من خلال الأسباب الآتية[١]:

١. حماية الأصول المعلوماتيّة الحرجة: إذ لا تقوم تقنية المعلومات في المنشأة، ولا الخدمات التي تقدّمها تلك المنشأة، إلّا على أصول معلوماتيّة مهمّة وحرجة يجب حمايتها من أيّ أخطار تهددها، ويجب المحافظة على استمراريتها وبقائها متاحة متوافرة في جميع الأوقات. فالحاجة لحماية هذه الأصول تأتي من وجهين: الوجه الأوّل أنّه لا يمكن للمنشأة أن تستمرّ دون بقاء هذه الأصول عاملة متاحة آمنة، والوجه الآخر أنّ توفير هذه الأصول كلّف مبالغ وجهودًا كبيرة تستحقّ أن يُبذل من أجلها الوقت والجهد والمال لحمايتها، ومن الأمثلة على الأصول المعلوماتيّة الحرجة ما يلي:
   - مراكز البيانات(Data Centers).
   - قواعد البيانات(Databases).
   - أجهزة الخوادم الرئيسة(Severs).
   - شبكات المعلومات المحلية(LAN) والواسعة(WAN).
   - أنظمة التشغيل(Operating Systems).
   - البرامج التطبيقيّة(Application Programs).
   - أجهزة تخزين المعلومات(Storage Devices).
   - المواقع والبوابات الإلكترونيّة سواءً داخلية أو على شبكة الإنترنت.

٢. حاجة أعمال المنشآت وأنشطتها إلى ذلك: حيث أصبحت المعلومات تشكّل ثروة حقيقيّة للمنشآت ومواردًا مهمًّا من مواردها، بل إنّ المعلومات في بعض المنشآت هي مصدر الدّخل الأول لها، ويقوم عليها نشاط المنشأة الأساسي، والتجارة الإلكترونيّة خير مثال لذلك.

٣. حاجة المستفيدين من الخدمات الإلكترونيّة إلى ذلك: ومعنى ذلك أنّ المستفيدين

---

١ Withman, M. and Mattord, H.(2005), "Principles of Information Security", Second Edition, p 35-38

من الخدمات الإلكترونيّة بحاجة إلى حماية معلوماتهم من كلّ ما يضرّ بها. فالمعلّم بحاجة إلى حماية معلوماته التي يستخدمها في أداء عمله، حتى ولو على المستوى الشخصي، وكذا الطبيب، والمهندس، والأستاذ الجامعي، ورجل الأعمال، والشخص العادي، كلّهم بحاجة إلى حماية معلوماتهم التي يملكونها. عندما يُنهي شخص تعاملاته البنكيّة أو يشتري سلعة من منزله، فإنّه لا بدّ أن يعتمد على أمن المعلومات في المحافظة على خصوصيته (كمعلوماته الخاصة في جهازه الشخصي) أولًا، وثانيًا على ممتلكاته (الإلكترونيّة)، كاسم المستخدم، وكلمة المرور، ومعلومات البطاقة الإئتمانيّة.

٤. انتشار الخدمات الإلكترونيّة عن بعد: مثل خدمات الحكومات الإلكترونيّة والتعليم عن بُعد، لدرجة أنّ المواطن يستطيع أن يُنهي جلّ أو جميع إجراءاته، وأن يحصل على درجته العلمية المناسبة من منزله. ولإتمام هذا النوع من الخدمات فلا بدّ من توفير الحماية اللازمة للمعلومات ولجميع الأنظمة والتجهيزات التي تخزّنها أو تعالجها أو تنقلها لدى كل من مقدِّم الخدمة والمستفيد على حدٍّ سواء.

٥. الحاجة إلى معرفة إمكانيّات المنشآت ومدى قدرتها على حماية معلوماتها ومعرفة التهديدات التي تواجهها: فلكي تكون آمنًا، فلا بدّ أن تعرف نفسك، وتعرف التهديدات التي تواجهك. ومن هنا جاءت الحاجة إلى أمن المعلومات التي من خلالها يمكن تقويم وضع الحماية في المنشأة، ومعرفة التهديدات التي تواجهها، وتحليل المخاطر المحيطة بها، من أجل أخذ التدابير اللازمة لمجابهة تلك التهديدات والمخاطر.

٦. كثرة التهديدات المعلوماتيّة وتنوّعها، وتعدّد مصادرها: والخطورة في ذلك أنّه قد توجد جُملة من التهديدات داخل المنشأة، في أنظمتها المعلوماتيّة أو في موظّفيها، إذا لم يُحتاط لها فقد تضر بالمعلومات. ولأهميّة ذلك فقد أفردتُ له موضوعًا مستقلًّا، (هو الموضوع الآتي).

٧. انتشار الهجمات الإلكترونيّة: ما انفكّت وسائل الإعلام- على اختلاف أنواعها- تطالعنا من حين إلى آخر بالمزيد من أخبار الهجمات الإلكترونيّة، واختراق الشبكات، وتدمير

الأنظمة، وظهور فيروسات الحاسب الآلي، كان آخرها الخبر الذي نشرته صحيفة الرياض الإلكترونيّة (الرياض.نت) على موقعها بشبكة الإنترنت في ٣١ مايو ٢٠١٢م عن ظهور فيروس "فليم"[١] . وهذا أحد أهم الأسباب الرئيسة للحاجة إلى أمن المعلومات، ولأهميّة ذلك فقد أفردت له موضوعًا مستقلًا في هذا الفصل، نتعرف من خلاله إلى تلك الهجمات وأنواعها.

٢-٤ تهديدات المعلومات وأنظمتها

قبل أن نتعرف إلى كيفيّة توفير الأنظمة اللازمة لحماية المعلومات يجب أن نتعرف أولًا إلى التهديدات المحيطة بالمعلومات والأنظمة والتجهيزات التي تتعامل معها، إمّا بتخزينٍ أو معالجةٍ أو نقلٍ. فهناك تهديدات كثيرة تحيط بأنظمة المعلومات شأنها في ذلك شأن أيّ نظام مفتوح يمكن الوصول إليه بعدّة طُرُق، ومن قِبل أشخاص مختلفين وفي أوقات مختلفة. تتعدّد هذه التهديدات وتتنوّع بتنوّع هياكل الأنظمة المعلوماتيّة ونقاط الضعف فيها، ويمكن تقسيم تهديدات أمن المعلومات إلى ثلاث فئات رئيسة تحتوي كل فئة منها عددًا كبيرًا من التهديدات التي تشترك في خصائص عامة واحدة، وهذه الفئات هي:

٢-٤-١ تهديدات فنية

وهي التهديدات الناجمة عن القصور والأخطاء الفنية في مختلف أنظمة أمن المعلومات، والتي يغلب عليها الطابع الفني، دون أن يكون هناك أي تدخل بشري، أو أن تكون بسبب كارثة طبيعيّة، ومنها:

تهديدات عيوب التصميم والتشغيل

وتشمل عيوب التصميم في الأجهزة والبرامج والشبكات وأدوات الربط والتخزين، أو أيّ

---

١ نشرت صحيفة الرياض.نت الخبر الآتي:(على الرابط: http://www.alriyadh.com/net/article/740573)
تعتزم وكالة تابعة للأمم المتحدة تضطلع بمساعدة الدول الأعضاء على تأمين بُنيتها التحتية إصدار تحذير قوي من خطر فيروس الكمبيوتر(فليم) الذي تم اكتشافه مؤخرًا في إيران ومناطق أخرى من الشرق الأوسط. وقال ماركو اوبيسو منسق الأمن الإلكتروني بالاتحاد الدولي للاتصالات التابع للأمم المتحدة ومقره جنيف "هذا أخطر تحذير(الكتروني) نوجهه على الإطلاق." وأضاف في مقابلة مع رويترز أنّ التحذير السرّي سيخطر الدول الاعضاء بأنّ الفيروس فليم أداة تجسّس خطيرة يمكن استخدامها في مهاجمة البُنية التحتية الحساسة، وأردف قائلا "يجب أن تكون(الدول) متنبهة."
هذا التحذير هو أحدث مؤشّر على أن حقبة جديدة من الحرب الإلكترونية بدأت بعد الهجوم بفيروس ستاكس نت الذي استهدف البرنامج النووي الإيراني.
وتشير أدلة إلى أن فيروس فليم ربما أعدّ لحساب الدولة نفسها او الدول التي طوّرت فيروس ستاكس نت الذي هاجم برنامج إيران النووي عام ٢٠١٠، وفقًا لما ذكرته شركة كاسبيرسكي لاب الروسية المتخصصة في برامج أمن الإنترنت التي أرجع إليها الفضل في اكتشاف الإصابات، وقال اوبيسو "اعتقد أن التهديد أخطر كثيرا من ستاكس نت.".

مكوّن آخر من مكوّنات الأنظمة المعلوماتيّة، وهنا تبرز أهميّـة تصميم البُنية التحتيّة لتقنية المعلومات وأمن المعلومات، كالبُنية التحتيّـة لخوارزميّات التشفير ومفاتيحه. ولا تقل أخطار عيوب التشغيل عن أخطار عيوب التصميم في إمكانيّة النّفوذ إلى المعلومات بصفة غير شرعيّة، أو التسبّب في فقدها بسبب خطأ تشغيلي قد يكـون بسيطًا. من الأمثلة على ذلك فتح منافذ اتصال بدلًا من إغلاقها، أو نسـخ المعلومات إلى أماكن خاطئة، أو توجيهها إلى غير وجهتها الصحيحة. ناهيك عن التهديدات المتعلّقة بأخطاء النسخ الاحتياطي التشغيليّة، كأخذ نسخة احتياطيّة لجزء من المعلومات فقط، أو استعادة معلومات قديمة بدلًا من المعلومات الحديثة عند إجراء عملية الاستعادة للمعلومات التي سبق أخذ نسخة احتياطية لها.

تهديد تشتّت المعلومات

إذا كانت معلومات المنشأة مشتّتة ومخزّنة في أماكن كثيرة، ويجري التعامل معها من خلال شبكات متعدّدة، فإنّ هـذا التشتّت يحتّم تطبيق أنظمة أمن معلومـات متعدّدة بتعدّد أماكن وجود هذه المعلومات؛ وهو ما يتسبّب في ضعف منظومة أمن المعلومات وتشتّتها، وكذلك زيادة تكاليف توفيرها وإدارتها والسيطرة عليها. ويؤدي هذا الأمر إلى نوع من تناثر وتعدد تطبيق مفاهيم أمن المعلومات، وقد يتسبب في وجود ولو ثغـرة أمنية واحدة في أحد الأماكن، يمكن النفاذ من خلالها إلى كامل منظومة المعلومات في المنشأة.

٢-٤-٢ تهديدات بشريّة

ويُقصـد بها التهديدات الناجمـة عن العنصر البشـري مباشرة. فقـد يتسبّب العنصر البشريّ- عمـدًا أو عن طريق الخطـأ- في الضرر أو الوصول إلى معلومـات والاطّلاع عليها دون أن يكون له صلاحية ذلك، أو إتلافها، أو تسريبها إلى جهات خارجيّة. وتزداد الخطورة عندما يكون لدى هذا العنصر صلاحية الدخول إلى أنظمة المعلومات، أو أن يكون أحد موظفي المنشأة، ولكنه يسيء استخدام صلاحيّاته. بشكل عام يمكن حصر أهم مصادر التهديدات البشرية للنظم المعلوماتيّة في الآتي:

- المستخدم الشرعي الفاسد.
- موظّف المنشأة الفاسد.

- المستخدم الشرعي وموظف المنشأة غير الواعيين بالمخاطر الأمنيّة، (مع أنّهما غير فاسدين).
- المؤسّسات التجاريّة ذات النوايا المنحرفة (قد يكون الدافع التنافس التجاري).
- المنظمات الإرهابية.
- موردو الأجهزة والبرامج.
- المهندسون والمبرمجون وفنيّو الصيانة والدعم الفني الخارجيّون.

٢-٤-٣ تهديدات طبيعيّة

يقصد بها الكوارث الطبيعيّة التي ليس للإنسان أو التجهيزات الفنيّة دخل في حدوثها، كالزلازل، والبراكين، والفيضانات، والصواعق، والحرائق، وموجات الغبار العاتية. وقد تُلحق مثل هذه الكوارث أضرارًا كبيرة بأنظمة المعلومات، وقد تؤدّي إلى انقطاع الخدمات الإلكترونيّة نهائيًّا في حال أصابت المراكز الرئيسة لتقديم تلك الخدمات.

أخيرًا، وبعد التعرّف إلى أنواع التهديدات المعلوماتيّة، تبرز الحاجة لأمن المعلومات من أجل تحليل هذه التهديدات باختلاف أنواعها: (مركزيّة، بشريّة، طبيعيّة)، و وضع الخطط والبرامج اللازمة للحماية منها، أو على الأقل التخفيف من آثارها، كما سيأتي معنا في الفصلين الثامن والتاسع.

٢-٥ الهجمات الإلكترونيّة والحاجة إلى الحماية منها

تشكّل المعلومات في عصرنا الحاضر رافدًا مهمًّا في حياة الدول والشعوب. وكغيرها من الروافد المهمة، فإنّه يحيط بها عدد من المخاطر أو الأعداء يجب حمايتها منهم، وكلّ خطر أو عدوّ من هؤلاء الأعداء لديه طرقه وأساليبه التي يستخدمها للوصول إلى هذه المعلومات، وبمجرّد النفاذ إلى المعلومات، فإنّه يمكن له نسخ أو تعديل أو حذف أو إساءة استخدامها، أو إلحاق الضرر بها بأيّ شكل من الأشكال، ومع تطوّر وسائل التقنية الحديثة أصبحت المعلومات معرّضة للخطر أكثر من السابق، وظهرت الحاجة الماسة إلى علم أمن المعلومات.

كركيزة أساسيّة لفهم الحاجة إلى أمن المعلومات يلزم المختصّين والجهات المسؤولة عن

تطبيق أمن المعلومات فهم طبيعة الهجمات الإلكترونيّة، والتعرّف إليها، والتقنيات المستخدمة فيها من أجل اختيار التقنيـات والآليات والطرق المناسبة لمكافحتهـا، وفيما يلي نتعرف إلى أشهـر الهجمات الإلكترونيّة المعاصـرة، والحاجة الماسة إلى أنظمة أمـن المعلومات اللازمة لمجابهتها [١، ٢]:

هجمات البرامج (أو الأكواد) الخبيثة (Malicious Code Attacks)

تشمل هجمات البرامج الخبيثة بشكل أساسي: هجمات فيروسات وديدان الحاسب الآلي، وبرامج أحصنة طروادة، وبرامج الاخـتراق، وبرامج التجسّس الإلكتروني. وقد تتسبب هذه البرامج في أضرار كثيرة تتراوح ما بين مجرد الإزعاج، إلى فقد البيانات، و وصولًا إلى سرقة الأموال. وسيتم التطرق بشيء من التفصيل لهذا النوع من الهجمات في الفصل السادس: أمن أجهزة الحاسب الآلي والبرمجيات والملفّات. ومن هنا تبرز الحاجة إلى وجود أنظمة مكافحة هذه البرامج وتحديثها والتدريب عليها.

هجمات الأبواب الخلفيّة (Back Door Attacks)

في بعض الأحيان، يترك المصمّمـون أو المبرمجون أو فنيو الصيانـة طرقًا خفيّة، تسمّى الابواب الخلفيّة، للوصول إلى الأجهزة والشبكات من أجل استخدامها لاحقًا لأعمال التطوير والصيانة عن بُعد، ويستغلّ المهاجمون هذه الطُّرق عند اكتشافها كأبواب خلفيّة للدخول إلى الأجهزة والشبكات بطرق غير شرعيّة. وعندما يترك مثل هذه الأبواب المصممون والفنيون والمبرمجون، فإنّه يكون من الصعوبة بمـكان اكتشاف هذه الأبواب؛ لأنّها عادة لا تكون تحت نظر برامج وأنظمة المتابعة والمراقبة، وإنّما هي أبواب خفيّة حتى على هذه الأنظمة، ومن هنا تبرز الحاجة إلى آليات وطرق الحماية اللازمة التي تكون مسؤولة عن اكتشاف هذه الأبواب، وترشيد استخدامها وتقنينه وتوقيته، أو منعها بالكليّة.

كسر كلمات المرور (Password Crack)

نعني بكسر كلمات المرور هنا عمليّة إعادة حساب كلمات المرور من البصمات الرقميّة (Hash

١ Withman, M. and Mattord, H.(2005), "Principles of Information Security".

٢ داود، حسن طاهر(٢٠٠٤ب)، «أمن شبكات المعلومات».

Values) لهذه الكلمات، التي تُحفظ عادة في ملفات خاصّة بذلك، ويمكن تنفيذ هذا النوع من الهجوم إمّا بإعادة حساب البصمة الرقميّة لكلمات المرور بطُرق رياضيّة معقّدة، أو من خلال الجمع بين هذه الطريقة وهجمات المعجم(Dictionary Attack). وما يتم عمله هو حساب البصمة الرقميّة لكلّ كلمة تنتج من هجوم المعجم، ثم مقارنتها مع البصمة الرقميّة المخزّنة في النظام المراد الهجوم عليه، وفي حال مطابقة هذه القيم فهذا يعني أنّه تمّ الحصول على كلمة المرور، وأمّا إذا اختلفت فيجري الانتقال لكلمة المرور التي تليها ... وهكذا. وهنا تبرز أهميّة التعرّف إلى هذه الطُّرق ومعرفتها، وأهميّة المحافظة الشديدة على الملفّات التي تحتوي كلمات مرور المستخدمين حتى ولو كانت مرمّزة أو مشفّرة أو محفوظة على شكل قيم مركّزة، وليس كلمات مرور صريحة.

الهجوم الأعمى(الاستقصائي)(Brute Force Attack)

يسمّى الهجوم الذي يحدث عن طريق تجريب جميع الاحتمالات الممكنة لكلمات المرور أو الأرقام السرية، أو أيّ معلومة يحتاج إليها المهاجم في عمليّة الهجوم بالهجوم الأعمى أو الاستقصائي. وسمّي بهذا الاسم لأنّه لا يعتمد علي أيّ عمليّة حسابيّة، أو أيّ عمليّة لتسريع الهجوم أو اختصار الوقت للازم لتنفيذه، وإنّما يحصل بمحاولة الدخول مرّة تلو الأخرى واستقصاء جميع الاحتمالات الممكنة. عادة ما يستخدم هذا النوع من الهجوم على الحسابات أو أسماء المستخدمين المشهورة التي تُكوَّن أثناء تنصيب الأنظمة، مثل حساب مدير النظام(Administrator) أو(Admin)، أو حساب الضيف(Gust). وهنا تبرز أهميّة تغيير هذه الحسابات من الأسماء الافتراضيّة لها المحدّدة من الشركات المنتجة إلى أسماء أخرى خاصّة بالمنشأة، وكذلك أهميّة تغيير الإعدادات التلقائية التي يمكن النفاذ من خلالها، مثل إعدادات المشاركة في الملفّات والطابعات.

هجمات المعجم(Dictionary Attacks)

تُعدُّ هجمات المعجم نوعًا من أنواع الهجوم الأعمى، خاصّة عند تخمين كلمات المرور. ففي هجوم المعجم يجري تضييق نطاق المحاولات إلى كلمات المعجم ذات المعاني، بدلًا من استخدام

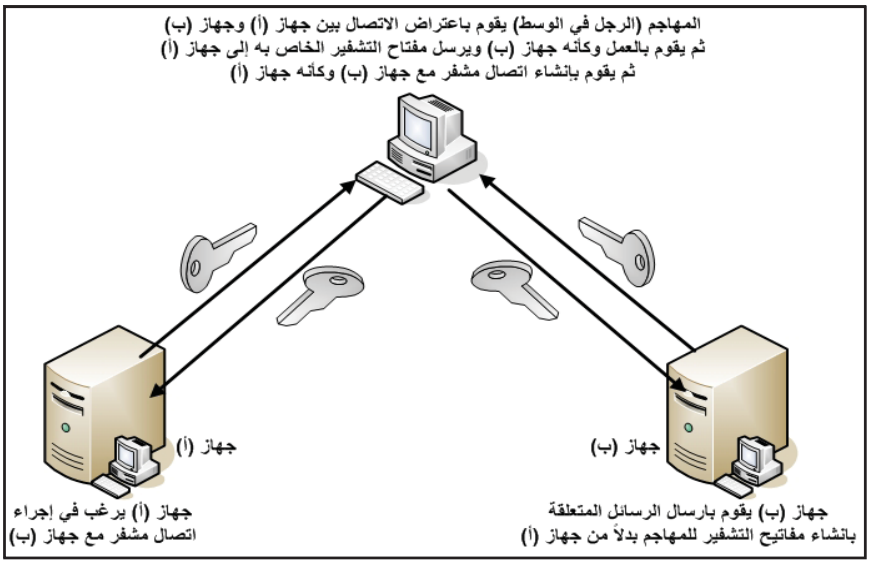
كلمات عشوائيّة ذات حروف عشوائيّة، يكون عددها هائلًا جدًا. وهنا تبرز أهميّة مكافحة هذا الهجوم من خلال تعطيل إعطاء كلمات مرور من المعجم عند عمل إعادة تعيين(Reset) لكلمة المرور. وعادة ما يُلجأ إلى هذه الطريقة عند نسيان المستخدم كلمة المرور، حيث يعطى كلمة مرور جديدة مؤقّتة يستخدمها للدخول مرّة واحدة، ثم يغيّرها بكلمة مرور جديدة وفق السياسة الأمنيّة لكلمات المرور، وكذلك تبرز أهميّة وضع السياسة الأمنيّة لكلمات المرور وتطبيقها ، التي يفرض فيها عدم استخدام كلمات من المعجم و وجوب استخدام حروف(كبيرة وصغيرة)، ورموز(مثل #، ٪، &، @)، وأرقام في كلمات المرور؛ من أجل مكافحة هذا النوع من الهجوم.

هجمات الرجل في الوسط(Man-in-the-Middle Attacks)

يُطلق على هذا الهجوم أيضًا هجوم اختطاف بروتوكول النقل(TCP Hijacking)(TCP Attack). ويحدث في هذا الهجوم التقاط حزم البيانات(Data Packets) المارّة في الشبكة، ثم تغييرها، ثم إعادتها مرة أخرى إلى الشبكة لتكمل مسارها، لكن بمعلومات معدّلة، فيمكن من خلال هذا الهجوم تعديل البيانات، أو الحذف منها، أو الزيادة عليها، أو تزويرها، أو تحويلها، أو إعادة توجيهها. ومن أشهر استخدامات هذا الهجوم انتحال هويّة جهاز(أو مكوّن) آخر في الشبكة، خاصّة عند الهجوم على عمليّة توزيع مفاتيح التشفير باستخدام الشهادات(Digital Certificates) فيظهر المهاجم كأنّه رجل(غير مرئي) في الوسط بين الجهازين اللذين تجري عملية تبادل مفاتيح التشفير بينهما، فينتحل شخصيّة أحدهما، ثم يتعامل مع الآخر كأنّه الجهاز(أو المكوّن) الحقيقي المقابل له، ومن ثم يمكن الحصول على معلومات مفاتيح التشفير، انظر الشكل(٢-١). وهنا تبرز جليًّا الحاجة لأمن المعلومات في هذا الجانب المهم الذي يهدّد سلامة أنظمة التشفير.

هجوم تعطيل الخدمة(Denial of Service (DoS) Attack)

في هذا النوع من الهجوم يُرسَل عدد هائل من طلبات الاتصال أو أوامر بروتوكولات الشبكات، مثل أمر(ping) إلى الجهاز الضحيّة من أجل إغراقه في معالجة هذا الطلبات، وتحميله أكثر من طاقته حتى وصوله لدرجة عدم الاستجابة، ومن ثم عدم قدرته على القيام



الشكل(٢-١): هجوم الرجل في الوسط

بمهامه المعتادة، وقد تصل درجة الإغراق في بعض الأحيان إلى تعطيل الهدف نهائيًّا وخروجه من الخدمة. وهناك نوع خطير من هذه الهجمات يسمّى هجوم تعطيل الخدمة الموزّع(Distributed Denial of Service(DDoS) Attack)، والذي يتم فيه توزيع البرامج المصدِّرة لسلسلة من طلبات و أوامر الإغراق عبر عدد كبير من الأجهزة الموزّعة في أماكن مختلفة التي تعمل عن بُعد، ومن ثم برمجة جميع هذه الأجهزة للهجوم معًا على الجهاز الضحيّة، ومن ثم إغراقه وتعطيله وإخراجه من الخدمة في وقت قصير. ويُعدُّ هذا النوع من الهجمات من أعتى الهجمات وأكثرها ضراوة، حيث لا توجد له حلول مباشرة مخصّصة له، وإنما تتم مكافحته بتكاتف عدد من الحلول. وتبرز هنا أهميّة وخطورة هذا الهجوم وضرورة مكافحته واكتشاف طلبات وأوامر الإغراق، وتعطيلها، خاصّة مع انتشار الأجهزة والشبكات المرتبطة بشبكة الإنترنت التي تقدّم خدمات الإنترنت المختلفة، مثل خدمة المواقع(WWW)، ونقل الملفّات(FTP)، والبريد الإلكتروني، والسبب في ذلك هو أنّ هذه الخدمات تستخدم بروتوكول(TCP) الذي يمكن استخدام بعض أوامره كأوامر إغراق ليس فقط لأجهزة الحاسب، الآلي وإنما يمكن توجيهها كذلك لإغراق أجهزة الشبكة كالموجّهات، وجدران الحماية.

هجمات الخداع (Spoofing Attacks)

هي طريقة للتمكّن من الوصول إلى الأجهزة بطريقة غـير شرعية عن طريق خداع هذه الأجهزة، بإرسال رسائل مخادعة تحتوي عنوان إنترنت (IP) يجعل الرسالة تبدو كأنّها قادمة من جهة موثوقة. ولإتمام هذا النوع من الهجوم فلا بدّ للمهاجم من استخدام طُرُق وأدوات الحصول على عنوان الإنترنت (IP) المناسب الذي يستطيع من خلاله خداع الجهاز الضحية، وكذلك الحصول على برامج يستطيع من خلالها تغيير المعلومات الموجودة في جزء الرأس من حزم البيانات (Packet Header) لتظهر هذه الحُزم كأنّها قادمة من جهة موثوقة ومعروفة لدى الجهـاز الضحية. وهنا تبرز الحاجـة لأنظمة أمن المعلومات التـي تستطيع كشف ذلك ومجابهته، خاصّة على مستوى الموجهات وجدران الحماية.

الرسائل غير المرغوب فيها (أو المزعجة) (Spam)

يَرِدُ إلى صناديق البريد الإلكتروني كثير من الرسائل (المُزعجة) غير المرغوب فيها. ويَعدُّ كثير من الناس أنّ هذه الرسائل لا تُعدُّ هجمات إلكترونيّة، لكن واقع الحال يقول إن كثيرًا منها يحتوي ملفات بها برامج أو أكواد خبيثة. ويمكن التخلّص من هذا النوع من الرسائل بتفعيل عمليّات التنقيح والفلترة الموجودة في خوادم البريـد الإلكتروني وكذلك بتوعية المستخدمين بحذف جميع الرسائل غير المرغوب فيها، وعدم الثقة في هذا النوع من الرسائل، وعدم فتحها.

تفجير البريد الإلكتروني (Mail Bombing)

وهذا أيضًا هجوم على البريد الإلكتروني لكن بنوع من أنواع هجوم تعطيل الخدمة، وهو هجوم تفجير البريد الإلكـتروني، أو قنبلة البريد الإلكتروني. وما يحدث في هذا الهجوم هو أنّ المهاجـم يوجّه عددًا هائلًا مـن الرسائل إلى عنوان البريد الإلكـتروني الضحية. ويمكن كذلك توظيف هجمـات الهندسة الاجتماعيّة لإرسـال هذا العدد الهائل مـن الرسائل (كما سيأتي معنا)، أو من خلال استغلال أوامر بروتوكول نقل البريد الإلكتروني (Simple Mail Transport Protocol) في خوادم البريد الإلكتروني ضعيفة التهيئة، التي من خلالها يمكن إغراق الضحية بعدد هائل من الرسائل حتى الوصول إلى درجة عدم قدرته على معالجتها،

ومن ثم يدخل في مرحلة تعطيله عن الخدمة. وهنا تبرز أهميّة أمن البريد الإلكتروني، الذي أضحى وسيلة أساسيّـة للتواصل وإنجاز الأعمال على المستويـات الحكوميّة والخاصّة كافّة، وحتى على مستوى الأفراد.

هجمات التشمّم أو الالتقاط (Sniffer Attacks)

المتشمّم هو برنامج أو جهاز يراقب البيانات المارّة عبر الشبكة ويلتقطها، ويمكن أن يكون هناك تشمّم أو التقاط شرعي لمراقبة الشبكة ومتابعها وإدارتها، ويمكن أن يكون غير شرعي لسرقة البيانات. ويُعدُّ هذا الهجوم خطيرًا جدًا على الشبكة لأنّه يمكن زرع المتشمّم في أيّ مكان في الشبكة، وغالبًا لا يمكن كشفه، وهذا ما يجعله محبّبًا لدى المهاجمين. ويزداد الأمر خطورة إذا كان نقل المعلومات يجري على الشبكة، سواءً أكانت محلية (LAN) أم واسعة (WAN)، في شكلها الأصلي غير مشفرة، لأنّ المتشمّم في هذه الحالة يستطيع قراءة كلمات المرور وكذلك محتويات الملفّات النصية مثل ملفات معالجة الكلمات. وهنا تبرز أهميّة توفير أنظمة الحماية التي تكشف وجود برامج وأجهزة التشمّم وتكافحها، وكذلك الأنظمة التي تحول دون الاستفادة من المعلومات المسروقة في حالة نجاح المتشمّم في سرقتها، كأن تكون مشفّرة مثلًا.

هجمات الهندسة الاجتماعيّة (Social Engineering Attacks)[1]

يخلط هذا النوع من الهجوم بين النواحي الاجتماعيّة واهتمامات الناس وبين المهارات الفنيّة في خداع الضحايا وكسب ثقتهم للإدلاء بمعلومات سريّة يتم استغلالها لسرقة المعلومات والأموال إلكترونيًا (انظر الفصل السابع: موضوع: التهديدات الرقميّة لشبكات الحاسب الآلي). وقد انتشر هذا النوع من الهجوم في الآونة الأخيرة انتشارًا كبيرًا؛ لأنّه لا يعتمد على كسر أنظمة الحماية التقنيّة التي تطوّرت مع مرور الوقت، وإنّما يعتمد على كسب ثقة الضحايا وإيهامهم بأنّ من يطلب منهم معلوماتهم السِّريّة (كاسم المستخدم وكلمة المرور وأرقام بطاقات الائتمان) هو جهة موثوقة (مصرف مثـلًا) وبعد ذلك يتم استغلال هذه المعلومات وانتحال شخصيّات الضحايا ومن ثم سرقتهم إلكترونيًّا عن طريق دخول يبدو شرعيًّا لأنظمة الحماية. ومن الأمثلة

١- الغثبر، خالد بن سليمان و القحطاني، محمد بن عبد الله(٢٠٠٩)، «أمن المعلومات بلغة ميسّرة»، ص ٣٣-٤٤.

الشهيرة على هذا النوع من الهجوم هو هجمات الاصطياد الإلكتروني[1].

هجوم تصفّح الكتف (Shoulder Surfing Attack)

يعني هجوم تصفّح الكتف أن يطّلع المهاجم على المعلومات المهمّة والحسّاسة كما لو كان ينظر إليها من فوق كتف الضحيّة، ويرى لوحة المفاتيح وما يقوم بضغطه من أزرار وما يُعرض على الشاشة من معلومات. ويستخدم هذا الهجوم في الأماكن العامّة أو أماكن العمل المشتركة، حيث ينظر المهاجم خلسة إلى شاشة الضحيّة، ومن ثم يعرف بعض المعلومات السِّريّة، التي يجب أن لا يعرفها. ومن الأمثلة على ذلك: استراق النظر خلسة إلى الأرقام السرية لبطاقات الصرف الآلي وقت إدخال مستخدمها لها، وكذلك معرفة كلمات المرور للحاسبات الآلية أو أجهزة الهاتف النقال وقت إدخالها، انظر الشكل(٢-٢).

الشكل(٢-٢): هجوم تصفح الكتف

هجمات المعلومات الجانبيّة (Side channel Attacks)

ظهر نوع حديث نسبيًّا وخطير جدًا من الهجمات الإلكترونيّة يعتمد على المعلومات الجانبيّة التي يجمعها المخترق من أجهزة التشفير، خاصّة أجهزة التشفير التي تعمل بأنظمة التشفير

١- الغثبر، خالد بن سليمان و بن هيشة،(٢٠٠٩)، «الاصطياد الإلكتروني: الأساليب والإجراءات المضادة».

بالمفتاح العام، ثم يحلّلها للحصول على المعلومات السِّريّة كمفاتيح التشفير. وما يحدث ليس كسرًا لأنظمة التشفير بشكل مباشر، وإنّما جمع المعلومات الجانبية مثل: الوقت المستغرق، أو كميّة الطاقة الكهربائيّة المستهلكة، لإتمام عملية حسابيّة معيّنة. فظهر هجوم يسمّى هجوم الوقت(Timing Attack)، الذي يعتمد على حساب الوقت المستغرق لكل عمليّة حسابيّة يقوم بها جهاز التشفير، وربط ذلك بقيمة مفتاح التشفير. فمن المعروف أنّ جهاز التشفير يستغرق وقتًا أطول عند إجراء العمليّات الحسابيّة عندما تكون قيمة الخانة الحاليّة في التمثيل الثنائي لمفتاح التشفير تساوي "١" و وقتًا أقلّ عندما تكون تلك القيمة تساوي "صفرًا" ومن ثَمَّ يمكن معرفة مفتاح التشفير بتكرار هذه العمليّة مع كلّ خانة من خانات المفتاح، وظهر هجوم مماثل يسمّى هجوم تحليل الطاقة الكهربائيّة(Power Analysis Attack)، الذي يعتمد على قياس الطاقة الكهربائيّة المستهلكة لكلّ عمليّة حسابيّة يقوم بها جهاز التشفير، وربط ذلك بقيمة مفتاح التشفير، فمن المعروف أنّ جهاز التشفير يستهلك طاقة كهربائيّة أكبر عند إجراء العمليّات الحسابيّة عندما تكون قيمة الخانة الحاليّة في التمثيل الثنائي لمفتاح التشفير تساوي "١" وطاقة أقلّ عندما تكون هذه القيمة "صفرًا" ومن ثمّ يمكن معرفة مفتاح التشفير بتكرار هذه العمليّة مع كل خانة من خانات المفتاح[١].

ملخّص الفصل

ليس أمن المعلومات ترفًا ولا سببًا لصرف الجهود والأموال الطائلة دون مبرّر قويّ وحاجة مُلحّة لذلك، فقد أثبت هذا الفصل أنّ أمن المعلومات ضرورة مُلحّة، وأجاب عن التساؤل الذي وُضِع عنوانًا للفصل وهو: «لماذا أمن المعلومات؟». وتركزت الإجابة على توضيح مفهوم أمن المعلومات والمحاور الرئيسة التي يشملها أولًا، ثم سرد الأسباب الرئيسة وراء الحاجة لأمن المعلومات. وليس أبلغ في إيصال فكرة ضرورة تطبيق أنظمة أمن المعلومات اللازمة لحماية المعلومات والأنظمة المعالجة لها من التعرّف إلى التهديدات المحيطة بها، والهجمات الإلكترونيّة التي قد تفتك بها. فلكي تكون المعلومات في مأمن، لا بدّ من التعرّف إلى تلك التهديدات والهجمات من أجل تسخير الطاقات الفنية والإداريّة لمجابهتها. فمّما أوضحه هذا الفصل أنّ

١- Mangard et. al.(2007), "Power Analysis Attacks: Revealing the Secrets of Smart Cards"

هناك تهديدات مركزيّة، كأخطاء التهيئة والتشغيل قد تكلّف الشيء الكثير، ولا تفيد في حماية المعلومة. وهناك تهديدات بشريّة يجب التنبه لها وتوعية العاملين والمستخدمين والمستفيدين بها، وهناك التهديدات الطبيعيّة التي قد تظهر في أيّ وقت، ويجب الاستعداد لها. على الجانب الآخر، فقد تنجح بعض الهجمات الإلكترونيّة في كسر أنظمة الحماية والوصول للمعلومات بطريقة غير شرعيّة، ومن الأمثلة التي أوردها هذا الفصل على ذلك هجمات البرامج الخبيثة على المعلومات الثابتة، وهجمات الهندسة الاجتماعيّة على المعلومات السِّريّة في شبكة الإنترنت، وهجمات الرجل في الوسط على المعلومات المرسلة، إلى غير ذلك من الهجمات التي تم شرحها.

مسائل

١. هل يمكن اعتبار أمن المعلومات قضيّة إداريّة بحتة أم تقنيّة بحتة أم خليطًا منهما؟ اشرح السبب.

٢. لماذا تُعدُّ المعلومات أهم مورد يجب حمايته؟ اشرح ذلك من خلال الأسباب الخمسة الرئيسة التي أبرزت الحاجة لأمن المعلومات.

٣. أيهما أصعب: حماية المعلومات الثابتة أم حماية المعلومات المتنقلة؟ اشرح ذلك. وهل يوجد حالات أخرى، خلاف الثابتة والمتنقلة، يمكن أن توجد فيها المعلومات؟ رتّب هذه الحالات حسب أولوية الحماية، مع ذكر السبب.

٤. ما أوجه الشبه والاختلاف بين التهديدات والهجمات الإلكترونيّة؟ كيف يمكن أن تتقاطع هذه المفاهيم في مناطق التقاء بينهما؟

٥. كيف يمكن أن يكون الموظفون تهديدًا لأمن المعلومات؟

٦. ما التدابير التي يمكن أن يتخذها الأفراد للحماية من هجوم تصفّح الكتف؟

٧. ما أنواع هجمات كسر كلمات المرور؟ مع إعطاء أمثلة. ماذا يمكن لمدير النظام أن يفعل للحماية من هذه الهجمات؟

٨. ما الفرق بين هجوم تعطيل الخدمة (DoS) وهجوم تعطيل الخدمة الموزّع (DDoS)؟ أيهما أخطر؟ ولماذا؟

٩. لنجاح هجوم التشمّم، ماذا يجب على المهاجم القيام به؟ وكيف يمكنه الوصول إلى الشبكة أولًا؛ ليستطيع القيام بالتشمّم؟

١٠. أعط أمثلة لأساليب هجمات الهندسة الاجتماعيّة، وكيف يمكن أن تختلف طبيعة هذه الهجمات إذا كان المستهدفون هم مديرو الأنظمة، وليس المستخدمون العاديون؟

١١. لو أن مهاجمًا استطاع أن يلتقط اسم المستخدم وكلمة المرور لمستخدم عادي ثم دخل إلى الشبكة بطريقة غير شرعية ثم كسر كلمة مرور مدير النظام (Administrator) لخادم قواعد البيانات، الذي تم تركه على الإعدادات التلقائية، ثم سرق أرقام بطاقات الائتمان لعملاء المنشأة؛ فأجب عن الأسئلة الآتية:

أ. كم نظام حماية جرى تجاوزه؟ اذكر تلك الأنظمة.

ب. كم فئة من فئات التهديدات توجد في هذا الهجوم؟ اذكرها.

ج. ما الثغرات التي جرى النفاذ من خلالها لخادم قواعد البيانات؟

د. ما رأيك في ثقة عملاء المنشأة بها بعد هذا الهجوم؟ وهل نجاح هذا الهجوم يهدّد بقاء المنشأة أم لا؟ اشرح ذلك.

الفصل الثالث

عناصر أمن المعلومات

أهداف الفصل

- التعريف بعناصر أمن المعلومات وتوضيح ماهيّتها.
- تحديد عناصر أمن المعلومات وشرحها بالتفصيل، مع إيراد أمثلة على كل عنصر.
- توضيح دور كل عنصر من عناصر أمن المعلومات والخروقات الممكنة في حال غيابه.
- إبراز دور التكامل بين عناصر أمن المعلومات لتوفير الحماية اللازمة للمعلومات.

ما ستتعلمه في هذا الفصل

- تعريف عناصر أمن المعلومات وماهيّتها من خلال أمثلة تطبيقيّة.
- عنصر التحقّق من الهُويّة: يوفر إمكانية التحقّق من هُويّة الأشخاص والجهات التي تتعامل مع المعلومات.
- عنصر التحكّم بالوصول: يوفر إمكانية التحكّم بالوصول إلى الموارد المتاحة.
- عنصر السِّريّة: يحدّ من قدرة الأشخاص غير المصرّح لهم على الاطلاع على المعلومات أو قراءتها أو فهمها.
- عنصر سلامة المعلومة وتكاملها: يوفر إمكانية كشف أيّ تعديل على المعلومة.
- عنصر عدم الإنكار: يمكن من خلاله منع أيّ شخص أو جهة من إنكار أيّ عمليّة قام بها وكشف ذلك.
- عنصر توافر المعلومة: يمكن من خلاله حماية المعلومات من كلّ ما يتسبّب في عدم توافرها لتبقى دائمًا متاحة.
- عنصر المتابعة (أو التدقيق): يُعنى بمتابعة عمليّات المستخدمين، والتحقّق من فرض سياسات أمن المعلومات عمليًّا على أرض الواقع.

عناصر أمن المعلومات

٣-١ مقدّمة

يتغيّر حدّ الأمان المطلوب لأيّ معلومة حسب حالة المعلومة نفسها، وأهميّتها، والبيئة التي تحفظ فيها، والوسائل التي تنتقل بواسطتها. فعلى سبيل المثال، إنّ المعلومة المدونة على ورق يمكن أن تحفظ بمكان آمـن، ويمكن التحكّم بالوصول إليها عن طريق أبواب دخول أو أدراج حفظ، ويمكن نقلها بواسطة البريد العادي. أمّا المعلومة التي تحفظ بأجهزة الحاسب الآلي فإنّها معلومة إلكترونيّة، وتحتاج إلى طريقة تأمين تختلف كثيرًا، حيث بالإمكان نسخها دون ترك أيّ أثر، أو الوصول إليها بطرق غير مشروعة. إذاً يجب أن تحفظ هذه المعلومات الإلكترونيّة على وسائط تخزين آمنه ومتوافرة، ولا يجب أن يصل إليها إلّا الأشخاص المصرّح لهم فقط.

وسواءً أكانت المعلومة مستقّرة في قواعد بيانـات أو وسائط تخزين ثابتة، أم يتم تبادلها بين طرفين، فإنه لا بد من وجود القناعة التامة بتحقيق حد معين من أمن المعلومات في حال استقرارها أو نقلها. ويتحقّق هذا الحدّ من خلال عناصر أمن المعلومات، التي هي عبارة عن عدة عناصر كلّ واحد منها يغطي جانبًا مهمًا من جوانب أمن المعلومات، وإذا كان هناك خلل أو غياب لأحد هذه العناصر، فإنّه سيكون هناك قصور في أمن المعلومة من ذلك الجانب.

لقـد حـدّد بعضـ المؤلّفـين ثـلاث ركائـز أساسيـة لأمـن المعلومـات هـي: السِّريّـة (Confidentiality)، وسلامـة المعلومـة وتكاملهـا (Integrity)، والتوفر (Availability)، وأُطلق على ذلك مثلث (CIA) (CIA Triangle). إلّا أنّ الاتحاد العالمي للاتصالات في توصيته[١] X.800 قد حدّد عناصر أساسية لأمن المعلومات يمكن حصرها في سبعة عناصر رئيسة، هي: التحقّق من الهُويّة، والتحكم بالوصول، والسرية، وسلامة المعلومة وتكاملها، وعدم الإنكار، وتوافر أو ديمومة المعلومة، والمتابعة أو التدقيق[٢،٣].

١- Stallings, William (2007), "Network Security Essentials: Applications and Standards"

٢- ذكر وليام ستولينج(Stallings William, (2006) أنـه لـيس هنـاك اتفاق عام على كثير من مصطلحات أمن المعلومات. فمثلًا قد تستخدم عبارة "سلامة المعلومة وتكاملها(Integrity)" للدلالة على جميع ما يخص أمن المعلومة. وقد يستخدم لفظ "التحقق من الهوية(Authentication)" للدلالة على التخويل(Authorization) أيضًا. وعلى أيّ= =حال، فإن المصطلحات المستخدمة في هذا الكتاب هي ترجمة تتفق مع ما ورد في وثائق كل من(X.800) و(RFC2828) معًا.

٣- وليام ستولينج(١٤٣٢)، «أساسيات أمن الشبكات: تطبيقات ومعايير»، كتاب مترجم إلى اللغة العربية، ص ١٧.

في هذا الفصل نبدأ أولًا بتوضيح ماهيّة عناصر أمن المعلومات الرئيسة مع ضرب أمثلة توضيحية لكل واحد منها، ثم ننتقل بعد ذلك إلى شرح كل عنصر من تلك العناصر على حدة وبشيء من التفصيل.

٣-٢ ماهيّة عناصر أمن المعلومات

يمكن تعريف عناصر أمن المعلومات بأنّها: «مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة، بحيث يغطّي كلّ عنصر من هذه العناصر جانبًا من جوانب الحماية المطلوبة. ومعنى ذلك هو أن تتكامل هذه العناصر حتى توفّر الحماية المطلوبة، وفي حال فقد أيّ منها فسيكون هنالك خلل أمنيٌّ في الجانب الذي يغطّيه هذا العنصر.

لتوضيح ما نقصده بعناصر أمن المعلومات، سوف نشرح ذلك من خلال مثال إرسال رسالة من شخص إلى آخر باستخدام الطريقة التقليدية (البريد العادي) ومقارنة ذلك بالطرق الحديثة التي يجري فيها إرسال الرسالة إلكترونيًّا. والسبب في اختيار هذا المثال هو أولًا لتقريب مفهوم عناصر أمن المعلومات، وثانيًا أنّ أغلب طُرُق الحصول على المعلومات وتبادلها يكون عن طريق طرفين: أحدهما مُرسِل والآخر مُستقبِل، أو عن طريق تقنية الخادم والعميل، أو تطبيقات شبكة الإنترنت، التي لا تخلو من تبادل المعلومات بين طرفين أو جهتين (قد تكون جهازين يعملان بشكل آلي).

عندما يريد شخص (أو جهة) أن يرسل رسالة (عاديّة) لشخص أو جهة أخرى، فإنّه يضع اسمه وعنوانه وكذلك اسم المرسل إليه وعنوانه على الرسالة؛ لإيضاح هويّة كلّ منهما، والهدف من ذلك هو ضمان توجيه الرسالة إلى المرسل إليه لا إلى غيره، وبالمقابل قد يرغب المرسل إليه عند استلام الرسالة في التحقّق من أنّ هذه الرسالة أرسلت بالفعل من المرسل بعينه لا من سواه. ويمكن تحقيق ذلك من مجرد تسليم الرسالة بواسطة ساعي بريد المرسل، المعروف سلفًا عند الطرفين. أمّا في حالة الرسالة الإلكترونيّة فيتم ذلك بتطبيق عنصر التحقّق من الهُويّة (Authentication).

ولضمان عدم رؤية الرسالة من قبل الآخرين، فإن المرسل يضع الرسالة داخل مظروف

مختوم. تحقّق هذه العملية جانبًا (عنصرًا) من جوانب أمن المعلومة، وهو عدم فتح (Access) هذه الرسالة إلا من قبل الشخص المعني، وإلا فإنه سيتم تشويه الختم، وسيعلم المستقبل أنه تم فتح المظروف من قبل شخص غير مصرح له. وطبقًا للقوانين المعمول بها فإنّه من المفترض أن لا يقوم بفتح هذا المظـروف إلا الشخص المصرّح له فقط، وهو المرسـل إليه. يقابل هذه العملية في حال إرسال رسالة إلكترونيّة تطبيق عنصر التحكم بالوصول (Access Control).

عندما تكون الرسالة الورقيّـة مهمّة وسريّة، فإنّه يمكن كتابتهـا بالحبر السري مثلًا، أو تشفيرها باستخدام رموز التشفـير التقليدي لضمان سرية (Confidentiality) المعلومات المدوّنة في الرسالة. فحتى لو تمكّن شخص غير مصرح له من رؤية الرسالة فإنّه لا يستطيع قراءة المعلومات المدوّنة فيهـا أو فهمها؛ لأنّها مكتوبة بالحبر السـرّي أو مشفّرة. يقابل هذه العملية في حال إرسال رسالة إلكترونيّة أن يشفّر المرسـل الرسالة (الإلكترونيّة) باستخدام تقنيات التشفير الإلكتروني الحديث.

لضمان سلامة الرسالة التقليدية من التعديل أو الحذف أو الإضافة، فإنّه يمكن التحقّق من ذلك بمجـرد تفحص الرسالـة لمعرفة سلامة محتواهـا، وهل جرى عليهـا أيّ تعديل أو حذف أو إضافة. أمّا في الرسالة الإلكترونيّة، فإنّ ذلك يكون بتطبيق عنصر سلامة المعلومة وتكاملها (Data Integrity).

قد تكون الرسالة التقليديّة في بعض الأحيان عبارة عن أوامر وتعليمات أو إجراءات يجب على مستلم الرسالة القيام بهـا. لذا قد ينكر المرسل إليه استـلام الرسالة. في هذه الحالة قد يتم إثبات ذلك بشهادة ساعي البريد مثلًا. أمّا في حالـة الرسالة الإلكترونيّة فيتم ذلك بتطبيق عنصر عدم الإنكار (Non-Repudiation).

لقد أظهرت التقنيات الحديثة الحاجة إلـى عنصرين مهمّين من عناصر أمن المعلومات قد لا يكون لهما مقابل في حال الرسائل التقليديّة، وهمـا: عنصر التوفر (Availability)، وعنصر التدقيق أو المتابعة (Auditing). فبتطبيق عنصر التوفر، يمكن ضمان توفر المعلومات للاطلاع عليها واستخدامها من قبل الأشخاص المصرّح لهم عند الحاجة، لاسيما أنّه يمكن

الوصول إلى هذه المعلومات إلكترونيًّا وفي أيّ وقت ومن أيّ مكان. لذلك يجب بعد تأمين المعلومة من جوانبها كافة ، توافرها بشكل دائـم لاستخدامها والاطّلاع عليها عند الحاجة، ومنع أيّ خطر قد يتسبّب في فقدها أو عدم توافرها، وبتطبيق عنصر التدقيق يمكن التأكّد من تطبيق أنظمة المعلومات بالشكل الصحيح، وإلزام المستخدمين ومديري الأنظمة والمشرفين والفنيّين بسياساتها وإجراءاتها، والتحقّق من عـدم وجود مخالفات أو ثغرات أمنيّة يمكن النفاذ من خلالها.

لك أن تتخيّـل ماذا سيكون عليه حـال أمن المعلومات في عصرنـا الحاضر الذي تعدّدت فيه وسائل الاتصـال وتنوّعت، وتزايد تبادل المعرفة، وزادت فيـه قيمة المعلومات المخزّنة في الحاسبات الآلية، وأصبح اعتماد الأشخاص والمؤسسات والحكومات عليها في أداء أعمالهم اليومية أمرًا واقعًا ملموسًا لا مفر منه. وفيما يلي نتطرق بشيء من التفصيل لكلّ عنصر من عناصر أمن المعلومات الحديثة.

٣-٣ التحقّق من الهُويّة (Authentication)

تعني الخدمة التي يمكن من خلالها التحقّق من هُويّة الشخص (أو الجهة) وأنّه الشخص المعني لا غيره. فعند اتصال شخصين (أو جهتين) بعضهما ببعض، فلا بدّ من أن يتعرّف كل منهما إلى الآخر، لضمان أن يتخاطب كلّ منهما مع الشخص أو الجهة المعنيّة وليس مع غيرها. بعبارة أخرى: فإنّ التحقّق من الهُويّة هو التحقّق مـن أنّ المستخدم لنظام ما هو بالفعل من ادّعى أنّه ذلك المستخدم[١]، وفي حال نقل المعلومات، فإنّه يجب التحقّق من هُويّة المرسل لضمان أنّ المعلومة قادمة من مصدرها الحقيقي، وكذلك يجب التحقّق من هُويّة المستلم لضمان أنّ المعلومة ذاهبة إلى وجهتها الصحيحة.

تبدأ عملية التحقّق مـن الهُويّة بالتعريف بالهوية أو تحديـد الهُويّة (Identification). ويمكن تحقيق ذلك من خلال اسم المستخدم أو رقم الحساب مثلًا. إنّ تحديد هوية الشخص أو التعريف به رقميًّا (إلكترونيًّا) أمر مهم، وقد يكون صعبًا في بعض الأحيان؛ إذ إنّ الشخص الواحد نفسه قد يكون لديه أكثر من هوية رقميّة. فمثلًا قد يكون لموظّف واحد اسم مستخدم

١- يعبّر عن ذلك في اللغة الإنجليزية بالعبارة الآتية: Verify that the user is the one who claim that he is.

للدخول إلى الشبكة المحليّة العاملـة على نظام النوافذ (Windows)، واسم مستخدم آخر على نظام اليونكس (Unix)، وثالث على النظام المركزي (Mainframe)، ورابع على نظام المحادثة الآنية ... وهكذا. وهذا ما يصعِّب كثيرًا من مهام التدقيق والمتابعة وتسجيل الأحداث لكلّ مستخدم؛ لذا يجب أن تتوافر في طريقة تحديد الهُويّة المعايير الآتية:

- أن تكون الهُويّة فريدة: ومعنى ذلك أن تكون غير قابلة للتكرار. ومثال ذلك أن يكون للشخص رقم هوية فريد خاص به لا يشترك معه غيره فيه. ومثال آخر هو استخدام الخصائص الحيويّة للإنسان، غير قابلة للتكرار، كبصمات الأصابع، وبصمات العين.
- أن تكون غير مفصِحة عـن معلومات المستخدم و وظيفته والغرض من وصوله إلى المعلومة. ومثال ذلك أن لا ينم اسم المستخدم لمدير النظام عن أنّه المدير، مثل استخدام عبارة "مدير" "Administrator" أو عبارة "Backup Operator" ... وهكذا.
- أن لا تكون مشتركة بين المستخدمين، كإعطاء قسم كامل به عدد من الموظفين اسم المستخدم نفسه.
- اتّباع معايير التسمية المعتمدة عند المنشأة عند إنشاء حسابات المستخدمين، كاستخدام أول حرف من اسم المستخدم الحقيقي متبوعًا برقم الهُويّة، أو غير ذلك من التسميات التي قد يستفاد منها في تحديد الشخص بسهولة عند إجراء عمليّات التدقيق والمتابعة.

يطلَق على عنصر التحقّق من الهُويّـة «المصادقة» أيضًا، وتعني المصادقة أن تكون جميع الاتصالات موثوقة[1]. ففي حالة إرسال رسالة باتجـاه واحد (من طرف واحد ولا تحتاج إلى رد) كرسائل التحذير أو الأوامـر والتعليمات، فإنّه يجب أن يكون لدى المستقبل الضمان بأنّ الرسالة التـي وصلته صادرة فعلًا من المصـدر الذي يدّعي أنّه أرسلهـا، وفي حالة الرسائل التفاعليّة بين طرفين، فإنّ المصادقة تضمـن أنّ الطرفين محدّدان، وأنّهما فعلًا الشخصان المعنيّان (أنهما فعلًا من يدّعيان أنهما كذلك).

تحدّد توصيات X.800 شقين رئيسين للتحقق من الهُويّة، هما[2]:

١- Stallings, William (2006), "Cryptography and Network Security: Principles and Practices".

٢- وليام ستولينج(١٤٣٢)، «أساسيات أمن الشبكات: تطبيقات ومعايير»، كتاب مترجم إلى اللغة العربية، ص ١٩.

- التحقّق من هويّة الشخص أو الجهـة(Peer Entity Authentication): ويوفر التحقّق من هويّة طرفي الاتصال في جميع مراحله، وضمان عدم قدرة المعتدي على انتحال شخصية أحد طرفي الاتصال. وتجدر الإشارة إلى ضرورة إعادة التحقّق من هويّة طرفي الاتصال في كلّ عمليّة اتصال منفـردة. ويجب ألا يكشف نظام التحقّق من الهُويّة انتحال شخصية أحد طـرفي الاتصال من قبل الغرباء فقط، ولكن أيضًا يكشف الإعادة غير المشروعة لاتصال سابق.
- التحقّق من أصل منشـأ المعلومة(Data Origin Authentication): أي التحقّق من أصـل المعلومة بأنّها صادرة من جهتها الأصليّـة، أو بعبارة أخرى: تأكيد مصدر المعلومات. مع العلم أنّ التحقّق من أصل منشأ المعلومة لا يوفر الحماية ضد عمليّات النسخ أو التعديل(يتم كشف ذلك عن طريق عنصر سلامة المعلومة وتكاملها)، وإنّما يصادق علـى أنّ الرسالة أرسلت بالفعل من الجهة التـي تدّعي أنّها أرسلتها. تظهر الحاجة إلى هذا النوع من التحقّق من الهُويّة في التطبيقات التي لا يكون فيها اتصال مسبق، كإرسال رسالة بريد إلكتروني لأول مرة.

يمكن استخدام معيار أو أكثر للتحقق من الهُويّة حسب درجة قوة التحقّق المطلوبة. فيمكن التحقّق باستخدام معيار واحد أو معيارين أو ثلاثة معايير معًا، كما يلي:

- التحقّق باستخدام معيار واحد: هذا المعيار هو «**ماذا تعرف؟**» كاستخدام كلمات المرور أو أرقام التعريـف الشخصيـة(Personal Identification Number-PIN). ويعتمد هـذا المعيار في التحقّق من الهُويّة على طلب(إدخـال) معلومة **لا يعرفها** إلا الشخص المعني فقط، ويُعدُّ من أدنى درجات التحقّق من الهُويّة.
- التحقّق باستخدام معيارين: ويتم ذلـك باستخدام معيار «**ماذا تعرف؟**»، بالإضافة إلـى معيار آخر هو «**ماذا تملـك؟**» وتعتمد هذه الطريقة في التحقّـق من الهُويّة على طلب(إدخال) معلومة **لا يعرفها** إلا الشخص المعني فقط، ومعلومة أخرى **لا يملكها** إلا الشخص نفسه أيضًا. ويوفّر التحقّق باستخدام معيارين درجة جيّدة من درجات

التحقّق من الهُويّة أعلى مـن التحقّق باستخدام معيار واحد. ومن الأمثلة على ذلك استخدام بطاقات الصّرف الإلكتروني (Automatic Teller Machine-ATM) حيث يتم التحقّق من هويّة الشخص من خلال رقم بطاقة الصراف التي لا يملكها إلا هو، ثم إدخال الرقم السرّي الذي لا يعرفه إلا هو كذلك، ولا يمكن أن يغني أحدهما عن الآخر. ومثال آخر هو ما تتخـذه بعض المصارف من إجراءات عند الدخول إلى الخدمات البنكيّة من خلال موقع المصرف على شبكة الإنترنت، حيث بعد أن يُدخِل المستخدم كلمة المرور التي لا يعرفهـا إلا هو يرسل له البنك رسالـة نصّية بها رقم سرّي عشوائي يُستخدم لمرّة واحدة على هاتف المستخدم المحمول الذي يفترض أنّه لا يملكه إلا هو، وسبق تسجيله لدى المصرف من قبل المستخدم.

- التحقّق باستخدام ثلاثة معايير: ويتم ذلك باستخدام معيار «**ماذا تعرف؟**» ومعيار «**ماذا تملك؟**» بالإضافة إلى معيار ثالث هو «**من أنت؟**». وتعتمد هذه الطريقة في التحقّق من الهُويّة على طلب (إدخال) معلومة **لا يعرفها** إلا الشخص المعني فقط، ومعلومة أخرى **لا يملكها** إلا الشخص نفسه، ومعلومة ثالثة من واحدة أو أكثر من **خصائص الشخص** الحيويّة التي تميّزه من غيره، كبصمات الأصابع والعين، وأبعاد راحة اليد والوجه، والتعرّف إلى الصوت، وغير ذلك. وتوفّر هذا الطريقة أعلى درجات التحقّق من الهُويّة، لكنها تحتاج إلى أجهزة وبرامج إضافيّة، وتُعدُّ أكثر تعقيدًا من سابقاتها. وفي بعض الحالات ومـن أجل إزالة التعقيد في هذه الطريقة قـد يُكتفى بمعيار «من أنت؟» فقط، والاستغناء عن المعيارين الآخريـن. فبمجرد تمرير الإصبع على قارئ البصمات يُسمح للمستخدم بالدخول دون طلب إدخال اسم المستخدم وكلمة المرور.

من الأمثلـة على الخروقات الممكنة لأمن المعلومات التي يمكـن أن تتم في حال عدم توفر عنصر "التحقّق من الهُويّة" هي إمكانية دخول أشخاص غير مصرّح لهم إلى شبكة المنشأة أو أنظمتها الداخليّة، و من ثَمَّ حصول اطّلاع غير مشروع على معلومات المنشأة. ومثال آخر هو إمكانيّة استخدام بعض منسوبي المنشأة أسماء مستخدمين وكلمات مرور لموظّفين آخرين،

والاطّلاع على معلومات غير مصرّح لهم بالاطّلاع عليها، أو القيام بأعمال وإجراءات ليست من اختصاصهم، أو قيامهم بأعمال تخريبيّة. ويمكن حصول ذلك عند استخدام نظام تحقّق من الهُويّة بمعيار واحد فقط. أمّا لو تم استخدام نظام تحقق من الهُويّة بثلاثة معايير فسيكون ذلك صعبًا جدًّا وقد يصل إلى درجة المستحيل.

٣-٤ التحكّم بالوصول (Access Control)

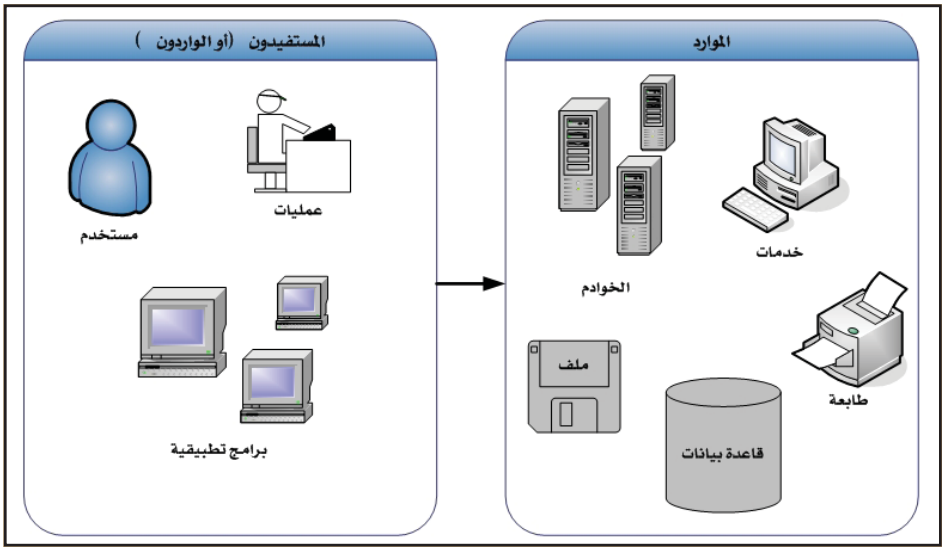
التحكّم بالوصول هو طُرُق (أو وظائف) الحماية التي تتحكّم بوصول المستخدمين أو الأنظمة إلى موارد المنشأة، كالأجهـزة الرئيسة والبيانات المركزيّة، أو بعبارة أخرى: منع الاستخدام غير المرخص به للموارد[1]. فتلك الطُّـرُق هي التي تحمي الأنظمة ومـوارد المنشأة المختلفة من الوصول غير الشرعي، كما أنها تساعد في تحديد مستوى التّخويل (Authorization) المصرّح به بعد نجاح عملية التحقّق من الهُويّة.

يأتي عنصر التحكّم بالوصول بعد عنصر التحقّق من الهُويّة. فعندما يتم التحقّق من هويّة الشخص ويُسمح له بالدخول إلى شبكة الحاسب الآلي مثلًا، فإنّه يجري التحكّم باستخدامه لموارد محدّدة من الشبكة، وليس جميع الموارد عن طريق التحكّم بالوصول. من أجل ذلك تُحدّد قائمة التحكّم بالوصول (Access Control List-ACL) للموارد المهمة في الشبكة، والتي تحدد الأشخاص المصرّح لهم فقط باستخدامها (وإن كان مصرحًا لهم بالدخول إلى الشبكة عمومًا). ويشمل ذلك منع الاستخدام غير المرخّص به لأيّ معلومة، وكذلك تحديد صلاحيّات محدّدة للأشخاص المصرّح لهم بالوصول إلى المعلومات، لاستخدامها والاطّلاع عليها تحت شروط محدّدة. فيمكن أن يكون هناك أشخاص لهم صلاحيّة الاطلاع (القراءة) فقط، وآخرون لهم صلاحيّة الطباعة، وآخرون لهم صلاحية الحذف ....، وهكذا.

ممّا تجدر الإشارة إليه أنّ التحكّم بالوصول لا يحكم عمليّة وصول المستخدمين للموارد المختلفة فحسب، بل يحكم كذلك وصول الأنظمة الأخرى (ليسوا مستخدمين عاديين) إلى تلك الموارد. ولتوضيح ذلك فإنّه يجب أولًا التعرّف إلى مفهومي «**المستفيد**» و «**المورد**». فيقصد بالمستفيد (ويمكن أن يطلق عليه «الوارد») هنا الشيء النّشط الذي يطلب الوصول إلى أيّ

١- يعبّر عن ذلك في اللغة الإنجليزية بالآتي: The prevention of unauthorized use of resources.

مورد من موارد المنشأة، سواءً أكان ذلك المستفيد شخصًا مستخدمًا (Normal User)، أم برنامجًا (Program)، أم عمليّـة (Process). والمورد هو الكائن غير النشط (أو الخامل) الذي يحتـوي المعلومات. ومن الأمثلة على الموارد: أجهزة الحاسـب الآلي، وقواعد البيانات، والملفّات، والطابعات، والأدلة، ... إلخ. فعندما تبحث في قاعدة البيانات فأنت المستفيد النّشط، وقاعدة البيانات هي المورد غير النشط، انظر الشكل (٣-١).

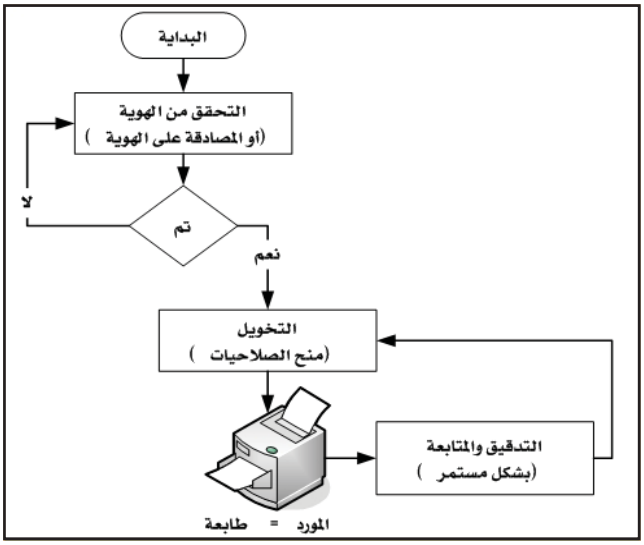


الشكل (٣-١): المستفيدون هم الأشياء النّشطة التي تصل إلى الموارد غير النشطة.

٣-٤-١ مراحل التحكّم بالوصول

يُعدُّ التحكّم بالوصول من أوائل خطوط الدفاع عن موارد المنشأة. فيمكن اعتبار أنّ مجرّد إدخال «اسم المستخدم» و «كلمة المرور» هو تحكّم بالوصول للشبكة أو للجهاز. وبعد إتمام عمليّة الدخول، قد يحاول المستخدم الوصـول إلى ملفّ معيّن، وهذا الملفّ لديه قائمة بالمستخدمين والمجموعات المسموح لهم بالوصول إليه (ACL) فإذا لم يكن ذلك المستخدم من ضمن تلك القائمة، فلن يُسمح له. كذلك الحال لموارد المنشأة الأخرى، كالأجهزة، والطابعات، والماسحات الضوئيّة، وقواعـد البيانات، وغير ذلك من الموارد المتاحة. ومن ثـمّ يمكن القول إنّ التحكّم بالوصول يعطي المنشأة إمكانيّة تقييد استخدام مواردها ومراقبة ذلك الاستخدام.

لكي يتمكّـن المستفيد (مستخدم أو برنامج أو عمليّة أو غيره) مـن الوصول إلى مورد ما، واستخدامه، أو الاستفادة منه، فإنّه يجب أن يمرّ بمرحلتين قبليّتين للتحكّم بوصوله إلى ذلك المورد هما: التحقّق من الهُويّة، والتخويل، ثم مرحلة ثالثة بعد وصوله للمورد واستخدامه: هي التدقيق والمراقبة، كما يوضح ذلك الشكل (٣-٢)[١].



الشكل (٣-٢): مراحل التحكّم بالوصول

و وفقًا لتلك المراحل فإنّه يجب على المستخدم أوّلًا أن يحدّد هويّته، وأنّه الشخص المعني لا غيره، ثم بعد ذلك يُثبت ما ادّعاه من أنّه ذلك الشخص من خلال أوراق الثبوتيّة التي يجب أن تكون بحوزته، ثم بعد ذلك يكون لديـه الحق في الوصول إلى ذلك المورد واستخدامه وفق صلاحيّات أو مزايا محدّدة. وبعد الوصول للمورد واستخدامه لا بدّ من متابعة ذلك الاستخدام وتسجيل ما يدور فيه من أجـل المحاسبة والمراقبة لجميع الأنشطة التـي تتم على المورد. ولا يمكن أن تتـم عمليّة المتابعة هذه ما لم يكن المستفيد معروفًـا ومحدّدًا بصفة فريدة قطعيّة، وما لم تكن جميع أنشطته واستخداماته للمورد مسجلة.

على الرغم من تقارب معاني هذه المراحل والتكامل فيما بينها، إلّا أنّ لكلٍّ منها دورًا محدّدًا في سلسلة التحكّم بالوصول، وتؤدّي مهمّة محدّدة. فقد يتم التعريف بالمستخدم والمصادقة على

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

هويته بصورة صحيحة، ويجتاز المستخـدم هذه المرحلة، لكن قد لا يكون لديه حقّ استخدام المورد، و من ثَمَّ فهو ليس مخوّلًا باستخدامه، وقد يكون المستخدم مخوّلًا باستخدام مورد من الموارد ولديه الامتيازات والصلاحيّات المطلوبة، لكن لم يجري التعرّف إليه، ولا المصادقة على هوّيته، و من ثَمَّ لا يمكنه الوصول إلى المورد. وفيما يلي نستعرض هذه المراحل بشكل موجز.

٣-٤-١-١ المرحلة الأولى: التحقّق من الهُويّة (Authentication)

كما مر معنا فإنّ التحقّق من الهُويّة هي طريقـة للتأكد من أن المستفيد هو من ادعى أنه هو. ويمكن تحقيق ذلك من خلال اسـم المستخدم أو رقم الحساب في الحالات البسيطة، أو باستخدام إحدى طُرُق التحقّق من الهُويّة، كما شرحناه سابقًا في موضوع «التحقّق من الهُويّة». وبشكل عام، فإنّه يلزم التحقّق من هويّة المستفيد كخطّة أولى للوصول إلى موارد المنشأة.

بعد إتمـام هذه المرحلة، يجري مقارنـة معلومات التحقّق من الهُويّـة المُحصّلة منها، مع المعلومات المخزّنة عن المورد، وفي حال عدم المطابقة يُعدُّ هذا المستفيد غير مصرّح له وغير معروف للمورّد، وتقف عمليّة التحكّم بالوصول هنا، و يُرفض طلب المستفيد. أمّا إذا تطابقت فهو معروف للمورد وتمّت المصادقة على هويّته، لكن لم تنته عمليّة التحكّم بالوصول بعد، إذ إنه حتى الآن لا يمكن للمستفيد أن يستخدم المورد دون الحصول على التخويل أو صلاحيّات الاستخدام اللازمة.

٣-٤-١-٢ المرحلة الثانية: التخويل أو الترخيص (Authorization)

بعد أن يصبح المستفيد معروفًا، وبعد أن تمت المصادقة على هويّته، تنتقل عمليّة التحكّم بالوصول إلى الخطوة الثانية، وهي التأكّد من أنّ المستفيد الذي جرى التعرف إليه والمصادقة على هويّته لديه الصلاحيّات والامتيازات التي تخوّله استخدام المورد وتنفيذ العمليّات التي يريدها عليه. ويمكن تحقيق ذلك من خلال فحص قوائم التحكّم بالوصول (ACLs) الخاصة بالمورد، لمعرفة هل لهذا المستفيد حق الاستخدام؟ ومـا الامتيازات والصلاحيّات التي يتمتع بها؟ ومن ثم ما العمليّات التي يمكن تنفيذها على ذلك المورد؟

يلعب التخويل دورًا رئيسًا في التحكّم بوصول المستخدمين إلى الموارد بشكل يضمن الاستخدام

الصحيح لتلك الموارد، دونما تقييد في الصلاحيّات الممنوحة، وهو ما قد يخلّ بالعمل، ودونما إفراط في منح الصلاحيّات، ينتج عنه عدم السيطرة على المورد وإساءة استخدامه، بل قد يتعدّى الأمر ذلك إلى الإخلال بمصالح المنشأة. فقد يقول قائل: ما الفائدة من أنظمة جيّدة للتعريف بالهويّة، والتحقّق من صحّتها، وهي في النهاية ستسمح للمستخدمين بالوصول إلى الموارد، ثم استخدامها دونما شرط أو قيد؟ لذلك جاء دور التخويل لمنح الصلاحيّات المناسبة للمستخدمين دونما إفراط أو تفريط. ويمكن التحكّم بمنح الصلاحيّات وفق المعايير الآتية:

- المنح بناءً على **دور** المستخدم: بهذا الطريقة يُمنح المستخدمون الصلاحيّات المناسبة بناءً على أدوارهم والمهام التي يقومون بها. فعلى سبيل المثال، لا بدّ أن يكون لدى الشخص الذي يقوم بمهمة أخذ النُّسخ الاحتياطيّة صلاحيّة القراءة وصلاحية النَّسخ، حتى يتسنّى له القيام بدوره، وأمّا الشخص الذي ينحصر دوره في الاطّلاع على سجلّات الأعمال (Log Files) من أجل قراءتها وتمريرها للمهندسين فتكفيه صلاحيّة القراءة، ولا يحتاج إلى صلاحيّة الحذف أو التعديل.
- المنح بناءً على **الموقع**: فيمكن السيطرة على مورد مهم من خلال عدم السماح بالدخول إليه من بعد، وإلزام من يرغب الدخول إليه أو استخدامه بالوجود في المكان نفسه الذي يوجد فيه المورد. ومن الأمثلة على ذلك عدم السماح بالعمل على الخوادم الرئيسة (Servers) من بعد، وإلزام من يرغب في العمل عليها بالحضور إلى مقر مركز البيانات (Data Center)، ومن ثم تسجيل دخوله. والسبب وراء ذلك هو من أجل ضمان إجراء عمليّات المتابعة والتحكم، ومعرفة كلّ ما يجري عمله على تلك الخوادم، والسيطرة المركزيّة على عمليّات التعديل والتهيئة التي تتم عليها.
- المنح في **أوقات** محدّدة: فيمكن منح المستخدم صلاحيّات الدخول (أيًّا كان نوعها) إلى مورد من الموارد في أوقات وتواريخ محدّدة. فمثلًا لا يسمح بالدخول إلى نظام الرواتب من الساعة الثامنة صباحًا حتى الساعة الثانية بعد الظهر في آخر ثلاثة أيام من كل شهر، ويمكن لبنك من البنوك أن يفرض عدم السماح بإجراء أيّ عمليّة بنكيّة خارج الدوام

الرسمي مهما كانت، وعندما يكون البنك مقفلًا. كذلك الحال يمكن لموظّف في إجازة أن يستمر باستخدام البريد الإلكتروني، لكن لا يمكنه الدخول إلى وثائق المنشأة الإلكترونيّة.

- المنح بناءً على **الإجراء** (أو العمليّة): يمكن استخدام هذا المعيار لتحديد نوع البيانات التي يتم الوصول إليها، وما العمليّات المسموح إجراؤها على هذه البيانات؟ فمثلًا، يمكن لبنك أن يسمح لعملائه بتصفح حساباتهم ومعرفة أرصدتهم من خلال موقع البنك على شبكة الإنترنت دون إجراء أيّ عمليّة تحويل ماليّة، حتى يحصل العميل على صلاحيّات ومستوى أمني أعلى. ويمكن لصرّاف البنك أن يصرف أيّ شيك بمبلغ ألفي ريال فأقل، وما فوق ذلك لا يمكنه صرفه حتى يوافق مدير العمليّات في البنك على ذلك من خلال إدخال كلمة المرور أو الكود الخاص به، ويمكن لمدير قاعدة البيانات أن ينشئ قاعدة بيانات للعاملين بالمنشأة، بينما لا يمكنه الاطّلاع على بعض الحقول السِّريّة المخزّنة فيها.
- منح الصلاحيّات **للمجموعات**: إذا كان هناك عدد من المستخدمين يحتاجون إلى الصلاحيّات نفسها على البيانات أو الموارد نفسها ، فإنّه من الأفضل ضمّ هؤلاء المستخدمين في مجموعة واحدة، ثم منح الصلاحيّات اللازمة لتلك المجموعة مرّة واحدة. وتتميّز هذه الطريقة بسهولة التنفيذ والمتابعة والتحكّم، وكذلك توفير الوقت والجهد اللازمين لإدارة العدد نفسه من المستخدمين، كما لو كانوا مستخدمًا واحدًا. وتلعب هذه الطريقة دورًا رئيسًا في إدارة صلاحيّات المستخدمين في الأنظمة الحديثة، حتى أصبحت من المسلَّمات الضرورية في كل نظام.
- استخدام طريقة **عدم السماح الافتراضي** أو التلقائي: ومعنى ذلك أن تكون الإعدادات الافتراضيّة هي عدم السماح لأيّ مستخدم حتى يتم منحه الصلاحيّة اللّازمة التي تحلّ محلّ الإعدادات الافتراضيّة. ويمكن استخدام العبارة الآتية لوصف هذا المعيار: « لا تمنح الصلاحيّة تلقائيًّا، وتبقى كذلك حتى تمنح عمليًّا». فبدلًا من منح الصلاحيّات كافة ، ثم البدء في تعطيل كلّ صلاحيّة لا يحتاج إليها المستخدم، فإنّ من الأفضل البدء من الصفر دون أيّ صلاحيّة، ثم منح كل صلاحيّة يحتاج إليها المستخدم واحدة تلو الأخرى، حتى

تكتمل جميع الصلاحيّات التي يحتاج إليها المستخدم. ومن الأمثلة الشهيرة على ذلك، هو أنّ قوائم التحكّم بالوصول في الموجّهات (Routers) تكون خالية تلقائيًّا، ثم تتم الإضافة إليها حسب الحاجة، ومثال آخر هو أنّ تكون إعدادات جدار الحماية (Firewall) مهيأة لعدم السماح بمرور أيّ نوع من أنواع حزم البيانات، ثم بعد ذلك تتم إضافة ما تظهر الحاجة إليه في حينه، ضمانًا للحصول على أعلى عمليّة تنقيح (أو فلترة) ممكنة.

- **مراجعة** الصلاحيّات دوريًّا: مع مرور الوقت ومع تنقّل الموظّف من قسم إلى قسم، ومن إدارة إلى أخرى، قد تختلف في مهامها، يتراكم لديه العديد من الصلاحيّات التي ربما لا يحتاج إليها في وضعه الحالي، وبذلك قد تكون بعض موارد المنشأة في خطر الاستخدام غير المشروع. لذلك يفضّل- بشدّة- أن تجري مراجعة الصلاحيّات الممنوحة لكلّ مستخدم، وهل ما زال يحتاج إليها؟ بشكل دوريّ[1] ، من أجل إلغاء الصلاحيّات التي انتفت الحاجة إليها.

أخيرًا، يمكن القول إنّ تقييد المعلومات بقوائم وصول طويلة ومعقّدة قد ينتج عنه عدم القدرة على الوصول للمعلومات أو الموارد المطلوبة في الأوقات المناسبة. وبالمقابل، فإنّ ترك الموارد المهمة مفتوحة لأيّ أحد قد يشكل خللًا أمنيًّا، وقد يتسبّب في استنزاف الموارد بشكل غير منضبط. ولتحقيق الموازنة المطلوبة فإنّ مستوى الحماية المطبّق لا بدّ أن يسمح بوصول معقول إلى المعلومات، مع الأخذ بالاعتبار جميع التهديدات المحتملة. فعلى سبيل المثال، ربما يشكّل حجب كامل قاعدة البيانات عاملًا رئيسًا في عدم الحصول على المعلومة، وعلى الجانب الآخر، فإنّ فتح قاعدة البيانات بالكامل يشكل خللًا أمنيًّا، والحلّ المناسب في هذه الحالة هو حجب بعض الحقول المهمّة في قاعدة البيانات، وترك بعضها الآخر (غير المهم) مفتوحًا.

٣-٤-١-٣ المرحلة الثالثة: التدقيق والمتابعة (Auditing)

تهدف عمليّة التدقيق هنا إلى متابعة عمليّات المستخدمين على الموارد، وتسجيلها من أجل مراجعتها، ومعرفة أيّ خلل أو تجاوز للصلاحيّات الممنوحة لكلّ مستخدم. وبناءً على نتائج هذه العمليّة تُتّخذ الإجراءات المناسبة للخلل أو التجاوز الموجودَين، ومن ذلك:

- حجب المستخدم نهائيًّا وتعطيل حسابه، و من ثَمَّ لا يمكنه استخدام أيّ مورد، وهذا

١- يوصي المؤلف بأن تتم مراجعة الصلاحيات بشكل عام كل ستة اشهر.

الإجراء يناسب التجاوزات الخطيرة المتكرّرة من مستخدم محدّد.

- حجب المورد عن جميع المستخدمين بمن فيهم من صدر منه التجاوز، وهذا الإجراء يناسب التجاوزات التي تتم على مورد مهم جدًّا وحسّاس، حتى لو كان التجاوز خفيفًا.
- حجب صلاحيّات معيّنة لدى المستخدم الذي صدر منه التجاوز، وهذا الإجراء يناسب التجاوزات الخفيفة، التي يمكن معالجتها في وقت قصير.

هناك إجراءات وآليات خاصّة بعمليّات التدقيق والمتابعة سنتناولها بالتفصيل عند شرح عنصر المتابعة، كأحد عناصر أمن المعلومات الرئيسة، ويحسُن بنا هنا الإشارة إلى أنّ الحاجة قائمة إلى عنصر المتابعة ليس فقط لإجراء عمليّات المتابعة والتدقيق على الموارد من أجل التحكّم بالوصول إليها فقط، وإنّما كعنصر أساسي نحتاج إليه لمراجعه جميع أنظمة حماية المعلومات، ومراقبتها، وتقييمها، وحل مشاكلها.

من الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توافر عنصر «التحكّم بالوصول» هي إمكانية طباعة بعض المستخدمين (ممن لديه صلاحية الاطّلاع على المعلومات المهمة والحساسة) بعد دخوله النظامي إلى شبكة المنشأة وثائق مهمّة وحسّاسة على ورق، و من ثَمَّ يمكن اطّلاع أيّ شخص على محتويات هذه الأوراق، حيث إنّها أصبحت خارج السيطرة. مثال آخر هو إمكانيّة وصول بعض المستخدمين إلى ملفّات النّسخ الاحتياطي أو ملفّات البريد الإلكتروني وحذفها، حتى ولو كان ذلك بالخطأ.

٣-٥ السِّريّة (Confidentiality)

يمكن أن يطلق على هذا العنصر أيضًا الخصوصيّة (Privacy) وتعني الحفاظ على المعلومات من أن يطّلع عليها (يقرأها ويفهمها) غير الأشخاص المصرّح لهم فقط، أو بعبارة أخرى: منع الكشف غير المصرّح به[1] . فعندما تُرسل رسالة «سريّة»، فإنّ ذلك يتطلّب أن لا يراها إلا المرسِل والمرسَل إليه فقط. فإنّ استطاع أحد الاطّلاع عليها، فإنّه لا يستطيع أن يفهم محتواها، أي يجب أن تكون غير مفهومة له.

تضمن السِّريّة وجود مستوى الحماية المطلوب في كلّ مكوّن من المكوّنات المعالجة للمعلومات،

١- يعبّر عن ذلك في اللغة الإنجليزية بالآتي: The prevention of unauthorized disclosure.

ما يساعد في الحماية من الكشف غير المصرّح به عن المعلومة. ويجب أن يتوافر هذا المستوى من الحماية في كلّ مرحلة من مراحل معالجة المعلومة، بحيث يشمل المعلومات المخزّنة، والمعلومات المرسلة، والمعلومات التي وصلت وجهتها النهائية. لذلك يجب أن تشمل السِّريّة حماية سيل البيانات من التحليل أثناء النقل (من قبل المتطفل أو من يحاول كسر سريتها). فعندما تكون البيانات مشفرة مثلًا، فإنّ ذلك يصعِّب من مهمة المحلّل بغرض فكّ شفرتها، إن لم يجعلها مستحيلة (قياسًا على الوقت المتاح).

هناك العديد من الطرق لتوفير السِّريّة تتراوح بين حجب المعلومة يدويًّا، وعدم تسليمها إلّا للأشخاص المصرّح لهم فقط إلى طُرُق التشفير الحديثة التي تعتمد على خوارزميّات رياضيّة معقّدة يصعب فكّها، إن لم يكن مستحيلًا. من هنا يمكن القول إنّه يمكن توفير عنصر السِّريّة من خلال تشفير البيانات سواءً، الثابتة منها أو المنقولة، وتطبيق سياسة صارمة للتحكّم بالوصول، وتصنيف المعلومات، وتدريب العاملين على أنظمة وسياسات أمن المعلومات تدريبًا جيّدًا.

قد يتبادر إلى ذهن بعضهم بأنه عندما يتوافر عنصر «السِّريّة» للمعلومة، فإنّها بذلك تصبح معلومة آمنة، أو بعبارة أخرى: إنّ التشفير (كوسيلة لتحقيق عنصر السِّريّة) يضمن أمن المعلومة بشكل كامل، وهذا مفهوم خاطئ، والصحيح أنّ السِّريّة ما هي إلا عنصر واحد من عدّة عناصر رئيسة، يجب توافرها جميعًا لتصبح المعلومة آمنة. فتوفُّر عنصر السِّريّة لا يضمن كشف تعديل البيانات أثناء النقل مثلًا. فقد يتم تغيير تاريخ معيّن في الرسالة المشفرة، وعندما يفكّ المستقبل شيفرة الرسالة يحصل على تاريخ مقبول ظاهريًّا له، لكنّه غير التاريخ الحقيقي، وكذلك فإنّ توافر عنصر السِّريّة لا يغني عن عنصري التحقّق من الهُويّة وعدم الإنكار.

قد يستطيع المهاجمون إحباط فاعليّة عنصر السِّريّة، باستخدام عدّة طُرُق من أهمّها: مراقبة الشبكة، وهجوم تصفّح الكتف، والهندسة الاجتماعيّة. قد يكشف المستخدم عن بعض المعلومات الحسّاسة عمدًا، أو عن طريق الخطأ عندما لا يقوم بتشفير هذه المعلومات، أو عندما

يقع ضحيّة لهجمات الهندسة الاجتماعيّة، أو بسبب اللامبالاة والإهمال وغياب الحسّ الأمني عند معالجة مثل هذه المعلومات.

من الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توافر عنصر «السِّريّة» هي إمكانية الاطّلاع على معلومات مهمّة و حسّاسة من قبل أيّ أحد، إذا ما وضعت هذه المعلومات في وسط تخزين خارجي(ذاكرة قلميّة مثلًا) وهي غير مشفّرة. فقد تكون هناك حاجة إلى نسخ بعض المعلومات على وسط تخزين خارجي، ومن ثم تصبح هذه المعلومات خارج منظومة أمن معلومات المنشأة، ولا يحميها لا تحقق من الهُويّة ولا تحكم بالوصول، إذا لم تكن مشفرة. ومثال آخر هو إرسال مرفق لبريد إلكتروني عبر البريد الإلكتروني العام،(Google أو Hotmail مثلًا)، وهو غير مشفّر وبه معلومات مهمّة جدًا. في هذه الحالة، فإنّ البريد الإلكتروني والمرفقات التي معه عرضة للاطّلاع عليها من قبل الآخرين بمن فيهم الشركة المقدّمة لخدمة البريد العام. من الأمثلة المشهورة على هذه الخروقات أيضًا، حفظ ملفات النّسخ الاحتياطي في مكان خارج المنشأة، لكنّها غير مشفّرة(وهو في حدّ ذاته إجراء سليم؛ لأنّه لا بدّ من حفظ بعض هذه النُّسخ في مكان بعيد عن المنشأة، حتى يمكن الرجوع إليها في حال تدمير المنشأة بالكامل، لكن لا بدّ من تشفيرها، إذا لم يقم نظام النسخ الاحتياطي بذلك). في هذه الحالة أُخرِجت معلومات المنشأة من داخل منظومة أمن معلوماتها نهائيًّا مهما كانت قوتها و وضعت خارجها. فإذا لم تكن مشفّرة فهي عرضة للاطّلاع عليها وفهمها من قبل الآخرين. وكذلك الحال فيما يتعلّق بالمعلومات المرسلة عبر دوائر الاتصال الخارجيّة للشبكة الواسعة(WAN)، إذا لم تكن مشفّرة. فهي في هذه الحالة عرضة للاطّلاع عليها من قبل الآخرين.

٦-٣ سلامة المعلومة وتكاملها(Data Integrity)

تعني الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة من التعديل، أو الحذف، أو الإضافة، أو إعادة التركيب، أو إعادة التوجيه. وهذا أمر مهمّ جدًّا لضمان الثقة في المعلومة وأنّها هي المعلومة الأصلية دون زيادة أو نقصان. فقد تكون المعلومة مشفّرة وسرّيّتها مضمونة،

لكن قد تتعرّض للتغيير طالما أنّها معلومة إلكترونيّة. هذا التغيير لا بدّ من إيجاد طريقة لكشفه، وهو ما يوفّره هذا العنصر، وقد يترتّب على ذلك إلغاء المعلومة وعدم الاعتماد عليها بالكليّة.

لا يهتم عنصر سلامة المعلومة وتكاملها بضمان دقّة المعلومة وسلامتها فحسب، لكن بالإضافة إلى ذللك فإنّه يُعنى بدقّة الأنظمة المُعالِجة لها وسلامتها من التلاعب أو التغيير غير المصرّح به، ويتطلّب ذلك أن تعمل الأجهزة والبرامج وأنظمة الشبكات بانسجام تامّ للمحافظة على المعلومة ومعالجتها ونقلها إلى وجهتها الصحيحة دون أيّ تغيير، أو تعديل غير متوقع. ويشمل كذلك الحفاظ على البيانات من أيّ تلويث خارجيّ، أو تداخل، أو تضارب، أو تشويش مع بيانات أخرى.

تعني سلامة المعلومة وتكاملها بأنّه تم تلقّي الرسالة تمامًا كما أرسلت بالفعل. وهذا الأمر يولّد الثقة لدى المتعامل مع المعلومة من أنّها كاملة في محتواها لم تنقص شيئًا، وأنّها صحيحة في مضمونها لم يطرأ عليها أيّ تغيير، وأنّه جرت معالجتها أثناء تنقّلها (كالحفظ وإعادة الإرسال) بالطرق الصحيحة التي لم تُحدث فيها أيّ تغيير متعّمد أو غير متعّمد.

يهتم هذا العنصر بعمليّة "كشف" عدم سلامة المعلومة وتكاملها أكثر من اهتمامه بعمليّة "منع" التعديل على المعلومة، أو "تصحيح" ذلك التعديل. والسبب في ذلك، أن أي تعديل غير مشروع على المعلومة، يجعلها معلومة غير آمنة حتى وإن جرى تصحيح التعديل. فما الفائدة من ذلك التصحيح إذا كانت المعلومة قد وصل إليها آخر وعرفها، وربما احتفظ بنسخة منها لديه؟ وهنا تبرز أهميّة كشف إعادة توجيه الرسالة وكشف إعادة تركيبها، لأنّه في مثل هذه الأحوال تصل الرسالة كاملة لكنّها غير سليمة، ولا تقف قدرة الكشف عند كشف التعديل الذي ينتج عنه تشويه واضح في المعلومة، بل يتعدى الأمر ذلك إلى كشف أيّ تعديل، حتى لو بقيت المعلومة بعده كأنها لم تتغيّر، ومثال ذلك أن يجري تغيير التاريخ أو الوقت أو اليوم إلى تاريخ أو وقت أو يوم آخرين يبدو لمتلقّي المعلومة معه أنّ شيئًا لم يتغيّر، بينما الواقع غير ذلك. فمثلًا يمكن تغيير جملة "الموعد هو يوم السبت"، لتصبح "الموعد هو يوم الأحد"، وعند استلام هذه المعلومة سيظن المتلقي أنّ المعلومة صحيحة (الموعد هو يوم الأحد)، لكن عنصر سلامة

المعلومة وتكاملها سيكشف أن هذه المعلومة قد غُيّرت، ومن ثم تفقد موثوقيتها.

من الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر "سلامة المعلومة وتكاملها" هي أخطاء المستخدمين التي ينتج عنها التعدّي على سلامة المعلومة أو الأنظمة المعالجة لها. فعلى سبيل المثال، من الممكن أن يحذف المستخدم الذي لديه صلاحيّة كاملة على محرك القرص الصلب ملفًّا من ملفات التهيئة عن غير قصد، ظنًّا منه أنّه ملفّ غير مهم، لأنّه لم يستخدمه مطلقًا، ومثال آخر هو أن يدخل المستخدم رقمًا أكبر أو أصغر مما يجب، خاصّة عند التعامل مع الأمور الماليّة، مثل إدخال(٥٠،٠٠٠) ريال بدلًا من(٥،٠٠٠) ريال. بالإضافة إلى أخطاء المستخدمين العاديين، فهناك مجال مهمّ آخر عرضة لأخطاء المبرمجين ومديري قواعد البيانات، وهو تغيير البيانات المخزّنة في قواعد البيانات أو إتلافها.

٣-٧ عدم الإنكار(Non-Repudiation)

هي الخدمة التي من خلالها يمكن منع أيّ شخص أو جهة من إنكار أيّ عمليّة قاموا بها وكشفهم. فعلى سبيل المثال إذا منحت جهة معيّنة الصلاحية لجهة أخرى لشراء منتج معيّن، ثم أنكرت بعد ذلك أنّها منحت هذه الصلاحية لتلك الجهة، فإنّ خدمة عدم الإنكار ستكشف ذلك.

في حالة إرسال رسالة بين طرفين، فإنّ عدم الإنكار يثبت إرسال المرسل لها ويثبت استقبال المستقبل لها، بحيث لا يمكن لأيّ منهما إنكار ذلك، وتزداد أهميّة هذا الإثبات بازدياد أهميّة الرسالة نفسها.

يلعب عنصر عدم الإنكار دورًا رئيسًا في إثبات وقوع العمليّات التفاعليّة(بين طرفين – أخذ وعطاء) كالعمليّات الماليّة، وعمليّات الحكومة الإلكترونيّة.

تشمل خدمة عدم الإنكار أيضًا إثبات وقوع العمليّات والإجراءات الإلكترونيّة في أوقات وتواريخ معيّنة عن طريق إلحاق بصمة التاريخ والوقت بالعمليّة نفسها(Time Stamping). فلو قام أحد ما بعمليّة إلكترونيّة معيّنة في وقت وتاريخ معيّنين ثم أنكر أنّه قام بها في ذلك الوقت

أو التاريخ، فإنّ خدمة عدم الإنكار ستكشف ذلك بالرجوع إلى بصمة التاريخ والوقت الأصليّة.

من الأمثلة على الخروقات الممكنة لأمن المعلومـات التي يمكن أن تتم في حال عدم توافر عنصر "عدم الإنـكار" إمكانيّة التنصّل من مسؤولية وثيقة معيّنة جرى توقيها (تصديقها) إلكترونيًّا من قبل أحد الأشخاص، فإذا لم يتوافر عنصر عدم الإنكار فلا يمكن إثبات أن هذا الشخص هو من وقّع هذه الوثيقة.

٣-٨ توافر المعلومة (Availability)

يقصد بتوافر المعلومة، أن تكون قابلة للوصول إليها واستخدامها حين الطلب من قبل أيّ شخص أو أيّ جهة معروفة ومحدّدة وفي أيّ وقت (مصرّح به)[١]. ويمكن القول إنّ خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحًا دائمًا (ومن هنا يطلق عليها أحيانًا «الديمومة») وهي موجّهة خصيصًا إلى أيّ خلل أو هجوم يمكن أن يؤدّي إلى عدم توافر الخدمات، ومن أمثلة ذلك: هجوم الفيروسات، وهجمـات حجب الخدمة أو منعها (Denial of Service-DoS). ويتطلّب هذا الأمر في غالب الأحيان حماية ماديّة تقنيّة (انظر التاسع الثامن: الحماية الماديّة) كتقنيات توفير نظم احتياطية للمعلومات والطاقة الكهربائيّة.

إنّ الهدف العام من عنصر توافر المعلومة هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليهـا المستخدم، وأن توفّر لها الحماية مما قد يتسبب في عطـل أو عدم توفر أي منها، وفي حال حدوث الأعطـال أو الكوارث المعلوماتيّة يجب أن تكون هناك شبكة وأجهزة وأنظمة وبرامج بديلة يجري إحلالها آليًّا وبسرعة فائقة محلّ تلك التي تعرّضت للعطـل أو الكارثة، وفق خطّة تشغيل للطوارئ يتم إقرارها والتدريب عليها جيّدًا قبل ذلك.

تجدر الإشارة إلى أنّه لا بدّ من الموازنة بين الحماية وتوافر المعلومات. فإذا سُمح لأيّ شخص بالدخول إلى المعلومة في أيّ وقت ومن أيّ مكان وبأيّ طريقة اتصال؛ فإنّنا بذلك نحصل على درجة عالية من توافر المعلومة، لكن في المقابل ينتج عن ذلك ثغرات أمنيّة كبيرة وكثيرة جدّاً، وبالمقابل، فإنّه إذا جرى تقييـد المعلومات بشكل كبير من أجل حمايتها فسيكون من الصعب

١- الناظر، سائد محمود(٢٠٠٥)، «التعمية وأمن الشبكات»، الجزء الأول.

توفير المعلومات لجميع الشرائح التي تحتاج إليها في الأوقات المناسبة، والمطلوب هو الموازنة بين ذلك؛ للوصول إلى منزلة وسطية بين المنـزلتين.

من الأمثلة على الخروقات الممكنة لأمن المعلومـات التي يمكن أن تتم في حال عدم توافر عنصر "توافر المعلومة" إمكانيّة تدمير أنظمة المنشأة باستخدام برنامج تدميري (أو فيروس تدميري) حديث الإنتاج، لا يوجد له برامج حماية أو تحديثات (رقع (Patches)) تلغي فاعليّته. ففي هذه الحالة إذا لم تكن هناك أنظمة احتياطيّة تُستخدم بدل التي دُمّرت وتضمن توافر المعلومة فسيكون هناك توقّف تام في عمل المنشأة، ولو لوقت محدود، والسبب في ذلك هو أنّ توفير التحديثات والرقع اللازمة لإلغاء فاعلية مثل هذه البرامج التدميرية والفيروسات يحتاج إلى وقت من أوّل ظهور لها، حتى يتم إنتاج التحديثـات والرقع المضادة لها ونشرها من قبل الجهات المنتجة للبرامج التطبيقيّة وأنظمة التشغيل.

٣-٩ المتابعة (أو التدقيق) (Auditing)

تهدف المتابعة (ويطلق عليها أحيانًا المحاسبة (Accountability)) إلى متابعة عمليّات المستخدمين والتحقق من فرض سياسات أمـن المعلومات، وأنّها تطبّق بشكل صحيح ودقيق. كما يمكن استخدام نتائج المتابعة كأدوات تحقيق (Investigation Tools) في حالة خرق أنظمة أمن المعلومات لإثبات وقوع بعض الأحداث، وإثبات إدانة المستخدم (أو المتهم) أو براءته من القيام بذلك الحدث. وهناك أسباب عديدة وراء ضرورة إجراء عمليّات التدقيق والمتابعة على موارد الشبكة ومستخدميها، نجملها فيما يلي:

١. التحقّق من أنّ الأجهزة والأنظمة والبرامج تعمل بشكل طبيعي (صحّي) من خلال مراجعة سجلّات الأحداث (Log Files)، ثم اتخاذ الإجراءات المناسبة، بناءً على المعلومات المتوافرة في تلك السجلّات، ومن ذلك:

أ. معرفة أيّ خطأ (Error) يقع، حيث سيكون هناك رسالة خطأ في سجّل الأحداث تشرح الخطأ، والسبب المتوقّع له، والمستخدمين أو الأنظمة أو الصلاحيّات ذات العلاقة بهذا الخطأ. وعادة ما يلجأ مديرو الشبكات والأنظمة إلى سجلّات الأحداث وعرضها على الجهات والشركات

المختصّة، كالشركات المنتجة لأنظمة التشغيل من أجل المساعدة في حلّ المشكلات والأعطال التي تحدث.

ب. معرفة رسائل التحذير (Alerts) التي تنبئ عن إمكانيّة حدوث مشكلة ما، ويستخدم هذا النوع من الرسائل التحذيريّة لمعرفة تاريخ المشكلة، ومتى بدأت؟ والظروف التي بدأت فيها، ومتى تحوّلت إلى مشكلة فعلًا؟

ج. توفير المعلومات(Information) عن الأحداث التي تتم لمجرّد الإخبار عنها فقط، وتستخدم هذه المعلومات في معرفة سلسلة الأحداث سواءً أكانت طبيعيّة وخاضعة لسياسات أمن المعلومات أم كانت مخالفة لها، ويمكن أن تستخدم هذه المعلومات لأغراض التحقيقات الجنائيّة في جرائم المعلوماتيّة.

٢. مراقبة العمليّات الضارة التي قد يقوم بها المستخدمون، عمدًا كان أو خطأً.

٣. الكشف عن عمليّات التطفّل والاختراقات.

٤. المساعدة على استعادة الأحداث ومعرفة متطلّبات الأنظمة وإعداداتها، لاستعادتها كما كانت قبل وقوع أي مشكلة.

٥. تشكّل مصدرًا قانونيًا رسميًّا للمنشأة لإثبات الأحداث أو نفيها.

٦. تشكّل مصدرًا من مصادر التقارير الرسميّة للمنشأة عن أنشطتها والمشكلات التي قد تقع فيها، أو في أنظمتها.

تعتمد المتابعة على تسجيل أنشطة كل من المستخدمين، والأنظمة، والبرامج التطبيقيّة بشكل مستمر. ويقصد بالمستخدمين: المستخدمين العاديّين، سواءً أكانوا أفرادًا أم مجموعات، ويقصد بالأنظمة: أنظمة التشغيل، سواءً أكانت لأجهزة الحاسب الآلي العادية والخوادم أم كانت للأجهزة الأخرى، كجدران الحماية(Firewalls)، والموجّهات(Routers). ويقصد بالبرامج التطبيقيّة برامج المنشأة الخاصة بأعمالها كبرامج الرواتب، والمبيعات، والمحاسبة، والميزانيّة، والبريد الإلكتروني، وبرامج السكرتارية، وغير ذلك.

تُعدُّ وثائق المتابعة(Auditing Documents) وملفّات سجلّات الأحداث(Log Files) مصادر مهمة لعمليّات المتابعة، حيث تحتوي كميّات هائلة جدًّا من المعلومات التي عادة

ما تكون بحاجة إلى تنسيق وترتيب وتلخيص؛ لجعلها في أشكال مقروءة ومفهومة يمكن الاستفادة منها.

عند إجراء عمليّات التدقيق والمتابعة يجب مراعاة النقاط الآتية:

- حفظ وثائق المتابعة كسجلّات الأحداث في مكان آمن.
- استخدام أدوات المتابعة المناسبة يؤدي إلى نتائج أفضل بحجم أقل من المعلومات، حيث إن من أكبر المشكلات التي تواجه أنظمة المتابعة هي كبر حجم معلومات المتابعة التي يلزم مراجعتها، وقد يكون بعضها غير ضروري.
- يجب المحافظة على معلومات المتابعة وسجلّات الأحداث من التغيير غير الشرعي حتى لا تفقد مصداقيتها وقانونيتها.
- يجب تدريب العاملين في حقل المتابعة، ومراجعة وثائق المتابعة جيّدًا؛ للحصول على أفضل النتائج وبأسرع الأوقات.
- حصر صلاحيّة حذف وثائق المتابعة وسجلّات الأعمال في مديري الأنظمة (Administrators) الموثوق بهم فقط.
- لا بدّ أن تشمل المتابعة جميع الأحداث، بما في ذلك الأحداث الخاصة بذوي الصلاحيّات العليا، مثل مديري الأنظمة.

تبعًا لحساسيّة عمل المنشأة وأهميّة الأحداث والمعلومات المتداولة فيها، يمكن تحديد الأنشطة التي يجب أن تدخل ضمن نطاق المتابعة، فقد تكون قائمة الأحداث الخاضعة للمتابعة طويلة جدًّا، وهذا ما يتسبّب في استهلاك الأجهزة المعالجة لها، ويستنفد مساحات التخزين المخصّصة لحفظ تلك الأحداث، وقد تكون قصيرة، وهو ما يفوّت بعض الأحداث المهمة التي كان يجب أن تتم متابعتها. وهناك حلول وسط يجري استخلاصها من التجارب السابقة للمنشآت الكبيرة والقديمة، تكفل متابعة العدد المناسب كمًّا ونوعًا من الأحداث المختلفة، وفيما يلي قائمة بأهم الأحداث التي يجب أن تدخل تحت مظلة المتابعة والتدقيق:

١. الأحداث على مستوى الأنظمة (كأنظمة تشغيل الأجهزة والخوادم)، وتشمل:

أ. أداء النظام من حيث سرعة الاستجابة للأوامر وتنفيذها.

ب. محاولات الدخول للنظام وأوقاتها وتواريخها، سواءً أكانت محاولات ناجحة أم فاشلة.

ج. عمليّات تعطيل (أو قفل) حسابات المستخدمين والنهايات الطرفيّة وأوقاتها وتواريخها.

د. عمليّات تنشيط (أو تشغيل) حسابات المستخدمين والنهايات الطرفيّة وأوقاتها وتواريخها.

ه. استخدام أدوات إدارة النظام، بحيث تشمل: الوقت والتاريخ، ومن قام بذلك.

و. استخدام الأجهزة، بحيث تشمل الوقت والتاريخ، ومن قام بذلك.

ز. العمليّات الأساسيّة، كالحذف والإضافة، بحيث تشمل: الوقت والتاريخ، ومن قام بذلك.

ح. طلبات تغيير إعدادات النظام، بحيث تشمل: الوقت والتاريخ، ومن قام بذلك.

٢. الأحداث على مستوى البرامج التطبيقيّة، وتشمل:

أ. رسائل الخطأ وأوقات ظهورها وتواريخها، والمستخدمين الذين ظهرت لديهم.

ب. الملفّات التي تُفتح أو تُغلق.

ج. التغييرات التي طرأت على الملفّات.

د. مخالفات أمن المعلومات والسياسات الأمنيّة التي ترتكب داخل البرنامج.

٣. الأحداث على مستوى المستخدمين، وتشمل:

أ. محاولات تحديد الهُويّة أو التعريف بها (Identification)، والمصادقة عليها (Authentication)، سواءً أكانت محاولات ناجحة أم فاشلة.

ب. الملفّات والمجلدات والخدمات والموارد التي يستخدمها.

ج. الأوامر (Commands) التي أنشأها.

د. مخالفات أمن المعلومات والسياسات الأمنيّة التي ارتكبها أو تسبب فيها.

يمكن مراجعة سجلّات المتابعة يدويًّا أو آليًّا، وفي كلتا الحالتين لا بدّ من تحديد طريقة المراجعة و وقتها، سواءً بشكل دوريّ أو عند حدوث أحداث معيّنة. ويمكن مراجعة سجلّات الأحداث للأنظمة المهمّة والمركزيّة بشكل يومي، بينما يمكن مراجعة سجلّات المتابعة الأخرى لفترات أطول قد تصل إلى ثلاثة أيام وإلى أسبوع في بعض الأحيان. أمّا في حالة حدوث أيّ خرق لأنظمة الحماية، أو محاولة لعمل أيّ شيء يخالف السياسات الأمنيّة للمنشأة، أو يخلّ بها؛ فيجب عندئذٍ مراجعة سجلّات الأحداث الخاصة بذلك مباشرة، وفي مثل هذه الحالات يفضّل استخدام أدوات المتابعة الآليّة، حيث يمكن لها متابعة أحداث محدّدة والرجوع لسجلّات كبيرة في أوقات قصيرة. ويمكن أيضًا استخدام أدوات تقليص حجم سجلّات الأحداث التي تقوم بإزالة المعلومات غير الضروريّة واستبقاء المعلومات المهمّة فقط. ويجب على مديري الأنظمة وضع جدول زمني لمراجعة سجلّات الأحداث ثم حفظها في مكان آمن، حتى يسهل الرجوع إليها عند الحاجة، وعادة ما تُحدّد هذا الجدول وطريقة المراجعة والحفظ ونوع البيانات التي يلزم استبقاؤها، وتلك التي يمكن حذفها في السياسة الأمنيّة الموضوعية الخاصة بذلك.

ملخص الفصل

أورد هذا الفصل شرحًا مفصلًا لعناصر أمن المعلومات الرئيسة التي يجب توافرها لحماية معلومات المنشأة، أيًّا كان نشاطها، وهذه العناصر هي: التحقّق من الهُويّة، والتحكّم بالوصول، والسِّريّة، وسلامة المعلومة وتكاملها، وعدم الإنكار، والتوفر، والتدقيق. وجميع هذه العناصر مهمّة ولا يغني أحدها عن الآخر، إذ إنّ كلًا منها يغطّي جانبًا مهمًّا من جوانب الحماية المنشودة، وإذا غاب ذلك العنصر أو كان ضعيفًا فسيكون هناك خلل أو ضعف في منظومة الحماية من ذاك الجانب الذي يغطيه ذلك العنصر. فالتحقّق من الهُويّة هو التحقّق من أنّ المستخدم سواءً أكان شخصًا أو جهازًا أو جهة لنظام ما هو حقًا من ادّعى بأنه ذلك المستخدم، والتحكّم بالوصول يمنع الاستخدام غير المرخّص به للموارد، ويُعنى عنصر السِّريّة بالحفاظ على المعلومات من أن يطّلع عليها غير الأشخاص المصرّح لهم، أو بعبارة أخرى:

منع الكشف غير المصرّح به للمعلومة، وسلامة المعلومة وتكاملها هي الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة من التعديل، أو الحذف، أو الإضافة، أو إعادة التركيب، أو إعادة التوجيه، وعدم الإنكار هي الخدمة التي مـن خلالها يمكن منع أي شخص أو جهة من إنكار أي عمليّة قام بها كشفه، وعنصر التوفر هو المسؤول عن بقاء النظام متاحًا دائمًا، ويتابع عنصر التدقيق عمليّات المستخدمين ويتحقّق من فرض سياسات أمن المعلومات وأنّها تطبّق بشكل صحيح ودقيق. وهكذا تتكامل هذه العناصر فيما بينها لتوفر سياج حماية كاملًا حول المعلومات والأنظمة المعالجة لها.

إنّ البيئات التقنيّة التي تتوافر فيها عناصر أمن المعلومات سالفة الذكر تكون في مأمن ضد تأثير الهجمات الإلكترونيّة أو أخطاء العاملين، وقـد أورد هذا الفصل أهميّة هذه العناصر، والحماية التي تقدّمها، والخروقات الأمنيّة الممكنة في حـال غيابها، ولم يبقَ إلا التعرّف إلى وسائل وتقنيات تطبيق هذه العناصر وتحقيقها على أرض الواقع، وهو ما سيتناوله الفصل الآتي.

مسائل

١. ما عنصر أمن المعلومات؟ ثم عدّد عناصر أمن المعلومات.

٢. هل هناك حدّ أدنى من عناصر أمن المعلومات؟ أم يجب توافرها جميعًا؟ اشرح ذلك.

٣. لماذا لا يكون عنصر التحقّق من الهُويّة كافيًا وبديلًا عن عنصر السِّريّة؟

٤. ما المقصود بسلامة المعلومة وتكاملها؟ ولماذا لا يكون عنصر السِّريّة كافيًا لتحقيق سلامة المعلومة وتكاملها؟

٥. ما الفرق بين التحقّق من هويّة الرسالة، والتحقق من هويّة مرسل الرسالة؟

٦. ما المقصود بعدم الإنكار؟ وضّح الحاجة له كعنصر من عناصر أمن المعلومات.

٧. تستخدم منشأة "أ" نظام التحقّق من الهُويّة ونظام التحكّم بالوصول. وتستخدم منشأة "ب" نظام التحقّق من الهُويّة فقط، وترى أنّه يغني عن التحكّم بالوصول. ناقش قوة نظام أمن المعلومات في كلا المنشأتين، مدعمًا تقييمك لكل نظام مع ذكر

الأسباب.

٨. ما "التخويل" (Authorization)؟ وهل يمكن عدّه عنصرًا ثامنًا من عناصر أمن المعلومات؟ اشرح ذلك بالاستعانة بالمراجع الموثوقة على شبكة الإنترنت.

٩. لماذا يُعدُّ عنصر "توفر المعلومة" عنصرًا من عناصر أمن المعلومات؟

١٠. وضح أهميّة عنصر التدقيق في تحقيق أمن المعلومات وكيف يتكامل مع العناصر الأخرى؟

١١. اشرح كيف يمكن استخدام عنصر التدقيق في التحقيق في تجاوزات أنظمة أمن المعلومات وخرقها؟ وفي جرائم الحاسب الآلي؟ مع إعطاء أمثلة لذلك.

١٢. ما علاقة عنصر التدقيق بعنصر عدم الإنكار؟ قارن بينهما. وهل يغني أحدهما عن الآخر؟ اشرح ذلك.

الفصل الرابع

وسائل تحقيق عنصر أمن المعلومات

أهداف الفصل

- تحديد التقنيات والوسائل التي يمكن استخدامها لتحقيق عناصر أمن المعلومات.
- التعريف بالتشفير وأنواعه، واستخدامات كل نوع، والفروق الأساسيّة بينها.
- توضيح مفهوم كلّ من التصديق الرقمي والبصمة الرقميّة واستخداماتهما.
- شرح تقنيات التحكّم بالوصول.
- شرح مفهوم الأنظمة والتجهيزات الرديفة، وكيفيّة استخدامها.
- عرض وسائل التدقيق والمتابعة وطرق استخدامها.
- توضيح كيفيّة تحقيق عناصر أمن المعلومات باستخدام الوسائل المتاحة.

ما ستتعلمه في هذا الفصل

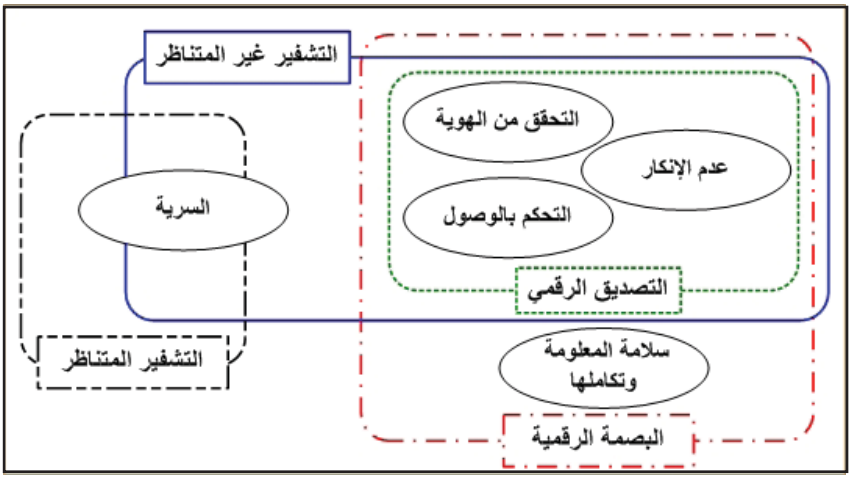
- التّشفير ومصطلحاته الأساسيّة وأنواعه: التّشفير المتناظر، والتّشفير التسلسلي، والتّشفير الكتلي، والتّشفير غير المتناظر.
- التصديق (التوقيع) الرقمي، وكيف تجري عمليّتا: التوقيع والتحقق من صحّته؟
- البصمة الرقميّة وكيفيّة استخراجها واستخدامها للتأكد من سلامة المعلومة.
- تحقيق عناصر التحقّق من الهُويّة، والتحكم بالوصول، والسرية، وسلامة المعلومة وتكاملها، وعدم الإنكار، باستخدام التّشفير والبصمة الرقميّة والتصديق الرقمي.
- مجموعة الوسائل والتقنيات المستخدمة لتحقيق عنصر التوفر.
- مجموعة الوسائل والتقنيات المستخدمة لتحقيق عنصر التدقيق.

وسائل تحقيق عناصر أمن المعلومات

٤-١ مقدّمة

رأينا في الفصل السابق عناصر أمن المعلومات وأهميّة توافر جميع هذه العناصر حتى يمكن الحصول على معلومة آمنة. لكن السؤال المطروح هو: كيف يجري تطبيق أو تحقيق كلّ عنصر من هذه العناصر؟ والجواب، هو أنّه يوجد وسائل (أو تقنيات) يمكن من خلالها تحقيق هذه العناصر، ويمكن استخدام الوسيلة نفسها لتحقيق أكثر من عنصر في الوقت نفسه ، ويلزم في بعض الأحيان استخدام أكثر من وسيلة معًا لتحقيق عنصرٍ واحدٍ من عناصر أمن المعلومات.

هناك ثلاث تقنيات رئيسة يمكن استخدامها كوحدات بناء أساسيّة لتحقيق بعض عناصر أمن المعلومات وهي: التّشفير (Encryption) بنوعيه: المتناظر وغير المتناظر، والتصديق الرقمي (Digital Signature)، والبصمة الرقميّة (Hash Value). فيمكن استخدام هذه الوسائل كوحدات بناء أساسية لتحقيق بعض عناصر أمن المعلومات وهي: التحقّق من الهُويّة، والتحكّم بالوصول، والسريّة، وسلامة المعلومة وتكاملها، كما هو موضح في الشكل (٤-١).



الشكل (٤-١): وسائل تحقيق بعض عناصر أمن المعلومات

فيمكن تحقيق عنصر السِّريّة باستخدام التّشفير المتناظر أو غير المتناظر أو بهما معًا، ويمكن تحقيق عناصر: التحقّق من الهُويّة، والتحكم بالوصول (للمنشآت الصغيرة)، وعدم

الإنكار باستخدام التّشفير غير المتناظر والتصديق الرقمي معًا. ويمكن تحقيق عنصر سلامة المعلومة وتكاملها باستخدام البصمة الرقميّة. كما يمكن استخدام التصديق الرقمي للتحقّق من هويّة الشخص(Entity Authentication)، ويستخدم مع البصمة الرقميّة للتحقق من هويّة الرسالة أو المعلومة(Data Origin Authentication).

يمكن استخدام تقنيات تسجيل الدخول الواحد، ومصفوفات قوائم التحكّم، وأنظمة كشف ومنع التطفّل؛ لتحقيق عنصر التحكّم بالوصول(Access Control) للمنشآت الكبيرة والمنشآت التي تحتاج إلى أنظمة تحكم بالوصول قويّة متخصّصة في ذلك.

أمّا عنصرا: التوفر والتدقيق فيحتاجان إلى وسائل وتقنيات أخرى، حيث يمكن تحقيق عنصر التوفر(Availability) باستخدام تقنيات الأجهزة والبرامج الرديفة وأنظمة الحماية ضدّ الهجمات التي تعطّل الخدمة(Denial of Service-DoS) ويمكن تحقيق عنصر التدقيق باستخدام تقنيات متابعة وتسجيل الأحداث، سواءً تلك التي ترد رفق أنظمة التشغيل أو التي يتم بنائها من قبل شركات متخصّصة في ذلك.

فيما يلي نوضح طريقة عمل كل وسيلة من هذه الوسائل، وكيفية استخدامها لتحقيق عناصر أمن المعلومات المرتبطة بها.

٤-٢ التّشفير(Encryption)

عرف الدكتور محمد السويل التعمية بأنها[١]: «تحويل نص واضح أو مقروء إلى نص غير واضح، أو نص معمى، بطريقة تستطيع بواسطتها الأطراف المتعارف عليها فقط أن تحل التعمية وتحول النص الغير واضح أو المعمى إلى النص المقروء». ويمكن من ذلك استخلاص تعريف التّشفير التالي: «التّشفير هو العملية التي من خلالها يتم تغيير البيانات وجعلها في شكل غير مفهوم أو غير مقروء(أي تعميتها)، بحيث لا يستطيع إرجاعها إلى وضعها الأصلي إلا الشخص أو الأشخاص المصرّح لهم فقط، الذين لديهم الأدوات اللازمة لذلك».

ويتألف التّشفير من عمليتين أساسيتين هما: التّشفير، وفك التّشفير. وحسب نوعية التّشفير، فإنّه يمكن استخدام مفتاح تشفير أو أكثر لإتمام هاتين العمليتين. وعمومًا، فهناك مصطلحات

١- السويل، محمد بن إبراهيم(١٤١٧)، «المدخل إلى علم التشفير»، ص ٢.

أساسية للتشفير لا يستغني أيّ باحث في هذا العلم من معرفتها، وهي:

- «النّص الصريح»(Plain Text): وهو الرسالة أو(البيانات) الأصليّة قبل إجراء أيّ عمليّة عليها.
- "النص المشفّر"(Cipher Text): يطلق على الرسالة المشفّرة بعد أن تشفّر.
- "التّشفير"(Encryption): تحويل الرسالة من نصّ صريح إلى نص مشفّر.
- "فك التّشفير"(Decryption): استرجاع النّصّ الصريح من النصّ المشفّر.
- "خوارزميّة التّشفير"(Encryption Algorithm): مجموعة الخطوات والعمليّات الرياضيّة التي يتم اتّباعها لتحويل النّص الصريح إلى نص مشفّر.
- "خوارزميّة فكّ التّشفير"(Decryption Algorithm): وهي الخوارزميّة العكسيّة لخوارزميّة التّشفير؛ لاسترجاع النّص الصريح من النّص المشفّر.
- "تحليل الشيفرة"(Cryptanalysis)، ويطلق عليها أيضًا(كسر الشيفرة)، وتعني التقنيات المستخدمة لفكّ تشفير رسالة بطريقة غير شرعيّة، أي كسر تشفيرها بوساطة طرف غير مصرّح له، ولا يعرف المفاتيح اللازمة لذلك[1].
- «المفتاح السِّرّي»(Key): وهو عبارة عن قيمة غير معتمدة على الرسالة يختارها نظام التّشفير أو المستخدم.

قبل أن نبدأ باستعراض عمليّات التّشفير وأنواعه، يحسن بنا أن نتعرف إلى بعض العمليّات الحسابيّة والمنطقيّة التي نحتاج إليها في هذا الفصل. فنبدأ أوّلًا بالتعرّف إلى عمليّات حسابيّة من نوع خاص تسمّى العمليّات الحسابيّة لقياس معيّن(Modular Arithmetic)، ثم نتعرف بعد ذلك إلى عمليّة منطقيّة شهيرة تستخدم بكثرة في مجال التّشفير، وهي العمليّة المنطقيّة "أو الحصريّة"(Exclusive OR-XOR).

العمليّات الحسابية لقياس معيّن(Modular Arithmetic)

هي العمليّات الحسابيّة التقليديّة: الجمع، والضرب، والقسمة، لكن لا يؤخذ الناتج كما هو، وإنّما يؤخذ باقي قسمته على القياس(Modulus)، فإذا كان القياس هو(ن)، فإنّ ناتج أي

١- السويل، محمد بن إبراهيم(١٤١٧)، «المدخل إلى علم التشفير»، ص ٢.

عمليّة سيكون الباقي من قسمة ذلك الناتج على(ن). ونبدأ بتعريف القياس، ثم ننتقل إلى العمليّات الحسابيّة لقياس معينّ، وهي: الجمع القياسي، والضرب القياسي، والقسمة القياسيّة.

تعريف «القياس»[1]: إذا كان لدينا الأعداد الصحيحة(أ ، ب ، ن) بحيث أن(ن > ٠)، فإنّ:

أ = ب قياس ن ، إذا كان(ن) يقسم(أ – ب).

ويسمّى(ن) «القياس»(Modulus)، و(ب) "الباقي".

ويمكن حساب الباقي من خلال الخاصية الآتية لأيّ عدد صحيح، حيث يمكن كتابة أيّ عدد صحيح كما يلي:

أ = ك × ن + ب لكل(٠ ≤ ب < ن).

وبما أن:(أ – ب = ك × ن)، فإنّ(ن) يقسم(أ – ب)، و من ثَمَّ فإنّ: أ = ب قياس ن.

لاحظ أن(ب) يكون محصورًا بين الصفر، و(ن – ١)، أي أنّ: ب ∈ {٠ ، ١، ٢، ... ، ن – ١}.

مثال(٤–١): إذا كان(أ = ٥٤) والقياس(ن = ١٣)، فإنّه يمكن كتابة العدد الصحيح(٥٤) كما يلي: ٥٤ = ٤ × ١٣ + ٢

و من ثَمَّ فإنّ: ٥٤ = ٢ قياس ١٣. ◊

الجمع القياسي(Modulo Addition): هو عمليّة جمع عددين، ثم قسمة الناتج على القياس(Modulus)، ثم تكون النتيجة هي الباقي من حاصل القسمة.

مثال(٤–٢): جمع العدد(٦) مع العدد(١٠) للقياس(١٣): يكون كما يلي:

(٦) +(١٠) = ١٦ = ٣ قياس ١٣.

لاحظ أن(٣) هي الباقي من قسمة(١٦) على(١٣). ولاحظ كذلك أن ناتج أي عمليّة جمع للقياس(١٣) سوف يكون محصورًا بين الصفر، و(١٢). ◊

وهناك جمع قياسي مهم ويستخدم بكثرة في تقنيات التّشفير، وهو الجمع القياسي للقياس(٢). ويجري على هذا النوع من الجمع ما يجري على الجمع القياسي العادي، غير أنّ القياس سيكون في هذه الحالة هو(٢)، وسيكون ناتج أيّ عمليّة جمع محصورًا بين الصفر، و(١).

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 14.

مثال(٤-٣): إذا كان لدينا العددين الصحيحين(أ، ب) ، فإنّ قيمة أيّ منهما للقياس(٢) ستكون إما(صفر) أو(١). وبذلك يمكن حصر جميع احتمالات هذا العددين، ثم جمعهما جمعًا قياسيًّا للقياس(٢) كما في الجدول الآتي:

أ	ب	(أ + ب) قياس ٢
٠	٠	٠
٠	١	١
١	٠	١
١	١	٠

الضرب القياسي(Modulo Multiplication): هو عمليّة ضرب عددين، ثم قسمة الناتج على القياس(Modulus)، ثم تكون النتيجة هي الباقي من حاصل القسمة.

مثال(٤-٤): ضرب العدد(٦) بالعدد(١٠) للقياس(١٣): يكون كما يلي:

(٦) × (١٠) = ٦٠ = ٨ قياس ٣.

لاحظ أن(٨) هي الباقي من قسمة(٦٠) على(١٣). ولاحظ كذلك أن ناتج أي عمليّة ضرب للقياس(١٣) سوف يكون محصورًا بين الصفر، و(١٢). ◊

القسمة القياسيّة(Modulo Division): يُستعاض عن عمليّة القسمة في هذه الحالة بضرب المقسوم بالمعكوس الضربي للمقسوم عليه، ثم قسمة الناتج على القياس(Modulus)، ثم تكون النتيجة هي الباقي من حاصل القسمة.

والمعكوس الضربي للعدد(ب) للقياس(ن) هو العدد(ع)، بحيث يحقق المعادلة الآتية:

ب × ع = ١ قياس ن

أي أنّه العدد الذي لو ضرب بالعدد(ب) للقياس(ن) لكانت النتيجة تساوي(١)، ويرمز له بالرمز($ب^{-١}$).

وبذلك فإنّ قسمة العدد(أ) على العدد(ب) للقياس(ن) ستكون كالتالي:

((أ) ÷ (ب)) قياس(ن) = ((أ) × (ب$^{-1}$)) قياس(ن).

مثال(٤-٥): قسمة العدد(٦) على العدد(١٠) للقياس(١٣): تكون كما يلي:

(٦) ÷ (١٠) = (٦) × (١٠$^{-1}$) قياس ١٣ = (٦) × (٤) = ٢٤ قياس ١٣ = ١١ قياس ١٣.

لاحظ أنّ(١٠×٤=٤٠ = ١ قياس ١٣)، أي أن معكوس(١٠) هو(٤) للقياس(١٣). وكذلك فإنّ ناتج أي عمليّة قسمة للقياس(١٣) سيكون محصورًا بين الصفر، و(١٢). ◊

العمليّة المنطقيّة «أو الحصريّة»(XOR): هي عمليّة منطقيّة(Logic Operation) تعمل على القيم الثنائية، البتات(Bits)، ولها عاملي إدخال(أ، ب) ومُخرَج واحد(ج)، ويرمز لها بالرمز(⊕). وتعمل العملية المنطقيـة: «أو الحصرية»(XOR) على عاملي الإدخال(أ، ب) وفق جدول الحقيقة المنطقي(Truth Table) الآتي:

أ	ب	أو الحصرية(أ ⊕ ب)
٠	٠	٠
٠	١	١
١	٠	١
١	١	٠

لاحظ أنّ جـدول الحقيقة المنطقي لهذه العمليّة ينطبق تمامًـا مع جدول الجمع القياسي للقياس(٢) الوارد في المثـال(٤-٣)، و من ثَمَّ فإنّه يمكن تنفيذ الجمع القياسي للقياس(٢) بتطبيق هذه العملية على العددين(الثنائيين) المراد جمعهما جمعًا قياسيًّا للقياس(٢).

وبعد أن تعرفنا إلى العمليّات الحسابيّة والمنطقيّة التي نحتاج إليها في هذا الفصل، ننتقل إلى تحديد أنواع التّشفير وتقسيماته، حيث يوجد نوعان رئيسان من التّشفير، هما:

- التّشفير المتناظر(Symmetric Encryption)، الذي ينقسم إلى:
  - التّشفير التسلسلي(Stream Cipher).
  - التّشفير الكتلي(Block Cipher).

- التّشفير غير المتناظر، أو ما يسمّى بالتّشفير باستخدام المفتاح العام(Public Key Encryption).

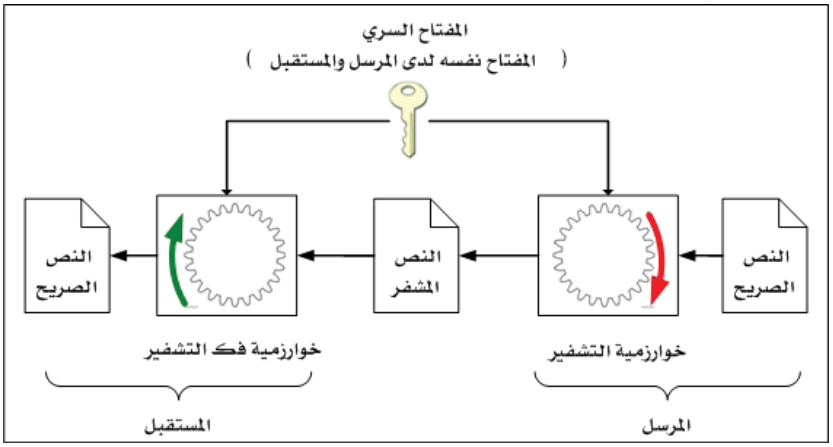
وفيما يلي نستعرض كلّ نوع من هذه الأنواع بشيء من التفصيل.

٤-٢-١ التّشفير المتناظر

هو نظام تشفير يستخدم مفتاحًا متناظرًا لدى كلٍّ من المرسل والمستقبل، بحيث يُستخدم المفتاح نفسه في عمليتي التّشفير وفكّ التّشفير، انظر الشكل(٤-٢)[١].

وتتم عمليتا التّشفير وفكّ التّشفير باستخدام الآتي:

- **عمليّة التّشفير:** تُشفّر الرسالة الأصليّة باستخدام خوارزميّة التّشفير والمفتاح السريّ المشترك للحصول على رسالة مشفرة.
- **عمليّة فك التّشفير:** يُفكّ تشفير الرسالة المشفّرة باستخدام خوارزميّة فكّ التّشفير والمفتاح السريّ المشترك للحصول على الرسالة الأصليّة.



الشكل(٤-٢): التّشفير المتناظر

كما هو موضّح في الشكل(٤-٢)، فإنّ نظام التّشفير المتناظر يتكوّن من خمسة مكوّنات رئيسة، هي:

١. النّص الصّريح: وهو النّص أو الرسالة الأصليّة المقروءة التي يجري إدخالها إلى خوارزميّة التّشفير.

١- Stinson, Douglas R.(2006), "Cryptography: Theory and Practice", Third Edition

٢. خوارزميّة التّشفير: وهي الطريقة التي تشتمل على مجموعة الخطوات التي يتم تنفيذها على النص الصريح لإنتاج النص المشفّر باستخدام المفتاح السِّريّ. وتتكون مدخلات خوارزميّة التّشفير من النص الصريح، والمفتاح السِّريّ ومخرجاتها من النص المشفّر. ومن أشهر خوارزميات التّشفير القياسي الثلاثي (Triple Data Encryption Standard (3DES)) وخوارزميّة التّشفير القياسي المتقدم (Advanced Encryption Standard-AES) .

٣. المفتاح السِّريّ: وهو المفتاح الذي يتم إدخاله إلى خوارزميّة التّشفير (بالإضافة إلى النص الصريح) لإنتاج النص المشفّر. وهو عبارة عن قيمة يتم اختيارها من قبل المستخدم أو إنتاجها من قبل النظام (مستحسن)، وهي نفس القيمة التي تستخدم للتشفير وفك التّشفير. وفي كل مرّة يجري فيها اختيار مفتاح مختلف يُنتج نص مشفَّر مختلف، حتى ولو كان للنص الصريح نفسه.

٤. النّص المشفّر: وهو الرسالة التي تنتجها خوارزميّة التّشفير من كلٍّ من النّص الصريح والمفتاح السِّريّ.

٥. خوارزميّة فك التّشفير: وهي خوارزميّة التّشفير نفسها، لكن تعمل بشكل عكسي لها، وتتكوّن مدخلات خوارزميّة فكّ التّشفير من النّص المشفّر والمفتاح السِّريّ، ومخرجاتها من النّص الصريح.

في هذا النوع من التّشفير، يجب توزيع مفتاح التّشفير بين الأطراف المرسلة والمستقبلة بطريقة آمنة جدًّا، ويمكن لعمليّة التوزيع هذه أن تحدث بشكل تقليدي (عن طريق قنوات آمنة غير إلكترونيّة) أو بإنتاج هذه المفاتيح بطريقة آلية آمنة ضمن نظام التّشفير، بحيث يُنتج المفتاح نفسه عند المرسل والمستقبل، وللحصول على نظام تشفير متناظر آمن، فإنّه يجب تحقق الشرطين الآتيين:

١. استخدام خوارزميّة تشفير (وفكّ تشفير) قويّة، والخوارزميّة القويّة هي التي لا يمكن إرجاع النصوص المشفّرة المنتجة منها إلى نصوص صريحة، حتى ولو كانت

الخوارزميّة نفسها معروفة عند من يحاول فك التّشفير(المعتدي). وعمومًا فإنّ خوارزميّة التّشفير القوية هي التي يكون المعتدي عليها غير قادر على فكّ تشفير النّص المشفّر أو اكتشاف المفاتيح السِّريّة، حتى ولو توفر لديه عدد من النصوص الصريحة والنصوص المشفّرة المقابلة لها.

٢. يجب توزيع المفتاح على كلٍّ من المرسل والمستقبل بشكل آمن، وأن يبقى هذا المفتاح سريًّا بينهما. فلو حصل أحد على المفتاح السِّريّ فإنّه سيصبح بإمكانه فكّ تشفير الرسائل المشفّرة باستخدام خوارزميّة التّشفير التي عادة ما تكون معروفة للجميع.

إنّ قوّة نظام التّشفير(سواءً أكان متناظرًا، أم غير متناظر) تكمن في سريّة المفتاح السِّريّ وقوّته، وليس في إبقاء خوارزميّة التّشفير سريّة. فمن المعروف أن لا تبقى الخوارزميّة سريّة وأن تكون معروفة حتى يمكن تطويرها من حين لآخر[١]. وللحصول على مفاتيح سرّ قوية فإنّه يمكن اتباع الآتي:

١. إنتاج المفاتيح السِّريّة بشكل آلي من قِبل النظام، وليس من قِبل المستخدم.

٢. استخدام مفاتيح سريّة عشوائيّة مختلفة لكلّ عمليّة إرسال مختلفة.

٣. استخدام مفاتيح سريّة طويلة لا تقل عن ٢٥٦ بت(Bit).

٤. استخدام مفاتيح سريّة في صيغتها الثنائيّة(٠ ، ١) فقط وليس في صيغتها المعتادة(الحروف والأرقام المعتادة).

كمثال بسيط على التّشفير المتناظر، سوف نُجري عمليّة تشفير وفكّ تشفير باستخدام خوارزميّة تبديل مواقع الحروف. يتلخّص عمل هذه الخوارزميّة في أنّها تستبدل الحرف المراد تشفيره بحرف آخر من الأحرف التي تليه في الترتيب الهجائي بناءً على مفتاح سرّي، هو عبارة عن رقم موقع الحرف البديل في الترتيب الهجائي. فمثلًا يمكن أن يُشفّر كلّ حرف

١- يقول كيركوف في نظريته الشهيرة التي افترضها عام ١٨٨٣م(المرجع: Christof Paar and Jan Pelzl(2010)): "لا بدّ أن يبقى نظام التشفير آمنًا حتى ولو عرف المهاجم كل التفاصيل عن النظام ما عدا مفتاح التشفير. وتحديدًا، يجب أن يبقى نظام التشفير آمنًا حتى ولو عرف المهاجم خوارزميّات التشفير وفك التشفير". وعلى الرغم من قدم هذه النظرية، إلا أنّها ما زالت صحيحة حتى يومنا هذا، وأثبتت الأيام أنّ الأنظمة التي تعتمد على سريّة تصميمها عرضة لهجوم الهندسة العكسيّة، كما حصل لنظام(Content Scrambling System(CSS)) لتشفير محتويات أقراص(DVD)، الذي تم كسره بمجرد معرفة تصميمه عن طريق الهندسة العكسيّة، انظر المرجع:(Christof Paar and Jan Pelzl(2010)).

باستبداله بثالث حرف يليه في الترتيب الهجائي، وبذلك يستبدل الحرف(أ) بالحرف(ث) كونه الحرف الثالث بعد الحرف(أ). ويوضح الجدول(٤-١) كلّ حرف من الحروف الهجائيّة والحرف المشفّر الذي يقابله باستخدام هذه الخوارزميّة[١]، ولفك تشفير أيّ حرف تُطبَّق خوارزميّة عكسيّة لخوارزميّة التّشفير، وهي استبدال الحرف المراد فكّ تشفيره بالحرف الثالث الذي يسبقه في الترتيب الهجائي، وفي هذه الحالة يكون فك تشفير الحرف(ث) هو الحرف(أ). ويمكن استخدام الجدول(٤-١) لكلا العمليّتين: التّشفير وفكّ التّشفير.

النّص الصريح	أ	ب	ت	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص
النّص المشفّر	ث	ج	ح	خ	د	ذ	ر	ز	س	ش	ص	ض	ط	ظ

النّص الصريح	ض	ط	ظ	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي
النّص المشفّر	ع	غ	ف	ق	ك	ل	م	ن	هـ	و	ي	أ	ب	ت

الجدول(٤-١): التّشفير المتناظر باستخدام طريقة إبدال الحروف الهجائية

يتكوّن هذا النظام البسيط من المكوّنات الأساسيّة الآتية:

١. النّص الصريح: أيّ كلمة أو جملة في اللّغة العربيّة.

٢. خوارزميّة التّشفير: استبدال الحرف بالحرف الثالث الذي يليه في الترتيب الهجائي.

٣. المفتاح السِّريّ للتشفير: (+٣).

٤. النّص المشفّر: أيّ كلمة أو جملة في اللّغة العربيّة.

٥. خوارزميّة فك التّشفير: استبدال الحرف بالحرف الثالث الذي يسبقه في الترتيب الأبجدي.

٦. المفتاح السِّريّ لفك التّشفير: (-٣).

١- السويل، محمد بن ابراهيم(١٤١٧)، «المدخل إلى علم التشفير»، ص ١٤.

لاحظ أنّ مفتاح التّشفير وفكّ التّشفير هو الرقم نفسه لكن بإشارة تختلف حسب الحالة. ففي حالة التّشفير نقوم بإضافة المفتاح(الرقم ٣) لترتيب(موقع) الحرف المراد تشفيره، وفي حالة فكّ التّشفير نطرح المفتاح(الرقم ٣) من ترتيب الحرف المراد فكّ تشفيره، وفي حالة تشفير حرف من الأحرف الثلاثة الأخيرة في الترتيب الهجائي، فإنّها تُستبدل بالأحرف في بداية الترتيب الهجائي، انظر الجدول(٤-١) و يُحسب موقع(ترتيب) الحرف بطريقة الجمع القياسي للقياس(٢٨). فمثلًا، ترتيب الحرف(أ) هو(٠)، و من ثَمَّ يمكن تشفيره إلى الحرف الذي ترتيبه: ٠ + ٣ = ٣ قياس ٢٨ = ٣، وهو الحرف(ث)، ومثال آخر: ترتيب الحرف(و) هو(٢٦)، و من ثَمَّ يمكن تشفيره إلى الحرف الذي ترتيبه: ٢٦ + ٣ = ٢٩ قياس ٢٨ = ١، وهو الحرف(ب) لاحظ أنّ ترتيب الحروف يبدأ بالرقم(٠) للحرف(أ) وينتهي بالرقم(٢٧) للحرف(ي).

بتشفير الجملة «أمن المعلومات» باستخدام النظام أعلاه فإنّنا نحصل على النّص المشفّر «ثوي ثهوقهبوثح»، كما أنه يمكن الحصول على الجملة(أمن المعلومات) مرّة أخرى بفكّ تشفير النّص المشفّر «ثوي ثهوقهبوثح» باستخدام النظام نفسه.

إنّ نظام التّشفير المتناظر باستخدام خوارزميّة تبديل الحروف فقط، يُعدُّ نظام تشفير ضعيفًا جدًا، والسبب في ذلك أنّه يمكن كسره بسهولة عن طريق تجريب جميع الاحتمالات لكلّ حرف التي لا تتعدى(٢٨) احتمالًا، حتى يمكن العثور على نصوص مقروءة ذات معنى واضح.

تجدر الإشارة إلى أنّ أنظمة التّشفير المتناظر المعاصرة، كنظام التّشفير القياسي المتقدم(AES)، تُعدُّ أنظمة آمنة ولم تُكسر حتى الآن، وهي تعتمد على خوارزميّات تشفير معقّدة روعي فيها احتمالات الهجوم عليها وسدّها. الشكل(٤-٣) يوضّح مقطعًا من ملفّ نصي(نص صريح) والنص المشفّر المقابل له باستخدام خوارزميّة التّشفير القياسي المتقدم(AES)، وبمفتاح بطول(٢٥٦) بت. يوضح هذا الشكل أنّه لا جدوى من محاولة كسره بطريقه تجريب كل الاحتمالات.

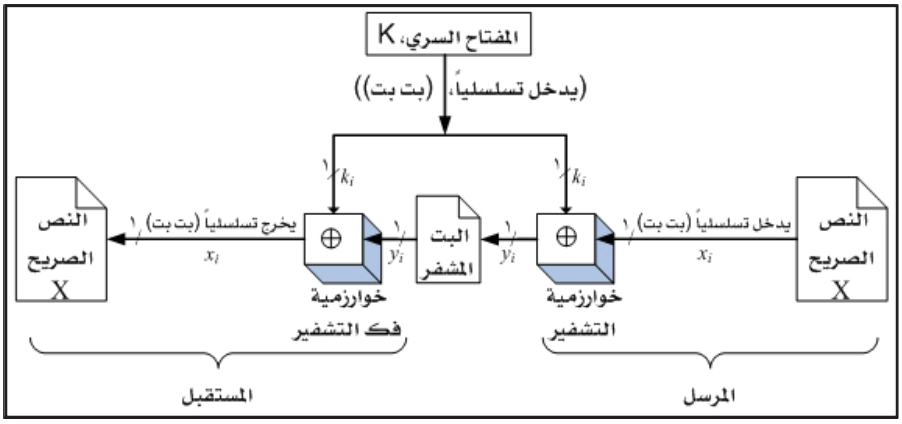
الشكل(٤-٣): مقطع من ملف نصي صريح والمقطع المقابل له المشفّر باستخدام خوارزميّة التّشفير القياسي المتقدم(AES)

طبقًا لما أورده كريستوف بار في كتابه(Understanding Cryptography)[١]، يمكن تقسيم التّشفير المتناظر إلى قسمين رئيسين، هما: التّشفير التسلسلي(Stream Cipher)، والتّشفير الكتلي(Block Cipher). وفيما يلي نستعرض هذين النوعين بشيء من التفصيل.

٤-٢-١-١ التّشفير التسلسلي(Stream Cipher)

في هذا النوع تُشفّر كلّ خانة ثنائيّة – بت – (Bit) من النّص الصريح وحدها بشكل منفرد، بحيث يؤخذ النّص الصريح تسلسليًّا خانةً خانةً (بتًا بتًا) حتى يجري الانتهاء منه، ويستخدم في هذه الحالة مفتاح تشفير تسلسلي أيضًا، بحيث تستخدم كل خانة (بت) منه لتشفير خانة واحدة (بتًا واحدًا) من النّص الصريح، وإنتاج خانة واحدة (بتًّا واحدًا) من النّص المشفّر، كما يوضح ذلك الشكل(٤-٤).

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 29.



الشكل(٤-٤): التّشفير التسلسلي

وتتم عمليتا التّشفير وفكّ التّشفير وفق الآتي:

- **عمليّة التّشفير:** تكون بتطبيق العمليّة المنطقيّة «أو الحصريّة»(XOR) (أو الجمع القياسي للقياس ٢ (Modulo 2) على بت النّص الصريح، والبت الذي يقابله من مفتاح التّشفير؛ لإنتاج بتّ واحد من النّص المشفّر، وفق المعادلة الرياضيّة الآتية:

$$y_i = x_i \oplus k_i$$

التي يمكن كتابتها أيضًا بالصيغة الآتية:

$$y_i = (x_i + k_i) \bmod 2$$

- **عمليّة فكّ التّشفير:** تتم بتطبيق العمليّة المنطقيّة «أو الحصريّة»(XOR) على بت النّص المشفّر، والبت الذي يقابلة من مفتاح التّشفير؛ لإنتاج بت واحد من النّص الصريح، وفق المعادلة الرياضيّة الآتية:

$$x_i = y_i \oplus k_i$$

كما هو موضّح في الشكل(٤-٤)، فإنّ النّص الصريح الكامل(X) يحوّل إلى سيل من البتات، (x_i)، قبل دخوله إلى خوارزميّة(دالة) التّشفير، وكذلك الحال لمفتاح التّشفير الكامل(K)، حيث يحوّل إلى سيل من البتات، (k_i)، قبل دخوله إلى خوارزميّة التّشفير، التي بدورها تستخدم هذا البت لتشفير بت النّص الصريح (x_i)، وتنتج بتًا واحدًا من النّص المشفّر،

(y_i). وكما في الشكل، يُعبر عن النّص الصريح الكامل بالحرف الكبير (X)، وعن كل بت منه بالحرف الصغير (x) ملحقًا بـه الحرف (i) (بوضع منخفض) ليشير إلى رقم موقع (خانة) ذلك البت في النّصـ الكامل، ويُعبر عن مفتاح التّشفير الكامـل بالحرف الكبير (K)، وعن كل بـت منه بالحرف الصغير (k) ملحقًـا به الحرف (i) (بوضع منخفضـ) ليشير إلى رقم موقع (خانة) ذلك البت في مفتاح التّشفير الكامل، ويُعبّر عن كل بت من النّص المشفّر بالحرف الصغيـر (y) ملحقًا بـه الحرف (i) (بوضع منخفض) ليشير إلـى رقم موقع (خانة) ذلك البت في النّص المشفّر الكامل، وبذلك يمكن الإشارة إلى البت الخامس من النّص الصريح بالرمز (x_5)، وإلـى البت الخامس من مفتاح التّشفير بالرمـز (k_5)، وإلى البت الخامس من النّص المشفّر بالرمز (y_5).

طالما أنّ عمليّة التّشفير تجري على كل بت من النّص الصريح، والبت الذي يقابله من مفتاح التّشفير منفردين؛ فإنّ قيمة كل منهما ستكون إمّا (صفر) أو (١). ولذلك يمكن حصر جميع احتمالات قيم هذين البتّين في أربع قيم، كمـا في الجدول (٤-٢). وبتطبيق العمليّة المنطقيّة «أو الحصريّة» (XOR) على كلّ قيمتين من هذه القيم الأربع نحصل على النتيجة الموضّحة في الجدول نفسه.

البت الصريح (x_i) (أو البت المشفّر (y_i))	بت مفتاح التّشفير (k_i)	$x_i \oplus k_i$ أو $(y_i \oplus k_i)$
٠	٠	٠
٠	١	١
١	٠	١
١	١	٠

الجدول (٤-٢): التّشفير (وفك التّشفير) باستخدام الجمع القياسي للقياس ٢

كذلك الحال لعمليّة فكّ التّشفير، فإنّ العمليّة نفسها ستجرى على كل بت من النّص المشفّر والبت الذي يقابله من مفتاح التّشفير منفردين، وستكون قيمة كل منهما إما (صفر) أو (١) وبذلك يمكـن حصر جميع احتمالات قيـم هذين البتين في نفس القيـم الأربع، كما في حالة

التّشفير، والحصول على نفس النتائج كذلك، انظـر الجدول(٤-٢). ومعنى ذلك أن عمليّة التّشفير مطابقة تمامًا لعملية فكّ التّشفـير، والاختلاف الوحيد بينهما هو أن الأولى تتعامل مع النّص الصريح، وأنّ الثانية تتعامل مع النّص المشفّر.

مثال(٤-٦): يمكن تشفير حرف الألف،(أ)، ثم فكّ تشفيره، باستخدام نظام التّشفير التسلسلي كما يلي:

١. يُمثّل حرف الألف في نظام(كود) الآسكي بالقيمة الثنائيّة الآتية:(١٠١٠٠١٠١).

٢. نفترض أن الثماني بتات الأولى من مفتاح التّشفير هي:(٠١١١٠١٠٠).

٣. بتطبيق العمليّة المنطقيّة "أو الحصريّة"(XOR) على كل بت من كود اللآسكي للحرف "أ"، والبت الذي يقابله من مفتاح التّشفير نحصل على:

(١٠١٠٠١٠١) ⊕ (٠١١١٠١٠٠) = (١١٠١٠٠٠١)

وبذلك يكون النّص المشفّر هو:(١١٠١٠٠٠١).

٤. يمكن فكّ تشفير هذا النّص، والحصول على كود الآسكي للحرف "أ" من جديد، بتطبيق العمليّة المنطقيّة "أو الحصرية"(XOR) على كلّ بت من النّص المشفّر(الحرف "أ" بعد تشفيره)، والبت الذي يقابله من مفتاح التّشفير نفسه؛ لنحصل على:

(١١٠١٠٠٠١) ⊕ (٠١١١٠١٠٠) = (١٠١٠٠١٠١)

وهو كود الآسكي للحرف «أ» ◊

مما سبق، يتّضح أنّ التّشفير التسلسلي يتميّز بالميزات الرئيسة الآتية:

- استخدام الخوارزميّة نفسها(الدالة) لعمليتي التّشفير وفك التّشفير، وهي في هذه الحالة العمليّة المنطقيّة «أو الحصريّة»(XOR)(أو الجمع القياسي للقياس ٢).
- سهولـة بناء نظـام تشفير سريـع وصغير الحجـم، سـواءً أكان نظامًـا برمجيًّا – برنامج –(Software)، أو نظامًـا ماديًّا – جهاز –(Hardware). وتعود هاتان

الخاصّيتان (السرعة، وصغر الحجم) إلى كونه نظام تشفير يتعامل مع خانة ثنائيّة واحدة (بت واحد فقط) في الوقت الواحد.

- إمكانية استخدام مفتاح تشفير تسلسلي طويل جدًا، إلى درجة أنه يمكن أن يكون طوله يساوي طول الرسالة المراد تشفيرها، وهو ما يعرف بنظام التّشفير بمفتاح المرّة الواحدة (One-Time Pad-OTP)، الذي يستخدم مفتاح تشفير عشوائيًّا يختلف في كل عمليّة تشفير.

توليد القيم الثنائية لمفتاح التّشفير

تعتمد قوّة التّشفير التسلسلي بشكل أساسي على طريقة توليد القيم الثنائيّة، البتات، لمفتاح التّشفير. فإذا كانت هذه القيم تُنتج بطريقة عشوائيّة جيدة، فسيكون من الصعب جدًّا التنبؤ بها، ومن ثم يمكن اعتبار نظام التّشفير برمّته قويًّا. ويمكن توليد سيل بتات مفتاح التّشفير بإحدى طريقتين[١]:

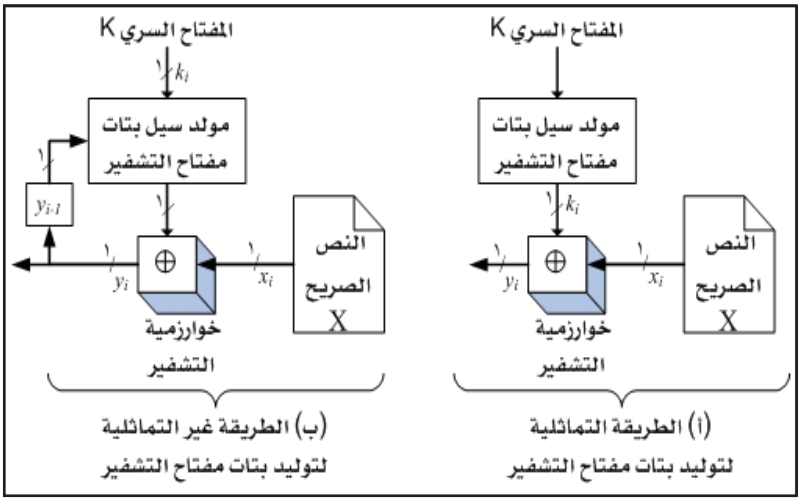
١. الطريقة التماثليّة: باستخدام مولّد يعتمد على البت الحالي، (k_i)، من مفتاح التّشفير وحده، كما هو موضح في الجزء (أ) من الشكل (٤-٥)؛ لتتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_i = x_i \oplus k_i$$

٢. الطريقة غير التماثليّة: باستخدام مولّد يعتمد على البت الحالي، (k_i)، من مفتاح التّشفير، والبت المشفّر السابق، (y_{i-1})، الذي يُربط بالمولد من خلال خط تغذية عكسيّة يغذي المولّد بالبتات المشفّرة؛ لإعادة استخدامها في التّشفير مرّة أخرى، كما هو موضّح في الجزء (ب) من الشكل (٤-٥)؛ لتتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_i = (y_{i-1} \oplus k_i) \oplus x_i$$

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 30.



الشكل(٤-٥): طُرُق توليد سيل بتات(Bits) مفتاح التّشفير في التّشفير التسلسلي

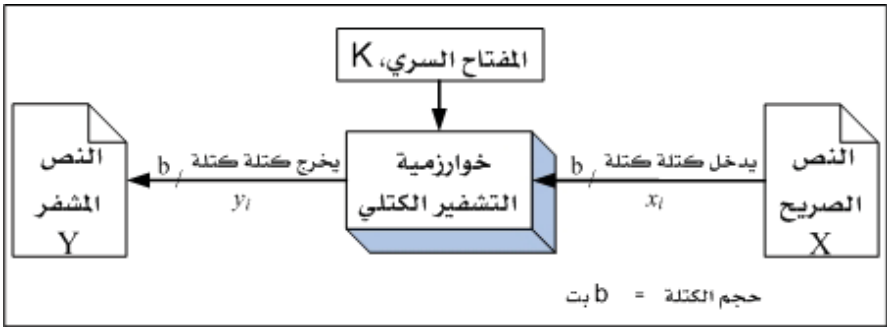
بقي أن نتعرّف مجالات استخدام التّشفير التسلسلي، حيث يُستخدم في المجالات التي تتطلّب أنظمة تشفير سريعة، وصغيرة الحجم، وفي الأجهزة التي تتوافر بها موارد حسابيّة(كالمعالجات، والذاكرات) قليلة. ويأتي تحقيق هاتين الصفتين(السرعة، وصغر الحجم) من خاصيته المذكورة آنفًا، من كونه نظام تشفير يتعامل مع خانة ثنائيّة واحدة فقط(بت واحد فقط) في الوقت الواحد، ومن أشهر مجالات استخدامه: تشفير الصوت في أنظمة الهواتف الخلويّة(Global System for Mobile Communication-GSM)، والتّشفير المضمّن في الأجهزة الصغيرة ذات الأنظمة المضمّنة(Embedded Systems)[١].

٤-٢-١-٢ التّشفير الكُتَلي(Block Cipher)

في هذا النوع من التّشفير يُجزّأ النّص الصريح إلى كُتل(Blocks) متساوية الحجم، ثم تُشفّر كلّ كتلة باستخدام نفس مفتاح التّشفير، انظر الشكل(٤-٦). لاحظ أنه يستخدم نفس مفتاح التّشفير مع كل كتلة من كتل النّص الصريح، ولا يشترط أن يكون حجمه(طوله) يساوي حجم كتلة النّص الصريح، ويختلف حجم الكتلة، وطول مفتاح التّشفير من خوارزميّة إلى أخرى. ففي خوارزميّة تشفير البيانات القياسي(Data Encryptionb Standard-DES) يكون حجم الكتلة(٦٤) بت((٨) بايتات)، وطول مفتاح التّشفير(٥٦) بت، بينما في

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 31.

خوارزميّة التّشفير القياسي المتقدم(Advanced Encryption Standard-AES)يكون حجم الكتلة(١٢٨) بت((١٦) بايت)، وطول مفتاح التّشفير(١٢٨) بت، أو(١٩٢) بت، أو(٢٥٦) بت، وإن كان(١٢٨) بت هو الأكثر انتشارًا.



الشكل(٤-٦): التّشفير الكتلي

وكما هو موضّح في الشكل(٤-٦)، فإنّ النّص الصريح الكامل(X) يحوّل إلى كُتل، (x_i)، متساوية الحجم(b بت) قبل دخوله إلى خوارزميّة التّشفير، التي بدورها تستخدم مفتاح التّشفير(K) لتشفير تلك الكتل، وإنتاج كتل النّص المشفّر(y_i) بنفس الحجم(b بت). وكما في الشكل أيضًا، يُعبّر عن النّص الصريح الكامل بالحرف الكبير(X)، وعن كل كتلة منه بالحرف الصغير(x) ملحقًا به الحرف(i)(بوضع منخفض) ليشير إلى رقم موقع(خانة) تلك الكتلة في النّص الكامل. ويُعبّر عن النّص المشفّر الكامل بالحرف الكبير(Y)، وعن كل كتلة منه بالحرف الصغير(y) ملحقًا به الحرف(i)(بوضع منخفض) ليشير إلى رقم موقع(خانة) تلك الكتلة في النّص المشفّر الكامل، وبذلك يمكن الإشارة إلى الكتلة الخامسة من النّص الصريح بالرمز(x_5)، وإلى الكتلة الخامسة من النّص المشفّر بالرمز(y_5).

تختلف عمليتا التّشفير وفكّ التّشفير، وطريقة استخدام مفتاح التّشفير من خوارزميّة إلى أخرى، ومن أشهر خوارزميات التّشفير الكتلي: خوارزميّة تشفير البيانات القياسي (Data Encryption Standard-DES)، وخوارزميّة تشفير البيانات القياسي الثلاثي(Triple Data Encryption Standard-3DES)، وخوارزميّة التّشفير القياسي المتقدّم(Advanced Encryption Standard-AES). ويتركّز عمل هذه الخوارزميّات

على تشفير كتل النّص الصريح باستخدام مفتاح التّشفير نفسه، فتشفر أي كتلة من النّص الصريح تدخل إليها، بغض النظر عن اسلوب(أو طريقة) إدخال هذه الكُتل أو طريقة توليد كتل التّشفير. فهذه الخوارزميات لا تختار الكتلة التي ستشفّرها من النّص الصريح، ولا كتلة التّشفير التي ستستخدمها في التّشفير، وإنّما تشفّر ما يدخل إليها دون أيّ تدخّل منها في الاختيار. ومن هنا برز موضوع "أساليب تشغيل التّشفير الكتلي"، الذي يبحث في أساليب اختيار هذه الكتل، وترتيب إدخالها إلى تلك الخوارزميّات، الذي هو موضوعنا الآتي.

٤-٢-١-٢-١ أساليب تشغيل التّشفير الكتلي

كما ذكرنا آنفًا، وبالرجوع إلى الشكل(٤-٦)، نجد أنّه نتيجةً لوجود عدّة خيارات لإدخال كتل النّص الصريح، وكتل النّص المشفّر إلى خوارزميّة التّشفير؛ فسيكون هنالك عدّة أساليب(Modes of Operation) لإجراء عمليّة التّشفير. فيمكن استخدام مفتاح التّشفير(K) لتشفير كتلة النّص الصريح الحاليّة(x_i)، كأحد الأساليب، كما يمكن إعادة استخدام كتلة النّص المشفّر السابقة(y_{i-1})، في تشفير كتلة النّص الصريح الحالية(x_i)، كأسلوب آخر، وبذلك يكون لدينا عدّة أساليب يمكن أن يعمل بها التّشفير الكُتَلي، من أشهرها:

١. أسلوب كتاب الترميز الإلكتروني(Electronic Code Book Mode-ECB)
٢. أسلوب كتل التّشفير المترابطة(Cipher Block Chaining Mode-CBC)
٣. أسلوب التغذية العكسية للمخرجات(Output Feedback Mode-OFB)
٤. أسلوب التغذية العكسية للنصوص المشفّرة(Cipher Feedback Mode-CFB)
٥. أسلوب العداد(Counter Mode-CTR)

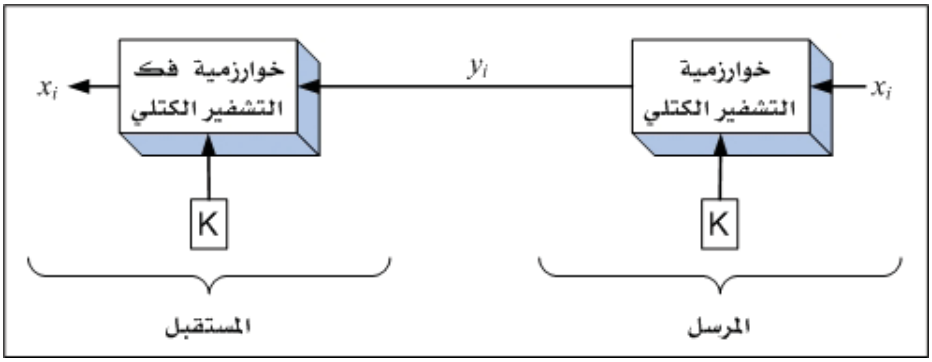
وفيما يلي نستعرض كيفية عمل هذه الأساليب.

١. أسلوب كتاب الترميز الإلكتروني(Electronic Code Book Mode-ECB)

في هذا الأسلوب، يتم تجزئة النّص الصريح إلى كتل متساوية الحجم. وتبعًا لحجم النّص الصريح فقد يكون هناك عدد من الكتل المتساوية في الحجم، ما عدا الكتلة الأخيرة قد تكون

ناقصة. فمثلًا، إذا كان حجم النّص الصريح (٦٠٠) بت؛ فيمكن تجزئته إلى أربع كتل من الحجم (١٢٨) بت ، وكتلة خامسة بحجم (٨٨) بت. ولأنّه لا بدّ أن تكون جميع الكتل متساوية في الحجم، فلا بدّ من تكملة (أو ملء (Padding)) الكتلة الأخيرة بإضافة قيم ثنائيّة ثابتة (لا علاقة لها بالنص الصريح) تلحق بها حتى يكتمل حجمها (١٢٨) بت كباقي الكتل. لذلك سيجري تكملة الكتلة الخامسة بإلحاق (٤٠) بت بها، حتى يصبح حجمها (١٢٨) بت، وهناك عدة طُرُق لإكمال حجم الكتلة الناقصة، من أشهرها إضافة بت واحد بالقيمة الثنائية "١" في نهاية الكتلة، متبوعًا بالعدد الكافي من البتات بالقيم الثنائية "صفر"، حتى يكتمل حجم الكتلة. ففي المثال السابق سيُضاف بت واحد بقيمة "١" في نهاية الكتلة الخامسة، متبوعًا بعدد (٣٩) بتًا بقيمة "صفر".

بعد ذلك يجري تشفير كلّ كتلة من النّص الصريح وحدها باستخدام مفتاح التّشفير، دون أن يكون هناك أيّ تأثير أو علاقة بعمليّة تشفير الكتل السابقة أو اللاحقة، كما يوضح ذلك الشكل (٤-٧) وتحديدًا تُشفّر كتلة النّص الصريح الأولى لتنتج كتلة النّص المشفّر (أو الكتلة المشفّرة) الأولى، وتُشفّر كتلة النّص الصريح الثانية لتنتج كتلة النّص المشفّر الثانية، ... وهكذا.



الشكل (٤-٧): اسلوب كتاب الترميز الالكتروني (ECB) للتشفير الكتلي

وتتم عمليتا التّشفير وفك التّشفير بهذا الاسلوب وفق التالي[١]:

- عمليّة التّشفير: تُشفّر كتلة النّص الصريح (x_i) باستخدام مفتاح التّشفير (K)؛

١- وليام ستولينج(١٤٣٢)، «أساسيات أمن الشبكات: تطبيقات ومعايير»، ص ٧٥-٧٧.

لإنتـاج كتلة النّص المشفّر (y_i). فلو افترضنا أنّ الرمـز (E_K) يرمز لعمليّة التّشفير باستخدام مفتاح التّشفير (K)؛ فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_i = E_K(x_i)$$

- عمليّة فكّ التّشفير: يُفكّ تشفير كتلة النّص المشفّر (y_i) باستخدام مفتاح التّشفير (K)؛ لإنتاج كتلة النّصـ الصريح (x_i). فلو افترضنـا أنّ الرمـز (E_K^{-1}) يرمز لعملية فكّ التّشفير (العمليّة العكسية للتشفـير) باستخدام مفتاح التّشفير (K)؛ فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_i = E_K^{-1}(y_i)$$

مما سبق، يتضح أنّ التّشفير الكُتَلي باستخدام أسلوب كتاب الترميز الالكتروني (ECB) يتميز بالميزات الرئيسة الآتية:

- يمكن تشفير أكثر من كُتلة في الوقت نفسه بالتوازي (Parallel) معًا. فيمكن تشفير الكتلـة رقم (١)، (أي الكتلـة x_1)، باستخدام وحدة التّشفير الأولـى، وتشفير الكتلة رقم (٢)، (أي الكتلة x_2)، باستخدام وحدة التّشفـير الثانية، ... وهكذا. كما يمكن تنفيذ عمليتي التّشفير وفك التّشفير بالتوازي معًا في الوقت نفسه ، فيمكن فكّ تشفير الكتلة رقم (٢)، (x_2)، من قبل وحدة فكّ التّشفير، بينما يجري- بالتوازي مع ذلك- تشفير الكتلة رقم (١)، (x_1)، من قبل وحدة التّشفير. وتجعل هذه الميزة (أي العمل بالتوازي) أسلوب كتاب الترميز الإلكتروني (ECB) مناسبًا للتطبيقات التي تحتاج إلى سرعة عالية في عمليّات التّشفير وفك التّشفير.
- لا يلزم اتّباع ترتيب الكتل نفسه بين عمليتي التّشفير وفكّ التّشفير. فيمكن تشفير كتل النّص الصريح بترتيب معيّن (الأولى، ثم الثانية، ثم الثالثة، مثلًا)، وفك تشفيرها بترتيب مختلف (الثالثة، ثم الثانية، ثم الأولى، مثلًا) والسبب في ذلك أنّ تشفير كل كتلة غير مرتبط بتشفير الكتل السابقة أو اللاحقة لها. وينتج عن ذلك أنّه لو فقدت بعض الكتل بعد تشفيرها، وهي في طريقها من المرسل إلى المستقبل لأيّ سبب كان،

بينمـا وصلت كتل أخرى، فإنّه يمكن فكّ تشفير الكتـل التي وصلت بغض النظر عن مصير الكتل المفقودة، التي يمكن إعادة تشفيرها وارسالها مرة اخرى.

- السهولة في البنـاء والتطبيق، حيـث إن أسلوب كتاب الترميـز الإلكتروني(ECB) هو أسهل الأساليب وأبسطها على الإطلاق؛ لأنـه يقتصر على استخدام كتل النّص الصريح الحاليـة،(x_i)، ومفتاح التّشفير(K) فقط، ولا يستخـدم أيّ نوع من أنواع التغذية العكسيّة أو الأماميّة، التي تتطلّب مزيدًا من الإجراءات، والمعادلات الرياضيّة، والدوائر الإلكترونيّة.

كأيّ نظام تشفير آخر، توجد في أسلوب كتاب الترميز الإلكتروني(ECB) العيوب الآتية:

- تشفـير كتـل متطابقـة مـن نصوص صريحـة ينتـج عنـه كتـل مشفّـرة متطابقة(Deterministic) بمعنـى أنّه لو كان لدينا كتـل متطابقة تحتوى القيم الثنائية نفسها، أي أنّ كلّ منها تساوي الأخرى، وتم تشفيرها باستخدام هذا الأسلوب، فسينتج لدينا كتل مشفرة متطابقة، وكلّ منها تساوي الأخرى أيضًا، طالما أنه يُستخدم نفس مفتاح التّشفير. والسبب في ذلك يعود إلى كون هذا الأسلوب يشبه كتاب ترميز (أو تكويد)، ومن هنا جاءت التسمية: أسلوب كتاب الترميز الإلكتروني، فكل حرف يقابله كود أو رمز معيّن لا يتغير طالما أنّ مفتاح ترميز الكتاب ثابت لا يتغيّر. وينتج عن هذا العيب نقاط الضعف الآتية:
  - يمكن للمهاجم مراقبة مخرجات وحدة التّشفير، وتحليل البيانات المارّة(Traffic Analysis)، ومعرفـة الكتل المشفّرة المتشابهة، و من ثَـمَّ يمكنه معرفة ما إذا تم إرسال الرسالة نفسها أو المعلومة مرّتين أو أكثر، ومـن ذلك أيضًا إمكانيّة معرفة بداية كلّ رسالة، من خـلال التعرّف إلى رأس الرسالـة(Message Header)، الذي عادة ما يتكرر مع كل رسالة جديدة، ويأتي في مقدّمتها، و من ثَمَّ يمكن معرفة بداية كلّ رسالة جديدة.
  - لا يصلح هـذا الأسلوب لتشفير الصور من نـوع(Bitmap) بمفتاح تشفير ثابت،

لأنّ المناطق المتشابهة في الصورة الأصليّة سينتج عنها مناطق متشابهة في الصورة المشفّرة، خاصّة في خلفيّة الصورة، التي تكون الاختلافات فيها ضئيلة جدًّا، و من ثَمَّ يمكن معرفة محتويات الصورة (حتى ولو تقريبيًّا) بالعين المجردة.

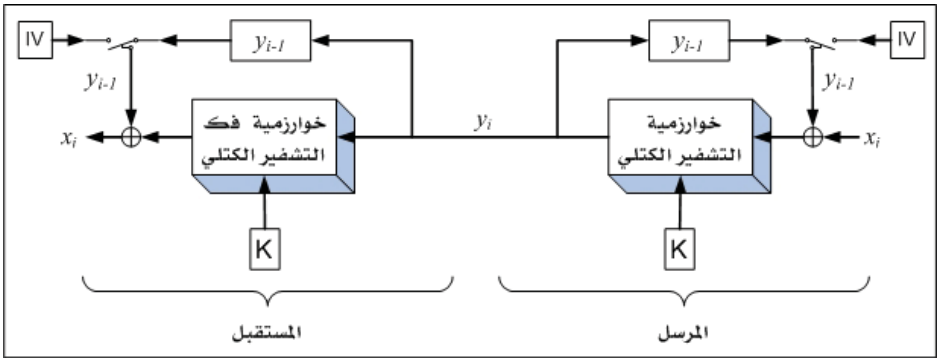
- بما أنه يتم تشفير كلّ كتلة من النّص الصريح وحدها دون التأثر بالكتل السابقة أو اللاحقة؛ فإنّ هذا الأسلوب عرضة لتغيير ترتيب الكتل المشفّرة أو حذفها دون التنبه لذلك، و من ثَمَّ قد تصل هذه الكتل إلى المستقبل مختلفة الترتيب أو بعضها مفقود، وقد ينتج عنها نصوص مقبولة لديه بعد فكّ تشفيرها، ومن ثم قد لا يتنبّه لعمليّة تغيير الترتيب أو الحذف التي حدثت.
- هذا الأسلوب عرضة لهجوم التعويض (Substitution Attack)، الذي يتم فيه استبدال النصوص المشفّرة بأخرى مشفرة ومعروفة لدى المهاجم، و من ثَمَّ يمكن توجيه الرسالة إلى غير وجهتها الأصلية، إذا لم يتم تطبيق عنصر سلامة وتكامل المعلومة، سواءً بحساب البصمة الرقميّة (Hash Value) للرسالة، أو بتوقيع الرسالة إلكترونيًّا.

٢. أسلوب كتل التّشفير المترابطة (Cipher Block Chaining Mode-CBC)

في هذا الأسلوب، يتم تجزئة النّص الصريح إلى كتل متساوية الحجم، مع تكملة (أو ملء (Padding) الكتلة الأخيرة، إذا كانت ناقصة، تمامًا كما في أسلوب كتاب الترميز الالكتروني (ECB). بعد ذلك يجري تشفير كل كتلة من النّص الصريح باستخدام مفتاح التّشفير، والكتلة المشفّرة السابقة، التي يمكن تخزينها، ثم إعادة تغذيتها إلى وحدة التّشفير من خلال خط تغذية عكسيّة، كما هو موضح في الشكل (٤-٨). وهنا تبرز مشكلة، وهي كيف يجري تشفير كتلة النّص الصريح الأولى، في ظل عدم وجود كتلة نص مشفرة سابقة لها، بما أنها هي الأولى، ولم يسبق أن تم تشفير أي كتلة قبلها؟ والحل هو استخدام كتلة استهلاليّة (أو ابتدائيّة) (Initialization Vector-IV) بالحجم نفسه ؛ لتحلّ محلّ الكتلة المشفّرة السابقة ولمرّة واحدة فقط عند تشفير كتلة النّص الصريح الأولى[١]. وكما هو موضّح في الشكل (٤-٨)

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 131.

يتـم التبديل بين خط التغذيـة العكسيّة، الذي يتم مـن خلاله تغذية عمليّـة التّشفير بالكتل المشفّرة السابقة، وبين الكتلة الاستهلالية باستخدام مفتاح تبديل(Switch) يسمح باستخدام الكتلة الاستهلالية عند تشفير كتلة النّص الصريح الأولى فقط، ثم يتحوّل إلى خط التغذية العكسيّة عند تشفير باقي الكتل، وتحديدًا يتم تشفير كتلة النّص الصريح الأولى باستخدام مفتاح التّشفـير والكتلة الاستهلالية(IV)، وتشفير كتلة النّصـ الصريح الثانية باستخدام مفتاح التّشفير والكتلة المشفّرة الأولى، وتشفير كتلة النّص الصريح الثالثة باستخدام مفتاح التّشفير والكتلة المشفّرة الثانية، ... وهكذ.



الشكل(٤-٨): أسلوب كتل التّشفير المترابطة(CBC) للتشفير الكتلي

ويتم فكّ تشفير الكتلة المشفّرة باستخدام مفتاح التّشفير، والكتلة المشفّرة السابقة، التي يمكن تخزينها، ثم تغذيتها إلى عمليّة فكّ التّشفير من خلال خط تغذية أمامية، كما يوضح ذلك الشكل(٤-٨). وتُستخـدم الكتلة الاستهلالية نفسها (IV) التـي سبق استخدامها في عمليّة التّشفير؛ لتحلّ محلّ الكتلـة المشفّرة السابقة ولمرة واحدة فقط عند فكّ تّشفير الكتلة المشفّرة الأولى، انظر الشكل(٤-٨). كما هو موضح في الشكل يتم التبديل بين خط التغذية الأمامية، الذي يتم من خلاله تغذية عمليّة فكّ التّشفير بالكتل المشفّرة السابقة، وبين الكتلة الاستهلالية باستخدام مفتـاح تبديل(Switch) يسمح باستخـدام الكتلة الاستهلالية عند فكّ تشفير الكتلة المشفّرة الأولى فقط، ثم يتحول إلى خط التغذية الأمامية عند فكّ تشفير باقي الكتل. وتحديدًا يتم فكّ تشفير الكتلة المشفّرة الأولى باستخدام مفتاح التّشفير والكتلة الاستهلالية(IV)، وفكّ تشفـير الكتلة المشفّـرة الثانية باستخدام مفتـاح التّشفير والكتلة

المشفّرة الأولى، وفكّ تشفير الكتلة المشفّرة الثالثة باستخدام مفتاح التشفير والكتلة المشفّرة الثانية، ... وهكذا.

وتجري عمليتا التّشفير وفك التّشفير بهذا الأسلوب وفق الآتي:

- **عمليّة التّشفير:**
  - أوّلًا: تشفير كتلة النّص الصريح الأولى: تُجمع كتلة النّص الصريح الأولى (x_1) مع الكتلة الاستهلاليـة (IV) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو الحصريّة" (XOR)، ثم يُدخل الناتج إلى خوارزميّة التّشفير ليتم تشفيره باستخدام مفتاح التّشفير (K)، وإنتاج كتلة النّص المشفّر الأولى (y_1) فلو افترضنـا أنّ الرمز (E_K) يرمـز لعملية التّشفـير باستخدام مفتاح التّشفير (K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_1 = E_K(x_1 \oplus IV)$$

  - ثانيًا: تشفير باقي كتل النّص الصريح: تُجمع كتلة النّص الصريح (x_i) مع الكتلة المشفّرة السابقة (y_{i-1}) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو الحصريّة" (XOR)، ثم يُدخل الناتج إلى خوارزميّة التّشفير ليتم تشفيره باستخدام مفتاح التّشفـير (K) وإنتاج كتلة النّص المشفّر (y_i). فلو افترضنا أنّ الرمز (E_K) يرمز لعمليّة التّشفير باستخدام مفتاح التّشفير (K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$i \geq 2 \text{ لكل } y_i = E_K(x_i \oplus y_{i-1})$$

- **عمليّة فكّ التّشفير:**
  - أوّلًا: فكّ تشفير الكتلة المشفّرة الأولى: تُدخـل الكتلة المشفّرة الأولى (y_1) إلى خوارزميّة فكّ التّشفير ليتم فكّ تشفيرها باستخدام مفتاح التّشفير (K)، ثم يُجمع الناتج مع الكتلة الاستهلاليـة (IV) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّـة المنطقيّـة: "أو الحصريّـة" (XOR)؛ لإنتاج كتلـة النّص الصريح

الأولى(x_1). فلو افترضنا أنّ الرمز (E_K^{-1}) يرمز لعمليّة فكّ التّشفير (العمليّة العكسيّة للتشفير) باستخدام مفتاح التّشفير (K)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_1 = E_K^{-1}(y_1) \oplus IV$$

- ثانيًا: فكّ تشفير باقي الكتل المشفّرة: تُدخل الكتلة المشفّرة(y_i) إلى خوارزميّة فكّ التّشفير ليتم فكّ تشفيرها باستخدام مفتاح التّشفير (K)، ثم يُجمع الناتج مع الكتلة المشفّرة السابقة(y_{i-1}) جمعًا قياسيًا للقياس ٢ باستخدام العمليّة المنطقية: "أو الحصرية" (XOR)؛ لإنتاج كتلة النّص الصريح (x_i). فلو افترضنا أن الرمز (E_K^{-1}) يرمز لعملية فكّ التّشفير (العمليّة العكسية للتشفير) باستخدام مفتاح التّشفير (K)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$i \geq 2 \text{ لكل } \quad x_i = E_K^{-1}(y_i) \oplus y_{i-1}$$

مما سبق، يتضح أن التّشفير الكتلي باستخدام أسلوب كتل التّشفير المترابطة (CBC) يتميز بالميزات الرئيسة الآتية:

- يمكن تجهيز الكتلة الاستهلالية (IV) بقيم ثنائيّة عشوائيّة مع كلّ عمليّة تشفير جديدة؛ لإضفاء مزيد من القوّة في هذا الأسلوب. فبهذه الطريقة يمكن الحصول على نصوص مشفّرة مختلفة للنّص الصريح نفسه و مفتاح التّشفير نفسه طالما تُستخدم كتلة استهلاليّة عشوائيّة مختلفة في كلّ مرّة، و من ثَمَّ فإنّ تشفير كتل متطابقة من نصوص صريحة لا ينتج عنه كتل مشفرة متطابقة (Non-deterministic)، و من ثَمَّ نحصل على نقاط القوة الآتية:
  - إذا راقب المهاجم مُخرجات وحدة التّشفير، وتحليل البيانات المارة (Traffic Analysis)، فستكون تلك البيانات عشوائية، و من ثَمَّ لا يمكنه معرفة الكتل المشفّرة المتشابهة، ولا ما إذا جرى إرسال الرسالة نفسها أو المعلومة مرّتين أو أكثر،

ولا معرفة بداية كل رسالة جديدة.

- يصلح هذا الأسلوب لتشفير الصور من نوع(Bitmap) بمفتاح تشفير ثابت، لأن المناطق المتشابهة في الصورة الأصلية لن ينتج عنها مناطق متشابهة في الصورة المشفّرة، بسبب عشوائية الكتلة الاستهلاليّة.
- تساعد هذه الخاصيّة في مجابهة هجوم التعويض(Substitution Attack)، حيث سيصعب على المهاجم معرفة الأجزاء التي تم استبدالها والاستفادة منها؛ لأنّها أصبحت عشوائية تختلف في كل عمليّة تشفير.

- بما أن تشفير كل كتلة من النّص الصريح يعتمد على نتيجة تشفير الكتلة التي تسبقها، من خلال خط التغذية العكسية، فيمكن أن نقول: أن الكتلة المشفّرة الأولى(y_1) تعتمد على كتلة النّص الصريح الاولى(x_1)، والكتلة الاستهلالية(IV)، وأن الكتلة المشفّرة الثانية (y_2) تعتمد على كتل النّص الصريح الاولى(x_1)، والثانية(x_2)، والكتلة الاستهلالية(IV)، وأن الكتلة المشفّرة الثالثة(y_3) تعتمد على كتل النّص الصريح الاولى(x_1)، والثانية(x_2)، والثالثة(x_3)، والكتلة الاستهلالية(IV)، ... وهكذا، وصولًا إلى الكتلة المشفّرة الأخيرة التي تعتمد على جميع كتل النّص الصريح السابقة والكتلة الاستهلالية، على شكل سلسلة مترابطة تعتمد كل حلقه منها على التي تسبقها؛ ومن هنا جاءت التسمية: أسلوب كتل التّشفير المترابطة(CBC). وتساعد هذه الخاصيّة على مجابهة هجوم تغيير تترتيب الكتل المشفّرة أو حذفها؛ لأنّ كلّ كتلة أصبحت تعتمد على سابقاتها، وستُكشَف أيّ عمليّة فقْد أو تبديل لأيّ كتلة.

وكأيّ نظام تشفير آخر توجد في أسلوب كتل التّشفير المترابطة(CBC) العيوب الآتية:

- يلزم اتباع ترتيب الكتل نفسه بين عمليتي التّشفير وفكّ التّشفير. فلا يمكن تشفير كتل النّص الصريح بترتيب معيّن(الأولى، ثم الثانية، ثم الثالثة، مثلًا)، وفك تشفيرها بترتيب مختلف(الثالثة، ثم الثانية، ثم الأولى، مثلًا). والسبب في ذلك أنّ تشفير أو فكّ تشفير أيّ كتلة مرتبط بوجود الكتلة المشفّرة السابقة

لها. وينتج عن ذلك أنّه لو فقـدت بعض الكتل بعد تشفيرها، وهي في طريقها من المرسل إلى المستقبل لأيّ سبب كان، و وصلت كتل أخرى، فإنّه لا يمكن إتمام عمليّة فكّ التّشفير للكتل التي وصلت؛ بسبب اعتماد ذلك على الكتل المفقودة.

- لا يمكن تشفير أكثر من كتلة في الوقت نفسه بالتوازي(Parallel) معًا؛ بسبب ارتباط تشفير أيّ كتلة بوجود الكتلة المشفّرة السابقة لها.
- يُعدُّ هذا الأسلوب أصعب في البنـاء والتطبيق من سابقه؛ لأنّه يستخدم الكتلة الاستهلاليّة، والتغذية العكسيّة في التّشفير، والتغذية الأماميّة في فكّ التّشفير، التي تتطلب مزيدًا من الإجراءات، والمعادلات الرياضيّة، والدوائر الإلكترونيّة.

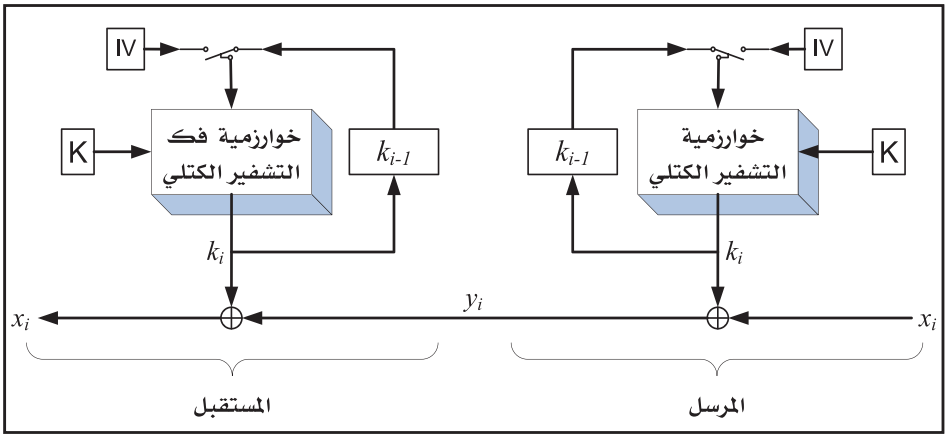
٣. أسلوب التغذية العكسيّة للمخرجات(Output Feedback Mod-OFB)

في هـذا الأسلـوب، يُجـزأ النّصـ الصريح إلـى كُتـل متساوية الحجـم، مـع تكملة(أو ملء(Padding) الكُتلـة الأخيرة، إذا كانت ناقصـة، تمامًا كما في أسلـوب كتاب الترميز الإلكـتروني(ECB). والفكـرة الجديدة في هـذا الأسلوب هـي الجمع بين التّشفـير الكُتلي والتسلسلي، حيث يستخدم التّشفير الكُتلي لإنتاج كُتل التّشفير، ويستخدم التّشفير التسلسلي لتشفير كُتـل النّص الصريح تسلسليًّا علـى مستوى الكُتلة باستخـدام العمليّة المنطقيّة "أو الحصريّة" (XOR)[١]. و تُنتج في هذا الأسلوب كُتل التّشفير بإعادة تشفير كُتل التّشفير السابقة، ومن هنا جاءت التسمية: التغذية العكسيّة للمخرجات، فمخرجات خوارزميّة التّشفير الكُتلي تعاد لها كمدخلات لإعادة تشفيرها مرّة أخرى وإنتاج كُتل التّشفير التالية.

تبدأ عمليّة التّشفير بتشفير الكُتلة الاستهلالية(IV) (تشفيرًا كُتليًّا) وإنتاج أول كُتلة من كُتل مفتاح التّشفير(كُتلة التّشفير)، التي ستستخدم لغرضين: الأول لتشفير كُتلة النّص الصريح الأولى تسلسليًا باستخدام العمليّة المنطقيّة "أو الحصريّة" (XOR)، والثاني لتخزينها وإعادة تغذيتها(Feedback) من خلال خط تغذية عكسيّة، لخوارزميّة التّشفير(الكُتلي) لتُشفَّر مرّة أخرى؛ لإنتاج كُتلة التّشفير التالية، كما يوضح ذلك الشكل(٤-٩). وبعد ذلك تستمر عمليّة

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 130.

التّشفير باستخدام كل كُتلة تشفير(k_i) لتشفير كُتلة النّص الصريح المقابلة لها(x_i)، باستخدام العمليّة المنطقيّة "أو الحصريّة" (XOR)، مع إعادة تغذيتها لخوارزميّة التّشفير الكُتلي لإنتاج كُتلة التّشفير الآتية(k_{i+1})، ... وهكذا. وتستخدم الكُتلة الاستهلاليّة في هذا الأسلوب لمرة واحدة فقط لإنتاج أول كُتلة تشفير، وبعد ذلك يتم التحول إلى خط التغذية العكسيّة من خلال مفتاح التبديل (Switch) الموضح في الشكل؛ لاستقبال كُتل التّشفير السابقة، وإعادة تشفيرها لانتاج كُتل التّشفير الآتية، وتحديدًا يتم تشفير كُتلة النّص الصريح الأولى باستخدام كُتلة التّشفير الأولى المنتجة من الكُتلة الاستهلالية (IV)، وتشفير كُتلة النّص الصريح الثانية باستخدام كُتلة التّشفير الثانية المنتجة من كُتلة التّشفير الأولى، وتشفير كُتلة النّص الصريح الثالثة باستخدام كُتلة التّشفير الثالثة المنتجة من كُتلة التّشفير الثانية، ... وهكذا.



الشكل (٤-٩): أسلوب التغذية العكسيّة للمخرجات (OFB) للتشفير الكُتلي

تبدأ عمليّة فكّ التّشفير بتشفير الكُتلة الاستهلاليّة (IV) (تشفيرًا كُتليًّا تمامًا كما تم في عمليّة التّشفير) وإنتاج أول كُتلة من كُتل فكّ التّشفير، التي ستستخدم لغرضين: الأوّل لفكّ تشفير الكُتلة المشفّرة الأولى باستخدام العمليّة المنطقيّة "أو الحصريّة" (XOR)، والثاني لتخزينها وإعادة تغذيتها (Feedback) من خلال خط تغذية عكسيّة، لخوارزميّة فكّ التّشفير (التي هي مطابقة لخوارزميّة التّشفير وليست عكسيّة لها) لتشفيرها مرّة أخرى، وإنتاج كُتلة فكّ التّشفير الآتية، كما يوضح ذلك الشكل (٤-٩). وبعد ذلك تستمر عمليّة فكّ

التّشفـير باستخدام كل كُتلة من كُتل فـكّ التّشفير (k_i) (وهي كُتل مطابقـة للكُتل المنتَجة في عمليّة التّشفير) لفكّ تشفير الكُتلة المشفّرة المقابلة لها (y_i)، باستخدام العمليّة المنطقيّة "أو الحصريّة" (XOR)، مع إعادة تغذيتها لخوارزميّة فكّ التّشفير لإنتاج كُتلة فكّ التّشفير الآتية (k_{i+1})، ... وهكذا. وتستخدم الكُتلة الاستهلاليّة بطريقة مشابهة لتلك التي في عمليّة التّشفير، وتحديدًا يجري فكّ تشفير الكُتلة المشفّرة الأولى باستخدام كُتلة فكّ التّشفير الأولى المنتجة من الكُتلة الاستهلالية (IV)، وفكّ تشفير الكُتلة المشفّرة الثانية باستخدام كُتلة فكّ التّشفير الثانية المنتجة من كُتلة فكّ التّشفير الأولى، وفكّ تشفير الكُتلة المشفّرة الثالثة باستخدام كُتلة فكّ التّشفير الثالثة المنتجة من كُتلة فكّ التّشفير الثانية، ... وهكذا.

وتتم عمليتا التّشفير وفك التّشفير بهذا الأسلوب وفق الآتي:

- **عمليّة التّشفير:**
  - أولًا: تشفـير كُتلة النّص الصريـح الأولى: تُشفَّـر الكُتلـة الاستهلاليّة (IV) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليـد كُتلة التّشفير الأولى (k_1)، التي يُجرى عليها الآتي:
    - تُجمع مع كُتلـة النّص الصريح الأولـى (x_1) جمعًا قياسيًّـا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو الحصريّة" (XOR)؛ لإنتاج الكُتلة المشفّرة الأولى (y_1).
    - تُخزّن ويعـاد تغذيتها، من خلال خـط التغذية العكسيّـة، لخوارزميّة التّشفير الكُتلي لتُشفَّر مرّة أخرى، لإنتاج كُتلة التّشفير الثانية.

    فلو افترضنا أن الرمز (E_K) يرمز لعملية التّشفير الكُتلي باستخدام مفتاح التّشفير (K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_1 = E_K(IV) \oplus x_1$$

  - ثانيًا: تشفير باقي كُتل النّصـ الصريح: تُشفَّر كُتلـة التّشفير السابقة (k_{i-1}) باستخـدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلـة التّشفير (k_i)، التي يُجرى

عليها التالي:

- تُجمع مع كُتلة النّص الصريح(x_i) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو الحصريّة" (XOR)؛ لإنتاج الكُتلة المشفّرة(y_i).
- تُخزّن ويعاد تغذيتها، من خلال خـط التغذية العكسيّة، لخوارزميّة التّشفير الكُتلي لتُشفَّر مرة أخرى، لإنتاج كُتلة التّشفير التالية(k_{i+1}).

فلو افترضنا أنّ الرمز(E_K) يرمز لعمليّة التّشفير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_i = E_K(k_{i-1}) \oplus x_i \quad \text{لكل} \quad i \geq 2$$

- **عمليّة فكّ التّشفير:**

- أولًا: فكّ تشفير الكُتلة المشفّرة الأولى: تشفّر الكُتلة الاستهلاليّة(IV) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلة فكّ التّشفير الأولى(k_1)، المطابقة لكلتة التّشفير الأولى، التي يُجرى عليها الآتي:
  - تُجمع مع الكُتلة المشفّرة الأولى(y_1) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّة المنطقية: "أو الحصرية" (XOR)؛ لإنتاج كُتلة النّص الصريح الأولى(x_1).
  - تُخزّن ويعاد تغذيتها، من خلال خـط التغذية العكسيّة، لخوارزميّة فكّ التّشفير(التي هي مطابقة لخوارزميّة التّشفير وليست عكسيّة لها) لتُشفَّر مرّة أخرى، لإنتاج كُتلة فكّ التّشفير الثانية.

  فلو افترضنا أنّ الرمز(E_K) يرمز لعملية فكّ التّشفير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_1 = E_K(IV) \oplus y_1$$

- ثانيًا: فـكّ تشفير باقي الكتل المشفّرة: تشفّر كُتلة فـكّ التّشفير السابقة(k_{i-1}) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلة فكّ التّشفير(k_i)، التي يُجرى

عليها التالي:

- تُجمع مع الكُتلة المشفّرة(y_i) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّة المنطقية: "أو الحصرية" (XOR)؛ لإنتاج كُتلة النّص الصريح(x_i).
- تُخزن ويعاد تغذيتها، من خلال خط التغذية العكسيّة، لخوارزميّة فكّ التّشفير ؛ لتُشفَّر مرّة أخرى، لإنتاج كُتلة فكّ التّشفير الآتية(k_{i+1}).

فلو افترضنا أن الرمز(E_K) يرمز لعملية فكّ التّشفير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_i = E_K(k_{i-1}) \oplus y_i \quad \text{لكل} \quad i \geq 2$$

مما سبق، يتضح أنّ التّشفير الكُتلي باستخدام أسلوب التغذية العكسيّة للمخرجات(OFB) يتميّز بالميزات الرئيسة التالية:

- يمكن أن يستخدم التّشفير الكُتلي باسلوب التغذية العكسيّة للمخرجات(OFB) لبناء نظام تشفير تسلسلي بجعل حجم الكُتلة يساوي "١". لاحظ أن التّشفير التسلسلي في هذا الأسلوب يمكن أن يتم على مستوى الكتل(Blockwise)، أي كُتلة كُتلة تسلسليًّا، أو على مستوى البت(Bitwise)، أي بتًّا بتًّا تسلسليًا.
- تتطابق عمليتا التّشفير وفكّ التّشفير في هذا الأسلوب، كما هي الحال في التّشفير التسلسلي. فخوارزميّة فكّ التّشفير في هذا الأسلوب ليست عكسيّة لخوارزميّة التّشفير وإنّما مطابقة لها تمامًا.
- لا تعتمد عمليّة توليد كُتل التّشفير على كُتل النّص الصريح، فهي منفصله عنها، ومن ثم يمكن حساب بعض كُتل التّشفير مسبقًا، وتخزينها؛ لاستخدامها لاحقًا.
- يمكن تجهيز الكُتلة الاستهلاليّة(IV) بقيم ثنائيّة عشوائيّة مع كل عمليّة تشفير جديدة؛ لإضفاء مزيدًا من القوّة في هذا الأسلوب. فبهذه الطريقة يمكن الحصول على نصوص مشفّرة مختلفة للنّص الصريح نفسه و لمفتاح التّشفير نفسه طالما تُستخدم كُتلة استهلاليّة عشوائيّة مختلفة في كل مرّة، ومن ثَـمَّ فإنّ تشفير كُتل متطابقة من

نصوص صريحة لا ينتج عنه كُتل مشفرة متطابقة(Non-deterministic)، و من ثَمَّ نحصل على نقاط القوة التالية:

- مقاومة هجمات تحليل البيانات المارّة(Traffic Analysis)، لأن البيانات المشفّرة ستكون عشوائيّة، و من ثَمَّ لا يمكن معرفة الكُتل المشفّرة المتشابهة، ولا ما إذا تم إرسال الرسالة نفسها أو المعلومة مرّتين أو أكثر، ولا معرفة بداية كلّ رسالة جديدة.
- يصلح هذا الأسلوب لتشفير الصور من نوع(Bitmap) بمفتاح تشفير ثابت، لأن المناطق المتشابهة في الصورة الأصليّة لن ينتج عنها مناطق متشابهة في الصورة المشفّرة، بسبب عشوائيّة الكُتلة الاستهلاليّة.
- تساعد هذه الخاصيّة في مجابهة هجوم التعويض(Substitution Attack)، حيث سيصعب على المهاجم معرفة الأجزاء التي تم استبدالها والاستفادة منها؛ لأنّها أصبحت عشوائيّة تختلف في كل عمليّة إرسال.

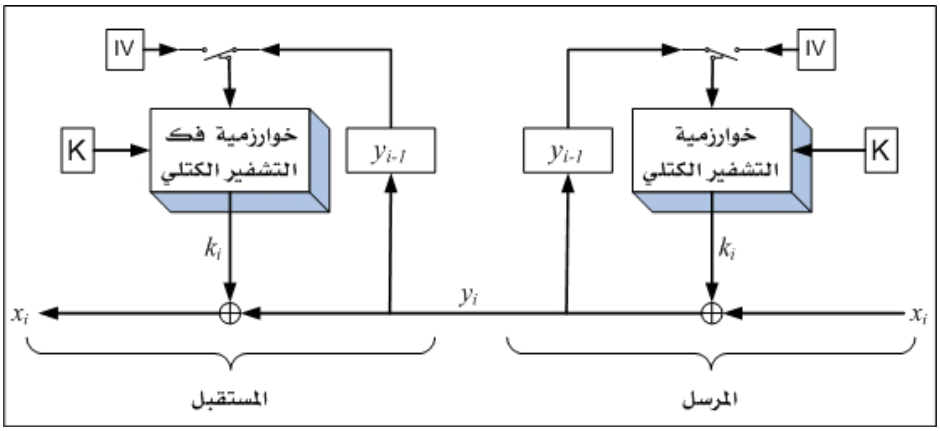
- يمكن تنفيذ عمليتي التّشفير وفكّ التّشفير بالتوازي(Parallel) معًا.

كأيّ نظام تشفير آخر توجد في أسلوب التغذية العكسيّة للمخرجات(OFB) العيوب التالية:

- يستخدم هذا الأسلوب كُتلة استهلالية، والتغذية العكسيّة في التّشفير وفي فكّ التّشفير، التي تتطلب مزيدًا من الإجراءات، والمعادلات الرياضيّة، والدوائر الإلكترونيّة.
- قد يكون هذا الأسلوب عرضة لهجوم تغيير ترتيب الكُتل المشفّرة.

٤. أسلوب التغذية العكسيّة للنصوص المشفّرة(Cipher Feedback Mod-CFB)

يعمل هذا الأسلوب بطريقة مشابهة جدًا لاسلوب التغذية العكسيّة للمخرجات(OFB)، مع كون التغذية العكسيّة للنصوص المشفّرة بدلًا من كونها لمخرجات خوارزميّة التّشفير الكُتلي، انظر الشكل(٤-١٠). ويتم استخدام التّشفير الكُتلي لإنتاج كُتل التّشفير، وليس لتشفير كُتل النّص الصريح، التي يتم تشفيرها تسلسليًا على مستوى الكُتلة باستخدام العمليّة المنطقيّة «أو الحصريّة»(XOR).



الشكل(٤-١٠): أسلوب التغذية العكسيّة للنصوص المشفّرة(CFB) للتشفير الكُتلي

لاحظ أنه يتم في هذا الأسلوب إنتاج كُتل التّشفير بإعـادة تشفير الكتل المشفّرة السابقة للنصوص الصريحة، ومن هنا جاءت التسمية: التغذية العكسيّة للنصوص المشفّرة، فالكُتل المشفّرة من النصوص الصريحة يعاد إدخالها إلى خوارزميّة التّشفير الكُتلي لاعادة تشفيرها مرة أخرى وانتاج كُتل التّشفير التالية.

وتتم عمليتا التّشفير وفك التّشفير بهذا الأسلوب وفق الآتي[١]:

- **عمليّة التّشفير:**
  - أولًا: تشفـير كُتلة النّص الصريـح الأولـى: تُشفَّر الكُتلـة الاستهلالية(IV) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلـة التّشفير الأولى(k_1)، التي تُجمع مع كُتلة النّص الصريح الأولى(x_1) جمعًا قياسيًا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو الحصريّة"(XOR)؛ لإنتاج الكُتلة المشفّرة الأولى(y_1)، التي تُخزن ويعاد تغذيتها، من خلال خط التغذية العكسيّة، لخوارزميّة التّشفير الكُتلي لتُشفَّر مرّة أخرى، لإنتاج كُتلة التّشفير الثانية.

فلـو افترضنـا أنّ الرمـز(E_K) يرمز لعمليـة التّشفـير الكُتلي باستخـدام مفتاح التّشفير(K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_1 = E_K(IV) \oplus x_1$$

١- Stallings, William (2007), "Network Security Essentials: App.lications and Standards", p 49-50.

- ثانيًا: تشفير باقي كُتل النّص الصريح: تُشفَّـر الكُتلة المشفّرة السابقة(y_{i-1}) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلة التّشفير(k_i)، التي تُجمع مع كُتلة النّص الصريح(x_i) جمعًا قياسيًّا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو الحصريّة" (XOR)؛ لإنتاج الكُتلة المشفّرة(y_i)، التي تُخزن ويعاد تغذيتها، من خلال خط التغذية العكسيّة، لخوارزميّة التّشفير الكُتلي لتُشفَّر مرّة أخرى، لإنتاج كُتلة التّشفير التالية(k_{i+1}).

فلو افترضنا أنّ الرمز(E_K) يرمز لعمليّة التّشفير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_i = E_K(y_{i-1}) \oplus x_i \quad \text{لكل} \quad i \geq 2$$

- **عمليّة فكّ التّشفير:**

- أولًا: فكّ تشفير الكُتلة المشفّرة الأولى: تشفر الكُتلة الاستهلالية(IV) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلة فكّ التّشفير الأولى(k_1)، المطابقة لكلتة التّشفير الأولى، التي تُجمع مع الكُتلة المشفّرة الأولى(y_1) جمعًا قياسيًا للقياس ٢ باستخدام العمليّة المنطقيّـة: "أو الحصريّة" (XOR)؛ لإنتاج كُتلة النّص الصريح الأولى(x_1). وتُخزن الكُتلة المشفّرة الأولى(y_1) ويعاد تغذيتها، من خلال خط التغذية الأماميّة، لخوارزميّة فكّ التّشفير(التي هي مطابقة لخوارزميّة التّشفير وليست عكسيّة لها) لتُشفَّر مرة أخرى، لإنتاج كُتلة فكّ التّشفير الثانية.

فلو افترضنا أنّ الرمـز(E_K) يرمز لعملية فكّ التّشفـير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_1 = E_K(IV) \oplus y_1$$

- ثانيًا: فكّ تشفـير باقي الكتل المشفّـرة: تشفر الكُتلة المشفّـرة السابقة(y_{i-1}) باستخدام خوارزميّة التّشفير الكُتلي؛ لتوليد كُتلة فكّ التّشفير(k_i)، التي تُجمع مع الكُتلة المشفّرة(y_i) جمعًا قياسيًا للقياس ٢ باستخدام العمليّة المنطقيّة: "أو

الحصريّة" (XOR)؛ لإنتاج كُتلة النّص الصريح(x_i). وتُخزّن الكُتلة المشفّرة السابقة(y_{i-1}) ويعاد تغذيتها، من خلال خط التغذية الأماميّة، لخوارزميّة فكّ التّشفير ؛ لتُشفَّر مرة أخرى، لإنتاج كُتلة فكّ التّشفير الآتية(k_{i+1}).

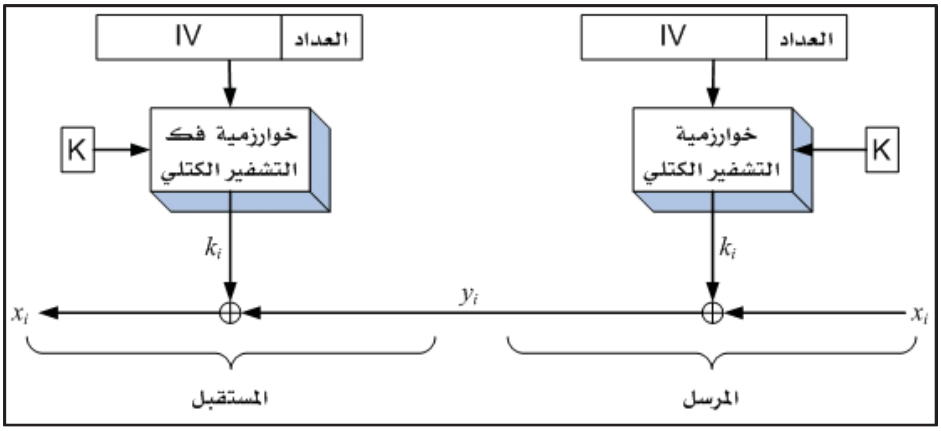
فلو افترضنا أن الرمز(E_K) يرمز لعملية فكّ التّشفير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_i = E_K(y_{i-1}) \oplus y_i \quad \text{لكل } i \geq 2$$

مما سبق، يتضح أنّ التّشفير الكُتلي باستخدام أسلوب التغذية العكسيّة للنصوص المشفّرة(CFB) يتمتع ميزات أسلوب التغذية العكسيّة للمخرجات (OFB) نفسه ويعاني من عيوبه نفسها.

٥. أسلوب العداد(Counter Mod-CTR)

يعمل هذا الأسلوب بطريقة مشابهة لأسلوبي التغذية العكسيّة للمخرجات(OFB)، والتغذية العكسيّة للنصوص المشفّرة(CFB)، من حيث كونه ينتج كُتل التّشفير بطريقة كتلية، ويشفر كُتل النّص الصريح تسلسليًّا، على مستوى الكُتلة(Blockwise). وبعبارة أخرى، يمكن في هذا الأسلوب استخدام التّشفير الكُتلي لبناء تشفير تسلسلي كما هي الحال في الأسلوبين السابقين؛ فتُنتج كُتل التّشفير كُتلة كُتلة باستخدام عداد(ومن هنا جاءت التسمية: أسلوب العداد)، ثم تطبق عمليّة "أو الحصريّة" (XOR) على كل كُتلة مع ما يقابلها من كُتل النّص الصريح؛ لإنتاج الكُتل المشفّرة. وكذلك الحال في عمليّة فكّ التّشفير، حيث يجري إنتاج كُتل فكّ تشفير مطابقة لكتل التّشفير باستخدام العداد نفسه ، ثم تطبق عمليّة "أو الحصريّة" (XOR) على كل كُتلة مع ما يقابلها من الكتل المشفّرة؛ لإنتاج كُتل النّص الصريح من جديد، انظر الشكل(٤-١١).



الشكل(٤-١١): أسلوب العداد(CTR) للتشفير الكُتلي

والسؤال المطروح هنا هو: كيف تُحدد القيمة الابتدائيّة للعدّاد؟ وهنا يجب الانتباه جيّدًا لمنع استخدام القيمة نفسها مرّتين؛ لأنه لو استطاع المهاجم معرفة النّص الصريح المقابل لإحدى هاتين القيمتين، فسيكون بمقدوره معرفة كُتلة مفتاح التّشفير المستخدمة في التّشفير، و من ثَمَّ فكّ تشفر كُتل نصوص صريحة أخرى. وللإجابة عن هذا السؤال، وحلّ هذه الاشكالية، يُقسَم العدّاد إلى جزئين: أحدهما كبير يستخدم ككُتلة استهلالية(IV)، والثاني صغير يستخدم كعدّاد، كما هو موضح في الشكل(٤-١١)[١]. فلو اعتبرنا أنّ حجم الكُتلة هو(١٢٨) بت، فيمكن أن يُقسَم العدّاد إلى كُتلة استهلالية بحجم(٩٦) بت، وإلى عدّاد بحجم(٣٢) بت. بعد ذلك تُجهّز الكُتلة الاستهلالية بقيمة عشوائيّة، ويصفّر العدّاد(أي يعطى القيمة: صفر) عند بداية كل عمليّة تشفير، ثم مع كل عمليّة تشفير كُتلي لإنتاج كُتلة تشفير واحدة،(K_i)، يزاد العدّاد ($CTR_i = CTR_i + 1$)، وتبقى الكُتلة الاستهلالية ثابتة، التي تبقى كذلك حتى استنفاذ جميع قيم العدّاد(٣٢٢ قيمة)، ثم تجهز بقيمة عشوائية ثانية تختلف عن سابقتها، ... وهكذا. وعند فكّ التّشفير يستخدم العدّاد نفسه ، و القيم العشوائية للكتلة الاستهلاليّة نفسها، حيث يمكن استخدام مولّد الارقام العشوائية نفسه لعمليتي التّشفير وفكّ التّشفير.

وتتم عمليتا التّشفير وفك التّشفير بهذا الأسلوب وفق الآتي:

- **عمليّة التّشفير:** تُجهّز الكُتلة الاستهلالية(IV) بقيمة عشوائية، ويصفّر العداد

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 133.

($CTR_i = 0$) عنـد بدايـة كل عمليّـة تشفـير، ثـم تستخدم هاتـان القيمتـان بعد لصقهما ببعضهما بعضًا حنبًا إلى جنب(Concatenation) لتصبح قيمة واحدة ($IV||CTR_i$) تُدخل إلى خوارزميّة التّشفير الكُتلي لإنتاج كُتلة التّشفير (K_i) باستخدام مفتاح التّشفير(K). ثم تُزاد قيمة العدّاد($CTR_i = CTR_i + 1$)، لاستخدامها في توليد كُتلة التّشفير الآتية(K_{i+1}). بعد ذلك تُستخدم كُتلة التّشفير(K_i) لتشفير كُتلة النّص الصريح(x_i) تسلسليًّا بتطبيق العمليّة المنطقيّة "أو الحصريّة"(XOR) على تلك الكتلتين، وإنتاج الكُتلة المشفّرة(y_i).

فلو افترضنا أنّ الرمز(E_K) يرمز لعملية التّشفير الكُتلي باستخدام مفتاح التّشفير(K)، فستتم عمليّة التّشفير وفق المعادلة الرياضيّة الآتية:

$$y_i = E_K(IV \| CTR_i) \oplus x_i \quad \text{لكل } i \geq 1$$

- **عمليّة فكّ التّشفير**: تجري بطريقة مطابقة لعمليّة التّشفير، ما عدا أن تحل الكُتلة المشفّرة(y_i) محلّ كُتلة النّص الصريح(x_i)، والعكس صحيح.

فلو افترضنا أنّ الرمز(E_K) يرمز لعملية فكّ التّشفير الكُتلي باستخدام مفتاح التّشفير(K) (لاحظ أنه رمز التّشفير نفسه وليس عكسيًّا له)، فستتم عمليّة فكّ التّشفير وفق المعادلة الرياضيّة الآتية:

$$x_i = E_K(IV \| CTR_i) \oplus y_i \quad \text{لكل } i \geq 1$$

مما سبق، يتضح أنّ التّشفير الكُتلي باستخدام أسلوب العداد(CTR) يتمتع بالميزات التالية:

- يمكن استخدام عدّاد عـادي يُزاد في كلّ مرّة بقيمة '١"، ويمكن استخدام عدّاد أكثر تعقيدًا يُزاد باستخدام معادلـة رياضيّة خاصّة به؛ من أجل زيادة قوة هذا الأسلوب التّشفيريّة.
- يمكن أن يعمل هذا الأسلوب بطريقة التوازي(Parallel)، حيث يمكن أن يكون لدينا أكثر من وحدة تشفير كُتلي تعمل في الوقت نفسه بالتوازي(الوحدة الأولى تستخدم العداد الأول(CTR_1)، والثانية تستخدم العداد الثاني(CTR_2)، ... وهكذا)، وهو ما يجعل هذا

الأسلوب مناسبًا للتطبيقات التي تحتاج إلى سرعات تشفير عالية.

- يمكـن أن يستخدم هـذا الأسلوب لبنـاء نظام تشفـير تسلسلي بجعل حجـم الكُتلة يساوي "١". لاحظ أن التّشفير التسلسلي في هذا الأسلوب يمكن أن يتم على مستوى الكتل (Blockwise)، أي كُتلة كُتلـة تسلسليًّا، أو على مستوى البت (Bitwise)، أي بتّا بتًّا تسلسليًّا.
- تتطابق عمليتا التّشفير وفك التّشفير في هذا الأسلـوب، كما هي الحال في التّشفير التسلسلي. فخوارزميّة فكّ التّشفير في هذا الأسلوب ليست عكسيّة لخوارزميّة التّشفير وإنّما مطابقة لها تمامًا.
- لا تعتمد عمليّة توليد كُتل التّشفير على كُتل النّص الصريح، فهي منفصلة عنها، ومن ثم يمكن حساب بعض كُتل التّشفير مسبقًا، وتخزينها؛ لاستخدامها لاحقًا.
- يمكن تجهيـز الكُتلة الاستهلاليّة (IV) بقيـم ثنائيّة عشوائيّة مـع كل عمليّة تشفير جديدة؛ لإضفاء مزيد من القوّة كما في الأساليب التي تستخدم الكتل الاستهلاليّة. فبهذه الطريقة يمكن الحصول على نصوص مشفّرة مختلفة للنّص الصريح نفسه و مفتاح التّشفير نفسه طالمـا تُستخدم كُتلة استهلالية عشوائيّة مختلفة في كل مرّة. و من ثَـمَّ فإنّ تشفير كُتـل متطابقة من نصوص صريحة لا ينتج عنـه كُتل مشفّرة متطابقة (Non-deterministic)، وستكون هناك مقاومة لهجمات تحليل البيانات المارّة (Traffic Analysis)، وهجمات التعويض (Substitution Attacks).

يوجد في أسلوب العدّاد (CTR) العيب التالي:

- يستخدم هذا الأسلوب العدّاد في عمليتي التّشفير وفكّ التّشفير، الذي يتطلب مزيدًا من الإجراءات، والمعادلات الرياضيّة، والدوائر الإلكترونيّة؛ لتشغيله والتحكّم فيه.

٤-٢-٢ التّشفير غير المتناظر (التّشفير باستخدام المفتاح العام)

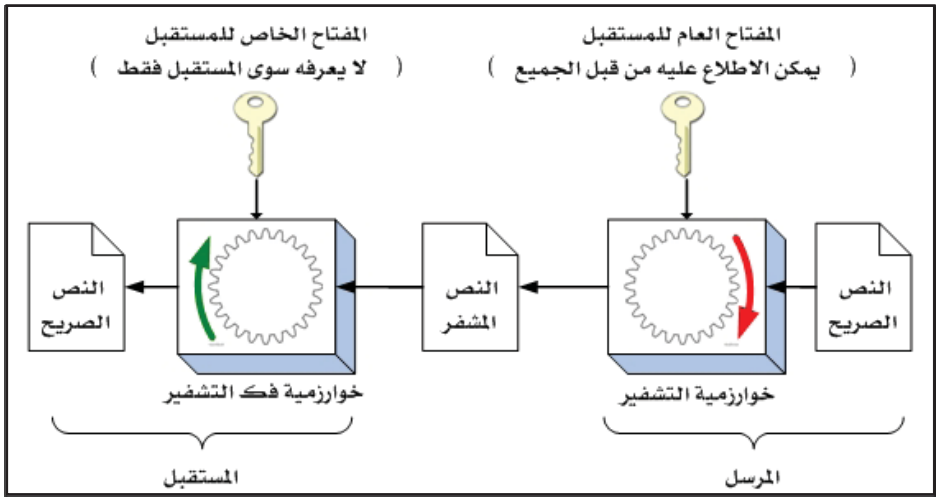
خلال عدّة سنوات من البحث العلمـي المستمر طُوِّر التّشفير المتناظر حتى تم إنتاج نظام التّشفير القياسي المتقدم (AES)، الـذي يُعدُّ آمنًا لنقل بيانات مشفرة بمفتاح بطول لا يقل

عن ٢٥٦ بتًّا. لكن المشكلة الأساسيّة التي توجد في نظام التّشفير المتناظر هي كيفية الحصول على المفتاح نفسه لكلٍّ من المرسل والمستقبل، أو ما يسمّى بمشكلة توزيع المفاتيح. ولحل هذه المشكلة جرى تطوير التّشفير باستخدام المفتاح العام.

قدَّم التّشفير باستخدام المفتاح العام طريقة جديدة تختلف تمامًا عن التّشفير المتناظر؛ فهو تشفير غير متناظر، أي لا يوجد مفتاح سرّي مشترك بين المرسل والمستقبل منذ البداية، وإنّما يُستخدَم مفتاحان منفصلان، يُستخدم أحدهما للتّشفير، والآخر (وهو مرتبط بالأول) لفك التّشفير.

في هذا النوع من التّشفير، يولّد كل مستخدم زوجًا من المفاتيح مرتبطين بعضهما ببعض (بطريقة رياضيّة معقّدة لا تسمح بكشف أيّ منهما إذا عُرف الآخر) أحدهما عام ويوضع في سجل (مجلّد) عام يمكن الاطّلاع عليه من قبل جميع المستخدمين، والآخر خاص ويُعدُّ مفتاحًا سريًّا خاصًّا بالمستخدم ويجب ألا يطّلع عليه الآخرون. ثم بعد ذلك تتم عمليتا التّشفير وفكّ التّشفير وفق الآتي: انظر الشكل (٤-١٢):

- عمليّة التّشفير: تُشفّر الرسالة الأصلية باستخدام خوارزميّة التّشفير والمفتاح العام للمستقبل للحصول على رسالة مشفرة. لاحظ أنّه يمكن للمرسل الحصول على المفتاح العام للمستقبل؛ لأنه علني (مشاع).



الشكل (٤-١٢): التّشفير بالمفتاح العام

- عمليّة فكّ التّشفير: يتم فكّ تشفير الرسالة المشفّرة باستخدام خوارزميّة فكّ التّشفير والمفتاح الخاص(السِّريّ) للمستقبل؛ للحصول على الرسالة الأصليّة، وبهذه الطريقة لن يستطيع أيّ شخص آخر فكّ تشفير الرسالة؛ لأنّه لا يملك المفتاح الخاص للمستقبل.

كما هو موضـح في الشكل(٤-١٢)، يتكوّن نظام التّشفير غـير المتناظر من ست مكوّنات رئيسة، هي:

١. النّص الصريح: وهو النّص أو الرسالة الأصليّة المقروءة التي يتم إدخالها إلى خوارزميّة التّشفير.

٢. خوارزميّة التّشفير: وهي الطريقة التي تشتمل على مجموعة الخطوات التي تُنفّذ على النّص الصريح لإنتاج النّص المشفّر باستخدام المفتاح العام للمستقبل، وتكون مدخلات خوارزميّة التّشفير هي النّص الصريح والمفتاح العام للمستقبل، ومخرجاتها هي النّص المشفّر، ومن أشهر خوارزميّات التّشفير بالمفتاح العام خوارزميّة آر إس أيه(RSA)، وخوارزميّة المنحنى البيضاوي(الإهليليجي) (Elliptic Curve).

٣. المفتاح العام(Public Key): وهو مفتاح عام(مشاع) بحيث يكون لكّل طرف مفتاح عام يستخدم لتشفير إي رساله ترسل إليه. ويمكن لأيّ شخص الاطّلاع على المفتاح العام واستخدامه في تشفير البيانات المرسلة إلى صاحب ذلك المفتاح العام، و يُفكّ تشفير الرسالة المشفّرة عن طريق المفتاح الخاص بالمستقبل (صاحب المفتاح العام الذي جرى التّشفير به).

٤. المفتاح الخاص(Private Key): وهو عبارة عن مفتاح خاص سرّي، بحيث يكون لكلّ طرف مفتاح خاص سرّي خاص به يتم استخدامه لفكّ تشفير الرسائل الواردة إليه، ويكون هذا المفتاح مرتبطًا بالمفتاح العام الخاص بالشخص نفسه.

٥. النّص المشفّر: وهو عبارة عن الرسالة التي تنتجها خوارزميّة التّشفير من كلّ من النّص الصريح والمفتاح العام للمرسل إليه.

٦. خوارزميّة فكّ التّشفير: وهي مجموعة الخطوات التي يتم تنفيذها على النّص المشفّر لإنتاج النّص الصريح، باستخدام المفتاح السِّريّ الخاص للمستقبل. وتكون

مدخلات خوارزميّة فكّ التّشفير هي النّص المشفّر والمفتاح السِّريّ للمستقبل، ومخرجاتها هي النّص الصريح.

يجب أن يملك جميع المشتركين في نظام التّشفير غير المتناظر حق الوصول إلى المفاتيح العامة واستخدامها في لتشفير، ويتم توليد المفاتيح الخاصة محليًّا لدى كل مستخدم (بشكل آلي) و من ثَمَّ فليس هناك حاجة لتوزيع المفاتيح كما هي الحال في التّشفير المتناظر، ويمكن لأيّ مستخدم تغيير مفتاحه الخاص في أيّ وقت شريطة إنتاج المفتاح العام الموافق له، ووضعه في السجّل المشترك (العام)، بحيث يطّلع عليه جميع المستخدمين، وللحصول على نظام تشفير آمن باستخدام المفتاح العام، فإنّه يجب تحقيق الشرطين الآتيين:

١. استخدام خوارزميّة قويّة، بحيث يكون من غير الممكن حسابيًّا تحديد المفتاح السِّريّ الخاص بالمرسل إليه بمجرد معرفة هذه الخوارزميّة والمفتاح العام (مفتاح التّشفير).

٢. يجب أن تبقى المفاتيح الخاصة سريّة، وأن تُنتَج بطريقة عشوائيّة وبطول لا يقل عن ٥١٢ بتًّا.

ولا يكاد يخلو بلد من نظام متكامل للتشفير غير المتناظر يسمّى البُنية التحتية للمفاتيح العامّة ((Public Key Infrastructure-PKI). يستخدم هذا النظام كعنصر رئيس بشكل منفرد أو بالتكامل مع بعض عناصر أمن المعلومات الأخرى؛ لتحقيق الأهداف الرئيسة الآتية للمشتركين فيه:

١. السِّريّة (أو الخصوصية): يمكِّن هذه النظام (نظام PKI) المستخدمين من تبادل المعلومات بشكل لا يمكّن الآخرين من قراءتها أو فهم طبيعتها.

٢. التحقّق من الهُويّة: يوفر ذلك إمكانية إثبات هويّة الشخص أو الجهة المستخدمة لهذا النظام بصفة قطعيّة.

٣. سلامة المعلومة وتكاملها: يوفر إمكانية اكتشاف أيّ تغيير أو حذف أو إضافة للمعلومة المتبادلة، أو لجزء منها.

٤. إجراء عمليّة التصديق الرقمي (أو التوقيع الإلكتروني): يوفر إمكانية توقيع الوثائق إلكترونيًّا، وكذلك إمكانيّة التثبّت من مصداقيّة (صحة) التوقيع الإلكتروني لدى استقبال الرسالة التي سبق توقيعها الكترونيًّا.

فيما يلي نتعرف إلى أشهر نظامين للتشفير غير المتناظر (أو التّشفير بالمفتاح العام)، و هما: نظام آر إس أيه (RSA)، ونظام المنحنى البيضاوي (Elliptic Curve Cryptosystem (Ecc).

٤-٢-٢-١ نظام تشفير رايفست وشاميروادليمان – آر إس أيه (RSA)

هو نظام تشفير غير متناظر تم ابتكاره من قبل ثلاثة علماء هم: رايفست وشامير وادليمان، وعرف بنظام آر إس أيه (Rivest-Shamir-Adleman-RSA) اختصارًا لاسماء هؤلاء العلماء. وقد انتشر هذا النظام انتشارًا كبيرًا لدرجة أنه يندر أن يتكلم أحد عن نظام التّشفير غير المتناظر ولا يتكلم عنه.

إنّ نظام آر إس أيه ليس بديلًا عن أنظمة التّشفير المتناظر، وإنما جاء كحلّ جذري لمشكلة توزيع المفاتيح في تلك الأنظمة. عمومًا يُستخدم نظام آر إس أيه في كثير من التطبيقات، إلا أن أشهرها تطبيقان اثنان هما:

- تشفير المعلومات صغيرة الحجم. ونقول هنا صغيرة الحجم لأن هذا النظام يعتمد على إجراء علميات حسابية تحتاج إلى وقت طويل مقارنة بأنظمة التّشفير المتناظر. لذلك يُعدُّ نظام آر إس أيه مناسبًا لتشفير مفاتيح أنظمة التّشفير المتناظر، لضمان تبادلها بشكل آمن، ثم بعد ذلك يُستخدم التّشفير المتناظر لتشفير البيانات والرسائل نفسها التي عادة ما تكون كبيرة الحجم.
- التصديق (أو التوقيع) الرقمي، كما سيأتي معنا.

ويكون لكل مستخدم لنظام آر إس أيه زوج من المفاتيح، هما:

- مفتاح عام يستخدم لعملية التّشفير، ويتكوّن من رقمين هما: (n،e)، حيث إن الرقم (n) هو القياس (Modulus) الذي ستعتمد عليه جميع العمليّات الحسابية في عمليتي التّشفير وفكّ التّشفير، والرقم (e) يتم اختياره من مدى محدّد من الأرقام [1 .. z-1]. لاحظ أنّ هذا المفتاح مشاع، ويمكن استخدامه من قِبل أيّ أحد يرغب في تشفير أيّ معلومة (صغيرة)، وبعثها لصاحب ذلك المفتاح العام، حيث لا يستطيع فكّ تشفيرها إلا هو باستخدام مفتاحه الخاص. ويتم إنتاج المفتاح العام

وفق الخطوات الآتية:

- اختيار رقمين أوليين كبيرين: p ، q
- حساب القياس (n): $n = p \times q$
- حساب الرقم (z) لتكوين المدي الذي سيتم اختيار الرقم (e) منه:

$$z = (p-1) \times (q-1)$$

- اختيار الرقم (e) بحيث يكون في المدي: [1 .. z-1]، ويكون القاسم المشترك الأعلى له وللرقم (z) هو الواحد.
- يكون المفتاح العام هو: (n ، e)
- مفتاح خاص (d) يستخدم لعملية فكّ التّشفير ويبقى سريًّا لدى المستخدم، ويحسب بالطرقة الآتية: $d = e^{-1} \bmod z$

أو بعبارة أخرى : $d \times e = 1 \bmod z$، أي أنّه المعكوس الضربي للرقم (e) للقياس (z).

وتتم عمليتا التّشفير وفك التّشفير في هذا النظام وفق الآتي[1]:

- عمليّة التّشفير: لتشفير نص صريح، يرمز له بالرمز (x)، وانتاج نص مشفَّر، يرمز له بالرمز (y)، يستخدم المفتاح العام (n،e)، وتطبق المعادلة الرياضيّة الآتية:

$$y = x^e \bmod n$$

- عمليّة فكّ التّشفير: لفك تشفير النّص المشفّر (y)، يستخدم المفتاح الخاص (d)، وتطبّق المعادلة الرياضيّة الآتية:

$$x = y^d \bmod n$$

مثال (٤-٧): حسب مستخدم لنظام آر إس أيه زوج المفاتيح الآتية:

- المفتاح العام (n،e)، وفق الخطوات الآتية:

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 174-175.

- اختيار رقمين أوليين: $p = 11 , q = 3$
- حساب القياس $n = 11 \times 3 = 33$
- حساب الرقم (z) لتكوين المدى الذي سيجري اختيار الرقم (e) منه:

$$z = (11-1) \times (3-1) = (10) \times (2) = 20$$

- اختيار الرقم (e)، بحيث يكون في المدي [19 .. 1]، ويكون القاسم المشترك الأعلى له وللرقم (٢٠) هو الواحد: $e = 3$
- يكون المفتاح العام هو: (n=33 , e=3) ، ويكون مشاعًا
- المفتاح الخاص (d) يستخدم لعملية فكّ التّشفير، ويبقى سريًّا لدى المستخدم، ويحسب بالطرقة الآتية:

$$d = 3^{-1} \bmod 20 = 7$$

لاحظ أن: $d \times e = 7 \times 3 = 21 \bmod 20 = 1 \bmod 20$

ولو افترضنا أن هناك رسالة ($x = 2$)، يرغب أحد في تشفيرها باستخدام المفتاح العام (n=33 , e=3)، فسيتم تشفيرها وفق الآتي:

$$y = x^e \bmod n = 2^3 \bmod 33 = 8 \bmod 33 = 8$$

وبذلك تكون الرسالة المشفّرة ($y = 8$).

ويُفك تشفيرالرسالة المشفّرة ($y = 8$) باستخدام الفتاح الخاص ($d = 7$) وفق الآتي:

$$x = y^d \bmod n = 8^7 \bmod 33 = 2097152 \bmod 33 = 2$$

وهي الرسالة الأصلية التي جرى تشفيرها باستخدام المفتاح العام. ◊

يتضح من المثال السابق كيف أن نظام آر إس أيه يتطلب إجراء عمليّات حسابيّة طويلة، فرأينا كيف أنّ فكّ تشفير رسالة صغيرة مكوّنة من رقم واحد فقط هو (٨) نتج عنه رقم كبير هو (٢٠٩٧١٥٢)، الذي احتاج إلى قسمته على القياس (٣٣) ثم أخذ المتبقي من ناتج القسمة وهو العدد (٢)، و هي كذلك عمليّة طويلة أيضًا. هذا في الحالات البسيطة، فما بالك لو كان الرقم عبارة عن رقم بطاقة أئتمانية مكون من (١٦) خانة أو كان ملفًا نصيًّا؟ وهذا يؤكد مناسبة نظام آر إس أيه لتشفير وتبادل مفاتيح تشفير أنظمة التّشفير المتناظر (كنظام

AES)، مع ترك عمليّة التّشفير نفسها لتلك الأنظمة التي تُعدُّ أسرع بكثير من نظام آر إس أيه. ولكي يكون نظام آر إس أيه آمنًا؛ فيجب اختيار الأرقام الأوليّة(p) و(q) لتكون كبيرة، بحيث يكون طول كل منهما(٥١٢) بت، وهو ما يجعل العمليّات الحسابيّة السابقة أصعب وأطول بكثير من الحالات البسيطة كما في المثال السابق.

كما ذكرنا سابقًا فإنّ كل مستخدم لنظام آر إس أيه يلزمه أن يكون لديه مفتاح عام مشاع للجميع يستطيع أيّ أحد أن يشفّر أيّ رسالة باستخدامه، ومفتاح خاص سرّيّ يستخدمه هو فقط لفكّ تشفير الرسائل الواردة إليه المشفّرة باستخدام مفتاحه العام. ومعنى ذلك أن من يتشفّر رسالة باستخدام المفتاح العام لمستخدم ما، فإنّه لا يستطيع فكّ تشفيرها هو، على الرغم من أنه هو الذي شفّرها؛ لأنه لا يمكن فكّ تشفيرها إلا باستخدام الزوج الآخر وهو المفتاح السِّريّ، الذي يوجد فقط لدى صاحب المفتاح العام. فلو كان لدينا مستخدمَين: عمر، وزيد، فيجب أن يكون لدى كلٍّ منهما مفتاح عام وآخر خاص، فإذا أراد عمر أن يرسل رسالة مشفرة لزيد؛ فسيقوم بتشفيرها باستخدام المفتاح العام لزيد(وليس مفتاحه العام هو)، ويستطيع زيد فقط أن يفك تشفيرها باستخدام مفتاحه السِّريّ، بينما لا يستطيع عمر أن يفكّ تشفيرها؛ لأنه لا يعرف المفتاح الخاص لزيد، على الرغم من أنّه الذي شفّرها.

٤-٢-٢-٢ نظام التّشفير بالمنحنى البيضاوي(الإهليلجي)(ECC)

كما رأينا في نظام آر إس أيه، فإنّ المشكلة التي يواجهها هي حاجته إلى عمليّات حسابيّة طويلة تحتاج إلى وقت طويل لتنفيذها، ويزداد هذا الوقت بازدياد حجم الأعداد الأولية(p) و(q)، وبازدياد حجم الرسالة المراد تشفيرها. لذلك ظهرت الحاجة إلى نظام تشفير غير متناظر، يعمل بفكرة المفتاح العام، ويمكن تنفيذ عمليتي التّشفير وفك التّشفير فيه في وقت أقل من نظام آر إس أيه، ويكون آمنًا بالدرجة نفسها أو أعلى.

ابتكر العالمان ميلار[١] وكوبلتز[٢] نظام التّشفير بالمنحنى البيضاوي (Elliptic Curve Cryptosystem-(ECC) في أواسط الثمانينيّات من القرن الميلادي

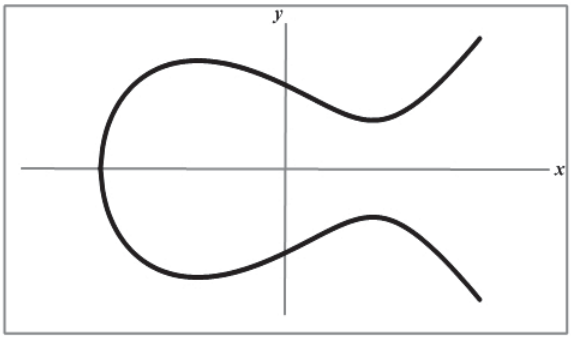
١- V. S. Miller(1986), "Use of elliptic curves in cryptography", Advances in Cryptology Proceedings of Crypto'85, Lecture Notes in Computer Science, 218(1986), Springer-Verlag, 417–426

٢- Koblitz Neal(1987), "Elliptic curve cryptosystems", Mathematics of Computation, 48(1987), 203–209

الماضي بشكل مستقلّ كل منهما عن الآخر، والمنحنى البيضاوي منحنى ذو خصائص معيّنة تجعله مناسبًا ليُبنى عليه نظام تشفير، ومعادلته الرياضيّة المستخدمة هي:

$$y^2 = x^3 + ax + b$$

حيث إنّ المعاملين(a) و(b) أعداد صحيحة تحقق الشرط الآتي: $4.a^3 + 27.b^2 \neq 0$، يمكن بتغيير قيمهما الحصول على عدد لا نهائي من المنحنيات البيضاوية، انظر الشكل(٤-١٣)، الذي يوضح منحنى بيضاويًّا بالمعاملين ($a = -3$)،($b = 3$).



الشكل(٤-١٣): المنحنى البيضاوي ذو المعادلة: $y^2 = x^3 - 3x + 3$

يعتمد نظام التّشفير بالمنحنى البيضاوي على تعريف عمليّة الجمع، "+"، لنقطتين من نقاط المنحنى وانتـاج نقطة ثالثة، من خلال إجراء بعض العمليّـات الحسابيّة على إحداثيّات تلك النقاط، كما سيأتي معنا. وقد تُجرى عمليّة الجمع على نقطتين مختلفتين عن بعضهما؛ فينتج لدينا جمع نقطتين، وقد تُجرى على النقطة نفسها ، بمعنـى أن يتم جمع النقطة مع نفسها؛ فينتج لدينا ما يعرف بمضاعفة النقطة. لذلك هناك عمليتان أساسيتان على نقاط المنحنى البيضاوي هما: جمع نقطتين، ومضاعفة نقطة، وتعريفهما كما يلي[١]:

- جمع نقطتين(P1 + P2 = P3): يتم جمع النقطة الأولى($P1 = (x_1, y_1)$) مع النقطة الثانية(($P2 = (x_2, y_2)$)؛ للحصول على النقطة الثالثة(($P3 = (x_3, y_3)$)، أي(($(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$)، بتنفيذ الخطوات التالية، انظر الجزء(أ) من الشكل(٤-١٤):

١- Hankerson D., et. al.,(2004), "A Guide to Elliptic Curve Cryptography".

- الوصل بين النقطتين(P1) و(P2) بخط مستقيم.
- سوف يقطع الخط المستقيم المنحنى عند نقطة ثالثة هي النقطة(R).
- يكون ناتج الإضافة هو النقطة(P3) النظيرة للنقطة(R) حول المحور السيني.

ويعبّر عن هذه العمليّة رياضيًا كما يلي:

$$x_3 = m^2 - x_1 - x_2 \mod p$$

$$y_3 = m\ (x_1 - x_3) - y_1 \mod p$$

حيث أن: $m = \frac{y_2 - y_1}{x_2 - x_1}$، وأن$(p)$ عدد أولي.

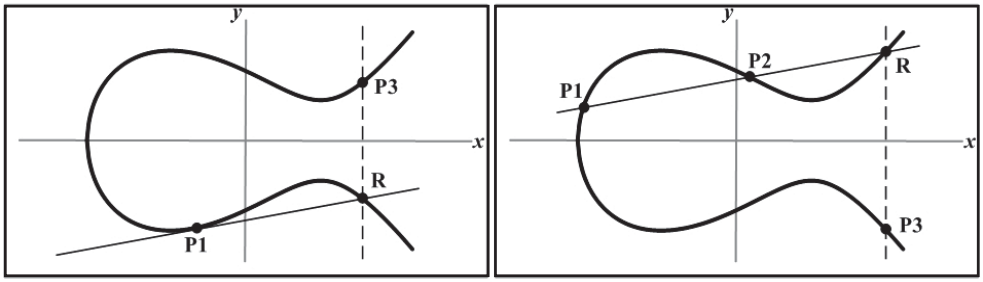
- مضاعفة نقطة(P1 + P1 = 2P1 = P3): يتم جمع النقطة($P1 = (x_1, y_1)$) مع نفسها؛ للحصول على النقطة($P3 = (x_3, y_3)$)، أي $(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ ، بتنفيذ الخطوات التالية، انظر الجزء(ب) من الشكل(٤-١٤):
  - رسم مماس للمنحنى يمرّ بالنقطة(P1).
  - سوف يقطع المماس المنحنى عند نقطة ثانية هي النقطة(R).
  - نـاتج المضاعفة هي النقطـة(P3) النظيرة للنقطـة(R) حول المحور السيني.

ويعبّر عن هذه العمليّة رياضيًّا كما يلي:

$$x_3 = m^2 - x_1 - x_1 \mod p$$

$$y_3 = m\ (x_1 - x_3) - y_1 \mod p$$

حيث إن: $m = \frac{3x_1^2 + a}{2y_1}$ ، وأن(p) عدد أولي.

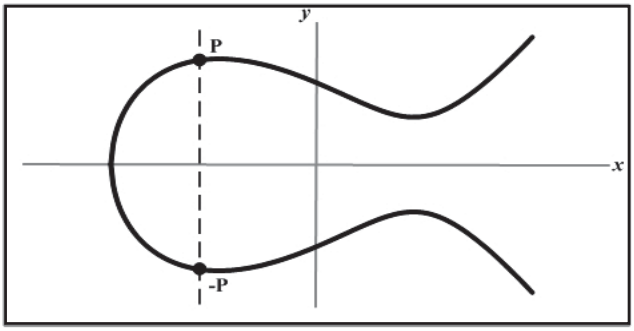


الشكل(٤-١٤): عمليّات جمع نقطتين، ومضاعفة نقطة على المنحنى البيضاوي

لكي تكتمل شروط تطبيق نظام التّشفير بالمنحنى البيضاوي، والحصول على مجموعه منتهية من النقاط، فلا بدّ من إيجاد عنصر(نقطة) الوحدة(O) الذي يحقق الشرط الآتي:($P + O = P$). وهذا العنصر يسمّى النقطة في اللانهاية(Point at Infinity)، الذي يمكن أن يستخدم لإيجاد معكوس النقطة(P) من خلال المعادلة:

$$P + (-P) = O$$

والسؤال المطروح هنا هو: كيف يمكن حساب المعكوس الجمعي للنقطة $P = (x_p, y_p)$؟ والجواب ببساطة هو: عكس إشارة الإحداث الصادي للنقطة(P)، لنحصل على: $(P = (x_p, - y_p)$ -)، أو بعبارة أخرى: معكوس النقطة (P) هو النقطة النظيرة لها حول محور السينات، انظر الشكل(٤-١٥)، وهي إحدى الخصائص المهمّة والسهلة المميّزة لنظام تشفير المنحنى البيضاوي.



الشكل(٤-١٥): معكوس نقطة على المنحنى البيضاوي

إنّ العمليّة الأساسيّة في نظام التّشفير بالمنحنى البيضاوي هي عمليّة ضرب نقطة من نقاط المنحنى بعدد سري صحيح يرمز له بالرمز(K)، التي تسمّى عمليّة الضرب التراكمي(Scalar Multiplication). فلو كان لدينا نقطة أساسيّة على المنحنى هي

$(P = (x_B, y_B))$، فإنّ الضرب التراكمي لهذه النقطة $(KP = K(x_B, y_B))$ هو عبارة عن جمع هذه النقطة مع نفسها عدد (K) مرة:

$$KP = \underbrace{P + P + P + \ldots + P}_{K \text{ مرة}}$$

عادة ما تتم هذه العمليّة عن طريق سلسلة من عمليّات مضاعفة النقطة الأساس، ثم جمع ناتج المضاعفة مع النقطة (P)، حتى يتم الحصول على النتيجة النهائية. فمثلًا، تنفّذ عمليّة ضرب النقطة (P) بالعدد الصحيح (3)؛ للحصول على (3P)، بحساب: (2P + P)، أي مضاعفة النقطة (P)؛ للحصول على (2P)، ثم جمع ناتج المضاعفة مع النقطة (P)؛ للحصول على (3P). ويمكن تنفيذ عمليّة ضرب النقطة (P) بالعدد الصحيح (9)؛ للحصول على (9P)، بحساب: (2(2(2P)) + P)، أي مضاعفة النقطة (P) للحصول على (2P)، ثم مضاعفة ناتج (2P) للحصول على (4P)، ثم مضاعفة ناتج (4P) للحصول على (8P)، ثم جمع ناتج (8P) مع النقطة (P)؛ للحصول على (9P).

مثال (٤-٨): يوضح هذا المثال عمليّة الضرب التراكمي، وكيف يُنفّذ من خلال سلسلة من عمليّات المضاعفة والجمع على نقاط المنحنى ذي المعادلة: $y^2 = x^3 + 2x + 2 \bmod 17$. فلو اعتبرنا أنّ النقطة الأساس (P) هي النقطة ذات الاحداثيات (5،1)، أي أن $(x_1 = 5, y_1 = 1)$، فيمكن إجراء عمليتي مضاعفة هذه النقطة، ثم جمع الناتج مع النقطة الأساس مرّة أخرى كما يلي:

- مضاعفة النقطة (5,1): $2P = (x_3, y_3) = (x_1, y_1) + (x_1, y_1) = (5,1) + (5,1)$

يمكن الحصول على النقطة (x_3, y_3)، بتطبيق المعادلات الرياضيّة لعمليّة مضاعفة النقطة كما يلي:

■ نبدأ أوّلًا بحساب m:

$$m = \frac{3x_1^2 + a}{2y_1} = (3 \times 5^2 + 2) \times (2 \times 1)^{-1} = (9) \times (9) = 81 = 13 \bmod 17$$

■ ثم نحسب إحداثيات النقطة $2P = (x_3, y_3)$:

$$x_3 = m^2 - x_1 - x_1 = 13^2 - 5 - 5 = 159 = 6 \bmod 17$$

$$y_3 = m\ (x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 = 3 \bmod 17$$

لتكون النتيجة النهائيّة:

$$2P = (x_3, y_3) = (x_1, y_1) + (x_1, y_1) = (5,1) + (5,1) = (6,3)$$

- جمع ناتج مضاعفة النقطة السابق، وهو$(6,3)$، مع النقطة الأساس$(5,1)$؛ للحصول على$(3P)$: $3P = (x_3, y_3) = (x_1, y_1) + (x_2, y_2) = (5,1) + (6,3)$: يمكن الحصول على النقطة (x_3, y_3) ، بتطبيق المعادلات الرياضيّة لعمليّة جمع نقطتين كما يلي:

■ نبدأ أولًا بحساب m:

$$m = \frac{y_2 - y_1}{x_2 - x_1} = (3 - 1) \times (6 - 5)^{-1} = (2) \times (1)^{-1} = (2) \times (1) = 2 \bmod 17$$

■ ثم نحسب إحداثيات النقطة $3P = (x_3, y_3)$:

$$x_3 = m^2 - x_1 - x_2 = 2^2 - 6 - 5 = -7 = 10 \bmod 17$$

$$y_3 = m\ (x_1 - x_3) - y_1 = 2(5 - 10) - 1 = -11 = 6 \bmod 17$$

لتكون النتيجة النهائية:

$$3P = (x_3, y_3) = (x_1, y_1) + (x_1, y_1) = (5,1) + (6,3) = (10,6)$$

بعد ذلك يمكن جمع ناتج$(3P)$، وهي النقطة$(10،6)$، مع النقطة الأساس$(5،1)$؛ للحصول$(4P)$،(التي يمكن الحصول عليها أيضًا بمضاعفة النقطة$(2P)$، .. وهكذا يمكن الحصول على النقاط التالية:

P =(5,1)	4P =(3,1)	7P =(0,6)	10P =(7,11)	13P =(16,4)	16P =(10,11)
2P =(3,6)	5P =(9,16)	8P =(13,7)	11P =(13,10)	14P =(9,1)	17P =(6,14)
3P =(10,6)	6P =(16,13)	9P =(7,6)	12P =(0,11)	15P =(3,16)	18P =(5,16)

ويمكن أن يستخدم نظام التّشفير بالمنحنى البيضاوي لتبادل المفاتيح بالطريقة الآتية، والمعروفة بطريقة دافي – هيلمان لتبادل المفاتيح نسبة إلى العالمين دافي وهيلمان اللذين ابتكرا أساس هذه الطريقة[1]. فيجب أوّلًا أن يتفق جميع مستخدمي هذا النظام على منحنى

١- هي طريقة لتوزيع المفاتيح بين المستخدمين تم اكتشافها قبل اكتشاف نظام التشفير بالمنحنى البيضاوي، انظر المرجع((Whitfield Diffie and Martin Hellman(1976)، وهي أصلًا تطبق على الأرقام الصحيحة، وتحديدًا رفع العدد(a) للقوة(a) ثم حساب الناتج للقياس بالعدد الأولي(P)، ويمكن تطبيقها علي نظام التشفير بالمنحنى البيضاوي بسهولة.

بيضاوي واحد، باستخدام المعاملين نفسيهما (a) و(b)، وعلى نقطة واحدة عليه تسمّى النقطة الأساس($P = (x_B, y_B)$). بعد ذلك يكون لدى كل مستخدم زوج من المفاتيح، هما:

- مفتاح خاص عبارة عن عدد صحيح(d) يستخدم لعملية فكّ التّشفير ويبقى سريًا لدى المستخدم.
- مفتاح عام يستخدم لعملية التّشفير، وهو نقطة على المنحنى ناتجة من حاصل ضرب النقطة الأساس($P = (x_B, y_B)$) بالمفتاح السِّريّ (d)؛ للحصول على: $dP = (x_d, y_d)$. لاحظ أنّ نتيجة هذا الضرب هي نقطة على المنحنى المتّفق عليه، وهي مشاعة، ويمكن استخدامها من قبل أيّ أحد يرغب في إنشاء مفتاح تشفير وتبادله بينه وبين المستخدم صاحب هذا المفتاح العام.

تتم عمليّة تبادل مفتاح تشفير سرّي مشترك(K) بين مستخدمين: مستخدم رقم(١)، ومستخدم رقم (٢)، وفقًا لطريقة دافي – هيلمان، كما يلي:

- **المستخدم رقم (١):**
  - يختار مفتاحًا خاصًّا سريًّا عبارة عن عدد صحيح (d1).
  - يحسب مفتاحه العام بضرب النقطة الأساس($P = (x_B, y_B)$) بمفتاحه السِّريّ (d1)؛ للحصول على: $d1.P = (x_{d1}, y_{d1})$
  - يحسب مفتاح التّشفير السِّريّ المشترك(K) بضرب المفتاح العام للمستخدم رقم(2)، وهو($d2.P = (x_{d2}, y_{d2})$)، بمفتاحه السِّريّ(d1)؛ للحصول على: $K = d1(d2.P) = (x_{d1d2}, y_{d1d2})$ ، أي الحصول على الإحداثيات: (x_{d1d2}, y_{d1d2}).

  لاحظ أن المفتاح العام للمستخدم رقم(٢) مشاع وهو عبارة عن نقطة على المنحنى، ويمكن الحصول عليه بسهوله أو إرساله من قبل المستخدم رقم(٢) نفسه.

- **المستخدم رقم(٢):**

■ يختار مفتاحًا خاصًّا سريًّا عبارة عن عدد صحيح(d2).

■ يحسب مفتاحه العام بضرب النقطة الأساس($P = (x_B, y_B)$) بمفتاحه السِّريّ(d2)؛ للحصول على: $d2.P = (x_{d2}, y_{d2})$

■ يحسب مفتاح التّشفير السِّريّ المشترك(K) بضرب المفتاح العام للمستخدم رقم(١)، وهو($d1.P = (x_{d1}, y_{d1})$)، بمفتاحه السِّريّ(d2)؛ للحصول على:

$K = d2(d1.P) = (x_{d2d1}, y_{d2d1}) = d1(d2.P) = (x_{d1d2}, y_{d1d2})$ ،

أي الحصول على الإحداثيات: (x_{d1d2}, y_{d1d2}) ، وهي الإحداثيات نفسها التي حصل عليها المستخدم رقم(١).

لاحظ أنّ المفتاح العام للمستخدم رقم(١) مشاع، وهو عبارة عن نقطة على المنحنى، ويمكن الحصول عليه بسهوله أو إرساله من قبل المستخدم رقم(١) نفسه.

مثال(٤-٩): بالاستناد إلى المثال السابق، يمكن تبادل مفتاح تشفير سرّيّ مشترك(K) بين مستخدمين: مستخدم رقم(١)، ومستخدم رقم(٢)، باستخدام نظام التّشفير بالمنحنى البيضاوي، و وفقًا لطريقة دافي – هيلمان، كما يلي:

- **المستخدم رقم(١):**
  - ■ يختار مفتاحًا خاصًّا سريًّا عبارة عن عدد صحيح(d1=3).
  - ■ يحسب مفتاحه العام بضرب النقطة الأساس ((5،1)=P) بمفتاحه السِّريّ(3)؛ للحصول على: (10،6) = 3P
  - ■ يحسب مفتاح التّشفير السِّريّ المشترك(K) بضرب المفتاح العام للمستخدم رقم(2)، وهو ((13،7) = 8P)، بمفتاحه السِّريّ(3)؛ للحصول على:، $K = 3(8P) = 3(13,7) = (9,16)$ أي الحصول على الاحداثيات:(9،16)
- **المستخدم رقم(٢):**
  - ■ يختار مفتاحًا خاصًّا سريًّا عبارة عن عدد صحيح(d2 = 8).

- يحسب مفتاحه العام بضرب النقطة الأساس(5،1) بمفتاحه السِّريّ(8)؛ للحصول على: 8P = (13،7)
- يحسب مفتاح التّشفير السِّريّ المشترك(K) بضرب المفتاح العام للمستخدم رقم(1)، وهو ((10،6) = 3P)، بمفتاحه السِّريّ(8)؛ للحصول على: $K = 8(3P) = 3(8P) = (9,16)$، أي الحصول على الإحداثيات: (9،16)، وهي الإحداثيات نفسها التي حصل عليها المستخدم رقم(1).

مقارنة بين التّشفير المتناظر وغير المتناظر

بعد أن استعرضنا أنظمة التّشفير المتناظر وغير المتناظر، وتعرّفنا إلى أشهر أساليبهما وأنظمتهما المطبقة حديثًا، يحسن بنا الآن أن نقارن بينهما. فلكل من نظام التّشفير المتناظر وغير المتناظر خصائصه التي تميزه، وتجعله مناسبًا لتطبيقات محدّدة لا تصلح مع الآخر. يلخص الجدول(٤-٣) المميزات المهمة لكل منهما، التي توضح أيضًا الفروق بينهما.

	التّشفير المتناظر		التّشفير غير المتناظر
١.	يتم استخدام نفس المفتاح عند المرسل والمستقبل ونفس الخوارزميّة لكل من عمليّة التّشفير وفك التّشفير.	١.	يتم استخدام نفس الخوارزميّة للتشفير وفك التّشفير.
٢.	يجب إن يتم توزيع المفتاح السِّريّ بطريقة آمنة.	٢.	يستخدم زوج من المفاتيح أحدهما عام يطلع عليه الآخرون، والآخر سري خاص بكل مستخدم(ليس نفس المفتاح عند المرسل والمستقبل)
٣.	يحتاج إلى عمليّة توزيع آمنة للمفاتيح السِّريّة.	٣.	لا يحتاج إلى عمليّة توزيع المفاتيح.

الجدول(٤-٣): مقارنة بين التّشفير المتناظر وغير المتناظر

ولا تكتمل صورة المقارنة حتى نتعرّف على قوة خوارزميّات كل نظام، من حيث معرفة طول مفتاح التّشفير اللازم لكل خوارزميّة حتى تكون آمنـة، ومن هنا ظهرت الحاجة إلى تعريف «مستـوى السِّريّـة»(Security Level)، الذي يمكـن استخدامه في عمليّـة المقارنة. يعرّف كرستوف بار مستوى السِّريّة كما يلي: يكون للخوارزميّة مستوى سرّيّة(n) بت إذا كان عدد خطوات أفضل هجـوم معروف عليها هو(2^n)[1]. وهذا التعريف يتفـق مع كون قوّة خوارزميّة التّشفير المتناظر تساوي طول مفتاح التّشفير فيها. يوضح الجدول(٤-٤) طول مفتاح التّشفير اللازم لبعض مستويات السِّريّة لبعض خوارزميات التّشفير بنوعيه: المتناظر وغير المتناظر.

نوع التّشفير	الخوارزميّة	مستوى السِّريّة(بت)			
		٨٠	١٢٨	١٩٢	٢٥٦
متناظر	التّشفير القياسي المتقدم(AES)	٨٠	١٢٨	١٩٢	٢٥٦
غير متناظر	آر إس أيه(RSA)	١٠٢٤	٣٠٧٢	٧٦٨٠	١٥٣٦٠
	المنحنى البضاوي(Elliptic Curve)	١٦٠	٢٥٦	٣٨٤	٥١٢

الجدول(٤-٤): طول مفتاح التّشفير اللازم لتحقيق مستوى سرّيّة معين

من الجدول(٤-٤)، يمكن القـول إنّه يمكن الحصول علـى خوارزميّة تشفير بقوة(٨٠) بـت،(أي تحتاج إلى(٢٨٠) خطوة لكسـر تشفيرها)، باستخـدام خوارزميّة تشفير متناظر بطـول(٨٠) بت، أو باستخـدام خوارزميّـة التّشفير غير المتناظـر آر إس أيـه بطول مفتاح تشفير(١٠٢٤)، أو باستخدام خورازمية التّشفير بالمنحنى البيضاوي بطول مفتاح تشفير(١٦٠) بت. وبصفة عامة فإنّ طول مفتاح التّشفير يزداد بازدياد مستوى السِّريّة لأيّ خوارزميّة، ومن الملاحظ من الجدول أعلاه أنه يمكن الحصول على مستوى السِّريّة لخوارزميّة التّشفير بالمنحنى البيضاوي نفسه باستخدام مفتاح تشفير أقل بكثير من طول مفتاح التّشفير لخوارزميّة آر إس أيه لمستوى السِّريّة نفسه ، أو باستخدام مفتاح تشفير بضعف طول مفتاح التّشفير المتناظر، لمستوى السِّريّة نفسه كذلك.

١- Christof Paar and Jan Pelzl(2010), "Understanding Cryptography", p 156.

٤-٣ التصديق (التوقيع) الرقمي

نتيجة للتطوّر الكبير في تقنية المعلومات بشكل عام، فقد ظهر في الوقت الحاضر كم هائل جدًّا من المعلومات الرقميّة المخزّنة هنا أو هناك، ويجري تبادلها بين جهات عدّة، وقد أصبحت المعلومات تحفظ على وسائط إلكترونيّة بهيئة رقميّة، ويجري تبادلها عبر وسائل الاتصال الحديثة. وطالما أنّ المعلومة أصبحت معلومة رقميّة، فقد أصبح بالإمكان نسخ آلاف النسخ المطابقة تمامًا للمعلومة الأصلية، بل تُعدُّ كل نسخة منها أصليّة بحد ذاتها.

إذن نحن بحاجة إلى إيجاد طريقة رقميّة لتصديق الوثائق والرسائل الإلكترونيّة لضمان مصداقية المعلومات التي تحتويها والجهة التي أصدرتها، ويجب ألا تعتمد هذه الطريقة على وسائط التخزين، كما هي الحال في الوسائل التقليديّة مثلًا (ظرف مختوم، حبر سرّيّ، ... إلخ)، بل يجب أن تعتمد على المعلومة الرقميّة نفسها (أي محتواها)، بالإضافة إلى التصديق الرقمي الخاص بالجهة التي أصدرتها.

٤-٣-١ ماهيّة التصديق (التوقيع) الرقمي

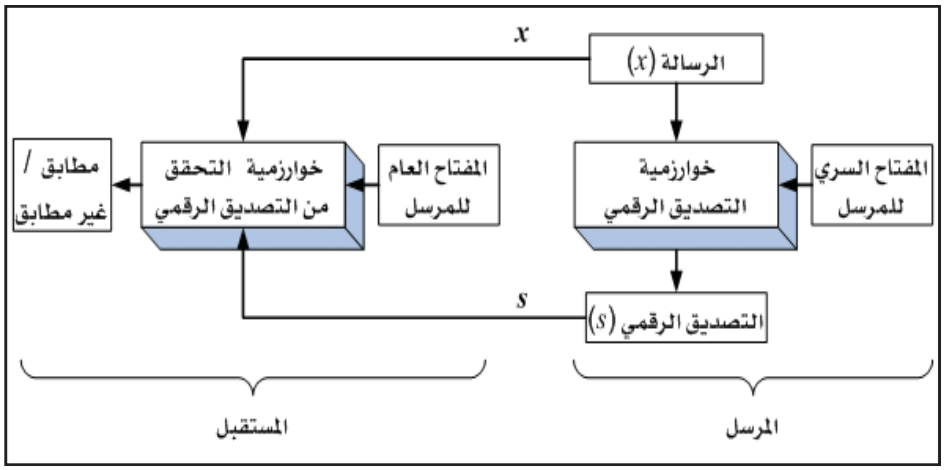
إنّ أحد أهم أدوات أمن المعلومات هو التصديق الرقمي (Digital Signature)، حيث يُعدُّ وحدة بناء أساسية لتحقيق عدد من عناصر أمن المعلومات، مثل التحقّق من هوية أصل البيانات (Data Origin Authentication)، وعدم الإنكار (Non-repudiation). وكما هو معروف فعندما يوقّع الشخص المخوّل بالتوقيع التقليدي (اليدوي) على رسالة أو خطاب معيّن، فإنّه يكتسب صيغته الرسميّة، أو بعبارة أخرى يتم التحقّق من أصل هذه البيانات بأنها صدرت من الجهة أو الشخص المخول بالتوقيع. لكن عند استخدام التصديق الرقمي فإنّ الأمر يختلف كثيرًا، إذ إن التصديق الرقمي لا يكفي أن يكون مجرّد صورة التوقيع اليدوي يتم لصقها بالرسالة. ففي هذه الحالة يمكن نسخ هذا التوقيع وإضافته لأيّ رسالة بسهولة، ولذلك فإنّ الأمر يتطلّب أن يعتمد التصديق الرقمي بدرجة أساسيّة على الرسالة نفسها، بالإضافة إلى توقيع الشخص المخوّل بالتصديق الرقمي من أجل إنتاج بصمة خاصّة بكل رسالة (Message Digest). وبهذه الطريقة يكون هناك بصمة فريدة لكل رسالة، بحيث لا

تنطبق بصمتان لرسالتين مختلفتين، حتى ولو صدرت من الشخص نفسه.

يعتمد التصديق الرقمي بشكل أساسي على نظام التّشفير بالمفتاح العام، لكن بطريقة عكسيّة له، حيث توقيع الرسالة من قبل معد الرسالة باستخدام مفتاحه السِّريّ(وليس المفتاح العام للمستقبل كما هي الحال في التّشفير بالمفتاح العام)، ويتم التحقّق من صحة التوقيع من قبل مستلم الرسالة باستخدام المفتاح العام للموقِّع. لاحظ أنّ الطرف الآخر- وهو مستلم الرسالة- يستخدم المفتاح العام للموقِّع للتّحقق من صحّة التوقيع، وليس من أجل تشفير الرسالة كما هي الحال في التّشفير بالمفتاح العام.

إذن فالتصديق الرقمي يتكوّن من عمليتين أساسيتين، كما هو موضح في الشكل(٤-١٦)، وهما:

- التوقيع(Sign): وهو عمليّة إجراء(إنتاج) التصديق الرقمي، ومدخلاتها هي: الرسالة والمفتاح السِّريّ للموقِّع، ونتيجتها هي التوقيع الرقمي نفسه، وهو رقم صحيح(طويل)،(٢٠٤٨) بت مثلًا.
- التحقّق من صحة التوقيع(Verify): وهو عمليّة التحقّق من أنّ التوقيع تم من الشخص المعنى على الرسالة المعنيّة. ومدخلاتها هي: الرسالة والمفتاح العام للموقِّع، ونتيجتها إحدى حالتين: إمّا مطابق، أو غير مطابق.



الشكل(٤-١٦): التصديق الرقمي

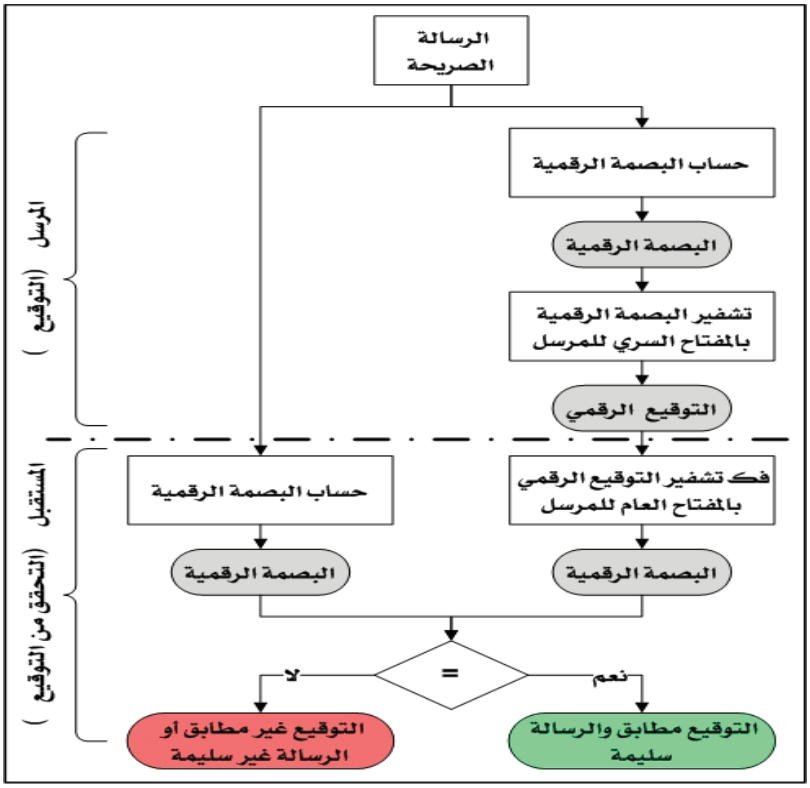
من أشهر طُـرُق التوقيع الرقمي هي الطريقة التي تعتمد علـى تصديق البصمة الرقميّة للرسالة وليس الرسالة الأصلية؛ لأنّه عادة ما تكون الرسائل الأصليّة طويلة،(قد يصل طول بعضها إلى مئات الصفحات)، وهو ما يجعل علميّة التصديق طويلة أيضًا. وتتلخص عمليتا التوقيع، والتحقق من صحّته بهذه الطريقة في الخطوات التالية، انظر الشكل(٤-١٧)[١]:

- عمليّة التوقيع:

١. يتم حساب البصمة الرقميّة(Hash Value) للرسالة(انظر موضوع: البصمة الرقميّة) المراد التوقيع عليها.

٢. يتم تشفير هذه البصمة الرقميّة باستخدام المفتاح السِّريّ للمرسل(الموقِّع) لإنتاج "التوقيع الرقمي" للرسالة.

٣. يتم إرسالها مع الرسالة الصريحة إلى المرسل إليه.



الشكل(٤-١٧): عمليتا التصديق الرقمي والتحقق من صحته

١- Bhaskar, S. M., and Ahson S. I., «Information Security: A practical Approach», p 98-102.

- عمليّة التحقّق من صحة التوقيع:

١. يفكّ المستقبل تشفير "التوقيع الرقمي"(ناتج الخطوة رقم(٢) في عمليّة التوقيع) باستخدام المفتاح العام للمرسل، لتظهر البصمة الرقميّة للرسالة الأصلية في صورتها الصريحة(غير المشفّرة).

٢. يحسب المستقبل البصمة الرقميّة للرسالة الصريحة(لاحظ أنّ المرسل إليه استقبل الرسالة الصريحة مع التوقيع الرقمي. الخطوة رقم(٣) في عمليّة التوقيع)، تمامًا كما فعل المرسل في الخطوة رقم(١) من عمليّة التوقيع لإنتاج البصمة الرقميّة للرسالة من جديد، لكن من طريق آخر لإجراء عمليّة المقارنة.

٣. يقارن المستقبل البصمة الرقميّة التي حسبها في الخطوة رقم(٢) أعلاه مع البصمة الرقميّة التي استقبلها مع الرسالة الأصلية. فإذا تطابقت هاتان القيمتان، فإنّ ذلك يكون كافيًا لإثبات أن هذه الرسالة مصدرها هو المرسل فعلًا، حيث تم التّشفير بواسطة مفتاحه الخاص، وأنّها سليمة لم يطرأ عليها أي تعديل، حيث أنتج النّص الوارد نفس البصمة الرقميّة، وأما إذا لم تتطابق، فهذا يعني أنّ التصديق الرقمي غير صحيح، أو أن الرسالة غير سليمة أو تم تعديلها.

مما سبق يتضح أن المرسل لا يستطيع إنكار أنّه أرسل هذه الرسالة؛ لأنّه وقّع عليها بمفتاحه السِّريّ، الذي لا يعرفه أحد ولا يملكه غيره، وكذلك فإنّ "البصمة الرقميّة" للرسالة ضمنت سلامة الرسالة الأصليّة، من حيث كشف أي حذف أو إضافة أو تعديل تم عليها.

٤-٣-٢ الاعتراف بالتصديق الرقمي

بدأ كثير من دول العالم باستخدام التصديق الرقمي(وبعضهم يطلق عليه التوقيع الإلكتروني) في تعاملاتها الإلكترونيّة وإصدار القوانين واللوائح المنظمة لذلك، ومن الدول التي بدأت في تطبيق ذلك، المملكة العربيّة السعودية، حيث أنشئ المركز الوطني للتصديق الرقمي[١]، ولكن ما الشروط الواجب توافرها للاعتراف بالتصديق الرقمي؟ فبالنظر إلى التوقيع اليدوي، نجد أنّ الأعراف والقوانين تجعله يحقق الشروط الآتية[٢]:

١- موقع المركز الوطني للتصديق الرقمي في المملكة العربيّة السعوديّة: http://www.pki.gov.sa/.

٢- داود، حسن طاهر(٢٠٠٤ب)، «أمن شبكات المعلومات».

١. التوقيع اليدوي هو التزام من الموقّع بما ورد في الوثيقة.

٢. لن يتم تغيير الوثيقة بعد توقيعها.

٣. لا يمكن نسخ التوقيع أو نقله إلى وثيقة أخرى.

- ويحقق التصديق الرقمي هذه الشروط على النحو الآتي:

١. يتم التوقيع الرقمي باستخدام المفتاح السِّريّ للمرسل، الذي لا يعرفه أحد، ولا يملكه غيره، بمعنى أنّه هو الذي وقّع الوثيقة، وأنّه ملتزم بما ورد فيها.

٢. التّوقيع الرقمي مستنتج من النّص الأصلي للرسالة؛ لأنه تم بتشفير البصمة الرقميّة للرسالة الأصليّة، وهذا يعني:

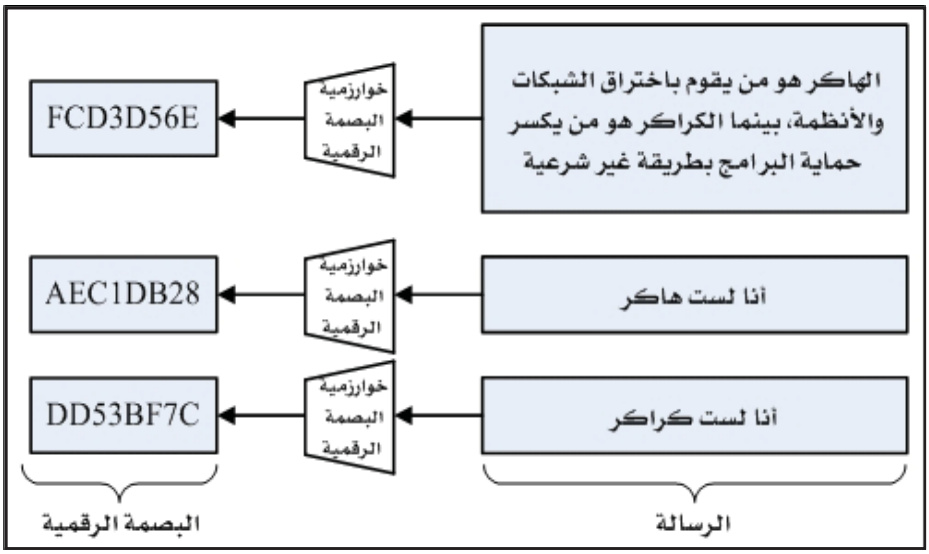
أ. أن الوثيقة لم يتم تغييرها بعد استخراج التوقيع الرقمي.

ب. أنه لا يمكن نسخ التوقيع الرقمي أو نقله إلى رسالة أخرى، وإلا فإنّه بعد فكّ تشفيره لن ينتج "البصمة الرقميّة" نفسها.

٤-٤ البصمة الرقميّة (Hash Value)

على الرغم من وجود تطبيقات كثيرة ومهمّة للبصمة الرقميّة، إلّا أنّ أشهرها هو استخدامها في التصديق الرقمي، كما مرّ معنا آنفًا. فعادة ما تكون الرسائل طويلة، قد يصل طول بعضها إلى مئات الصفحات، وهو ما يجعل تطبيق التصديق الرقمي عليها صعبًا جدًّا. ومن هنا جاءت البصمة الرقميّة (أو القيمة المركّزة) لتحلّ مشكلة التعامل مع الرسائل الطويلة. فالبصمة الرقميّة هي «سلسلة قصيرة وثابتة الطول من البتّات تشكّل بصمة فريدة لكل رسالة» ومعنى ذلك أن يكون لدينا بصمة رقميّة مختلفة لكلّ رسالة، لكن جميع البصمات طولها واحد مكوّن من العدد نفسه من البتّات، ١٦٠ بت مثلًا، مهما كان طول الرسالة. يوضح الشكل (٤-١٨) أمثلة لبعض الرسائل وبصماتها الرقميّة. لاحظ أنّ لكلّ رسالة في الشكل بصمة رقميّة مختلفة، لكن جميعها بطول (٣٢) بت (ثماني خانات بالتمثيل السِّت عشري كل واحدة منها أربعة بتات) ومن أهم ما يميز البصمات الرقميّة أن أي تعديل، ولو كان بسيطًا جدًا، في الرسالة ينتج عنه تغيير كبير في البصمة الرقميّة، وهذا واضح من البصمات الرقميّة للرسالتين الثانية

والثالثة في الشكل (٤-١٨)، حيث إن الفرق بين الرسالتين هو حرفان فقط، بينما الفرق بين بصمتيهما الرقميّة كبير جدًّا.



الشكل (٤-١٨): بعض الرسائل وبصماتها الرقميّة

تحسب البصمة الرقميّة باستخدام خوارزميّات خاصّة بذلك، بحيث يتم الحصول من خلالها على بصمة رقميّة فريدة لكل رسالة، من أشهرها: خوارزميّة (Message Digest-5-MD5)، وخوارزميّة (Secure Hash Algorithm-1-SHA-1)، وخوارزميّة (SHA-2)، وهناك خوارزميّة حديثة تحت التصميم والتجربة يتوقّع أن تُقنّن لتصبح قياسيّة عالميًّا في العام ٢٠١٢م، هي خوارزميّة (SHA-3).

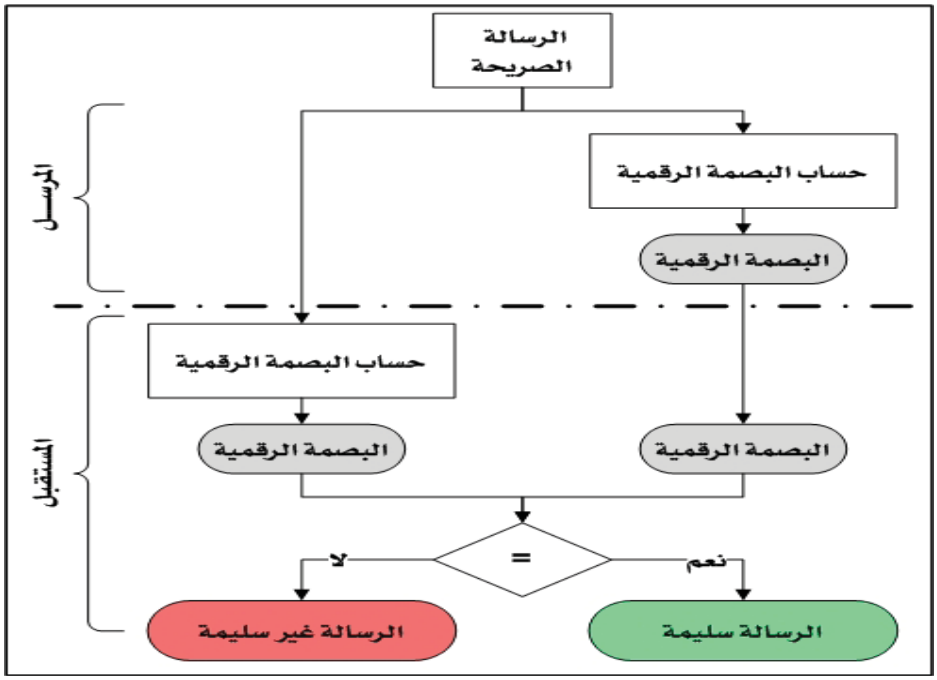
بما أنّ البصمة الرقميّة تُظهر بوضوح أيّ تغيير- ولو كان بسيطًا جدًا- على الرسالة الأصليّة؛ فإنّه يمكن من خلال ذلك كشف أيّ تعديل أو حذف أو إضافة على الرسالة الأصليّة. وتتلخص طريقة استخدام البصمة الرقميّة للتحقق من سلامة محتوى الرسالة فيما يلي، انظر الشكل (٤-١٩):

١. يحسب المرسل البصمة الرقميّة للرسالة باستخدام إحدى خوارزميّات البصمة الرقميّة.

٢. يرسل المرسل الرسالة الأصليّة متبوعة بالبصمة الرقميّة.

٣. عند استلام الرسالة من قبل المستقبل يُعيد حساب البصمة الرقميّة للرسالة التي استلمها.

٤. يقارن المستقبل البصمة الرقميّة التي حصل عليها في الخطوة السابقة(رقم ٣) مع البصمة الرقميّة التي استلمها مع الرسالة، فإذا تطابقت القيمتان، فهذا دليل على أنّ الرسالة سليمة ولم يطرأ عليها أيّ تغيير، أمّا إذا لم تتطابق فهذا دليل على أنّ الرسالة غير سليمة، أو أنه طرأ عليها تغيير ما.



الشكل(٤-١٩): التحقّق من سلامة وتكامل الرسالة باستخدام البصمة الرقميّة

عادة ما تستخدم البصمة الرقميّة مع التّشفير غير المتناظر لكشف التعديل أو الحذف والإضافة التي تطرأ على الرسالة الأصليّة بفعل فاعل.

٤-٥ كيفية تحقيق عناصر أمن المعلومات

تعرّفنا فيما مضى من هذا الفصل الوسائل التي يمكن استخدامها كوحدات بناء أساسية لتحقيق بعض عناصر أمن المعلومات، وهذه الوسائل هي: التّشفير، والتصديق الرقمي، والبصمة الرقميّة. وفيما يلي نشرح كيفية تحقيق عناصر أمن المعلومات سواءً باستخدام هذه الوسائل، كما هي الحال في عناصر التحقّق من الهُويّة، والسِّريّة، وسلامة المعلومة وتكاملها،

وعدم الإنكار، أم باستخدام وسائل أخرى كما هي الحال في عناصر التحكّم بالوصول، وتوفر المعلومة، والتدقيق.

٤-٥-١ تحقيق عنصري التحقّق من الهُويّة وعدم الإنكار

يستخدم التّشفير غير المتناظر مع التصديق الرقمي لتحقيق عناصر التحقّق من الهُويّة، وعدم الإنكار. وكيفيّة ذلك هي أنّه يتم إنتاج التوقيع الرقمي(انظر الشكل(٤-١٧)) باستخدام الرقم السِّريّ للمستخدم الذي لا يعرفه ولا يملكه إلا الشخص أو الجهة المعنيّة فقط، وبهذه الطريقة يتم التحقّق من هويّة المستخدم، ومن أصل منشأ البيانات، من أنّه الشخص المعني أو الجهة المعنيّة لا غيرها. كذلك يتم تحقيق عنصر عدم الإنكار حيث لا يستطيع المرسل(المستخدم) إنكار أنّه أرسل الرسالة لأنه وقّع عليها بمفتاحه السِّريّ الذي لا يعرفه ولا يملكه غيره.

٤-٥-٢ تحقيق عنصر التحكّم بالوصول

في المنشآت الصغيرة وفي البيئات التي لا تتطلّب أدوات تحكّم بالوصول خاصّة تضفي مزيدًا من الحماية لمواردها يمكن الاكتفاء باسم المستخدم وكلمة المرور للتحكّم بالوصول للموارد. وفي هذه الطريقة يُمنح المستخدم الصلاحيّات اللازمة التي بمجرد نجاح عمليّة الدخول تكون متاحة له كما هي الحال في البرامج التطبيقيّة التي تُدير مستخدميها بنفسها، وبذلك يكون للمستخدم حقّ الوصول إلى الموارد(ملفات، وطابعات، وقواعد وبيانات، وبرامج، ... إلخ) التي يحتاج إليها دون غيره من المستخدمين، وبذلك يتحقق عنصر التحكّم بالوصول. أمّا في حالة المنشآت الكبيرة التي يوجد فيها برامج تطبيقيّة كثيرة، يصعب معها استخدام اسم مستخدم وكلمة مرور لكل برنامج، والمنشآت ذات الطابع الحساس، فيلزم استخدام تقنيات التحكّم بالوصول التخصّصية، مثل: تقنية تسجيل الدخول الواحد، ومصفوفات التحكّم بالوصول، وأنظمة كشف التطفل، وأنظمة منع التطفل، وفيما يلي نستعرض كل تقنية من هذه التقنيات.

٤-٥-٢-١ تسجيل الدخول الواحد(Single Sign-on)

مع تعدّد أنظمة التشغيل، وتعدّد أنواع الشبكات والبرامج التطبيقيّة، قد يجد المستخدم نفسه

أمام عدد لا بأس به من أسماء المستخدمين وكلمات المرور التي يجب أن يحفظها ويستخدمها عند الرغبة في الدخول إلى أيٍّ من تلك الأنظمة أو الشبكات أو البرامج، وبذلك يكون من الصعب على مديري الشبكات والأنظمة متابعة هذا العدد الكبير من أسماء المستخدمين وكلمات المرور، وفرض السياسات الأمنيّة المختلفة عليها. فمثلًا قد ينسى المستخدم كلمات المرور الخاصة به، أو يخلط فيما بينها، وهو ما قد يتسبب في عدم قدرته على الدخول للأنظمة التي يحتاج إليها. وهذا الأمر يدفع مديري تلك الأنظمة إلى إلغاء جميع كلمات المرور الخاصة بذلك المستخدم، ومن هنا ظهرت فكرة استخدام تقنية تسجيل الدخول الواحد (Single Sign-on)، حيث يدخل المستخدم مرّة واحدة من خلال نظام موحّد مخصّص لهذا الغرض، وبعدئذ تكون جميع موارد الشبكة التي يحتاج إليها في متناوله، وفق الصلاحيّات الممنوحة له. قد يبدو للوهلة الأولى أنّ هذه الطريقة تضعف من أمن تلك الأنظمة، لكن الواقع يشير إلى أنّها تقوّي أمنها؛ لأنّ المستخدم الذي لديه عدد كبير من أسماء المستخدمين وكلمات المرور عادة ما يضطر إلى تسجيلها في مذكراته أو في حاسبة الشخصي؛ لتسهيل عمليّة الرجوع إليها وتذكرها، وهذا أمر ينافي السياسات الأمنيّة لكلمات المرور؛ لأنّها تكون بذلك عرضة لانكشافها للآخرين، (انظر الفصل الخامس: موضوع: السياسة الأمنيّة لكلمات المرور).

من تقنيات تسجيل الدخول الواحد نظام «كيربورس» (Kerberos). وهو نظام تسجيل واحد للشبكات الموزّعة، ويخدم أنظمة الخادم/ العميل (Client/Server) تم تطويره في أواسط الثمانينيّات الميلاديّة، ويستخدم نظام التّشفير المتناظر لتشفير كلمات المرور عبر الشبكات. ويحتوي نظام كيربورس مركز توزيع المفاتيح (Key Distribution Center-KDC) الذي يحتفظ بجميع أرقام المستخدمين السِّريّة. فعندما يريد المستخدم الدخول للشبكة يُرسل اسم المستخدم الخاص به إلى مركز توزيع المفاتيح (KDC) ليخصّص بدوره رقمًا سريًّا و يرسله إليه مشفّرًا باستخدام تقنية التّشفير المتناظر، وعند وصول الرقم السِّريّ إلى جهاز المستخدم يطلب منه إدخال كلمة المرور الخاصة به لفك تشفير الرقم السِّريّ. فإذا كانت كلمة المرور صحيحة يتم فكّ تشفير الرقم السِّريّ، والسماح له بالدخول، وتصبح موارد

الشبكة متاحة له، وإلا فلا يسمح له.

ثمّة تقنية أخرى لتسجيل الدخول الواحد تسمّى تقنية العميل اللطيف (أو الرقيق) (Thin Client). في هـذه التقنية، تُستخـدم نهايات طرفيّـة (Terminals) وليس أجهزة حاسب آلي (Workstations) للدخول إلى الشبكة من خلال نظام مركزيّ محمّل على جهاز خادم رئيس (Server). ولا يوجد في هـذه النهايات الطرفيّة نظام تشغيل ولا يتم تخزين البيانات عليها محليًّا، وعند رغبة المستخدم في الدخول إلى الشبكة تُشغّل النهاية الطرفيّة التي بدورها تُشغّل قائمة قصيرة من الأوامر تكفي لتحميل نظـام التشغيل من الخادم الرئيس والبرامج التطبيقيّة التي يحتاج إليها المستخدم فقط، وفق الصلاحيّات المحدّدة له. ولا يمكن للمستخدم الوصول إلى أيّ مورد من موارد الشبكة أو تشغيـل أيّ برنامج تطبيقي حتى يتم التعرّف إلى هويّته والمصادقة عليها من قبل الخادم الرئيسي، وبذلك يكون التحكّم بالصلاحيّات لجميع المستخدمين مركزيًّا.

٤-٥-٢-٢ مصفوفة التحكّم بالوصول

مصفوفة التحكّم بالوصول (Access Control Matrix) هي جدول يحتوي المستفيدين كصفوف، والموارد كأعمدة، ويحدّد ما العمليّـات الممكنة لكل مستفيد على كل مورد، كما هو موضّح في الجدول (٤-٥).

المستفيد	ملف١	ملف٢	ملف٣	ملف٤
أحمد	قراءة	قراءة، كتابة	قراءة	قراءة، كتابة
علي	تحكم كامل	لا يوجد	تحكم كامل	قراءة
محمد	قراءة، كتابة	لا يوجد	قراءة	تحكم كامل
صالح	تحكم كامل	تحكم كامل	لا يوجد	لا يوجد

الجدول (٤-٥): مصفوفة التحكّم بالوصول.

يحتوي كل صف إمكانـات (Capabilities) المستخدم المحدّد في ذلـك الصف. فمثلًا، تكـون إمكانات المستخدم "علي" هـي: "تحكم كامـل" (Full Control) على "الملف١"،

و "لا توجد" لـه أيّ إمكانيّـة على "الملـف٢"، و "تحكّم كامـل" على "الملـف٣" وإمكانية "القراءة" على "الملف٤". ويحتوي كل عمود قائمة التحكّم بالوصول(Access Control List-ACL) للمورد المحدّد في ذلك العمود. فمثلًا قائمة التحكّم بالوصول "للملف٣" هي: "قراءة" للمستخدم "أحمد"، و "تحكّم كامل" للمستخدم "علي"، و "قراءة" للمستخدم "محمد"، و "لا توجد" إمكانية للمستخدم "صالح".

٤-٥-٢-٣ أنظمة كشف التطفل(IDSs)

يقصـد بكشـف التطفـل عمليّـة كشـف الاستخـدام غـير الشرعـي أو الهجـوم علـى الأجهـزة والشبـكات وأنظمـة الاتصـالات، والمهمـة الأساسيّـة لأنظمـة كشـف التطفـل (Intrusion Detection Systems-IDSs) هي التقـاط أيّ شيء مريب أو مشكوك فيه يحدث في الشبكة، والتنبيه على ذلك بشكل رسالة(فلاش) على شاشة مدير النظام أو رسالة قصيرة(SMS) أو بريد إلكتروني. وعادة ما تقوم أدوات كشف التطفل بتفحص سيل البيانات وسجلّات الأحداث، وكشف أي بيانات غير طبيعيّة والتنبيه عليها.

تتكوّن أغلب أنظمة كشف التطفل من ثلاثة مكوّنات رئيسة هي: الحسّاسات(Sensors)، وأدوات التحليل(Analyzing tools)، و واجهات التواصل مع مديري الأنظمة(Interfaces). تُجمّع الحسّاسات البيانات وأنشطة المستخدمين وترسلها لأدوات التحليل، وتُحلّل أدوات التحليل البيانـات والأحداث الواردة إليها مـن الحسّاسات، والتعرّف إلى أيّ بيانـات أو أنشطة تبدو مريبة أو غير طبيعيّة، وعند وجود أيّ نتائج إيجابيّة لدى أدوات التحليل، تُرسل إلى واجهات التواصل مع مديري الأنظمة لإخطارهم بوجود شيء مُريب وغير طبيعي.

أنواع أنظمة كشف التطفل

هناك نوعان رئيسان من أنظمة كشف التطفل، هما: أنظمة كشف التطفل الشبكية، وأنظمة كشف التطفل على الأجهزة.

أ. أنظمة كشف التطفل الشبكية

هي عبارة عن حسّاسات خاصّة بذلك، تسمى صناديق(أجهزة) كشف التطفل (Intrusion

Detection Appliance) صمّمت خصّيصًا لهذا الغرض، و تُركّب في أماكن محدّدة في الشبكة. وقد تكون أجهزة حاسب آلي مُعدّة لهذا الغرض، ويركّب عليها برامج كشف التطفل اللازمة، وفي كلا الحالتين فإنّ هذه الأجهزة تُربط بالشبكة من خلال كرت الشبكة (Network Interface Card-NIC) الذي بدوره يستطيع متابعة جميع البيانات المارّة في الوسط الناقل. في الأحوال العادية ينسخ كرت الشبكة حُزم البيانات(Packets) الموجّهة إليه، والتي تحمل عنوانه فقط، و بالتالي التي تخصّه، ثم يدفعها إلى بروتوكولات الشبكة لمعالجتها. لكن في حالة كشف التطفّل يتم إعداد كرت الشبكة لينسخ حزم البيانات المارة في الوسط الناقل كافّة ، ثم إرسال نسخة منها للمحلّل(Analyzer) ليفحصها ويبحث عن أيّ حزم بيانات مُريبة.

تجدر الإشارة إلى أنّ هذا النوع من أجهزة كشف التطفّل تستطيع متابعة حُزم البيانات المريبة في الوسط الناقل، ولا تستطيع معرفة ما يدور في أجهزة الحاسب الآلي، فهي بذلك لا تغني عن الحاجة إلى أنظمة كشف التطفل على الأجهزة نفسها.

ب. أنظمة كشف التطفل على الأجهزة

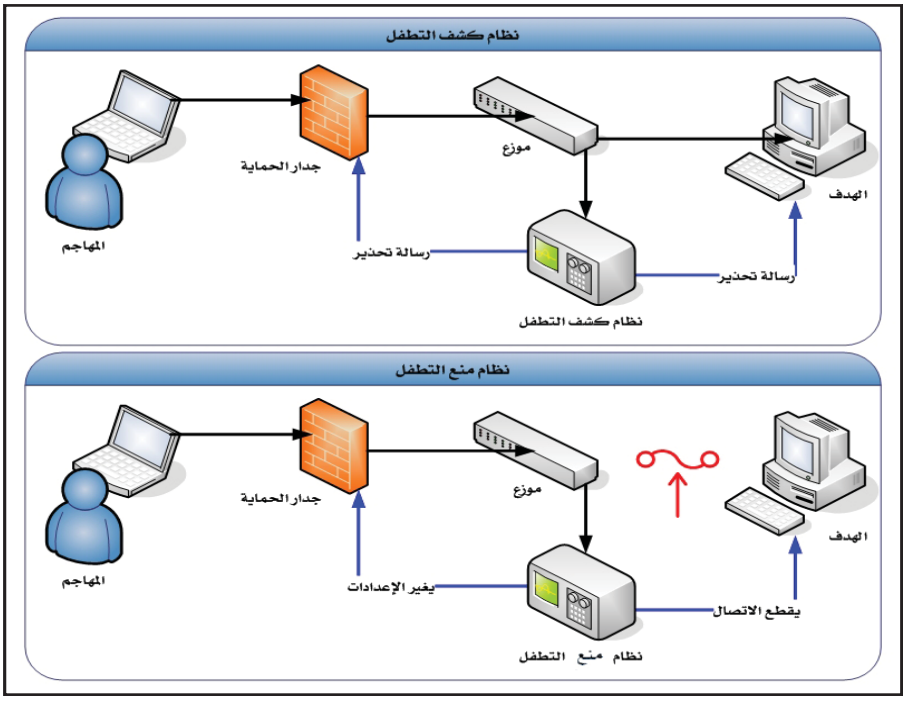
هي برامج كشف تطفل تُركّب على أجهزة الحاسب الآلي(Workstations) أو الخوادم(Servers)، لمراقبة أيّ أنشطة مُريبة عليها. وعادةً ما تستخدم هذه الأنظمة لمتابعة المستخدمين، والتأكد من عدم قيامهم بحذف ملفّات النظام أو إعادة تهيئة الأجهزة والخوادم، أو تغيير إعداداتها المهمّة والحرجة، أو إجراء أيّ تغييرات من شأنها أن تجعل تلك الأجهزة والخوادم معرّضة للخطر. فكما أنّ أنظمة كشف التطفّل الشبكيّة مختصّة بمتابعة البيانات المارّة عبر الوسط الناقل في الشبكة، ولا تستطيع أن تعرف ماهيّة الأنشطة التي تُنفذ على الأجهزة، تكون هذه الأنظمة مختصّة بأجهزة الحاسب الآلي نفسها، وليس الشبكة؛ للكشف عن أيّ نشاط غير طبيعي عليها.

عادة ما يُركّب هذا النوع من الأنظمة على أجهزة الخوادم المهمّة والحساسة فقط، مع عدم تركيبها على جميع الخوادم والأجهزة؛ نظرًا لما تحتاج إليه من مساحات تخزين عالية، وكذلك

حتى لا يتم تحميل جميع الأجهزة بأعمال إضافيّة كثيرة تتسبّب في بطء الشبكة بشكل عام.

٤-٥-٢-٤ أنظمة منع التطفل(IPSs)

في أنظمة كشف التطفل يُكشف عن البيانات والأنشطة غير الطبيعيّة، ومن ثم التنبيه عليها فقط. أمّا أنظمة منع التطفل(Intrusion Prevention Systems-IPSs) فتكشف البيانات والأنشطة غير الطبيعيّة، ثم تمنعها من الوصول إلى أهدافها، كما يوضح ذلك الشكل(٤-٢٠). وبذلك فإنّ أنظمة منع التطفل تقوم بخطوات استباقيّة لمنع المتطفّل من الوصول إلى أهدافه. فكما يتّضح من الشكل(٤-٢٠)، يقطع جهاز منع التطفل المضمّن(Inline IPS) الاتصال بين المهاجم والهدف عند وجود بيانات مريبة، كما يتدخل مباشرة، ويعدّل قوائم التحكّم بالوصول(ACLs) لجدار الحماية.



الشكل(٤-٢٠): مقارنة بين أنظمة كشف التطفل وأنظمة منع التطفل

وكما هي الحال في أنظمة كشف التطفل يوجد نوعان من أنظمة منع التطفل، هما: أنظمة

منع التطفل الشبكيّة، وأنظمة منع التطفل على الأجهزة، وتعمل هذه الأنظمة بصورة مشابهة لأنظمة كشف التطفل، إلا أنّها تزيد عليها بأنّها تقطع الاتصال وتوقف عمل الأجهزة في حالة وجود بيانات أو أنشطة مُريبة على الشبكة أو على الأجهزة.

٤-٥-٣ تحقيق عنصر السِّريّة

لتحقيق عنصر السِّريّة، فإنّه يمكن استخدام أيٍّ من تقنيات التّشفير، سواءً المتناظر أم غير المتناظر، وبمجرّد تطبيق ذلك سيتحقّق هذا العنصر بدرجة تتناسب مع قوّة نظام التّشفير المستخدم.

٤-٥-٤ تحقيق عنصر سلامة المعلومة وتكاملها

يمكن التحقّق من سلامة الرسالة وخلوّها من أيّ حذف أو تعديل أو إضافة باستخدام البصمة الرقميّة. فبمجرد تطبيق تقنية البصمة الرقميّة سيتم كشف أيّ تعديل أو حذف أو إضافة، وبذلك يتحقق عنصر سلامة المعلومة وتكاملها.

كما يمكن تحقيق سلامة البيانات وضبط عمل المستخدمين من خلال تحديد خيارات محدّدة (مثل القوائم المنسدلة)، التي يجري التعامل معها لاختيار البيانات وإدخالها في الأنظمة والبرامج المختلفة، ثم تنفيذ العمليّات على تلك البيانات (كالتعديل والحذف)، وفق صلاحيّات محدّدة ودقيقة، ومن ذلك أيضًا التحكّم بالملفّات المهمة وحجب إمكانيّة الوصول إليها عن المستخدمين العاديين، وتزويد البرامج التطبيقيّة بوسائل التحقّق من صحة البيانات المدخلة، ورفض البيانات غير المعقولة أو غير المتوقّعة حسب طبيعة حقول تلك البيانات، كإدخال بيانات مالية كبيرة في حقول صغيرة (أو العكس)، أو إدخال حروف في حقل تاريخ مثلًا. أمّا قواعد البيانات فيجب أن يُحصر التعامل معها في أشخاص محدّدين ذوي قدرة وكفاءة عالية، مع توفير آليات للتراجع عن التعديلات الخاطئة والعودة إلى النسخة السابقة قبل التعديل وكذلك، حماية البيانات المنقولة من التغيير أثناء إرسالها أو استقبالها من قواعد البيانات وإليها.

٤-٥-٥ تحقيق عنصر توفر المعلومة

بعد ظهور هجمات تعطيل الخدمة (DoS)، أصبح عنصر توفر المعلومات عنصرًا أساسيًا

في أمن المعلومات، ومع تقدم استخدام الإنترنت وانتشارها، أصبح توفر مواقع الخدمات على الشبكة أمرًا ضروريًّا يحتم على مديري هذه المواقع العناية التامة بتوفر (ديمومة) المواقع، وحصر خروجها من الخدمة في أضيق نطاق. وهناك وسائل أساسية لتحقيق عنصر توفر المعلومات، وهي:

- أن يكون هناك سعة كافية في الشبكة والأنظمة والخوادم وأجهزة التخزين ومركز البيانات (Data Center) بشكل عام، من أجل أن تعمل بمستوى جيّد وباستمرارية وبكفاءة عالية.
- القدرة على العودة بعد حدوث الأعطال أو التوقّفات بطريقة سريعة وآمنة.
- تجنّب وجود نقطة العطل الوحيدة (Single Point of Failure)، الذي تتسبب في التوقّف الكامل في حال تعرضها للعطل.
- أخذ نسخ احتياطيّة من البيانات والأنظمة والبرامج، وكذلك من إعدادات أجهزة الشبكة، سواءً المحلية (LAN)، أم الواسعة (WAN)، وأي أجهزة أخرى حسب طبيعة عمل المنشأة؛ للرجوع إليها عند الحاجة.
- توفير أجهزة وأنظمة وتقنيات رديفة (في نفس مركز البيانات) تعمل جنبًا إلى جنب مع الأجهزة والأنظمة والتقنيات الأساسيّة، حسب الحاجة والأهمية. ويمكن أن يتم توفير هذه التجهيزات بإحدى طريقتين:
  - طريقة التناوب بتقنية نشط/غير نشط (Active/Passive) وهي طريقة تعتمد على توفير تجهيزات رديفة تكون جاهزة للعمل، لكن غير نشطة، ويجري التحوّل إليها عند الحاجة إما يدويًا أو باستخدام برامج وتجهيزات خاصّة بذلك. وتتميز هذه الطريقة بسهولة الحصول عليها، وسهولة إعدادها والتحكم فيها، إلا أنّه لا يتم التحوّل للتجهيزات غير النشطة بسرعة عالية، ولا يتم استغلالها الاستغلال الأمثل، حيث إنها لا تستخدم إلا وقت الأعطال فقط، وتبقى غير نشطة (خاملة) طوال الأوقات الأخرى.

- طريقة التناوب الآلي الكامـل، أو ما يعرف بتقنيـة نشط/نشط(Active/Active) وهي طريقة تعتمد على توفير تجهيزات رديفه تعمل جنبًا إلى جنب مع التجهيزات الأساسيّة في الوقت نفسه، ومطابقة لها تمامًا، ويجري التحوّل فيما بينها آليًّا عند الحاجة. وتتميز هذه الطريقة بميزتين رئيستين: الأولى أن كلًّا من التجهيزات الرئيسة (أيًّا كان نوعها ومهمتها) والرديفة بعضها بديل لبعض وتتبادل فيما بينهما آليًّا ومباشرة وبسرعة عالية، لدرجة أنّه يمكن أن يطلق على الرئيس بديل والبديل رئيس. والثانية، هي إمكانية توزيع الأحمال على كلا التجهيزات الأساسيّة والرديفة بالتساوي، واستغلالهما الاستغلال الأمثل في جميع الأوقات بما في ذلك الأوقات التي لا يوجد بها أعطال، التي تشكل النسبة العظمى من أوقات العمل، و من ثَمَّ تسريع أداء كل منهما بدلًا من إبقاء أحدهما غير نشط(خامل) طوال الأوقات العادية على الرغم من جاهزيته، كما هي الحال في تقنية نشط/غير نشط.

- الحماية من التأثيرات السلبية للمكوّنات الطبيعية كالحرارة والرطوبة والغبار والملوثات والكهرباء الساكنة، مع ضرورة تأريض الدوائر الكهربائيّة وتوفير موانع الصواعق.
- توفير مركز بيانات رديـف(Disaster Recovery Data Center)؛ لاستخدامه عند وقوع الكوارث، ويتم التحـول إليه آليًّا عند وقوع الأعطـال الكبيرة أو الكوارث المعلوماتيّة، التي تسبّب توقّـف مركز البيانات الرئيس. ويجب في هذه الحالة توفير جميع الأجهزة والبرامج وأجهزة الربط وخطوطها اللازمة في مركز البيانات الرديف والرئيس التي تضمن شيئين رئيسين هما:
  - تحديث البيانات في المركز الرديف بشكل مستمر؛ لضمان الحصول على نُسخ مطابقة لما في مركز البيانات الرئيس، بما في ذلك قواعد البيانات، وبيانات الإعدادات والتهيئة لجميع الأجهزة.
  - سهولة وضمان التحوّل السلس والسّريع من المركز الرئيس إلى الرديف

عنـد الحاجة، بمـا في ذلك تحـوّل جميـع المستخدمـين، دون الحاجة لإجراء أي تعديلات على أجهـزة المستخدمين، أو علـى أي من أجهزة الربط مثل الموزعـات(Switches) والموجهـات(Routers) وجدران الحماية(Firewalls).

- التدريب الجيد للعاملين على التعامل مع الأعطال، والتحويل إلى التجهيزات الرديفة، ومتابعة ذلك وإدارته.
- استخدام أنظمة مكافحة البرامج الضـارة، كفيروسات حذف الملفّات التي تتسبب في عدم توفـر المعلومة(انظر الفصل السادس: موضوع: البرامـج الضارة وطرق مكافحتها).
- استخدام أنظمـة الطاقة الكهربائيّـة الاحتياطيّة(انظر الفصـل التاسع: الحماية الماديّة).
- استخدام أنظمة كشف هجمات تعطيل الخدمة(DoS) ومكافحتها.

وتشير الدراسات الحديثة إلى أنّ عدم توفـر المعلومة لا يُعزا للأعطال والأسباب المتعلّقة بالأجهزة والبرمجيات، وإنّما قد تحدث كذلك بسبب أخطاء الفنيين ومديري الأنظمة، أو بسبب عدم القدرة على التعامل مع الإنذارات المبكرة أو إهمالها، وتؤكد تلك الدراسات على ضرورة التدريب والتأهيل الجيّد لجميع من يتعامل مع المعلومة من: مستخدمين وفنيّين ومديرين.

٤-٥- ٦ تحقيق عنصر المتابعة

يمكن تحقيق عنصر المتابعة والتدقيق على مستويات مختلفة، تتراوح من مجرّد متابعة ما يجري على الحاسب الشخصي، إلى متابعة مراكز البيانات والشبكات الكبيرة، وهناك وسائل وأنظمة تدقيق ومتابعة لكل مستوى، منها:

- سجلّات أحداث نظام التشغيـل(Operating System Events Log) التي ترد رفق أنظمة التشغيل، لمتابعة الأحداث التـي تتم على مستوى الأجهزة الشخصية أو محطات العمل وتدقيقها.

- سجـلّات أحـداث الشبكـة(Network Events Log) الخاصة بأنظمـة تشغيل الشبكات وإدارة المستخدمين، لمتابعة ما يدور في الشبكة وما يقوم به المستخدمون، وأوقات تلك الأحداث وتواريخها.
- سجلّات أحـداث قاعـدة البيانـات(Database Events Log) الخاصة بقواعد البيانات، لمتابعة ما يدور في قواعد البيانات، وأوقات تلك الأحداث وتواريخها.

ويمكن استخدام هذه الأنظمة والاستفادة منها في إجراء عمليّات المتابعة والتدقيق بإحدى الطرق التالية:

- إجراء عمليّات تدقيق ومتابعة تاريخيّة(Historical) بعد انتهاء الأحداث، ثم اتخاذ الإجراءات المناسبة وفقًا لنتائج هذه العمليّات.
- إجراء عمليّات تدقيق ومتابعة حيّة مباشرة(Online) وقت وقوع الأحداث لإخطار المسؤولين عن معالجة تلك الأحداث في حينه بمـا يجري، ومن ذلك: إرسال رسالة بريد إلكتروني، أو رسالة قصيرة(SMS) على الهاتف المحمول ليعملوا على حلّها.
- أجراء عمليّات تدقيق ومتابعة وقائية(Preventive)، بحيث تعالج أنظمة التدقيق نفسها الأخطاء عند وقوعها مباشرة، أو على الأقل إيقاف مصدر الخطر أو الخلل دون انتظار تدخل المسؤولين.

ملخّص الفصل

قدّم هذا الفصل الوسائل والتقنيات المتاحة التي يمكن استخدامها لتحقيق عناصر أمن المعلومات السبعة. وهذه الوسائـل هي: التّشفير بنوعيه: المتناظر وغـير المتناظر، والبصمة الرقميّة، والتصديـق الرقمي، وتسجيـل الدخول الواحـد، ومصفوفات التحكّـم بالوصول، وأنظمة كشف التطفـل، وأنظمة منع التطفل، والأنظمة الرديفـة، وأنظمة تسجيل الأحداث. فيمكن تحقيـق عنصر السِّريّة باستخـدام التّشفير المتناظـر أو غير المتناظـر أو بهما معًا. ويمكـن تحقيق عناصر التحقّق مـن الهُويّة، والتحكـم بالوصول للمنشـآت الصغيرة، وعدم الإنكار باستخدام التّشفير غير المتناظر والتصديق الرقمي معًا. ويمكن تحقيق عنصر سلامة المعلومة وتكاملها باستخدام البصمة الرقميّة. كما يمكن استخدام التصديق الرقمي للتحقق

من هويّة الشخص(Entity Authentication) ويستخدم مع البصمة الرقميّة للتحقق من هويّة الرسالة أو المعلومة(Data Origin Authentication). ويمكن استخدام تقنيات تسجيل الدخول الواحد، ومصفوفات قوائم التحكّم، وأنظمة كشف التطفل ومنعه؛ لتحقيق عنصر التحكّم بالوصول للمنشآت الكبيرة والمنشآت ذات الطابع الحسّاس. ويمكن تحقيق عنصر التوفر باستخدام تقنيات الأجهزة والبرامج الرديفة وأنظمة الحماية ضد الهجمات التي تعطل الخدمة(Denial of Service-DoS). ويمكن تحقيق عنصر التدقيق باستخدام تقنيات متابعة وتسجيل الأحداث، سواءً تلك التي ترد رفق أنظمة التشغيل، أم التي تبنيها شركات متخصّصة في ذلك.

مسائل

١. قارن بين التّشفير المتناظر والتّشفير غير المتناظر.

٢. قارن بين التّشفير التسلسلي والتّشفير الكُتلي.

٣. قارن بين أساليب تشغيل التّشفير الكُتلي من حيث مميزات كل منها وعيوبه.

٤. قارن بين نظام آر إس أيه(RSA) ونظام التّشفير بالمنحنى البيضاوي(ECC).

٥. إذا كانت قيم العددين الأوليين(p) و(q) لنظام آر إس أيه هي:

$(p = 5)$، $(q = 11)$؛ فقم بالآتي:

أ. أي من القيم الآتية مناسبًا للعدد(e): (3) أم(4)؟ ولماذا؟

ب. احسب المفتاح العام(n, e).

ج. احسب المفتاح الخاص(d).

د. شفّر الرسالة$(x = 9)$، ثم فكّ تشفيرها، ثم قارن ما حصلت عليه.

٦. إذا كانت معادلة المنحنى البيضاوي هي: $y^2 = x^3 + 4x + 20 \bmod 29$

احسب الآتي للقياس(29):

أ. مضاعفة النقطة $(x_1 , y_1) = (5,22)$.

ب. حاصل جمع النقطتين: $(x_1 , y_1) + (x_2 , y_2) = (5,22) + (16,27)$.

ج. نتيجة الضرب التراكمي $(8P)$ إذا كانت: $P = (x_1 , y_1) = (5,22)$

٧. عرّف مستوى السِّريّة لخوارزميّة التّشفير. ولماذا تكون مفاتيح التّشفير غير المتناظر أطول من مفتاح التّشفير المتناظر للحصول على مستوى السِّريّة نفسه لكل منهما؟

٨. لماذا لا يعوّل كثيرًا على إخفاء خوارزميّة التّشفير، بينما يجب إخفاء المفتاح السِّريّ؟

٩. بالرجوع إلى الشكل (٤-١)، اشرح إمكانية تحقيق عنصر من عناصر أمن المعلومات بأكثر من وسيلة، وكذلك اشتراك أكثر من وسيلة لتحقيق عنصر واحد.

١٠. اشرح طريقة الحصول على كل من التصديق الرقمي (التوقيع) والبصمة الرقميّة، ثم قارن بينهما على ضوء الشكلين (٤-١٧) و(٤-١٩).

١١. في الشكل (٤-١٧)، يتم إرسال الرسالة الأصليّة (الصريحة) دون تشفير. هل يُعدُّ هذا ثغرة أمنية؟ إذا كان الجواب بنعم، فاقترح طريقة لتحسين ذلك، وإذا كان الجواب بلا، فلماذا؟

١٢. اشرح كيف يمكن الاعتراف بالتوقيع الرقمي (الإلكتروني).

١٣. قارن بين أنظمة كشف التطفل الشبكية، وأنظمة كشف التطفل على الأجهزة.

١٤. هل يمكن أن تغني أنظمة منع التطفل عن أنظمة كشف التطفل؟ ولماذا؟

١٥. بالرجوع إلى شبكة الإنترنت، اقترح خوارزميات خلاف ما ذكر في هذا الفصل لكل من: التّشفير المتناظر، والتّشفير غير المتناظر، وحساب البصمة الرقميّة.

١٦. لماذا تُعدُّ المعلومات أهم مورد يجب حمايته؟ اشرح ذلك من خلال الأسباب الخمسة الرئيسة التي أبرزت الحاجة إلى أمن المعلومات.

١٧. بالرجوع إلى شبكة الإنترنت، حدّد الأجهزة والأنظمة اللازمة لبناء مركز بيانات رديف (Disaster Recovery Data Center) يعمل بالتناوب الآلي مع مركز

البيانات الرئيس، ويتم التحوّل الكامل إليه تلقائيًا عند الحاجة.

١٨. بالرجوع إلى شبكة الإنترنت، أعط أمثلة لوسائل إضافية لتنفيذ عمليّات التدقيق والمراقبة على مستوى مركز البيانات، وعلى مستوى الشبكة، خلاف ما ذكر في هذا الفصل.

١٩. بالرجوع إلى شبكة الإنترنت، حدّد الإمكانات المتاحة في سجّل الأحداث (Event Viewer) الخاص بنظام التشغيل ويندوز لأجهزة الحاسب الآلي الشخصيّة.

الفصل الخامس

سياسات أمن المعلومات ومعاييره وتوجيهاته وإجراءاته

أهداف الفصل

- شرح مفهوم السياسات الأمنيّة وأنواعها وخصائصهـا، والبنود التي يجب أن تحتويها، وبيان أهميتها لحماية المعلومات، مع إيراد أمثلة لكل نوع من أنواع السياسات.
- شرح مفهوم المعايير القياسية وكيفية تطبيقها وعلاقتها بالسياسات الأمنيّة.
- شرح مفهوم التوجيهات واستخداماتها.
- شرح مفهوم الإجراءات ومن يقوم بها، والأنظمة التي تطبّق عليها.
- شرح مفهوم تصنيف المعلومات مع تحديد مستويات التصنيف المشهورة.
- التدريب والتوعية بأمن المعلومات كركيزة أساسية لتطبيق المفاهيم السابقة.

ما ستتعلمه في هذا الفصل

- السياسة الأمنيّة ومدى الحاجة لها والجوانب والإجراءات الإداريّة فيها.
- أنواع السياسـات الأمنيّة: السياسات الأمنيّـة العامّة، والسياسـات الأمنيّة الموضوعيّة، والسياسات الخاصّة بأنظمة محدّدة.
- المعايير القياسية وكيفيّة ضبط استخدام منتجات تقنية المعلومات في المنشأة.
- الخط الأساسي كمرجع يكون قياس وضع أمن المعلومات في المنشأة قربًا منه وبُعدًا.
- التوجيهات كإرشادات غير إلزاميّة للمساعدة في تطبيق السياسات الأمنيّة.
- الإجراءات كخطوات تفصيليّة لتنفيذ المهام وفق برنامج أمن المعلومات.
- مستويات تصنيف المعلومات وخطوات التصنيف.
- التدريب والتوعية بأمن المعلومات لضمان تطبيق المفاهيم السابقة.

سياسات أمن المعلومات ومعاييره وتوجيهاته وإجراءاته

٥-١ مقدّمة

للحصول على بيئة آمنة، فإنّ على إدارة المنشأة أولًا فهم القوانين والأنظمة المتعلّقة بأمن المعلومات ثم البدء في تطبيقها من أعلى مستوى إداري في المنشأة إلى أقل مستوى تنفيذي فيها، ومن ذلك معرفة ما يجب حمايته، ومن يتعامل معه لضمان أنّ المنشأة تسير وفق برنامج عام يضمن الالتزام التام بقوانين أمن المعلومات وأخلاقياتها.

من المعروف أنّه كلّما كانت هناك إجراءات أكثر تفصيلًا ودقة كانت معرفة من يخالف؟ وأين؟ ومتى؟ تقع المخالفة أسهل. وكلما كانت القواعد مكتوبة رسميًا كان فرضها ومتابعتها أسهل. لذا يجب أن يشتمل برنامج أمن المعلومات على: السياسات الأمنيّة(Policies)، والمعايير القياسيّة(Standards)، والخطوط الأساسيّة(Baselines)، والمبادئ التوجيهيّة(Guidelines)، والإجراءات(Procedures)، وبرامج التدريب والتوعية(Awareness and Training) المنظِّمة لأمن المعلومات في المنشأة. فالسياسة الأمنيّة تشكل الأساس الذي يتم بناء برنامج أمن المعلومات عليه، بينما تشكل المعايير القياسية، والخطوط الأساسيّة، والمبادئ التوجيهية، والإجراءات إطار العمل لهذا البرنامج، ويجب تقديم هذه المفاهيم وطرحها بشكل واقعي، يميل إلى التعبير عن كل منها بما يحاكي الواقع، ويصف الأشياء كما هي. فتجد أنّ المنشآت المتقدّمة(الأكثر تنظيمًا) تتّبع مبادئ توجيهيّة منظمة وإجراءات مقنّنة، وفق خطوات محدّدة ومكتوبة، تضمن الإذعان لشروط أمن المعلومات، وفي الوقت نفسه تسهّل عمليّات السيطرة على الإجراءات ومتابعتها، بل وتسهم في تطويرها وتحديثها وفق ما يخدم مصلحة المنشأة، ويرفع مستوى الحماية لمعلوماتها.

عند تعيين موظف جديد بالمنشأة، أو ربط جهاز جديد بالشبكة، فيجب أن يخضع ذلك الموظف وذلك الجهاز لسياسة المنشأة العامة، ولسياسة أمن المعلومات بصفة خاصّة، من أجل أن يكون كلّ منهما إضافة لأمن المعلومات، وليس تهديدًا جديدًا لها. وهذا الإجراء بمنزلة إعداد خطة تفصيلية لما يجب أن يكون عليه مستوى أمن المعلومات عند هذا الموظف أو هذا

الجهاز. فيتم تحديد الإجراءات اللازم اتباعهـا، والشروط الواجب توافرها، وطرق تطبيق ذلك، ثم مراقبته والتدريب عليه.

في هذا الفصل نستعرض بشيء مـن التفصيل سياسات أمن المعلومات بأنواعها الثلاثة: العامة، والموضوعية (أو التخصصية)، والسياسة الأمنيّة للأنظمة، كركيزة أساسية وتوجيهات عامة وتفصيلية، للحفاظ على أمن المعلومات، وتحقيق أهداف المنشأة في ذلك. ثم ننتقل بعد ذلك إلى المعايير القياسية، سواءً أكانت معايير عامة تأتي من خارج المنشأة وتطبق داخلها، أم معايير داخليـة تنشأ وتطبّق داخل المنشأة. يلي ذلك موضوع يتـم الرجوع إليه كحدّ أدنى من الحماية المطلوبة، ويُقـارَن وضع أمن المعلومات في المنشأة به، وهو الخط الأساسي. يأتي بعد ذلك التوجيهات التي تُستخدم عند وجود حالات غموض في السياسات الأمنيّة أو المعايير أو الإجراءات، وهي توجيهات مستحسنة وليست إلزامية التنفيذ. يلي ذلك موضوع مهم يوفر التفاصيل التنفيذية للسياسات الأمنيّة والمعايير القياسية، وهو الإجراءات.

بنظرة عامة تكامليـة، خصّصنا موضوعًا مستقلًا لربط هذه المفاهيم مع بعضها بعضًا، وشرحنـا كيف يكمل كل منها الآخر. بعـد ذلك انتقلنا إلى موضوع مهـم آخر، وهو تصنيف المعلومات إلى مستويات تصنيف أمنية، تتناسب مع حجم المنشأة وطبيعة عملها؛ ليتم- بناءً عليه- التعامل مع كل صنف بما يناسبه، وتوفير الحماية المناسبة له. وأخيرًا لا يمكن أن يتم تطبيق جميع المفاهيم السابقة والتعامل معها بالشكل الصحيح، ما لم يكن هناك تدريب جيّد وبرامج توعويّة مستمرة، لشرح تلك المفاهيم وطرق التعامل معها وتطبيقها على أرض الواقع، وهو الموضوع الأخير في هذا الفصل.

٥-٢ السياسة الأمنيّة (Security Policy)

السياسة الأمنيّة هي الوثيقة الرسمية للمنشأة التي تصدرهـا الإدارة العليا للمنشأة (أو اللجنة المختصة بذلك)، والتي تنص على دور أمن المعلومات في المنشأة، ويمكن تعريفها بشكل أدق بأنها: «الطريقة أو الخطوات المكتوبة التي تحدّدها الإدارة العليا للمنشأة لتحديد كيفية أداء الأعمال ذات العلاقة بأمن المعلومـات وكيف تُعالج أيّ نشاط يخص المعلومة أو الأنظمة

والأشخاص المعالجين لها». وتُعدُّ السياسة الأمنيّة هي حجر الزاوية للتخطيط لأمن المعلومات، التي يمكن الانطلاق منها لتطبيق خطّة متكاملة لأمن المعلومات على أرض الواقع.

لا تقدّم السياسة الأمنيّة وصفًا لاستخدام جهاز أو نظام أو برنامج معيّن، بل تقدم طريقة محدّدة و واضحة يمكن اتباعها عند أداء الأعمـال ومعالجة أيّ حدث يخص أمن المعلومات عبر خطوات(إداريّة) تؤدي إمّا إلى حل المشكلة أو رفعها إلى مستوى إداري أعلى، ويجب أن لا تتعارض السياسة الأمنيّة مع القانون أو الأنظمة المعمول بها في المنشأة بأي حال من الأحوال.

تجدر الإشـارة إلى أنّ هناك جانبًا كبيرًا من أمن المعلومـات هو في حقيقته جانب إداري وإجرائي بالدرجة الأولى، يتمثل في السياسات الأمنيّة، حيث إن السياسات الأمنيّة هي إجراءات إداريّـة يجري تطبيقها على أرض الواقع من خلال الأنظمـة والبرامج المتاحة. فمثلًا، يمكن وضع سياسة أمنيّة تنص على أنّه في حال عدم إدخال كلمة المرور بشكل صحيح لثلاث مرات متتالية فسيتم تعطيل حساب ذلك المستخـدم ولا يفتح مرّة أخرى إلا من قبل مدير الشبكة. وهذا إجراء إداري يتم تطبيقه من خلال التحكّم بكلمـات المرور، وقد تختلف هذه السياسة من جهة إلى أخرى، فمثلًا قد تجد أن عدد المحاولات الخاطئة المسموح بها لكلمات المرور أقل أو أكثر من ثلاث مرات، حسب حساسية المعلومات التي سيتم الدخول عليها.

يمكن القول إنّ السياسات الأمنيّة هي بمنزلة قانون للمنشأة، يحدّد التعريفات والإجراءات المقبولة على المستويات الإداريّة كافّة من المديرين ومتخذي القرارات والمنفّذين، وعلى هذا، فإنّ السياسة الأمنيّة لا بدّ أن تكون واضحة ودقيقة، وتحدّد ما الشيء الصحيح؟ وما الشيء الخاطئ؟ وما الإجراء في حاله الصواب، والإجراء في حالة الخطأ؟

أهميّة السياسة الأمنيّة:

يمكن تلخيص أهميّة السياسة الأمنيّة في النقـاط الآتية، التي يمكن اعتبارها إجابة عن السؤال: لماذا يجب أن يكون هناك سياسة أمنية؟

- تحديد موارد المنشأة الرئيسة، التي تُعدُّ ذات قيمة كبيرة للمنشأة؛ لأنّ المقصود هو حمايتها.

- بموجب السياسة الأمنيّة يُخوَّل فريق أمن المعلومات بممارسة مهامه.
- تشكّل مرجعًا رئيسًا وموحدًا للرجوع إليه عند تعارض المهام الخاصة بأمن المعلومات مع بعضها بعضًا، أو مع غيرها، أو عند عدم قبولها أو عدم تطبيقها.
- تحدّد أهداف المنشأة المتعلّقة بأمن المعلومات.
- توضح مسؤوليات الموظفين وتحدّدها، فيما يخص معالجة المعلومات.
- تساعد في منع حدوث المفاجآت في الإجراءات أو الطلبات أو أحداث العمل اليومية.
- تحدّد نطاق عمل فريق أمن المعلومات ومهامه.
- توضّح مسؤوليات الاستجابة للأحداث التي تقع والتي تخص أمن المعلومات.
- توضّح استجابة المنشأة ومسؤوليتها تجاه القوانين والمعايير العامة والخاصة.

٥-٢-١ أنواع السياسات الأمنيّة

مما لا شك فيه فإنّه يجب أن يكون هناك سياسة أمنيّة عامة للمنشأة، تُعنى بعموميات أمن المعلومات، وتوثّق رؤية المنشأة وأهدافها، وآليات تحقيق تلك الأهداف، وبعد ذلك تأتي السياسات الموضوعية المتخصصة في موضوعات محدّدة أو أنظمة محدّدة؛ لتحدد وتوثّق كيفية التعامل مع تلك الموضوعات أو الأنظمة، فتكون هناك سياسة أمنيّة لصلاحيّات المستخدمين، وسياسة أمنيّة لاستخدام شبكة الإنترنت، وسياسة أمنيّة لاستخدام البريد الإلكتروني، ... وهكذا.

طبقًا لنشرات المعهد الوطني للقياسات الأمريكي(NISTSP)[١]، فإنّ هناك ثلاثة أنواع من السياسات الأمنيّة هي: السياسة الأمنيّة العامة(أو الهيكلية) (Enterprise or General Information Security Policy)، التي تتبع الأهداف والتوجهات العامة للمنشأة، والسياسة الموضوعية(Issue-Specific Security Policy)، التي تتبع لموضوع أو تخصّص محدّد، وسياسة الأنظمة(System-Specific Security Policy)، التي تتبع لنظام محدّد مطبّق في المنشأة. في كل الأحوال لا بدّ أن تكون السياسة شاملة لموضوعها الذي تتبعه، وأن تحقق أهداف المنشأة وتطلعاتها في تطبيق أمن المعلومات على أرض الواقع في مجالها، وفيما يلي نتطرق بشئ من التفصيل لكل نوع من هذه الأنواع.

١- Withman, M. and Mattord, H.(2005), "Principles of Information Security".

٥-٢-١-١ السياسة الأمنيّة العامة

السياسة الأمنيّة العامة هي السياسة التي تعتمد على رؤية المنشأة وأهدافها العامّة، وتحدد توجهاتها ونطاق الأعمال الخاصة بأمن المعلومات فيها. وتبدأ السياسة الأمنيّة العامة بتحديد برنامج أمن المعلومات وأهدافه، ثم تنتقل إلى منح الصلاحيّات وتحديد المسؤوليات اللازمة لتنفيذه، وتنتهي بوضع الآليات والطرق التي تضمن فرض البرنامج وتطبيقه على أرض الواقع.

يجب أن توضح السياسة الأمنيّة العامة القوانين ذات العلاقة، والقواعد التنظيمية والمسؤوليات القانونية (أو الالتزامات) وكيفية تطبيقها. ويجب أن تحتوي كذلك التوجهات والإستراتيجيات المستقبلية لأمن المعلومات، وأن تحدّد مستويات الأخطار التي يمكن قبولها.

إنّ للسياسة الأمنيّة العامة معايير ومميزات يجب فهمها وتطبيقها، وهي:

- أن يجري إنشاء السياسة الأمنيّة وتطبيقها وفق أهداف المنشأة العامة، بل يجب أن تكون أهداف المنشأة هي المحرّك لها وتحت مظلتها. وبعبارة أخرى: يجب أن لا تتعارض السياسة الأمنيّة مع أهداف المنشأة.
- يجب أن تكون سهلة الفهم واضحة المعاني ومرجعًا أساسًا لموظفي المنشأة وإداريها كافة.
- يجب أن تعدَّ بطريقة يتم فيها تضمين أمن المعلومات في جميع إجراءات المنشأة وأقسامها.
- يجب أن تعدَّ بالاستناد إلى القوانين والتشريعات والقواعد المطبّقة على المنشأة (من الحكومة أو الجهات التشريعية)، وأن تدعمها.
- يجب أن تُراجع وتُحدّث دوريًا، وعند إضافة أو حذف نشاط أو قسم من أقسام المنشأة، أو عند دمج المنشأة مع غيرها، أو عند تغيير مرجعيّتها أو ملكيّتها.
- أن يجري إصدار وتحديث السياسة الأمنيّة على شكل إصدارات أو طبعات مؤرخة، مثل: الطبعة الأولى، الطبعة الثانية، ... وهكذا.
- أن يكون لدى الوحدات والأشخاص المطبّقة عليهم السياسة الأمنيّة إمكانية الوصول إلى

الأجزاء التي يحتاجون إليها بسهولة، ولا يشترط عليهم قراءة باقي أجزاء السياسة.

- أن تكون قابلة للتطبيق لعدة سنوات، بحيث يمكن الاستفادة منها على المدى القريب والمتوسط، وأن تكون لديها القدرة على استيعاب المتغيرات خلال تلك الفترة.
- استخدام لغة سهلة ومحدّدة المعاني، والبعد عن استخدام الألفاظ التي تحتمل أكثر من معنى أو لا تكون محدّدة، مثـل "ربما" أو "من الأفضل" أو "يحسن"، وكذلك البعد عن الألفاظ التي لا تكون معروفة لغالبية الناس، حتى وإن كانت محدّدة.
- غالبًا ما تكون السياسة الأمنيّة العامة ثابتة قليلة تكرار التحديث.

٥-٢-١-١-١ خصائص وثيقة السياسة الأمنيّة العامة

يجب أن تكون السياسة الأمنيّة العامة مكتوبة على شكل وثيقة تفصيلية، وبهذه الطريقة يمكن أن يستفيد منها جميع موظفي المنشأة على جميع مستوياتهم الإداريّة، بدءًا من الطبقة القيادية في النواحي الإشرافيـة والتوجيهية، وانتهاءً بأحدث موظـف بالمنشأة في أداء عمله اليومي، واتصاله بالآخرين، ويجب أن تتصف هذه الوثيقة بالخصائص الآتية:

١. أن تكون منظّمة ومرتبة ومبوبة وفق مهام المنشأة الأساسيّة.

٢. أن تكون مكتوبة بلغة واضحة سهلة الفهم والتطبيق.

٣. أن تُحدّد فيها المسؤوليات والصلاحيّات بكل دقة. فمثلًا، يجب تحديد من لديهم صلاحية حرمان المستخدم من الدخول إلى الشبكة عند مخالفته للسياسة الأمنيّة، وتحديد الأشخاص المسؤولين عن إيقاف خدمة معيّنة إذا كانت تضرّ بشبكة المنشأة.

٤. تحديد الإجراءات التي يجب اتّباعها عند ظهور أيّ مشكلة بشكل تفصيلي، وعدم ترك الموظف في حيرة من أمره.

٥-٢-١-١-٢ محتوى وثيقة السياسة الأمنيّة العامة

يجب أن تحتوي وثيقة السياسة الأمنيّة العامة البنود الآتية (على الأقل):

١. الإجراءات اللازم اتّخاذها فيما يخص أمن المعلومات وموارد المنشأة لدى تعيين موظف جديد، أو عند إنهاء خدمات موظف حالي.

٢. تحديد صلاحيّات المستخدمين وتقسيمهم إلى مجموعات، وتحديد صلاحيّات كل مجموعة.

٣. وضع الشروط والقيود اللازمة لكلمات المرور لضمان أمن حسابات المستخدمين وحمايتها.

٤. تحديد متى يجب إيقاف حساب المستخدم، ومنعه من الدخول إلى شبكة، المنشأة أو تعطيل حسابه لمدّة محدودة، ومتى يجب إعادة تفعيله.

٥. تحديد المستخدمين أو المجموعات الذين يسمح لهم بتركيب أجهزة أو برامج إضافية على أجهزتهم.

٦. الإجراءات اللازم اتباعها والشروط اللازم استيفاؤها قبل توصيل أي جهاز جديد بشبكة المنشاة.

٧. إجراءات أمن المعلومات التي يجب تطبيقها على الشبكة بشكل عام، وعلى كل جهاز على حدة، كقفل منافذ الاتصال وتفعيل التحديث التلقائي لأنظمة التشغيل والبرامج وتحديد الأوقات المناسبة لذلك.

٨. الإجراءات اللازم اتباعها لحماية شبكة المنشأة من الفيروسات.

٩. شروط استخدام شبكة الإنترنت وقيودها وإجراءات الاتصال بها.

١٠. الإجراءات اللازم اتخاذها للحصول على بريد إلكتروني وشروط استخدامه وقيودها.

١١. آلية النسخ الاحتياطي وتحديد مسؤوليات وصلاحيّات عمل ذلك.

يمكن القول إنّه لا توجد سياسة أمنيّة تغطّي جوانب أمن المعلومات كافة في جميع إجراءات المنشأة. فلا بدّ من وضع طريقة مناسبة للتعديل أو الإضافة على السياسة الأمنيّة، وترك مجال لذلك وفق ضوابط وشروط محدّدة. ويجب مراعاة إمكانية مراجعة السياسة الأمنيّة، والتعديل فيها مع مرور الزمن أثناء التطبيق.

٥-٢-١-٢ السياسة الأمنيّة الموضوعيّة

السياسة الأمنيّة الموضوعيّة (أو التخصصية) هي سياسة أمنيّة متخّصصة في موضوع أو تخصص معيّن بشكل تفصيلي أكثر من السياسة الأمنيّـة العامة، وتُعدُّ مثل هذه السياسات عندما تظهر الحاجة للتركيز على تخصص أو إجراء أو قسم معيّن لأهميته، أو لكثرة التفاصيل فيه التي يجب أن يكون الموظفون على اطّلاع عليها وعلم بها.

وللسياسة الأمنيّة الموضوعية معايير ومميزات يجب فهمها وتطبيقها، وهي:

- أنّها تركز على تقنية محدّدة (كالبريد الإلكتروني مثلًا).
- تحتاج إلى التحديث بشكل مستمر وبتكرار أكثر من السياسة العامة.
- يجب أن تحتوي النصوص اللازمة لتحديـد موقف المنشأة من موضوعات محدّدة،

.قلشنلا لخاد تنرتنلإا قكبش مادختساب نيفظوملل حامسلا لثم

من الأمثلة على الموضوعات التي قد تكون لها سياسات أمنيّة تخصّصيّة مستقلّة ما يلي:

- استخدام البريد الإلكتروني.
- استخدام شبكة الإنترنت.
- إدارة المخاطر المعلوماتيّة (انظر الفصل الثامن).
- الحد الأدنى من الإعدادات اللازمة على أجهزة الحاسب الآلي لحمايتها من البرامج الضارّة، كالديدان والفيروسات.
- الاختبارات وأدوات الاختراق المستخدمة ضد شبكة المنشأة، من أجل اختبار كفاءة أنظمة الحماية.
- الاستخدام المنزلي للأجهزة والبرامج المملوكة للمنشأة.
- استخدام الأجهزة والبرامج الشخصيّة على شبكة المنشأة.
- استخدام أجهزة الاتصالات، مثل: الفاكسات والهواتف الثابتة والمتنقلة.
- استخدام أجهزة التصوير والطباعة.

من الأمثلة على السياسات الأمنيّـة الموضوعيّة: «السياسة الأمنيّـة للبريد الإلكتروني» و

«السياسة الأمنيّة لاستخدام شبكة الإنترنت» وفيما يلي نستعرض أبرز ما يجب أن تنصّ عليه هاتان السياستان.

٥-٢-١-٢-١ السياسة الأمنيّة لاستخدام البريد الإلكتروني

تحدّد هذه السياسة ما تستطيع وما لا تستطيع أن تفعله المنشأة تجاه رسائل البريد الإلكتروني لموظفيها لأغراض التدقيق والتحكم، وما الإجراءات المتاحة للموظفين، التي يسمح لهم أن ينجزوها عبر البريد الإلكتروني، وتحدّد كذلك معايير الخصوصيّة لكل من المنشأة والموظف، وفق ما يلي:

- تستطيع إدارة المنشأة أن تطّلع على رسالة الموظف المخزّنة على الخادم الرئيس للبريد الإلكتروني، ولا تستطيع أن تطلع على الرسائل المخزّنة على جهازه المكتبي.
- لا يستطيع الموظفون نشر المعلومات والمواد السِّريّة للمنشأة ومشاركتها مع الآخرين.
- يجب أن يطّلع الموظفون على السياسة الأمنيّة للبريد الإلكتروني، وأن يؤكدوا ذلك إمّا بالتوقيع على وثيقة تأكيد القراءة (تسمّى أحيانًا وثيقة القبول والاستخدام)، أو بالضغط على زر "موافق" أو "قبول" في مربع حوار تأكيد القراءة في حالة قراءة النسخة الإلكترونيّة للسياسة.

يجب أن تضم وثيقة السياسة الأمنيّة لاستخدام البريد الإلكتروني عددًا من التوجيهات التنظيميّة وفق صيغة "افعل" و "لا تفعل"، كما يلي:

افعل ما يلي:

١. التأكد من عنوان الموقع أو الصفحة المزوِّدة بخدمة البريد الإلكتروني.

٢. التأكد من أن رسائل البريد الإلكتروني الصادرة منك، تتضمّن عناوين الاتصال الخاصة بك.

٣. التأكد من صحّة عنوان البريد الإلكتروني للمرسل إليه، وكذلك عنوان من تريد أن تزوّدهم بصورة كربونية (Carbon Copy-CC)، أو صورة معماة (Blind Carbon Copy-BCC)، حيث إن الأخطاء في مثل ذلك قد تؤدي إلى عواقب وخيمة.

٤. التأكد من أن مرفقات البريد الإلكتروني هي نفسها ما قصدتها وليس غيرها. فالإهمال في ذلك قد يؤدي إلى إرسال معلومات مهمة وحساسة إلى جهات ليس لها الحق في الاطّلاع عليها.

٥. ضغط الملفّات والمجلّدات كبيرة الحجم قبل إرفاقها بالبريد الإلكتروني.

٦. تشفير المحتويات والمرفقات المهمة قبل إرسالها.(لاحظ أنه يفضل بشدة ضغط الملفّات قبل تشفيرها، حتى يمكن الاستفادة من عمليّة الضغط أقصى ما يمكن).

٧. التأكد من فحص جميع الرسائل الواردة إليك؛ لتنقيتها من البرامج الضارة.

٨. حذف الرسائل غير الضرورية، سواءً المرسلة أم المستقبلة، والرسائل غير موثوقة المصدر، خاصّة التي بها روابط دعائية.

٩. ترتيب الرسائل وحفظها في مجلدات حسب طبيعة عملك واحتياجك.

١٠. الإبلاغ عن أيّ خطأ ارتكبته أو بريد إلكتروني أرسلته بالخطأ، أو ورد إليك بالخطأ، أو استقبلته وفيه روابط غير موثوقة، أو فيه برامج ضارة.

لا تفعل ما يلي:

١. استخدام الروابط التي ترد مع البريد الإلكتروني غير المتأكد من صحتها.

٢. استخدام البريد الإلكتروني لأشخاص آخرين، وقراءة محتواه، أو إرسال الرسائل منه.

٣. إرسال رسائل بريد إلكتروني، أو مرفقات غير مصرّح بها، كالرسائل الدعائية، والنكت، وأخبار الأندية الرياضيّة.

٤. تفعيل التمرير الآلي للبريد الإلكتروني إلى خارج المنشأة، أو إلى الجهات غير المصرّح لها.

٥. فتح رسائل البريد الإلكتروني مجهولة المصدر والموضوعات.

٦. إرسال أو فتح الرسائل أو المرفقات غير اللائقة، أو التي بها محتويات غير مناسبة.

٥-٢-١-٢-٢ السياسة الأمنيّة لاستخدام شبكة الإنترنت

توفّر شبكة الإنترنت للعاملين في المنشأة لتسهيل القيام بأعمالهم والتواصل فيما بينهم، ومع الجهات الخارجيّة حسب حاجة العمل، وكذلك للحصول على المعلومات الضرورية من الشبكة، وتصفّح المواقع ذات العلاقة بعمل المنشأة من المواقع ذات الفائدة والمصداقية العالية.

لقد أدى الاستخدام الواسع والمتسارع لخدمات الإنترنت إلى تحسين الكفاءة والوصول بشكل أكبر وأسرع لمصادر المعلومات الضخمة المتوافرة على شبكة الإنترنت، إلا أنّ هناك بعض المخاطر المتأصّلة في استخدام الإنترنت قد تتسبّب في الإضرار البالغ بشبكة الحاسب الآلي الداخليّة وقواعد البيانات المهمة والحسّاسة للمنشأة، وقد تعرّضها للاختراق أو الفقد أو عدم التوافر. من أجل ذلك توضع السياسة الأمنيّة لاستخدام شبكة الإنترنت في صيغة «افعل» و «لا تفعل» لعدد من التوجيهات المنظمة لذلك كما يلي:

افعل ما يلي:

١. التأكّد من عنوان الموقع أو الصفحة المراد زيارتها على شبكة الإنترنت.

٢. التأكّد من موثوقيّة مصادر الروابط المستخدمة للدخول إلى المواقع.

٣. تخزين الروابط المهمة وكثيرة الاستخدام في قائمة المفضلة؛ للرجوع إليها وقت الحاجة، وكذلك لضمان صحتها عند استخدامها.

٤. المعرفة التامة بأنواع الملفّات التنفيذية التي تحمل أكوادًا ضارة، مثل "أكتف إكس" (ActiveX).

٥. الإبلاغ عن أي خطأ ارتكبته أو موقع زرته، واتضح أنه موقع ضار، أو أي برامج ضارة حمّلتها على أيّ جهاز من أجهزة المنشأة.

لا تفعل ما يلي:

١. استخدام روابط غير متأكد من صحتها، أو التي تكون من مواقع غير موثوقة.

٢. استخدام النوافذ المنبثقة غير الموثوقة.

٣. تخطي رقابة الشبكة للدخول إلى مواقع محجوبة.

٤. قضاء أوقات طويلة في تصفح مواقع ليس لها علاقة بعمل المنشأة.

٥. ترك الوصول إلى الإنترنت مفتوحًا طوال اليوم لأغراض ليس لها علاقة بعمل المنشأة.

٦. تنزيل الصور والفيديو والصوتيات التي ليس لها علاقة بعمل المنشأة.

٧. تنزيل المواد والبرامج بطريقة تنتهك حقوق ملكية الآخرين.

٨. تنزيل البرامج وتشغيلها أو تثبيتها على الأجهزة دون إذن مسبق.

٩. تنزيل أو تثبيت البرامج الضارة وبرامج الاختراق والتجسّس بأيّ شكل من الأشكال.

١٠. القيام بأيّ نشاط تخريبي أو تجسّسي أو وصول غير مشروع من خلال أجهزة المنشأة وشبكتها.

٥-٢-١-٣ السياسة الأمنيّة للأنظمة

هي السياسة الأمنيّة الخاصة بتنظيم قرارات إدارة المنشأة وتنفيذها المتعلِّقة بأنظمة تقنية المعلومات المستخدمة، كالحاسبات الآلية، والشبكات، والبرامج التطبيقيّة، والبيانات، ومن ثم فإنّ من أهم مهام هذه السياسة أن توضح ما يلي:

- القائمة المعتمدة بالبرامج التطبيقيّة لدى المنشأة، والمسموح بتركيبها واستخدامها على أجهزة المنشأة.
- كيفيّة حماية قواعد البيانات واستخدامها.
- شروط استخدام الأجهزة الطرفيّة، كالحاسبات الآلية، والطابعات، والماسحات الضوئيّة، ومتى تُفصل عن الشبكة؟ ومتى تُقفل نهائيًّا؟

من الأمثلة على السياسات الأمنيّة للأنظمة "السياسة الأمنيّة لكلمات المرور"، سواءً أكانت كلمة المرور مستخدمة للدخول إلى الشبكة أو أنظمة التشغيل أو البرامج التطبيقيّة المختلفة، وفيما يلي نستعرض أبرز ما يجب أن تنص عليه هذه السياسة.

٥-٢-١-٣-١ السياسة الأمنيّة لكلمات المرور

من أقدم الأدوات المستخدمة لحماية المعلومات هي استخدام كلمات المرور (كلمات السر)، للدخول إلى الأنظمــة أو المعلومات. وبذلك فإنّ جانبًا مهمًّا من حماية المعلومات يقع بالكامل في أيدي المستخدمين.

إنّ عدم استخدام كلمات مــرور جيّدة (صعبة)، أو الإهمال في المحافظة عليها من جانب المستخدمين، يعرّض أمن المعلومات للخطر، ومن الأمثلة على ذلك استخدام كلمات مرور سهلة مثل «١٢٣»، أو عدم تغيــير كلمات المرور مدّة طويلة، ولتغطية جوانــب القصور في استخدام كلمات المرور، ظهرت الحاجة إلى إيجاد سياسة أمنيّة تحكم كلمات المرور، وتضمن رفع المستوى الأمني لها، وتتلخّص أهم بنود السياسة الأمنيّة لكلمات المرور فيما يلي:

افعل ما يلي:

١. استخدم كلمات مرور تكون خليطًا من الأحرف (أ – ي) والأرقام (صفر – ٩) والرموز (٪ ، @ ، & ...إلخ) .

٢. غيّر كلمة المرور الخاصة دوريًّا، ويمكن وضع تاريخ صلاحيّة محدّد لكلمات المرور من قبل مدير الشبكة أو النظام، بحيث تكون غير صالحة للاستخدام بعد ذلك التاريخ، ويفضل أن يجري تغيير كلمات المرور كل ثلاثين يومًا، بغض النظر عن أيّ تغييرات أخرى لفترات أقصر من ذلك.

٣. استخدام حدّ أدنى من طول كلمات المرور، وينصح بشدة أن لا يقل عن عشر خانات، مكوّنة من: أرقام وحروف ورموز.

٤. غيّر كلمة المرور المقدّمة إليك عند فتح حساب جديد، أو إعطائك صلاحيّة الدخول إلى نظام خاص بالمنشأة لأول مرة.

٥. وضع حدّ معيّن لعمر كلمة المرور، بحيث يجب استخدام كلمة المرور طوال مدّة (عمر) معيّنة، ولا يسمح للمستخدم بتغييرها قبل اكتمال تلك المدّة، والسبب في ذلك أنّه وجِدَ أنّ هناك كلمات مرور مفضّلة عند المستخدمين. فتجد أنّ كلّ مستخدم يفضّل استخدام كلمة مرور معيّنة يحاول دائمًا الوصول إليها ومحاولة تخطي البند الذي

يجبره على عدم استخدام آخر خمس كلمات مرور(البند رقم ٥ في الجزء "لا تفعل"). فتجده يستخدم كلّ كلمة مرور لمدّة بسيطة جدًا، من أجل إكمال دورة استخدام خمس كلمات مرور؛ ليعود إلى كلمة المرور المفضلة لديه، ويجب أن لا يقل عمر كلمة المرور عن يوم كامل.

٦. استخدام كلمات مرور عشوائيّة للأنظمة عالية الحساسية. وفي هذه الحالة يجب إنتاج كلمة مرور مختلفة في كل مرة، بحيث لا يستطيع أحد التنبؤ بها قبل استخدامها، بما في ذلك مستخدم كلمة المرور نفسه. وقد يتبادر إلى الذهن السؤال التالي: كيف يتعرف النظام إلى كلمات مرور عشوائيّة؟ وكيف يحصل المستخدم على هذه النوعية من كلمات المرور؟ الجواب هو أن هناك طرقًا مختلفة لتحقيق ذلك، ومن أشهرها أن يستخدم وصلة ذاكرة "توكن"(Token) تنتج أرقامًا عشوائيّة، ويقابلها برنامج مماثل لها، يركّب على النظام المراد الدخول إليه، ينتج الأرقام العشوائية نفسها.

٧. تعطيل(أو إلغاء) كلمة المرور بعد ثلاث محاولات خاطئة. وعادة ما يتحكّم مدير النظام في ذلك، ولكن إذا حصل أن استطعت أن تستخدم كلمة المرور بعد ثلاث محاولات خاطئة، فأبلغ مدير النظام وغيّر كلمة المرور الخاصة بك فورًا.

لا تفعل ما يلي:

١. استخدام كلمات مرور مكوّنة من كلمات موجودة في المعجم؛ بمعنى يجب أن لا تكون كلمات عاديّة يمكن لطُرق الاختراق المعتمِدة على المعاجم أن تكسرها.

٢. استخدام اسم المستخدم أو أيّ جزء منه، أو أيّ جزء من الاسم العادي للمستخدم، ككلمات مرور.

٣. كتابة كلمات المرور على ورق أو ملصقات من أجل تذكرها.

٤. استخدام كلمات المرور التلقائية(Default) ككلمات مرور أساسية. ويتأكد ذلك لحسابات المديرين(Admin)،(Administrator)، وذوي الصلاحيّات العالية مثل: صلاحية تركيب البرامج(Setup)، وصلاحية النسخ الاحتياطي(Backup).

٥. استخدام أيّ كلمة مرور من آخر خمس كلمات مرور استخدمت في الماضي.

٦. إطلاع غيرك على كلمة المرور الخاصة بك، حتى ولو كان مدير النظام.

٧. استخدام كلمة المرور نفسها في عدّة حسابات وأنظمة. (مثال ذلك: استخدام كلمة المرور نفسها للبريد الإلكتروني (العام)، وللدخول إلى شبكة الحاسب الآلي المحلية للمنشأة).

٨. تخزين كلمة المرور على الحاسب الآلي.

٥-٣ المعايير القياسيّة (Standards)

المعايير القياسيّة، أو اختصارًا «المعايير»، هي الأنشطة والأعمال واللوائح الإلزامية التي يجب التقيد بها في جميع أنشطة المنشأة. والمعايير هي التي تدعم السياسات الأمنيّة بكافة أنواعها وتجعلها تأخذ صفة القطعية وصفة إلزامية التنفيذ. وقد تكون هذه المعايير داخلية المنشأ والتطبيق، أي تنشأ من المنشأة نفسها، وتطبق داخلها، وقد تكون خارجية المنشأ (مثل المعايير الحكومية) داخلية التطبيق.

تحدد معايير المنشأة كيفية استخدام منتجات تقنية المعلومات من الأجهزة والبرامج، وكيفية تطبيق هذه التقنيات في المنشأة بطريقة متجانسة غير متغيرة. ومن الأمثلة على المعايير القياسية التي يمكن تطبيقها داخل المنشأة ما يلي[١]:

- إلزام الموظفين بإبراز بطاقات التعريف (الهويات) الخاصة بهم؛ ليسهل التعرف عليهم وقراءتها سواءً قراءة عادية أم إلكترونيّة.
- إلزام الموظفين بتشفير البيانات السِّريّة داخل المنشأة، وأيّ بيانات تُخزّن على الأجهزة المحمولة.
- إلزام الموظّفين باستخدام الخصائص الحيوية (مثل، بصمة الأصابع، وبصمة العين، ... إلخ)؛ للتحقق من هوياتهم عند الدخول للأنظمة عالية الحساسية، وحسبما يتطلبه وضع المنشأة.

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

- إلزام الموظفين بتحديث معلوماتهم وعناوينهم دوريًا.

٥-٤ الخط الأساسي(Baseline)

هو المستوى الأدنى أو الحد الأدنى من الحماية المطلوبة. فعند إجراء أيّ تغيير في المنشأة، أو في أيّ نشاط من أنشطتها، أو إذا تعرّضت المنشأة لوقوع خطر من الأخطار، فإنّه يجب المحافظة على حدّ أدنى من الحماية يسمّى الخط الأساسي، ويُعدُّ مرجعًا يتم الرجوع إليه لقياس مدى القرب أو البعد منه قبل وقوع الخطر وبعده، و من ثَمَّ معرفة ما يمكن القيام به لتجاوز هذا الخطر، والبقاء دائمًا فوق الخط الأساسي.

من الأمثلة على التغييرات التي قد تحدث، ويجب عندها مراجعة الخط الأساسي، هي تركيب أنظمة تشغيل جديدة وتفعيلها أو برامج تطبيقيّة جديدة أو تحديثات جديدة، قد يترتب عليها النزول دون الحد الأدنى من الحماية.

إذا لم يطبّق مفهوم الخط الأساسي في المنشأة، أو لم يراجع المختصّون هذا الخط بعد إجراء أيّ تعديل، فقد ينتج عن ذلك ثغرات أمنيّة يمكن النفاذ من خلالها.

٥-٥ التوجيهات(Guidelines)

هي مجموعة الأعمال المستحسنة والتوجيهات التشغيليّة الموجّهة للمستخدمين، والمشغّلين، والمختصين في تقنية المعلومات، وتشمل طُرُق الاستخدام للتقنيات المتاحة في المنشأة التي تساعد المستخدمين على التعامل مع تلك التقنيات بشكل جيّد.

وكما مرّ معنا فإنّ «المعايير» هي قواعد محدّدة يجب الالتزام بها، بينما «التوجيهات» هي إرشادات عامّة غير إلزاميّة يرجع لها المستخدمون في الظروف غير الواضحة، التي تحتاج إلى مرونة(وليس إلى صفة القطعيّة) في التشغيل أو التطبيق. وعادة يتم الرجوع للتوجيهات في حالة وجود غموض في السياسات الأمنيّة أو المعايير أو الإجراءات، للحصول على معلومات أكثر تفصيلًا. فمثلًا قد تنصّ السياسة الأمنيّة على أن تجري مراقبة البيانات السِّريّة وتدقيقها، وتأتي التوجيهات لتوضح المعلومات التفصيلية التي يجب مراقبتها وتوثيقها، وتحدّد المرونة الممكنة في ذلك.

٥-٦ الإجراءات(Procedures)

هي الخطوات التفصيليّة(خطوة بخطوة) المطلوب القيـام بها لتحقيق هدف معيّن، وقد يقوم بهذه الخطوات المستخدمون، أو المختصون بتقنيـة المعلومات، أو المشغّلون، أو غيرهم، حسب طبيعة الهدف المراد تحقيقه، ومن الأمثلة على الإجراءات ما يلي[١]:

- الخطوات التفصيليّة لتنصيب نظام التشغيل.
- الخطوات التفصيليّة لتغيير إعدادات أنظمة الحماية وآلياتها.
- الخطوات التفصيليّة لتطبيق قوائم التحكّم بالوصول(Access Control Lists).
- الخطوات التفصيليّة لتعريف مستخدمين جدد إلى الشبكة.
- الخطوات التفصيليّة لمنح الصلاحيّات على الأجهزة.

تأتي الإجراءات بعد تحديـد السياسات الأمنيّة وتطبيقها، وهـي أقرب إلى المستخدمين والأجهزة من السياسة الأمنيّة؛ لأنّها توفر الخطوات التفصيليّة للتركيب والإعداد والتهيئة.

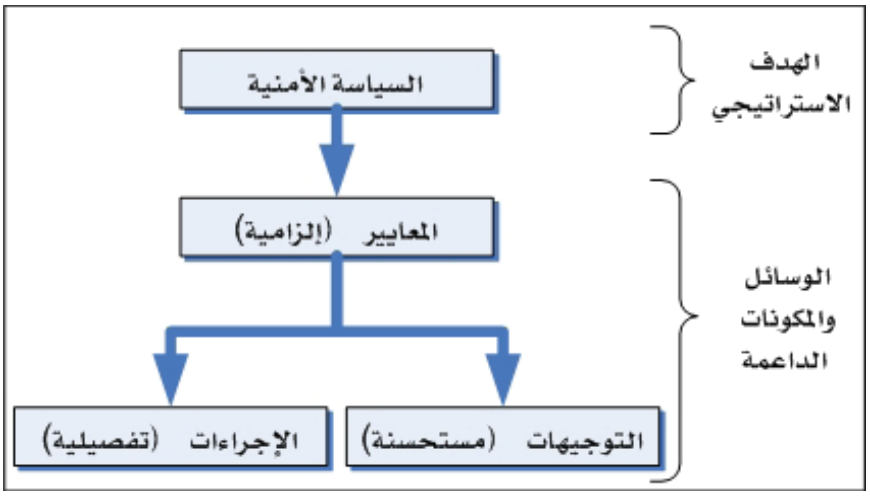
تحـدد الإجراءات كذلك كيفيـة تطبيق كل من السياسـات الأمنيّة، والمعايـير القياسية، والتوجيهات على أرض الواقع، وكيفية نقلها من الطرح النظري إلى إجراءات واقعية تُنفّذ في بيئة تشغيلية حقيقية. فعلى سبيل المثال، لو نصّت السياسـة الأمنيّة على وجوب التحقّق من هويّة من لهم حق الوصول إلى المعلومات السِّريّة، فإنّ الإجراءات ستوضح الخطوات التفصيلية لتطبيق ذلك، وكيفية تطبيق معايير التحقّق من الهُويّة، ثم كيفيّة مراقبة وتدقيق هذه العمليّة، ولو نصّت المعايير القياسيّة على ضرورة أخذ نسخة احتياطية من البيانات، فإنّ الإجراءات ستوضح الخطوات التفصيليّة لأخذ النسخ الاحتياطيّة مشتملة على أوقات أخذ هذه النسخ على شكل جدول زمني(يومي، وأسبوعي، وشهري، وسنوي)، ونوع وسائط التخزين التي ستخزن عليها تلك النسخ، وأماكن حفظها.

٥-٧ نظرة تكاملية

بنظـرة عامة فـإنّ «السياسـة الأمنيّـة» هي بمنزلـة هـدف استراتيجي للمنشـأة يجب

١- Bidgoli, Hossein(2006a), "Handbook of Information Security", Volume 1.

تحقيقه، وإن «المعايير القياسية» و «التوجيهات» و «الإجراءات» هي بمنزلة الوسائل والمكوّنات الداعمة (التكتيكية) لتحقيق ذلك الهدف، انظر الشكل (٥-١).



الشكل (٥-١): السياسة الأمنيّة تشكل الهدف الاستراتيجي والمعايير القياسية والتوجيهات والإجراءات هي المكوّنات الداعمة والتكتيكية

فبعد أن تعرّفنا ماهيّة كل من «السياسات الأمنيّة» و «المعايير القياسية» و«الخطوط الأساسيّة» و «التوجيهات» و «الإجراءات» بشكل منفرد، فإنّ من المستحسن أن ننظر إليها بشكل مترابط، يكمّل بعضها بعضًا من خلال المثال الآتي: تنصّ السياسة الأمنيّة (أيًّا كان نوعها) على «حماية المعلومات السِّريّة بشكل جيّد». وهذه عبارة عامة واسعة النطاق يمكن تحقيقها بأشكال كثيرة مختلفة. لتأتي بعد ذلك «المعايير القياسية»؛ لتنصّ على الالتزام بتشفير معلومات عملاء المنشأة المخزّنة في قواعد البيانات، باستخدام خوارزميّة التّشفير القياسي المتقدم (AES)، وأن لا تنقل هذه البيانات على شبكة الإنترنت إلا بعد تشفيرها باستخدام تقنية (Internet Protocol Security-IPSec) وبذلك حددت المعايير القياسيّة نوع الحماية المطلوبة ونوع التقنية المستخدمة، وقدّمت تفصيلًا وإيضاحًا أكثر من السياسة الأمنيّة، وتأتي بعد ذلك "الإجراءات"، لتشرح كيف تطبّق تقنية خوارزميّة التّشفير القياسي المتقدّم (AES)، وتقنية (IPSec) وأخيرًا توفر "التوجيهات" الإرشادات اللازمة لمعالجة

البيانات المعطوبة أثناء عمليّة التّشفير وبعدها، وأثناء إرسالها عبر شبكة الإنترنت.

أخيرًا، فإنّ من المفترض أن لا تُجمع "المعايير" و "التوجيهات" و "الخطوط الأساسيّة" في وثيقة واحدة قد تكون كبيرة الحجم ويصعب التعامل معها، بل يجب أن تكون كل واحدة منها منفصلة في وثيقة مستقلة، فلكلّ منها مهامها وأهدافها وطريقة خاصّة بعرضها والتعامل معها، والسبب الرئيس في ضرورة فصل كل منها عن الآخر هو اختلاف مرجعيّة كل منها. فالوثيقة التي تصف كيفية تطبيق "معايير" معيّنة وعدم مخالفتها يجب أن توجه إلى إدارة المنشأة، بينما الوثيقة التي تصف الخطوات التفصيلية لكيفية حماية نظام التشغيل يجب أن توجه للمختصين في تقنية المعلومات، وعليه، فإنّ فصل كل وثيقة وحدها يساعد على التوزيع المناسب لتلك الوثائق، ويسهّل توجيهها إلى الجهات المختصة مباشرة.

٨-٥ تصنيف المعلومات

من الأهمية بمكان التعرّف إلى المعلومات الحرجة والمهمة بالنسبة للمنشأة، ثم تحديد القيمة المناسبة لها من أجل حمايتها، والسبب وراء تحديد قيم هذه المعلومات هو من أجل تخصيص الميزانيات المناسبة لحمايتها، وترتيب أولويات تطبيق أنظمة الحماية لها، وتحديد درجة قوة الحماية المطلوبة، ومن هنا ظهرت أهميّة تصنيف المعلومات.

يكمن الهدف الرئيس لتصنيف المعلومات في تنظيم هذه المعلومات وترتيبها، وفقًا لدرجة حساسيتها لكل من: إمكانية فقدها، وإمكانية الكشف عنها، وإمكانية عدم توفرها، ومن ثم يمكن تحديد المستوى المطلوب من كل عنصر من عناصر أمن المعلومات، وبالدرجة الأولى المستوى المطلوب من: السِّريّة، وسلامة المعلومة وتكاملها، والتوفر أو الديمومة، وبناءً على ذلك تستطيع المنشأة أن تقرر توجيه أنظمة الحماية المناسبة لكل نوع من أنواع المعلومات وفقًا للتصنيف المعتمد.

لا يقوم تصنيف المعلومات بتصنيف المعلومات فحسب، بل يحدّد الطرق والآليات التي يتم التعامل بها مع كل صنف، ومن تلك الطرق والآليات: آلية الوصول إلى المعلومات من الصنف نفسه ، وكيفيّة استخدامها، ثم أخيرًا التخلّص منها أو إتلافها. فلكل صنف آلية وصول وطريقة للاستخدام وطريقة للإتلاف خاصّة به.

لتوضيح ذلك سنأخذ المثال الآتي: لو صُنّفت معلومات منشأة من المنشآت إلى ثلاثة أصناف: سريّة، وحسّاسة، وعاديّة؛ فسيكون التعامل مع كل صنف وفق الآتي:

- عند التعامل مع المعلومات السِّريّة يجب أن يتم الوصول إليها من قبل الإدارة العليا فقط، أو من قبل أشخاص محدودين، ويمكن السيطرة على ذلك بأن لا يمكن الوصول إلى المعلومة إلا بعد إدخال كلمتي مرور مختلفتين من قبل شخصين مختلفين، ويجب أن تُجرى على هذه المعلومات من هذا الصنف عمليّات تدقيق ومراقبة تفصيليّة تسجل من خلالها جميع الإجراءات التي تتم عليها، ومن قام بها؟ وأوقات وتواريخ تلك الإجراءات، (مثل: الاطّلاع، والطباعة، والبحث، والحذف، والإرسال)، وأن تُراجَع نتائج هذه المراقبة والتدقيق بشكل يومي، ويمكن حفظ الأوراق التي تطبع من هذا الصنف من المعلومات في خزانات فولاذية مقفلة، وعند الرغبة في التخلص من هذه المعلومات أو حذفها يجب استخدام تقنية مسح، مثل تقنية التصفير (Zeroization)، (وهو يجعل جميع قيم المعلومة صفرًا بالتمثيل الثنائي)، لضمان مسح البيانات بشكل تام، يضمن عدم إمكانية استعادتها بعد الحذف.
- عند التعامل مع المعلومات الحسّاسة، فإنّه يمكن الوصول إليها من قبل مجموعة من الأشخاص أكبر عددًا من المعلومات السِّريّة، ويمكن الوصول إليها بعد إدخال كلمة مرور واحدة فقط، ويجب أن تُجرى على هذا الصنف عمليّات تدقيق ومراقبة مثل المعلومات السِّريّة، لكن يمكن أن لا تجري مراجعتها بشكل يومي، ويمكن أن يُكتفى بمراجعتها أسبوعيًّا. ويمكن حفظ الأوراق التي تطبع من هذا الصنف في أدراج عادية مقفلة، وعند الرغبة في التخلّص من هذه المعلومات أو حذفها يمكن استخدام تقنيات الحذف العاديّة (Deletion).
- يمكن التعامل مع المعلومات العاديّة كمعلومات عامّة يمكن أن يصل إليها أيّ أحد، ولا تجري مراجعتها ولا تدقيقها، ويمكن حفظ الأوراق المطبوعة منها في أدراج عاديّة، كما يمكن حذفها بأيّ طريقة، ومن قبل أيّ أحد.

لإتمام عمليّة تصنيف المعلومات بشكل جيّد، يجب أوّلًا تحديد واختيار مستويات التصنيف وعددها، ثم بعد ذلك توزيع المعلومات على تلك المستويات. فقد تكتفي منشأة بمستويَين من التصنيف، بينما تحتاج أخرى إلى أربعة مستويات أو أكثر. يوضح الجدول(٥-١) مستويات التصنيف المعروفة والمشهورة التي يمكن الاختيار من بينها، وعددها ثمانية مستويات[١].

من المهم أن يحتوي سلّم التصنيف العدد المناسب من المستويات، بما يلائم المنشأة، ويراعي طبيعة عملها، وأهمية معلوماتها، وهل هي حكومية أم خاصّة؟ فيجب ألا يكون عدد المستويات كبيرًا يصعب التعامل معه، ولا صغيرًا يسبّب اللّبس والخلط في توزيع المعلومات على مستويات التصنيف، ويجعلها تتداخل فيما بينها. يجب كذلك مراعاة أن يكون كل مستوى فريدًا ومفصولًا عن المستويات الأخرى.

فمثلًا قد يكون من المناسب لجهة حكومية تتعامل مع أنواع متعدّدة من المعلومات تختلف في درجة سريّتها وحساسيتها أن تختار مستويات التصنيف الآتية، مرتّبة حسب درجة السِّريّة والحساسية، من الأعلى إلى الأسفل، كما يلي:

- معلومات غاية في السِّريّة.
- معلومات سريّة.
- معلومات محظورة النشر.
- معلومات حسّاسة لكن غير مصنّفة.
- معلومات غير مصنّفة.

وقد تختار مؤسسة تجاريّة مستويات التصنيف الآتية مرتبة حسب درجة سرّيّتها وحساسيتها من الأعلى إلى الأسفل، كما يلي:

- معلومات محظورة النشر.
- معلومات خاصّة.
- معلومات حساسة.
- معلومات عامّة

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

المستوى	خصائصه	أمثله عليه
عامة	• لا يحبذ نشر المعلومات ولكن في حالة النشر يجب أن لا يضر بالمنشأة أو الأشخاص.	• عدد العاملين في مشروع معيّن. • المشروعات المستقبلية.
حساسة	• يتطلب نظام حماية لسرية المعلومة وتكاملها وسلامتها من التغيير أو الحذف غير المصرّح به. • يتطلب مستوى أعلى من العادي من الدقة والشمول.	• المعلومات المالية. • معلومات تفاصيل المشاريع. • معلومات الأرباح والفوائد والتنبؤات المستقبلية.
خاصّة	• المعلومات الشخصية المستخدمة داخل المنشأة. • الكشف عن المعلومات التي تضر بالموظفين أو المنشأة.	• تاريخ العمل. • معلومات العاملين. • المعلومات الطبية.
محظور النشر	• للاستخدام داخل المنشأة فقط. • البيانات المعفاة من عدم الكشف بسبب حرية المعلومات أو القوانين التي تسمح بذلك. • الكشف غير المصرّح به من هذا المستوى قد يضرّ بالمنشأة بدرجة كبيرة جدًا.	• الأسرار التجارية أو المتعلّقة بعمل المنشأة الأساسي. • معلومات العناية الطبية. • أكواد البرامج الأصليّة(Source Codes). • المعلومات التي تحافظ على مستوى التنافس.
غير مصنفة	• البيانات غير الحساسة أو التي لا تتبع لأيّ مستوى.	• دليل استخدام الحاسب الآلي العادي ومعلومات الضمان المجانية. • المعلومات التطوعية.
حسّاسة لكن غير مصنفة	• سرية قليلة جدًا. • لو تم الكشف عنها قد تسبّب عطلًا أو خرابًا.	• المعلومات الطبية. • إجابة أسئلة الاختبار والتقييم.
سرية	• لو تم الكشف عنها، فقد تسبب ضررا كبيرًا يمتد لشريحة كبيرة قد تصل إلى مستوى البلد كاملًا.	• خطط العمل وتوزيع المهام السِّريّة. • الترتيب لمهمة سرية مثل إنتاج منتج سري.
سري للغاية	• لو تم الكشف عنها، فقد تتسبب في انهيار المنشأة أو اختفائها بالكلية.	• أسرار سلاح حديث في حالة الحرب. • التجسّس على معلومات الأقمار الصناعيّة. • المعلومات التجسّسية.

الجدول(٥-١): مستويات تصنيف المعلومات الثمانية

بعد تحديد مستويـات التصنيف، يتم الانتقال إلى المرحلة الثانيـة، وهي توزيع معلومات المنشأة على المستويات التي تم تحديدها، وفيما يلي نسرد بعض المعايير التي يمكن استخدامها في توزيع المعلومات على مستويات التصنيف، التي تساعد على تحديد درجة حساسيّة المعلومة وأهميتها للمنشأة، وهي:

- الفائدة من المعلومة.
- قيمة المعلومة (قد تكون تلك القيمة ماديّة أو معنوية).
- عمر المعلومة، فقد تفقد المعلومة حساسيتها وأهميتها مع مرور الوقت.
- مستوى الضرر الذي ينتج عند الكشف عن المعلومة.
- مستوى الضرر الذي ينتج عند تغيير المعلومات أو تلفها.
- المسؤولية القانونيّة على المنشأة تجاه حماية المعلومة.
- التأثير الذي تملكه المعلومة (أو ينتج عنها) على وجود المنشأة أو بقاء أو انهيارها.
- من الشخص (أو الأشخاص) الذي لديه صلاحية الوصول إلى المعلومة؟
- من الشخص (أو الأشخاص) الذي لديه إمكانية التعامل مع المعلومة؟
- من الشخص (أو الأشخاص) الذي لديه إمكانية إعادة إصدار (أو إنتاج) المعلومة؟
- أين يجب أن تحفظ المعلومة؟
- ما المعلومات التي تحتاج إلى ترقيم أو وضع علامات إرشادية عليها؟
- هل يلزم تشفير المعلومة أم لا؟
- هل يلزم فصل المهام المتعلِّقة بالمعلومة عن بعضها بعضًا أم لا؟
- الخسائر المتوقّعة في حال عدم توافر المعلومة أو تلفها.

يجب ألا يقتصر التصنيف على تصنيف المعلومات فقط، بل يجب أن يشمل كذلك البرامج والأنظمة التي تتعامل مع المعلومات المصنفة، فيجب تصنيف البرامج التطبيقيّة وفقًا لدرجة تصنيف المعلومات التي تتعامل معها، وكذلك الحال للأنظمة التي تعالج المعلومات أو تخزّنها أو تنقلها، إذ يجب أن تُصنّف بما يحقق درجة السِّريّة المناسبة لتلك الأنظمة وللمعلومات التي

تعالجها أو تخزّنها أو تنقلها. ويجب أن تشمل قواعد التصنيف المطبقة كذلك جميع أشكال المعلومات، سواءً أكانت رقميّة أم ورقية أم فيديو أم فاكس أم معلومات صوتية أم غير ذلك.

٥-٩ التدريب والتوعية بأمن المعلومات

تحتوي السياسات الأمنيّة والمعايير القياسية والإجراءات والتوجيهات الأوامر والتعليمات من إدارة المنشأة حول تطبيق أمن المعلومات في المنشأة والآليات المنظّمة لذلك. لكن كيف يمكن تحقيق توجهات إدارة المنشأة إذا كان العاملون في المنشأة لا يعرفون تلك السياسات والمعايير والإجراءات والتوجيهات، ولا يستطيعون تنفيذها، ولا التعامل معها. من هنا كان التدريب على أمن المعلومات والتوعية به ضرورة مُلحّة لإكمال منظومة أمن المعلومات.

الهدف الرئيس من التدريب والتوعية بأمن المعلومات هو إيصال مفهوم أمن المعلومات والسياسات الأمنيّة العامة لكل موظف في المنشأة، ثم بعد ذلك التأكد من أن كل من السياسات الأمنيّة الموضوعية أو المختصة بأنظمة محدّدة والمعايير القياسيّة والإجراءات والتوجيهات قد وصلت بالصورة الصحيحة لكلّ شخص يتطلب عمله فهمها وتطبيقها والتعامل معها، وأنّها وصلت كذلك إلى كلّ قسم أو نشاط في المنشأة يجب أن تحكمه وتحدّد مساره. وبهذه الطريقة يمكن معرفة من يحتاج إلى التدريب أو التوعية وفي أيّ مجال، ويمكن كذلك معرفة النتائج والمسؤوليّات المترتّبة على عدم تطبيق ما تم التدريب عليه والعلم به.

يشتمل كل من التدريب والتوعية بأمن المعلومات، سواءً أكان يتم التعامل معهما كوحدة واحدة أم منفصلين عن بعضهما بعضًا، على ثلاثة مستويات:

- المستوى الأعلى: وهو مستوى عام شامل يحتوي مواد تدريبية وتوعويّة، قصيرة المدّة، عامّة المفاهيم؛ لمعرفة الخطوط العريضة لكلّ من السياسات الأمنيّة والمعايير القياسية والتوجيهات والإجراءات، دون الدخول في التفاصيل، ويستهدف المستويات العليا من إدارة المنشأة.
- المستوى المتوسط: متوسّط الشمولية، ويحتوي مواد تدريبية وتوعوية متوسطة المدّة ومتوسّطة التفاصيل، ويستهدف: المهندسين والاستشاريين ورؤساء الأقسام.

- المستوى الأدنى: وهو مستوى تفصيلي يحتوي مواد تدريبيّة وتوعويّة طويلة المدة، تحتوي معلومات تفصيليّة عن كيفيّة تطبيق السياسات الأمنيّة والمعايير القياسيّة والتوجيهات والإجراءات خطوة بخطوة على أرض الواقع، ويستهدف الأفراد والجهات التنفيذية من: فنيين ومستخدمين ومستفيدين.
- يجب أن يكون كلٌّ من التدريب والتوعية بأمن المعلومات مستمرين طوال العام، وبصفة دوريّة، وأن يتمّا على كل مستوى من المستويات الثلاثة لمرّة واحدة على الأقل في كلّ سنة. يوضح الجدول(٥-٢) سمات كل من التدريب والتوعية بأمن المعلومات والطُّرق المستخدمة لتنفيذ كل منهما.

السمة	التوعية	التدريب
يجيب عن السؤال	ماذا؟	كيف؟
العمق	معلومات فقط	يوفر المعرفة اللازمة
الهدف التعليمي	التعرّف إلى المفاهيم وطرق استبقائها واستحضارها	صقل المهارات
أمثلة لطرق التعليم	• كورسات قصيرة • فيديو • نشرات إخبارية • لوحات إعلانية(بوسترات)	• محاضرات • تدريب على عينات • حالات دراسة سابقة • تدريب مباشر حي
المدة الزمنية	قصيرة(بالساعات أو الأيام)	متوسطة(بالأيام أو الأسابيع)

الجدول(٥-٢): سمات التدريب والتوعية بأمن المعلومات وطرق تنفيذهما

ملخّص الفصل

تؤدّي السياسات الأمنيّة دورًا بارزًا في توطيد أمن المعلومات في المنشأة كركيزة أساسية للتوجيهات العامّة والتفصيليّة للحفاظ على أمن المعلومات، و من ثَمَّ تحقيق أهداف المنشأة.

فهناك السياسة الأمنيّة العامّة التي تُعنى بتحديد برنامج أمن المعلومات وأهدافه، ومنح الصلاحيّات وتحديد المسؤوليات اللازمة لتنفيذه، و وضع الآليات والطرق التي تضمن فرض البرنامج وتطبيقه على أرض الواقع، وهناك السياسة الموضوعيّة المتخصّصة في موضوعات أو تخصّصات معيّنة بشكل تفصيلي أكثر من السياسة الأمنيّة العامّة، وهناك السياسة الأمنيّة الخاصّة بأنظمة محدّدة، كتلك الخاصّة بتنفيذ قرارات إدارة المنشأة المتعلّقة بأنظمة تقنية المعلومات المستخدمة فيها، كالحاسبات الآلية، والشبكات، والبرامج التطبيقيّة، والبيانات.

إنّ المعايير القياسيّة هي التي تدعم السياسات الأمنيّة بأنواعها كافة، وتمنحها صفة القطعية، سواءً أكانت تلك المعايير خاصّة بالمنشأة، أم عامة تفرض على المنشأة من الجهات العليا، وتحدّد معايير المنشأة كيفيّة استخدام منتجات تقنية المعلومات من الأجهزة والبرامج، وكيفيّة تطبيق هذه التقنيات في المنشأة بطريقة آمنة.

يحدد الخط الأساسي مرجعًا موحّدًا وموثوقًا للمنشأة يُرجَع إليه عند وجود أيّ تغيير في المنشأة أو أنشطتها أو أنظمتها أو موظفيها؛ لمقارنة وضع أمن المعلومات في المنشأة معه، ومعرفة مدى بُعدها عنه من أجل اتّخاذ اللازم للعودة إليه.

إنّ التوجيهات هي إرشادات عامة غير إلزاميّة، يرجع لها المستخدمون في الظروف غير الواضحة، التي تحتاج إلى مرونة في التطبيق، ويرجع إليها كذلك لتفسير السياسات الأمنيّة، والمعايير، والإجراءات؛ لإعطاء المستخدم المعلومات التفصيلية التي يحتاج إليها.

أمّا الإجراءات فتحدّد كيفية تطبيق كل من السياسات الأمنيّة، والمعايير القياسية، والتوجيهات على أرض الواقع، ونقلها من الطرح النظري إلى إجراءات واقعية تنفّذ في بيئة تشغيليّة حقيقيّة. فهي التي تحدّد الخطوات التفصيليّة لتنفيذ المهام والأنشطة ذات العلاقة بالمعلومات.

لتصنيف المعلومات أهميّة بالغة في تنظيم المعلومات وترتيبها، وفقًا لدرجة حساسيتها وأهميتها للمنشأة. فيحدد عدد من مستويات التصنيف المناسبة لمعلومات المنشأة، ليُصار بعد ذلك إلى توزيع المعلومات على تلك المستويات، وتسهّل هذه العمليّة كذلك تصنيف الأنظمة

المعالجة للمعلومات وفقًا لمستويات المعلومات نفسها، ثم إجراء عمليّات التدقيق والمراقبة عليها.

أخيرًا، لا يمكن تحقيق الاستفادة التامّة من السياسات الأمنيّة والمعايير والتوجيهات والإجراءات دون برنامج توعية وتدريب مُحكم، يعرِّف جميع مستويات منسوبي المنشأة بتلك المفاهيم وطرق تفعيلها واستخدام الأنظمة المحققة لها.

مسائل

١. ما السياسة الأمنيّة؟ وما أنواعها؟ وما خصائص كل نوع؟

٢. لماذا تحتاج السياسة الأمنيّة الموضوعية للتحديث بشكل مستمر ومتكرر أكثر من السياسة الأمنيّة العامة؟

٣. قارن بين السياسات الأمنيّة والمعايير والتوجيهات والخط الأساسي والإجراءات، من حيث: المفهوم، والمهمة التي تؤديها، وخصائصها، مع إعطاء أمثلة على كل منها.

٤. ما الفوائد المترتبة على تصنيف المعلومات؟ وهل يزيد ذلك من حماية المعلومات أم ينقصها؟ اشرح ذلك.

٥. المنشأة(أ) هي منشأة تقنية تطوِّر وتنتج برامج الحاسب الآلي التطبيقيّة، والمنشأة(ب) هي منشأة ماليّة تجاريّة تعتمد بشكل أساسي على التجارة الإلكترونيّة. بناء عليه فإن المطلوب هو الآتي:

أ. اقترح مستويات تصنيف المعلومات المناسبة لكل منشأة.

ب. وزّع معلومات كل منشأة على مستويات التصنيف التي حددتها في الفقرة(أ).

ج. وزّع أنظمة تقنيات المعلومات المستخدمة في كلّ منشأة على مستويات التصنيف التي حددتها في الفقرة(أ).

د. أعط أمثلة للخطوط الأساس التي يجب مراجعتها لكل منشأة.

ه. أعط أمثلة للأحداث التي يجب عندها مراجعة هذه الخطوط في كل منشأة.

٦. يؤدي عمر المعلومة دورًا رئيسًا في تصنيفها. اشرح ذلك مع إعطاء أمثلة.

٧. مستعينًا بالبحث في شبكة الإنترنت أعط أمثلة على السياسات الأمنيّة الموضوعيّة، خلاف ما ذكر في هذا الفصل، مع سرد البنود التي تحتويها.

٨. مستعينًا بالبحث في شبكة الإنترنت، أعط أمثلة على السياسات الأمنيّة للأنظمة، خلاف ما ذكر في هذا الفصل مع سرد البنود التي تحتوي عليها.

٩. مستعينًا بالبحث في شبكة الإنترنت ضع برنامجًا توعويًّا لأمن المعلومات موجّهًا للإداريين، وآخر موجّهًا للتنفيذيين؛ بحيث يشمل كل منهما: السياسات الأمنيّة، والمعايير، والتوجيهات، والخط الأساسي، والإجراءات.

الفصل السادس

أمن الحاسبات والبرمجيات والملفّات

أهداف الفصل

- تحديد أصول أنظمة الحاسب الآلي، وتهديدات كل منها، وكيفية تأمينها.
- التعريف بالبرامج الضارّة: الفيروسات، والديدان، وأحصنة طروادة، وخصائصها، وأنواعها، وأعراض الإصابة بها، ثم طُرُق مكافحتها.
- التعريف ببرامج التجسّس وأنواعها، وتوضيح طريقة عملها، ثم طُرُق مكافحتها.
- حماية البيانات وصلاحيّات الملفّات.

ما ستتعلمه في هذا الفصل

- أصول أنظمة الحاسب الآلي: الأجهزة، والبرمجيات، والبيانات.
- تهديدات أجهزة الحاسب الآلي، البرمجيات، والبيانات التي يجب الحماية منها.
- تعريف فيروسات الحاسب الآلي، وخصائصها، وكيف تعمل بشكل عام.
- ديدان الحاسب الآلي، والفرق بينها وبين الفيروسات، وكيف تعمل.
- سبب تسمية أحصنة طروادة بهذا الاسم، وماذا تعمل في الحاسب الضحية؟ والفرق بينها وبين الفيروسات والديدان.
- الخطوات اللازمة للحصول على حماية جيدة ضد البرامج الضارة.
- برامج التجسّس وخطورتها، وماذا تفعل في الجهاز الضحية، وطرق مكافحتها.
- برنامج راصد المفاتيح كمثال على برامج الرصد والتسجيل.
- العناصر الرئيسة الأربعة كحد أدنى لتأمين أنظمة الحاسب الآلي: السِّريّة، والسلامية والتكاملية، والتوفر، والتحقق من الهُويّة.
- الصلاحيّات على الملفّات، وماذا يمكن أن توفره كل صلاحية للمستخدم؟

أمن الحاسبات والبرمجيات والملفّات

٦-١ مقدّمة

تؤدي أجهزة الحاسب الآلي دورًا رئيسًا في إنجاز الأعمال اليوميّة على المستويات كافة، وهذا ما يجعلها جديرة بالاهتمام بتوفير الحماية اللازمة لها، وعلى الرغم من ذلك فإنّ أجهزة الحاسب الآلي وحدها لا تؤدّي أيّ غرض، ولا تنفّذ أيّ مهمّة، دون وجود أنظمة التشغيل والبرامج التطبيقيّة عليها، ويمكن القول إنّ أجهزة الحاسب الآلي ما هي إلا مواد لا تستجيب ولا تنتج أي عمل إلا بإدخال نظام التشغيل (القلب النابض) إليها، ومعنى ذلك أنّ هناك أصولًا أساسيّة للحاسب الآلي، تتمثل في: الأجهزة، والبرامج، والبيانات (المخزّنة في ملفات)، التي يجب حمايتها وضمان عملها بالشكل الصحيح، وإلا سيكون هناك خلل في مكون أساسي من أصول أنظمة الحاسب الآلي.

يقصد بأمن الحاسبات هنا، أمن أجهزة الحاسب الآلي (كعتاد صلد)، ويقصد بأمن البرمجيات أمن أنظمة التشغيل التي تتحكم بالأجهزة، وأمن البرامج التطبيقيّة التي يتعامل معها المستخدم لأداء مهامه اليومية، ويقصد بأمن الملفّات أمن الملفّات نفسها كأوعية لتخزين المعلومات، مثل: ملفات معالجة النصوص، والجداول الإلكترونيّة، وقواعد البيانات، ورسائل البريد الإلكتروني، وأمن نظام الملفّات (File System) الذي يتحكم بإدارة جميع الملفّات.

في هذا الفصل سوف نوضح أولًا التهديدات التي تتعرض لها الأجهزة والبرمجيات والملفّات، ثم نوضح طُرُق حمايتها من خلال تأمين هذه الأصول، وتأمين الملفّات كأوعية المعلومات الرئيسة التي لا يمكن أن يعمل دونها أيّ جهاز حاسب آلي، أو نظام تشغيل، أو برنامج تطبيقي.

٦-٢ التهديدات الرقميّة للحاسبات والبرمجيات والملفّات

يكمن التهديد الرئيس لجهاز الحاسب الآلي (الصلد) في وفرته. فالجهاز هو أكثر المناطق ضعفًا في مواجهة الهجمات، وأكثرها طاعة لضوابط الرقابة التلقائية. وتشمل تهديدات أجهزة الحاسب الآلي كذلك: السرقة، وإلحاق الضرر بها سواءً عن طريق الخطأ أم العمد.

إنّ انتشار أجهزة الحاسبات الشخصية والاعتماد عليها في إنجاز كثير من الأعمال،

والزيادة المطّردة في استخدام شبكات الحاسب الآلي، زادت من احتمالات فقد الأجهزة. لذلك فإنّ الاحتياطات الأمنيّة الماديّة (الفيزيقية) والإداريّة ضرورية للتعامل مع تلك التهديدات.

يكمن التهديد الرئيس للبرمجيات في الهجمات على توفر البرنامج، خاصّة البرامج التطبيقيّة، حيث غالبًا ما تكون سهلة الحذف، ومن التهديدات كذلك تغيير البرامج التطبيقيّة أو إتلافها؛ لتصبح غير مفيدة. ومن أكثر المشكلات التي يجب التعامل معها في مجال البرمجيات هو التعديلات التي تحدث في البرنامج الذي لا يزال يعمل، لكنه يجري تحديثه بطريقة مختلفة عن الطريقة السابقة. ولحل هذه المشكلة يجب توزيع البرامج بعناية عن طريق إنشاء النسخ وفق إصدارات تدريجية، وتوزيع النسخ الأحدث منها. المشكلة الأخيرة التي تواجه البرمجيات هي الخصوصية، ومع أن هنالك كثيرًا من الاحتياطات التي اتخذت، إلّا أنّ مشكلة النسخ غير المرخّص له للبرامج ما زالت بدون حل.

إن أمن أجهزة الحاسب الآلي (الصلدة) والبرمجيات هي بالتحديد مخاوف اختصاصيي مراكز الحاسب الآلي ومستخدميه من الأفراد. والمشكلة الأوسع انتشارًا هي أمن البيانات، التي تشمل الملفّات والأشكال الأخرى للبيانات، التي يتحكم فيها الأفراد، والمجموعات ومنظمات الأعمال الحكومية والتجارية.

إنّ التهديدات الأمنيّة بخصوص البيانات واسعة جدًّا لدرجة أنها تشمل تهديدات توفرها وتهديدات سرّيّتها، وتهديدات سلامتها وتكاملها. ففي حالة التوفر، فإنّ التهديدات تكمن في إتلاف ملفات البيانات، التي قد تحدث إمّا عن طريق الخطأ أو بشكل متعمّد، وفي حالة السِّريّة، تكمن التهديدات في القراءة غير المسموح بها لملفات البيانات أو قواعد البيانات، وفي حالة سلامة البيانات وتكاملها، تكمن التهديدات في تغيير البيانات، إمّا بحذف أو إضافة أو تعديل، وهذا المجال قد أضحى أكثر المجالات اهتمامًا بالأبحاث والجهود المبذولة من جانب المختصين في أمن المعلومات. وهناك تهديد آخر لكنه أقل ظهورًا، وهو تحليل البيانات وتحليل تصاميم قواعد البيانات من أجل كسر حمايتها، ويمكن القول إن سلامة البيانات هي الهاجس الأكبر في معظم المنشآت؛ لأن التعديلات التي تجرى على ملفات البيانات قد تترتب عليها

نتائج تتراوح بين المخاطر الصغيرة إلى المخاطر الكارثية.

يوضح تقرير معهد أمن الحاسب الآلي(Computer Security Institute-CSI) لعام ٢٠١٠/٢٠١١م[١] أن(١٦,٨٪) من الجهات التي أجريت الدراسة المسحيّة عليها(شملت الدراسة جهات حكومية وشركات مختلفة ومعاهد ماليّة وطبيّة وجامعات) قد تعرّضت لهجوم تعطيل الخدمة(DoS)، وأن(١١,٤٪) تعرضت لسرقة كلمات المرور، وأن(٣٣,٥٪) تعرّضت لسرقة الأجهزة المحمولة، وأن(٨,٧٪) تعرّضت لاحتيال ماليّ، وأن(٧,٤٪) تعرّضت لاستغلال الشبكات اللاسلكيّة، وأن(٦٧,١٪) تعرّضت لهجمات البرامج الخبيثة.

هناك تهديدات رئيسة تُعدُّ قاسمًا مشتركًا بين تهديدات الحاسبات والبرمجيات والبيانات، وتهدّد كلًّا منها إمّا بشكل منفصل أو بشكل تكاملي، وهذه التهديدات هي: البرامج الضارة(Malware)، وبرامج التجسّس(Spyware) ولأهمية هذه التهديدات فقد أفردنا لكل منها موضوعًا مستقلًا نتعرف فيه ماهيّة هذه التهديدات، وأنواعها، وطريقة عملها، وطرق مكافحتها.

٦-٢-١ البرامج الضارّة(Malware)

هو مصطلح جديد نسبيًّا في مجال الأمان. وقد استخدم هذا المصطلح للحاجة إلى مناقشة البرامج أو التطبيقات التي صمّمت خصّيصًا بحيث تحتوي مهام اختراق الأنظمة، وكسر سياسات الأمان وخططه، أو القيام بأعمال ماكرة أو عمليّات مدمّرة. ولأنّ هذا النوع من البرامج قد بدأ يأخذ أشكالًا كثيرة مختلفة، مثل: الأبواب الخلفية، وخدع البيانات، ونشر مانعات الخدمة(Deny of Service-DoS)، وحصان طروادة، والفيروسات، والديدان، لذا فإنّ هذا التعبير أصبح يستخدم لمجموعة كبيرة من البرامج الضارّة، والمخادعة، والماكرة.

رغم أنّ مصطلح "البرامج الضارّة" عادة ما يستخدم بطريقة عمومية؛ ليكون مرادفًا للفيروس، إلا أنه بنفس الطريقة أصبح يطلق اسم "فيروس" ببساطة لوصف أي نوع من مشكلات الحاسب الآلي؛ مما سبب بعض اللبس وصعوبة التفريق بين أنواع البرامج الضارة. ولم يقف الأمر عند ذلك الحد، بل أصبح هناك خلط واضح بين الفيروسات، والديدان،

١- Computer Security Institute(CSI) Survey(2011), The 15th Annual Computer Crime and Security Survey.

وأحصنة طروادة، رغم أن لكل منها خصائصه التي تميزه من غيره، وإن كان القاسم المشترك بينها هو إلحاق الضرر.

فيما يلي نقدّم شرحًا لأغلب البرامج الضارّة وأشهرها، وهي: الفيروسات، والديدان، وبرامج أحصنة طروادة، وسيكون ذلك من خلال تعريف كل منها وتوضيح خصائصه، وأنواعه، والطرق التي ينتشر بها، وبعد ذلك نقدم طُرُق مكافحة هذه البرامج بشكل موحّد، حيث إن أغلب برامج الحماية الحالية توفر حماية متكاملة لجميع هذه البرامج من خلال حزم برامج موحّدة لها جميعًا.

٦-٢-١-١ فيروسات الحاسب الآلي

بدأ ظهور الفيروسات في السبعينيّات من القرن الميلادي الماضي، وكانت بداياته بسيطة جدًّا، ولم تكن على مستوى الخطورة التدميريّة الحاصلة في عصرنا الحاضر. فكما يكتب المبرمج برامج مفيدة، يمكنه أيضًا أن يكتب برامج ضارّة تسمّى الفيروسات، ومن أمثلة ذلك أن يكتب برنامجًا بسيطًا يُنفّذ حلقة غير منتهية من الأوامر الفارغة، أو ما يسمّى بالحلقة اللامنتهية (Infinite Loop) التي تجعل المعالج المركزي يدخل في تنفيذها ولا يخرج منها، ما يتسبّب في تجمّد (تعليق) الجهاز. لقد أصبحت الفيروسات أكثر خطرًا وانتشارًا من ذي قبل، خصوصًا مع تزايد استخدام الحاسب الآلي واتساع استخدام شبكة الإنترنت.

تُعدُّ الفيروسات أكبر فئات البرامج الضارّة من ناحية عدد الأشكال المعروفة، ومن ناحية أثرها في بيئة الحاسب الآلي، ولذلك فإنّ كلمة "فيروسات" تميل لأن تكون مرادفًا في ذهن العامة لكل أنواع البرامج غير السوية أو الشرعية.

إنّ سبب تسمية فيروسات الحاسب الآلي بهذا الاسم هو تشابهها الكبير مع الفيروسات التي تصيب الإنسان. فإنّ فيروس الحاسب الآلي يبدأ بعدوى، أي انتقال من جهاز إلى آخر، ثم مرحلة حضانة أو ركود، ثم بعد ذلك يبدأ بالعمل والتكاثر (نسخ نفسه)، ثم تظهر أعراضه، ثم يحدث بعد ذلك الخراب والدمار الذي يسببه، سواء أكان صغيرًا أو كبيرًا.

فيروس الحاسب الآلي هو برنامج يُعدُّ لينسخ وينشر نفسه، وينتشر ذاتيًّا دون علم وتعاون مع المالك أو المستخدم للجهاز، ولم يتم التوصل بعد لتعريف موحد للفيروسات متفق عليه من

الباحثين كافّة، والتعريف العام هو تعريف فريد كوهين[1]، الذي يعرّف الفيروس بأنه: «برنامج يعدّل البرامج الأخرى لكي تحتوي نسخة معدّلة من نفسها» ورغم أنّ هذا التعريف يصف جُلّ الفيروسات، وأن كثيرًا من الباحثين ما زالوا يصرّون على استخدامه، إلّا أنّه يقتصر على البرامج التي تقحم نفسها بنفسها في البرامج الأخرى فقط، وهو بذلك يهمل كثيرًا من الفيروسات التي تقحم نفسها في الملفّات التي ليست برامج بطبيعتها، كالوثائق مثلًا. وعليه يمكن تعريف الفيروسات بصورة عامة بأنّها: «البرامج التي تُقحم نفسها بنفسها في مادّة أخرى قد تكون برنامجًا أو قرصًا أو وثيقة أو رسالة بريد إلكتروني أو نظام كمبيوتر أو أيَّ صيغة معلوماتيّة».

لدى كثير من الناس انطباع بأنّ أيّ شيء لا يسير على ما يرام في الحاسب الآلي يكون؛ سببه فيروس، ابتداءً من فشل القرص الصلب، وحتى أخطاء الاستخدام، والحقيقة أنّه ليس بالضرورة أن ينتج عن الفيروس ضرر ما. فقد يتم بناء الفيروسات لكي تكون وسيلة نقش إلكتروني لعلامة تخلد اسم مصممه في العالم، وفي بعض الأحيان يُعرض اسم مصمم الفيروس في أيّ مناسبة مع عنوانه ورقم هاتفه، واسم الشركة أو الحزب السياسي الذي ينتمي إليه، من أجل الشهرة فقط دون إلحاق أي ضرر.

خصائص الفيروسات

لا تحدث فيروسات الحاسب الآلي أو تنتج طبيعيًّا، وإنّما هي برامج يكتبها مبرمجون، وكذلك فهي لا تظهر من خلال بعض التطورات الإلكترونيّة فقط، وإنّما تكتب بصورة متعمّدة عن طريق أناس متخصّصين، وتبقى الفيروسات مختبئة داخل الجهاز المصاب حتى يستثيرها المستخدم، كفتح الملف المصاب، أو تشغيل البرنامج المصاب؛ لتبدأ بالعمل والتكاثر والانتشار. أي أنّها لا تبدأ بعملها حتى يستثيرها المستخدم، وهناك عدّة خصائص لفيروسات الحاسب الآلي تميزها من غيرها من البرامج الضارّة، وتساعدها على الانتشار وإصابة أجهزة الحاسب الآلي دون علم مستخدميها، وهي:

- التخفّي: ويعني القدرة على الارتباط ببرامج أو ملفّات أخرى تبدو سليمة ومألوفة

[1]- Bidgoli, Hossein(2006c), "Handbook of Information Security", Volume 3, Part 1

للمستخدم، بحيث يلحق الفيروس نفسه بالملف المصـاب خفية ليصبح جزءًا منه. ومن أشهر طُرُق تخفي الفيروسات ما يلي:

- التخفّي في مرفقات البريد الإلكتروني.
- التخفّي في الملفّات التي يجري تحميلها من مواقع الإنترنت، خاصّة تلك التي تشغّل ملفات الصوتيات والفيديو وتتبادلها.
- التخفي وراء الروابط والأوامر الموجـودة في صفحات الإنترنت والبريد الإلكتروني.
- التخفّي وراء روابط وملفات الإعلانات والبريد الدعائي.
- التخفّي مع البرامج المنسوخة بشكل غير قانوني.

- التضاعف: ويعني ذلك أن ينسخ الفيروس نفسـه عدّة نسخ تصل في بعض الأحيان إلى ملايين النسخ، بمعنى أنه يتكاثر ليصيب أكبر قدر ممكن من الملفّات والبرامج داخل جهاز الحاسب الآلي نفسه أو داخل الأجهزة الأخرى المرتبطة به. وتبدأ عمليّة التضاعف عندما يتم تحميل برنامـج الفيروس إلى ذاكرة الحاسـب الآلي وينفّذه المعالج المركزي.
- الانتشار: ويعني انتقال الفيروس من جهـاز إلى آخر عبر شبكات الحاسب الآلي أو وسائط التخزيـن المختلفة، ومعنى ذلـك أنّ لدى الفيروس القـدرة على نقل نفسه عند استثارته، كتشغيل أمر النسخ، أو عند اكتشاف اتصال الحاسب الآلي المصاب بحاسب آلي آخر، ومن أشهر طُرُق انتشار الفيروسات ما يلي:
  - تحميل ملفات مصابة من مواقع شبكة الإنترنـت أو زيارة مواقع تنشر الفيروسات بشكل تلقائي.
  - فتح مرفقات بريد إلكتروني مصابة.
  - أن ينسـخ المستخدم ملفـات مصابة دون علمه، ويخزّنهـا على وسائط تخزين خارجية تنتشر معها، أو يرسلها عبر الشبكة (كاستخدام المجلّدات

المشتركة)، فتنتشر عبرها.

■ أن ينسخ الفيروس نفسه، ثم يرفق تلك النسخة مع أيّ ملف آخر عند استثارته.

أنواع الفيروسات

ثمة أنواع كثيرة جدًا من الفيروسات. لكن ما يهمنا هنا هو الأنواع (أو المجموعات) الرئيسة الأكثر انتشارًا، التي يشكّل كلّ نوع منها مجموعة من الفيروسات لها البُنية نفسها وتؤدي مهام متشابهة إلى حدّ كبير، وهذه الأنواع هي:

- فيروسات قطاع بدء التشغيل (الإقلاع): يوجد لكل نظام تشغيل قطاع في قرص التخزين الصلب، مخصّص لبدء عمليّة التشغيل (الإقلاع) وعادة ما يكون هذا القطاع هو القطاع الأول (Track 0)، وعند وجود أيّ خلل فيه فإنّ الحاسب الآلي لن يستطيع البدء بالتشغيل. وفيروسات قطاع بدء التشغيل (Boot Sector Viruses) هي الفيروسات التي تصيب قطاع بدء التشغيل في قرص التخزين الصلب، وتكمن خطورة هذا النوع من الفيروسات في إصابتها لمكان مهم جدًّا يتم من خلاله توجيه الجهاز لتنفيذ البرامج التي يجري من خلالها استكمال تجهيز جهاز الحاسب الآلي للعمل، وبدلًا من ذلك يوجّه الفيروس الحاسب الآلي لتنفيذ الكود الخاص بالفيروس، و من ثَمَّ يفشل الجهاز في عمليّة الإقلاع ولا يمكنه العمل.
- فيروسات الملفّات (File Infecting Viruses): هي الفيروسات التي تصيب الملفّات بشتى أنواعها؛ فيمكن أن تصيب ملفّات نظام التشغيل كملف (Command.com) في نظام الويندوز أو أيّ ملف آخر، وعادة ما ينتج عن هذه الفيروسات زيادة في أحجام الملفّات.
- الفيروسات الجزئيّة الكبيرة: تستخدم الفيروسات الجزئيّة الكبيرة (Macro Viruses) البرمجة الجزئية الخاصة بتطبيق معيّن، مثل معالج الكلمات، للبدء بنشاطها. وتضرب هذه النوعيّة من الفيروسات ملفات البيانات (مثل ملفات برامج

وورد وإكسل وأكسس)، وتظل ساكنة أو مقيمة في التطبيق نفسه عن طريق إصابة حقل التهيئة الخاص به. وعلى الرغم من أنّ الفيروسات الجزئية الكبيرة تصيب ملفات البيانات، إلا أنّها عمومًا لا تعدّ من فيروسات الملفّات، والسبب في ذلك أن فيروسات الملفّات قد تصيب البرامج وملفات البيانات، بينما لا تصيب فيروسات الجزئية الكبيرة إلا ملفات البيانات فقط.

- فيروسات البريد الإلكتروني: هي الفيروسات التي تنتقل بوساطة البريد الإلكتروني. فبإضافة بعض الوظائف (عن طريق الفيروس) لبرنامج مقدم خدمة البريد الإلكتروني القياسي (مثل أوتلوك (Outlook)) أصبح للفيروسات إمكانية الانتشار عبر العالم خلال ساعات فقط، بدلًا من شهور. ومن أشهر فيروسات البريد الإلكتروني فيروس ماليسا (Melissa) وماليسا ليس أول فيروس بريد إلكتروني، بل أول فيروس بريد إلكتروني انتشر بنجاح بصورة شرسة هو فيروس كريستما إكسك (Christma Exec) في خريف ١٩٨٧م[١]. لكن فيروس ماليسا هو أول فيروسات البريد الإلكتروني السّريعة التكاثر والانتشار، وكذلك الأول الذي صار معروفًا لشريحة واسعة من عامّة الناس. ويُعدُّ ماليسا من الفيروسات الجزئية الكبيرة، فبالإضافة إلى أنّه فيروس بريد إلكتروني، إلا أنه يمكن أن يرسل نفسه ذاتيًا في شكل وثيقة مصابة بالفيروس.

أعراض الإصابة بالفيروسات

عندما يصاب جهاز الحاسب الآلي بفيروس فإنّه قد يظهر عليه بعض الأعراض الآتية:

- البطء الشديد: يعمل الحاسب الآلي ببطء ملحوظ، وتصبح سرعة البرامج المركبة عليه أبطأ من المعتاد، ومن ذلك أن نظام التشغيل يعمل ببطء شديد عند بداية التشغيل، أو عند إيقاف التشغيل، وقد يكون سبب هذا البطء هو النقص الشديد في الذاكرة العشوائية (RAM).
- تعليق (أو تجمد) الحاسب الآلي: يدخل الحاسب الآلي في حالة من الجمود وعدم الاستجابة لأيّ أمر؛ فلا يمكن في هذه الحالة تشغيل أيّ برنامج، أو حتى إيقاف عمل الجهاز.

١- Bidgoli, Hossein(2006c), "Handbook of Information Security", Volume 3, Part 1

- انهيار الحاسب الآلي: في أغلب حالات انهيار الحاسب الآلي تظهر شاشة غريبة (كالشاشات الزرقاء في نظام التشغيل ويندوز)، وعندئذ يتوقف الحاسب الآلي عن العمل.
- إضاءة لمبة القرص الصلب بشكل عشوائي ومتّصل.
- زيادة أحجام الملفّات وزيادة الزمن اللازم لفتح الملفّات أو تشغيل البرامج.
- وجود بيانات تالفة كانت صالحة من قبل.
- ظهور رسائل خطأ، ومربعات حوار غير مألوفة وغير متوقعة.
- إعادة تشغيل الحاسب الآلي بشكل آلي ومستمر دون تدخل المستخدم.

٦-٢-١-٢ ديدان الحاسب الآلي

دودة الحاسب الآلي (Worm Computer) هي عبارة عن برنامج مستقل بذاته، وله ملف خاص به. فالدودة تُعدُّ برنامجًا تطبيقيًّا متكاملًا يمكن أن يعمل لوحده، ولا يحتاج لأن يضيف نفسه لملف آخر، كما هي الحال في الفيروسات. ويمكن للدودة أيضًا أن تعمل بمفردها وتحمّل نفسها إلى ذاكرة الحاسب الآلي، وتبدأ بالعمل بشكل آلي.

من الفوارق الأصليّة، هي أن الديدان تستخدم الشبكات وروابط الاتصالات لكي تنتشر، وهي خلافًا للفيروسات لا تلتحم مباشرة بالملفّات القابلة للتنفيذ. وتصيب الديدان أجهزة الحاسب الآلي المرتبطة بشبكات الحاسب الآلي المصابة دون تدخل المستخدم أو قيامه باستثارتها كفتح ملف معين أو تشغيل برنامج، كما هي الحال في الفيروسات. فقد تنتقل إلى الجهاز بمجرّد تصفّح بعض مواقع الإنترنت، أو بمجرّد فتح بريد إلكتروني (إذا لم يكن الجهاز محميًا ببرنامج حماية محدّث) وهذا الأمر يجعلها تنتشر بشكل أسرع وأوسع من الفيروسات.

من خلال البحوث السابقة في مجال البرامج الضارّة، تُستخدم كلمتا دودة وفيروس بالترادف؛ حيث كان يعتقد أنّ الفرق الفني بينهما غير ضروري لمعظم المستخدمين. وأصل مصطلح برنامج "دودة" يتواءم فنيًّا مع طُرُق انتشار الديدان في الوقت الحاضر. فنجد أنّ برنامج الدودة يتكوّن من أجزاء (رأس وجسم كما في الدودة الطبيعية) تعمل في أجهزة حاسب

متفرقة، تتواصل فيما بينها عبر الشبكة، فيمكـن أن تجد رأس البرنامج في جهاز، وذيله في جهاز آخر بعيد.

في خريف عـام ١٩٨٨م، لم تضع دودة الإنترنـت يونيكس موريـس(UNIX/Morris) الإنترنت عامة والبريد الإلكتروني خاصّة في حالة شبه توقف فقط، بل لقد استطاعت تشغيل الإصدارات الحديثة لنظم التشغيل يونكس وترويجها في منصّات أقراص صلبة محدّدة[١]، وخلال هذه العاصفة البريدية، تأثرت كثير من الأجهزة بالفصل بين البريد الإلكتروني وقائمة توزيع البريد، وفُقد بعض رسائل البريد نهائيًّا، ومعظم البريد جرى تأخيره، وفي بعض الأحوال تم توجيهه نحو طُرُق أقل كفاءة؛ ما تسبّب في فقده أو تأخيره. وفي الحالات الأخرى التي تأثرت فيها الأجهزة الرئيسة بالمشكلة كانت ببساطة أبطأ في نقل البريد، وكذلك توقفت في بعض الأجهزة الأخـرى برامج نقل البريد، وخرجت من الخدمة مع تأخير ملحـوظ في إرسال البريد. ومن المفارقة في هذه العاصفة، أنّ البريد الإلكتروني يشكّل الوسيلة الأساسيّة التي يحاول مختلف الأطراف التعامل مع المشكلة من خلاله، وكانوا يحاولون استخدامه للتواصل فيما بينهم؛ ما زاد الأمر سوءًا. وعند دخول رأس الدودة إلى النظام، يُغذّى بالبرنامج الرئيسي،(الجسم)، من الموقع الذي أصيب مسبقًا، ويستُخدم برنامجان:(رأس وجسم)، أحدهما في الموقع المصاب، والآخر في الموقع المستضيف(الجديد) وإذا لم يستطع أيٌّ من البرنامجين العمل، تُزيل الدودة نفسها بنفسها، وإن كان المستضيف الجديد غير مناسب، فإنّ الدودة ستبحث عن مستضيفين آخرين وتوصيلات أخرى.

طُرُق انتشار الديدان

من أهـم خصائص الديدان هي قدرتها علـى الانتشار والتكاثر عـبر الاتصال بشبكات الحاسب الآلي، ومن أهم الطرق التي تنتشر بها الديدان ما يلي:

- مرفقات البريد الإلكتروني المصابة.
- التحميل التلقائي عند زيارة بعض مواقع الإنترنت التي من خلالها تنتشر الديدان، أو عند استخدام أحد الارتباطات داخل البريد الإلكتروني.

١- Bidgoli, Hossein(2006c), "Handbook of Information Security", Volume 3, Part 1.

- التسلل عبر الثغرات الأمنيّة في أنظمة التشغيل أو برامج الحماية.
- أضرار الديدان
- لا تقل أضرار الديدان عن الفيروسات من ناحية التلف، أو فقْد البيانات التي تسببها، ومن أهم أضرار الديدان ما يلي:
- تتيح للمهاجم أن يستخدم الحاسب الآلي المصاب لمهاجمة أجهزة أخرى، أو مواقع الإنترنت، أو إرسال بريد إلكتروني، أو تحميل برامج ضارّة إليه.
- يمكن من خلالها فتح باب خلفي (Back Door) في الجهاز المصاب، حيث يمكن التحكّم به من خلال ذلك الباب.
- يمكن للديدان أن تنسخ نفسها، وترسل نسخة إلى كل بريد إلكتروني في عناوين البريد المخزّنة في جهاز الحاسب الآلي المصاب.

٦-٢-١-٣ برامج أحصنة طروادة

في مجال أمان الحاسب الآلي، يعرّف حصان طروادة بأنّه جزء من برنامج (كود) قابل للتنفيذ يؤدي بعض المهام لا يتوقعها المستخدم، ويقيم في البرنامج المصاب. وطروادة يمكن أن يوضع في برنامج بريء عند تأليفه وجمعه، أو يمكن إضافته للبرنامج بعد جمعه. وسبب تسمية هذا البرنامج الضار بهذا الاسم هو تشابه عمله مع أسطورة الحصان الخشبي الذي اختبأ به عدد من الجنود اليونانيين، وكانوا سببًا في فتح مدينة طروادة[١]. فبرنامج حصان طروادة هو برنامج ضار (الجنود)، مختبئ داخل برنامج بريء (حصان خشبي).

إنّ مصطلح حصان طروادة يحمل في طيّاته دلالة سالبة جدًّا، بسبب وفرة أحصنة طروادة المنتشرة، التي صُمّمت بغرض إغراق أجهزة الكمبيوتر. وعلى الأقل يمكن لحصان طروادة ألا يكون أكثر من مجرد إزعاج، وفي أسوأ مراحله يمكن لحصان طروادة أن يدمّر بالكامل عمل الجهاز الذي يسكنه. وكمثال لحصان طروادة الذي يكون مجرّد مصدر إزعاج هو "وحش خاصية الاسترجاع"، الذي يحثّ المستخدم على الدخول إلى الكلمة (cookie) بصورة دوريّة، ومثال لحصان طروادة الماكر هو برنامج التجسّس (الذي قد يدمج في برنامج، أو يكون قائمًا

١- البداينة، ذياب(٢٠٠٦)، «الأمن وحرب المعلومات».

بذاته)، الذي يتم نشره بواسطة مورد البرامج؛ ليرسل معلومات تتعلّق بالمستخدم لجهة تستغل هذه المعلومات بصفة غير شرعيّة. وبعض برامج حصان طروادة الماكرة تسجّل الضغطات على أزرار لوحة المفاتيح الخاصة بالمستخدمين وتحفظها في ملف مخفي يمكن من خلاله انتحال شخصية المستخدمين عند الحصول على ذلك الملف المخفي في وقت لاحق.

عمومًا يمكن تقسيم برامج حصان طروادة إلى تلك التي تنتشر عن طريق تغيير شيفرة (كود) المصدر (Source Code)، وتلك التي تنتشر عن طريق إصابة الملف القابل للتنفيذ يدويًّا. وطريقة الانتشار السابقة تفترض أنّ لدى مؤلّف حصان طروادة لديه القدرة على تحوير شيفرة المصدر لكي تحتوي برنامج حصان طروادة، وأنّ لديه القدرة بعد ذلك على جمع البرنامج البريء ونشره، وهذا الخيار لا يكون دائما ممكنًا، ولذلك فإنّ مؤلفي أحصنة طروادة قد يلجؤون في بعض الأحيان لتحوير الملفّات الموجودة مسبقًا والقابلة للتنفيذ. والبرامج التي يجري تحويرها بهذه الطريقة هي البرامج العامّة، التي توفّر بغرض تحميل برامج أخرى، أو برامج نظم التشغيل التي تكون في الجهاز محل الهجوم.

تختلف أحصنة طروادة عن فيروسات وديدان الحاسب الآلي بأنها لا تتكاثر أو تتضاعف. ففيروسات الحاسب الآلي هي برامج تتضاعف عن طريق إصابة البرامج الأخرى، وتحتاج إلى استثارتها من قبل المستخدم لكي تنتشر، والديدان قد تصيب البرامج التنفيذية أو لا تصيبها، ولا تتطلّب عادة استثارتها من قبل المستخدم بصورة واضحة لكي تتضاعف، إلا أنّها تتضاعف وتنتشر بطريقة أسرع من الفيروسات. وقد ظهر الفرق بين الفيروس والدودة بمرور السنوات، لكن الفارق الرئيس بينهما وبين حصان طروادة هو أنّ هذا الأخير لا يتكاثر.

٦-٢-١-٤ مكافحة البرامج الضارّة

بدأت تظهر في الآونة الأخيرة إصابات ليست فيروسيّة صرفة ولا دوديّة محضة، وإنّما خليط من تقنيات الفيروسات والديدان لكي تنتشر بصورة أسرع وأكثر نجاعة، و"رسالة حب" هي مثال لهذا التحول في تقنيات الإنتاج لهذه الآفات. وكذلك فإنّ "نيمدا" هو مثال للدودة، لكنه أيضًا ينتشر بطرق أخرى كثيرة؛ لذا يمكن عدّها فيروس بريد إلكترونيًّا في الوقت نفسه. وهذا التحول في التقنيات سيكون مشكلة إضافية في المستقبل، ويجب مراعاة

ذلك في طُرُق الحماية المتبعة.

يمكن مكافحة البرامج الضارّة باستخدام حزمة برامج واحدة لمكافحة كل من الفيروسات والديدان وأحصنة طروادة في آن واحد؛ لذا لا بدّ من تثبيت برنامج مكافحة جيّد وتحديثه دوريًّا لتوفير الحماية المطلوبة. ولا بدّ أن تشتمل برامج الحماية ليس فقط على كشف الإصابات فقط، وإنّما إزالتها أيضًا، وهناك عدّة برامج (أو حزم) مشهورة لمكافحة البرامج الضارّة يمكن الاعتماد عليها، ومن أشهرها:

- حزمة برامج مكافي (McAfee).
- حزمة برامج سيمانتك (Symantec).
- حزمة برامج كاسبر سكاي (Kasper SKY).
- حزمة برامج نورتون (NORTON).
- وفي جميع الحالات لا بدّ من اتّباع الخطوات الآتية للحصول على مكافحة جيدة:
- تحديث برنامج المكافحة آليًّا ودوريًّا لضمان كشف الفيروسات والديدان وأحصنة طروادة الحديثة ومنعها.
- تحديث نظام التشغيل آليًّا ودوريًّا عن طريق تنشيط خاصية التحديث التلقائي لسد الثغرات الأمنيّة عند ظهورها.
- تحميل ملفات الإصلاح الأمنيّة الخاصة بأنظمة التشغيل وبعض البرامج التطبيقيّة الأخرى، (كحزمة برامج الأوفيس) التي تصدرها الشركات المصنّعة (كشركة مايكروسوفت) بشكل مستقلّ لسدّ ثغرة أمنيّة خاصّة لم يتم سدها من خلال التحديث التلقائي، وكذلك تحميل حزم الخدمة (Service Pack) الجديدة حال ظهورها.
- عدم فتح مرفقات البريد الإلكتروني التي لها الامتدادات التشغيليّة مثل: (scr) (exe) (vbs)، أو التي لها أكثر من امتداد مثل (txt.vbs).
- ويمكن أن تعمل برامج المكافحة بإحدى الطرق الآتية أو جميعها:
- باستخدام جدول زمني معيّن يحدّد من خلاله عمل برنامج المكافحة؛ ليبدأ بفحص

جميع مكوّنات الجهاز عند أوقات محدّدة (عند منتصف الليل من كل يوم مثلًا).

- عند الطلب من قبل المستخدم، ويمكن أن يكون ذلك في أيّ وقت.
- عند تشغيل البرامج أو فتح الملفّات أيًّا كان نوعها، وفي هذه الحالة يفحص برنامج المكافحة الملف المراد فتحة قبل أن تتم عمليّة الفتح الفعليّة؛ للتأكد من خلوّه من الفيروسات والديدان وأحصنة طروادة، ومن الأفضل تفعيل جميع هذه الطرق لتوفير حماية أفضل وأشمل.

٦-٢-٢ برامج التجسّس

لقد عُرفت فيروسات الحاسب الآلي بصورة موسعة في أواخر الثمانينيّات. فهي كائنات غريبة ولافتة للنظر، وفي كل مرة يوجّه الفيروس ضرباته يكون هو موضوع الأخبار، خاصّة إذا انتشر بسرعة. وخلال السنوات القليلة الماضية ظهرت فئة جديدة من البرامج الماكرة هي برامج التجسّس، وبرنامج التجسّس ليس بفيروس، لكن فعله أقوى وأخطر من الفيروسات والديدان وأحصنة طروادة. فبالرغم من عدم تسببه في تلف البيانات، إلا أنه يفعل فعله من وراء الكواليس بكل هدوء، ودون علم المستخدم، وينقل المعلومات لمالكه. وبرنامج التجسّس هو عبارة عن خدعة ماكرة، مثله في ذلك مثل الفيروس، لكنه عمومًا أقل شهرة.

حاليًا تقحم برامج التجسّس في المئات من برامج المشاركة المعروفة، بل وصل الحد لإنتاج البرامج التجارية من هذه الفئة، وحسب التقديرات التي قيست في النصف الأول من العام ٢٠١٢م فإنّ نحو (١٥٪) من أجهزة الحاسب المحمولة و(٢١٪) من أجهزة الحاسب المكتبية مصابة ببرامج التجسّس[١]. ويوضح تقرير معهد أمن الحاسب الآلي (Computer Security Institute-CSI) لعام ٢٠١٠/٢٠١١م أن(١١,٤٪) من عينة الدراسة تعرضوا لسرقة كلمات المرور، وأن(٨,٧٪) تعرضوا لاحتيال مالي، وأن(٧,٤٪) تعرضوا لاستغلال الشبكات اللاسلكية[١].

على الرغم من الجدل الذي يكتنف تعريف برنامج التجسّس الدقيق، إلا أنّه في النهاية

١- PC Pitstop statistics: Spyware and adware(2012): www.pcpitstop.com/research/spyware.asp(Spyware by PC Type).

١- Computer Security Institute(CSI) Survey(2011), The 15th Annual Computer Crime and Security Survey.

كائن (إلكتروني) يتجسّس عليك، ونتيجة لذلك يتركز الجانب المهم من موضوع برنامج التجسّس عادةً حول مسألة الخصوصيّة. ويُعـدُّ تعريف ويبوديا[٢] لبرنامج التجسّس أفضل التعريفات الموجودة، حيث عرّفه بأنه: «أيّ برنامج يحصل –سرًّا– على معلومات عن المستخدم عن طريق الربط بالإنترنت، وخاصة بدعاوى دعائية وإعلانيـة». عادةً ما يتم تضمين برامج التجسّس في شكل مكوّنات مجانيّة خفية، أو برامج مشاركة يمكن تنـزيلها من شبكة الإنترنت، وبمجرّد تركيب برنامج التجسّس يبدأ بمراقبة حركة المستخدم علـى الإنترنت، وينقل المعلومات من وراء الكواليس لجهة أخرى.

٦-٢-٢-١ أنواع برامج التجسّس

كما رأينا في تعريف برامج التجسّس، فهي برامـج خطيرة تتسلل إلى الحواسيب وتعرف المعلومـات الخاصة والسِّريّة المخزّنة بها، وربما ترسلها إلـى أجهزة أخرى بمجرد توفر خط الاتصال، وبناءً على طريقة عملها، يمكن تصنيف برامج التجسّس إلى نوعين رئيسين: برامج رصد وتسجيل، وبرامج تتبع.

النوع المعروف من برامج الرصد والتسجيل هو مسجل أو راصد المفاتيح (من لوحة المفاتيح) وحركات الفأرة. فهو يعمل في صمت في الخلف ويقوم بتسجيل ضغطات المفاتيح وحركات الفأرة لكي يعيد ترتيب وتكوين ما يفعله المستخدم، وهـذه الطريقة شديدة الخطورة، إذ يمكن من خلالها معرفة الأرقام السِّريّة أو الأرقام الخاصة التي يُدخلها المستخدم عبر لوحة المفاتيح. وخلافًا لراصد عمل المفاتيح، هناك أيضًا راصدات ومسجلّات للبريد الإلكتروني والدردشة. وراصدات عمل المفاتيح مشهورة؛ لأنّها هي أكثر الأنواع شيوعًا وإزعاجًا في عمليّة سرقة كلمات السر وأرقام بطاقات الائتمان.

أمّا المتتبّعات فتراقب عادات الاستخدام وأنماطه وتخزّنها كبيانات إحصائيّة بهدف إعداد التقارير بناءً عليها. وقد تكون البيانات عبارة عن عادات التصفح للشخص المستهدف، مثل استخدام برنامج معيّن أو خاصية محدّدة في ذلك البرنامج. ويتم تجميع هذه المعلومات عن الشخص الضحية ثم تحليلها واستخدامها في الهجوم عليه أو سرقة معلوماته.

٢- Bidgoli, Hossein(2006b), "Handbook of Information Security", Volume 2.

٦-٢-٢-٢ طريقة عمل برنامج التجسّس

فنيًّا لا يصنف برنامج التجسّس كفيروس، ولذلك لا يمكن مكافحته بشكل كامل من خلال البرامج المصمّمة لمكافحة الفيروسات. وعلى وجه التحديد تُتلف الفيروسات البيانات على جهاز الحاسب الآلي وتنسخ نفسها ذاتيًّا، في حين تعمل برامج التجسّس خلسة، ولا تتلف البيانات، بل تتجسّس عليها. ويمكن لبرامج التجسّس أن تنسخ نفسها على الجهاز وتعمل كمهمة خلفية، ثم تنقل المعلومات السِّريّة الخاصة بالمستخدم لمالكها دون علم المستخدم.

لدى برنامج التجسّس مكوّنان أساسيّان: ففي الواجهة الأمامية هو برنامج عادي يعمل في العلن، ويوفر وظائف مفيدة، بينما هو في الخلف برنامج تجسّس يراقب وينقل المعلومات. ويمكن لبرنامج التجسّس البقاء في أيّ صورة أو شكل من أشكال البرامج القابلة للتنفيذ، بما في ذلك التطبيقات مثل(ActiveX، Plug-in)، أو أكواد(Applets).

عادة لا تجمع برامج التجسّس المعلومات الشخصيّة فقط، لكن بالإضافة إلى ذلك تجمّع المعلومات الديموغرافية وعادات التصفح. ومن المحتمل أن تباع هذه المعلومات المتحصل عليها، أو أن تضاف لقواعد البيانات الأخرى لبناء سجلّات عن المستخدم وعادات استخدامه، وعن طريق ربطها بالبيانات الشخصية، مثل: الاسم والعنوان وعنوان البريد الإلكتروني والعمر والجنس والدخل وتاريخ الائتمان، قد تكون من أقوى وسائل التسويق. ومن الطبيعي أن يكون من السهل التعرّف إلى المعلومات والبيانات التي أرسلت لمالك برنامج التجسّس، وربطها مع البيانات الاخرى بطريقة صحيحة. وهناك عدد من الطرق والوسائل لإنشاء سجّل بالمعارف الفريدة(GUIDs) عن كل ضحية، وهذه الطرق والوسائل عادة ما يجري إنشاؤها أثناء عمليّة تركيب برنامج التجسّس والاحتفاظ بها في حاسب الضحية، وينسخ البرنامج(الذي في جهاز الضحية) في كل مرّة المعلومات من جهاز الضحيّة بغرض تحديث سجّل الضحية لدى مالك برنامج التجسّس. ورغم أنّ مجموعة الأشخاص الذين جرى التعرف إليهم وترميزهم أصبحوا ضحايا ومعلوماتهم مخترقة، إلا أن خصائص الحاسب الآلي والأجهزة المرتبطة به مثل كرت الشبكة وعنوان بروتوكول الإنترنت(IP) يمكن استخدامها كلها في المزيد من

عمليّات التجسّس والتتبع وإيقاع ضحايا آخرين.

٦-٢-٢-٣ أعراض وجود برامج التجسّس وطرق انتقالها

بما أنّ برامج التجسّس تعمل على جمع المعلومـات الخاصة بالحاسب الآلي ومستخدمه، وإرسالها إلى مواقع أو أجهزة أخرى، فإنّ الأمر يتطلب القيام بأعمال إضافية غير التي يقوم بها المستخدم، ولهذا تظهر لها بعض الأعراض، ومنها:

- نشاط أعلى من الحد المعتاد: ويتضح ذلك أكثر عندما يرسل الحاسب الآلي ويستقبل كميّات كبيرة من البيانات عبر الشبكة أو الإنترنت، في حين أن المستخدم لا يستخدم أيّ برامج تستوجب ذلك، ويمكن ملاحظة ذلك عن طريق مراقبة عمل جهاز المودم وعرض كميّة البيانات التي أرسلها واستقبلها.
- طلب الاتصال بالإنترنت تلقائيًا: وتظهر هذه الحالـة في الأجهزة التي لا يوجد بها جهاز مـودم (Digital Subscriber Line-DSL)، حيث يشغّل برنامج التجسّس طلب الاتصال الهاتفي من أجل الارتباط بالإنترنت.
- ظهور أشرطة أدوات غير مألوفة تُضاف إلى متصفّح الإنترنت.
- اختيار صفحة بداية لمتصفّح الإنترنت خلاف الصفحة التي تم ضبط المتصفّح عليها من قبل المستخدم.

ومن أشهر الطرق التي تنتقل بها برامج التجسّس طريقتان، هما:

- تظهر كأنها برامج عادية حتى يتم تثبيتها من قبل المستخدم وبعلمه.
- الاختفاء في برامج أخرى، بحيث يجري تثبيتها مع هذه البرنامج دون علم المستخدم.

٦-٢-٢-٤ مكافحة برامج التجسّس

من أخطر ما تفعله برامج التجسّس هو أنها تُزيل برامج مكافحة التجسّس. ويمكن القول إنّه ليس هناك برنامج يحمي من برامج التجسّس بدرجة كاملة، لكن يمكن أخذ بعض التدابير الوقائية، ومنها:

١- فلاتر خصائص استرجاع البيانات

يمكن تفعيل أو تعطيل وسائل استرجـاع البيانات، أو ما يسمّى بملفات الكوكي(Cookie Files)، الخاصة بالمواقع التي تتم زيارتها من خلال المتصفّح، وهذه الميزة تجعل من السهل تصفح المواقع التي تمت زيارتها خلال الجلسة الواحدة. وللشخص الحق في قبول كل أو بعض وسائل استرجاع البيانات أو رفضها بالكامل، وكثير من المستخدمين يُعطّلون وسائل استرجاع البيانـات كافة، كإجراء احترازي من برامج التجسّس، إلا أن هذا الإجراء قد لا ينصح به، لأن كثيرًا من المواقع تتطلب تفعيل هذه الخدمة بالكامل، وعمومًا يُعدُّ تفعيل استرجاع بيانات الجلسـة آمنًـا؛ لأن صلاحيتها تنتهي فـور مغادرة المستخـدم الموقع، والبديـل الآخر لتفعيل استرجـاع البيانات بالكامل هـو استخدام خاصيـة "التحذير قبل القبـول" لكي يتم تنقيح المسترجعات يدويًّا، لكن هذا من شأنه أن يؤدّي إلى امتلاء الجهاز بأوامر حثّ تشغيل ملفات الكوكي عند تصفح الإنترنت. ويمكن للموقع أن ينشـئ خطّة "خصوصيّة" تنظّم استخدام ملفات الكوكي وطريقة حذفها أو التخلص منها بعد الانتهاء منها. وفي متصفّحات الإنترنت الحديثة يمكن للمستخدمين نقل إعدادات الخصوصية للمواقع التي تتم زيارتها، وسيرفض المتصفّح الاسترجاعات تلقائيًّا بالنسبة للمواقـع التي ليس بها سياسة خصوصية، أو المواقع التي لا تقتصر خطتها على الجلسة المحدّدة فقط.

٢- حاجبات الإعلانات والنوافذ المنبثقة(Pop-UP Blockers)

هي برامج تقوم على إجهاض تنـزيل وعرض صور الإعلانات الدعائيّة والإغراق الإعلاني، ومنع النوافذ المنبثقة من الظهور التلقائي. ففي صفحات المواقع التي تشير إلى وجود إعلانات دعائية، فإنّ هذه الحاجبات تعمل على تنقيحها قبل التنـزيل. وعن طريق تجنّب الإعلانات التي تظهر على الشاشة تلقائيًّا والوسائـط المتعدّدة التي تستهلك موارد الجهاز، يمكن لحاجبات الإعـلان أن تحسّن من أداء المتصفّح، ويمكن للمستخدمـين أن يحافظوا على خلوّ الأقراص الصلبة الخاصة بهم من أيّ ملفات غير ضرورية باستخدام حاجبات الإعلانات، ويمكن لبعض حاجبات الإعلانات أن تحسّن من عمليّة الخصوصية عن طريق تحديد المعلومات المعطاة. ومن

جهة أخرى، فإنّ لدى مانعات الإعلان بعض الأثر السلبي الخفيف، حيث إنها تعمل على حجب بعض الإعلانات المفيدة من خلال بعض المواقع غير الموقع الأصلي للإعلان. وينصح بشدة بعدم السماح للنوافذ المنبثقة التي تظهر تلقائيًّا عند زيارة بعض المواقع، وعدم استخدامها إلا بعد التأكّد من مرجعيتها، وصحة العنوان الذي تحمله.

٣- استخدام مضادات برامج التجسّس

إنّ أفضل وسيلة متاحة للدفاع ضد برامج التجسّس وإزالتها في حال وجودها هي استخدام برامج مكافحة التجسّس(Antispyware Scanners) وهي برامج شبيهة ببرامج مضادات الفيروسات، من حيث طريقة تركيبها وتشغيلها وتحديثها. ويعمل برنامج مكافحة برامج التجسّس بطريقة برنامج مكافحة الفيروسات نفسها ، حيث يستعرض(يمسح) جهاز الحاسب الآلي بحثًا عن الملفّات المرتبطة ببرامج التجسّس. وبعد عمليّة المسح يحدّد البرنامج المشكلات المحتمل حدوثها، ويسمح للمستخدمين بتقرير ماهية البرامج التي يتوجب إزالتها. كما يحذف برنامج مكافحة التجسّس ملفات الكوكي غير الآمنة.

٤- استخدام جدار النار الشخصي وبرامج كشف التطفل

بما أنّ كثيرًا من برامج التجسّس يمكن أن تثبّت نفسها أثناء تصفّح الإنترنت؛ فإنّ تثبيت برنامج الجدار الناري(Personal Firewall) قد يوفر بعض الحماية، وهذه الجدران الناريّة هي مكوّنات برمجيّة تشابه في عملها أجهزة الجدران النارية(انظر الفصل السابع) وتحجب برامج التجسّس إن وُجِدت وتمنعها من الاتصال بالإنترنت دون إذن المستخدم. ويمكن للمستخدم أيضًا أن يحجر على عنوان بروتوكول الإنترنت(IP) الخاص بأجهزة الخادم لبرنامج التجسّس(أي مالك برنامج التجسّس) ويمكن للجدران الناريّة تنبيه المستخدمين إلى أيّ محاولات للدخول إلى جهاز الحاسب أثناء تصفح الإنترنت، وكذلك يعمل على إعلام المستخدمين إن كان هناك أيّ برنامج على الحاسب يحاول إرسال بيانات دون تفويض بذلك.

تستخدم برامج كشف التطفل (IDS Programs) لرصد محاولات الدخول غير المصرّح به، وكذلك مراقبة حركة الشبكة أو حالة النظام، ويعتمد برنامج كشف التطفل على الخطة

الموضوعة له. فهو يتطلب قاعدة بيانات تحدّد ما السلوكيات السيئة أو غير المقبولة؟ وعن طريق قاعدة البيانات هذه يتعرّف نظام كشف التطفل ماهيّة الأنشطة العاديّة، ومن ثم يمكنه مراقبة التغييرات التي جرت، التي تدلّ على عمليّة التطفل أو النشاط المشكوك فيه.

٥- تأمين متصفّح الإنترنت

من الإجراءات المضادّة لبرامج التجسّس هي ضبط إعدادات أمان متصفّح الإنترنت لدرجة مقبولة من الأمان، حيث يجب وضع الأمان في المستوى المتوسّط أو العالي، مع الخيارات الآتية لكل من(ActiveX) و(Plug-ins) (في أنظمة تشغيل ويندوز)[١]:

- إبطال كود أكتيف إكس(ActiveX) غير المؤشر عليها بأنها آمنة.
- تنشيط التحكّم بتنزيل أكتيف إكس(ActiveX)، من خلال السماح للمعروفة منها بأنها آمنة(Singed) ومنع غير الآمنة(Unsigned).
- تنشيط التحكّم بكل من أكتيف إكس(ActiveX)، وبلق – إنز(Plug-ins).

٦- تأمين إدخال كلمات المرور

ومن إحدى طُرُق مكافحة برامج التجسّس استخدام لوحة مفاتيح افتراضيّة مرسومة على الشاشة، عوضًا عن لوحة المفاتيح العادية عند إدخال كلمات المرور والأرقام السِّريّة، ويمكن استخدام الفأرة للضغط على أي مفتاح، بدلًا من الضغط على الأزرار في لوحة المفاتيح العادية.

يمكن من خلال هذا الإجراء منع برامج الرصد والتسجيل من التقاط الأزرار التي يتم الضغط عليها من قبل المستخدم، وقد استخدم هذه الطريقة كثير من مواقع البنوك التجاريّة.

٦-٣ أمن أنظمة التشغيل والملفّات

إنّ فهم نوعيات التهديدات التي تواجه أنظمة التشغيل والملفّات، يسهل تحديد المتطلبات الأمنيّة اللازمة للحصول على أنظمة آمنة. ويكمن كثير من العمل في المجال الأمني للمعلومات وحمايتها، عندما يتعلق الأمر بأنظمة التشغيل والملفّات، في تحقيق عناصر أمن المعلومات(انظر الفصل الثالث: عناصر أمن المعلومات). ومن هنا، فإنّ هناك أربعة عناصر رئيسة يمكن من خلالها تحقيق الحد الأدنى لأمن أنظمة التشغيل والملفّات، وهي:

١- [١] يمكن الحصول على مزيد من المعلومات حول ذلك في المرجع: الغثبر، خالد بن سليمان و القحطاني، محمد بن عبد الله(٢٠٠٩)، «أمن المعلومات بلغة ميسرة».

١. التحقّق من الهُويّة: يتطلب ذلك أن تكون أصول أجهزة الحاسب الآلي(أنظمة التشغيل، والملفّات، والأجهزة نفسها) قادرة على التحقّق من هويّة المستخدم، ومن هويّة البرامج والبيانات.

٢. السِّريّة: وتتطلب أن يكون الدخول إلى أنظمة الحاسب الآلي والبيانات المخزّنة بها من قبل الجهات المصرّح لها فقط، وأن تبقى البيانات والمعلومات سرّيّة(غير مقروءة) لمن ليس له حق الاطّلاع عليها. وفي أنظمة التشغيل تكون المعلومات السِّريّة للقراءة فقط من قبل الجهات المصرّح لها بذلك فقط، وهذا النوع من الدخول يشمل: الطباعة، والعرض، وأنواع الاستعراض(التصفح) الأخرى، وكذلك يشمل إمكانية الكشف عن وجود العنصر(ملف أو مجلد مثلًا).

٣. السلامة والتكاملية: ويتطلب ذلك إمكانية تعديل أصول أنظمة الحاسب الآلي بوساطة الجهات المصرّح لها بذلك فقط، والتعديل يشمل: الكتابة، والتغيير، وتغيير الوضع، والحذف والإنشاء.

٤. التوافر: يتطلب ذلك أن تكون أصول أنظمة الحاسب الآلي متوافرة للجهات المخول لها باستخدامها.

وتهدف هـذه العناصر في مجملها إلى تحقيق الغايات الآتية، التي تُعدُّ هي جوهر أمن أي نظام تشغيل:

- ضبط الدخول: ويهتم هذا بتنظيم دخول المستخدم إلى كامل نظام التشغيل، والأنظمة الفرعية والبيانات، وينظّم عمليّة الدخول إلى مختلف الموارد في النظام.
- ضبط تدفق المعلومات: ينظّم تدفق البيانات في النظام وتسليمها إلى المستخدمين .
- التأكيد: يتعلّق بإثبات أنّ الدخول وآليات ضبط التدفق تعمل وفقًا لمواصفاتها، وأنّها تفرض الحماية المطلوبة والسياسات الأمنيّة.

٦-٣-١ صلاحيّات الملفّات والوصول الجماعي

في الأنظمة التي تسمح بعدد كبير من المشغلين، كثيرًا ما تظهر الحاجة إلى عرض الملفّات المشتركة وتعديلها التي يتشارك فيها عدد من المستخدمين. وتبرز هنا قضيتان هما: صلاحيّات

المستخدمين، والوصول الجماعي للملفات.

صلاحيّات المستخدمين

يجب أن يوفر نظام الملفّات أداة مرنة تسمح بالمشاركة المكثفة للملفات بين المستخدمين، ويجب أن يقّدم نظام الملفّات عددًا من الخيارات، بحيث يمكن ضبط الطريقة التي يتم الدخول بها إلى الملف المحدّد.

كإجراء مثالي، يجب منح المستخدم (أو مجموعة المستخدمين) صلاحيّات معيّنة للدخول إلى الملفّات، بحيث يستخدم مدى واسع من أنـواع الوصول إلى الملفّات. والقائمة الآتية تمثل صلاحيّات الملفّات التي يمكن منحها لشخص أو مجموعة معيّنة ولملف محدّد.

- دون صلاحية: في هذه الحالة، لا يعرف المستخدم مـا إذا كان الملف موجودًا أم لا، ويكون هناك عدد قليل جدًّا ممن له حق الدخول إلى ذلك الملف، ولفرض هذا القيد، لا يسمح للمستخدم بقراءة دليل الملفّات (Directory)، الذي يحتوي ذلك الملف.
- صلاحية العلم: بإمكان المستخدم تحديد وجود الملف ومن هو مالكه، وبعد ذلك يمكن للمستخدم أن يطلب من المالـك حق الوصول إلى ذلك الملف، ونـوع ذلك الوصول، وغالبًا ما يكون مالك الملف هو الشخص الذي أنشأه.
- صلاحية التنفيذ: بإمكان المستخدم أن يحمِّـل الملف (أو البرنامج) ويشغّله، لكن لا يمكنه أن ينسخه، وغالبًا ما يتم إنشاء الملفّات والبرامج بهذه الخاصية تلقائيًّا.
- صلاحية القراءة: بإمكان المستخدم أن يقرأ (يشاهد) الملف لأيّ غرض، بما في ذلك النسخ والتنفيذ، وفي بعض أنظمة التشغيل يمكن فرض تمييز بين المشاهدة والنسخ. في حالة المشاهدة يمكن عرض محتويات الملف للمستخدم، بينما ليس له حق نسخه.
- صلاحية التذييل: بإمكان المستخدم إضافة بيانات للملف، لكن في نهاية الملف فقط، ولا يمكنه تعديل أيٍّ من محتويات الملـف أو حذفها. تفيد هذه الصلاحية في تجميع البيانات من كثير من المصادر.
- صلاحية التحديث: بإمكان المستخدم التعديل، والحذف، والإضافة إلى الملف. وهذا

يشمل عادة التعديل في أي مكان في الملف، وإعادة كتابته بالكامل أو جزء منه، وإزالة كل البيانات أو بعضها، وبعض أنظمة التشغيل تميّز بين مختلف درجات التحديث.

- صلاحية تغيير الحماية: بإمكان المستخدم تغيير الصلاحيّات الممنوحة للمستخدمين الآخرين. وبشكل عام فإنّ مالك الملف هو الوحيد الذي يحمل هذه الصلاحية، ويمكن للمالك منح هذه الصلاحية للآخرين. ولمنع إساءة استخدام هذه الصلاحية، يمكن للمالك تحديد أيّ الصلاحيّات التي يمكن تغييرها من قبل من منحه هذه الصلاحية.
- صلاحية الحذف: بإمكان المستخدم أن يحذف الملف من نظام الملفّات.

يمكن استخدام هذه الصلاحيّات بشكل تراكمي هرمي. فمنح أيّ صلاحيّة يشمل جميع الصلاحيّات التي قبلها. فمثلًا، إذا مُنح مستخدم معيّن صلاحية التحديث لملف محدّد، فإنّ ذلك المستخدم يمنح أيضًا الصلاحيّات الآتية: العلم، والتنفيذ، والقراءة، والتذييل، وإذا عُيِّن أحد المستخدمين مالكًا لملف محدّد، فإنّه يصبح مالكًا لجميع الصلاحيّات على ذلك الملف(عادة ما يكون لدى المالك جميع الصلاحيّات بلا استثناء)، ويمكنه أن يمنح أيًّا منها لمستخدمين آخرين.

يمكن منح أيٍّ من الصلاحيّات السابقة لأيّ مجموعة من المستخدمين وفق الآتي:

- المستخدم المحدّد: المستخدمون الأفراد الذين تُمنح لهم بعض الصلاحيّات بصورة منفردة.
- مجموعات المستخدمين: مجموعة من المستخدمين الذين لم يُحدّدوا انفراديًّا. فيمكن منح أي من الصلاحيّات المذكورة سابقًا لمجموعة من المستخدمين، كما لو كانوا شخصًا واحدًا. ويجب أن يكون لدى نظام الملفّات طريقة جيدة لتتبع عضويّة مجموعات المستخدمين والتحكّم بها وإدارتها.
- الجميع: يكون لجميع المستخدمين الصلاحية نفسها.

الوصول الجماعي للملفات

يمكن أن تُمنح الصلاحية نفسها لعدد من المستخدمين في الوقت نفسه. فيمكن أن يقرأ

الملف أكثر من مستخدم في الوقت نفسه، لكن عندما تُمنح صلاحية التذييل أو التحديث في الملف لأكثر من مستخـدم، فإنّ نظام التشغيل أو نظام إدارة الملفّـات يجب أن يفرض قانونًا يضبط ذلك الحق لضمان توافق البيانات(Data Consistency) ومن ذلك أن يُقفل الملف بالكامل عندما يريد أحد المستخدمين تحديثه، ويُترك مفتوحًا لذلك المستخدم فقط، وبذلك يمكن ضمان حصول جميع المستخدمين على آخر التحديثات للملفات.

ملخّص الفصل

بدأ هذا الفصل بتوضيح التهديدات التي تتعرّض لها الأجهزة والبرمجيات والملفّات للتعرف إليها أولًا، ثم طرح طُرُق الحماية المناسبة لكل منها. وتأتي البرامج الضارّة على رأس تهديدات الحاسبات الآلية والبرامج والملفّات، وتشمل: الفيروسات، والديدان، وبرامج أحصنة طروادة. وقد قدَّم هذا الفصل تعريفًا لكل منها، مع توضيح خصائصه وأنواعه، والطرق التي ينتشر بها، وبعد ذلك قدَّم طُرُق مكافحة هذه البرامج بشكل موحّد، حيث إن أغلب برامج الحماية الحالية توفر حماية متكاملة لجميع هذه البرامج من خلال حُزم برامج موحّدة لها جميعًا.

من تهديدات الحاسبات الآلية والبرامج والبيانات برامـج التجسّس، وبرنامج التجسّس ليس بفيروس، لكن فعلـه أقوى وأخطر مـن الفيروسات والديدان وأحصنـة طروادة. فعلى الرغم من عدم تسبّبه في تلف البيانات، إلا أنّه يفعل فعله من وراء الكواليس بكل هدوء، ودون علم المستخدم، وينقل المعلومات لمالكه. وقد قدَّم هذا الفصل بعض التدابير الوقائية لبرامج التجسّس، كفلاتـر خصائص استرجاع البيانـات، وحاجبات الإعلانـات والنوافذ المنبثقة، واستخدام جدار النار الشخصي وبرامج كشف التطفل، بالإضافة لاستخدام مضادات برامج التجسّس.

لتحقيق أمن أنظمة التشغيل والملفّات فقد طرح هذا الفصل آليات الحماية التي تُعدُّ جوهر أمن أي نظام تشغيل، وهي: ضبط الدخول؛ لتنظيم دخول المستخدم إلى كامل نظام التشغيل والأنظمة الفرعية والبيانات، ولتنظيم عمليّة الدخول إلى مختلف الموارد في النظام، وضبط تدفق المعلومات؛ لتنظيم تدفق البيانات في النظام وتسليمها إلى المستخدمين، والتأكيد؛ الذي

يضمن إثبات أن الدخول وآليات ضبط التدفق تعمل وفقًا لمواصفاتها، وأنها تفرض الحماية المطلوبة والسياسات الأمنيّة.

أخيرًا جرى تحديد صلاحيّات المستخدمين والمجموعات الأكثر انتشارًا (دون صلاحية، والعلم، والتنفيذ، والقراءة، والتذييل، والتحديث، وتغيير الحماية، والحذف)، وكذلك طريقة الوصول الجماعي للملفات.

مسائل

١. ما أصول أنظمة الحاسب الآلي؟ اذكر تهديدًا واحدًا على الأقل لكل أصل من هذه الأصول.

٢. عرّف فيروسات الحاسب الآلي، ثم عدِّد خصائصها.

٣. عرّف ديدان الحاسب الآلي، ثم عدِّد طُرُق انتشارها.

٤. اشرح الفرق بين الفيروسات والديدان وأحصنة طروادة وبرامج التجسّس، من حيث بدء عملها (استثارتها).

٥. لماذا سمّيت فيروسات الحاسب الآلي وديدانه بهذه الأسماء؟

٦. عرف برامج التجسّس، ثم اذكر أنواعها.

٧. لماذا تُعدُّ الديدان أسرع البرامج الضارّة انتشارًا ؟ وما دام الحال كذلك، فهل هناك إمكانية لبرنامج ما أن ينتقل كدودة (لينتشر بسرعة)، ويقوم بعمل برنامج تجسّس؟ أعط مثالًا.

٨. ما أعراض وجود برنامج تجسّس في جهازك؟ وهل يلزم أن تظهر جميع الأعراض؟ وماذا يجب عليك فعله عندئذٍ؟

٩. أيّهما أفضل، مراقبة ظهور أعراض البرامج الضارّة وبرامج التجسّس أم الاعتماد على برامج الكشف والحماية ؟

١٠. ملفات الكوكي سلاح ذو حدين. اشرح ذلك.

١١. أُعطي مستخدم عادي صلاحية التنفيذ على برنامج ما. فما هذه الصلاحية؟ وما الصلاحيّات الأخرى التي يمكن أن يمارسها بمجرّد منحه هذه الصلاحية؟ وهل يستطيع أن يمنحها مستخدمًا آخر؟

١٢. ما المقصود بالوصول الجماعي للملفات؟ وما الفائدة منه؟ وماذا يمكن أن ينتج عنه في حالة عدم التحكّم به؟

١٣. بالرجوع إلى شبكة الإنترنت، اختر أحد أنظمة التشغيل المشهورة، ثم ابحث عن الثغرات الأمنيّة فيه – إن وجدت – وكيفية معالجتها.

الفصل السابع

أمن شبكات الحاسب الآلي

أهداف الفصل

- التعريف بتهديدات الشبكات: الهجوم الإلكتروني والهندسة الاجتماعيّة.
- التنبيه على الثغرات الممكن النفاذ من خلالها، وتحديد أنواعها.
- إيضاح التدابير الأمنيّة العامة لأمن شبكات الحاسب الآلي.
- كيفية تأمين وسائط نقل المعلومات في شبكات الحاسب الآلي.
- التعريف بجدار النار وأساسيات عمله، والحماية التي يوفرها، ومميزاته وعيوبه.
- التعريف بالشبكة الخاصة الافتراضيّة، وطريقة عملها، والحماية التي توفرها.
- التعريف بالشبكة المحلية الافتراضيّة وطريقة عملها، والحماية التي توفرها.
- شرح طُرُق وتقنيات حماية خوادم وبرامج الويب، وطبقات شبكات الحاسب الآلي.

ما ستتعلمه في هذا الفصل

- الهجوم الإلكتروني، وأنواع المهاجمين، وأهدافهم.
- أدوات مسح شبكات الحاسب الآلي التي تستخدم للبحث عن الثغرات الأمنيّة.
- التدابير الأمنيّة العامة الأربعة عشر لأمن شبكات الحاسب الآلي.
- الإجراءات اللازمة لتوفير الحماية لوسائط نقل المعلومات في شبكات الحاسب.
- جدار النار، وكيفية عمله، والمكان المناسب الذي يجب أن يوضع فيه في شبكة الحاسب.
- الشبكة الخاصة الافتراضيّة(VPN)، وطريقة عملها، ومزاياها وعيوبها.
- الشبكة المحلية الافتراضيّة(VLAN)، وطريقة عملها، ومزاياها وعيوبها.
- نظام الحماية ذو الطبقتين، ونظام الحماية ذو الثلاث طبقات.
- كيفية حماية طبقات شبكات الحاسب الآلي.

أمن شبكات الحاسب الآلي

٧-١ مقدّمة

في عصرنا الحاضر، أصبحت شبكات الحاسب الآلي من التجهيزات الأساسيّة لأيّ منشأة. فقلما تجد منشأة – بغض النظر عن حجمها وطبيعة عملها – ليس لديها شبكة حاسب آلي، ولم يقتصر استخدام شبكات الحاسب الآلي على الشبكات المحلية (LAN) فقط، بل أصبحت هذه الشبكات مرتبطة بعضها ببعض باستخدام شبكات واسعة النطاق (WAN)، سواءً باستخدام خطوط اتصال خاصّة، أم عن طريق استخدام شبكة الإنترنت كناقل متوفر رخيص الثمن وسهل الاستخدام. وأصبح من المألوف أن تجد منشأة تتوزّع فروعها في أنحاء شتّى من العالم، وتؤدّي أعمالها اليوميّة كما لو كانت في بناية واحدة.

ما يؤرق مالكي شبكات الحاسب الآلي ومستخدميها، هو موضوع أمن هذه الشبكات، خاصّة في ظل تزايد استخدام شبكة الإنترنت (غير الآمنة) كناقل رئيس للبيانات الموزّعة، وظهرت الحاجة الملحّة إلى استخدام وسائل حماية خاصّة لهذا الغرض، كاستخدام جدران النار (Firewalls)، والشبكات الخاصة الافتراضيّة (Virtual Private Networks-VPNs).

في الحقيقة فإنّ موضوع أمن شبكات الحاسب الآلي هو موضوع مهم وكبير ويحتاج إلى كتاب مستقل لتغطيته بالشكل الصحيح، لكن ما أردنا إيراده في هذا الفصل هو توضيح أشهر التهديدات الرقميّة لشبكات الحاسب الآلي، ثم استعراض المتطلبات الأساسيّة لأمن الشبكات والتقنيات والآليات اللازمة لذلك على النحو الآتي:

- التدابير الأمنيّة العامة لأمن شبكات الحاسب الآلي.
- أمن وسائط نقل المعلومات.
- استخدام جدران النار.
- استخدام الشبكات الخاصة الافتراضيّة (VPNs).
- استخدام الشبكات المحلية الافتراضيّة (VLANs).
- نظام الحماية ذو الطبقات المتعدّدة.

- أمن طبقات شبكات الحاسب الآلي.

٧-٢ التهديدات الرقميّة لشبكات الحاسب الآلي

يوضح تقرير معهد أمن الحاسب الآلي(Computer Security Institute-CSI) لعام ٢٠١٠/٢٠١١م[١] أن(١٦,٨٪) من الجهات التي أجريت الدراسة المسحيّة عليها(شملت الدراسة جهات حكومية وشركات مختلفة ومعاهد ماليّة وطبيّة وجامعات) قد تعرضوا لهجوم تعطيل الخدمة(DoS)، وأن(١١,٤٪) تعرضوا لسرقة كلمات المرور، وأن(٧,٤٪) تعرضوا لاستغلال الشبكات اللاسلكية، وهي جميعًا هجمات نجحت في اختراق شبكات الحاسب الآلي بشكل أساسي، لكن هناك تهديدات رئيسة تشكّل السواد الأعظم من التهديدات الرقميّة لشبكات الحاسب الآلي، هي: الهجوم الإلكتروني، وهجمات الهندسة الاجتماعيّة.

٧-٢-١ الهجوم الإلكتروني

غدا الهجوم الإلكتروني سهلًا ما دام أن معظم أجهزة الكمبيوتر قد ربطت بالإنترنت أو بالشبكات الخاصة، بالإضافة إلى ذلك فإنّ الأجهزة المحمولة والمرتبطة بالإنترنت قد زادت أعدادها بصورة مطّردة. فهذه البيئة الإلكترونيّة المتنامية تسهل عمليّة الهجوم من بُعد، وتصعِّب من عمليّة رصد مصادرها، والزيادة المتلاحقة في عدد الأجهزة المرتبطة بالشبكات تعني أيضًا زيادة الأهداف الجاذبة والمتاحة للهجوم(أو الاختراق).

يعرف الاختراق بأنه: "القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف" وهذا الفصل يقدّم فكرة شاملة عن الهجوم الإلكتروني، موضّحًا أنواع المهاجمين، وأهداف المهاجم، ومراحل الهجوم المتبعة غالبًا، والثغرات المستغلة، ومعظم التركيز هنا هو على الهجوم باستخدام الشبكات، لكن هذا لا يعني أنّ كل الهجمات الإلكترونيّة تتم عبر الشبكة، فهناك إمكانية لتعرّض الأنظمة المعلوماتيّة لهجوم داخلي لا يخلو عادةً من عمليّات خيانة أو تواطؤ داخلي، ومن الأمثلة على ذلك نشر فيروس تدميري داخليًّا بطريقة يدويّة.

١- Computer Security Institute(CSI) Survey(2011), The 15th Annual Computer Crime and Security Survey.

٧-٢-١-١ أنواع المهاجمين

يمكن تصنيف المهاجمين بعدّة طُرُق مختلفة، ومن هذه الطرق، العلاقة بين المهاجم والهدف. فيمكن أن يكون الهجوم داخليًّا أو خارجيًّا، وتشير الدراسات إلى أنّ الهجوم الداخلي هو الأكثر شيوعًا وأهمية خلال السنوات الماضية [١] ، والسبب في ذلك هو أن لدى الأفراد الذين يعملون داخل المنشأة نفسها بعض الميزات التي يستغلونها، ويمكنها زيادة احتمال نجاح الهجوم، مثل ثقة المنشأة في ذلك الموظف، وعلمه بكيفية عمل النظم داخل المنشأة وأنواع الدفاعات المستخدمة. لكن مع وجود الربط الكلّي بالشبكات في عالم اليوم، أصبح الهجوم الخارجي أكثر شيوعا من أي وقت مضى.

يمكن أيضًا تصنيف المهاجمين إلى: هواة أو محترفين. فكثير من الناس قد ينظرون إلى المهاجم نظرة تقليديّة على أنه الشخص في عمر المراهقة («هاكر» أو «أطفال الشفرات») الذين لديهم وقت فراغ كبير، وهذا النوع النمطي من المخترقين تم الترويج له من خلال الشخصيات الروائية في الأفلام، وكذلك الشخصيات الحقيقية التي ألقي القبض عليها بهذا الخصوص. فعلى سبيل المثال، قبض في مايو عام ٢٠٠٤م على ذلك المراهق ذي الثمانية عشر عامًا المعروف باسم «سفين جاشان». وقد أدين وعوقب بأن يكتب عن الكيفية التي تعمل بها أكثر أنواع الديدان خطورة في العام ٢٠٠٤م، بما في ذلك ديدان(Sassar and Netsky)، التي تشكل(٧٠٪) من أنواع الديدان التي انتشرت في العالم في النصف الأول من العام ٢٠٠٤م [٢] .

٧-٢-١-٢ أهداف المهاجمين

يعتمد الهدف من الهجوم الإلكتروني على نوعية المهاجم نفسه، ولأن هناك عدة أنواع مختلفة من المهاجمين، فيمكن أن يكون الهدف كل شيء تقريبًا، بدءًا من التسلية والشهرة، و وصولًا إلى الابتزاز والحصول على الأرباح و التجسّس والانتقام، و انتهاءً بالتعدّي على الأجندة السياسية. فالمهاجم المراهق عادة ما يُعتقد بأن هدفه الشهرة والتسلية. فعلى سبيل المثال- وبحسب تقارير وسائل الإعلام- كانت أغراض(الهاكر) الشاب «سفين جاشان» في

١- CERT Site: http://www.cert.org

٢- Bidgoli, Hossein(2006b), "Handbook of Information Security", Volume 2, Part 1.

الأساس حب الاستطلاع، وقد يكون حسن النية.

إنّ الهـدف العام الشائع هو الهجوم على الخصوصية، أو سرقـة البيانات السِّريّة. وهذا واضح من خلال تصاعد وتيرة هجوم برامج التجسّس وسرقة البيانات السِّريّة (انظر الفصل السادس: موضوع: برامج التجسّس وطرق مكافحتها).

٧-٢-١-٣ مراحل الهجوم

عادة ما يتم الهجوم الإلكتروني عبر سلسلة من الخطوات شبيهة بخطوات الهجوم المكاني. فالخطـوة الأولى في الهجوم، هي المناورة لجمع المعلومـات الاستخباراتية الضرورية، بهدف التجهيز للهجوم الفعلـي، والخطوة الثانية هي مرحلة الهجوم الفعلي، الذي قد يكون له عدة وسائـل مختلفة، وأثناء عمليّة الهجـوم وبعدها، قد يحاول المهاجم اتخـاذ بعض الإجراءات لإزالة آثاره لتجنب رصده.

١. مرحلة المناورة

إذا كان المهاجم يود تعريض نظام حاسـب آلي بعينه للاختراق، فمن الطبيعي أن يجهز لعملية الهجوم عن طريق معرفة كل شـيء ممكن عن الهدف، وقد تكشف له مرحلة المناورة جملة من المعلومات، مثل: أسماء الحسابات، والعناوين، ونظم التشغيل، أو حتى كلمات السر التي من شأنها أن تزيد من احتمالات نجاح الهجوم. وفضلًا عن ذلك، فلا ينظر إلى معظم تقنيات المناورة على أنها غير قانونية أو ماكرة، وقد تتم دون أن تكون هناك مخاطرة كبيرة لتنبيه الهدف المحتمل.

هناك العديد من تقنيات المناورة التي يمكن استخدامها، وعادةً لا يتبع المهاجمون الخطوات نفسها بالترتيب نفسه في كل مناورة، لكن هناك خطوتان عامتان يتم عملهما بالترتيب لاكتشاف أكبر قدر من المعلومات عن الهدف المحتمل، وهما: تتبع الأثر، ومسح أمكانية الاختراق.

أ. تتبع الأثر

الخطوة الأولى في المنـاورة (أو الاكتشـاف) تسمّى تتبـع الأثر (أو البصمـة أو الترقيم) (Footprinting). وتتوافـر كميّـة كبيرة مـن المعلومات جاهزة على شبكـة الإنترنت على

شكل قواعد بيانات، يمكـن استخدامها لكشف بعض المعلومات المهمة، ويمكن الحصول على معلومات من قواعد البيانات تلك بوساطة عدد من الوسائل مثل،(nslookup) أو(dig)[1].

تحتوي قواعـد المعلومات الخاصـة بالاستفسار معلومات تتعلق بعناويـن الإنترنت(IP)، وتسجيـل أسمـاء النطاقـات(Domains)، اتصالات الأفـراد. وتسجّل أسمـاء النطاقات مثل(www.mycompany.com) عن طريق مركز معلومات الإنترنت(Internet Network Information Center-InterNIC) وهو اتحاد مالي مكون من عدة شركات، بالإضافة إلى حكومة الولايات المتحدة الأمريكية[2]، وبخصوص اسم النطاق، فإنّ قاعدة بيانات أسماء النطاقات يمكن أن توفر اسم الجهة المسجلة، والعنوان، وأجهزة الخادمات الخاصة بالنطاق، ومعلومات الاتصال.

أمّا المعلومات الخاصة بمـدى تغطية عنـوان IP، فتوفر قاعدة تسجيـل أرقام الإنترنت الأمريكية(American Registry for Internet Numbers-ARIN) آلية الحصول على جهة الاتصال وتسجيل المعلومات الخاصة بالموارد، مثل عناوين IP، وأرقام الاتصال المستقلة للمؤسسات المسجلة في الأمريكتين، ويمكن تحديد عناوين IP الأوربية عن طريق مركز تنسيق الشبكة الأوربية(RIPE NCC) وبالمثل يمكن تحديـد عناوين IP في آسيا عن طريق مركز شبكة معلومات آسيا والباسفيك(APNIC).

من ضمن قواعد البيانات المهمة الأخرى نظام اسم النطاق(Domain Name System-DNS) وهذا النطاق عبارة عن هرم من أجهزة الخوادم المستخدمة لربط أسماء النطاقات، وتحديد عناوين IP، وخادمات البريد، ويمتد الهرم مـن أجهزة الخادم(DNS) الأساسيّة حتى أجهزة الخوادم الخاصة بالمؤسسات الفردية والشبكات. وتحتوي أجهزة الخادم(DNS) معلومات عن أجهزة الخوادم الأخرى ذات المستوى الأقل، وعناوين IP للاستضافة الفردية.

ب. مسح إمكانية الاختراق

عن طريق استخدام مسح الشبكة العام(Scanning)، يمكن للمهاجم اكتشاف معلومات

١- Bidgoli, Hossein(2006b), "Handbook of Information Security", Volume 2, Part 1

٢- المرجع السابق.

عامـة كثيرة عن الهدف المحتمـل، مثل عناويـن الاستضافـة، وبُنية (طوبوغرافيا) الشبكة، والأبواب المفتوحة، وأنظمة التشغيـل. والخطوة الآتية في المناورة، هـي المسح بغرض معرفة نقاط الضعف للاختراق التي قد تستغل في الهجوم. ومن الممكن عمل المسح يدويًّا لمعرفة نقاط الضعف، لكن ذلك سيأخذ وقتًا كبيرًا للتأكد من وجود كثير من الثغرات في كثير من الأجهزة. ويتوافر العديد من الماسحات الأوتوماتيكيـة التي عادة ما يستخدمها مديرو الأنظمة لتقييم أمان الشبكة الداخليّة، لكنها قد تستغل لإجراء المسح لأغراض الاختراق[1].

أدوات المسح

يتوافر كثير من أدوات المسح التجارية والمجانية، ويستخدم عدد منها لأغراض مشروعة عن طريق مديري الأنظمة والشبكات، ومن الأمثلة على ذلك ماسحة الإنترنت الأمنيّة (Internet Security Scan-ISS) وأداة التحليل الأمني لتدقيق البيانات (Security Analysis Tool for Auditing Network-SATAN) التـي عـادةً ما يستخدمها مديـرو الشبكات لمسح الشبكة، لمعرفة الخلل فيها وإصلاحه، لكنها قد تستغل لأغراض الاختراق[2]، ومن الأمثلة الأخرى لهذه الأدوات المجانيّة هي أداة (CyberKit) وشيوبس، وأداة شيوبس. هي أداة عامة سهلة الاستخدام تقوم بعمل خريطة الشبكة بطريقة آلية، حيث ترسم بُنية (طوبوغرافيا) الشبكة بناء على المستضيفين المكتشفين وعلى المسافـات، وكذلك تكشف عن الخدمات النشطة عن طريق المسح والتعرّف إلى أنظمة التشغيل.

من أمثلة الأدوات التجارية (NetScanTools Pro)، التي تشتمل على: أداة تتبع المسار، وماسحة الشبكة، ونظام التعرف (Whois)، ونظام (Nslookup)، وصلاحية عنوان البريد الإلكتروني، والتعرّف إلى نظام التشغيل.

أنواع الثغرات

هناك كثير من أنواع الثغرات التي تبحث عنها الماسحات، ومنها:

- نقاط الضعف التلقائية في التهيئة: يوجد في أنظمة التشغيل والبرامج التطبيقيّة كثير

١- البداينة، ذياب(٢٠٠٦)، «الأمن وحرب المعلومات».

٢- المرجع السابق.

من الحسابات وكلمات المرور التلقائية، وهذه تساعد على تركيب النظام أو تبسيط إجراءات حلّ المشكلات في حال فقدان كلمات المرور، ومن المفترض أن يتم تغيير كلمات المرور التلقائية، لكن في بعض الأحيان تُهمل أو تُنسى، ويبحث المهاجمون عن وجود تهيئة تلقائية؛ لأنّها توفر طريقة سهلة لاختراق النظام.

- أخطاء التهيئة: تتطلب تهيئة أجهزة الشبكات خبرة جيدة من أجل عمل التهيئة بصورة آمنة. ومن المعروف أن إعدادات تهيئة غير آمنة يمكن أن تضعف أيًّا من وسائل الأمان لأجهزة الشبكة، وكمثال لذلك، فإنّ التهيئة غير الآمنة للجدار الناري (انظر الفصل السابع: أمن شبكات الحاسب الآلي، جدران النار)، قد تتسبب في السماح بدخول رزم بيانات تسهل عمليّة الاختراق.
- الثغرات الشهيرة في أنظمة التشغيل والبرامج التطبيقيّة: يُكشف عن ثغرات جديدة دوريًّا في أنظمة التشغيل والتطبيقات، وتُنشر هذه الثغرات ويُعرّف بها بوساطة المورّدين مع توفير الرقع (Patches) اللازمة لسد هذه الثغرات. لكن هذا يتطلب قدرًا كبيرًا من الوقت والجهد من قبل الموردين للإلمام بنشرات الأمان والترقيع. والمدّة ما بين تاريخ نشر الثغرات الأمنيّة وتركيب الرُّقع يتيح فرصة للمهاجمين لاستغلال هذه الثغرات.

٢. مرحلة الهجوم الفعلي

يمكن أن تتخذ مرحلة الهجوم الفعلي عدّة أشكال مختلفة، وتخدم أهدافًا متنوعة، ومن الأمثلة على ذلك: سرقة البيانات السِّريّة، والتلاعب بتكاملية البيانات، والدخول غير المصرّح به للنظام. وهذه الأنواع المحدّدة للهجوم يمكن أن توجه نحو أهداف محدّدة بعينها، أو نحو البُنية التحتية العامة للشبكة، وفي كثير من الحالات تكون الهجمات العشوائيّة الواسعة النطاق ذات أثر واسع في تعطيل أجهزة الحاسب الآلي والشبكات، حتى وإن كان ذلك ليس هو المقصود، وفي هذه الحالة، تكون لها آثار بعيدة المدى؛ لأنّها جرت عن طريق الشبكة التي يرتبط بها عدد كبير من الأهداف.

من الأنواع الرئيسة للهجوم الفعلي: اختطاف الجلسات، والهجوم على كلمات المرور،

والاستغلال، وهجمات الهندسة الاجتماعيّة ، والهجوم بحصان طروادة، وأجهزة التنصت، والتجسّس الإعلاني، وزرع الفيروسات والديدان، والإغراق برسائل البريد الإلكتروني، ومنع الخدمة(DoS). وهذه القائمــة ليست حصرية، لكنها فقط أمثلة لأنواع الهجوم المهمة التي تجري حاليًا.

٧-٢-٢ هجمات الهندسة الاجتماعيّة

الهندسة الاجتماعيّة هي عمليّة استخدام المهارات الاجتماعيّة لإقناع الأشخاص بالإفصاح عن المعلومات السِّريّة[١]، وعلى المستوى المادي يمكن تعريفها بأنها: «انتحال شخصيات المهندسين، وفنيي الصيانة، ومن في حكمهــم؛ للدخول إلى أماكن مهمة وحساسة، على أن لديهم أعمالًا مركزيّة تتطلب وجودهم أو دخولهم، وهم في الحقيقة لهم أغراض أخرى غير ذلك»[٢].

يمكن تنفيذ هجمات الهندسة الاجتماعيّة بعدة طُرُق حسب طبيعة الضحية وحسب الوسائل المتاحة للمهاجم، ومن أشهر هذه الطرق رسائل الاصطياد الإلكتروني [٣]، التي يتم فيها إقناع الضحية بأن المهاجم هو منشأة أو جهة(مصرف مثلًا) شرعية مصرّح لها، ومن ثم الإيقاع به لتزويد المهاجم بالمعلومات السِّريّــة الخاصة به، مثل: اسم المستخدم، وكلمة المرور، ورقم الهُويّة، ورقم بطاقة الائتمان. ويستغل مرسلو رسائل الاصطياد الإلكتروني الجانب الاجتماعي، بالإضافة إلى الجانب الفني في عمليّة الاحتيال على الضحية، من خلال اختيار فكرة رسالة الاصطياد بما يلامس اهتمامات الضحية، ثم وضعها في قالب فني مخادع يولّد القناعة لديها بأنها رسائل حقيقية من مصادر موثوقة.

ثمة طريقة ثانية لهجمات الهندسة الاجتماعيّة يتم فيهــا إقناع الضحية بأن المهاجم هو شخصــ أهم منه وأعلى منه مرتبــة في المنشأة أو في المجتمع، من أجـل كسب ثقته، ومن ثم الحصول على معلوماته السِّريّة واستخدامها بطريقة غــير شرعية. وعادة ما تستخدم هذه الطريقة في هجمات الهندســة الاجتماعيّة الداخليّة التي تتم داخـل المنشأة. ويمكن تقسيم الهجمة الواحدة من هذا النوع إلى عــدّة هجمات منفصلة عن بعضها البعض من أجل عدم

١- Withman, M. and Mattord, H.(2005), “Principles of Information Security”.

٢- البداينة، ذياب(٢٠٠٦)، «الأمن وحرب المعلومات».

٣ - الغثبر، خالد بن سليمان و بن هيشة، سليمان بن عبدالعزيز(٢٠٠٩)، «الاصطياد الإلكتروني: الأساليب والإجراءات المضادة».

إثارة الانتباه، بحيث يتم الحصول من كل هجمة على معلومات سرية منفصلة، ثم تجمع لاحقًا للحصول على معلومات سرية متكاملة يمكن استخدامها في هجوم متكامل. ومن الأمثلة على ذلك أن يتّصل المهاجم بمأمور السنترال ثم سؤاله عن اسم مدير المنشأة بطريقة ذكية، وبعد ذلك يستخدم هذه المعلومة لكسب ثقة أشخاص آخرين داخل المنشأة، يُظهر لهم فيها أنه يعرف مدير المنشأة، وأنه على اتصال به، ومن ثم الحصول منهم على معلومات إضافية، مثل بريده الإلكتروني، أو رقم هاتفه، أو اهتماماته التي يمكن أن يستغلها لصياغة رسالة اصطياد إلكتروني لمدير المنشأة، أو لأيّ شخص آخر داخلها.

٧-٣ التدابير الأمنيّة العامة لأمن شبكات الحاسب الآلي

يعتمد مستوى درجة الحماية اللازمة لشبكة الحاسب الآلي على حساسية المعلومات التي تنقلها وأهميتها، والسبب في ذلك هو أن تكاليف الحماية والقيود المفروضة على المستخدمين تزداد بازدياد مستوى الحماية المطبق. ومن هذا المنطلق لا بدّ من الموازنة بين مستوى الحماية وتكاليف تطبيقها، وكذلك مستوى التقييد الناتج على المستخدمين، وعلى موارد الشبكة المشتركة. وبشكل عام، هناك بعض الإجراءات التي تساعد على المحافظة على أمن شبكات الحاسب الآلي، ويجب تطبيقها بشكل عام، وهي:

١. تطبيق سياسة أمن معلومات المنشأة وتفعيلها ومراجعتها، ومن ذلك- على سبيل المثال- سياسة كلمات المرور(انظر الفصل الخامس: موضوع: سياسات أمن المعلومات).

٢. التدريب المتقَن للمستخدمين على التعامل مع إجراءات وبرامج أمن المعلومات.

٣. التأكد من أمن المعدّات وصعوبة الوصول إليها من غير المخوّلين.

٤. تشفير البيانات عند الحاجة .

٥. تزويد المستخدمين بأجهزة لا تحتوي محرّكات أقراص مرنة أو مضغوطة، أو حتى أقراصًا صلبة قدر الإمكان، وكخيار آخر إبطال عمل هذه المحرّكات وقفل جميع منافذ الاتصال غير الضرورية.

٦. تفعيل خدمات تسجيل جميع العمليّات، التي يتم إجراؤها على الأجهزة الرئيسة وقواعد البيانات(Log Files) للرجوع إليها عند الضرورة.

٧. إعطاء أذونات(Permissions) للمستخدمين للوصول للبيانات والمعدّات، كل حسب طبيعة عمله، وفي هذه الحالة يجب مشاركة البيانات والمعدّات للسماح للآخرين باستخدامها.

٨. تزويد المستخدمين بحقوق(Rights) تحدّد الأنشطة والعمليّات المسموح لهم بإجرائها على النظام.

٩. التنقيح(الفلترة) باستخدام العنوان الفيزيائي لبطاقة الشبكة(MAC Address) كآلية لتحديد أو توفير الوصول إلى الشبكة، على اعتبار أن العناوين الفيزيائية مسجّلة ضمن المكوّنات الإلكترونيّة لبطاقة الشبكة و من ثَمَّ يستحيل تغييرها من قبل المستخدمين العاديين.

١٠. حماية وسائط نقل المعلومات من كابلات وأجهزة ربط، ولأهمية ذلك فقد أفردنا له موضوعًا مستقلًا.

١١. استخدام جدران النار(أو جدران الحماية) ولأهمية ذلك فقد أفردنا له موضوعًا مستقلًا.

١٢. استخدام الشبكات الخاصة الافتراضيّة(VPNs) ولأهمية ذلك فقد أفردنا له موضوعًا مستقلًا.

١٣. استخدام الشبكات المحلية الافتراضيّة(VLANs) ولأهمية ذلك فقد أفردنا له موضوعًا مستقلًا.

١٤. تأمين خوادم ومواقع الإنترنت، ولأهمية ذلك فقد أفردنا له موضوعًا مستقلًا.

٧-٤ أمن وسائط نقل المعلومات

إنّ أحد أهم أجزاء شبكات الحاسب الآلي التي يجب أخذها بعين الاعتبار عند تطبيق وسائل أمن المعلومات وتقنياتها، هي وسائط نقل البيانات من أجهزة ربط وكابلات، ومن أهم

ما يوفر الحماية لهذه المكوّنات ما يلي:

- وضع جميع الكابلات داخل مجارٍ خاصّة بها، (أو دكتات) مغلقة تحميها من الوصول إليها، ومن وصل أي أدوات بها قد تلتقط المعلومات من خلالها، وتوفر لها أيضًا الحماية من التلف جراء العوامل الطبيعية أو القوارض.
- استخدام كبائن مُحكمة الغلق لتجميع الكابلات بها، ويستحسن كثيرًا وضع غرفة تحكّم (أو كبينه في حالة الأحجام الصغيرة) خاصّة بكل جزء من المبنى (كل دور مثلًا)، و وصل هذه الغرف بغرفة التحكّم الرئيسة (أو مركز البيانات (Data Center) مباشرة) بخطوط ألياف بصرية، تضمن توفير سعات نقل بيانات عالية، وتقلل عدد الكابلات المستخدمة بين الكبائن.
- استخدام كابلات الألياف البصرية للربط بين المباني وفي المناطق المهمة والحسّاسة؛ لما تتميز به من عدم إمكانية تداخل الإشارات، وعدم القدرة على التقاط البيانات المارّة بها.
- عدم التمديد في الأماكن العامة في المنشأة أو خارج المباني إلا عند الضرورة القصوى.

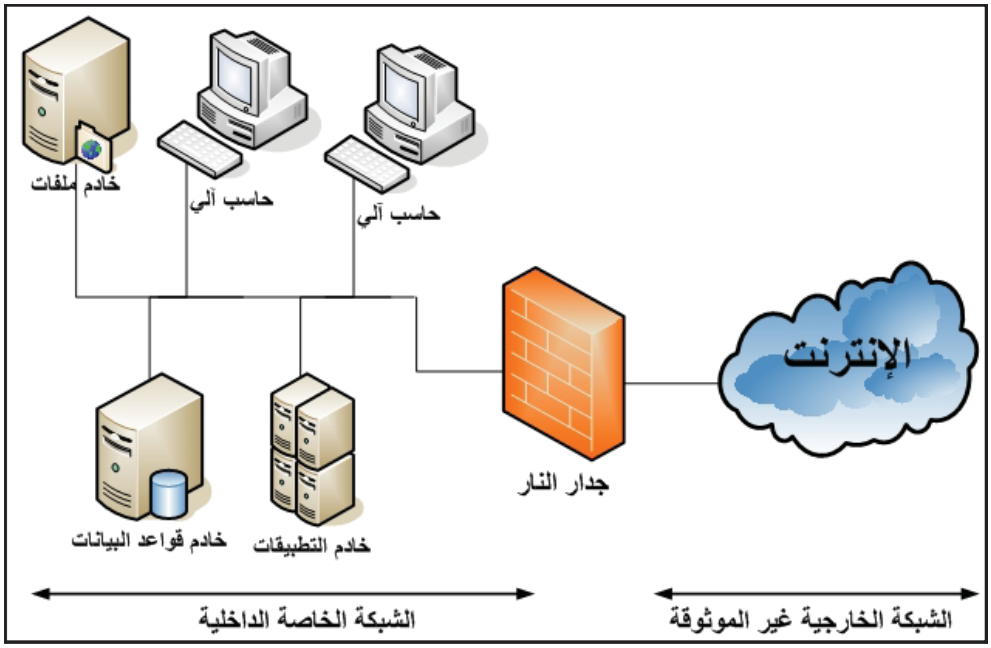
٧-٥ جدار النار (Firewall)

عندما تكون شبكة الحاسب الآلي الخاصة بالمنشأة (أو الحاسب الآلي الخاص) متصلة بشبكة الإنترنت، أو أيّ شبكة خارجية، فإنّ ثمة طريقين للاتصال: أحدهما يصل من الخارج إلى شبكة المنشأة، والآخر من شبكة المنشأة إلى الخارج. ولمنع أيّ وصول غير مصرّح به لشبكة المنشأة فيجب استخدام أداة منع خاصّة تسمّى «جدار النار»، أو «جدار الحماية». وجدار النار إمّا أن يكون جهازًا مستقلًا خاصًا يصنع لهذا الغرض وبه برامجه الخاصة به، أو يكون برنامجًا يُركّب على أجهزة الحاسب الآلي العاديّة.

٧-٥-١ أساسيات عمل جدار النار

يعمل جدار النار كمصفٍ أو منقحٍ لرزم (Packets) البيانات الداخلة والخارجة من شبكة المنشأة وإليها، أي أنه يكوّن طبقة عازلة بين شبكة المنشأة والعالم الخارجي. انظر الشكل (٧-١).

تمر جميع رزم البيانات الداخلة والخارجة من شبكة المنشأة وإليها عبر جدار النار ليصفّيها ويسمح فقط للرزم أو الأنشطة المصرّح لها بالمرور. هذه التصفية تكون على عدة أشكال، فإمّا أن تكون على أساس نوع البيانات فمثلًا قد يمنع أيّ رزمة من النوع الناقل للملفات(FTP) من المرور، أو تكون على أساس النوع والتاريخ والوقت، فمثلًا قد يمنع أيّ رزمة من نوع(HTTP) أثناء أوقات الدوام الرسمي للمنشأة، أو تكون على أساس أيّ تصفية أخرى حسب الحاجة.

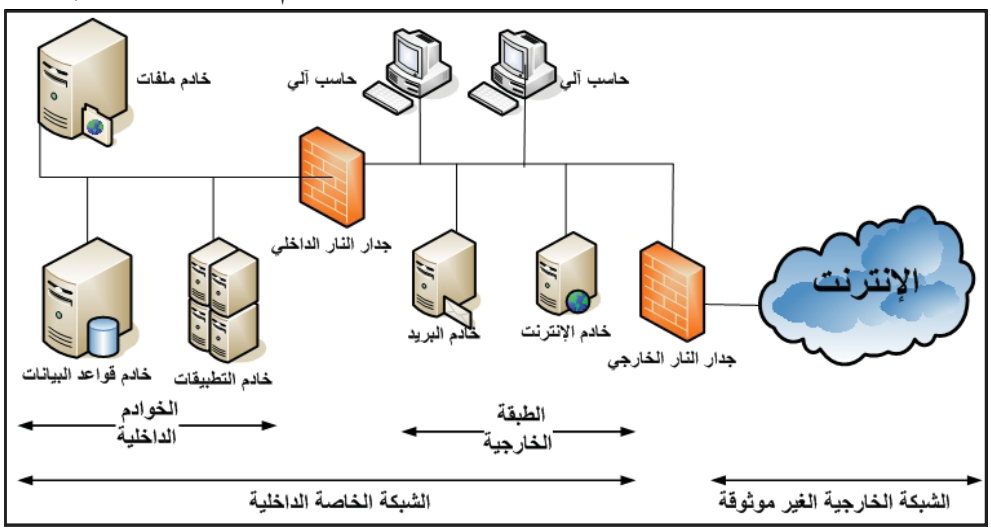


الشكل(٧-١): أساسيّات عمل جدار النار

إنّ جدار النار الموضّح في الشكل أعلاه يكون مناسبًا للشبكات التي تكون فيها الأخطار المتوقّعة على المعلومات الخارجيّة(الإنترنت مثلًا) لكن في التصاميم الحديثة لشبكات الحاسب الآلي لا يكون ذلك كافيًا، بل يجب أن يوضع جدار نار آخر كطبقة عازلة بين أجهزة الخوادم الرئيسة والشبكة الداخليّة لمنع الأخطار الداخليّة أيضًا. انظر الشكل(٧-٢).

يوضح الشكل(٧-٢) كيف يمكن عزل أجهزة الخوادم الرئيسة عن الشبكة الداخليّة، وهو ما يساعد في حماية هذه الأجهزة من أخطاء المستخدمين أو من رزم البيانات الداخليّة الضارّة. وتوضح الدراسات الحديثة أنّ(٧٠ – ٨٠ ٪) من المخاطر التي تتعرض لها الأجهزة

الرئيسة تكون من المستخدمين الداخليين الذين عادة ما يكون لهم صلاحية الدخول إليها.



الشكل(٧-٢): استخدام طبقتين من جدران النار لمزيد من الحماية

هنا تظهر جليًّا أهميّة جدار النار، حيث إنّ لديه القدرة على تصفية رُزم البيانات القادمة من المستخدمين المصرّح لهم، ومنع الرُّزم التي قد يكون فيها خطر على الأجهزة الرئيسة أو المعلومات المهمة، وتظهر هنا أيضًا أهميّة عمل التهيئة والتعريفات اللازمة لجدار النار بالشكل الصحيح، وإلا سيؤدي ذلك إلى وجود ثغرات أمنيّة. ومن المعروف أن عمل تهيئة خاطئة لجدار النار قد يكون له أثر سلبي أكثر مما لو لم يكن هناك جدار نار أساسًا، لأن ذلك يكون بمنزلة تضليل لمديري الشبكات بالاعتماد على جدار النار، بينما هو في الحقيقة لا يقدّم الحماية الكافية، أو بعبارة أخرى يعطى حسًّا أمنيًّا خاطئًا.

تعتمد جدران النار في عملها على جداول التنقيح(الفلترة) التي يتم تخزينها داخل جدار النار، ويُسمح لرُزم البيانات بالمرور من عدمه بعد الرجوع لهذه الجداول، ومعرفة الرُّزم المسموح بها، والرُّزم غير المسموح بها، وهناك نوعان من عمليّة التنقيح:

- التنقيح الإيجابي: يسمح لرُزم البيانات المطابقة للشروط المدوّنة في جدول التنقيح بالمرور، وتُمنع جميع الرُّزم الأخرى.
- التنقيح السلبي: تُمنع رزم البيانات المطابقة للشروط المدوّنة في جدول التنقيح من

المرور، ويسمح لجميع الرُّزم الأخرى.

يمكن أن يطبّق أيّ من عمليّات التنقيح هذه على كلا الاتجاهين من الشبكة الداخليّة وإليها، وسواءً أكان التنقيح سلبيًّا أم إيجابيًّا فهناك عدة طُرُق للتنقيح من أشهرها[1]:

١. التنقيح باستخدام العناوين(Address Filtering): يسمح لرزم البيانات باستخدام جداول تنقيح العناوين، بحيث تحتوي هذه الجداول العناوين المسموح بالإرسال إليها أو المسموح بالاستقبال منها، وهذه الطريقة وحدها لا توفر حماية جيدة بسبب كثرة العناوين التي تتطلب تخزين جداول كبيرة الحجم، وكذلك تتطلب تحديثًا مستمرًا لهذه الجداول.

٢. التنقيح باستخدام المنافذ(Port Filtering): وهذه الطريقة من أشهر طُرُق التنقيح وأكثرها انتشارًا، وفيها يسمح لرزم البيانات بالمرور بناءً على رقم المنفذ المستخدم. فعلى سبيل المثال يستخدم بروتوكول نقل الملفّات(FTP) المنفذين رقم(٢٠، ٢١)، ويمكن السيطرة على هذه النوعية من الرزم بقفل هذه المنافذ، وينتج عن ذلك عدم القدرة على نقل الملفّات. وكذلك تستخدم رُزم تصفح الإنترنت(HTTP) المنفذ رقم(٨٠)، ويمكن أيضًا التحكّم بها من خلال قفل هذا المنفذ.

٣. التنقيح باستخدام النطاق(Domain Filtering) وتستخدم هذه الطريقة لقفل النطاقات غير المرغوب فيها، ومنعها من الوصول إلى الشبكة الداخليّة.

٧-٥-٢ مميزات جدار النار وعيوبه

تتلخّص مميزات الجدار الناري فيما يلي:

- طريقة حماية جيدة لشبكات الحاسب الآلي ومصادر المعلومات المهمة في حالة تهيئتها ومراقبتها بالشكل الصحيح.
- يمكن أن يحمي جدار ناريّ واحد عددًا كبيرًا من الأجهزة خلفه، وبذا يمكن تقليل تكلفة الحماية.
- يشكّل جدار النار نقطة تحكم مركزيّة يمكن التحكّم فيها بسهولة.

١- وليام ستولينج(١٤٣٢)، «أساسيات أمن الشبكات: تطبيقات ومعايير»، كتاب مترجم إلى اللغة العربية.

- وتتلخص عيوبه فيما يلي:
- لا بدّ من تهيئته وإدارته ومراقبته من قبل أشخاص مدرَّبين جيّدًا.
- تشكل التهيئة الخاطئة لجدار النار ثغرة أمنيّة كبيرة.
- يؤدّي استخدام جدار النار إلى تخفيض سرعة أداء الشبكة عند تهيئته بشكل معقّد في بعض الحالات.

تجدر الإشارة إلى ضرورة عدم الاعتماد على جدار النار لعمل الحماية الكاملة للشبكات. فجدران النار لا تؤدي الحماية الكاملة لكل شيء. فعلى سبيل المثال، فإنّ استخدام جدران النار لا يلغي الحاجة إلى استخدام برامج مكافحة الفيروسات.

٧-٦ الشبكة الخاصة الافتراضيّة (VPN)

قبل استغلال شبكة الإنترنت في إيجاد خطوط اتصال خاصّة بالمنشآت، كانت الطريقة المثلى للحصول على خطوط اتصال لنقل البيانات هي استخدام الخطوط المستأجرة(Leased Lines). وهذه الخطوط لا تتوافر بسرعات عالية، وتُعدُّ تكلفتها عالية جدًّا مقارنة بتكلفة الاتصال بشبكة الإنترنت.

عندما انتشر استخدام شبكة الإنترنت، ظهرت إمكانية استخدام هذه الشبكة كناقل للمعلومات الخاصة بالمنشآت، وظهرت فكرة إنشاء خطوط خاصّة على هذه الشبكة العملاقة، أو ما يسمّى بالشبكة الخاصة الافتراضيّة(Virtual Private Network-VPN). فقد تحتاج بعض المنشآت إلى إيجاد طريقة مناسبة لربط فروعها بعضها ببعض، ومن الخيارات المطروحة استخدام شبكة الإنترنت؛ لما تتميّز به من انخفاض التكلفة، وإمكانية ربط الفروع حتى ولو كانت منتشرة في أكثر من قارّة. لكن السؤال الذي يُطرح هنا: هل يمكن الحصول على خطوط اتصال تظهر كأنها خاصّة بالمنشأة رغم أنها في حقيقتها مبنية على شبكة الإنترنت، وتتميز بالديمومة والآمان؟ والجواب هو استخدام الشبكة الخاصة الافتراضيّة.

١-٦-٧ ماهيّة الشبكة الخاصّة الافتراضيّة وطريقة عملها

إنّ أفضل طريقة لتعريف الشبكة الخاصة الافتراضيّة هي تحليل كل كلمة بشكل منفصل،

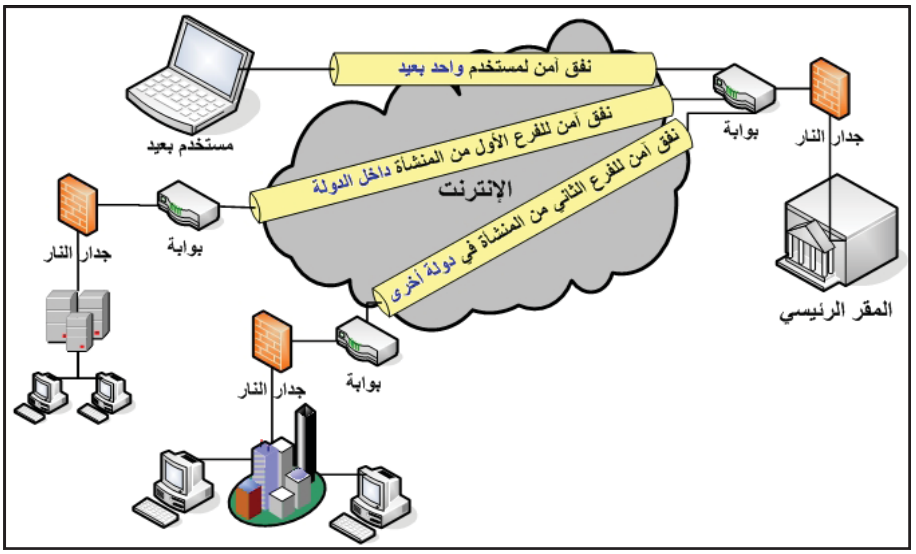
وعلى هذا، عرف بيدجولي[1] الشبكة الخاصة الافتراضيّة(VPN) بأنها: "شبكة خاصّة مبنيّة ضمن إطار بُنية الشبكة العامة، مثل شبكة الإنترنت العالمية" ويعرّفها آخرون بأنّها: "الشبكة التي تسمح لشبكتين خاصّتين أو أكثر بالارتباط بعضها مع بعض من خلال شبكة عامة يمكن الوصول إليها". وتُعدُّ الميزة الأساسيّة للشبكة الخاصة الافتراضيّة هي استخدامها للشبكات العامة، مثل الإنترنت، أكثر من استخدامها للخطوط الخاصة المؤجرة أو العالية الكلفة.

تقوم فكرة الشبكات الخاصّة الافتراضيّة على إنشاء خطوط اتصال على شبكة الإنترنت(أو شبكة عامة كشبكة (Multi-Protocol Label Switching-MPLS) تظهر كأنها خاصّة بالمنشأة وتعمل كشبكة نقل بيانـات منفصلة تمامًا، ويمكن أن تخدم فروع المنشأة في مناطق جغرافية متباعدة، سواءً أكانت داخل البلاد أم على مستوى العالم، بحيث تكون خاصّة بالمنشأة، ولا يستطيع أحد أو طرف آخر استخدامها رغم أنها في حقيقة الأمر مبنية على شبكة الإنترنت.

يقوم عمل الشبكة الخاصة الافتراضيّة على بنـاء "نفق"(VPN Tunnel) خاص بين فروع المنشأة، كما هو موضح في الشكل(٧-٣). يجري تبادل المعلومات من خلال هذا النفق، والنفق هو آلية لتغليف البيانات الخاصة بالمنشأة، وجعلها تسير في مسار محدّد(نفق) ضمن شبكـة الإنترنت، بحيث تكـون هذه البيانات غير مرئيـة الآخرين. وتتكـوّن الشبكة الخاصة الافتراضيّة من ثلاثة مكوّنات رئيسة هي:

- جهاز البوابة(Gateway) الذي يربط طرفي النفق بالفروع.
- النفق الذي تنقل من خلاله البيانات، ويشمل البرمجيات والبروتوكولات اللازمة.
- جدار النار لحجب البيانات غير المرغوب فيها عن المرور خلال النفق.

١- Bidgoli, Hossein(2006c), "Handbook of Information Security", Volume 3, Part 3.



الشكل (٧-٣): الشبكة الخاصة الافتراضيّة (VPN)

٧-٦-٢ مميزات الشبكات الخاصة الافتراضيّة وعيوبها

تتلخّص مميزات الشبكات الخاصة الافتراضيّة فيما يلي:

- إمكانية التوسّع المستقبلي بسهولة (Scalability).
- سهولة إضافة المستخدمين وحذفهم.
- قليلة الكلفة مقارنة بالخطوط المستأجرة.
- إمكانية التعديل والنقل للشبكة، وسهولة إضافة الفروع وحذفها (Mobility).
- تحقيق حدّ مقبول من أمن المعلومات، من خلال توفير الخصوصية للخطوط، مقارنة بالإنترنت.

وتتلخص عيوبها فيما يلي:

- تحتاج إلى تطبيق معايير أمنيّة أكثر صرامة.
- ما زال هناك بعض المعايير لم تصل إلى الدرجة القياسيّة عالميًّا.
- يتأثر أداؤها بمدى بالضغط الحاصل على شبكة الإنترنت، الذي لا يمكن التنبؤ به.

٧-٦-٣ أمن الشبكات الخاصة الافتراضيّة

لقد حلّت الشبكات الافتراضيّة الخاصّة مشكلة إيجاد خطوط اتصال لنقل البيانات، تكون

زهيدة الثمن، وتغطّي أي مكان في العالم تقريبًا، وكذلك فإنها تضمن جزءًا من الخصوصية لهذه الخطوط، فلا يمكن استخدامها من قبل الآخرين. ولكن طالما أن الحامل الحقيقي لهذه البيانات هي شبكة الإنترنت، فإنها تُعدُّ طريقة غير آمنة لنقل البيانات، ويجب توفير الحماية اللازمة.

إنّ توفير الحماية اللازمة يعني ضمان تغطية جميع جوانب أمن المعلومات، من خلال تحقيق عناصر أمن المعلومات، (انظر الفصل الثالث)، كالآتي:

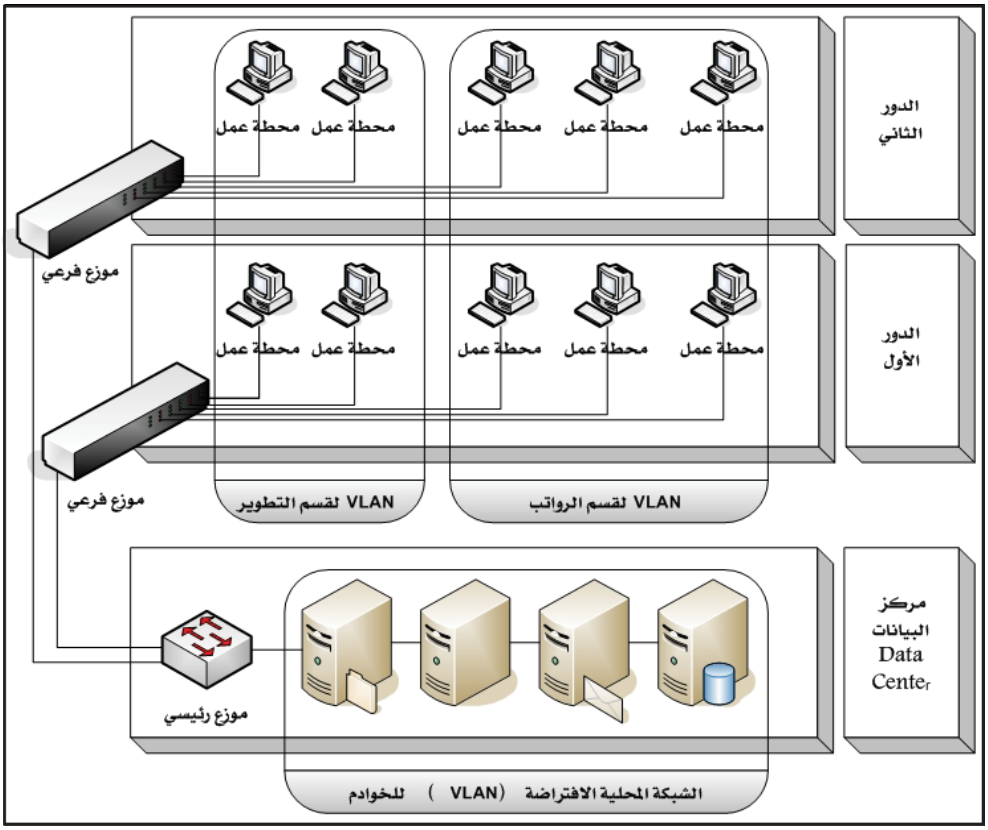
- التحقّق من الهُويّة: ضمان أنّ المرسلين والمستقبلين هم من يصرّحون عن أنفسهم بالفعل، فيمكن أداء التحقّق من الهُويّة من خلال تأكيد أن الطرف الآخر لديه المعرفة، أو لديه بعض المعلومات المشتركة، أو المفتاح السِّريّ الفريد.
- السِّريّة (أو الخصوصيّة): أن يستطيع الأطراف المخوّلون أن يدخلوا إلى حركة الشبكة الخاصة الافتراضيّة، ويتبادلوا المعلومات بشكل سرّيّ لا يمكن أن يطلّع عليها غيرهم، ويمكن تحقيق الخصوصيّة من خلال تطبيق التّشفير.
- سلامة البيانات تكاملها: أن لا تستطيع حركة الشبكة الخاصة الافتراضيّة التغيير في البيانات دون كشفها، فيمكن تحقيق سلامة البيانات تكاملها من خلال تطبيق البصمة الرقميّة.
- عدم الإنكار: أن لا يمكن للمستقبلين والمرسلين فيما بعد أن ينكروا علاقتهم بما تم عمله، ويمكن تحقيق ذلك من خلال استخدام التصديق (التوقيع) الرقمي، فعند وضع إجراءات عدم الإنكار لا يمكن للمستقبل أن ينكر استلام المعاملة، ولا يستطيع المرسل أن ينكر إرسالها.

٧-٧ الشبكات المحلية الافتراضيّة (Virtual LAN-VLAN)

قدَّمت تقنيات الموزعات (Switches) الحديثة إمكانية إنشاء شبكات محلية افتراضيّة (أو تخيلية) (Virtual Local Area Networks-VLANs) كثيرة على مكوّنات الشبكة الفعلية (الماديّة) الواحدة نفسها، وبهذه الطريقة يمكن تقسيم الحاسبات الآلية في شبكة

المنشأة (التي قد تتكون من عدّة شبـكات محلية (LAN) مرتبطة بشبكة واسعة (WAN)) إلى عدة مجموعات افتراضيّة تبدو كل واحدة منها كأنها مجموعة مستقلة، بغض النظر عن مواقعها الجغرافية مهما كانت متباعدة. وتستخدم هذه الطريقة لتلبية حاجة المنشأة لتقسيم موارد الشبكة تبعًا لحاجة الأعمال والإجراءات لديها، ولتحقيق مستوى أعلى من أمن المعلومات.

يوضح الشكل (٧-٤) كيف يمكـن أن يكون هناك جهازان أحدهما إلى جانب الآخر، لكن كل منهما ينتمي إلى شبكـة افتراضيّة مختلفة رغم اشتراكهما في التجهيزات الماديّة نفسها من موزعات رئيسة وفرعية وكابلات وموجهات وخلافه.



الشكل (٧-٤): الشبكات المحلية الافتراضيّة (VLANs)

كما يوضح الشكل (٧-٤) فإنّ أيّ اتصال من أيّ جهاز في قسم الرواتب لأيّ جهاز في قسم التطوير لا بدّ أن يتم توجيهه (Routed) من خلال المـوزّع الرئيس، حتى ولو كان الجهازان

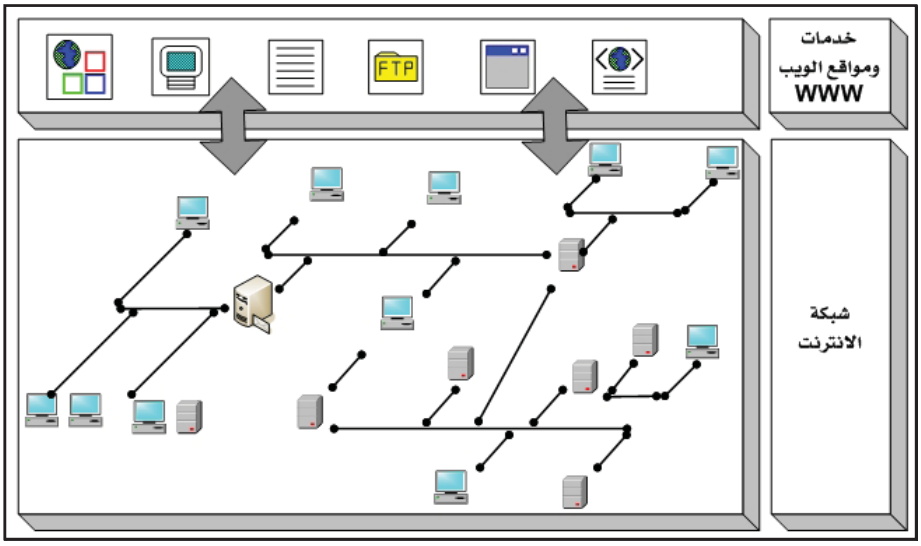
متجاورين على طاولة واحدة.

تقدّم الشبكات المحليّة الافتراضيّة عدّة خدمات لتحسين أمن المعلومات ورفع مستواه، تتلخص في الآتي:

- فصل موارد الشبكة المهمة والحساسة، مثل الخوادم في شبكة محلية افتراضيّة (أو أكثر)، منفصلة لا يصل إليها إلا المستخدمون المصرّح لهم فقط.
- تساعد في الحماية ضد هجمات البرامج الضارّة، مثل الفيروسات، بحيث إذا أصيبت شبكة افتراضيّة واحدة لا تنتقل العدوى إلى الشبكات الافتراضيّة الأخرى.
- تساعد في إدارة الشبكة ومراقبتها بسهولة، إضافة إلى تسهيل إدارة الأجهزة والموارد الأخرى، أو إخراجها من الشبكة.
- تسهيل تطبيق سياسات أمن المعلومات باختلاف أنواعها، من خلال تطبيق السياسة المناسبة لكل شبكة افتراضيّة على حدة. فمثلًا قد يحتاج قسم الرواتب إلى تطبيق سياسة أمنيّة صارمة للتحكّم بمنافذ الأجهزة (منافذ USB مثلًا). فيمكن وضع أجهزة قسم الرواتب في شبكة محليّة افتراضيّة واحدة، حتى لو كانت تلك الأجهزة تتوزّع على أدوار ومبانٍ مختلفة، ثم تطبيق سياسة المنافذ عليها بشكل مستقلّ، مع الإبقاء على منافذ الأجهزة في الأقسام الأخرى مفتوحة. ولو لم توجد في الشبكات المحلية الافتراضيّة إلا هذه الميزة لكانت كافية لضرورة تطبيقها، خاصّة في المنشآت المهمة والحساسة.
- حصر البيانات التي تبث لجميع الأجهزة (Broadcasting) في كل شبكة افتراضيّة وحدها؛ ما يساعد على تحسن الأداء والتحكّم فيه بشكل أفضل.

٧-٨ أمن خوادم وتطبيقات الويب

ظهر مصطلح «الويب» (Web) الذي ما هو إلا طبقة تعمل فوق شبكة الإنترنت. فتوفّر شبكة الإنترنت الأجهزة والبرامج وأنظمة التشغيل وأدوات الاتصال، بينما يوفّر الويب خدمة المواقع وتشغيل البرامج والمهام والخدمات الإلكترونيّة المختلفة، كما يوضح ذلك الشكل (٧-٥).

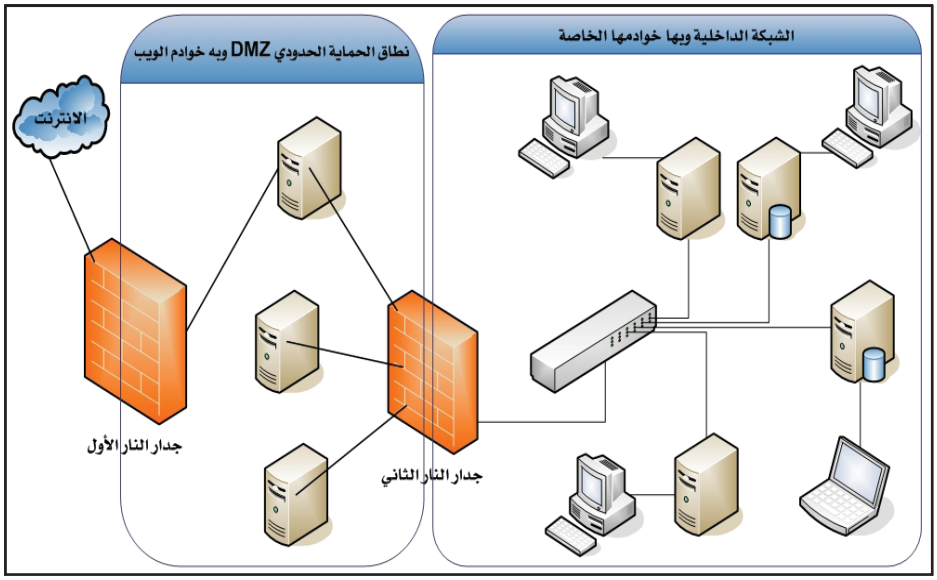


الشكل(٧-٥): الويب كطبقة مهام وخدمات إلكترونيّة فوق شبكة الإنترنت

بقدر ما تقدّمه هذه التقنيات للشركات والمنظّمات والهيئات والحكومات والأفراد من توفير إمكانية التواصل وتبادل المعلومات ومشاركتها بينها وبين منسوبيها من طرف، وبينها وبين عملائها والمستفيدين من خدماتها من طرف آخر، فإنها تفتح الباب أمام المتطفلين والمخترقين وسارقي المعلومات الرقميّة؛ للدخول إلى مواقع هذه الخدمات والعبث بها، أو استغلالها بطرق غير شرعية. لذلك فمن المهم جدًّا توفير وسائل الحماية اللازمة لهذه التقنيات حتى يُستفاد مما تقدمه من خدمات، وحتى يتم تقليل المخاطر الناجمة عنها قدر الإمكان أو تجنّبها.

في البداية كانت خوادم الويب جزءًا من شبكات المنشأة الداخليّة، ومرتبطة بشكل مباشر مع شبكة المنشأة ومع شبكة الإنترنت في آن واحد، وكان يعوّل في حماية هذه الخوادم على وجود صفحات ساكنة (جامدة) (Static Pages) توفر المعلومات باتجاه واحد من خوادم الويب إلى المستخدم، وليس هناك أيّ صفحات تفاعلية، ولا تُقبل أيّ معلومات من شبكة الإنترنت أو المستخدمين باتجاه هذه الخوادم. وظلّت هذه هي الحال حتى تطور استخدام الإنترنت، وظهرت الحاجة إلى صفحات تفاعلية، وظهرت تقنية (Common Gateway Interface-

CGI)، التي تسمح للمستخدمين بإدخال معلوماتهم وطلباتهم إلى خوادم الويب. عند ذلك أصبح لزامًا وضع خوادم الويب في نطاق حماية حدودي(Demilitarized Zone-DMZ) بدلًا من وجودها في نطاق شبكة المنشأة الداخليّـة، وهو ما قد يعرض شبكة المنشأة للخطر، انظر الشكل(٧-٦).

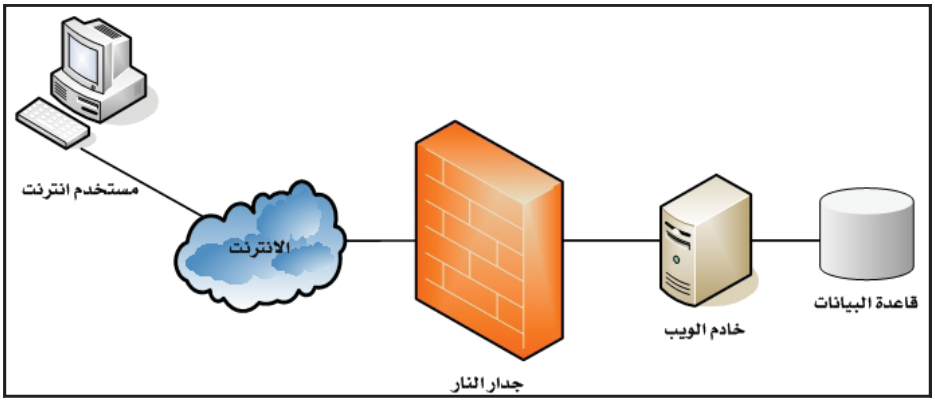


الشكل(٧-٦): وضع خوادم الويب في نطاق حماية حدودي مستقل عن نطاق شبكة المنشأة

مع تطور تطبيقات الويب وظهور الحاجة إلى تخزين معلومات المستخدمين وطلباتهم التي ترد من خلال صفحات الويب التفاعلية ظهرت الحاجة إلى تخزين هذه المعلومات في قواعد بيانات تقـع في نطاق الحماية الحـدودي(DMZ) نفسه، وتعمل جنبًا إلـى جنب مع خوادم الويب، لاستقبال المعلومات وإرسالها من شبكة الإنترنت واليها، ويجب حمايتها.

ومع وجود خوادم الويب وقواعد بياناتها في نطاق(DMZ) المعزول عن شبكة المنشأة(انظر الشكل(٧-٦)) كان ذلك حماية جيدة لشبكة المنشأة، إلا أنه ومع مرور الوقت ظهرت هناك مشكلة في نطاق الحماية الحدودي(DMZ) نفسه، حيث يمكن الوصول بطرق غير شرعية إلى قواعد البيانات في نطاق الحماية الحدودي؛ لوجود ارتباط مباشر بين خوادم الويب وقواعد

البيانات، وهذا الأمر مكّن المخترقين من الوصول إلى المعلومات السِّريّة في قواعد البيانات، التي تخص المنشأة أو تخص مستخدمين آخرين. انظر الشكل(٧-٧).



الشكل(٧-٧): يستطيع المهاجم الوصول إلى قواعد البيانات إذا كانت مرتبطة مباشرة مع خوادم الويب

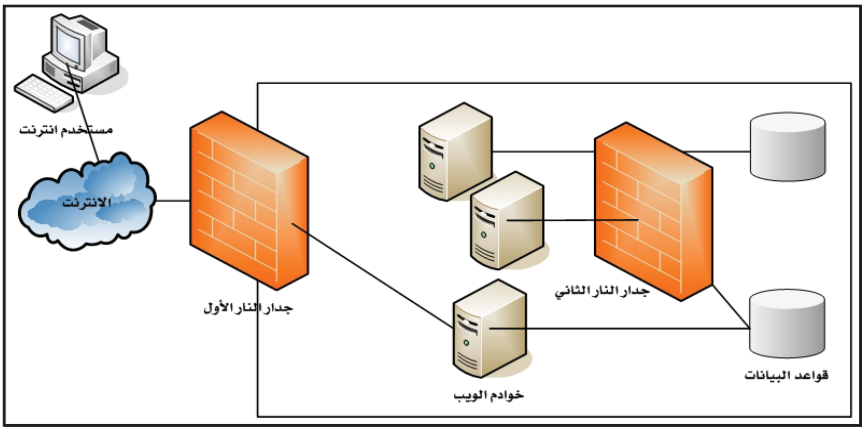
لو أخذنا الشركات التجارية كمثال لوجدنا أنّها مع مرور الوقت تقترب من الإنترنت أكثر فأكثر، وتوفر خدماتها وتستقبل طلبات المستخدمين وأرقام بطاقاتهم الائتمانية، ثم تُحصّل مستحقاتها الماليّة، وكلّ ذلك عبر الإنترنت، ومن خلال خوادم وقواعد بيانات الويب التفاعلية. وإذا كانت قواعد البيانات التي تحوي هذه المعلومات المهمة والحساسة في خطر فإنّه يجب حمايتها، ومن أنظمة الحماية الممكنة: نظام الحماية ذو الطبقتين(Two-Tier Architecture) ونظام الحماية ذو الطبقات الثلاث(Three-Tier Architecture).

٧-٨-١ نظام الحماية ذو الطبقتين(Two-Tier Architecture)

يحتوي نظام الحماية ذو الطبقتين خطين من التجهيزات: أمامي مكون من خوادم الويب التي توفر تطبيقات الويب وشاشات التواصل مع المستخدمين، وآخر خلفي يحتوي قواعد البيانات المهمة والحساسة. يفصل الخط الأول عن الإنترنت جدار حماية أولي، ويفصل خوادم الويب عن قواعد البيانات جدار حماية ثاني، كما في الشكل(٧-٨)[١]. ولا بدّ أن تختلف إعدادات التنقيح(الفلترة) في جدار الحماية الأولي عنها في جدار الحماية الثاني، وإلا سيكون بمقدور

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

من يستطيع اختراق جدار الحماية الأولي أن يخترق جدار الحماية الثاني.



الشكل(٧-٨): نظام الحماية ذو الطبقتين(Two-Tier Architecture)

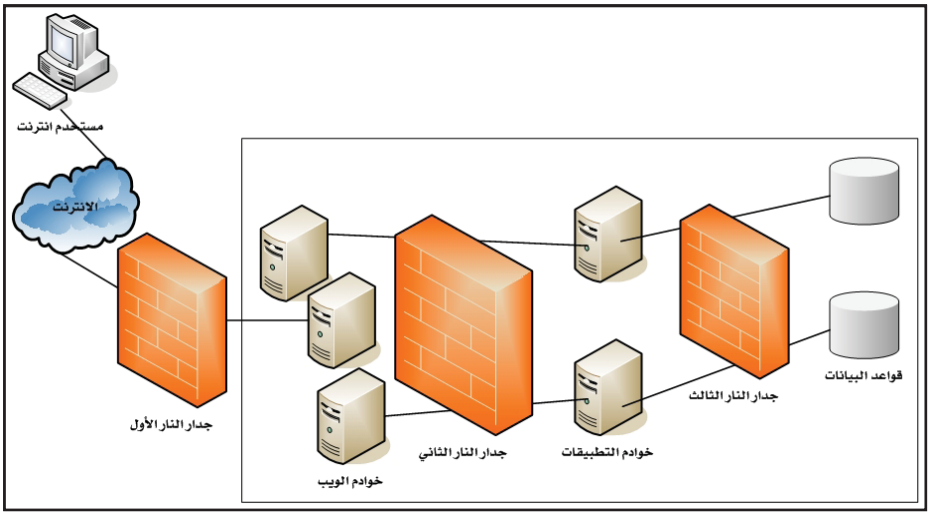
٧-٨-٢ نظام الحماية ذو الطبقات الثلاث(Three-Tier Architecture)

يناسب نظام الحماية ذو الطبقتين بعض الجهات التي تقدّم خدمات عاديّة. أمّا الجهات التي تقدم خدمات عالية الحساسية، مثل المصارف التجارية التي تستقبل بطاقات الائتمان وتخزّنها، فإنّ نظام الحماية ذو الطبقات الثلاث هو الأنسب لها.

يتكوّن نظام الحماية ذو الطبقات الثلاث من خطّين من الخوادم، وخط ثالث من قواعد البيانات كما في الشكل(٧-٩)[١]. يحتوي الخط الأول خوادم الويب كما في نظام الحماية ذي الطبقتين، إلا أنها مرتبطة بعضها مع بعض بشكل تبادلي(Clustered) (أو كما يطلق عليه في بعض الأحيان عنقودي)، بحيث إذا تعطل أحدها فيُغطى من خلال الخوادم الأخرى، وفي الوقت نفسه توزّع الحمل فيما بينها بالتساوي؛ لتحمّل الضغط الناتج من طلبات المستخدمين و من ثَمَّ تقدّم خدمات وتصفح أسرع. يحتوي الخط الثاني خوادم التطبيقات(Application Servers) التي تشغّل برامج وتطبيقات ذات خصائص ومهام محدّدة خاصّة بكل منشأة(ليست مثل مهام وخصائص تطبيقات الويب) وتقوم بعملية الاتصال مع خوادم الويب في الخطّ الأول ومع قواعد البيانات في الخط الثالث، وعادة ما تقوم خوادم التطبيقات في الخط الثاني بالعمليّات والمهام التي تحتاج إلى سرعة وكفاءة عاليتين، وأخيرًا. يحوي الخط الثالث قواعد

١- المرجع السابق.

البيانات التي تحتوي البيانات المهمّة والحسّاسة، كما في نظام الحماية ذي الطبقتين. ويفصل هذه النظام عن الإنترنت جدار حماية أوّليّ، ثم يفصل خوادم الويب عن خوادم التطبيقات جدار حماية ثانٍ، ويفصل خوادم التطبيقات عن قواعد البيانات جدار حماية ثالث. وكما في نظام الحماية ذي الطبقتين، لا بدّ أن تختلف إعدادات هذه الجدران عن بعضها بعضًا، وبما يناسب الحماية المطلوبة من كلّ منها، وإلا ستكون عرضه للاختراق في حال اختراق أحدها، خاصة جدار الحماية الأوّل.



الشكل (٧-٩): نظام الحماية ذو الطبقات الثلاث (Three-Tier Architecture)

إنّ أهم ما يميز نظام الحماية ذا الطبقات الثلاث هو قدرته على تطبيق أمن المعلومات بشكل تدريجيّ منطقي، وفي مناطق مختلفة، ومن ذلك أن يطبّق جدار الحماية الأول سياسات أمن معلومات محدّدة تسمح لأكبر عدد ممكن من المستخدمين بالاطّلاع على برامج المنشأة وخدماتها العامة، التي عادة ما يكون من المفروض أن يطّلع عليها أيّ زائر للموقع، ويكون في الوقت نفسه خط الدفاع الأول ضد برامج الاختراق والفيروسات والبرامج الخبيثة الأخرى. يأتي بعد ذلك جدار الحماية الثاني الذي يسمح لعدد أقل بالدخول إلى خوادم التطبيقات، ممن تنطبق عليهم شروط محدّدة أكثر حصرًا وصرامة من سابقتها، ويحتاجون إلى الخدمات والعمليّات الموجودة على تلك الخوادم. وأخيرًا يحجب الجدار الثالث قواعد البيانات تمامًا

من وصول المستخدمين المباشر إليها، ويسمح فقط بالوصول إليها من خلال البرامج الموجودة في خوادم التطبيقات في الخط الثاني، وليس من خلال المستخدمين أنفسهم.

لقد استعرضنا فيما سبق نُظَم الحماية ذات الطبقتين وذات الطبقات الثلاث من الجانب التصميمي والتجهيزات الفنيّة اللازمة لتطبيق هذه الأنظمة، لكن يبقى هناك وجود ثغرات أمنيّة في الأجزاء الصغيرة من مكوّنات هذه الأنظمة، وفي إعداداتها الفنية التفصيلية. فيمكن بناء نظام حماية ذي الطبقات الثلاث بوضع جُدُر الحماية وتوزيع خوادم الويب والتطبيقات وقواعد البيانات كما سبق، لكن يبقى احتمال قدرة المهاجم على النفاذ من خلال البروتوكولات والمكوّنات الصغيرة والخدمات التي توجد في أنظمة التشغيل أو في البرامج التطبيقيّة. ومن الهجمات المحتملة في هذه الحالة هي هجوم تعطيل الخدمة (Denial of Service-DoS)، والالتقاط أو التنصّت، وحقن أوامر (Sequential Query Language-SQL). وبعبارة أخرى يمكن للمنشأة إعداد البُنية التحتية لنظام حماية ذي طبقتين، وقد يفشل في صدّ هجمات المخترقين بسبب عدم توفير التحديثات (أو الرُّقع) (Patches) اللازمة لأمن المعلومات وأنظمة التشغيل. يوضح ذلك كيف أنّ الثغرات الأمنيّة يمكن أن تكون في أكواد (أو رموز) البرامج التطبيقيّة، التي قد لا يهتم بها مديرو الشبكات وأمن المعلومات، أو قد لا يكون لديهم الخلفية التامة عنها.

كما هو معلوم، فإنّ هناك مكوّنين أساسيين لأيّ نظام حاسب آلي، سواء أكان نظام حماية أم نظامًا عاديًّا، وهما: المكوّن المادي (أو العتاد) (Hardware)، والمكون البرمجي (Software). وقد تكون هناك ثغرات ونقاط ضعف أمنيّة في أيٍّ من هذين المكوّنين، وقد ولا يقتصر الضرر على أحدهما فقط، وإنما قد يؤثر في المكوّن الآخر. لذلك لا بد من معرفة الثغرات المحتملة في أيٍّ من هذه المكونين ومتابعتها وتحديثها باستمرار، ومن الأمثلة على هذه الثغرات ما يلي:

- الإعدادات الخاطئة لجدران الحماية.
- الهجمات عن طريق الثغرات في أنظمة التشغيل وبرامج الويب في خوادم الويب.
- قبول قواعد البيانات أيّ طلب من أيّ مصدر، وعدم حصرها من خلال خوادم

التطبيقات.

- عدم حماية قواعد البيانات بخط من جدران الحماية.
- عدم تعطيل البروتوكولات والخدمات التي ليس لها حاجة.
- عدم وجود نظام منع التطفل(IPS)، أو على الأقل نظام كشف التطفل(IDS).
- عدم التحديث المستمر للحواسيب وتزويدها بالتحديثات والرقع الجديدة سواءً على مستوى أنظمة التشغيل، أو البرامج التطبيقيّة(مثل متصفّح الإنترنت).
- عدم التدريب الجيد للعاملين في تطوير أنظمة أمن المعلومات وإدارتها ومتابعتها.
- عدم تطهير البيانات المدخلة من قبل المستخدمين في نماذج وبرامج الويب المركبة على خوادم الويب، خاصّة إذا كان هناك رفع ملفات من قبل المستخدمين إلى خوادم الويب التي قد تحتوي برامج خبيثة.

قد يكون هناك غيرها من الثغرات، لكن المقصود هنا هو إيضاح أنّ الثغرات قد تكون داخل أنظمة التشغيل، أو في أكواد البرامج التطبيقيّة، وهو ما يزيد الأمر تعقيدًا وخطورة، وهذا يقودنا إلى أهميّة بناء برامج آمنة وخالية من الثغرات الأمنيّة، وهذا الأمر قد لا يروق للمطورين الذين ينظرون فقط إلى بناء برامج ذات خدمات أكثر وأسرع، ويتطلّعون إلى تقديم إمكانات وخدمات ملموسة من قبل المستخدم؛ لأن تغطية الثغرات الأمنيّة في أكواد البرامج تحتاج إلى مجهود أكبر وخبرات عالية الكلفة، وفي الوقت نفسه يكون ما تقوم به غير مرئي، وربما غير مقدَّر من قبل المستخدم.

٧-٩ أمن طبقات شبكات الحاسب الآلي

بنظرة أشمل إلى الثغرات الأمنيّة والهجمات على أنظمة المعلومات والتهديدات المحتملة نجد أنها توجد في طبقات شبكات الحاسب الآلي المختلفة(انظر الفصل الأول: طبقات الشبكات) وهذا الوجود يمكن أن يكون كذلك في المكوّنات الماديّة(العتاد)، أو في البرامج العاملة في تلك الطبقات. فعلى سبيل المثال، فإنّ الهجوم باستخدام طريقة خداع عنوان الإنترنت(IP Spoofing) هو هجوم على مستوى الطبقة الثالثة: طبقة الشبكة، وهجوم تشمّم أو التقاط

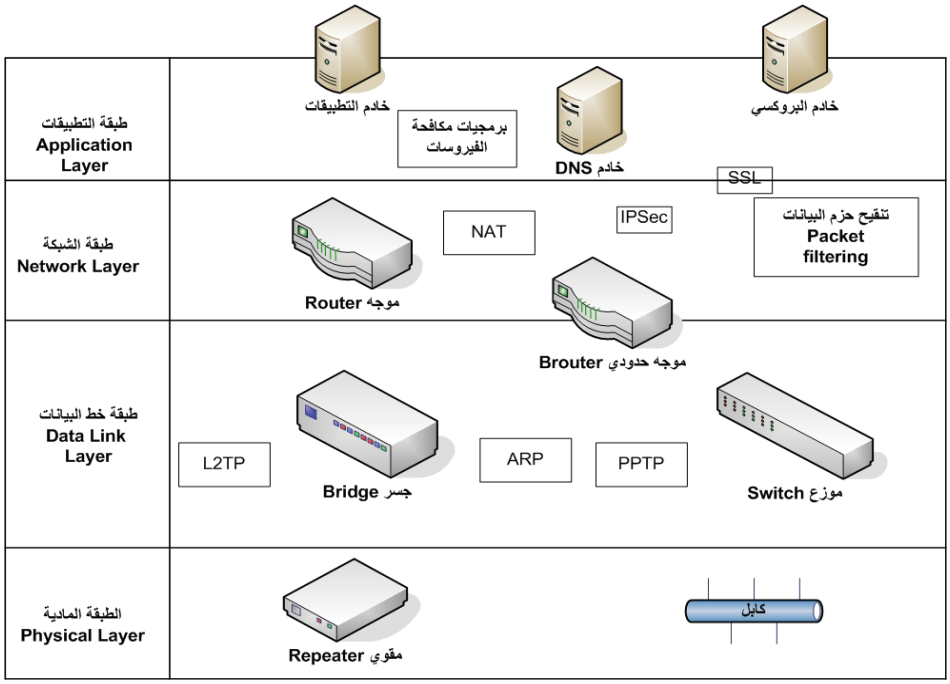
البيانات المارّة يمكن أن يقع في عدّة طبقات في آن واحد معًا، وتدخل الفيروسات إلى الشبكات من خلال الطبقة السابعة(طبقة التطبيقات) وهذا يعني أنه لا بدّ من تأمين طبقات شبكات الحاسب الآلي كافة، وعدم ترك أيّ منها أو إهماله. فالمنشأة التي تكتفي بتطبيق شروط وسياسات صارمة لتأمين كلمات المرور وتعتمد على جدران الحماية فقط، فإنها ليست في مأمن من هجمات كثيرة على طبقات مختلفة من شبكتها. فكلمات المرور وجدران الحماية ما هما إلا مكونان أساسيان لأمن المعلومات ولا يقدّمان وحدهما حلًا كاملًا لأمن معلومات المنشأة التي تحتاج إلى منظومة متكاملة من الأجهزة والبرامج والبروتوكولات على طبقات الشبكة كافة.

قد يختلف عدد الطبقات من شبكة إلى أخرى، وقد تُضم طبقتان إلى بعضهما بعضًا وذلك حسب طبيعة عمل المنشأة، ودرجة حساسية بياناتها، ولا يشترط أن تتوافر الطبقات السبع في جميع الأحوال. فيما يلي نستعرض أهم التهديدات المحتملة واشهرها، وأدوات الحماية أو المضادات المستخدمة في كلّ طبقة من الطبقات الرئيسة الأربع من طبقات شبكات الحاسب الآلي: الطبقة الأولى – الطبقة الماديّة، والطبقة الثانية – طبقة خط البيانات، والطبقة الثالثة – طبقة الشبكة، والطبقة السابعة – طبقة التطبيقات، كما يوضح ذلك الشكل(٧-١٠)[١].

- جدار الحماية قبل خوادم التطبيقات: يعمل في طبقة التطبيقات، ويحمي تلك الخوادم ضد عدد من الهجمات، منها: الوصول غير المصرّح به، والهجوم المبني على خدع حزم البيانات.
- تحوير عناوين الشبكة(Network Address Translation-NAT): يعمل في طبقة التطبيقات ويحجب عناوين الشبكة(IP) للشبكة المحلية(LAN) والطبوغرافيا الخاصة بها عن الشبكة الواسعة(WAN) وعن الإنترنت.
- الكابلات المجدولة(Shielded Twisted Pair-STP): تعمل في الطبقة الأولى وتساعد في الحماية من اعتراض وتداخل الإشارات.
- حسّاسات كشف التطفل: تعمل في طبقتي الشبكة والنقل وتراقب البيانات المارة وتكشف بيانات التطفل فيها، وخاصة بيانات الهجمات الشهيرة والمعروفة مسبقًا.

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

- أداة تأمين عنوان الإنترنت(IPSec): تعمل في طبقة الشبكة وتشفّر البيانات وتحمي من هجمات التنكّر، وهجمات التعدّي على البيانات المارّة وتعدّل فيها، وهجمات الوصول غير المصرّح به، والجدير بالذكر أن هذه الأداة هي أداة برمجيّة فعّالة في حماية الشبكات الخاصة الافتراضيّة(VPN).



الشكل(٧-١٠): مواقع الأجهزة والبروتوكولات في طبقات شبكات الحاسب حسب نموذج(OSI)

- قفل المنافذ(كمنافذ USP) والخدمات غير الضرورية: يعمل في طبقتي الشبكة والنقل، ويحافظ على أمن الأجهزة الطرفيّة المرتبطة بالشبكة، ويقلّل نقاط الدخول للشبكة، ويساعد في الحماية من هجوم تعطيل الخدمة(DoS).
- طبقة المقابس الآمنة(Secure Sockets Layer-SSL): تعمل في طبقة النقل، وتستخدم للتحكم بدخول المستخدمين للمعلومات السِّريّة الشخصية، وهي أداة مناسبة لتحقيق عنصري: السِّريّة وسلامة المعلومة وتكاملها، وتساعد في الحماية ضد هجمات التنكر.

- ماسح الشبكة: يشغل مجسًّا (دوريًّا) يمسح منافذ الشبكة للبحث عن أيّ ثغرات أمنيّة، وهذا يساعد في الحماية ضدّ الثغرات الناتجة عن التغيير في الإعدادات، أو تلك الناتجة عن إضافة أجهزة وتقنيات وأنظمة جديدة.
- استخدام أنظمة وبرامج تشفير مضمّنة في خوادم الويب: يعمل في طبقة التطبيقات، ويحقق عنصر السِّريّة للمعلومات، ويحدّ من تنفيذ إجراءات أو برامج خطرة.
- نظام الشهادات الرقميّة (Digital Certificates): يعمل في طبقة التطبيقات، ويستخدم للتحقق من هويّة كل خادم من خوادم الويب، ويساعد في الحماية ضد هجمات اختطاف الجلسات والتنكّر.

توضح هذه القائمة جزءًا من الحماية التي يجب تطبيقها في كلّ طبقة من طبقات شبكات الحاسب الآلي في نموذج (OSI) وفي حال غياب أحد هذه الأجهزة أو البرامج، أو إذا ما أعدِّت بطريقة خاطئة، فسيكون هناك خلل في أمن الشبكة، و من ثَمَّ سيكون هناك إمكانية لوصول المخترقين إلى أماكن كان من المفروض ألا يصلوا إليها.

ملخّص الفصل

كما ذكرنا في مقدّمة الفصل فإنّ ما يؤرّق مالكي شبكات الحاسب الآلي ومستخدميها، هو موضوع أمن هذه الشبكات، خاصّة في ظل تزايد استخدام شبكة الإنترنت كناقل رئيس للبيانات، وشبكة يشترك فيها الجميع، وظهرت الحاجة الملحّة لاستخدام وسائل حماية خاصّة لهذا الغرض.

ما أردناه في هذا الفصل هو توضيح أشهر التهديدات الرقميّة لشبكات الحاسب الآلي، التي يأتي على رأسها: الهجوم الإلكتروني، وهجمات الهندسة الاجتماعيّة، ثم استعراض المتطلبات الأساسيّة لأمن شبكات الحاسب الآلي، والتقنيات والآليات اللازمة لذلك. فقد شرحنا هذه التهديدات وخطورتها على شبكات الحاسب الآلي وأهدافها، وآليات المهاجمين وخدعهم التي يستخدمونها، وبعد ذلك عرضنا التدابير والآليات والتقنيات لحماية شبكات الحاسب الآلي، وهي:

- التدابير الأمنيّة العامة لأمن شبكات الحاسب الآلي.
- أمن وسائط نقل المعلومات.
- استخدام جدران النار.
- استخدام الشبكات الخاصة الافتراضيّة(VPNs).
- استخدام الشبكات المحلية الافتراضيّة(VLANs).
- تأمين خوادم الويب وبرامجه من خلال نظامي الحماية ذوا الطبقتين أو الثلاث.
- أمن طبقات شبكات الحاسب الآلي(Network Layers Security).

وقد شُرحت هذه التدابير والآليات والتقنيات بالتفصيل، مع بيان كيفية تطبيقها والثغرات الأمنيّة التي تغطيها، ومميزات كل منها وعيوبه.

مسائل

١. عدّد أهم ثلاثة تدابير عامة لأمن شبكة الحاسب الآلي لجهة ماليّة تستخدم الإنترنت لنقل بياناتها بين فروعها.

٢. من التدابير الجيّدة لحماية شبكة الحاسب الآلي، تفعيل خدمة تسجيل العمليّات والأحداث(Log File) لنظام تشغيل الشبكة. اشرح كيف يمكن الاستفادة من ذلك.

٣. عرّف جدار النار، ثم اشرح عمليّات التنقيح الممكنة.

٤. أيّهما أقوى حمايةً للشبكة: التنقيح باستخدام العناوين، أم التنقيح باستخدام المنافذ؟ ولماذا؟ أعط أمثلة.

٥. اذكر مميزات الجدار الناري وعيوبه، ولماذا يشكل عدم التهيئة الصحيحة له ثغرة أمنيّة؟

٦. قارن بين خطوط نقل البيانات في الشبكات الخاصة الافتراضيّة والخطوط المستأجرة(Leased Lines).

٧. هل يمكن استخدام الشبكة الخاصة الافتراضيّة دون جدران نار في نهايتي النفق؟ ولماذا؟

٨. كيف يتم تحقيق عنصر السِّريّة في الشبكات الخاصة الافتراضيّة؟

٩. من مميزات الشبكة الخاصة الافتراضيّة، سهولة التوسع المستقبلي، فلماذا؟ اشرح ذلك.

١٠. من عيوب الشبكة الخاصة الافتراضيّة، تأثر أدائها بالضغط الحاصل على الإنترنت، فلماذا؟ اشرح ذلك.

١١. من مراحل الهجوم مرحلة المناورة؛ ما فائدة ذلك للمهاجم؟

الفصل الثامن

إدارة المخاطر المعلوماتيّة

أهداف الفصل

- توضيح مفهوم إدارة المخاطر المعلوماتيّة مع شرح العمليّات الرئيسة لذلك.
- شرح طُرُق تحليل المخاطر وكيفية إجراء التحليل بالأمثلة.
- كيفية اختيار أنظمة الحماية ومضادات التهديدات بناءً على نتائج التحليل.
- شرح مفهوم معالجة الكوارث المعلوماتيّة والمراحل المتبعة في ذلك.

ما ستتعلمه في هذا الفصل

- المفاهيم الرئيسة في إدارة المخاطر: الضعف، والتهديد، والخطر، والتعرض، والمضادات.
- السياسة الأمنيّة لإدارة المخاطر المعلوماتيّة.
- العمليّات الرئيسة الثلاث لإدارة المخاطر: تحليل المخاطر، واختيار أنظمة الحماية، والإجراءات الاحتياطية لمواجهة المخاطر.
- الأسئلة الرئيسة التي يجب الإجابة عنها لإتمام عمليّة تحليل المخاطر.
- التحليل الكمّي والتحليل النوعي للمخاطر المعلوماتيّة.
- تحليل الكلفة والفاعليّة.
- مجموعة التدابير الاحترازيّة لمواجهة الكوارث المعلوماتيّة.
- الخطوات المتّبعة لمعالجة الكوارث المعلوماتيّة بعد حدوثها.
- شجرة الإنذار وكيفية عملها واستخدامها.

إدارة المخاطر المعلوماتيّة

٨-١ مقدّمة

من المعلوم أن ليس هناك بيئة تقنية آمنة كاملة بنسبة (١٠٠٪) فكلّ بيئة يوجد بها نقاط ضعف وقابليـة للإصابة ومخاطر إلى درجة معيّنة، والمطلوب مـن إدارة المخاطر المعلوماتيّة هو تحديد هذه النقاط والتهديدات، ثم تقويم احتمال حدوث أي منها، وتقييم الضرر الناتج عن ذلك، ثم أخذ الخطوات والتدابير اللازمة لتقليل الخطر بشكل عام إلى المستوى المقبول الذي تحدّده المنشأة.

يمكن للمخاطر المعلوماتيّة أن تكون في أشكال متعدّدة، وليس بالضرورة أن تكون كلها ذات علاقة بالحاسب الآلي. فقد يكون الموظف غير المدرّب جيّدًا أحد التهديدات المهمة. وكذلك فإنّ وضع أشرطة النسخ الاحتياطي في مكان غـير محصّن وغير محمي بنظم حماية ماديّة إداريّة أو المركزيّة هو تهديد لأمن المعلومات المخزّنة في تلك الأشرطة.

لتحقيق أمن المعلومات بشـكل متكامل، فلا بدّ من الأخذ في الاعتبار جميع أنواع المخاطر وأشكالها المختلفة، والتعامل معها بشكل جيّد، ومن أشهر أنواع المخاطر المعلوماتيّة ما يلي:

- الضرر المـادي: وهو الضرر الناتج عـن الحرائق، والمياه، والتخريـب، وفقد الطاقة الكهربائيّة، والكوارث الطبيعية، إلى غير ذلك من المسبّبات الماديّة.
- التعامل البشري: وهو ما ينتج عن التعامل العرضي، أو المتعمد، أو التراخي المتسبب في تعطل الإنتاجية، أو الإضرار بأمن المعلومة.
- تعطل الأجهزة: مثل تعطل الأجهزة الرئيسة (الخوادم)، أو الأجهزة الطرفيّة، أو تعطّل الأنظمة التي تتكون من أجهزة وبرمجيات مضمّنة مع بعضها بعضًا.
- الهجوم بنوعيه الداخلي والخارجي: ويشمل ذلك كلّ أنواع الهجوم (Attacking)، والقرصنة (Hacking) التقنية، وكسر أنظمة الحماية (Cracking).
- إساءة استخدام البيانات: مثل نشر البيانات السِّريّة، والاحتيال، والتجسّس الرقمي، وسرقة البيانات.

- فقْد البيانات: ويشمل الفقد العرضي نتيجة للإهمال أو التراخي، أو عدم القدرة على التعامل مع المعلومة بشكل صحيح، أو الفقد المتعمد.
- أخطاء البرامج التطبيقيّة: مثل الأخطاء الحسابيّة، والإدخال الخاطئ للمعلومات.

مما تجدر الإشارة إليه أنه يصعب قياس الأخطار الحقيقية، لكن يساعد في ذلك تصنيفها إلى فئات محدّدة، ثم ترتيبها وفق أولويات تتناسب مع تلك الفئات، وتحدّد أيّ الأنواع يجب التعامل معه أولًا وفقًا لأولويته. وكما ذكرنا سابقًا، فليس هناك بيئة تقنية آمنة، ومن الطبيعي أن توجد قائمة من التهديدات المحتملة. فلو أن لدى المسؤول عن أمن المعلومات قائمة بتلك التهديدات، ولديه ميزانيّة محدّدة لا تكفي لمواجهة جميع هذه التهديدات، فإنّ دور إدارة المخاطر المعلوماتيّة سيكون ترتيب هذه التهديدات وفقًا لدرجة خطرها، ثم توجيه الميزانية المتوفرة لمواجهة أكثرها خطرًا على المنشأة.

إنّ أيّ منشأة تعتمد في عملها على الحاسبات الآلية وشبكات المعلومات لا بدّ أن تضع في حسابها أن هناك مخاطر تحيط بمعلوماتها، يجب معرفتها، وأخذ التدابير اللازمة للحيلولة دون وقوعها، وهذا ما يسمّى بإدارة المخاطر المعلوماتيّة(Information Risk Management) وقد يحدث أن تتعرّض معلومات المنشأة إلى كارثة حقيقية، سواءً كارثة طبيعيّة، أو تحوّل بعض الأخطار إلى كارثة حقيقيّة تحل بالمنشأة ومعلوماتها، وهذا ما يسمّى بمعالجة الكوارث المعلوماتيّة.

يبدأ هذا الفصل بشرح المصطلحات والمفاهيم الأساسيّة لإدارة المخاطر المعلوماتيّة كأساس لفهم باقي موضوعات الفصل، ثم ينتقل إلى شرح السياسة الأمنيّة(الموضوعية) لإدارة المخاطر المعلوماتيّة وما يجب أن تحتويه هذه السياسة[1]. يلي ذلك موضوع مهم في إدارة المخاطر المعلوماتيّة، ويُعدُّ حجر الزاوية في هذا المجال، وهو تحليل المخاطر المعلوماتيّة، والطرق المتبعة لإجراء التحليل، وكيفية الاستفادة من نتائجه. وكنتيجة منطقية لإدارة المخاطر المعلوماتيّة، نختتم هذا الفصل بموضوعين مهمّين هما: اتخاذ الإجراءات الاحترازيّة لمواجهة

١- أوردنا هذه السياسة هنا، ولم نضعها ضمن السياسات الأمنية الموضوعية في الفصل الخامس؛ لأنها سياسة موضوعية يمكن أن تتبع لموضوعها، ومن أجل تحقيق الترابط بين مفاهيم هذا الفصل ومعانيه.

المخاطر المعلوماتيّة، ومعالجة الأخطار والكوارث المعلوماتيّة بعد وقوعها.

٨-٢ مصطلحات إدارة المخاطر المعلوماتيّة ومفاهيمها

في الحالات العادية، قد تستخدم كلمة «الخطر» ليقصد بها «التهديد»، أو العكس. وبمعنى آخر قد تحل أي من كلمتي «الخطر» و «التهديد» محل الأخرى دونما تغيير في المعنى بالنسبة للأشخاص غير المتخصصين في أمن المعلومات. وقد تستخدم المصطلحات: «الضعف»، و«التهديد»، و«الخطر» ، و«التعرض» للتعبير عن نفس الشيء رغم أن لكل منها معنى مختلفًا في علم أمن المعلومات، وأن كلًا منها ليست بديلًا للآخر. لذا يجب قبل البدء بدراسة «إدارة المخاطر المعلوماتيّة» تعريف كلّ مصطلح من هذه المصطلحات بشكل دقيق ومعرفة معناه والعلاقة التي تربطه بالمصطلحات الأخرى.

الضعف أو قابلية الإصابة (Vulnerability): هي ضعف الأجهزة أو البرامج أو الإجراءات في أنظمة الحماية، التي ينتج عنها نقاط ضعف أو ثغرات أو أبواب مفتوحة، يمكن للمهاجم النفاذ من خلالها إلى الشبكة والأجهزة، ومن ثم الوصول غير المصرّح به إلى معلومات المنشأة ومواردها المختلفة، ومن الأمثلة على نقاط الضعف ما يلي:

- خدمة أو برنامج صغير غير مؤمّن على أحد الخوادم الرئيسة يمكن استغلالها من قبل برامج الاختراق.
- نظام تشغيل أو برنامج تطبيقي غير محدّث بآخر تحديثات الأمان.
- الارتباط غير المحدّد وغير الآمن بالشبكات الواسعة (WAN).
- المنافذ المفتوحة في جدران الحماية.
- تراخي الحماية الماديّة، سواءً أكانت حماية ماديّة المركزيّة أو إداريّة، في السماح لأيّ أحد بالدخول إلى مراكز البيانات والمناطق الحسّاسة.
- استخدام كلمات مرور تلقائيّة أو ضعيفة للدخول إلى الخوادم والأجهزة الطرفيّة المرتبطة بالشبكة.

التهديد (Threat): هو أيّ شيء (مكوّن) يشكّل انكشافًا محتملًا للمعلومات أو الأنظمة.

وبعبـارة أخرى هو أيّ شخصـ أو أداة تحدّد نقطة من نقاط الضعـف، كأيّ نقطة من نقاط الضعف السابقة، ومن ثم استخدامها ضد المنشأة أو شخص آخر، وتسمّى الجهة أو الأداة أو الشخص الذي يستغلّ نقاط الضعف، ويشـكّل تهديدًا للمنشأة، «عامل التهديد» ومن الأمثلة على عوامل التهديد ما يلي:

- متطفّل يمكنه الدخول إلى الشبكة عبر أحد منافذ الجدار الناري.
- عمليّة أو برنامج يمكنه الوصول إلى البيانات مخالفًا سياسات أمن المعلومات.
- مصادر التهديدات الطبيعيّة المختلفة.
- الموظف الذي يخطئ أخطاء فادحة تؤدي إلى كشف البيانات السِّريّة أو تلفها.

الخطر (Risk): هو احتمال أن يستغلّ عامل التهديد وجود نقطة ضعف، أو حالة القابلية للإصابـة، ومن ثم النفاذ من خلالها، فكلّما ازداد عدد المنافـذ المفتوحة في جدار الحماية، ازداد احتمال أن يستغل المتطفّل أحد هذه المنافذ ويدخل من خلاله بطريقة غير مشروعة إلى الشبكة، وكلّما كان الموظّـف غير مدرّب جيّدًا على العمليّات والإجراءات زاد احتمال ارتكابه للأخطاء الفادحة التي قد تـؤدّي إلى فقْد البيانات أو تدميرهـا، وإذا لم يركّب نظام كشف التسلل (IDS) في الشبكة، ازداد احتمال التسلّل بشكل غير ملحوظ، بل ويتأخر كشف ذلك، و من ثَمَّ لا يمكن تجنبه، وبناءً على ذلك، يمكن القول إنّ الخطر هو الحلقة التي تربط بين كلٍّ من: الضعف أو القابلية للإصابـة، والتهديد، واستغلال الثغرات الموجودة من جهة، والتأثير الناجم عن ذلك في العمل من جهة أخرى.

التعرّض (Exposure): هو حالة تعرّض لخسائر نجمت عـن عامل تهديد. ففي حال وجود الضعف أو القابليّة للإصابة تتعرّض المنشأة لفقدٍ او تدميرٍ محتملٍ للبيانات، وفي حال وجود تراخٍ في حماية قواعد بيانات كلمات المرور وإدارتها فإنّ كلمات مرور المستخدمين ستكون عرضة للالتقاط، ومن ثم استخدامها بطُرق غير مشروعة. وإذا لم تستخدم المنشأة أنظمة كشف الحريق ومنعه، و وضع التدابير اللازمة لمكافحته؛ فستكون عرضة لنشوب حريق مدمّر.

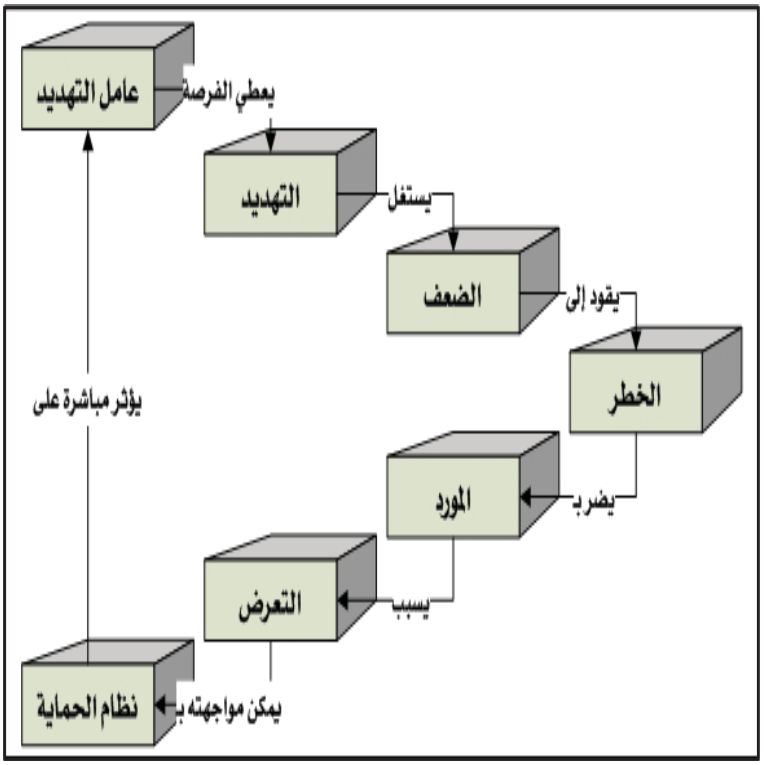
المضـادّات (Countermeasures) (**أو الحمايـة** (Safeguard)): تستخدم المضادّات

أو أنظمة الحماية لمجابهة الأخطار المحتملة، والتخفيف من آثارها. وقد يكون المضاد عبارة عن إعدادات معيّنــة للبرامج، أو جهاز محدّد يؤدي وظيفة محــدّدة، أو إجراءات معيّنة تُتّبع لمجابه الخطر والتخفيف من آثاره. وعادة ما يقضي المضاد على نقاط الضعف، ويقلّل احتمال استغلال عامل التهديد لنقاط الضعف الموجودة، ومن الأمثلة على المضادات ما يلي:

- وجود إدارة صارمة لكلمات المرور.
- وجود حرّاس أمن للمناطق المهمّة والحساسة.
- تطبيق آلية للتحكم بالوصول على مستوى نظام التشغيل.
- استخدام كلمات مرور على مستوى نظام الدخل والخرج الأساسي(BIOS).
- التدريب والتوعية بأمن المعلومات.

يوضح الشكل(٨-١) العلاقة بين المفاهيم الأساسيّة لإدارة المخاطر المعلوماتيّة. ولتوضيح ذلك بشكل تفصيلي فسنأخذ المثال الآتي: لو أنّ لدى شركة معيّنة نظام مكافحة للفيروسات، لكن لا يُحــدّث بتعريفات الفيروسات دوريًّا فــإنّ ذلك يشكّل **ضعفًا** في نظــام الحماية، ويُعدُّ حالة من **القابليّة للإصابة**، ويكمن **التهديد** في أن الفيروس قد يظهر في أيّ وقت، ويؤثر في عمل المنشأة، **والخطــر** في هذه الحالة هو احتمال ظهور الفيروســ في الشبكة مسبّبًا تلفًا أو فقدًا للبيانات، ولو ظهر الفيروس وتسلّل إلى شبكة الشركة، فهذا يعني أنّه قد جرى استغلال **الضعف**(القابليّة للإصابة) وأصبحت الشركة **عرضة** لخسارة بياناتها. **والمضاد** في هذا المثال هو تحديث نظام مكافحة الفيروسات بتعريفات الفيروسات دوريًّا،(قد يكون يوميًّا في البيئات المهمّة والحسّاسة)، وتركيبه على جميع أجهزة الشبكة.

إنّ الترتيب النظريّ لهذه المفاهيم هو الترتيب الآتي، كما يوضح ذلك الشكل(٨-٢): وجود **عامل التهديد** يعطــي الفرصة **للتهديد** أن يستغل **الضعــف** الموجود، وهو ما يقود إلى وجود **الخطــر**. و وجود الخطر يضرّ بموارد المنشأة مسببًا **تعرض** المنشأة للخسارة. وتتم مجابهة ذلك **بنظام الحماية**، الذي يفترض أن يؤثر تأثيرًا مباشرًا في وجود عامل التهديد.



الشكل(٨-٢): العلاقة بين المفاهيم الأساسيّة لإدارة المخاطر المعلوماتيّة

والترتيب المنطقي لتقويم هذه المفاهيم لدى تطبيقها في المنشأة هو الترتيب الآتي: التهديد، التعرّض للخسارة، الضعف أو القابليّة للإصابة، المضادات، وأخيرًا الخطر. والسبب في ذلك هو أنّه قد يكون هنـاك تهديد ما، لكن لن تكـون المنشأة عرضة للخسارة طالمـا أنّه لا يوجد ضعف ما، أو قابلية للإصابة يمكن استغلالها من قبل عامل التهديد، وإذا كان هناك ضعف معيّن(وهو أمر وارد) فلا بدّ من استخدام المضادّات لمواجهة الخطر أو التقليل من آثاره.

وأخيرًا، فإنّ تطبيق المضاد أو نظام الحماية المناسب سيلغي الضعف والتعرض للخسارة، ومن ثم يقلل الخطر. ومن المعـروف أنّه لا يمكن إلغاء عوامل التهديـد، لكن يمكن منع هذه العوامل من استغلال نقاط الضعف والنفاذ من خلالها.

٨-٣ السياسة الأمنيّة لإدارة المخاطر المعلوماتيّة

تتطلب إدارة المخاطر المعلوماتيّة تحديد الإجراءات المتعلّقة بإدارة المخاطر وتوثيقها، ثم

تفويض فريق إدارة المخاطر لممارسة مهامه، وفوق ذلك دعم الإدارة العليا في المنشاة. ويجب أن تكون سياسة إدارة المخاطر المعلوماتيّة تابعة لسياسة أمن المعلومات العامة للمنشأة، وتصبّ في تحقيق أهدافها الرئيسة.

من العناصر المهمّة التي يجب أن تحتويها سياسة إدارة المخاطر المعلوماتيّة ما يلي :

- أهداف فريق إدارة المخاطر المعلوماتيّة .
- مستوى الخطر المقبول لدى المنشأة، الذي بعد تحديده يُقبل أيّ خطر أقل منه، ويواجَه أيّ خطر يوازيه أو أعلى منه.
- الإجراءات الرسميّة لدى المنشأة المتبعة في تعريف الخطر وتحديده.
- العلاقة بين السياسة الأمنيّة لإدارة المخاطر المعلوماتيّة والخطة الإستراتيجية.
- مسؤوليات إدارة المخاطر المعلوماتيّة والأدوار والمهام المطلوبة للقيام بها .
- آليات تعديل مهام فريق إدارة المخاطر المعلوماتيّة والإجراءات التي يحتاج إليها عند الحاجة لذلك، بناءً على ما ينتج من عمليّة تحليل المخاطر .
- آليات رفع المعلومات المتعلّقة بالمخاطر المعلوماتيّة إلى إدارة المنشأة العليا، وآليات تنفيذ القرارات الصادرة منها لمجابهة المخاطر.

عادة ما ينفّذ السياسة الأمنيّة لإدارة المخاطر المعلوماتيّة فريق متخصّص يختلف عدد أفراده وقدراتهم، بناء على حجم المنشأة ومهامها. والهدف الرئيس لهذا الفريق هو توفير الحماية اللازمة لمعلومات المنشأة، بطريقة تجمع ما بين تحقيق هذا الهدف والموارد المتاحة، ولتحقيق هذا الهدف فإنّه لا بدّ من توفير الأدوات الآتية:

- تحديد مستوى الخطر المقبول وبناؤه من لدن الإدارة العليا في المنشأة .
- عمليّات وإجراءات موثقة لتقدير المخاطر والتدريب عليها.
- إجراءات تعريف المخاطر وإجراءات مجابهتها.
- موارد وميزانيّة مناسبة لفريق إدارة المخاطر المعلوماتيّة.
- التدريب والتوعية بأمن المعلومات لجميع الجهات والهيئات التي لها علاقة بالمعلومات.

- أدوات قياس المخاطر المعلوماتيّة وتحليلها.
- القدرة على تحديد المخاطر الجديدة وتقديرها التي تظهر عند تغيير البيئة التقنية وتطويرها في المنشأة.
- التنسيق بين فريق إدارة المخاطر المعلوماتيّة وعمليّات التحكّم بالتغيير في المنشأة؛ لضمان عدم ظهور نقاط ضعف جديدة عند حدوث أيّ تغيير في المنشأة.

٨-٤ تحليل المخاطر المعلوماتيّة

كما مرّ معنا فإنّ الخطر هو احتمال استغلال أيّ ضعف موجود في نظام الحماية، و من ثَمَّ احتمال حدوث ضرر ما. وإدارة المخاطر المعلوماتيّة(Information Risk Management) هي عمليّة تحديد الخطر، ثم تقويمه، ثم العمل على تقليله وتقليل الآثار الناتجة عنه إلى أقل مستوى ممكن(المستوى المقبول)، ثم تطبيق الآليات اللازمة للمحافظة عليه عند هذا المستوى. ولا يمكن لإدارة المخاطر المعلوماتيّة أن تكون فاعلة وذات فائدة للمنشأة ما لم تقم على أساس تحليل المخاطر، وفق المنهج العلمي الصحيح.

إنّ عمليّة "تحليل المخاطر" هي أداة من أدوات إدارة المخاطر المعلوماتيّة، ويمكن تعريفها بأنّها: "طريقة تحديد نقاط الضعف والتهديدات وتقدير الأضرار المحتملة لها، ومن ثم تحديد أماكن تطبيق أنظمة الحماية المجابهة لها" و من ثَمَّ فإنّ تحليل الخطر هو أداة تساعد على إعطاء الأولوية المناسبة لكل خطر، ثم تحديد المتطلبات اللازمة لمجابهته، سواءً أكانت المركزيّة أو إداريّة أو ماليّة.

وهناك أربعة أهداف رئيسة لتحليل المخاطر المعلوماتيّة هي:

١. تحديد موارد المنشأة والموجودات والعناصر المراد حمايتها، وقيمة كل منها للمنشاة.

٢. تحديد نقاط الضعف والقابلية للإصابة والتهديدات المختلفة.

٣. تحديد قيم كميّة يمكن قياسها للتهديدات المحتملة وللتأثيرات الناجمة عنها.

٤. توفير توازن اقتصادي ومادي بين تأثير التهديدات والتكلفة الماديّة المطلوبة لأنظمة الحماية اللازمة لمواجهتها.

عادة ما يقوم بعمليـة تحليل المخاطر فريـق متخصص في ذلك يتم تشكيلـه من أقسام المنشأة المختلفة، ويضم التخصّصات الأساسيّة لنشاط المنشأة، مثل: إدارة المنشأة، ومهندسي ومبرمجي تقنية المعلومات، والمختصّين في إجراءات نشاط المنشأة الأساسي، والمختصّين في إجراءات التكامل فيما بين أقسام المنشأة. ومن الأخطاء الدارجة في تشكيل فريق تحليل المخاطر هو اقتصار أعضاء هـذا الفريق على المختصّين في تقنية المعلومات فقط، دون التخصّصات الأخرى، وينتج عن ذلك أن تكون مُخرَجات الفريق غير شاملة للتهديدات المحتملة، كتهديدات الكوارث الطبيعية، أو التهديدات الناتجة من موظفي المنشأة نفسها؛ نتيجة عدم الإلمام الجيّد بالإجراءات، أو عدم التدريب الجيّد على الأنظمة المستخدمة.

عند ممارسة عمليّـة تحليل المخاطر فإنّ من المهـمّ استحضار الأسئلـة الآتية، حيث إنّ إبرازها من وقت لآخر يجعل فريق تحليل المخاطر وإدارة المنشأة على اطّلاع مستمر، و وعي تامّ بما هو المهمّ، وما هو الأهم، وما يجب البدء به، وهذه الأسئلة هي:

- ما التهديدات المحتملة؟ ولأهمية ذلك فقد أفردت موضوعًا مستقلًا لتعريف التهديدات وتحديدها.
- ما تأثيرات التهديدات في حال وقوعها؟
- ما احتمال تكرار حدوث هذه التهديدات؟
- ما درجة حساسية المعلومات والأجهزة والبرامج الخاصة بالمنشأة؟
- من الجهة أو الشخص الأكثر احتماليّة أن يعتدي على معلومات المنشأة؟ وما الدافع وراء ذلك؟
- ما الذي يمكن إن يحصل عليه المعتدي من معلومات؟
- ما مستوى الفشل المتوقع في درء الأخطار؟
- ما نقاط الضعف الموجودة؟
- ما الإجراءات المتبعة لمنع حدوث الأذى؟
- إذا حدث الخطر، كيف يتم تقدير ضرره؟

- ما درجة السِّريّة المتوقعة في الإجابة عن الأسئلة السابقة؟ ففي بعض الحالات والجهات الحساسة تكون الإجابة عن هذه الأسئلة محظورة ومحدودة في أضيق نطاق، من أجل عدم كشف نقاط الضعف في أنظمة الحماية.

والإجابة عن هذه الأسئلة تحدّد كميّة المعلومات الواجب جمعها وتحليلها عن الأخطار المحتملة. فمحاولة درء المخاطر عن المعلومات الحكوميّة الحسّاسة أو الصناعية البالغة التعقيد والسِّريّة يجب أن تشمل الأخطار المحتملة كافة، وأن تُعالج بطريقة صحيحة ومنهجيّة، تختلف جذريًّا عن طُرُق حماية معلومات المنشآت العادية، ويجب أن تشتمل عمليّة تحليل المخاطر على الخطوات الآتية:

١- تحديد التهديدات

كما مرّ معنا، فإنّ الخطر هو احتماليّة أن يستغل عامل التهديد نقاط الضعف الموجودة، مسبّبًا ضررًا للأجهزة والشبكات، و من ثَمَّ الإضرار بنشاط المنشأة. وهناك عوامل كثيرة من عوامل التهديد التي يمكن أن تستغل وجود عدد من نقاط الضعف ونقاط القابلية للإصابة مسببةً مجموعة متنوعة من التهديدات، كما يوضح ذلك الجدول(٨-١).

هناك عدد كبير من التهديدات تتراوح بين الأخطاء الفنيّة، والهجمات الإلكترونيّة، إلى الجواسيس، والمجرمين، والغاضبين، وفيما يلي مجموعة من مصادر التهديدات العامة المحتملة:

أ. الناس: الناس الغرباء والمستخدمون من أكثر المهدّدات لأمن المعلومات. فالناس هم الذين يكتبون فيروسات الحاسب، ويخترقون النظم، ويسرقون البرامج، ويمكن أن يحدث أيّ من هذه الأخطار، سواء من الغرباء، أم من موظفي المنشأة، عمدًا أو بالخطأ.

ب. الأجهزة: ويقصد بالأجهزة هنا معدات المعلومات، من أجهزة حاسب آلي، و وسائط تخزين، وأدوات ربط، وأيّ جهاز يعالج معلومة أو يحفظها أو يخرجها أو ينقلها. وعادة ما تكون الأجهزة هدفًا للأخطار المحتملة، خاصّة التخريب والسرقة، ومن الأمثلة على ذلك وأكثرها انتشارًا هي سرقة أجهزة الحاسب الآلي المحمولة.

عامل التهديد	يستطيع استغلال نقطة الضعف الآتية	يتسبب في التهديد الآتي
الفيروس	عدم وجود برمجيات مكافحة الفيروسات	الإصابة بفيروس حاسب آلي
المخترق	برمجيات غير آمنة تعمل على الخوادم	الوصول غير الشرعي للبيانات السِّريّة
المستخدمون	الإعدادات الخاطئة لنظام التشغيل	اختراق نظام التشغيل
الحرائق	عدم وجود نظام كشف الحرائق ومكافحتها	خراب الأجهزة وتعريض حياة العاملين للخطر
الموظفون	عدم وجود التدريب الجيد، عدم تطبيق اللوائح والأنظمة، عدم وجود المراقبة والتدقيق	الإفصاح عن المعلومات الحساسة والإستراتيجية، الخطأ في إدخال البيانات أو إخراجها أو معالجتها
المقاول	التراخي في تطبيق آليات التحكّم بالدخول	سرقة البيانات أو الأجهزة السِّريّة
المهاجم	وجود برامج تطبيقيّة غير آمنة، عدم إعداد جدار الحماية وتهيئته بشكل جيد	وقوع بعض الهجمات مثل هجوم تعطيل الخدمة (Denial of Service-DoS)
متسلل (بشري)	عدم وجود أنظمة الحماية الماديّة	سرقة الأجهزة

الجدول (٨-١): أمثلة توضح العلاقة بين عوامل التهديد، والتهديد، ونقاط الضعف

ج. البرمجيّات: تعدّ البرمجيات الأداة المسؤولة عن تنفيذ المهام في الحاسب الآلي، وتتعرض البرمجيات لتهديدات كثيرة، منها: النّسخ غير القانوني، والسرقة، والتعديل، والتخريب، وتعريضها للفيروسات أو الفقد النهائي.

د. الكوارث الطبيعية والبيئيّة: تشكّل الكوارث الطبيعية، كالحرائق، والفيضانات، والهزّات الأرضيّة خطرًا على المباني ونظم الحاسب الآلي على حدٍّ سواء، وكذلك

الحال لكوارث المناخ والتبريد وخدمات الكهرباء.

٢- جمع المعلومات وتحليلها

وتشمل هذه الخطوة جمع المعلومات الضرورية عن كل تهديد محتمل، وتبويبها، وترتيبها، و وضع احتماليّة حدوث كل منها. وتشمل كذلك تحديد الأسباب التي قد تؤدي لوقوع الخطر، وما مجالات التعرّض التي تؤدي إلى ذلك، وما هي الإجراءات غير المناسبة التي كانت متوفرة، وما هي الإجراءات المطلوب إيجادها الآن. وتساعد هذه الخطوة في ترتيب أولويات مواجهة الأخطار، التي تنعكس بدورها على قياس حجم المخاطر، ثم الإجراءات الاحتياطية التي يجب اتخاذها قبل وقوع الخطر. ويمكن جمع هذه المعلومات بعدة طُرُق من أهمها: استخدام النماذج والاستبانات المعدة مسبقًا، والمسح الميداني، والمقابلات الشخصية، و ورش العمل.

عندما تُحدّد التهديدات والثغرات المقابلة لها، التي يمكن النفاذ من خلالها، فإنّ مهمة تحليل المخاطر ستكون أسهل، وسيكون بالإمكان تحديد الخسائر الفوريّة والمستقبلية إذا ما تحوّل تهديد ما إلى خطر حقيقي حل بالمنشأة. ومن الأمثلة على الخسائر الفورية: تدمير البيانات، وتعطل الأنظمة والخدمات، والكشف عن البيانات السِّريّة، وانخفاض إنتاجية الموظفين، ومن الأمثلة على الخسائر المستقبلية: انخفاض أداء المنشأة بمرور الوقت، وتطبيق عقوبات التأخير في تقديم الخدمات أو توفير المنتجات، وارتفاع تكاليف إعادة بيئة المنشأة إلى وضعها السابق كما كان قبل وقوع التهديد.

٨-٤-١ طُرُق تحليل المخاطر المعلوماتيّة

هناك نوعان رئيسان من أنواع تحليل المخاطر المعلوماتيّة هما: التحليل الكمّي والتحليل النوعي(أو الكيفي)[١]، ولكلٍّ منهما مفهومه وخطواته ومميزاته، وقد يناسب أحد هذين النوعين من التحليل بيئة معيّنة، نتيجة لطبيعة عملها وطبيعة التهديدات المحتملة لمواردها وقدرة موظفيها، بينما لا يناسب بيئة أخرى، وفيما يلي نتطرق بشيء من التفصيل لهذين النوعين.

٨-٤-١-١ التحليل الكمّي للمخاطر المعلوماتيّة

يعتمد التحليل الكمّي على إعطاء أرقام حقيقية ذات معنى لكل عنصر من عناصر التحليل

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

المعلوماتـي، بحيث يمكن قياس هـذا العنصر من خلال الرقم المخصص له. وتختلف هذه العناصر باختلاف المنشأة وطبيعـة نشاطها الأساسي، إلا أن هنـاك مجموعة من العناصر الأساسيّة التي يعتمد عليها التحليل الكمّي في الغالب، وهي:

- تكلفة الحماية الماديّة بشقيها: الحماية الماديّة الإداريّة، والحماية الماديّة الفنيّة.
- قيمة موارد المنشأة المراد حمايتها، مثل: البرامج التطبيقيّة، وقواعد البيانات، وأجهزة الخوادم الرئيسة، ومرافق المنشأة.
- درجة التأثير في نشاط المنشأة.
- تكرار التهديد.
- جودة أنظمة الحماية الماديّة.
- احتمال استغلال الثغرات.
- خطورة نقاط الضعف.

ما يتم في التحليل الكمّي للمخاطر المعلوماتيّة هو تحديد رقم مناسب لكل عنصر من هذه العناصر، ثـم إدخال هذه الأرقام في معادلات رياضية لإجـراء حسابات التحليل عليها، كما سيأتي معنا، ومن ثم الحصول على نتائج التحليل، و من ثَمَّ تحديد أنظمة الحماية المناسبة.

خطوات التحليل الكمّي

هناك عدد كبير من عناصـر التحليل الكمّي، وهناك عدد من المعـادلات الرياضيّة التي تستخدم مع قيم هذه العناصر لإجراء عمليّة التحليل. ويتم تنفيذ عمليّة التحليل الكمّي من خلال خطوات محدّدة تطبق مع كل عمليّة تحليل لكل خطر، وهذه الخطوات هي:

أولًا: إعطاء أو تحديد قيمة (بالريال) لموارد المنشـأة والمكوّنات المراد حمايتها من خلال الإجابة عن كل سؤال من الأسئلة الرئيسة الآتية:

- ما قيمة هـذا المورد أو المكوّن بالنسبـة للمنشأة؟ لاحظ أنّه يمكـن إعطاء قيمة عليا لأهم مورد على الإطـلاق، وقيمة صغرى لأقل مورد، ثم توزيـع قيم بقية الموارد بين هاتين القيمتين.

- كم تكلفة الاحتفاظ بهذا المكوّن والاستمرار بالاستفادة منه؟
- كم قيمة مساهمة هذا المورد في إنتاجية المنشأة؟
- كم تكلفة إعادة الحصول عليه في حالة فقده، سواءً بإعادة إنشائه (كإعادة كتابة برنامج تطبيقي من جديد)، أو استرجاعه (كاسترجاع برنامج تطبيقي مفقود، أو معطوب وإعادته كما كان في السابق)؟

ثانيًا: تقدير الخسارة الناتجة عن التهديد من خلال الإجابة عن الأسئلة الآتية:

- ما الدمار أو العطب الذي يسببه التهديد؟ وكم تكلفة ذلك الدمار أو العطب؟
- ما الخسارة الماديّة أو الخسارة في الإنتاجية التي يسببها التهديد؟ وكم تكلفة ذلك؟
- ما قيمة الخسارة التقديرية في حالة انكشاف المعلومات السِّريّة؟
- ما تكلفة استعادة الوضع من هذا التهديد؟
- ما القيمة المفقودة في حال تعطل الأجهزة أو قصورها عن العمل؟
- ما قيمة الخسارة الأحاديّة المتوقعة (Single Loss Expectancy-SLE) لكل مورد من موارد المنشأة ولكل تهديد. وقيمة الخسارة الأحادية المتوقعة هي قيمة خسارة المنشأة في حالة حدوث التهديد لمرّة واحدة، وتحسب كالآتي:

SLE = قيمة المورد × عامل التعرض (Exposure Factor-EF)، حيث إنّ:

قيمة المورد = القيمة المحدّد للمورد كما في الخطوة "أولا".

EF = عامل التعرّض، وهو النسبة المئوية التي يتم خسارتها من قيمة المورد عند وقوع تهديد معين عليه.

مثال (٨-١): لو اعتبرنا أن أحد موارد المنشأة هو مستودع الأجهزة، وأن قيمة هذا المستودع تساوي (١٥٠،٠٠٠) ريال، وأن من المتوقع خسارة (٢٥٪) من المستودع لو أصابه حريق، وليس أكثر من ذلك؛ لأن أنظمة مكافحة الحرائق سوف تعمل وتقلل من الخسائر، فإنّ:

الخسارة الأحادية المتوقّعة (SLE) = ١٥٠،٠٠٠ × ٠,٢٥ = ٣٧،٥٠٠ ريال.

في هذه الحالة، لاحظ أن المورد هو "المستودع"، وأن التهديد هو "الحريق". ◊

ثالثًا: تحليل التهديد باتباع الخطوتين الآتيتين:

- تجميع المعلومات اللازمة عن احتمال كل تهديد ينتج عن البشر في كل قسم من أقسام المنشأة، ويمكن في هذه الخطوة الرجوع لسجلّات أمن المعلومات لدى لكل قسم.
- حساب معدل الظهور (أو الحدوث) السنوي للتهديد (Annual Rate of Occurrence-ARO) وهذا المعدّل هو عدد مرّات ظهور التهديد (أي تكرار الظهور) في مدّة اثني عشر شهرًا.

مثال (٨-٢): لو كان احتمال حدوث فيضان في منطقة وجود المنشأة هو مرّة واحدة كل عشر سنوات فإنّ:

معدّل الظهور السنوي للفيضان (ARO) = ١ ÷ ١٠ = ٠,١ ◊

رابعًا: حساب الخسارة السنويّة الإجماليّة لكل تهديد، ويتم ذلك بالطريقة الآتية:

- ربط الخسارة باحتمال حدوث التهديد، بمعنى أنّه يمكن أن يتكرّر حدوث التهديد لأكثر من مرّة خلال العام، و من ثَمَّ يجب أن يتم حساب الخسارة الإجمالية الناتجة من مجموع حالات تكرار التهديد.
- حساب الخسارة السنوية المتوقعة (Annual Loss Expectancy-ALE) لكل تهديد باستخدام المعلومات المستنتجة من الخطوات الثلاث السابقة، كالآتي:
- الخسارة السنويّة المتوقّعة (ALE) = قيمة الخسارة الأحادية المتوقعة (SLE) × معدّل الظهور السنوي (ARO).

مثال (٨-٣): بالرجوع لمثال (٨-١)، وباعتبار أنّ معدل الظهور السنوي للحريق هو (٠,١)، أي مرّة واحدة لكل عشر سنوات، فإنّ:

الخسارة السنويّة المتوقعة (ALE) = ٣٧،٥٠٠ × ٠,١ = ٣،٧٥٠ ريال. ◊

خامسًا: تحديد أنظمة الحماية والمضادات اللازمة لمكافحة كل تهديد، ثم حساب نسبة التكلفة إلى الفائدة (التكلفة/الفائدة) لهذه الأنظمة، ثم الاختيار من بين الخيارات الآتية لكل خطر حسب نتائج الخطوات السابقة:

- تقليل الخطر: ويقصد بذلك تقليل آثار الخطر، ويمكن فعل ذلك ببعض أو بكل الطرق الآتية:
  - تركيب أدوات تحكم إضافية وتشغيلها.
  - تحسين طريقة الأداء والعمل.
  - تعديل بيئة العمل بما يقلل من الخطر.
  - توفير أنظمة كشف الخلل في وقت مبكر.
  - تنفيذ المزيد من التدريب والتوعية بأمن المعلومات، مع التركيز على الخطر محل التحليل.
- تحويل الخطر: ويقصد بذلك ترحيل آثار الخطر إلى موارد أخرى أقل أهميّة من الموارد التي يهدّدها الخطر أصلًا، كالتأمين على المورد، ثم ترحيل الخطر أو الخسارة إلى شركة التأمين.
- قبول الخطر: ويقصد بذلك التعايش مع الخطر دون بذل مزيد من الجهود والتكاليف للحماية منه، ومعنى ذلك أن المنشأة على علم بالخطر وبمستواه، وبالخسائر المتوقعة منه، لكنّها قررت قبوله. ويمكن اختيار هذا الخيار في حالات الأخطار التي يمكن التعايش معها، وليس كل الأخطار، وفي الحالات التي يشير فيها تحليل الكلفة والفاعلية إلى أنّ تكلفة نظام الحماية من هذا الخطر تفوق الخسائر المتوقعة منه.
- تفادي الخطر أو منعه: ويقصد بذلك تطبيق نظام حماية جيّد يمنع من وقوع الخطر، أو في حالة فشل ذلك إيقاف النشاط(إن أمكن ذلك) الذي سبب هذا الخطر بشكل تام، وبذلك يمكن تلافي الخطر كليًّا. ومن الأمثلة على ذلك السماح للمستخدمين باستخدام نظام المحادثة أو الرسائل الآني(Instant Messaging)، الذي قد يسبّب بعض الثغرات الأمنيّة، خاصّة إذا لم يتم تدريب مستخدميه على الاحتياطات الأمنيّة جيّدًا. فإيقاف استخدام هذا النظام خاصّة إذا كان لا يتطلبه نشاط المنشأة الأساسي يحول دون وقوع الأخطار الناتجة عنه، ويمكن بذلك تلافيها جميعًا.

نتائج التحليل الكمّي

بعد القيام بالخطوات الخمس السابقة لكل تهديد محتمل على كل مورد من موارد المنشأة، فسيكون لدى فريق التحليل وإدارة المنشأة المعلومات الكافية على شكل أرقام حقيقيّة، يمكن من خلالها تحديد أولويات التعامل مع التهديدات كلٌّ على حدة، ومعرفة أي التهديدات يجب البدء بمواجهته أولًا؟ وأيّها يمكن التعايش معه؟ ومن أهم نتائج التحليل الكمّي ما يلي:

- معرفة قيمة موارد المنشأة على شكل أرقام تمثل قيمة كل مورد بالريال.
- تحديد قائمة بالتهديدات المحتملة وأولوية كل منها.
- معرفة معدل الظهور السنويّ لكل تهديد.
- معرفة الخسارة السنويّة الناتجة عن كل تهديد.
- تحديد أنظمة الحماية والمضادات المقترحة لمجابهة كل تهديد.

مثال(٨-٤): أجري التحليل الكمّي للمخاطر المعلوماتيّة التي تهدّد منشأة تجاريّة وفق الخطوات السابقة، وقد جاءت النتائج كما في الجدول(٨-٢)[١] وقد اشتمل هذا التحليل على تهديد واحد فقط لكل مورد من موارد المنشأة، من أجل تسهيل عمليّة التحليل، رغم أنّه يجب أن يشمل التحليل جميع التهديدات المحتملة لكلّ مورد من الموارد. ◊

تساعد بيانات نتائج التحليل الكمّي في جدول(٨-٢) إدارة المنشأة في اتخاذ عدد من القرارات، ومعرفة احتمال وقوع كلّ تهديد، والخسارة الناتجة عنه. فمثلًا تشكّل معلومات البطاقات الائتمانية لعملاء المنشأة في الجدول (٨-٢) أهم الموارد على الإطلاق لأنّها أعلاها قيمة، ويشكل تهديد «سرقة» هذه المعلومات أهم التهديدات

١- مأخوذ من المرجع: Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

المورد	التهديد	الخسارة الأحادية المتوقعة(SLE)	معدل الظهور السنوي(ARO)	الخسارة السنوية المتوقعة(ALE)
مرفق من المرافق	الحريق	٢٣٠،٠٠٠ ر.س.	٠,١	٢٣,٠٠٠ ر.س.
أسرار تجارية	السرقة	٤٠،٠٠٠ ر.س.	٠,٠١	٤٠٠ ر.س.
جهاز خادم الملفّات	التعطل	١١،٥٠٠ ر.س.	٠,١	١،١٥٠ ر.س.
البيانات	الفيروسات	٦،٥٠٠ ر.س.	١,٠	٦،٥٠٠ ر.س.
معلومات البطاقات الائتمانية	السرقة	٣٠٠،٠٠٠ ر.س.	٣,٠	٩٠٠،٠٠٠ ر.س.

الجدول(٨-٢): جدول نتائج التحليل الكمّي للمخاطر المعلوماتيّة لمنشأة تجارية

التي يجب البدء بمواجهتها، حيث إنه يملك أعلى معدّل ظهور سنوي، ومن المتوقع أن تكون هناك خسارة سنويّة من هذا التهديد تقدر بمبلغ تسعمائة ألف ريال، وهي أعلى خسارة سنويّة متوقّعة مقارنة بباقي التهديدات. وكذلك فإنّ من المنطقي والمفروض أن لا تتجاوز تكلفة نظام مكافحة الفيروسات مبلغ(٦،٥٠٠) ريال لكل سنة، طالما أنّ الخسارة السنويّة المتوقّعة من تهديد الفيروسات لا تتجاوز ذلك المبلغ، وكذلك فإنّ من الضروري جلب هذا النظام؛ لأنّ معدل ظهور الفيروسات هو مرّة واحدة لكل سنة، وهذا يعني أن المنشأة ستتعرض لهجوم فيروسي كل عام، ويجب الاستعداد له.

٨-٤-١-٢ التحليل النوعي للمخاطر المعلوماتيّة

لا يعتمد هذا النوع من التحليل على تحديد أرقام ومبالغ ماليّة لموارد المنشأة يصعب تحديدها، ولا على عمليّات حسابيّة معقدة، وإنّما يعتمد على آراء الخبراء في تقويم خطورة(أو جدية) التهديد من خلال إعطاء كل تهديد درجة خطورة(درجة جدية) محدّدة، ثم تقويم

قابلية تطبيق أنظمة الحماية المضادة له. ويمكن إجراء التحليل النوعي من خلال تطبيق عدد من آليات معالجة الآراء، ومنهـا: التحكيم، والخبرات العلميّة والعمليّة، والحدس واستنباط المعرفة، والتجارب السابقة. ولا شكّ أنّ هذه الآليات تحتاج إلى طُرُق لجمع المعلومات التي يمكن من خلالها تنفيذ هذه الآليات، ومن هذه الطرق: العصف الذهني، و ورش العمل، والزيارات الميدانية، والاستبانات التـي على شكل أسئلة، وقوائم الخيـارات، والاجتماعات، والمقابلات الشخصية. يجب علـى الفريق القائم بهذا النوع من التحليل اختيـار آلية التحليل المناسبة، وطريقة جمع المعلومات المناسبة لطبيعة التهديد، وطبيعة عمل المنشأة؛ إذ قد يكون هناك آلية وطريقة لجمع المعلومات لكل تهديد مختلفة عن الآليات والطرق المستخدمة للتهديدات الأخرى.

يمكن تلخيص خطوات التحليل النوعي للمخاطر المعلوماتيّة في الخطوات الآتية:

أولًا: تحديد الموظفين الذين لديهم الخبرة العمليّة والخلفية العلمية الجيّدة عن التهديد محلّ التحليل (الخبراء)، ثم تزويدهم بالمعلومات اللازمة عن التهديد، بعد جمعها باستخدام إحدى طُرُق جمع المعلومات المذكورة آنفًا، علـى شكل سيناريو يصف أسباب التهديد، وكيف يقع؟ وآثاره وملابساته في حدود صفحة أو صفحتين فقط.

ثانيًا: يقـدّم كل شخص من هؤلاء الخـبراء تقويمه للتهديد من خـلال نموذج معدّ لهذا الغرض (من قبل فريق التحليل النوعي)، بحيث يشمل رأيه في كل مما يأتي:

- احتمال وقوع التهديد.
- تقدير الخسارة الناتجة عن التهديد لدى وقوعه.
- تقويم نظم الحماية أو المضادات المناسبة لهذا التهديد (سيحدّدها له فريق التحليل)، ومن ثم تحديد أولويات تطبيق هذه الأنظمة.

يمكن تحديد قيم كل من احتمال وقوع التهديد والخسارة الناتجة عنه بإحدى طريقتين: إمّا باختيار أحد المستويات: عالٍ، أو وسط، أو منخفض، أو باختيار القيمة المناسبة من التدريج من (١) إلى (٥) (أو من (١) إلى (١٠)) الذي يُحدّده فريق التحليل.

ثالثًا: جمع تقارير هؤلاء الخبراء من قبل فريق التحليل، ثم دمجها في تقرير موحّد يقدّم

لإدارة المنشأة للمساعدة في اتخاذ قرار مواجهة التهديد.

مثال(٨-٥)[١]: كتب فريق التحليل النوعي سيناريو مكونًا من صفحة واحدة يشرح أحد التهديدات، وهو عبارة عن وصول مهاجم غير شرعي لبيانات سريّة مخزّنة على خمسة خوادم ملفّات لدى إحدى الشركات المتخصصة في تطوير البرمجيات. ثم وزّع فريق التحليل هذا السيناريو على خمسة من الموظفين الخبراء فيها، وهم: مدير إدارة تقنية المعلومات، ومدير قواعد البيانات، وكبير المبرمجين، ومهندس نظام التشغيل، ومدير إدارة الجودة، وجرى تزويدهم كذلك بنموذج تقويم لتقويم: درجة خطورة التهديد، والخسارة المتوقعة، ومدى ملاءمة وكفاءة كلٍّ من المضادات الآتية: تركيب جدار حماية(Firewall)، وتركيب نظام كشف التطفل(Intrusion Detection System-IDS)، وتركيب نظام فخ العسل(Honeypot System)[٢]، على أن يجري التقويم باختيار القيمة المناسبة على التدريج من(١) إلى(٥)، حيث إن(١) هو أقل خطورةً أو أقل كفاءةً أو أقل احتمالًا و(٥) هو أعلاها، وقد جاءت النتائج كما في الجدول(٨-٣) وقُدِّمت هذه النتائج على شكل تقرير لإدارة المنشأة، كانت نتيجته أن تركيب نظام جدار الحماية سيحمي من هذا التهديد أفضل من المضادات الأخرى؛ لأنّ متوسّط آراء الخبراء في كفاءة هذا المضاد هو الأعلى مقارنة بمتوسط المضادّات الأخرى. ◊

١- مأخوذ من المرجع: Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

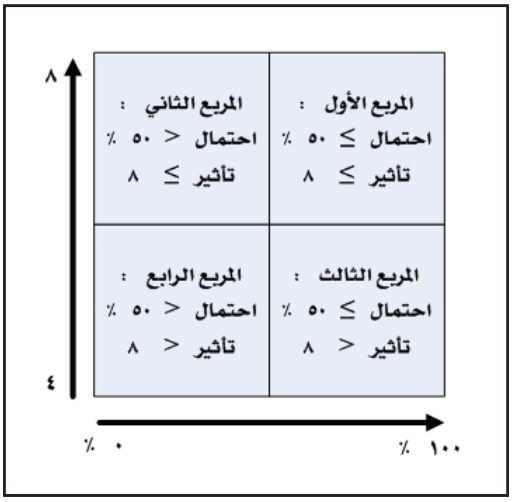
٢- نظام فخ العسل: هو نظام، قد يكون برنامجًا تطبيقيًا أو موقعًا على شبكة الإنترنت، للإيقاع بالمهاجم وكشف هويته من خلال طريقة تعامله مع النظام(الفخ) أو من خلال المعلومات التي يختارها أو يدخلها.

التهديد = مهاجمة المعلومات السِّريّة	خطورة (جدية) التهديد	احتمال وقوع التهديد	الخسارة المتوقعة	درجة كفاءة المضادات المكنة		
				جدار الحماية	نظام كشف التطفل	نظام فخ العسل
مدير إدارة تقنية المعلومات	٤	٢	٤	٤	٣	٢
مدير قواعد البيانات	٤	٤	٤	٣	٤	٢
كبير المبرمجين	٢	٣	٣	٤	٢	١
مهندس نظام التشغيل	٣	٤	٣	٤	٢	١
مدير إدارة الجودة	٥	٤	٤	٤	٤	٢
متوسط المجاميع	٣,٦	٣,٤	٣,٦	٣,٨	٣	١,٤

الجدول(٨-٣): التحليل النوعي للمخاطر المعلوماتيّة

يوضح المثال السابق طريقة التحليل النوعي لتهديد واحد فقط، هو «الوصول للمعلومات السِّريّة من قبل مهاجم غير شرعي» وعلى فريق التحليل النوعي تقديم تقارير مشابهة لكل تهديد من التهديدات المحتملة؛ ليتم على ضوئها ترتيب أولويات التعامل مع تلك التهديدات، وتحديد أنظمة الحماية المناسبة لها بشكل متكامل.

من الآليات المتّبعة للتحليل النوعي الجماعي لجميع التهديدات المحتملة هو استخدام مصفوفة المخاطر، التي تتكوّن من أربعة مربعات كما في الشكل(٨-٢).



الشكل(٨-٢): مصفوفة المخاطر

يحتوي المربع الأول(العلوي الأيمـن) من المصفوفة المخاطر عالية التأثير وعالية احتمال الحدوث، ويحتوي المربع الثاني(العلوي الأيسر) المخاطر عالية التأثير وقليلة احتمال الحدوث، ويحتوي المربع الثالث(السفلي الأيمن) المخاطر قليلة التأثير وعالية احتمال الحدوث، ويحتوي المربع الرابع(السفلي الأيسر) المخاطر قليلة التأثير وقليلة احتمال الحدوث، وتحتوي المصفوفة كذلك تدريجًا أفقيًّا من اليسار إلى اليمين يبدأ من(صفر٪) إلى(١٠٠٪) يعكس احتمال حدوث كل خطر، وعلى تدريج رأسي من الأسفل إلى الأعلى يبدأ من(٤) إلى(١٢) يعكس درجة تأثير كل خطر، وبذلك فإنّ المربع الأول يحتوي المخاطر التي لها احتمال حدوث من(٥٠٪) فأعلى، وتأثير من(٨) فأعلى، ويحتوي المربع الثاني المخاطر التي لها احتمال حدوث أقل من(٥٠٪) وتأثير من(٨) فأعلى، ويحتوي المربع الثالث المخاطر التي لها احتمال حدوث من(٥٠٪) فأعلى وتأثير أقل مـن(٨)، ويحتوي المربع الرابع المخاطر التي لهـا احتمال حدوث أقل من(٥٠٪) وتأثير أقل من(٨). بناءً على ذلك فإنّ مجموعة المخاطر التي تقع في المربع الأوّل هي المخاطر ذات الأولويّة في الاستعداد لهـا ومجابهتها، والمخاطر التي تقع في الزاوية العلويّة اليمنى من هذا المربع هي المخاطر ذات الأولويّة القصوى من بين تلك المخاطر.

٨-٤-١-٣ مقارنة بين التحليل الكمّي والنوعي

رغم أنّ التحليل الكمّي يقدّم نتائج واضحة ومحدّدة على شكل أرقام، إلا أنه من الصعوبة

بمكان إجراء مثل هذا النوع من التحليل في البيئات التقنيّة نظرًا لصعوبة تحديد قيم موارد المنشأة (بالريال) بشكل دقيق، واعتماده على إجراء عمليّات حسابيّة معقدّة. فمثلًا لا يمكن الجزم بأنّ معدّل حدوث حريق في مرفق من مرافق المنشأة هو مرّة واحدة كل عشر سنوات، وأنّ الخسارة المتوقعة لذلك هي (٢٣٠،٠٠٠) ريال، انظر الجدول (٨-٢).

وفي المقابل يعتمد التحليل النوعي بدرجة أساسية على آراء الخبراء وتقويمهم للتهديد والأنظمة المضادة له، دون إجراء أيّ عمليّات حسابيّة معقّدة، وهو ما يجعل نتائج التحليل واختيار أنظمة الحماية المضادة تختلف باختلاف تلك الآراء، وباختلاف خلفيّاتهم العلميّة وخبراتهم العمليّة.

كغيرها من أنواع التحليل فإنّ لكل من التحليل الكمّي والتحليل النوعي مميزاته الخاصة به، التي يمكن استخدامها في المقارنة فيما بينهما، واختيار التحليل المناسب لكل تهديد. فمثلًا يمكن أتمتة التحليل الكمّي وتنفيذه بشكل آلي، بينما لا يمكن عمل ذلك في التحليل النوعي، وعلى الجانب الآخر، يقدّم التحليل النوعي مساحة أكبر لتحليل التهديدات بشكل جماعي، ويوفر المؤشرات اللازمة لذلك، بينما لا يوفر ذلك التحليل الكمّي، انظر الجدول (٨-٤)[١].

الخاصية	التحليل الكمّي	التحليل النوعي
لا يحتاج إلى عمليّات حسابية معقدة	لا	نعم
يحتوي عمليّات تخمين	لا	نعم
يوفر مساحات ومؤشرات أكبر للتحليل	لا	نعم
أسهل للتقويم وتنفيذه بشكل آلي	نعم	لا
يستخدم لمتابعة الأداء لاحقًا	نعم	لا
يساعد على إجراء تحليل الكلفة/الفائدة	نعم	لا
يستخدم معايير تقويم مستقلة	نعم	لا
يقدم آراء الخبراء الذين لديهم الخلفية عن العمل	لا	نعم
يقدم الخسارة المتوقعة في سنة كاملة بشكل محدّد	نعم	لا

الجدول (٨-٤): مقارنة بين كل من التحليل الكمّي والتحليل النوعي للمخاطر المعلوماتيّة

١- مأخوذ من المرجع: Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

٨-٥ اختيار أنظمة الحماية

بعد إجراء عمليّة التحليل للمخاطر المعلوماتيّة سواءً أكان تحليلًا كميًّا أم نوعيًّا، فإنّ الخطوة الآتية هي اختيار نظام الحماية المناسب، الذي يطلق عليه أحيانًا النظام المضاد للخطر. ورغم أن هناك عددًا كبيرًا من التهديدات، فإنّه لا بدّ من دراسة كل تهديد على حدة، وتحليله ثم وضع النظام المضادّ المناسب له. وكنتيجة لتعدّد التهديدات، فإنّ هناك عددًا كبيرًا أيضًا من أنظمة الحماية المتاحة، التي أصبحت معروفة ومناسبة للبيئات التقنية، منها: التحكّم بالوصول، وأنظمة مكافحة البرمجيات الضارّة، وأنظمة مكافحة الهجوم والتجسّس والاصطياد الإلكتروني، وحماية شبكات الحاسب الآلي، وأنظمة استمرارية الأعمال والنّسخ الاحتياطي، إلى غير ذلك من أنظمة الحماية التي يحتويها هذا الكتاب.

يجب أن يجري اختيار نظام الحماية الذي يستطيع أن يقدّم الحماية المطلوبة وبكلفة مناسبة، تضمن عدم تجاوز تكلفة الخسائر المترتبة عن التهديد حال وقوعه، وهذا يتطلّب نوعًا آخر من التحليل يسمّى تحليل الكلفة/الفائدة (أو الكلفة/الفاعلية). ويعتمد هذا التحليل على معرفة قيمة نظام الحماية للمنشأة (بالريال)، التي يمكن الحصول عليها من المعادلة الرياضيّة الآتية:

قيمة نظام الحماية = (قيمة الخسارة السنوية المتوقعة (ALE) قبل تطبيق نظام الحماية) - (قيمة الخسارة السنوية المتوقعة (ALE) بعد تطبيق نظام الحماية) - (التكلفة السنوية لنظام الحماية).

كلما كانت هذه القيمة أعلى كان نظام الحماية أفضل وذا فائدة أو فاعلية أعلى للمنشأة، حيث إنه سيشكّل قيمة ماديّة أكبر من مجموع الخسارة الناتجة عن التهديد وتكلفة تشغيله وصيانته.

مثال (٨-٦): لو كانت قيمة (ALE) قبل تطبيق نظام الحماية لتهديد ما هي (١٢،٠٠٠) ريال، وقيمتها بعد تطبيق نظام الحماية هي (٣،٠٠٠) ريال، والتكلفة السنوية لتشغيل وصيانة نظام الحماية هي (٦٥٠) ريالًا، فإنّ قيمة نظام الحماية للمنشأة هي (٨،٣٥٠) ريالًا لكل سنة.

بمعنى أنه يمكن اعتبار أن نظام الحماية هذا سيوفّر على المنشأة مبلغ(٨،٣٥٠) ريالًا سنويًا، وأن المنشأة قد تتعرّض لخسارة قيمتها(١٢،٠٠٠) ريالًا في حال عدم تطبيقه. ◊

٨-٦ اتخاذ الإجراءات الاحترازيّة لمواجهة المخاطر المعلوماتيّة

يقصد بها الإجـراءات والإحتياطات القبْلية التي يجب اتخاذهـا قبل حدوث الخطر، أو بعبارة أخرى: تحديد الإجراءات المضادة لكل تهديد محتمل، ويجب أن تشمل جميع المخاطر المحتملة، التي حُدّدت وجُمعت المعلومات الضرورية عنها في مرحلة تحليل المخاطر، وفي هذه المرحلة يجري تحديد وتوثيق جميع ما يجب عمله، وإيجاد البدائل المناسبة لكل حدث، وليس بالضرورة تنفيذ ذلك فـورًا، إذ إن هناك بعض الإجراءات لا تنفّـذ إلا عند التأكد من قرب وقوع الخطر، أو عند وقوعه فعلًا.

هناك جملة من الاستعدادات والتدابير الاحترازيّة التي يجب الأخذ بها لمواجهة أيّ خطر يهدّد النظام المعلوماتي بالمنشأة. وتساعد هذه التدابير كذلك على مواجهة الكوارث المعلوماتيّة التي تنشأ عن بعض الأخطار التي تحوّلت إلى كوارث معلوماتيّة أو الكوارث التي تفاجئ المنشأة والعاملين بها، خاصّة الطبيعية منها، ومن هذه الاستعدادات والتدابير الاحترازيّة ما يلي:

تجهيز البدائل والمعدّات مسبقًا

يجب توفير الحلول البديلة من أجهزه وبرامج ومعدّات لاستخدامها في حال وقوع الخطر أو تحوّلـه إلى كارثة، ويجب أن تكـون هذه البدائل جاهزة، مع ضـرورة التدريب الجيّد على استخدامها، ومن أهم ما يجب توفيره كبدائل جاهزة ما يلي:

- أجهزة خوادم رئيسة مثبّت عليها جميع البرامج اللازمة.
- أجهزة حاسب آلي طرفيّة مثبّت عليها جميع البرامج اللازمة.
- أجهزة الربط الرئيسة المركزيّة لشبكة الحاسب الآلي.
- نُسخ أصلية جاهزة للاستخدام مـن أنظمة التشغيل والبرامج التطبيقيّة العاملة مع أرقامها التسلسلية ومفاتيح حمايتها.
- أشرطة وأقراص تخزين خالية ومهيّأة للاستخدام الفوري.

- العِدد والأدوات التي قد تظهر الحاجة إليها عند وقوع الخطر (أو الكارثة)، مثل عدد الصيانة والبطاريات ومصابيح الإضاءة (الكشافات).
- بعض الكابلات الإضافية و وصلات الكابلات.

النسخ الاحتياطي

إنّ من أهم ما يعوّل عليه في استعادة المعلومات المفقودة، أو إعادة تشغيل النظام المعلوماتي باستخدام أجهزة جديدة بعد حدوث خطر أو كارثة معلوماتيّة، هو وجود نُسخ احتياطيّة سليمة وشاملة لجميع المعلومات المفقودة. لذلك يجب أن تكون خطة النّسخ الاحتياطي سليمة ومعدّة بعناية، كما يجب أن تُختبَر باستمرار، ومن أهم التدابير اللازمة لذلك:

- وضع جدول زمني للنّسخ الاحتياطي، بحيث يكون هناك نُسخ يوميّة، وأسبوعيّة، وشهريّة، وسنويّة.
- أخذ نُسخ احتياطية كاملة (Full)، وأخرى للإضافات اليومية (Incremental) فقط، بحيث يشمل كلّ منهما جميع معلومات المنشأة، بما في ذلك جميع قواعد البيانات، والملفّات، ومعلومات حسابات المستخدمين.
- يجب مراعاة أن تكون المعلومات المنسوخة حديثة وبفترات زمنية متقاربة، حتى يمكن استعادة آخر تحديث على المعلومات عند الحاجة.
- تخزين أشرطة أو وسائط النسخ الاحتياطي في أماكن تخزين مناسبة ومعدّة لهذا الغرض.
- القيام بعملية استرجاع (Restore) للمعلومات من وسائط النسخ الاحتياطيّة إلى أجهزة فعليّة مشابهة تمامًا للأجهزة العاملة دوريًّا؛ من أجل التأكّد من صحّة عمليّة الاسترجاع نفسها، وأنّه يمكن تنفيذها في أيّ وقت متى ما دعت الحاجة إلى ذلك، وكذلك للتأكد من سلامة النسخ الاحتياطية الموجودة.

خرائط الموقع والشبكة ومخططاتها

يجب تجهيز الخرائط والمخططات الآتية من أجل استخدامها عند الحاجة:

- خريطة الموقع بشكل عام.
- مخطّط شبكة الحاسب الآلي، بما في ذلك نقاط التجميع (الكبائن) الرئيسة، وأجهزة الموزّعات (Switches) والموجّهات (Routers)، والتمديدات الخارجيّة، وخطوط الألياف البصريّة، وخطوط الربط مع الشبكة الواسعة (WAN)، وأجهزة أمن المعلومات، مثل جدران النار، وأجهزة تخزين المعلومات.
- مخطط مركز البيانات (Data Center) (أو غرفة الأجهزة الرئيسة) بشكل تفصيلي وبجميع محتوياته.
- خريطة خطوط تغذية الطاقة الكهربائيّة.
- خريطة المداخل والمخارج العادية وأخرى لمخارج الطوارئ.

يجب وضع المعلومات الضروريّة عن محتويات كلّ مخطّط أو خريطة على المخطّط أو الخريطة نفسها، وحفظ هذه المخطّطات والخرائط بطريقة يسهل الرجوع إليها عند الحاجة، وينصح بشدّة عمل مخطّط واحد كبير الحجم يحوي جلّ هذه المخطّطات والمعلومات، و وضعه في مكانٍ مناسب وبشكلٍ دائم.

يجب كذلك تجهيز المعلومات الضروريّة عن كل برنامج أو نظام تشغيل يجري استخدامه بحيث تشمل ما يأتي:

- وصف موجز للنظام والمهام التي يؤدّيها.
- الإصدار المستَخدم، مع توضيح ذلك على الأقراص الخاصّة به.
- الطريقة التفصيليّة لتثبيت البرنامج أو نظام التشغيل على الأجهزة من جديد.
- متطلّبات البرنامج أو نظام التشغيل من أجهزة وذاكرة ومساحة تخزين فارغة على الأجهزة المراد تثبيته عليها، والبرامج التي يجب تثبيتها قبل تثبيته.

ملفات سجلّات الأعمال (Log Files)

يُقصد بملفات سجلّات الأعمال (Log Files) الملفّات التي سجَّل الأعمال التي تمت على الأجهزة والبرامج فيها برامج التشغيل وأنظمته والمستخدمون. وعادة ما تتوافر هذه الخدمة

في أنظمة التشغيل والبرامج بحيث يتم تهيئتها مرّة واحدة، وبعد ذلك تسجّل جميع الأحداث والتغييرات والأخطاء والتحذيرات وتواريخها وأوقاتهـا آليًّا، وتخزّنها على ملفّ نصيّ يمكن فتحه وقراءتـه بسهولة من أيّ نظام تشغيل. ويمكن من خلال هذه الملفّات تتبع ما حدث قبل وأثنـاء وقوع الخطر (أو الكارثة) الأمـر الذي يساعد على استعادة الوضـع الذي كانت عليه البرامج والأجهزة من قبل.

تشكّل ملفات سجلّات الأعمال أهميّة بالغة لحلّ الأعطال والمشكلات التي تطرأ على الأنظمة، وليس بالضرورة أنّها لا تستخدم إلا في حالة الأخطار والكوارث فقط. فعند تعطّل نظام التشغيل مثلًا، يمكن إرسال نسخة من ملفّ سجلّات الأعمال إلى الشركة المنتجة لدراسته، ومعرفة ماذا حدث، وما أسباب الأعطال؟ ومن ثم إخبار المهندس المسؤول عن إصلاح النظام بالإجراءات والخطوات التي يجب أن يتبعها لحلّ العطل أو استعادة النظام.

٨-٧ معالجة الأخطار والكوارث المعلوماتيّة بعد وقوعها

الكوارث المعلوماتيّة هي ما يحلّ بالمعلومات أو أجهزة وبرامج معالجة المعلومات باختلاف أنواعها من خـراب أو دمار جرّاء تعرّضهـا لكوارث حقيقيّة وقعت، سـواءً أكانت متعمّدة أم بأسبـاب خارجة عن إرادة البشر. وعند حـدوث الكارثة المعلوماتيّة سـواءً أكانت طبيعيّة أم بفعل فاعل، فإنّه يجب اتباع خطوات محدّدة لمعالجة هذه الكارثة والتعامل معها، بحيث يكون هدفها النهائي هو استعادة الوضع كما كان عليه قبل وقوع الكارثة. ويجب وضع خطّة محكمة لذلك، تشمل جميع الخطوات المطلوبة، وما تحتاج إليه كلّ خطوة من: معدّات وأجهزة وبرامج وأشخاص مدربين ومؤهلين لتنفيذها على أكمل وجه، وتتلخّص هذه الخطوات فيما يلي:

تقييم الأضرار

في هذه الخطوة يُقوَّم الوضع بشكل عام، وتُحصر الأضـرار الناتجة عن الكارثة، وتُحدّد الأجهزة والبرامج التي توقفت عن العمل، وتلك التي ما زالت تعمل، وعلاقة كل منها بالآخر. إنّ التقويم الصحيح لوضع النظام المعلوماتي بعد حدوث الكارثة يحدّد جميع الخطوات التي تليه. فمثلًا، لو جرى تقويم الوضع، و وجد أن هناك بعض مغذيّات الطاقة الاحتياطيّة ما زالت

تعمل، وأنّ هناك معلومات في وضع حرج جـدًّا، فيجب البدء على الفور بأخذ نسخ فوريّة من هذه المعلومات قبل فقْدها نهائيًّا، أو إيقاف تشغيل طبيعي للأجهزة وقواعد البيانات، يضمن عدم تعرّض المعلومات والبرامج التطبيقيّة للخطر.

التوثيق المبدئي

يجب توثيق ما يتم عملـه مبدئيًّا وبطريقة لا تشكّل عبئًا إضافيًّا علـى الأعمال الأساسيّة لمعالجة الكارثة، وتتسبّب في تأخيرها، ففي هذه المرحلة، يتم توثيق الأشياء الرئيسة فقط(رؤوس الموضوعات) التي سيجري استكمالها لاحقًا.

تحديد الأعمال التي يجب القيام بها وتنفيذها وترتيب أولوياتها

في هذه الخطوة يتم تحديد الأعمال التي يجب القيام بها لمعالجة الكارثة، وتوزيعها على المنفّذين بشكل متناسق، يلـي ذلك البدء الفعلي في تنفيذ هذه الأعمال مع مراعاة أولوية كل منها في التنفيذ. وتختلف هـذه الأعمال وأولوياتها باختلاف نوع الكارثـة. فلو كانت الكارثة هجومًا على شبكة الحاسب الآلي المحلية مثلًا، فمن الأفضل فصل الشبكة عن الإنترنت فورًا، وحفظ ملفات سجلّات الأعمال لتعقب المهاجم، وفي بعض الحالات الأخرى يتم قبول الضرر الأخف تفاديًا لوقـوع الضرر الأكبر، ومن الأمثلـة على ذلك إغلاق الأجهـزة إغلاقًا سريعًا آمنًا(Graceful Shutdown)، وقطع الخدمة عن المستفيدين دون إبلاغ مسبق، قبل انتشار برنامج تدميري على الشبكة.

استعادة الوضع

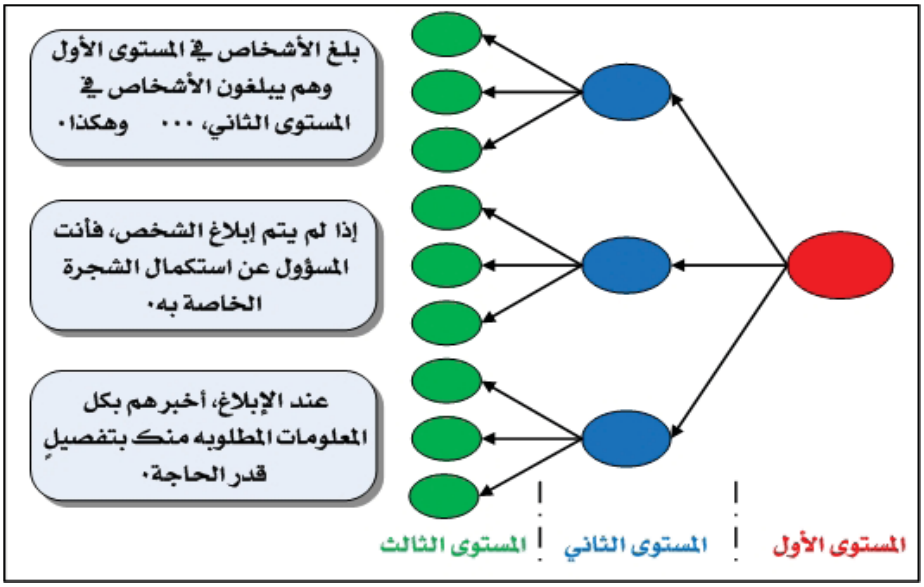
تهدف هذه الخطوة إلى استعادة الوضع للنظام المعلوماتي كاملًا كما كان عليه قبل وقوع الكارثة، ويمكن استعادة الوضع كنتيجة لتنفيذ الأعمال التي تم تحديدها في الخطوة السابقة وربطها مع بعضها بعضًا في شكل منظومة متكاملة.

يمكن إعادة بنـاء النظام المعلوماتي كاملًا مـن واقع النسخ الاحتياطيـة، إذا كانت هذه النُّسخ محفوظة بشكل جيّد وتُحدّث باستمرار، وتغطي معلومات المنشأة والشبكة والمستخدمين وأنظمـة التشغيل وقواعد البيانات كافة. فلو تم تدمير الأجهـزة والبرامج كافة، وكان هناك

نُسخٌ احتياطيّة جيّـدة وشاملة، فإنّه يمكن جلب أجهزة جديـدة واستعادة النظام المعلوماتي كاملًا من هذه النسخ.

الإبلاغ وطريقة التصعيد (Escalation Process)

عند حدوث الكارثة لا بدّ من إبلاغ الجهات والأشخاص المسؤولين بذلك، والطلب منهم إبلاغ من يلزم إبلاغه، والحضور لموقع الكارثة، والقيام بالأعمال المطلوبة منهم، ويجب في هذه الحالة إبلاغ المديرين ومديري مراكز المعلومات والمشرفين والفنيّين والاستشاريين. ويمكن استخدام «شجرة الإنذار» للاتصال بهؤلاء الأشخاص، كما يبينها الشكل (٨-٣)، بحيث تكون مهمّة كلّ شخص الاتصال بمجموعة أشخاص محدّدين لا يزيد عددهم على ثلاثة أشخاص مثلا[١].



الشكل (٨-٣): شجرة الإنذار[٢]

بهذه الطريقة يمكن توصيل الرسالة لأكبر عدد من الأشخاص في أقصر وقت ممكن، ولا يشترط أن تعكس هذه الشجـرة أيّ ترتيب إداريّ أو تنظيمي في المنشـأة. كما يجب أن تكون الرسالة المبلغة واضحة وشاملة، ويمكن إعداد نصـ مسبق لها يمكن استخدامه بعد تعديله وفقًا للظروف وقت وقوع الكارثة ونوعيتها.

١- داود، حسن طاهر (٢٠٠٤ب)، «أمن شبكات المعلومات»

٢- المرجع السابق

وقد لا يقتصر الوضع على إبلاغ أشخاص وجهات داخل المنشأة فقط، بل يتعدى الأمر ذلك إلى إبلاغ جهات أخرى، كجهات توريد الأجهزة، والمنشآت المماثلة، من أجل تقديم العون، أو أخذ الحيطة والحذر، ومن ذلك:

- إبلاغ المواقع الأخرى البعيدة التابعة للمنشأة.
- إبلاغ الشركة الموردة، والشركة (أو الشركات) التي تتولى تقديم خدمات أخرى ذات علاقة، لاحتمال الحاجة إلى مساعدتهم في علاج آثار الكارثة.
- إبلاغ الشركات أو الجهات التي تقوم بخدمات الدعم الفني والصيانة.
- إبلاغ أي جهة أخرى قد تكون عرضة للكارثة.

توثيق الحادث

ذكرنا في الخطوة الثانية ضرورة البدء بالتوثيق للموضوعات الرئيسة دون تفاصيل، وهنا وبعد استعادة الوضع يجب توثيق جميع ما حدث، بدءًا من الكارثة نفسها، وانتهاءً باستعادة النظام كاملًا. ففي هذه الخطوة يتم توثيق كل ما تم عمله من إجراءات، وما تم اكتشافه من أخطاء وملاحظات تفيد في اكتشاف مدى الضرر الذي حدث، وفي اتخاذ الإجراءات التي تضمن عدم تكرار هذا الحادث. كما تفيد أيضًا في توثيق القرائن والدلائل التي تدل على الجاني، وتساعد في ملاحقته، ومن أهم ما يجب توثيقه ما يلي:

- سجل الأحداث والوقائع، ويفضل إرفاق نسخة مطبوعة من ملفات سجلّات الأعمال (Log Files).
- الاتصالات التي تمت، وتواريخها، وأوقاتها، وأطرافها، وملخّص ما تم فيها.
- القرارات التي اتُّخذت.
- الأعمال التي أُنجزت، والأشخاص أو الجهات التي أنجزتها، وأوقات البدء فيها والانتهاء منها وتواريخها.
- المشكلات والأخطاء التي ظهرت، وكيف كان حلّها؟ ومن الأمثلة على ذلك اكتشاف أنّ بعض النُّسخ الاحتياطية كانت غير سليمة.

- الخلاصة لما حـدث، والتوصيات المستقبلية لمنـع تكرار ذلك أو محاولـة اجتنابه أو التخفيف من آثاره.
- تزويد الجهـات التي جرى إبلاغها بالكارثة(في الخطوة رقـم ٥) بالنتيجة، وتزويد الجهات الداخليّة في المنشـأة والأشخاص المعنيين بها بنسخة من التوثيق كاملًا، مع التركيز على التوصيات والتدابير والتعليمات المستقبلية التي أُقرّت.

ملخّص الفصل

إنّ معرفة التهديـدات التي تحيط بالمنشأة والمخاطر التي قد تنشـأ عنها، ثم تحليل هذه المخاطـر بالطرق العلميّة الصحيحة هـو الطريق الصحيح الذي يؤدي إلـى معرفة التدابير اللازمة للحيلولة دون وقوعها. فبدأ هذا الفصل بشرح المصطلحات والمفاهيم الأساسيّة لإدارة المخاطر المعلوماتيّة، وهي: الضعف، والتهديد، والخطر، والتعرّض، والمضادات، وكذلك شرح السياسة الأمنيّة الموضوعيّة لإدارة المخاطـر المعلوماتيّة، وما يجب أن تحتويه هذه السياسة؛ من أجل بناء الأساس العلمي الصحيح لفهم عمليّة إدارة المخاطر المعلوماتيّة.

لقد توصلنا إلـى أن إدارة المخاطر المعلوماتيّة هي عمليّة تحديـد الخطر، ثم تقييمه، ثم العمل على تلافيه، أو تقليل الآثار الناتجة عنه إلى أقل مستوى، وصولًا إلى ما يعرف بالمستوى المقبول، ثم تطبيق الآليات اللازمة للمحافظة عليه عند هذا المستوى. ولا يمكن لإدارة المخاطر المعلوماتيّة أن تكـون فاعلة وذات فائدة ما لم تقـم على أساس تحليـل المخاطر، وفق المنهج العلمي الصحيح.

إنّ عمليّة "تحليل المخاطر" هي العمليّة الأهم وحجر الزاوية في إدارة المخاطر المعلوماتيّة، وهي التي يمكن من خلالها تحديد نقاط الضعف والتهديدات وتقدير الأضرار المحتملة لها، ومن ثم تحديد أماكن تطبيق أنظمة الحماية المجابهة لها، و من ثَمَّ فإنّ تحليل الخطر هو أداة تساعد على إعطاء الأولوية المناسبة لكل خطر، ثم تحديد المتطلبات اللازمة لمجابهته، سواءً أكانت المركزيّة أم إداريّة أم مالية.

لقد شرحنا نوعـين رئيسين من أنواع تحليـل المخاطر المعلوماتيّة، همـا: التحليل الكمّي،

والتحليل النوعي (أو الكيفي). فالتحليل الكمّي يعتمد على إعطاء أرقام حقيقية ذات معنى لكل عنصر من عناصر التحليل المعلوماتي، بحيث يمكن قياس هذا العنصر من خلال الرقم المخصص له. بينما لا يعتمد التحليل النوعي على تحديد أرقام ومبالغ مالية لموارد المنشأة، ولا على عمليّات حسابية معقّدة، وإنما يعتمد على آراء الخبراء في تقويم خطورة (أو جديّة) التهديد من خلال إعطاء كلّ تهديد درجة خطورة (درجة جديّة) محدّدة، ثم تقويم قابليّة تطبيق أنظمة الحماية المضادة له. وقد يناسب أحد هذين النوعين من التحليل بيئة معيّنة، فيما لا يناسبها الآخر، وقد شُرِحت طُرُق إجراء هذه التحليلات من خلال أمثلة قريبة جدًّا من واقع المنشآت التقنية الحديثة.

كنتيجة لتحليل المخاطر المعلوماتيّة يجري اختيار نظام الحماية الذي يستطيع أن يقدّم الحماية المطلوبة وبكلفة مناسبة تضمن عدم تجاوز تكلفة الخسائر المترتبة عن وقوع المخاطر التي تم تحليلها، وقد يتطلب ذلك نوعًا ثالثًا من التحليل يسمّى تحليل الكلفة/الفائدة (أو الكلفة/الفاعلية)؛ لاختيار نظام الحماية المناسب.

أخيرًا قدم هذا الفصل مجموعة من الطرق والآليات الاحترازيّة التي يجب أخذها لمجابهة الكوارث المعلوماتيّة التي قد تقع فجأة، إمّا بسبب تفاقم الأخطار، أو بسبب كوارث طبيعيّة. كما قدّم مجموعة أخرى من التدابير والآليات التي يمكن اتباعها لمعالجة الكارثة المعلوماتيّة بعد وقوعها، وأنجع الطرق للخروج منها.

مسائل

١. عرّف كلًا من الخطر، وإدارة المخاطر، ثم اذكر العمليّات الرئيسة لإدارة المخاطر.

٢. ما الضعف؟ وماذا ينتج عنه؟ وكيف يمكن تحديده؟

٣. ما تحليل المخاطر؟ وما أنواعه؟ قارن بينها.

٤. ما المستوى المقبول؟ وكيف يمكن تحديده؟

٥. صف العمليّات الآتية ثم قارن بينها: تلافي الخطر، وتقليل الخطر، وتحويل الخطر.

٦. ما علاقة المفاهيم الآتية بعضها ببعض: الضعف، والتهديد، والخطر، والتعرض، والمضادات؟

٧. ما الفرق بين إدارة المخاطر ومعالجة الكوارث؟

٨. من التهديدات العامة المحتملة: الناس، والأجهزة، والبرمجيات، كيف يكون ذلك؟

٩. ما تحليل الكلفة والفاعلية؟ اشرح كيف يتم إجراء هذا التحليل.

١٠. عدّد الإجراءات الاحترازيّة الواجب اتباعها لمواجهة المخاطر؟ هل يمكن أن تساعد هذه الإجراءات في تجنب أضرار الكوارث المعلوماتيّة أو تخفيفها؟ اشرح ذلك.

١١. اشرح كيف أن تقويم الأضرار بعد حدوث الكارثة يساعد في ترتيب أولويات الأعمال وترتيب الخطوات التي يجب البدء بها. أعط أمثلة.

١٢. من أهم ما يعوّل عليه في استعادة الوضع بعد حدوث كارثة معلوماتيّة، هي النُّسخ الاحتياطية. اشرح ذلك.

١٣. لماذا لا يغني التوثيق النهائي عن التوثيق المبدئي في معالجة الكوارث المعلوماتيّة بعد حدوثها؟ وما الفائدة من ذلك؟

١٤. ما شجرة الإنذار؟ اشرح طريقة عملها.

١٥. أيهما أسرع في إيصال البلاغ: شجرة إنذار يبلِّغ كل شخص فيها ثلاثة أشخاص آخرين، أم شجرة إنذار يبلِّغ كل شخص فيها شخصين آخرين؟ هل لذلك علاقة بنوع الكارثة؟ ولماذا؟

الفصل التاسع

الحماية الماديّة (الحسيّة)

أهداف الفصل

- شرح مفهوم الحماية الماديّة، والدور الذي تلعبه في منظومة أمن المعلومات.
- شرح مفهوم الحماية الماديّة الإداريّة، والإجراءات التي يمكن تطبيقها لتحقيق ذلك.
- شرح مفهوم الحماية الماديّة التقنية، والمكوّنات التقنية الواجب توافرها لإتمام ذلك.
- شرح مفهوم طبقات الحماية الماديّة.
- توضيح المعايير التي يجري اختيار موقع مركز البيانات(Data Center) بناءً عليها.
- تحديد المتطلبات المهمة الواجب توافرها لتوفير حماية ماديّة جيّدة لمركز البيانات.
- شرح أهميّة توفير الطاقة الكهربائيّة باستمرار، والطرق المتّبعة لتوفيرها في الحالات الطارئة.

ما ستتعلمه في هذا الفصل

- المقصود بالحماية الماديّة، وماذا تقدّمه من حماية لأنظمة ومصادر المعلومات.
- التهديدات الماديّة التي يجب الحماية منها.
- مجموعة الإجراءات الإداريّة المنظّمة للحصول على حماية ماديّة جيدة.
- الطرق الفنية، والأدوات اللازمة، لتوفير حماية تقنية ماديّة جيدة.
- طبقات الحماية الماديّة، وكيف تُغلّف كل منها الأخرى لتوفير الحماية المطلوبة.
- المعايير الواجب اتّباعها لاختيار موقع مركز البيانات(المناسب).
- المتطلبات الفنية الواجب توافرها كحدّ أدنى لتوفير حماية ماديّة جيّدة لمركز البيانات من خلال تطبيق مفهوم طبقات الحماية الماديّة.
- نُظم التغذية بالطاقة الكهربائيّة، والمستويات المستخدمة منها في الحالات الطارئة.

الحماية الماديّة (الحسيّة)

٩-١ مقدّمة

لم تكن الحماية الماديّة لأنظمة المعلومات تشكل هاجسًا كبيرًا ولا تحديًّا يجب مراعاته عندما كانت أنظمة المعلومات محدودة الاستخدام والانتشار، وعندما كانت المعلومات في عموم حالاتها تُخزن في الأجهزة المركزيّة الكبيرة (Mainframes)، التي لا يصل إليها إلا أناس محدودون ومعروفون. لكن مع التطوّر الكبير في تلك الأنظمة، وانتشار شبكات الحاسب الآلي في كل مكان، وظهور المفاهيم والحلول التقنية الحديثة، كالحوسبة السحابية، أصبحت الحاجة للوصول إلى المعلومات أكبر واتّسعت شريحة الناس الذين يصلون إليها، وظهرت مع ذلك الحاجة للحماية الماديّة.

تؤدّي الحماية الماديّة أو الفيزيقية (Physical Security) كما يسمّيها بعضهم، دورًا أساسيًّا في منظومة أمن المعلومات، فهي تحمي أنظمة المعلومات من المخاطر الماديّة المباشرة، كالوصول إلى مناطق غير مسموح بها، والسرقة، والتخريب المتعمد، وعبث المعتدين والفضوليين، إضافةً إلى حمايتها من الأخطار الطبيعية كالحرائق، والفيضانات، والزلازل، والبراكين. فمهما وُضِعت من تجهيزات المركزيّة وبرمجيات حماية، ومهما كلف ذلك من مبالغ كبيرة، فإنها ببساطة لن تؤدي دورها إذا سُرقت أو خُرّبت. فأجهزة وبرمجيات أمن المعلومات باختلاف أنواعها ومستوياتها لا تستطيع الدفاع عن نفسها، ولا تملك حرّاسًا ولا أسلحة، ولذلك تولي المنشآت الحكوميّة والخاصة اهتمامًا كبيرًا بالأمن المادي لمواقعها بشكل عام، ولأنظمة المعلومات ومصادر المعلومات فيها بشكل خاص.

نبدأ هذا الفصل بالتعرّف إلى التهديدات الماديّة لأنظمة المعلومات، حيث ستوجّه الحماية الماديّة لمجابهتها؛ لذا يجب التعرف إليها أولًا قبل الولوج في وسائل الحماية منها. بعد ذلك نستعرض الحماية الماديّة الإداريّة، وهي الإجراءات الإداريّة المتّبعة لتوفير الحماية الماديّة، ثم نستعرض الحماية الماديّة التقنية، التي تهتم بتوفير وسائل وتقنيات الحماية الماديّة الآلية. ننتقل

بعد ذلك إلى موضوع مهم وهو طبقات الحماية الماديّة، حيث تشير الدراسات[٢٠١] إلى ضرورة توفير الحماية الماديّة على شكل طبقات يغلف كل منها الأخرى وتحيط جميعًا بالمورد أو المرفق المراد حمايته ماديًا. ولأهميّة مركز البيانات(Data Center) وما يحويه من أجهزة حاسب آلي رئيسة وقواعد بيانات وأجهزة ربط مركزية، فقد أفردنا له موضوعًا مستقلًا نتطرق فيه لطبقات الحماية الماديّة الواجب توفيرها لحمايته، آخذين ذلك كمثال واقعي ومهم لتطبيق مفهوم طبقات الحماية الماديّة على أرض الواقع. وأخيرًا، نشرح موضوعًا مهمًّا، وهو نظام التغذية بالطاقة الكهربائيّة، الذي يشمل: نظام التغذية الرئيسة، ونظام التغذية في الحالات الطارئة.

٢-٩ التهديدات الماديّة

لدى الأمن المادي مجموعة من التهديدات الماديّة تختلف في طبيعتها عن التهديدات التقنية الموجهة للمعلومات. فالمختص في الحماية الماديّة ينظر إلى التهديدات من النوع المادي، كالدخول إلى أحد المرافق المهمّة بطريقة غير شرعية، أو التخريب، أو السرقة، بينما المختص في أمن المعلومات(من الناحية التقنية) ينظر إلى التهديدات من النوع البرمجي والتقني، كالنفاذ من خلال أحد المنافذ في الشبكة أو في أحد البرامج، أو من خلال الشبكة اللاسلكية، وعلى ذلك، فإنّ لدى الحماية الماديّة مجموعة من التهديدات نجملها في الأصناف الرئيسة الآتية:

- تهديدات بشرية: كالوصول غير المشروع إلى مناطق محظورة، واستغلال النفوذ، والتخريب، والسرقة.
- تهديدات مصادر الخدمات الرئيسة: كانقطاع التيار الكهربائي، أو انقطاع وسائل الاتصال، أو تهديدات مصادر توليد الطاقة الكهربائيّة، مثل انقطاع الوقود، أو الغاز، أو الماء.
- تهديدات طبيعيّة: كالحرائق، والفيضانات، والزلازل، والبراكين، والأعاصير، وموجات الغبار، والحرارة الشديدة، والبرودة الشديدة.

١- Shon Harris(2008), "All-in-One CISSP Exam Guide", Fourth Edition.

٢- Withman, M. and Mattord, H.(2005), "Principles of Information Security".

- تهديدات عسكرية وإجراميّة: كالصواريخ، والمتفجرات، والعمليّات الإرهابية، والشغب، والعصيان المدني.

٩-٣ الحماية الماديّة الإداريّة

يقصد بالحماية الماديّة الإداريّة اتخاذ التدابير والإجراءات الإداريّة التي من شأنها الحفاظ على مصادر المعلومات والأجهزة التي تحتويها. وهذه الإجراءات تبدأ من الخارج إلى الداخل وتتوزّع على طبقات الحماية الماديّة، وصولًا إلى المورد أو المرفق المعلوماتي المراد حمايته، ومن هذه الإجراءات الإداريّة ما يلي:

- وضع نقاط حراسة ومراقبة خارجية على الأسـوار الخارجيّة. ويراقب هذه النقاط ويحرسها أشخاص مدربون ومؤهلون لهذا الغرض.
- وضع العلامات الإرشادية والتحذيرية في الأماكن المناسبة.
- تجهيز خرائط تفصيلية كبيرة الحجم، سواء أكانت عادية أم رقميّة، وإسقاط جميع نقاط المراقبة والكاميرات عليها؛ لمعرفة مكان أي حدث، وتسهيل عمليّة الوصول إليه.
- التحكّم بدخول الأفراد، سواءً أكانوا موظفين أو زوّارًا، باستخدام أنظمة جيّدة كأجهزة بصمة اليد أو العين، أو البطاقات الذكيّة التي تحدّد موقع صاحبها.
- التحكّم بدخول المواد والأجهزة وخروجها، وتوثيق ذلـك، ويفضّل استخدام الأرقام التسلسلية للأجهزة؛ لضبط ذلك بشكل دقيق.
- تطبيق خطط إدارة المخاطر ومعالجة الكوارث ذات العلاقة بالحماية الماديّة، (انظر الفصل الثامن: إدارة المخاطر المعلوماتيّة).
- تطبيق بنود السياسات الأمنيّة ذات العلاقة بالحماية الماديّة (انظر الفصل الخامس: سياسات ومعايير وتوجيهات وإجراءات أمن المعلومات).
- تثقيف العاملين وتدريبهم على الإجراءات والقواعد الأمنيّة الصحيحة دوريًّا.
- تحديد الأشخاص والقيادات وتوزيع المسؤوليات والصلاحيّات الخاصة بالأمن الحسّي عليهم بدقة.

- القيام بالزيارات والاستشارات المتخصصة في مجال الحماية الماديّة.
- رفع التقارير الدوريّة والملاحظات والاقتراحات عن الحماية الماديّة للقيادات العليا.
- التأكد من كفاءة العاملين في الحراسات والمراقبة الأمنيّة، وقيامهم بواجباتهم دوريًا.

٩-٤ الحماية الماديّة التقنية

يقصد بالحماية الماديّة التقنية، توفير المعدات والأجهزة الفنية التي توفر الحماية التقنية ضد الأعطال والقصور في الموارد الأصليّة، وغالبًا ما تعمل هذه المكوّنات بشكل آلي دون تدخل بشري، ولهذا صُنِّفت بأنها حماية ماديّة تقنية، ومنها:

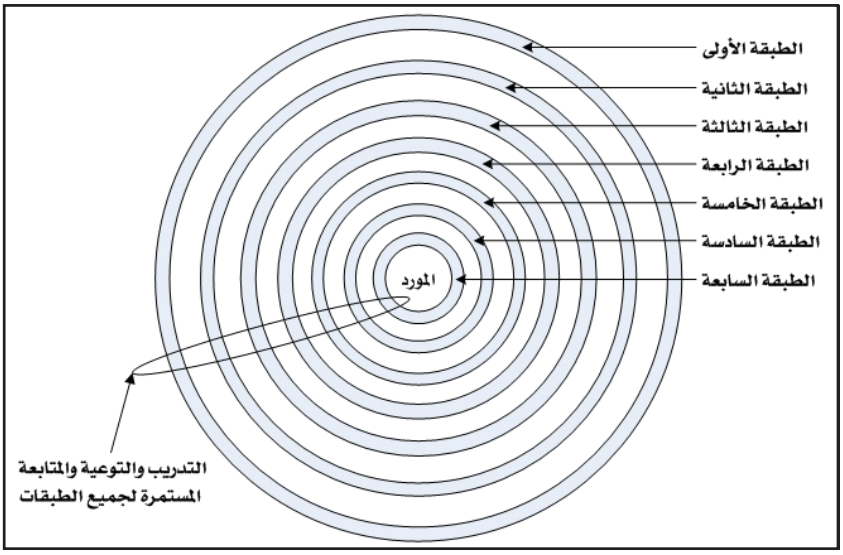
- استخدام دوائر مراقبة مغلقة، كشبكات التلفزيون المغلقة، أو شبكات(IP) لمراقبة جميع المداخل والمخارج والممرات ومركز البيانات والبوابات عن طريق الكاميرات. ويجب تدريب العاملين على هذه الدوائر تدريبًا جيّدًا، وأن تكون لدى هذه الدوائر القدرة على تخزين لقطات الكاميرات ومقاطع من التسجيل(مقاطع فيديو) بشكل منتظم للرجوع إليها عند الحاجة، مع مراعاة تسجيل التاريخ والوقت على كل هذه اللقطات والمقاطع.
- استخدام بوابات كشف المعادن في الأماكن المناسبة، حيث إن استخدام مثل هذه الأدوات يكشف المعادن المخفية، ويغطي القصور الحاصل في استخدام الكاميرات التي لا تستطيع كشف ذلك.
- استخدام حسّاسات قياس درجتي الحرارة والرطوبة، وربطها بالانظمة التي تعالج مخرجاتها، وتقارنها بالحدود الطبيعية، ومن ثم تتخذ الإجراء المناسب.

٩-٥ طبقات الحماية الماديّة

للحصول على حماية ماديّة جيّدة؛ يجب أن تُوفّر هذه الحماية على شكل طبقات حماية متتالية تغلّف كل منها الأخرى، وتحيط بالمرفق أو المورد المعلوماتي المراد حمايته. فباتّباع هذه الطريقة يكون من الصعب على المهاجم(أو المُهدد) تجاوز هذه الطبقات، لأنه لو تجاوز إحداها فستكون الطبقة الآتية في طريقه، ... وهكذا، وصولًا إلى جوهر هذه الطبقات، وهو

المرفق أو المورد المعلوماتي المـراد حمايته، الذي من المفترض أن لا يصله إلا شخص مصرّح له، أو شخص استطاع تجاوز جميع طبقات الحماية المغلفة له.

تتكامل الحماية الماديّة الإداريّة، والحماية الماديّة الفنية فيما بينهما؛ لتكوّن طبقات الحماية المطلوبة كما في الشكل(٩-١) فقد تكون طبقــة الحماية طبقة إداريّة صرفة كاختيار وتوزيع الحراس، وقد تكون طبقة المركزيّة صرفة كتركيب كميرات مراقبة في أماكن تغطية مناسبة، وقد تكون خليطًا منهما بأن تكون طبقة إداريّة تُنفَّذ من خلال أدوات حماية تقنية، مثل أنظمة كشف المتجاوزين والمتطفلين.



الشكل(٩-١): طبقات الحماية الماديّة

كما يوضح الشكل(٩-١) يتألف نظام الحماية الماديّة من عدد من الطبقات تزيد وتنقص حسب أهميّة الموارد والمرافق المعلوماتيّة المراد حمايتها، وحسب الإمكانات المتاحة لكل منشأة، وهذه الطبقات هي:

- الطبقة الأولى: وهي الطبقة الخارجيّة وخط الدفاع المادي الأول، وتتألف من تسيير الدوريات، و وضع نقاط الحراسة، واختيار الأشخاص المدربين والمؤهلين لذلك.
- الطبقة الثانية: التي تتألّف من وضع سياج خارجي يتناسب مع طبيعة عمل المنشأة.

فقد يكون هذا السياج مجـرّد حائط بارتفاع مناسب، وقد يكـون حواجز اسمنتية، وقد يكـون أسلاكًا شائكة، أو خليطًا منها جميعًا، وقـد يكون غير ذلك. من الناحية التقنية يمكن تزويد هذه الطبقة بأجهزة كشف محاولي الاختراق أو المتطفلين آليًّا، كالكابلات التـي تستشعر أيّ حركـة تقطعها، وكأجهزة الاستشعـار التي يمكنها أن تكتشف من يتجاوزها، وتميّز ما إذا كان بشرًا أم حيوانًا. وتشمل هذه الطبقة أيضًا وضع العلامات الارشادية والتحذيرية باختلاف أنواعها.

- الطبقة الثالثة: وتتألف من أنظمة الحماية بالإنارة، حيث يتم من خلال هذه الطبقة توفير إنارة قويّة وكافية لإطلاع أجهزة المراقبة التقنية والإداريّة على ما يجرى، وتغطي المواقع المهمة كافة ، ولا تترك أيّ مكان مُظلم يمكن النفاذ من خلاله.
- الطبقة الرابعة: وهي طبقة التحكّم بالدخول للمرافق، ومن أشهر أدواتها استخدام أبواب، وأقفال مناسبـة، سواءً ميكانيكيـة أم إلكترونيّة، ويمكن ربـط هذه الأبواب والأقفال بأنظمة الأنذار، التي ترصد حالاتها (مفتوح، أو مغلق)، وأوقات هذه الحالات، وتكشف وجود أيّ حالة خاطئة في وقت خاطئ، كأن يكون هناك باب مفتوح خارج وقت الدوام الرسمي للمنشأة، كان من المفروض أن يكون مغلقًا. كما يمكن تجهيز الأبواب بأقفال إلكترونيّة لا تفتح إلا بإدخال أرقام سريّة، أو بتمرير بطاقات ذكيّة عليها، أو بفحص خاصيّة أو أكثر من الخصائص الحيويّة للأشخاص، مثل: بصمات الأصابع وراحة اليد، أو بصمات العين. وهناك حلـول حديثة للتحكّم بالدخول للمرافق منها استخدام شرائـح ذكيّة تسمح لحاملها بالمـرور وتفتح له الأبواب التـي يحتاج إليها في الأوقات المسمـوح بها، وتحدد في الوقـت نفسه أماكن وجـوده، ويمكن ربط هذه الشرائح مع طبقة الحماية الآتية (طبقـة المراقبة)، حيث يمكن اظهار أماكن وجود حاملها على خريطة الموقـع. وقد تعدى الأمر ذلك فأصبح هنـاك بوابات إلكترونيّة (Electronic Gate-E-Gate) تتعرف إلى هوية الشخص تلقائيًّا من خصائصه الحيوية، مثل: الطول، وأبعاد الوجه، وبصمة العين، بمجرد مروره من خلال البوابة،

وأصبحت هذه الحلول مطبقة في بعض مطارات الدول المتقدمة. وتشمل هذه الطبقة كذلك استخدام بوابات كشف المعادن، التي توضع في الأماكن المهمة من أجل كشف خروج أو دخول أي معـدن؛ للحيلولة دون خـروج أو دخول مواد غـير مرغوب فيها، كوسائط التخزين (التي بها معدن).

- الطبقة الخامسة: طبقة المراقبة، التي يجري فيها مراقبة جميع المداخل، والمخارج، والممرات، والأبواب، والغرف المهمة، وأيّ مرفق يتطلب ذلك، من خلال أجهزة وكميرات وشبكات المراقبة التي تصب في غرفة المراقبة والتحكم، التي عادة ما تُزوَّد بشاشات العرض المناسبة مدعّمة بخرائط الموقع. ومن ذلك أيضًا استخدام حسّاسات استشعار الحركة، التـي تستطيع كشف وجود أي جسم يتحرك، ومـن أهم تطبيقات ذلك هو كشف وجود أي حركة في مركز البيانات (Data Center) عندما يكون مغلقًا، أو في الأوقات التي من المفروض أن لا يكون بها أحد.
- الطبقة السادسة: طبقة الحماية من التهديدات الطبيعية، التي تشمل أنظمة مكافحة الحرائـق، والفيضانات، واستشعار وجود زلازل أو براكـين، وأنظمة مراقبة درجات الحرارة والرطوبة، خاصّة في غرف مراكز البيانات. ويمكن ربط هذه الأنظمة بأنظمة إنذار مبكّر ترسل رسائل إنذار عند تجاوز أيّ من مؤشرات هذه التهديدات لحدوده الطبيعية، ويمكن أن تكـون رسائل الإنذار بعدة أشكال، فقد تكون عبارة عن إصدار أصوات (جرس) إنذار، أو تكون بإرسال رسالة نصية (SMS) لأشخاص محدّدين، أو بإرسال بريد إلكتروني، أو بأيّ خليط منها، وقد يتعدّى الأمر من مجرّد إصدر إنذار إلى تنفيذ بعض الإجـراءات آليًّا، كفتح أبواب الطـوارئ، أو إغلاق مصادر الماء، أو تشغيل أنظمة إطفاء الحرائق آليًّا، أو إيقاف عمل أجهزة وخوادم الحاسب الآلي آليًّا.
- الطبقة السابعة: ويمكن أن نطلق عليها اسم «الطبقة الخاصة»، حيث تشمل التجهيزات والإجـراءات الخاصة بمرفق معيّن مـن مرافق المنشـأة، التي عادة مـا تختلف من مرفق إلى آخر حسب طبيعة محتويات هذا المرفق ودوره في عمل المنشأة. فتجهيزات

الحماية الماديّة الخاصّـة بمستودع أجهزة الحاسـب الآلي تختلف عن تلك الخاصة بمركز البيانات، ومن الأمثلة على ذلك: تجهيزات حماية التغذية بالطاقة الكهربائيّة والتكييف لمركز البيانات.

لا يمكن أن تـؤدي هذه الطبقات دورها بالشكل الصحيـح دون أن يرافقها برنامج توعية وتدريب لجميع المتعاملين معها، ودون أن يكون هناك إشراف ومتابعة من قبل الجهات الإشرافية والإداريّة في المنشأة.

بقي أن نذكّر أن هذه الطبقات يجب أن تُجهّز لتعمل بالأسلوبين الآتيين، وأن يتم التدريب عليهما تدريبًا جيّدًا: الأول أثناء وقت الدوام الرسمي للمنشأة، حين يكون عدد الموظفين كبيرًا، ويكون التعامل مع أنظمة المعلومات المختلفة في ذروته، وتكون الحركة في مرافق المنشأة كبيرة، والثاني خارج وقت الدوام الرسمي، حين تقل هذه الأنشطة، ويصل بعضها إلى درجة التوقف، وحين يكون بعض المرافق مقفلًا لا يُسمح بالدخول إليه. أمّا العمل في أوقات الطوارئ فيجب أن يتم حسب خطط الطوارئ المعدّة مسبقًا لهذا الغرض، التي قد تقع أثناء الدوام الرسمي أو خارجه.

٩-٦ الحماية الماديّة لمركز البيانات (Data Center)

يُعدُّ مركز البيانات هو الجوهرة الغالية، والمورد الأهم للمنشآت التي تعتمد في عملها على المعلومات، وخدمـات تقنية المعلومات، مثـل: البنوك ومواقع الحكومـة الإلكترونيّة، وإن كان الاعتماد على أنظمة المعلومات بدا واضحًا وجليًّا لدى المنشئآت عمومًا. ومن هنا، فإنّ مركز البيانات هو المرفق الأجـدر بالحماية الماديّة الجيدة. وفيما يلي نتعرف إلى كيفية توفير هذه الحماية لهذا المرفق المهم، فنبدأ أولًا بطريقة اختيار الموقع المناسب له، ثم نتعرف إلى كيفية توفير الحماية الماديّة اللازمة، من خلال توفير طبقات الحماية الماديّة التي تعرفنا إليها في الموضوع السابق.

٩-٦-١ موقع مركز البيانات

تبدأ الحماية الماديّة لمركز البيانات في وقت مبكر، وذلك باختيار الموقع المناسب له ابتداءً،

وهو ما يساعد على توفير حمايـة ماديّة جيّدة له مستقبلًا. ونحن هنا نركّز على موقع مركز البيانات، ونترك مواقـع الأجهزة الفرعية؛ لأن هذه المراكز هي التـي تحوي قواعد البيانات والأجهزة الرئيسة المهمة، وهي المنطقـة الأولى بالحماية، وطبيعتها مركزيّة يمكن السيطرة عليها، ويجب اختيار موقع مركز البيانات وفقًا للمعايير الآتية:

- يفضّل وضعه في الطابق الأرضي أو تحت الأرض؛ لتوفير حماية إنشائيّة جيّدة، كون هذه المناطق عادة ما تكون قويّة إنشائيًّا، وتساعد على الحماية ضد الهدم، والانهيار، والهجمات الحربية أو الإجرامية، وكذلك من أجل تسهيل عمليّة الدخول والخروج، لا سيما في الحـالات الطارئة، كنشوب الحرائق والانهيـارات، وتسهيل نقل الأجهزة والمعدات(الثقيلة) من المركز وإليه.
- مراعاة اختيار الموقع الذي يساعد على الحماية من تسرب المياه وسيول الأمطار[1].
- اختيار الموقع الذي يساعد على التحكّم والسيطرة على المداخل والمخارج، وفي الوقت نفسه، الوصول إلى مخارج الطوارئ بسهولة.
- يفضل أن يكـون الموقع في وسـط الطابق؛ لتسهيـل عمليّات تمديد كابـلات الطاقة الكهربائيّة إلى المركز، وكابلات نقل المعلومات إلى الطوابق كافة.
- استخـدام المواقع المجاورة للمركـز للأغراض ذات العلاقة بـه، كمعامل البرمجة، ومركز مراقبة عمليّات الشبكة(Network Operation Center-NOC)، ومركز عمليّات أمن الشبكة(Security Operation Center-SOC).
- مراعاة أن يكون هناك مساحة كافية للتوسع المستقبلي.
- يفضل أن يكون المبنى الـذي به مركز البيانات بعيدًا عن الطـرق العامة والسّريعة، ومهابط الطائرات، والسكك الحديدية؛ تفاديًا لتعرضه لأيّ حادث.

٩-٦-٢ طبقات الحماية الماديّة لمركز البيانات

نحن هنا بصدد تطبيق طبقات الحماية الماديّة التي تعرفنا إليها سابقًا على مرفق محدّد، وهو "مركز البيانات" فيمكن توفير حماية ماديّـة ملائمة لمركز البيانات من خلال طبقات

١- صادق، دلال و الفتال، حميد ناصر(٢٠٠٨)، «أمن المعلومات»، ص ٣٢.

الحماية الماديّـة التي تحتوي جملة من التجهيزات والمتطلبـات التقنية، والإجراءات الإداريّة اللازمة، وفق الآتي:

- الطبقات الأولى، والثانية، والثالثـة: إذا كان مركز البيانات يقع ضمن موقع المنشأة فستكون هذه الطبقات مشمولة ضمن طبقات الحماية الأولى، والثانية، والثالثة للموقع العام، وإلا فيجب توفيرها لمركز البيانات وفـق التجهيزات والإجراءات المذكورة في هذه الطبقات سابقًا.
- الطبقة الرابعة: وهي طبقة التحكّم بالدخول لمركز البيانات، ويمكن تطبيق ما يناسب المركز من تجهيزات وإجراءات ذكرناها في هذه الطبقة سابقًا.
- الطبقة الخامسة: طبقة المراقبـة، التي يجري فيها مراقبـة المواقع والصالات التي توجد بها أجهزة الخوادم الرئيسية(Servers)، وأجهزة تخزين المعلومات، وأجهزة الربط بالشبكـة، إضافة إلى جميـع المداخل، والمخارج، والممـرّات، والغرف التابعة للمركز، ويمكن تطبيق التجهيزات والإجراءات المذكورة سابقًا في هذه الطبقة على مركز البيانات.
- الطبقة السادسة: طبقة الحماية من التهديدات الطبيعية، التي تشمل: أنظمة مكافحة الحرائـق، والفيضانات، واستشعار وجود زلازل أو براكـين، وأنظمة مراقبة درجات الحرارة والرطوبة، حيث يجب تركيب هذه الأنظمة في مركز البيانات، وفق ما ذُكر سابقًا في هذه الطبقة.
- الطبقة السابعة: وهي طبقة «خاصّة» بمركز البيانات، وهنا يمكن أن نلاحظ الفرق عن الطبقات السابقة، حيث تشمـل هذه الطبقة التجهيـزات والإجراءات الخاصة بالمركز، وهي:
  - تجهيز المركز بمواد غير قابلة للاشتعال أو بطيئة الاشتعال، ويكون الأثاث بسيطًا، وفي أضيق الحدود، وحسبما تستدعي الحاجة فقط.
  - تجهيزه بنظام تكييف جيّد، وهناك أنظمة تكييف خاصّة بمراكز البيانات، ولها

طُرُق تمديد وتوزيع للهواء تعدّ خصيصًا لمثل هذه المواقع.

- تجهيزه بنظام جيّد لمكافحة الحريق.
- تجهيزه بنظام جيّد لمكافحة تسرب المياه.
- استخدام الأرضيات المرتفعة (Raising Floor)؛ لتسهيل تحريك الكبائن والأجهزة فوقها والتمديدات تحتها، وتقليل المساحة اللازم تبريدها.
- استخدام كبائن لوضع الأجهزة الرئيسة وأجهزة التخزين ومغذّيات الطاقة بداخلها، مع تزويدها بنظام أقفال إلكترونيّة للتحكم بها.
- استخدام خزّانات خاصّة فولاذيّة مضادّة للرطوبة والحريق والهدم؛ لتخزين أقراص وأشرطة النسخ الاحتياطية فيها.
- مراقبة درجة حرارة المركز ومستوى الرطوبة فيه وضبطهما تحت المعدلات القياسية لذلك.
- استخدام نظام تغذية للطاقة الكهربائيّة متعدّد المستويات، ولأهمية ذلك فقد أفردنا له الموضوع الآتي.

٩-٧ نظام التغذية بالطاقة الكهربائيّة

يجب توفير الطاقة الكهربائيّة لجميع مصادر المعلومات ومراكز البيانات باستمرار، ويشمل ذلك مراعاة الأمور والمتطلبات الفنية في التغذية الرئيسة، وكذلك طُرُق توفير الطاقة البديلة في الحالات الطارئة.

٩-٧-١ التغذية الكهربائيّة الرئيسة

إنّ الطاقة الكهربائيّة لمصادر وأنظمة المعلومات هي بمنزلة الدم في الجسد. ويجب توفير هذه الطاقة بالطرق الفنية الصحيحة التي تضمن استمرار تدفقها، وحمايتها ماديًّا، ومن ذلك مراعاة الأمور الآتية[١]:

- أن تتم تغذية مركز البيانات من مصادر الطاقة الكهربائيّة الرئيسة مباشرة دون إشراك أيّ جهة أخرى معه في المصدر نفسه؛ لما قد يسببه ذلك من عدم استقرار

١- صادق، دلال و الفتال، حميد ناصر(٢٠٠٨)، «أمن المعلومات»، ص ٤٠.

مصدر الطاقة.

- يجب أن تتـم التغذية بالطاقة الكهربائيّة لمركز البيانـات ومصادر المعلومات المهمّة عبر مصدرين مختلفين، يمكن التحوّل من أيّ منهمـا إلى الآخر بسهولة، وعادة ما يكون المصدر الأول هو شبكة التغذية العامّـة، والمصدر الثاني هو مولّدات كهربائيّة خاصّة بالمركز.

٩-٧-٢ التغذية الكهربائيّة في الحالات الطارئة

لا بدّ من إيجاد حلول بديلة تستخدم عند توقّف التغذية الرئيسة بالطاقة الكهربائيّة لأيّ طارئ. وتُعدُّ هذه الطريقة مـن أكثر خطط الطوارئ نجاحًا واستخدامًا على مستوى العالم. فخطط الطوارئ الأخرى كالفيضانـات والحرائق تكون عادة أقل تكـرارًا من انقطاع التيار الكهربائي المفاجئ. فتجد أنّ المنشأة تستخدم الطاقة الكهربائيّة البديلة عدّة مرات، في حين أنّها لم تستخدم نظام إطفاء الحرائق مطلقًا. ويتكـوّن نظام التغذية بالطاقة الكهربائيّة في الحالات الطارئة من مستويين، هما:

المستـوى الأول: استخـدام مولّـدات الطاقـة الكهربائيّـة الاحتياطيـة، وهنـا يستخـدم مولّد (Generator) احتياطي للطاقة الكهربائيّة للمنشأة عامةً، وآخر لمركز البيانات خاصّة، وهو مولّد عـادة ما يكون خارج المبنى، ويتـم التبديل إليه إمّا يدويًّـا أو آليًّا، حسب حساسيّة البيانات وقدرة أجهزة التبديل.

المستوى الثاني: استخدام أجهزة موانع انقطاع التيـار الكهربائي(Uninterruptable Power Supply-UPS) وهي أجهزة خاصّة تركّب داخل غرف مراكز البيانات، وتُزوِّد الأجهزة الرئيسة وأجهزة التخزين بالطاقة الكهربائيّة عند انقطاعها بشكل آلي سريع جدًّا، وتعتمد في عملها على تخزين الطاقة الكهربائيّة في بطاريات، وعند الحاجة إليها يتم استخدام هذه البطاريّات لإعادة توليد تيـار كهربائي مستمرّ لمدّة محدودة. وتتميّز هذه الأجهزة باتصالها المباشر مع أجهزة الحاسـب الآلي الرئيسة، و وجود برمجيّات خاصّـة بها تعمل على إيقاف عمل الأجهزة بصورة طبيعيّة للحيلولة دون تلف البيانات أو فقدها؛ إلا أنها لا تستطيع توفير

الطاقة لفترات طويلة (بناءً على سعة البطاريات وعددها)، وإن كان بعضها يوفر الطاقة لفترة قد تصل في بعض الأحيان إلى ثلاث ساعات أو أكثر.

ملخص الفصل

اتضح من خلال هذا الفصل أنه مهما كان هناك من أنظمة حماية تقنية وبرامج، ومهما كلف ذلك من مبالغ مالية كبيرة، فإنها ببساطة لن تؤدي دورها إذا تم سرقتها أو تخريبها. فأجهزة وبرمجيات أمن المعلومات على اختلاف أنواعها ومستوياتها لا تستطيع الدفاع عن نفسها، ولا تملك حرّاسًا ولا أسلحة. ولذلك لا بد من توفير الحماية الماديّة والأمن المادي (الحسي) لمواقعها عامةً ولأنظمة المعلومات ومصادرها خاصّة.

استعرض هذا الفصل التهديدات الماديّة التي غالبًا ما تُوجّه الحماية الماديّة لمجابهتها، ثم شرح الفرعين الرئيسين للحماية الماديّة، وهما: الأول: الحماية الماديّة الإداريّة، التي تشمل مجموعة الإجراءات الإداريّة المتّبعة لتوفير الحماية الماديّة، والثاني وهو الحماية الماديّة التقنية، التي تتضمّن توفير وتشغيل وسائل وتقنيات الحماية الماديّة الآلية.

لقد شرح هذا الفصل كيف أنه يمكن توفير الحماية الماديّة على شكل طبقات حماية تغلّف كل منها الأخرى وتحيط جميعًا بالمورد أو المرفق المعلوماتي المراد حمايته ماديًّا. بعد ذلك جرى تطبيق مفهوم طبقات الحماية الماديّة على مركز البيانات كأهم مرفق وأكثرها حساسية، ورأينا كيف أمكن من خلال ذلك حصر وتحديد التقنيات والإجراءات اللازمة لحماية المركز.

أخيرًا، قدّم هذا الفصل شرحًا وافيًا عن نظام التغذية بالطاقة الكهربائيّة، الذي يشمل: نظام التغذية الرئيسة، ونظام التغذية في الحالات الطارئة.

مسائل

١. ما المقصود بالأمن المادي؟ أعط ثلاثة أمثلة من المخاطر التي يمكن أن يساعد في الحماية منها.

٢. ما الفرق بين الحماية الماديّة الإداريّة والحماية الماديّة التقنية؟ ثم اذكر مثالين لكل منهما.

٣. اشرح مفهوم "طبقات الحماية الماديّة"، ثم أجب عن الأسئلة الآتية:

أ. هل عدد الطبقات ثابت؟ وهل يمكن تطبيق العدد نفسه من الطبقات على أيّ منشأة؟

ب. هلى يمكن تغيير ترتيب الطبقات؟ ولماذا؟

ج. طبّق هذا المفهوم لتوفير الحماية الماديّة لمستودع يحوي تجهيزات تقنية.

٤. يجب اختيار موقع مركز البيانات(Data Center) بعناية تامة. عدّد المعايير المنظمة لذلك.

٥. لماذا لا يجب إشراك أكثر من جهة مع مركز البيانات في مصدر الطاقة الكهربائيّة؟ وهل هذا المطلب ممكن التطبيق دائمًا؟ اشرح ذلك.

٦. ما مميزات استخدام مانع انقطاع التيار الكهربائي(UPS)؟ هل يغني عن استخدام مولد احتياطي؟ ولماذا؟

٧. بالرجوع إلى شبكة الإنترنت، اشرح ماذا نعني بكل مما يلي؟ وكيف يسهم كل منهما في أمن المعلومات:

أ. مركز مراقبة عمليّات الشبكة(Network Operation Center-NOC)

ب. مركز عمليّات أمن الشبكة(Security Operation Center-SOC).

الفصل العاشر

أمن المعلومات والأدلة الرقميّة

أهداف الفصل

- التعريف بجرائم المعلوماتيّــة وأهدافها، وإيضاح خصائصهــا التي تميزها من غيرها؛ تمهيدًا لتسهيل طرح إجراءات التعامل معها.
- التعريف بعلم التحقيق الجنائي للحاسب الآلي والحاجة إلى ذلك.
- تحديد الإجراءات التحضيرية للتحقيق الجنائي للحاسب الآلي.
- شرح مفهوم الأدلة الرقميّة وإجراءات الحصول عليها.
- تحديد خطوات فحص الأدلة الرقميّة وتحليلها.
- توضيح العلاقة بين علم أمن المعلومات وجرائم المعلوماتيّة والتحقيق فيها.

ما ستتعلمه في هذا الفصل

- جرائم المعلوماتيّة والفرق بينها وبين الجرائم التقليدية.
- المقصود بالتحقيق الجنائي للحاسب الآلي.
- مجموعة الإجراءات التحضيرية داخل معمل التحقيق الجنائي للحاسب الآلي.
- مواصفات الدليل الرقمي الجيّد.
- الإجراءات الواجب اتباعها للحصول على الأدلة الرقميّة في حالة جيّدة.
- التوزيع الهرمي للأدلة الرقميّة.
- أهم مصادر الأدلة الرقميّة.
- طُرُق الفحص والتحليل.
- المكوّنات التي يجب أن تشملها عمليّة الفحص والتحليل.
- العلاقة بين علم أمن المعلومات وجرائم المعلوماتيّة وعلم التحقيق فيها.

أمن المعلومات والأدلة الرقميّة

١٠-١ مقدّمة

في مجتمع اليوم، أصبحت أجهزة الحاسب الآلي، وما تحويه من معلومات، ذات قيمة عظيمة وفي معظم الأحوال لا تقدّر بثمن. ويستخدم الحاسب الآلي في كثير من الأعمال، فأصبحت البنوك والأجهزة الحكومية والشركات في معظم دول العالم، بما فيها الدول العربيّة، تعتمد على نظم الحاسبات الآلية بشكل أساسي.

تُعدُّ أجهزة الحاسب الآلي وشبكاته أهدافًا مغرية للهجوم عليها، حيث أوضحت ذلك الإحصاءات التي ترصد تكرار جرائم المعلوماتيّة وانتشارها. فمثلًا أوضح تقرير معهد أمن الحاسب الآلي(CSI Survey) في تقريره لعام ٢٠١٠/٢٠١١م[١] أنّ(٣٨,٩٪) من الجهات التي شملها التقرير تعرضوا لرسائل اصطياد إلكتروني، وأنّ(١١,٤٪) تعرضوا لسرقة كلمات المرور، وأنّ(٣٣,٥٪) تعرضوا لسرقة أجهزة الحاسب الآلي المحمولة، وأنّ(٨,٧٪) تعرضوا لاحتيال مالي. ويزيد الأمر صعوبة وغموضًا أنّ ضحايا جرائم المعلوماتيّة لا يُفصحون عنها، ولا يعلنون عن الخسائر الناتجة عنها خوفًا من تداعيات عدم الثقة في أنظمة الحماية لديهم، وإنما يقومون بإجراءات علاجية ودفاعية فقط.

يُعدُّ علم التحقيق الجنائي للحاسب الآلي(Computer Forensics) علمًا حديثًا ظهرت الحاجة إليه عند انتشار جرائم المعلوماتيّة(الجريمة الإلكترونيّة) بشكل كبير، وأصبح استخدام الحاسب الآلي وتقنيات المعلومات والاتصالات في الجرائم عامةً، وجرائم المعلوماتيّة خاصّة ركنًا أساسيًّا في التخطيط والتنفيذ، إن لم تكن هي الهدف الأساسي والمباشر لهذه الجرائم. مما لا شكّ فيه فإنّ أيّ مجرم يستخدم الحاسب الآلي في التخطيط لجريمته أو تنفيذها، أو الاتصال بأعضاء آخرين فيها، فإنّ من المتوقع أن يترك أثرًا في الحاسب الآلي الذي استخدمه، بحفظه لبعض الملفّات عليه، أو إجراء بعض المراسلات والاتصالات من خلاله. ويأتي علم التحقيق الجنائي للحاسب الآلي ليبحث في كيفية تحرير ذلك، والبحث عن القرائن والدلائل واستخراجها دون المساس بذلك الجهاز أو محتوياته، ودون تدمير أيّ معلومة أو تغيير حالتها

١- Computer Security Institute(CSI) Survey(2011), The 15th Annual Computer Crime and Security Survey.

بشكل قد ينتج عنه فقْد دليل أو قرينة مهمّة.

يقدّم هذا الفصل شرحًا وافيًا عن جرائم المعلوماتيّة من الجوانب الآتية: تعريف جرائم الحاسب، وأهدافها، وخصائصها. يلي ذلك التعريف بعلم التحقيق الجنائي للحاسب الآلي، ثم نتناول الإجـراءات التحضيرية لإجراء عمليّة التحقيق. بعد ذلـك، نعرّف الأدلة الرقميّة وخصائص الدليل الرقمي الجيد، وطرق الحصول على الأدلة الرقميّة. يلي ذلك شرح عمليّة الفحص والتحليل للأجهزة و وسائط التخزين المختلفة، والخطوات العلمية المتبعة في ذلك، ونختم باستعراض أشهر الأدلة الرقميّة التي يمكن الحصول عليها كنتائج لعمليّات الفحص والتحليل.

١٠-٢ جرائم المعلوماتيّة

في عصرنا الحاضر، تعدّدت أشكال جرائم المعلوماتيّة وأنواعها وتغيرت، لدرجة أنه يطلق عليها عدّة مسمّيات في الوقت نفسه. فهناك من يستخدم لفظ «الجريمة الإلكترونيّة»، وآخر يستخدم لفظ «جرائم الإنترنت»، وثالث يستخدم «جرائم الحاسب الآلي أو الحاسوب»، ورابع يمزج بين اثنين أو أكثر من ذلك. ومهما تعددت المسمّيات فإنّه يمكننا القول إنّه لا يمكن أن تتم جريمة معلوماتيّة إلا بوجود قصور أو تراخٍ في أنظمة أمن المعلومات، أو بتجاوز تلك الأنظمة بطرق غير شرعية، وعليه فإنّ هناك علاقة وطيدة بين أمـن المعلومات وجرائم المعلوماتيّة. فأمن المعلومات يشـكّل الدرع الواقي من تلك الجرائم، وهـذه الجرائم تحاول اختراق ذلك الدرع وهناك صراع دائم بين الطرفين.

يعرّف مكتـب التقييم الأمريكي[١] جريمة الحاسب الآلي بأنهـا: «الجريمة التي يؤدي فيها الحاسب الآلي دورًا رئيسًا». ويُعـدُّ هذا التعريف تعريفًا عامًّا شاملًا لشريحة كبيرة جدًّا من الجرائم لدرجة أنه يمكن أن يشمل بعض الجرائم التقليدية.

يشمل تعريف وزارة العدل الأمريكيـة[٢] أيّ جريمة وظّف مرتكبها معرفته بتقنية الحاسب الآلي في جريمته، ومنها:

١- Bidgoli, Hossein(2006b), "Handbook of Information Security", Volume 2, Part 3

٢- المرجع السابق.

- الجريمة ذات العلاقة بالحاسب الآلي(Computer Crimes).
- إساءة استخدام الحاسب الآلي(Computer Abuse).
- التحايل باستخدام الحاسب الآلي(Computer Fraud).
- الوصول غير المرخّص(Unauthorized Access of Computer Systems).

مما سبق يمكن تعريف الجريمة المعلوماتيّة بأنها: «كلّ عمل ينتج عنه ضرر متعمّد يستخدم الحاسب الآلي وتقنية المعلومات لإلحاق الضرر بالمعلومات أو أجهزتها أو مستخدميها».

إنّ جرائم المعلوماتيّة هي جرائم غير تقليدية، وعندما تُرتكب فإنّ الضرر الناجم عنها يكون غير تقليدي أيضًا، وقد يكون الضرر الناجم عن جريمة المعلوماتيّة كبيرًا جدًّا، ويمتد لعدد كبير من الضحايا، وذلك بناءً على أهداف الجريمة نفسها. فجريمة إنشاء فيروس حاسب آلي بهدف نشره وتدمير أكبر عدد من الأجهزة تختلف عن جريمة سرقة المعلومات السِّريّة لشخص واحد؛ بهدف سرقة أمواله أو معلوماته، وقد يكون الضرر ماديًّا أو معنويًّا، وقد يشملهما معًا، ومن أهداف جرائم المعلوماتيّة ما يلي:

- التخريب وتدمير الأجهزة والبيانات.
- تعطيل الخدمة.
- تحقيق أرباح ماديّة.
- التجسّس بأنواعه.
- إبراز المهارة والعبث من قبل الهواة.

١٠-٢-١ خصائص جرائم المعلوماتيّة

لجرائم المعلوماتيّة(أو جرائم الحاسب الآلي) أنماط وسمات تميزها من الجرائم التقليدية، وتكمن خطورتها في ضعف إيجاد الصلة بين المجرم و وسيلة ارتكابه للجريمة، وصعوبة التعرّف إلى شخصيته، وبُعده أحيانًا عن موقع الجريمة. يمكن تلخيص أهم خصائص جرائم المعلوماتيّة فيما يلي[١]:

١. الصعوبة في كشفها: وتعني الصعوبة في اكتشاف أن هناك جريمة وقعت، بغض

١- الخليفة، محسن بن سليمان(٢٠٠٣)، «جرائم الحاسب الآلي وعقوبتها في الفقه والنظام»، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية.

النظر عن مرتكبيها. فقد تقع جرائم معلوماتيّة معيّنة ولا يشعر أحد بأن هناك جريمة وقعت إلا بعد مرور وقت طويل، وربما لا تكتشف نهائيًّا، والسبب في ذلك يعود إلى أن جرائم المعلوماتيّة عادةً تقع في بيئة افتراضيّة غير ملموسة في غالب الأحيان، ولا يمكن استشعارها بشكل مادي محسوس.

٢. صعوبة إثباتها: وتعني الصعوبة في إثبات وقوع الجريمة بعد اكتشافها، أو بعبارة أخرى: الصعوبة في إثبات التنفيذ. فبعد اكتشاف الجريمة والعلم بوقوعها، هناك صعوبة في إثبات أحداثها، والسبب في ذلك هو أن هذا النوع من الجرائم غالبًا ما يتم تنفيذه بطرق المركزيّة صعبة ومهارات تخصصيّة عالية، ويتم في الوقت نفسه إخفاء أو مسح أي آثار قد يتركها الجاني.

٣. الصعوبة في تحديد مرتكبيها: وتعني الصعوبة في تحديد الشخص أو الجهة التي ارتكبت الجريمة. فبعد اكتشاف وقوع الجريمة وبعد التثبت من أنها نفّذت بالفعل، هناك صعوبة في تحديد الشخص أو الجهة التي نفّذت، والسبب في ذلك هو أن جرائم المعلوماتيّة غالبًا ما تُنفّذ بطرق احترافيّة لا يوجد فيها روابط(واضحة) تربط الأحداث بمن نفّذ هذه الأحداث. ويطلق بعضهم على جرائم المعلوماتيّة «جرائم ذوي الياقات البيضاء»؛ لأنه قد يرتكبها أناس مؤهّلون تأهيلًا عاليًا، وربما يحملون درجات علمية متقدمة تبعد الشكوك عنهم، ولا تدلّ مظاهرهم على أنّهم مجرمون، وهذا ما يصعب عمليّة الربط بين هؤلاء الأشخاص والجرائم التي يرتكبونها، حتى لو كان الدافع من وراء ذلك هو إبراز المهارة وممارسة الهواية فقط.

٤. لا تحتاج إلى أدوات وأنشطة غير مألوفة: كل ما يحتاج إليه مرتكب جرائم المعلوماتيّة في غالب الأحيان هو جهاز حاسب آلي واتصال بشبكة الإنترنت. فلا تجده يحتاج إلى أدوات تثير الاهتمام – كالسلاح مثلًا – بل يمكنه أن يرتكب الجريمة وهو يعمل على جهازه، كما لو كان يؤدّي عملًا من الأعمال العادية، وأيضًا لا يحتاج إلى القيام بأنشطة تثير الشكوك – كالتخفّي وراء سواتر، أو لبس اللثام مثلًا – بل يمكنه أن يرتكب الجريمة وهو في أحسن هيئة وأجمل مظهر.

٥. لا تتأثر بعاملي الزمان والمكان: يطلق بعضهم على جرائم المعلوماتيّة «الجرائم العابرة للحدود» فيمكن ارتكاب الجريمة من أيّ مكان في العالم، بل من الممكن أن

تكون الضحية في بلد أو قارة، والجاني في بلد أو قارة أُخريين، وكذلك، يمكن ارتكاب جريمة المعلوماتيّة في أيّ وقت من ليل أو نهار، بل يمكن برمجة الجريمة، بحيث لا تقع إلا في أوقات محدّدة، بعد أن يتمكن الجاني من الاختفاء ومسح الآثار. وبناءً على ذلك، فإنّ هذا النوع من الجرائم لا يتأثر بعاملي الزمان والمكان، ويستطيع الجاني التغلب على القيود الناتجة عن هذين العاملين، وهذا بدوره يشكل عائقًا كبيرًا في كشف مرتكبي هذا النوع من الجرائم وتحديدهم وإثباتها عليهم، خاصّة في ظل اختلاف القوانين والتشريعات من بلد إلى آخر، فما يمكن عدّه جريمة معلوماتيّة في بلد قد لا يكون جريمة في بلد آخر.

٦. سرعة التنفيذ ودقته: تعتمد جرائم المعلوماتيّة على أجهزة وبرمجيات تقنية المعلومات، التي هي بطبيعتها سريعة في أدائها ودقيقة في تنفيذها. لذلك تتصف هذه النوعية من الجرائم بإصابتها لأهدافها المحدّدة بدقة بالغة، وأنّها تبدأ وتنتهي بشكل سريع.

هذه الخصائص جعلت من جرائم المعلوماتيّة الجرائم الأكثر بروزًا في العصر الحديث، بل تعدّى الأمر ذلك، حتى أنّ كثيرًا من الجرائم التقليدية (كالسرقة والسطو المسلح) ينسّق لها المجرمون، ويحصلون على المعلومات الضروريّة لتنفيذها باستخدام ما وفّرته التقنية، خاصةً الحاسبات والاتصالات والإنترنت.

١٠-٣ الأدلة الرقميّة وطرق الحصول عليها

مرّ معنا في الفصل الثالث (عناصر أمن المعلومات) كيف أنّ عمليّات المتابعة تسجّل الأعمال والأنشطة المختلفة للمستخدمين ومديري الأنظمة، وكذلك تسجّل ما يجري من عمليّات على موارد المنشأة من أجل متابعته، وهل هناك أيّ خروق أو ضعف في أنظمة الحماية؟ لتتم معالجتها على الفور، وتستخدم هذه المعلومات كذلك في عمليّات التحقيق في تلك الأحداث، ومن قام بها؟ إذا ما كان هناك خرق لأنظمة الحماية قد تقود إلى جريمة معلوماتيّة، ربما تكون كبيرة.

ظهر في وقتنا الحاضر مفهوم «الدليل الرقمي» (Digital Evidence)، الذي أصبح ركيزة أساسية في إدانة المتهمين بارتكاب جرائم معلوماتيّة أو تبرئتهم. ومن أهم ما يهدف إليه علم التحقيق الجنائي للحاسب الآلي (Computer Forensics) هو الحصول على

الأدلة الرقميّة وتوثيقها وحفظها، ومن ثم استخدامها في إدانة المتهم أو تبرئته، وتأتي مهمة المحققين والباحثين في جرائم المعلوماتيّة بالدرجة الأولى في تحديد الأدلة الرقميّة، التي يمكن استخدامها في التحقيق وأمام المحاكم لإثبات أحداث معيّنة أو نفيها أو تتبّعها، ومن هنا برزت الحاجة إلى التعرّف إلى الأدلة الرقميّة وطرق التعامل معها، والحصول عليها بطريقة آمنة تحافظ على سلامتها وحجيّتها.

ويعرّف علم التحقيق الجنائي للحاسب الآلي(Computer Forensics) بأنه: «العلم الذي يبحث في استخراج الشواهد أو القرائن الرقميّة(الإلكترونيّة) وحفظها وتوثيقها، سواءً أكانت توجد في وسائط تخزين المعلومات أو منقولة عبر شبكات المعلومات» وهو علم يشابه بدرجة كبيرة علم الطب الشرعي من ناحية فحص جهاز الحاسب الآلي ومعرفة حالته ومحتواه، ومن ثم استخراج القرائن والدلائل الموجودة فيه.

١٠-٣-١ التعامل مع الأدلة الرقميّة

عادة ما يستخدم المجرم(التقليدي) بعض الأدوات في جريمته، ويترك آثارًا تدل على قيامه ببعض الأعمال باستخدام هذه الأدوات، وهذا ما يمكن أن نسمّيه «الأدلة التقليدية»، كبصمات الأصابع، وبقع الدم، وبقايا الشعر. وتشكّل الأدلة التقليدية أهميّة بالغة في إثبات حدث ما أو نفيه، أو ربطه بشخص معيّن، إلا أنّ الأمر يزداد أهميّة(وصعوبة) إذا كانت الأدوات المستخدمة والآثار المتروكة رقميّة(إلكترونيّة)، وقد تكون في معظمها غير ملموسة، وتقع في عالم افتراضي يصعب تحديدها والتعامل معها فيه.

لقد انتشر في الآونة الأخيرة مفهوم «الأدلة الرقميّة»(Digital Evidences)، التي يمكن تعريفها بأنها: "القرائن والشواهد التي توجد على شكل معلومات مخزّنة أو منقولة في شكل رقمي(إلكتروني)" وتكون طبيعة هذه المعلومات أنّها معلومات إثباتية يمكن من خلالها الاستدلال أو التأكد من قيام المستخدم بعمل ما، ومن الأمثلة على ذلك إنشاء ملفّ في تاريخ معيّن، به معلومات مهمة تخصّ القضيّة أو الجريمة، أو إرسال بريد إلكتروني، أو وجود صور فوتوغرافية رقميّة، أو مخرجات نظام المعلومات الجغرافية ونظام تحديد المواقع، أو سجلّات

الأقفال الإلكترونيّة، أو مقاطع الصوت والفيديو الرقميّة، وعادة ما ينم الحاسب الآلي ومحتوياته عن مستخدمه، خاصّة في عصرنا الحاضر الذي أصبح فيه استخدام الحاسب الآلي في إنجاز كثير من الأعمال والمراسلات أمرًا عاديًّا.

١٠-٣-٢ مواصفات الدليل الرقمي الجيد

قد يكون هناك دليل رقمي على شكل ملف نصّيّ صغير الحجم، يمكن تخزينه على ذاكرة قلميّة صغيرة، لكن عدد صفحاته يتعدّى الألف صفحة. فالدليل الرقميّ قد يكون كبير الحجم، وقد يكون معقّدًا، وكذلك هو بطبيعته معرّض للتدمير والتعديل بسهولة، وعلى الجانب الآخر، قد يكون الدليل الرقمي معبّرًا ويصف الحال أو الحدث بدقّة و وضوح، بل قد يصل في بعض الأحيان إلى أن يكون جزءًا منه هو تاريخ و وقت حدوثه. وفي ظل هذه المفارقات تبرز أهميّة تحديد مواصفات الدليل الرقمي الجيّد، حيث إنّه إذا لم يكن الدليل الرقمي جيّدًا في حالته والمعلومة التي يحملها، فإنّ الاستفادة منه ستكون محدودة، ويمكن تحديد الدليل الرقمي الجيد بأنه الدليل الذي تتوافر به الخصائص الآتية[١]:

- الموثوقيّة(Authentic): لم يعبث به، وهو فعلًا ما تم الحصول عليه دون زيادة ولا نقص، وأنّه هو الدليل الرقمي المعنيّ لا غيره. ومثال ذلك أن يكون الدليل الرقمي عبارة عن رسالة بريد إلكتروني، وتعني الموثوقيّة في هذه الحالة أنّ هذا البريد هو البريد الخاص بالقضية محل التحقيق نفسه لا غيره، وأنّه يعود للشخص المعني نفسه لا غيره.
- الدقة(Accurate): دقيق في معلوماته وما يحتويه، ويمكن وصفه بكل وضوح. ومثال ذلك أن يكون الدليل الرقمي ملفًا نصيًّا(وثيقةً) يحتوي معلومات عن خطة تنفيذ الجريمة، وتعني الدقة في هذه الحالة أنّ معلومات الخطّة واضحة ودقيقة ولا يوجد فيها غموض.
- شامل كامل(Complete): أي لا يوجد به نواقص ولا نقاط مفقودة في موضوعه الذي يدل عليه. ومثال ذلك أن يكون الدليل الرقمي صورة كربونيّة(Carbon Copy-CC) لبريد إلكتروني، لكن لا يوجد عنوان المرسل إليه في خانة الصورة الكربونية

١- Bidgoli, Hossein(2006b), "Handbook of Information Security", Volume 2, Part 3.

من الرسالة، وبذلك يُعدُّ دليل غير شامل.

- مقنـع(Convincing) : يولّد القناعـة التامّة لدى المطّلع عليـه، فلا يوجد هناك تناقض أو تعارض أو أجزاء غير مفهومة. ومثال ذلك أن يكون الدليل الرقمي مقطع فيديو تم تصويره في إحدى المدن، لكن تظهر فيه مقاطع من مدينة أخرى، و من ثَمَّ لا تكون هناك قناعة تامّة بهذا الدليل.
- مطابق(مؤكـد) (Conform) : أي مطابـق للقواعد والأنظمة التـي تحكم الأدلة الرقميّـة، التي تحدّد إمكانية عـدّه دليلًا رقميًّا أم لا. فالمعلومـات العاديّة الخاصّة بالمستخدم وملفّات أنظمة التشغيل والبرامج التطبيقيّة العادية قد لا تكون أدلّة رقميّة.
- الاحتفاظ بخصائصـه التقنيـة(Handle Technology Changes) : يحتفظ بخصائصه التقنية بغض النظر عن الوسط الذي خُزّن عليه، أو تقدم وتغير التقنية المحيطة بـه. ومعنى ذلك، أنه يكون بالإمكان قراءة الدليـل الرقمي والاطّلاع عليه ومعرفة محتواه في أيّ وقت مستقبلًا، وليس مرتبطًا ببرامج معيّنة(غير قياسية) لا يمكن قراءته أو الاطّلاع عليه إلا من خلالها.
- مقروء ومفهوم للبشر(Human Readable) : أي يكون في شكل كلمات وعبارات بلغة معروفة لدى من يطّلع عليه. وبعبارة أخرى: لا يكون في شكل رقمي ثنائي(Digital) لا يقرأه ولا يفهمه إلا الآلة، أي لا يكون بلغة الآلة(Machine Language).

١٠-٣-٣ الحصول على الأدلة الرقميّة

للحصول على الأدلة الرقميّة، فإنّه يلزم الاطّلاع على محتويات الحاسب الآلي ومعالجة المشكلات الفنيّة فيها- إن وجدت- وبعد ذلك يجري فحصها وتحليلها للحصول على المعلومات التي قد تدين صاحب الجهاز أو تثبت قيامه بعمل ما. يجب اتباع طُرُق علميّة مركزيّة صحيحة تضمن الحصول على دليل رقمـي جيّد، وفي وضع سليم غير متأثر بعملية الحصول نفسها، وفيما يلي نورد أهم الإجراءات التي يجب اتباعها للحصول على دليل رقمي جيد:

١. يجب توثيق كل ما يخص الدليل الرقمي، سواءً أكان توثيقًا كتابيًا أم إلكترونيًّا. كما

يجب أن يكون التوثيق النهائي مطبوعًا على ورق، بحيث يشمل هذا التوثيق المعلومات الآتية:

- تاريخ التوثيق و وقته.
- اسم الموثّق واسم معالج الدليل الرقمي وجهة عمله.
- وصف تفصيلي للدليل الرقمي والوسط التخزيني(قرص صلب ، جهاز محمول ، ذاكرة قلمية، ... إلخ) ، بحيث يشمل اسم الشركة المصنّعة والطراز(model) والرقم التسلسلي.
- وصف تفصيلي لجميع الخطوات التي جرى اتخاذها والتي ستُنفّذ وتاريخ كل منها و وقتها. ويشمل ذلك أيّ عمليّـات إصلاح لوسط التخزين الذي يحمل الدليل الرقمي إذا لزم الأمر، وما الذي جرى عمله؟ ولماذا؟ وكيف تم ذلك؟
- مكان تخزين(حفظ) الدليل الرقمي بعد الانتهاء منه، وتاريخ الحفظ وقته.

٢. أخذ نسخة كاملة من الدليل الرقمي(قرص صلب ، جهاز محمول ، ذاكرة قلمية، ... إلخ) على وسائط تخزين أخرى جديدة مُعدّة للفحص دون المساس بوسط التخزين الأصلي للدليل الرقمي، و دون تشغيل الجهاز مطلقًا.

٣. التحقّق من النُّسخ التي أُخذت لوسائط التخزين الأصليّة وأنّها مطابقة تمامًا للوسائط الأصليّة حرفًا بحرف، ويمكن التحقّق من ذلك باستخدام طريقة حساب البصمة الرقميّة(Hash Value) للأقراص الأصليّة والمنسوخة؛ للتأكد من تطابق هاتين القيمتين، وهناك عدّة خوارزميّات لحساب البصمة الرقميّة، ومن أشهرها خوارزميّة(SHA-2)،(انظر الفصل الرابع).

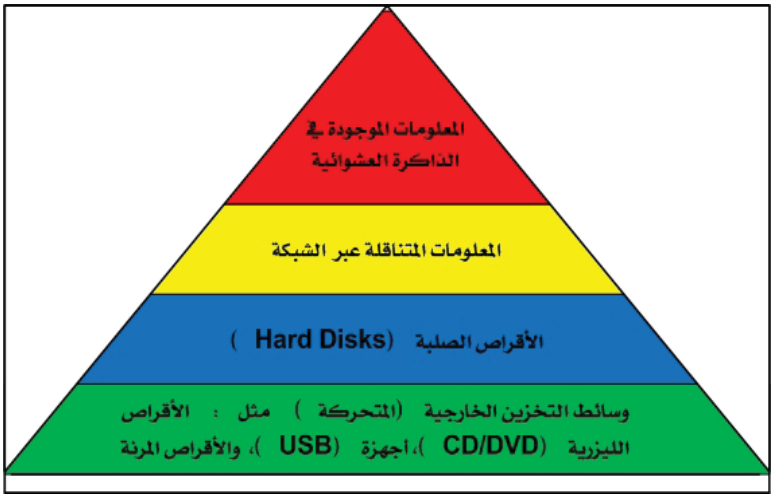
٤. ينصح بشدة باستخدام وسائط تخزين جديدة سواء، كانت صلبة أو خارجية(USB Disks)، أو ليزريّة لعمل نُسخ الفحص عليها. وعند استخدام وسائط سبق استخدامها فمن الأفضل عمل محو نهائي غير مسترجع(Wipe) لمحتوياتها، لضمان خلوّها تمامًا من أيّ معلومات سابقة قابلة للاسترجاع. وتجدر الإشارة إلى أن عمل التهيئة العادية(Format) قد لا يكون كافيًا لمسح جميع المحتويات السابقة، وتُعدُّ عمليّة المحو النهائي غير المسترجع(Wipe) هي أنسب الطرق وأقواها في هذه

الحالة.

٥. يجب المحافظة على سلامة الدليل الرقمي وتكامله(Digital Evidence Integrity)؛ لضمان بقائه على حالته التي وُجِد عليها دون أيّ تعديل أو زيادة أو نقص. ويمكن عمل ذلك بحساب البصمة الرقميّة(Hash Value) للدليل الرقمي عند الحصول عليه مباشرة لاستخدام هذه القيمة مستقبلًا، لإثبات أن الدليل بقي على حالته التي وُجِد عليها، وذلك بإعادة حساب هذه القيمة كلما دعت الحاجة إلى ذلك، وإثبات أنّها مطابقة للقيمة الأولى تمامًا.

٦. تحليل وسائط التخزين المُعدّة للفحص باستخدام أجهزة أخرى(غالبًا ما تكون مخصصة لهذا الغرض)، والاحتفاظ بالوسائط الأصليّة والجهاز الأصلي على ما هي عليه، خاصة من ناحية تواريخ إنشائها أو آخر تعديل أجري عليها.

يمكن الحصول على الأدلة الرقميّة من عدّة مصادر، بعضها قابل للتغيير أو الفقد، ويجب التعامل معه والحصول عليه فورًا، وبعضها ثابت يمكن الحصول عليه في أيّ وقت بسهولة. وتتراوح حالة الدليل الرقمي من كونه قابلًا للتغيير أو الفقْد إلى الثبات بحسب نوع الدليل الرقمي ومكان وجوده. فالأدلة الرقميّة التي توجد في جهاز حاسب آلي يعمل(شغّال) ويتم عرضها على الشاشة، فإنها تكون مخزّنة في الذاكرة العشوائية(RAM) وستفقد فورًا إذا أطفئ الجهاز. أمّا الأدلة التي توجد على قرص تخزين صلب أو ليزري، فهي أدلة ثابتة غير قابلة للفقد الفوري، ويمكن الحصول عليها ومعالجتها لاحقًا. يوضح الشكل(١٠-١) التوزيع الهرمي للأدلة الرقميّة، من حيث ثباتها وقابليتها للفقد، حسب مكان وجودها. فالأدلة الرقميّة في أسفل الهرم هي أدلة ثابتة وكثيرة العدد، كالأدلة المخزّنة على الأقراص المدمجة(Compact Disk-CD)، وأقراص الفيديو الرقميّة(Digital Video Disk-DVD)، بينما الأدلة في أعلى الهرم هي أدلة قليلة العدد وقابلة للفقد الفوري، كمخرجات البرامج وصفحات الإنترنت المعروضة على شاشة الحاسب الآلي أثناء تشغيله، التي عادة ما تكون مخزنة على الذاكرة العشوائية(RAM) وستفقد عند إطفاء الجهاز أو فصل التيار الكهربائي عنه.



الشكل(١٠-١): التوزيع الهرمي للأدلة الرقميّة حسب ثباتها وقابليتها للفقد

بغض النظر عن مكان وجود الدليل الرقمي في أيّ مستوى من الهرم وحالته، من حيث قابليته للفقد أو الثبات، فإنّه يُعدُّ دليلًا رقميًّا مهمًا طالما جرى الحصول عليه بحالته التي وُجِد عليها، ومن أهم مصادر الأدلة الرقميّة ما يلي:

- البريد الإلكتروني والروابط الإلكترونيّة.
- الصور بشتى أنواعها.
- الوثائق وملفّات النصوص بشتّى أنواعها، ومنها على سبيل المثال لا الحصر: ملفّات معالج الكلمات(الخطابات)(كملفّات برنامج الوورد)، وملفّات الجداول الإلكترونيّة(كملفات برنامج إكسل)، وملفات العروض التقديمية(كملفات برنامج البوربوينت)، وملفات(pdf)، والملفّات النصية(txt)، وملفات الصور، وملفات الفيديو، وملفات الصوت. انظر الجدول(١-٥) في الفصل الأول.
- الخرائط الرقميّة ومخرجات أنظمة المعلومات الجغرافية وتحديد المواقع.
- مقاطع الصوت والفيديو الرقميّة.
- جداول البيانات.
- سجلّات الدردشة.

- قوائم الاتصال.
- البرامج المنسوخة بطريقة غير شرعية، أو غيرها من مواد محفوظة الحقوق.
- الملفّات المؤقتة (Temp Files) وملفات الكوكي(Cookie Files) .
- الملفّات المحذوفة، وهنا لا بدّ من استخدام برمجيات استعادة الملفّات المحذوفة، سواءً التي تأتي ضمن حزمة برامج التحقيق الرقمي أو البرامج المستقلة. وهذه الملفّات يجب أن تشكل أهميّة بالغة للمحقق والمحلل، لأنه عادة ما تُحذف الملفّات التي تحتوي شواهد أو دلائل على الحدث أو الجريمة من قبل الجاني. وتجدر الإشارة إلى أنّه قد لا يمكن استعادة الملفّات المحذوفة حتى باستخدام برمجيات الاستعادة أو برمجيات التحقيق الرقمي، وذلك إذا كُتب عليها من قبل نظام التشغيل(على أماكن تخزين هذه الملفّات على قرص التخزين) وعادة ما يحصل ذلك للملفّات المحذوفة منذ وقت طويل.
- ملفّات التسجيل والمتابعة(Log Files) .

ملخّص الفصل

أوضح هذا الفصل أن لا جريمة معلوماتيّة أو جريمة حاسب آلي إلا بالتعدّي على أنظمة أمن المعلومات بشكل أو بآخر. ومما لا شك فيه أن أيّ مجرم يستخدم الحاسب الآلي في التخطيط لجريمته أو تنفيذها أو الاتصال بأعضاء آخرين فيها، فمن المتوقع أن يترك أثرًا في الحاسب الآلي الذي استخدمه بحفظه لبعض الملفّات عليه، أو إجراء بعض المراسلات والاتصالات من خلاله. ويأتي علم التحقيق الجنائي للحاسب الآلي ليبحث في كيفية تحرير ذلك، والبحث عن القرائن والدلائل واستخراجها، دون المساس بذلك الجهاز أو محتوياته، ودون تدمير أيّ معلومة، أو تغيير حالتها بشكل قد ينتج عنه فقد دليل أو قرينه مهمة.

ظهر من خلال هذا الفصل أهميّة التحقيق الجنائي للحاسب الآلي، حيث تبيّن أنّه الحلقة الواصلة بين علم أمن المعلومات وجرائم المعلوماتيّة. فالتحقيق الجنائي للحاسب الآلي يهدف بالدرجة الأولى إلى استخراج الأدلة الرقميّة التي تدين المتهم أو تبرئه، وعلم أمن المعلومات هو الذي يحافظ على مصداقية هذه الأدلة وموثوقيتها، كما هي الحال في ملفات سجلّات

الأحداث(Log Files). من أجل ذلك شرح هذا الفصل الإجراءات التحضيرية لإجراء عمليّة التحقيق، وعرّف الأدلة الرقميّة، وحدّد خصائص الدليل الرقمي الجيد، وطرق الحصول عليه. أخيرًا قـدّم هذا الفصل شرحًا وافيًا لعمليّة الفحص والتحليـل للأجهزة و وسائط التخزين المختلفة، والخطوات العلميّـة المتّبعة في ذلـك، واستعرض أشهر الأدلـة الرقميّة التي يمكن الحصول عليها كنتائج لعمليّات الفحص والتحليل.

مسائل

١. عرّف جرائم المعلوماتيّة، ثم اذكر أهم أهدافها.

٢. لجرائم المعلوماتيّة خصائص تميزها من الجرائم التقليدية. اذكر هذه الخصائص موضّحًا سبب وجود كل خاصية في هذا النوع من الجرائم.

٣. لماذا تسمّى جرائم المعلوماتيّة في بعض الأحيان "جرائم ذوي الياقات البيضاء"؟

٤. لا تتأثر جرائم المعلوماتيّة بعاملي الزمان والمكان. اشرح ذلك.

٥. أيّهما أصعب في التحقيق، الجرائم التقليديّة أم جرائم المعلوماتيّة؟ ولماذا؟

٦. لماذا يجب عدم تشغيل أي جهاز حاسب آلي، سواءً وجد في مسرح الجريمة، أو كان تحت الفحص والتحليل؟ اشرح ذلك من خلال أمثلة.

٧. لماذا يجب تصوير شاشة الحاسب الآلي الذي وجد وهو يعمل في مسرح الجريمة؟ اشرح ذلك من خلال أمثلة.

٨. تشكل كلمات المرور(كلمات السر) التي يستخدمها المتهم، سواءً للبريد الإلكتروني، أو حماية الملفّات، أو دخول المنتديات – قيمة مهمة للمحقق. كيف يمكن الحصول عليها في كل مرحلة من مراحل التحقيق الجنائي للحاسب الآلي؟

٩. ما علم التحقيق الجنائي للحاسب الآلي؟ وما العلاقة بينه وبين علم أمن المعلومات؟

١٠. يشكل التاريخ والوقت أهميّة بالغة في علم التحقيق الجنائي للحاسب الآلي. اشرح ذلك معتبرًا المكوّنات التي يمكن أن يكون لها تاريخ أو وقت(ملفات، مجلدات، ...

وغيرها)، وكيف يفيد ذلك في إثبات التهمة أو نفيها؟

١١. يصف دليل استخدام برنامج أو نظام تشغيل أو جهاز طريقة استخدام ذلك البرنامج أو النظام أو الجهاز. كيف يمكن الاستفادة من دليل المستخدم في التحقيق الجنائي للحاسب الآلي؟ رغم أنه شيء عام ويمكن أن يوجد في أي مكان.

١٢. ما هو الدليل الرقمي؟ وما هي خصائص الدليل الرقمي الجيد؟ أعط مثالًا لكل خاصية.

١٣. كيف يمكن المحافظة على سلامة الدليل الرقمي وتكامله؟

١٤. ماذا نعني بالتوزيع الهرمي للأدلة الرقميّة؟ اشرح ذلك مع إعطاء أمثلة.

١٥. عدد أهم مصادر الأدلة الرقميّة.

١٦. من أهم مصادر الأدلة الرقميّة البريد الإلكتروني. أعط مثالًا على ذلك معتبرًا حالة افتراضيّة. (مساعدة: سعيد أرسل لزيد، وزيد أرسل لعمر).

١٧. ما الطرق التي يمكن أن تتم بها عمليّة الفحص والتحليل للأدلة الرقميّة؟ وما أفضلها؟ ولماذا؟

١٨. لماذا يجري فحص جميع الملفّات بما في ذلك المؤقتة منها في عمليّة الفحص؟ أعط مثالًا واحدًا على الأقل لملفّ يجب فحصه بصورة قطعيّة، ومثالًا آخر لملف يمكن عدم فحصه.

١٩. لماذا يجب فحص الملفّات المحذوفة؟ وكيف يمكن استعادتها لتتم عمليّة الفحص؟ وهل يمكن استعادة جميع ما حُذف من ملفات؟

٢٠. استخدم شبكة الإنترنت للبحث عن برنامج مجاني للتحقيق الجنائي للحاسب الآلي، ثم قم بما يلي:

أ. دراسته جيّدًا واستشارة متخصّص في إمكانية تركيبه على جهازك.

ب. قراءة دليل الاستخدام جيّدًا.

ج. تحميله من الإنترنت إلى جهازك، ثم تركيبه (تنصيبه) عليه.

د. افحص جهازك، وابحث عن ملفات معيّنة، وأدلة رقميّة وهميّة من اختيارك.

هـ. احذف بعض الملفّات ثم حاول استعادتها، وكذلك حاول استعادة ملفات محذوفة منذ وقت طويل.

المصطلحات الرئيسة

Access Control	التحكّم بالوصول
Access Control List(ACL)	قائمة التحكّم بالوصول
Access Control Matrix	مصفوفة التحكّم بالوصول
Accountability	المحاسبة
Active/Active	نشط / نشط
Active/Passive	نشط / غير نشط
Active X	برنامج أكتف إكس
Address Filtering	التنقيح باستخدام العنوان
Advanced Encryption Standard(AES)	خوارزميّة التّشفير القياسي المتقدم
American Registry for Internet Numbers(ARIN)	قاعدة تسجيل أرقام الإنترنت الأمريكية
Analog	تماثلي
Annual Loss Expectancy(ALE)	الخسارة السنويّة المتوقعة
Annual Rate of Occurrence(ARO)	معدل الظهور (أو الحدوث) السنوي
Antispyware	برامج مكافحة التجسّس
APNIC	مركز شبكة معلومات آسيا والباسفيك
Application Layer	طبقة التطبيقات
Application Programs	البرامج التطبيقيّة
Application Servers	خوادم التطبيقات
ASCII Code	كود الآسكي
Auditing	التدقيق (أو المتابعة)
Authentication	التحقّق من الهُويّة
Authorization	التخويل
Automatic Teller Machine(ATM)	آلة الصرف الآلي (مكينة الصرف الآلي للبنوك)
Availability	التوفر (أو الإتاحية)
Awareness	التوعية
Back Door Attacks	هجمات الأبواب الخلفية
Baseline	الخط الأساس
Basic Input Output System(BIOS)	نظام الدخل والخرج الأساسي
Binary Digital System	النظام الثنائي الرقمي

Bit	بت وهو خانة واحدة في النظام الثنائي الرقمي
Blind Carbon Copy(BCC)	صورة معمّاة
Block	كُتلة
Block Cipher	التّشفير الكُتلي
Boot Sector Viruses	فيروسات قطاع بدء التشغيل
Broadcasting	بث لجميع الأجهزة
Brute Force Attack	الهجوم الأعمى(أو الاستقصائي)
Bus Topology	البُنية الخطية
Byte	حرف(أو بيات) وهو ثماني خانات(بتات)
Cache Memory	الذاكرة المخبأة(أو الكاش)
Carbon Copy(CC)	صورة كربونية
Cipher Block Chaining Mode(CBC)	أسلوب كُتل التّشفير المترابطة
Cipher Feedback Mode(CFB)	أسلوب التغذية العكسيّة للنصوص المشفّرة
Cipher Text	النّص المشفّر
Client/Server	الخادم/ العميل
Cloud Computing	الحوسبة السحابية
Clustered	تبادلي(عنقودي)
Committee on National Security Systems(CNSS)	لجنة أنظمة الأمن القومي الأمريكية
Common Gateway Interface(CGI)	واجهة البوابة المشتركة
Compact Disk(CD)	الأقراص المدمجة
Computer Abuse	إساءة استخدام الحاسب الآلي
Computer Forensics	علم التحقيق الجنائي للحاسب الآلي
Computer Fraud	التحايل باستخدام الحاسب الآلي
Computer Security Institute(CSI)	معهد أمن الحاسب الآلي
Computer Worm	دودة الحاسب الآلي
Concatenation	اللصق جنبًا إلى جنب
Confidentiality	السِّريّة
Cookie File	ملف الكوكي
Counter Mode(CTR)	أسلوب العداد
Countermeasures	المضادات
Cracking	كسر أنظمة الحماية
Cryptanalysis	تحليل الشيفرة(أو كسر الشيفرة)

Cryptography	علم التّشفير
Data Center	مركز البيانات
Data Consistency	توافق البيانات
Data Encryption Standard(DES)	خوارزميّة تشفير البيانات القياسي
Data Integrity	سلامة البيانات(أو المعلومة) وتكاملها
Data Link Layer	طبقة خط البيانات
Data Origin Authentication	التحقّق من أصل منشأ المعلومة
Database	قاعدة بيانات
Database Events Log	سجل أحداث قاعدة البيانات
Decryption	فكّ التّشفير
Decryption Algorithm	خوارزميّة فكّ التّشفير
Demilitarized Zone(DMZ)	نطاق حماية حدودي
Denial of Service(DoS) Attack	هجوم تعطيل الخدمة
Dictionary Attack	هجوم المعجم
Digital	رقمي(ثنائي)
Digital Certificates	الشهادات الرقميّة
Digital Evidence	الدليل الرقمي
Digital Signature	التصديق(أو التوقيع) الرقمي
Digital Subscriber Line(DSL)	خطوط الاتصال الرقميّة
Digital Video Disk(DVD)	أقراص الفيديو الرقميّة
Disaster Recovery Data Center	مركز بيانات رديف
Distributed Denial of Service(DDoS) Attack	هجوم تعطيل الخدمة الموزع
Domain Filtering	التنقيح باستخدام النطاق
Domain Name	اسم النطاق(أو الموقع على الإنترنت)
Electronic Code Book Mode(ECB)	أسلوب كتاب الترميز الإلكتروني
Elliptic Curve Cryptosystem(ECC)	نظام التّشفير بالمنحنى البيضاوي(الإهليلجي)
Embedded Systems	الأنظمة المضمنة
Encryption	التّشفير
Encryption Algorithm	خوارزميّة التّشفير
Enterprise Information Security Policy	السياسة الأمنيّة العامة(أو الهيكلية)
Escalation Process	عمليّة التصعيد
Exclusive OR(XOR)	العمليّة المنطقيّة: «أو الحصريّة»

Exposure	التعرّض
Exposure Factor(EF)	عامل التعرّض
Feedback	إعادة التغذية
File Infecting Viruses	فيروسات الملفّات
File Server	خادم الملفّات
File System	نظام الملفّات
File Transfer Protocol(FTP)	بروتوكول نقل الملفّات
Firewall	جدار النار (أو جدار الحماية)
Footprinting	تتبع الأثر (أو البصمة أو الترقيم)
Format	التهيئة
General Purpose	لغرض عام
Global System for Mobile Communication(GSM)	أنظمة الهواتف الخلوية
Globally Unique Identifier(GUID)	سجل بالمعارف الفريدة
Graceful Shutdown	إغلاق سريع أمن
Guidelines	المبادئ التوجيهية
Hacking	القرصنة التقنية
Hardware	الأجهزة (أو العتاد الصلد)
Hash Value	البصمة الرقميّة (أو القيمة المركزة)
Header	الرأس (أو الترويسة)
Hertz(Hz)	هيرتز
Hexadecimal	ست عشري
Honeypot System	نظام فخ العسل
Human Readable	مقروء ومفهوم للبشر
Hypertext Markup Language(HTML)	لغة توصيف النّص الفائق (التشعبي)
Hypertext Transfer Protocol(HTTP)	بروتوكول النّص الفائق
I/O Management	إدارة الدخل والخرج
Identification	تحديد الهُويّة
Infinite Loop	الحلقة اللامنتهية
Information Risk Management	إدارة المخاطر المعلوماتيّة
Information Security	أمن المعلومات
Initialization Vector(IV)	كُتلة استهلالية (أو ابتدائية)
Instant Messaging	التراسل الآني
International Organization for Standardization(IOS)	المنظمة العالمية للقياس

Internet Layer	طبقة الإنترنت
Internet Network Information Center(InterNIC)	مركز معلومات الإنترنت
Internet Protocol(IP)	بروتوكول الإنترنت
Internet Protocol(IP) Address	عنوان بروتوكول الإنترنت
Internet Security Scan(ISS)	ماسحة الإنترنت الأمنيّة
Internet Service Provider(ISP)	مزود خدمة الإنترنت
Intrusion Detection Systems(IDSs)	أنظمة كشف التطفل
Intrusion Prevention Systems(IPSs)	أنظمة منع التطفل
IP Spoofing	خداع عنوان الإنترنت
Internet Protocol Security(IPSec)	أمن بروتوكول الإنترنت
Issue-Specific Security Policy	السياسة الأمنيّة لموضوع محدّد
Java Applets	برامج جافا
Kerberos	نظام «كيربورس»
Key	المفتاح السِّريّ(أو مفتاح التّشفير)
Key Distribution Center(KDC)	مركز توزيع المفاتيح
Leased Lines	الخطوط المستأجرة
Link Layer	طبقة الربط
Local Area Network(LAN)	شبكة حاسب آلي محلية
Log Files	سجلّات الأحداث
Machine Language	لغة الآلة
Macro Viruses	الفيروسات الجزئية الكبيرة
Mail Bombing	تفجير البريد الإلكتروني
Mainframe	النظام المركزي(مينفريم)
Malicious Code Attacks	هجمات البرامج(أو الأكواد) الخبيثة
Malware	البرامج الضارّة
Man-in-the-Middle Attacks	هجمات الرجل في الوسط
Media Access Control(MAC) Address	العنوان الفيزيائي لبطاقة الشبكة(عنوان الماك)
Memory Management	إدارة الذاكرة
Message Digest	بصمة(أو خلاصة) الرسالة
Message Digest Algorithm-5(MD5)	خوارزميّة(MD5)
Modes of Operation	أساليب التشغيل

Modular Arithmetic	العمليّات الحسابيّة لقياس معيّن (أو المقاسيّة)
Modulo Addition	الجمع القياسي
Modulo Division	القسمة القياسية
Modulo Multiplication	الضرب القياسي
Modulus	القياس
Multi-Protocol Label Switching(MPLS)	شبكة (MPLS)
Need-to-know	المعرفة بقدر الحاجة
Network Address Translation(NAT)	تحوير عناوين الشبكة
Network Events Log	سجل أحداث الشبكة
Network Interface Card(NIC)	كرت الشبكة
Network Layer	طبقة الشبكة
Network Operation Center(NOC)	مركز مراقبة عمليّات الشبكة
Non-Repudiation	عدم الإنكار
Non-structured Data	بيانات غير هيكلية
One-Time Pad(OTP)	التّشفير بمفتاح المرة الواحدة
Open System Interconnection(OSI) Model	نظام الربط البيني المفتوح
Operating System	نظام التشغيل
Operating System Events Log	سجل أحداث نظام التشغيل
Output Feedback Mode(OFB)	أسلوب التغذية العكسيّة للمخرجات
Packet Header	رأس (أو ترويسة) رزمة البيانات
Packets	رزم (أو حزم) البيانات
Padding	تكملة (أو ملء)
Parallel	التوازي
Password Crack	كسر كلمات المرور
Patches	تحديثات (أو رقع)
Peer Entity Authentication	التحقّق من هوية الشخص أو الجهة
Peer-to-Peer	شبكة الند للند
Permissions	أذونات
Personal Identification Number(PIN)	رقم التعريف الشخصي
Physical Layer	الطبقة الماديّة
Physical Security	الحماية الماديّة أو الفيزيقية

Plain Text	النّص الصريح (قبل تشفيره)
Point at Infinity	النقطة في اللانهاية
Policies	السياسات الأمنيّة
Pop-UP Blockers	حاجبات النوافذ المنبثقة
Port Filtering	التنقيح باستخدام المنفذ
Power Analysis Attack	هجوم تحليل الطاقة الكهربائيّة
Presentation Layer	طبقة العرض
Print Server	خادم الطباعة
Privacy	الخصوصية
Private Key	مفتاح خاص
Procedures	الإجراءات
Process Management	إدارة العمليّات
Public Key	مفتاح عام
Public Key Encryption	التّشفير غير المتناظر (أو التّشفير بالمفتاح العام)
Public Key Infrastructure(PKI)	البُنية التحتية للمفاتيح العامة
Random Access Memory(RAM)	الذاكرة العشوائية
Read Only Memory(ROM)	الذاكرة القرائية فقط
Rights	حقوق
Ring Topology	البُنية الحلقية
RIPE NCC	مركز تنسيق الشبكة الأوربية
Risk	الخطر
Rivest-Shamir-Adleman(RSA)	نظام تشفير رايفست وشامير وادليمان – آر إس أيه
RJ41	مقبس الهاتف
RJ45	مقبس شبكة الحاسب الآلي
Router	موجِّه
Scalar Multiplication	الضرب التراكمي
Secure Hash Algorithm-1(SHA-1)	خوارزميّة (SHA-1)
Secure Hash Algorithm-2(SHA-2)	خوارزميّة (SHA-2)
Secure Hash Algorithm-3(SHA-3)	خوارزميّة (SHA-3)
Secure Sockets Layer(SSL)	طبقة المقابس الآمنة

Security Analysis Tool for Auditing Network(SATAN)	أداة التحليل الأمني لتدقيق البيانات
Security Level	مستوى السِّريّة
Security Operation Center(SOC)	مركز عمليّات أمن الشبكة
Sequential Query Language(SQL)	لغة الاستفسار العلائقية
Server	جهاز مركزي(خادم)
Session Layer	طبقة الجلسة
Shielded Twisted Pair(STP)	الكابلات المجدولة
Short Message Service(SMS)	خدمة الرسائل القصيرة
Shoulder Surfing Attack	هجوم تصفح الكتف
Side channel Attacks	هجمات المعلومات الجانبية
Simple Mail Transport Protocol	بروتوكول نقل البريد الإلكتروني البسيط
Single Loss Expectancy(SLE)	قيمة الخسارة الأحادية المتوقعة
Single Point of Failure	نقطة العطل الوحيدة
Single Sign-on	تسجيل الدخول الواحد
Sniffer Attacks	هجمات التشمم أو الالتقاط
Social Engineering Attacks	هجمات الهندسة الاجتماعيّة
Software	البرامج(أو البرمجيات)
Source Code	شيفرة(كود) المصدر
Spam	الرسائل غير المرغوب فيها(أو المزعجة)
Special Purpose	لغرض خاص
Spoofing Attacks	هجمات الخداع
Spyware	برامج التجسّس
Standards	المعايير القياسية
Star Topology	البُنية النجمية
Star Tree Topology	البُنية النجمية الشجرية
Static Pages	صفحات ساكنة(جامدة)
Stream Cipher	التّشفير التسلسلي
Structured Data	بيانات هيكلية
Substitution Attack	هجوم التعويض
Switch	موزع
Symmetric Key Encryption	التّشفير المتناظر
System-Specific Security Policy	السياسة الأمنيّة لنظام محدّد

T-Connector	أداة ربط خاصّة تكون على شكل حرف (T)
TCP Hijacking Attack	هجوم اختطاف بروتوكول النقل
Terminal	نهايات طرفية
Terminator	سدادة
Thin Client	العميل اللطيف (أو الرقيق)
Threat	التهديد
Three-Tier Architecture	نظام الحماية ذو الطبقات الثلاث
Time Stamping	بصمة التاريخ والوقت
Timing Attack	هجوم الوقت
Token	وصلة ذاكرة «توكن»
Track 0	قطاع الصفر (أول قطاع في قرص التخزين)
Traffic Analysis	تحليل البيانات المارة
Transmission Control Protocol(TCP)	بروتوكول التحكّم بالنقل
Transport Control Protocol/Internet Protocol(TCP/IP)	بروتوكول التحكّم بالنقل بعنوان الإنترنت
Transport Layer	طبقة النقل
Triple Data Encryption Standard(3DES)	خوارزميّة تشفير البيانات القياسي الثلاثي
Two-Tier Architecture	نظام الحماية ذو الطبقتين
Uniform Resource Location(URL)	محدّد مواقع الويب (أو الرابط)
Uninterruptable Power Supply(UPS)	مانع انقطاع التيار الكهربائي
Universal Serial Bus(USB)	الناقل التسلسلي العالمي
Virtual Local Area Network(VLAN)	شبكة محلية افتراضيّة (أو تخيلية)
Virtual Private Network(VPN)	الشبكة الخاصة الافتراضيّة
VPN Tunnel	نفق في الشبكة الخاصة الافتراضيّة
Vulnerability	الضعف أو قابلية الإصابة
Web Server	خادم الشبكة العنكبوتية (خادم الويب)
Wide Area Network(WAN)	شبكة حاسب آلي واسعة
Wipe	محو نهائي غير مسترجع
Workstation	محطة عمل (جهاز حاسب آلي)
World Wide Web(WWW)	الشبكة العنكبوتية العالمية (الويب)
Zeroization	التصفير (جعل جميع القيم صفرًا)

المراجع العربيّة

[١] إبراهيم، خالد ممدوح(٢٠٠٨)، "أمن المعلومات الإلكترونيّة"، الدار الجامعية، الإسكندرية، مصر، ٢٠٠٨.

[٢] إبراهيم، خالد ممدوح(٢٠٠٨)، "أمن الحكومة الإلكترونيّة"، الدار الجامعية، الإسكندرية، مصر، ٢٠٠٨.

[٣] البداينة، ذياب(٢٠٠٦)، "الأمن وحرب المعلومات"، دار الشروق للنشر والتوزيع، عمان، الأردن، ٢٠٠٦.

[٤] البداينة، ذياب(١٩٩٩)، "جرائم الحاسب والإنترنت"، ورقة مقدّمة في الندوة العلمية "الجرائم المستحدثة في الوطن العربي"، تونس، جامعة نايف العربيّة للعلوم الأمنيّة، ١٩٩٩.

[٥] بدران، عدنان(٢٠٠٧)، "الحكومة الإلكترونيّة من الإستراتيجية إلى التطبيق"، المؤسّسة العربيّة للدراسات والنشر، بيروت، ٢٠٠٤.

[٦] توماس، طوم(٢٠٠٤)، "الخطوة الأولى نحو أمان الشبكات"، كتاب مترجم، الدار العربيّة للعلوم، بيروت، لبنان، ٢٠٠٤.

[٧] الخليفة، محسن بن سليمان(٢٠٠٣)، "جرائم الحاسب الآلي وعقوبتها في الفقه والنظام"، رسالة ماجستير، جامعة نايف العربيّة للعلوم الأمنيّة، الرياض، ٢٠٠٣.

[٨] داود، حسن طاهر(٢٠٠٢)، "جرائم نظم المعلومات"، جامعة نايف العربيّة للعلوم الأمنيّة، الرياض، ٢٠٠٢.

[٩] داود، حسن طاهر(٢٠٠٤أ)، "الأمن في عصر المعلومات"، جامعة نايف العربيّة للعلوم الأمنيّة، الرياض، ٢٠٠٤.

[١٠] داود، حسن طاهر(٢٠٠٤ب)، "أمن شبكات المعلومات"، معهد الإدارة العامة، الرياض، ٢٠٠٤.

[١١] السرحاني،محمدبنناصر(٢٠٠٤)،"مهاراتالتحقيقالجنائيالفنيفيجرائمالحاسوب

والإنترنت"، رسالة ماجستير، جامعة نايف العربيّة للعلوم الأمنيّة، الرياض، ٢٠٠٤.

[١٢] السويل، محمد بن ابراهيم(١٤١٧)، "المدخل إلى علم التّشفير"، دار الخريجي للنشر والتوزيع، الرياض، ١٤١٧هـ.

[١٣] صادق، دلال و الفتال، حميد ناصر(٢٠٠٨)، "أمن المعلومات"، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، ٢٠٠٨.

[١٤] الغثبر، خالد بن سليمان و القحطاني، محمد بن عبدالله(٢٠٠٩)، "أمن المعلومات بلغة ميسرة"، مركز التميز لأمن المعلومات، جامعة الملك سعود، ٢٠٠٩.

[١٥] الغثبر، خالد بن سليمان و بن هيشة، سليمان بن عبدالعزيز(٢٠٠٩)، "الإصطياد الإلكتروني: الأساليب والإجراءات المضادة"، مركز التميز لأمن المعلومات، جامعة الملك سعود، ٢٠٠٩.

[١٦] الناظر، سائد محمود(٢٠٠٥)، "التعمية وأمن الشبكات"، الجزء الأول، شعاع للنشر والتوزيع، حلب، سوريا، ٢٠٠٥.

[١٧] وليام ستولينج(١٤٣٢)، "أساسيات أمن الشبكات: تطبيقات ومعايير"، كتاب مترجم إلى اللغة العربيّة، العبيكان للنشر والتوزيع، الرياض، ١٤٣٢ هـ.

المراجع الأجنبية

[1] Al-Gahtani, Theeb A.(2006), “Dynamic Projective Coordinates in Elliptic Curve Cryptography”, Ph. D. Dissertation, King Fahd University for Petroleum and Minerals, Dahran, Saudi Arabia, 2006.

[2] Anderson, Ross J.(2008), “Security Engineering: A Guide to Building Dependable Distributed Systems” , Wiley Publishing, Inc., Indianapolis, Indiana, USA, 2008.

[3] Bhaskar, S. M., and Ahson S. I., “Information Security: A practical Approach”, Alpha Science International LTD, Oxford, U.K., 2008.

[4] Bhaskar, S.M and Ramachandran, P.(2006), “Handbook of Security, Cryptography and Digital Signature”, Viva Books Private Ltd., New Delhi, 2006.

[5] Bidgoli, Hossein(2006a), “Handbook of Information Security”, Volume 1, John Wiley & Sons, Inc., Hoboken, New jersey, 2006.

[6] Bidgoli, Hossein(2006b), “Handbook of Information Security”, Volume 2, John Wiley & Sons, Inc., Hoboken, New jersey, 2006.

[7] Bidgoli, Hossein(2006c), “Handbook of Information Security”, Volume 3, John Wiley & Sons, Inc., Hoboken, New jersey, 2006.

[8] Casey, Eoghan(2004), “Digital Evidence and Computer Crime”, Second Edition, ACADEMIC Press, 2004.

[9] Christof Paar and Jan Pelzl(2010), “Understanding Cryptography”, Springer-Verlag Berlin Heidelberg, 2010.

[10] Eric Col et. al.(2003), “SANS Security Essentials with CISSP CBK”, Volume 1, The SANS Institute, 2003.

[11] Eric Col et. al.(2003), “SANS Security Essentials with CISSP CBK”, Volume 2, The SANS Institute, 2003.

[12] Ferguson, Niels and Schneier Bruce (2003), “Practical Cryptography”, Wiley Publishing, Inc., Indianapolis, Indiana, USA, 2003.

[13] Fugini, Mariagrazia, et. Al.(2004), “Information Security Policies and Action in Modern Integrated Systems”, Idea Group Inc., 2004.

[14] Goldreich, Oded(2001), “Foundations of Cryptography: Volume 1 Basic Tools”, Cambridge University Press, 2001.

[15] Goldreich, Oded(2004), “Foundations of Cryptography: Volume II Basic Applications”, Cambridge University Press, 2004.

[16] Gollmann, Dieter(2006), “Computer Security”, Second edition, John Wiley & Sons, Ltd, England, 2006.

[17] Hankerson D., et. al.,(2004), “A Guide to Elliptic Curve Cryptography”, Springer-Verlag, Ney York, Inc., 2004.

[18] Herold, Rebecca(2005), “Managing an Information Security, Privacy Awareness and Training”, Auerbach publications Taylor & Francis Group, Boca Raton, Florida, 2005.

[19] Koblitz, Neal(2006), “A Course in Number Theory and Cryptography”, Second Edition, Springer Science and Business Media, LLC., 2006.

[20] Koblitz Neal(1987), “Elliptic curve cryptosystems”, Mathematics of Computation, 48(1987), 203–209.

[21] Mangard et. al.(2007), “Power Analysis Attacks: Revealing the Secrets of Smart Cards”, Springer Science and Business Media, LCC, 2007.

[22] Mao, Wenbo(2004), “Modern Cryptography: Theory and Practice”, Prentice-Hall, Inc., 2004.

[23] McDaniel, George(1994), “IBM Dictionary of Computing”, McGraw-Hill, Inc, New York, 1994.

[24] Menezes, A. et. al.(1997), “Handbook of Applied Cryptography”, CRC Press, Boca Raton, Florida, USA, 1997.

[25] V. S. Miller(1986), “Use of elliptic curves in cryptography”, Advances in Cryptology Proceedings of Crypto’85, Lecture Notes in Computer Science, 218(1986), Springer-Verlag, 417–426.

[26] Nichols, Randall K. and Lekkas, Panos C.(2002), “Wireless Security: Models, Threats, and Solutions”, McGraw-Hill Companies, Inc., 2002.

[27] Salomon, David(2003), “Data Privacy and Security”, Springer-Verlag, New York, 2003.

[28] Schneier, Bruce (1996), “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, Second Edition, John Wiley & Sons, Inc., 1996.

[29] Shon Harris(2008), “All-in-One CISSP Exam Guide”, Fourth Edition, McGraw-Hill Companies, 2008.

[30] Stallings, William (2006), “Cryptography and Network Security: Principles and Practices”, Fourth Edition, Prentice-Hall, 2006.

[31] Stallings, William (2007), “Network Security Essentials: Applications and Standards”, Third Edition, Prentice-Hall, 2007.

[32] Stamp, Mark (2006), “Information Security : Principles and Practice”, John Wiley & Sons, Inc., 2006.

[33] Stinson, Douglas R.(2006), “Cryptography: Theory and Practice”, Third Edition, Taylor & Francis Group, LLC., 2006.

[34] Tipton, H. and Krause, M.(2005), “Information Security Management Handbook”, Fifth Edition, Vol. 2, CRC Press LLC., 2005.

[35] Trappe, Wade and Washington, Lawrence C.(2006), “Introduction to Cryptography with Coding Theory”, Second Edition, Prentice-Hall, Inc., 2006.

[36] Viega, John and McGraw Gary(2002), “Building Secure Software: How to Avoid Security Problems the Right Way”, Addison-Wesley, 2002.

[37] Whitfield Diffie and Martin Hellman(1976), “New Directins in Cryptography”, IEEE Transactions on Information Theory, IT-22:644-654, 1976.

[38] Withman, M. and Mattord, H.(2005), “Principles of Information Security”, Second Edition, Thomson Course Technology, 2005.

المراجع من شبكة الإنترنت

[١] موقع المركز الوطني للتصديق الرقمي في المملكة العربيّة السعودية
http://www.pki.gov.sa/

[٢] موقع مركز التميز لأمن المعلومات بجامعة الملك سعود، المملكة العربيّة السعودية
http://coeia.edu.sa/

[3] CERT Site:
http://www.cert.org/tech_tips/FBI_investigates_crime.html

[4] Computer Security Institute(CSI) Survey(2011), The 15th Annual Computer Crime and Security Survey:
http://www.GoCSI.com

[5] FBI Handbook of Forensic Services:
http://www.fbi.gov/hq/lab/handbook/intro.htm

[6] Federal Guidelines for Search and Seizing Computers:
http://www.usdoj.gov/criminal/cybercrime/search_docs

[7] File Extensions Organization:
http://www.file-extensions.org/

[8] Forensics Science and Law Enforcement:
http://www.ssc.msu.edu/~forensic/links.html

[9] PC Pitstop statistics: Spyware and adware(2004):
http://www.pcpitstop.com/research/spyware.asp

[10] The Committee on National Security Systems:
http://www.cnss.gov

عن الكتاب:

يعرِّف هذا الكتاب "أمن المعلومات" ويُجيب على التساؤل الكبير: لماذا أمن المعلومات؟ ثم يستعرض مفاهيم وتقنيات ووسائل أمن المعلومات؛ فيبدأ بتعريف وشرح عناصر أمن المعلومات، وهي: التحقق من الهوية، والتحكم بالوصول، والسرية، وسلامة المعلومة وتكاملها، وعدم الإنكار وتوفر المعلومة، والتدقيق. بعد ذلك يشرح طرق ووسائل تحقيق عناصر أمن المعلومات ومنها: التشفير بأنواعه، والتصديق الرقمي، والبصمة الرقمية، كما يقدم شرحًا وافيًا لسياسات ومعايير وتوجيهات وإجراءات أمن المعلومات التي تعدّ الركيزة النظرية والإدارية لأمن المعلومات، ثم يستعرض مفاهيم ووسائل أمن الحاسبات والبرمجيات والملفات وكذلك أمن شبكات الحاسب الآلي بشكل تفصيلي. يشرح بعدها إدارة المخاطر المعلوماتية وطرق تحليل تلك المخاطر ويقدم أمثلة لذلك، ثم الحماية المادية (الحسّية) للمعلومات بشقيها الإداري والتقني وكيف يمكن وضعها على شكل حلقات حماية كل منها يغلف الآخر لتقدم في مجملها الحماية المادية المطلوبة. ويختتم الكتاب بالتعريف بجرائم المعلوماتية وخصائصها والأدلة الرقمية وطرق الحصول عليها ومواصفات الدليل الرقمي الجيد، ثم يوضح العلاقة بين أمن المعلومات والأدلة الرقمية.

المؤلف:

حصل على درجة الدكتوراة من جامعة الملك فهد للبترول والمعادن عام ٢٠٠٦م في علوم وهندسة الحاسب الآلي، ودرجة الماجستير من جامعة الملك سعود عام ١٩٩٧م في هندسة الحاسب الآلي، ودرجة البكالوريوس من جامعة الملك سعود عام ١٩٩١م في هندسة الحاسب الآلي، وقد التحق بعدها للعمل بمجال الحاسب الآلي وتقنية المعلومات بوزارة الداخلية وما زال يعمل بها حتى الآن.

حاصل على أربع براءات اختراع في مجال أمن المعلومات والتشفير مسجلة ومنشورة لدى مكتب براءات الاختراع الامريكي، كما حصل على الميدالية الذهبية في معرض جنيف الدولي للمخترعين للعام ٢٠١٢م.

مدينة الملك عبدالعزيز للعلوم والتقنية KACST

تعمل مدينة الملك عبد العزيز للعلوم والتقنية على توفير المعرفة للقارئ العربي. فقامت في هذا الإطار بنشر سلسلة من الكتب والمجلات العلمية وأتاحتها للقراء دون مقابل بصيغتيها الرقمية والورقية. فجميع إصدارات المدينة متاحة على موقعها الإلكتروني ليتمكن المتصفح من تحميلها أو قراءتها على الإنترنت.

هاتف: ٠١١ ٤٨٨٣٤٤٤ - ٠١١ ٤٨٨٣٥٥٥
فاكس: ٠١١ ٤٨٨٣٧٥٦
ص.ب. ٦٠٨٦ الرياض ١١٤٤٢
المملكة العربية السعودية
مدينة الملك عبدالعزيز للعلوم والتقنية

الموقع الالكتروني: www.kacst.edu.sa
إصدارات المدينة: publications.kacst.edu.sa
البريد الالكتروني: awareness@kacst.edu.sa

مطابع مدينة الملك عبدالعزيز للعلوم والتقنية
رقم: ٣٥٠١٠٥
ردمك: ٨-٧٧-٨٠٤٩-٦٠٣-٩٧٨