جامعة نايف العربية للعلوم الأمنية

Naif Arab University For Security Sciences

أمن المعلومات الجنائية وطرق الحماية والحفظ

د. عبدالرحمن بن عبدالعزيز الشنيفي

٢٠٠٢م

أمن المعلومات الجنائية
وسبل الحماية والحفظ

د. عبدالرحمن بن عبدالعزيز الشنيفي

أمن المعلومات الجنائية وسبل الحماية والحفظ

المقدمـــــة

إن الطلب على المعلومات المعالجة قد ازداد بدرجة كبيرة بحيث وصل إلى أن الكثير من المنشآت لا يمكن أن تدير شئونها بدون تلك المعلومات، بل تصل إلى أن معظم أن لم يكن كل نشاطاتها معرضة للتوقف لو تعرض نظامها الآلي إلى التخريب أو أن معلوماتها المخزنة تعرضت للتلف من خلال الاختراقات الأمنية التي قد تعرض لها النظام.

إن كثرة هذا الطلب سيجعلها عرضة للابتزاز من قبل الكثير من الانتهازيين والخارجين عن القانون.

وبالإمكان أن ينطبق ذلك على الكثير من المعلومات الأمنية والتي من ضمنها المعلومات الجنائية. لذا فإنه من الضروري حماية هذه المعلومات من خلال العديد من الإجراءات التي ستتطرق اليها هذه المحاضرة

أهداف البحث

إن أحد أهم أهداف الحماية الأمنية للمعلومات هو ضمان استمرارية توفرها للمستفيدين من جانب والتأكد من أن هذه المعلومات لن تصل إلا للمستفيد المصرح له فقط من جانب آخر.

يهدف هذا البحث إلى معالجة بعض الجوانب المتصلة بأمن المعلومات الأمنية والتي من ضمنها المعلومات الجنائية وسبل حمايتها لذا فإن الجزء الأول سيتطرق إلى المخاطر المادية وغير المادية وسبل مواجهتها.

أما الجزء الثاني فيتناول النواحي القانونية لأمن الحاسب الآلي. الجزء الثالث فسيتطرق إلى المفاهيم الأمنية وما تحتويه من أهداف ومسئوليات الجزء الرابع فيشمل الخاتمة والتوصيات.

الجزء الأول : المخاطر المادية وغير المادية ومواجهتها

يمكننا القول أن المخاطر المادية وغير المادية تحدث بين الحين والآخر لبعض مراكز المعلومات. في هذا الجزء من المحاضرة سنتطرق إلى الكثير من هذه المخاطر والتي قد تحدث لأية مركز معلومات سواء كان ذا طابق أمني أو خلافه، بالإضافة إلى بعض الإجراءات الوقائية التي عادة ما ترعى لتفادي هذه المخاطر.

أولاً : أمن الأجهزة

إن هذه الأجهزة الآلية لا يمكن أن يحدث منها أي تصرف خطر، بل أن مصدر هذا الخطر ينبع من سوء التصرف من بعض الفنيين العاملين على هذه الأجهزة والتي منها على سبيل المثال :

١ ـ زرع أجهزة تنصت للقيام بارسال معلومات إلى الجهة المستفيدة صاحبة أجهزة التنصت هذه.

٢ ـ استخدام بعض قطع الغيار التي تحتوي على أجهزة تنصت.

٣ ـ تصميم ومن ثم تركيب أجهزة تنصت داخل اللوحات الالكترونية على شكل ذاكرة يمكن تخزين معلومات هامة جداً ومن ثم استبدالها أو نزعها عندما يتم التوصل إلى الهدف المنشود.

٤ ـ إخراج ومن ثم استغلال قطع الغيار التالفة والتي تحتوي على وسائل تخزين المعلومات بحجة إصلاحها.

٥ ـ وضع أجهزة خاصة أو هوائيات داخل غرفة الأجهزة المركزية تقوم بالتقاط وبث الاشارات الصادرة من هذه الأجهزة .

٦ ـ استخدام بعض البرامج والأجهزة الغربية والغير معروفة بحجة إجراء بعض التجارب والفحوصات الفنية .

٧ ـ جعل بعض البرامج والأجهزة تعمل بطريقة غريبة والذي بدوره يؤثر على هذه الأجهزة والبرامج وجعلها تقوم بتغيير أو تسريب المعلومات للأطراف الراغبة في الاختراق لتحقيق أهدافهم .

ولتفادي الاخطار الناجمة عن هذه التصرفات ، فإن هناك بعض الإجراءات التي يمكن اتباعها منها على سبيل المثال :

١ ـ تركيب أجهزة مراقبة تلفزيونية في جميع منشآت الحاسب الآلي مع التركيز على غرفة الأجهزة والاتصالات .

٢ ـ ضرورة تواجد كوادر وطنية نزيهة ذات معرفة تامة بالنظام في غرفة الأجهزة والاتصالات .

٣ ـ التنبيه للمشغلين والمبرمجين بضرورة الابلاغ عن أية أجهزة وبرامج غريبة في غرفة الأجهزة والاتصالات .

٤ ـ ضرورة استخدام جميع قطع الغيار الأصلية والتأكد من ذلك إدارياً وفنياً .

٥ ـ ضرورة التأكد من أن قطع الغيار التالفة سترسل إلى المصنع الأصلي وانها خالية من أية معلومات وعدم السماح باخراجها إلا في اضيق الحدود .

٦ ـ ضرورة وجود أجهزة خاصة بالكشف عن أجهزة التنصت أو الإرسال والقيام بمسح دوري لمنشآت الحاسب الآلي .

ثانياً : أمن البرامج

بالإضافة إلى ما سبق الإشارة اليه في بداية هذا الجزء، فإنه بالإمكان القول أن برامج الحاسب الآلي سواء كانت نظماً تشغيلية أو برامج تطبيقية أو قواعد المعلومات قد تكون غير خالية من الفجوات والأخطاء، بالإضافة إلى عدم قدرة الأجهزة والبرامج إلى التعرف على نوعية المستفيد وأهدافه وذلك لانها لا تملك هذه القدرة على التمييز بين أهداف المستخدمين.

هناك العديد من البرامج المتطورة جداً وذلك للقيام بالأعمال التخريبية. هذه البرامج لديها القدرة على استغلال نقاط الضعف في برامج الحاسب الآلي وأنظمته. لقد صممت هذه البرامج بطرق يصعب حتى على ذوي الاختصاص كشفها ومن ثم الغاؤها وحتى الوقاية منها ذلك أنها كتبت بواسطة أناس محترفين اوجدوا داخلها العديد من الحيل لتفادي الكشف عنها من قبل العاملين على الحاسب الآلي.

لقد طورت هذه البرامج لتتوافق مع طبيعة الأهداف التخريبية التي بنيت على أساسها. وفيما يلي بعضاً من الأضرار التي يمكن أن تحدثها هذه البرامج:

١ ـ تبديد طاقة الحاسب الآلي التخزينية.

٢ ـ ايقاف الأجهزة وأنظمتها.

٣ ـ إتلاف المعلومات المخزنة.

٤ ـ التقليل من سرعة أداء النظام.

٥ ـ إحداث ملفات غير مشروعة.

٦ ـ حرمان المستفيد من الوصول إلى النظام.

٧ ـ إرسال معلومات إلى جهات غير مصرح لها .

٨ ـ تمكين أفراد غير مصرح لهم من الدخول على النظام .

٩ ـ تغيير وخلط مكونات الملفات وبنيتها الأساسية .

هناك العديد من البرامج التخريبية والتي منها القنابل الموقوتة، حصان طروادة، الديدان، الفيروسات بأنواعها والتي لا مجال هنا للتحدث عنها بالتفصيل .

١ ـ الردع

هذا الإجراء يكفل عدم دخول أي برنامج أو برامج تخريبية أو وصول أي طرف غير مرخص له وتمكنه من استخدام النظام، وفي حالة الفشل في ذلك فإنه يجب اتخاذ الإجراءات الفنية اللازمة لتفادي وعدم تمكين هذه البرامج من أداء مهامها التخريبية وعرقلة انتشارها .

٢ ـ التحري

تتطلب هذه العملية دراسة فنية واجرائية للآثار التي قد يخلفها البرنامج التخريبي والاسلوب الذي اتبعه في وظائفه وذلك في محاولة لدراسة سلوكه ومن ثم تطوير الاسلوب الامثل للقضاء عليه ومن ثم الحماية منه في المستقبل .

٣ ـ الاحتواء

بعد اكتشاف هذه البرامج أو البرنامج التخريبي يجب عزل المعلومات غير الملوثة بالإضافة إلى عزله عزلاً تاماً ومنع انتشاره وهذا عادة يتطلب إجراء بعض التعديلات في نظام التشغيل وغيره من البرامج والتي كان يستخدمها في الانتشار . بل قد يتطلب الأمر إيقاف النظام .

٤ ـ استرجاع القدرة التشغيلية

يهدف هذا الإجراء إلى التأكد من قدرة النظام إلى العودة لطبيعته التشغيلية وذلك بعد التأكد من خلوه من البرنامج أو البرامج التخريبية .

هناك العديد من الإجراءات الوقائية التي يلزم اتباعها وذلك للوصول إلى مستوى أمني عال والتي منها :

١ ـ الاحتفاظ بنسخة رئيسية للبرامج خارج مقر الحاسب الآلي بالإضافة إلى البيانات والتي تحدث بصفة دورية أو كلما دعت الحاجة .

٢ ـ مقارنة البرامج الاحتياطية بالموجودة في النظام وذلك للتأكد من مطابقتها لبعض .

٣ ـ رصد وتسجيل جميع الأخطاء والمخالفات الأمنية التي قد تحدث والرجوع إليها عند الحاجة .

هناك أسس يجب حمايتها والتي تعتبر من المقومات المهمة جداً لأمن النظام . هذه الأسس هي كما يلي :

١ ـ السرية

تتضمن هذه الخاصية سرية المعلومات المخزنة داخل النظام إذ لا تسمح لطرف غير مصرح له بالدخول إلى الملفات والبرامج بقصد استغلالها . هذه السرية قد تشتمل على برنامج كامل أو جزء من هذا البرنامج .

٢ ـ التكامل والخصوصية

هذه الخاصية تعتبر الأساس في حماية المعلومات والبرامج إذ تمنع إدخال أو تعديل أو إضافة أو حذف للمعلومات التي تحتويها الملفات والبرامج إلا بعد أخذ الإذن اللازم لعمل ذلك .

٣ ـ التوفر والاتاحة

نعني بذلك إمكانية الدخول إلى النظام والوصول إلى المعلومات والبرامج المخزنة بداخله . هذا ويتضمن النظام برامج تحدد هذا التوفر وذلك لحمايته من الدخول غير المشروع . إن الإطاحة بهذا الأساس يمكن أن ينجم عنه الإخلال بإجراءات الأمن الأخرى التي بني عليها النظام الأمني فتصبح مدخلاً يتعرض منه النظام إلى عمليات السطو والتخريب الأخرى .

ثالثاً : أمن الشبكة

شبكة الحاسب الآلي عبارة عن مجموعة من البرامج والأجهزة مرتبطة بنظام الحاسب الآلي وذلك لنقل البيانات بين وحدات النظام أو بين نظامين مستقلين أو الإثنين معاً . هناك نوعين من شبكات الحاسب الآلي هما الشبكات المحلية (LAN) والشبكات بعيدة المدى (WAN) . الشبكة المحلية لا يتعدى نطاقها منشأة واحدة متوسطة الحجم .

أما الشبكات بعيدة المدى فلا حدود لها والذي قد يمتد مداها داخل البلد الواحد أو بين عدة بلدان متجاورة أو بين قارات .

ونظراً لتعدد هذه الشبكات سواء من حيث الحجم أو الأجهزة والبرامج فإن الصعوبة تكمن في عزل مخاطرها المختلفة . لذا سوف يعالج هذا القسم بعضاً من هذه الأخطار والإجراءات الوقائية التي في الإمكان اتخاذها .

هناك العديد من المخاطر التي قد تتعرض لها شبكات الحاسب الآلي والتي منها على سبيل المثال :

١ ـ طبيعية : وتقصد بها الأخطار التي تعزي إلى قدرة الله سبحانه وتعالى والتي منها الزلازل ، الأمطار ، الأتربة ، والغبار وغيرها .

٢ ـ بيئية : والتي تنشأ من عوامل موجودة في الطبيعة والتي منها تسرب المياه من مصادر التكييف أو شبكة المياه، الحرائق التي مصدرها التماس كهربائي، تعطل خطوط الهاتف وذلك لعوامل طبيعية .

٣ ـ بشرية : تنطوي هذه الخطورة من وجود عناصر بشرية غير نزيهة سواء داخل المنشأة أو خارجها .

هناك العديد من الإجراءات الوقائية التي في الإمكان اتخاذها والتي منها على سبيل المثال :

١ ـ دراسة الوضع الجغرافي لمواقع هذه المنشآت مع التأكيد على وضع مواصفات فنية دقيقة جداً لهذه المنشآت .

٢ ـ تطبيق الصيانة الوقائية لجميع مكونات المنشأة سواء لأجهزة الحاسب الآلي والاتصالات أو المنشأة .

٣ ـ التأكد من نزاهة جميع الأفراد العاملين على الأجهزة والبرامج للنظام وشبكة الاتصالات .

رابعاً : أمن الوثائق

جميع أنظمة الحاسب الآلي وشبكات الاتصالات تكون مصحوبة بجميع الوثائق اللازمة والتي تعكس واقع هذه الأنظمة . ومع ضرورة تواجد هذه الوثائق وما تحمله من اهمية كبرى، فإنها قد تكون مصدر قلق على أمن النظام إذا وقعت في أيد غير نزيهة أو غير مصرح لها بذلك .

ولتفادي هذا القلق فإن هناك العديد من الإجراءات الواجب اتباعها لحماية هذه الوثائق والتي منها :

١ ـ تحديد إدارة تكون مسئولة عن أمن وسلامة هذه الوثائق .

٢ ـ تحديث هذه الوثائق طبقاً لما يستجد على النظام من تحديث .
٣ ـ عدم الإطلاع على هذه الوثائق إلا من قبل الأشخاص المصرح لهم .
٤ ـ إتلاف التقارير أو الوثائق التي تصدر من النظام .

خامساً : أمن العاملين

نظراً لقدرة أجهزة الحاسب الآلي على تلبية احتياجات المستفيد دون أي تفرقة تذكر لعدم امتلاكها للحواس والطبائع البشرية القادرة على التمييز بين سلوك المستفيدين . هذه القدرة تعتبر خطراً على أمن المعلومات المخزنة إذا ما اسئ استخدامها من قبل هؤلاء العاملين .

لقد قام دان باركر (Dan Parker) من معهد ستانفورد للبحوث بعمل استبيان في عام ١٩٧٦م شمل ٥٧٣ قضية جنائية وسوء استخدام للحاسب الآلي وقام بتصنيف هذه القضايا ونسبة وقوعها وذلك حسب طبيعتها ومصدرها واشتملت على الآتي (١) :

١ ـ تجهيز البيانات والتقارير	٣٣٪
٢ ـ تشغيل الحاسب الآلي	٢٦٪
٣ ـ خارج نطاق تجهيزات الحاسب الآلي	١٣٪
٤ ـ النهايات الطرفية المرتبطة بالنظام	٩٪
٥ ـ إدارات البرمجة	٧٪
٦ ـ أسباب أخرى	١٢٪

أما أسباب وقوع هذه القضايا فقد اشتملت على الآتي :

١ ـ الإجراءات الإدارية	٤١٪

٢ ـ أمن المنشآت	٪١٣
٣ ـ الأمانة واخلاقيات العمل	٪١٢
٤ ـ الاهمال	٪١١
٥ ـ التحكم في البرامج	٪٩
٦ ـ أسباب أخرى	٪١٤

من هذا الاستبيان يتضح مقدار سوء استخدام المعلومات واحتكارها من قبل العاملين على الحاسب الآلي. ولتفادي الأخطار الناجمة عن ذلك لابد من التأكد من نزاهة هؤلاء العاملين مع تحصينهم ضد الاغراءات المادية التي قد يتعرضون لها من جهات عدة.

الجزء الثاني : النواحي القانونية لأمن الحاسب الآلي

إن تطوير جميع نشاطات وكالات العدل الجنائي عن طريق الحاسب الآلي تعزز من قدرة هذه الوكالات في كل مجال تقريباً ذا أهمية. والواضح بأن الحاسب الآلي تستعمله الكثير من الوكالات والأجهزة الحكومية لاغراض السيطرة، وبدون شك فإن استخدام الحاسب الآلي لقيامهم بواجباتهم في أقصر وقت.

ويستخدم مكتب المباحث الاتحادي «وكالة التحري الأمريكية» والذي سوف يرمز إليه فيما بعد بالأحرف اللاتينية المشهور بها FBI، نظام المعلومات بدرجة كبيرة. إن مركز المعلومات الوطني للجرائم والذي يرمز اختصاره بالأحرف اللاتينية NCIC هي شبكة معلومات آلية في جميع أنحاء البلاد

(1) Squires,Tony, Computer security: The personnel aspect NCC publications, Manchester,England,1980,pp.100-101.

للشرطة . ويتم ربط النهايات الطرفية لاقسام الشرطة المحلية بحاسب الشرطة المركزية في الولايات المختلفة وكذلك يتم توصيله مع مركز المعلومات الوطني للجرائم NCIC في العاصمة الأمريكية واشنطن دي سي .

وبهذا يمكن الدخول إلى سجلات الاعتقال الخاصة بالأفراد في اقصر وقت ممكن . أن التوصل لمثل هذه المعلومات يساعد رجال الأمن في اتخاذ قراراتهم بخصوص اعتقال وتفتيش واحتجاز واستجواب والتحقيق مع اولئك الذين يشك في انهم ارتكبوا الجرائم . ومن امثلة استخدام مثل هذا النظام ما ذكرته مجلة الكمبيوتر في عددها الصادر بتاريخ ٢٤ مارس ١٩٧١م . حيث تم اعتقال أحد المسافرين المتطفلين الذين يوقفون السيارات ويركبونها مجاناً في بينفيل بولاية كنتاكي حيث توق لاستعمال دورات المياه التابعة لاحدى اقسام الشرطة ، حيث انه وبفحص روتيني مع مركز المعلومات الوطني للجرائم NCIC تبين بأن هذا الشخص قد أخل بوعده الذي قطعه على نفسه بأن لا يغادر مقر إقامته بعد إطلاق سراحه مؤقتاً وذلك في لانسنج في ميتشجان [1] .

وفي عام ١٩٦٨م قام الكونغرس الأمريكي بتشريع قانون الشوارع الآمنة والسيطرة على الجريمة والذي تم على ضوئه إنشاء «الإدارة المساعدة لتعزيز القانون» (LEAA) وتكون هذه الإدارة جهازاً حكومياً يتبع وزارة العمل . وقد تم استخدام بعض المنح التابعة للإدارة المساعدة لتعزيز القانون في شراء أجهزة حاسب آلي لاستعمالها من قبل قوات الشرطة المحلية والتابعة للدولة . ورغم أن نظام المعلومات التابع لمكتب المباحث الاتحادي

(1) Donald sanders and stanley Brikin,Computer and Management in A Changing Society McGraw-Hill Book Co.New York,1980,p.421.

يساعد الجهات المسئولة عن تطبيق الأمن ضمن حدود قضائية جغرافية محددة وذلك ليتكيف مع النشاطات المتزايدة للمجرمين الرحالة، فان بعض الناس المهتمين بهذا الموضوع يعتقدون بأن ذلك العمل هو انتهاك لحقوق خصوصية الفرد. فعلى سبيل المثال، فقد بدأت الإدارة المساعدة لتعزيز القانون (LEAA) بعد عدة سنوات مشروع (Search) وهو مشروع التحليل والاسترجاع الالكتروني للتاريخ الجنائي، وهو مشروع بلغت تكلفته سبعة ملايين دولار أمريكي وذلك لإنشاء شبكة حاسب آلي على مستوى الولايات المتحدة للأجهزة التي تعمل على تعزيز النظام على المستوى الفدرالي والمحلي وعلى مستوى الولاية من أجل تبادل المعلومات عن التاريخ الجنائي [1].

الهدف والمبادئ الأساسية للحماية القانونية:

إن أجهزة الحاسب الآلي قابلة لأن يتم استخدامها لأعمال غير مشروعة، وإذا ما استخدمت بسوء نية. ويتم توجيه القانون لتوفير العديد من المجالات الأمنية ويشمل ذلك عدم حدوث ومنع الإصابات والكشف والانتهاكات ويعمل كذلك على إصلاح الضرر. والقانون نفسه يمر بتغييرات، ولا يمكن أن نتنبأ بالنتائج إذا ما تم تطبيق القانون بشكل متسرع في مجالات تشمل تقنية الحاسب الآلي، ونتيجة لقابلية الحاسب الآلي للاختراق والخسائر الكبيرة فانه يجب تطبيق إجراءات أمن الحاسب الآلي واستمرارها. وبدون هذه الإجراءات فإن الحماية القانونية تكاد تكون لا معنى لها.

---

(1) Ibid,p.422.

ويجب أن ننظر إلى القانون في مجال حماية وأمن الحاسب الآلي كوسيلة لزيادة درجة الحماية وتوفير التقويم القانوني للمخالفات أو المخالفات المحتملة. إن اختراق حماية الحاسب الآلي يعتبر مخالفة جنائية يعاقب عليها القانون لذا فإنه يجب أن نأخذ النواحي القانونية بعين الاعتبار لتأكيد ما يلي[1]:

١ ـ الأعمال الممنوعة بشكل دقيق وكذلك الإجراءات والأنظمة التي يجب اتخاذها لمنع تكرار مثل هذه الاعمال.

٢ ـ المتطلبات القانونية والنظامية لاثبات ارتكاب تلك الأعمال والإجراءات والأنظمة التي يجب تطبيقها واتباعها للحفاظ على مثل هذه الأنواع من الأدلة.

٣ ـ الإجراءات الواجب اتباعها في التحقيق بالقيام بعمل ممنوع وتشجيع المساعدة في محاكمة المخالفين.

٤ ـ العقوبات الواجب تطبيقها والتأثير العميق المحتمل لمنع هذه المخالفات الأمنية.

وعلى أية حال، فإن المشكلة الرئيسية في تطبيق النظام والقانون بالنسبة لمجال الحاسب الآلي هو فشل القوانين في مسايرة التقدم السريع في مجال الاختراعات والتجديدات في هذا المجال. ان هذه القوانين ترتبط بشكل عام بالكثير من مخاطر النظام. وبفحص القوانين يتبين لنا الأعمال الممنوعة والاصلاح أو العقوبات في حالة المخالفة. ان الناس الذين يعملون في مجال أمن الحاسب الآلي يجب أن يكون لديهم وعي أمني وذلك لتجنب المخالفات الجنائية ومواجهة الاحتياجات بعناية لكي لا يتعرضوا لمسئولية مدنية، ولا

(1) Clarles Wood, William Cresson and W.Banks, Computer Security A Wilay Interscience Pub.,New York.1987,p.134.

يهدف هذا التحليل لاعطاء رأي قانوني لأي مشكلة محددة بل هو بيان عام عن النواحي القانونية المعنية لأمن الحاسب الآلي .

إن التشريعات القضائية المتنوعة التي تنطبق على أمن الحاسب الآلي يجب النظر اليها لكي تحدد ما هي النشاطات الممنوعة وذلك من أجل توضيح وتأكيد نطاق الحماية القانونية . ولهذا فانه يجب ان يتم التركيز بشكل كبير على عدم استخدام الحاسب الآلي دون تصريح أو عمل سجلات مزورة أو اتلاف المعلومات أو سرقة النقود أو ممتلكات أخرى حيث أن هذه تؤثر على العمل الخاص والعمل الحكومي . إن الإعمال المحددة المتعلقة بالحاسب الآلي والممنوعة بشكل عام عندما تكون غير شرعية تشمل الآتي [1] :

١ ـ الدخول إلى الحاسب الآلي .

٢ ـ الدخول إلى المعلومات أو البرامج .

٣ ـ استخدام الحاسب الآلي .

٤ ـ استخدام المعلومات أو البرامج .

٥ ـ نسخ المعلومات أو البرامج .

٦ ـ نشر المعلومات أو البرامج .

٧ ـ الحصول على معلومات سرية مثل بطاقات الأئتمان .

٨ ـ تعديل أو تغيير المعلومات أو البرامج .

٩ ـ ادخال معلومات مزورة في ملفات الأئتمان أو السجلات العامة على سبيل المثال .

١٠ ـ وقف أو مقاطعة تشغيل الحاسب الآلي .

---

(1) Ibid,p.135

١١ ـ وقف عملية حكومية أو خدمات عامة .
١٢ ـ عدم السماح للمستخدمين المرخصين باستعمال الحاسب الآلي .
١٣ ـ أخذ البيانات أو البرامج .
١٤ ـ اتلاف البيانات أو البرامج .
١٥ ـ إنشاء أو تعديل آلات مالية أو تحويل النقد بالنظام الالكتروني .
١٦ ـ استخدام أو نشر كلمة السر .
١٧ ـ اختراق النظام الأمني للحاسب الآلي .
١٨ ـ اتلاف الحاسب الآلي .
١٩ ـ أخذ الحاسب الآلي .
٢٠ ـ تدمير الحاسب الآلي .
٢١ ـ تعديل معدات أو مستلزمات الحاسب الآلي .
٢٢ ـ أخذ معدات أو مستلزمات الحاسب الآلي .
٢٣ ـ تدمير معدات أو مستلزمات الحاسب الآلي .
٢٤ ـ تصميم أو تنفيذ برنامج أو خطة للتزوير .
٢٥ ـ الحصول أو السيطرة على النقود أو الممتلكات أو الخدمات بطريقة مزورة .

إن سهولة ارتكاب الجرائم عن طريق الحاسب الآلي والخسائر الفادحة التي تترتب عليها هي من القوى الدافعة لانشاء علاج قانوني لها . إن مثال شركة التأمين للتمويل (EFIC) هي من الأمثلة البارزة لعملية التزوير بعدة ملايين من الدولارات باستخدام الحاسب الآلي عن طريق تصميم خطة تعتمد على إنشاء عدد كبير جداً من بوالص التأمين المزورة . ومن الأمثلة

الأخرى البارزة هي نشاطات عصابة الملواكي رقم ٤١٤ وهم مجموعة من الشباب المأجورين في سن الراهقة، والذين استطاعوا الدخول إلى العديد من أجهزة الحاسب الآلي الخاصة والحكومية التي يفترض أن تكون آمنة ضد الاختراق. وعلى شكل سيناريو حقيقي من فلم «العاب الحرب» حيث قاموا بشكل تصويري بعرض وتوضيح مدى سهولة الدخول إلى الحاسب الآلي ومدى خطورة سوء استخدامه.

إن ارتكاب عمل خاطئ دون سوء قصد حيثما كانت النية عنصراً اساسياً في الجريمة لا يعتبر مخالفة للقانون، ففي الجرائم التقليدية فان عنصر النية أي الحالة الذهنية للشخص الذي يرتكب العمل قد يكون من الصعب اثباتها بالنسبة للعمل بسوء قصد. أما عند التعامل مع معدات الكترونية مثل الحاسب الآلي فإن الأمثلة المتعلقة بالعمل المادي والدليل المادي قد تشكل نوعاً من الاعاقة حيث انه يصعب اثبات وجود دليل مادي. أن صعوبة اثبات عناصر الجريمة ضمن التشريعات والقوانين الجنائية التقليدية أدى إلى ضرورة تشريع قوانين محددة لنشاطات الحاسب الآلي. ونظراً لصعوبة فهم مبادئ الحاسب الآلي فانه من الصعب على القضاء والمشرعين اصدار حكم في قضايا الحاسب الآلي وقد لا يتوصلون إلى قرار ناجح.

وفي التحليل النهائي فان مدى فعالية القوانين الموجهة ضد جرائم الحاسب الآلي يجب قياسها بمدى نجاحها في مقاضاة ومنع مثل هذه الجرائم. ان الأنظمة القانونية تقوم حالياً بالتغير فيما يتعلق بالسياسات الجديدة والقوانين الخاصة بالحاسب الآلي وذلك لسد النقص في القوانين القائمة حالياً.

الجزء الثالث : المفاهيم الأمنية والأهداف والمسئوليات

الحاجة إلى أمن المعلومات الجنائية:

هناك سببان رئيسان لحماية المعلومات الجنائية . السبب الأول مبني على الحفاظ على هذه المعلومات الهامة وذات الصفة المميزة للمنشأة . أما السبب الثاني فيعتمد على حماية هذه المعلومات ذات الحساسية الأمنية والسرية .

الشكل رقم (١) يبين المخاطر التي تم تصنيفها من قبل شركة أي بي أم (IBM) هذا الشكل يتطرق إلى المخاطر الستة للمعلومات والتي اشتملت على التعديل، الانشاء سواء بقصد أم بغير قصد، والتدمير [١] .

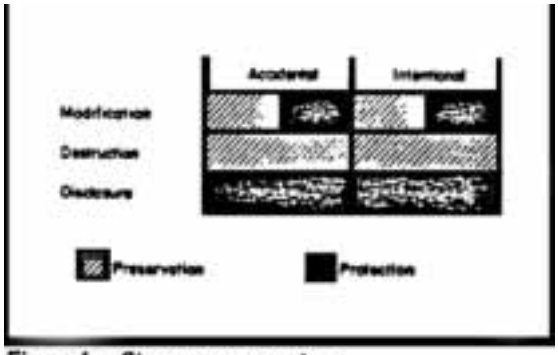

Figure 1. Six exposures to data

(1) Richard Koeing “Planning for an Information Programme” Information Age, Butterworth Co.Pub.,1984, p.145-146.

لذا فلو اعتبر الانشاد بقصد أو بغير قصد فإنه يمكن القول أن الانشاد يصبح شأناً ذو طابع الحماية ولا علاقة له بالحاجة إلى الحفاظ على المعلومات. ولكن عندما يكون هناك تخريب لهذه المعلومات الأمنية الجنائية فإن ذلك يكون ذو علاقة بالحفظ لهذه المعلومات. أما التعديل في المعلومات المخزنة فإن الأمر ينطوي على الاثنين معاً، وهما الحماية والحفظ، أن اهمية الحماية لهذه المعلومات تنبع من وتعتمد على منع أية محاولة مقصودة وغير مقصودة لها بتعديل المعلومات وذلك لاغراض شخصية أما الحفاظ على هذه المعلومات فيعني بالأخطاء أو التعديل المقصود مما يجعل هذه المعلومات تفقد طابعها الأمني والسري وتصبح عديمة الفائدة للمستفيدين [1].

الأهداف الأمنية والمسؤوليات

إن الهدف الرئيس الأول لأمن المعلومات هو الحفاظ على استمرارية تدفق هذه المعلومات على المستفيد. أما الهدف الثاني فهو حماية المعلومات الحساسة للمنشأة سواء أكانت ملكاً لها أو تحت سيطرتها.

لقد دار ولا يزال الحديث يدور بين بعض المسئولين في مراكز المعلومات الأمنية حول ما إذا لو حدث توقف للنظام لفترة طويلة أو تعرض المعلومات المخزنة للتلف. وهذا الحديث للأسف لا يدار بطريقة مباشرة وذلك من أجل تفادي إثارة القلق لدى المسؤولين في الإدارات العليا. بل أن البعض يتجنب الخوض في هذا الحديث.

إن مسئولية أمن المعلومات والتخطيط الوقائي موضوع مهمل إلى حد

---

(١) المرجع السابق، ص١٤٦.

كبير والسبب في ذلك يرجع إلى أن بعض المسئولين لا يجدون صعوبة في إقناع أنفسهم بأنه لن تحدث كارثة . لكن يمكن اعتبار ذلك الاقتناع شيئاً جانبياً لأن المسئولية تكمن في الحفاظ على استمرارية النظام والتأكد من عدم تعرض المعلومات الأمنية لأية تخريب . لذا فإن عدم الاهتمام بذلك يعتبر تقصيراً كبيراً من قبل هؤلاء المسؤولين في الوفاء بمسئولياتهم وتحملها بغض النظر عن وجهة نظرهم .

حراجة الموقف

إن تقدير حراجة الموقف ذو أهمية كبيرة ذلك أن هذا التقدير يعتبر المفتاح الرئيسي لمعرفة التقديرات المالية للنظام الاحتياطي وإعادة القدرة التشغيلية للنظام الاحتياطي .

هناك بعض الاختيارات التي يلزم النظر فيها بعناية والتي تشتمل على الآتي [1] :

أولاً : هل يشمل الاحتياط نظام كامل ببرامجه في موقع آخر .

ثانياً : هل لدى النظام إجراءات يدوية ومتكاملة لاستخدامها في حالة انهيار النظام الآلي وهل هذه الإجراءات ملك للمنشأة .

ثالثاً : هل بالإمكان استخدام أجزاء من النظام اليدوي والآلي معاً لانعاش النظام وإجراءاته للمستفيدين ولتعريف حراجة الموقف فان معظم المنشآت قد اتفقت على التصنيف التالي [2] :

١ ـ حيوي : يعتمد عليه بقاء المنشأة .

---

(١) المرجع السابق، ص١٤٧ .

(٢) المرجع السابق، ص١٤٧ .

٢ـ حرج : يعتمد عليه بقاء المشأة بأهدافها .

٣ـ عام : يشمل جميع الأنظمة المعمول بها .

السرية

في مجال حماية المعلومات السرية فان الإجراءات تنصب على عناصر السجلات أو البيانات وتقدير مستوى السرية لذلك .

لذا فإن مستوى السرية يصبح عكس ما ذكر في حراجة الموقف للنظام (من اعلى إلى اسفل) . بمعنى آخر أن مستوى السرية للمعلومات والحفاظ عليها يبدأ من البيانات والتي يلزم النظر اليها لمعرفة مستوى سريتها . ان الملفات والبرامج التي تستخدم للوصول إلى هذه الملفات تصبح ذات اهمية قصوى في مجال أمن المعلومات .

لذا يمكن اعتبار أن السرية تبدأ من أسفل فصاعداً وأن الحكم على ذلك يبدأ من أسفل الهيكل التنظيمي للمنشأة[١] .

هناك العديد من التصنيفات التي تم التداول بها لتحديد مستوى السرية والتي من ضمنها على سبيل المثال :

١ ـ سري .

٢ ـ سري جداً .

٣ـ سري جداً للغاية . . . الخ .

---

(١) المرجع السابق، ص١٤٧ .

تصنيف المسؤولية

إن الراعي الأساسي للمنشأة والمعلومات التي تملكها أو تسيطر عليها هو الوحيد الذي يمكن أن يقرر مستوى السرية لهذه المعلومات. وللتشبيه في هذا الصدد، فإن الراعي أو المالك للنظام الآلي هو الوحيد الذي يمكن أن يقرر مستوى حراجة الموقف للنظام والمعلومات المخزنة بداخله. إذاً فإنه من المنطق القول بأن المسئولية الأولى لتحديد هذه المسئوليات يقع على راعي المنشأة، ذلك أنه هو الوحيد الذي يتحمل جميع تبعات هذه المسئولية في حماية المعلومات والحفاظ عليها وسريتها [1].

التوصيـــات

يمكننا القول أن المخاطر المادية وغير المادية تحدث بين الحين والآخر لبعض مراكز المعلومات وما تحتويه من معلومات أمنية وحساسة والتي من ضمنها المعلومات الجنائية. والسبب الرئيسي يعود في ذلك أن هنالك العديد من البرامج المتطورة جداً مصممة خصيصاً للقيام بالاعمال التخريبية. هذه البرامج لديها القدرة على استغلال نقاط الضعف في برامج الحاسب الآلي وأنظمته. لقد صممت هذه البرامج بطرق يصعب حتى على ذوي الاختصاص كشفها ومن ثم الغائها وحتى الوقاية منها ذلك أنها كتبت بواسطة أناس محترفين أوجدوا داخلها العديد من الحيل لتفادي الكشف عنها من قبل العاملين على الحاسب الآلي.

---

(١) المرجع السابق، ص١٤٨.

إن الهدف الرئيسي الأول لأمن المعلومات هو الحفاظ على استمرارية النظام وتوفره للمستفيدين، أما الهدف الثاني فهو حماية وحفظ المعلومات الحساسة والسرية للمنشأة سواء أكانت ملكاً لها أو تحت سيطرتها.

١ ـ عدم استخدام شبكات الحاسب الآلي المفتوحة لتداول المعلومات الأمنية.

٢ ـ التأكد من أن الكوادر البشرية العاملة على النظام تمتلك صفات النزاهة والوطنية وتحصينها من الإغراءات المادية.

٣ ـ إجراء مسح أمني شامل لجميع مكونات النظام للتأكد من خلوه من التغيرات.

٤ ـ ضرورة سن القوانين الجنائية اللازمة من تسرب وإفشاء المعلومات وتخريبها وسرقتها.

المراجع

المراجـــــع

Sanders, Donald, Computer and Management in A Changing Society, McGraw-Hill Book Co.,New York,1980.

Squires, Tony, Computer Security:The Personnel Aspect,NCC Publications,Manshester,England,1980.

Koeing,Richard “Planning for an Integrated Information Programmeس Information Age,Butteworth Co.Pub.,1984.

Wood,Charles Computer Security, A Wilay Interscience Pub., New York,1987.