ورقة مقدمة لمؤتمر حرية تداول المعلومات فى مصر
"المعلومات حق لكل مواطن"
بعنوان: الأمن المعلوماتي: مابين تحديات الداخل والخارج

إعداد

هشام بشير

باحث دكتوارة

فبراير ٢٠٠٨

المحتويات

الأمـن المعلوماتـي ٢

مفهوم أمن المعلومات ٤

القصور التشريعي في مجال أمن المعلومات ٥

أهم أدوات (وسائل) الحماية ٧

دور الجامعات والمعاهد العلمية في تطوير آلية التعامل مع النظم المعلوماتية:.....١١

حرج المؤسسات الكبيرة ١١

اقتراحات في هذا المجال ١٢

خاتمة ١٣

الأمـن المعلوماتى

مما لاشك فيه أن التطور العلمي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الكمبيـوتر في أغلب الاحتياجات التقنية والمعلوماتيـة. فمنـذ الحـرب البـاردة والـصراع المعلومـاتي والتجسـسى بـين الدولتين العظميين آنذاك على أشده، ومع بروز مناطق جديدة للصراع في العالم وتغـير الطبيعـة المعلوماتيـة للأنظمة والدول، أصبح الاعتماد كليا على الحاسوب الآلي وعن طريقه أصبح الاختراق من اجـل الحـصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية وهنـا تـبرز أهميـة الأمـن المعلومـاتي للـدول وللأفراد والمؤسسات[1].

وبعبارة أخرى قد أدت ثورة المعلومات إلى أنماط جديـدة مـن التحـديات والجـرائم منهـا لـصوص الحاسب الذين يدخلون إلى أنظمة الحاسب وقواعد المعلومات ويسرقونها أو يعبثون بها والجرائم الحديثـة التي تخترق الحماية الأمنية في النظم القانونية، ومـن الجـدير بالـذكر أن الجانـب المظلـم للمعلومـات هـو استثمارها في جوانب مهددة للأمن البشري ولذا فان حرب المعلومات، حيث تستخدم المعلومـات كـأداة في الهجوم المعلوماتي على الخصم من التعدي وتـوفير ميـزات لنـا في الـسيطرة والاتـصال والتوجيـه. كمـا أن المعلومات مصدر من مصادر تهديد امني لأنها تمثل رابطا تعتمد عليها العديـد مـن القطاعـات ممـا يـسهل الأضرار بالطرف المقابل أو الاستفادة منه دون عناء.

وتشمل حرب المعلومات قوة مضادة وقيمة مضادة في الحرب بشكل كبير وتوصـيل المعلومـات مـن خلال النظم العسكرية (القيادة، السيطرة، الاتصالات) عملية هامة تساعد على التوجيه الدقيق للـضربات وتدمير البناء المعلوماتي يؤدي إلى هزيمة سريعة لكل دولة، وتهدد المعلومات الأمن الوطني ذلـك إن البنـاء التحتي الاجتماعي والاقتصادي والعسكري والاتصالات كبني عليهـا المعلومـات بنـاء تحـتي ترتكـز عليـه النظم السياسية والاجتماعية والتربوية والإدارية، مما يجعلها ذات قيمة عالية من طرف قراصنة الحاسـب والعابثين، وقد ولدت المعلومات نموذجا جديدا في الأمن، وفي مجتمع المعلومات شـكلت المعلومـات البنيـة التحتية للمجموعات والمؤسسات ومع ازدياد استعمال تقنيات المعلومات زادت احتمالية التعرض للفشل أو التخريب مما يهدد الأمن الوطني للمجتمع والدولة.

(1) http://www.uaeec.com/news.php?action=show&id=3139

ومن الجدير بالذكر أنه قد حدث في عام ٢٠٠٥ أنه قد تم إيقاف شاب مغربي بنـاء علـى تنـسيق دولي في إطار محاربة الإجرام المعلوماتي، وقد اتهم الشاب بتخريب شبكات معلومـات أمريكيـة والتواطـؤ مع شبكات تزوير البطاقات البنكية، حيث تمكّن من الدخول إلى ١٢٠٠ مـوزع معلومـاتي ووُجـد بحوزتـه ٦٠ ألف ملف معلوماتي آخر دمرها بعد اكتشاف أمـره، هـذه القـضية هـي واحـدة مـن عـشرات الجـرائم اليومية التي تتعـرض لهـا شـبكات المعلومـات في العـالم، والناتجـة عـن الطفـرة الهائلـة في مجـال تقنيـة المعلومات[٢].

تنامي ظاهرة العدوان على البيئة المعلوماتية[٣]:

يشكّل العدوان على البيئة المعلوماتية الوجه القبيح للتقنية الحديثة، فالجرائم المتحققـة عـن هـذا العدوان تتميز عن الجرائم العادية بسرعتها الفائقة وتأثيرهـا المـدمّر، وقـدرة مرتكبيهـا علـى الإفـلات مـن الملاحقة والعقاب في ظل افتقاد كثير من الدول أنظمة قانونية قادرة على التعامل مع هذا العدوان والجـرائم الناجمة عنه.

وتشير الإحصاءات الدولية إلى أن هنـاك أكثـر مـن مليـاري شـخص مـستخدم لأجهـزة الحاسـب الآلي، فضلاً عن وجود أكثر من (١٣) مليار صـفحة علـى شـبكة المعلومـات الدوليـة (الإنترنـت)، ونحـو (٣٠٠) مليون موقع عليها. وهكذا اتسعت البيئة المعلوماتية لتصبح ميداناً فسيحاً للعدوان عليها، ولتـشكل تحدياً رهيباً لمختلف الأجهزة في مواجهة هذا العدوان وما ينجم عنه من جرائم.

وتشير إحدى الدراسات إلى أن (٢٤٪ إلى ٤٢٪) مـن المنظمـات في القطـاعين الحكـومي والخـاص كانت ضحيّة لجرائم مرتبطة بالتقنية الحاسوبية، وأن (١٤٥ إلى ٧٣٠) مليـون دولار سـنوياً خـسارة (٧٢) شركة بسبب جرائم الحاسب الآلي، وبيّنت دراسة للأمم المتحدة عـن مخـاطر الحاسـب الآلـي أن (٧٣٪) من الجرائم داخلي، (٢٣٪) منها يرجع إلى مصادر خارجية، وقدّرت الخسائر الاقتـصادية لهـذه الجـرائم عام (١٩٩٣م) بنحو (٢) مليار دولار؛ وفي دراسة عن حـالات الاخـتراق كوجـه مـن أوجـه العـدوان علـى أجهزة الحكومة الأمريكية لعام ١٩٩٥م، وجد أن هناك (٢٥٠,٠٠٠) حالة اختراق، ٦٤٪ منهـا ناجحـة، وأن (١٪) إلى (٤٪) منها تم اكتشافه، وأعلن فقط عن (١٪) من هذه الاختراقات.

(2) http://www.alarabiya.net/programs/2006/01/15/20304.html

(3) http://www.kkmaq.gov.sa/detail.asp?InNewsItemID=164260&InTemplateKey=print

أما في المملكة العربية السعودية،فإن قطاع تقنية المعلومـات يـشهد نمـواً متزايـداً، وخـصوصاً مـع دخول شبكة المعلومات الدولية، مما عرّض الكثير من النظم والشبكات التي كانت معزولة في الماضي لخطر الاختراقات الخارجية، ومكّن كثيراً من المستخدمين من التعرُّف على الـبرامج الـتي تـساعد علـى اخـتراق الأنظمة الحاسوبية والحصول عليها بسهولة، وذلك يضع عبئاً أكبر على مشغلي الأنظمة لمتابعة المعلومـات الأمنية، وطرق الاختراقات المستحدثة لحماية أنظمة التشغيل الخاصة بهم، وحيث إن الخـبرات لازالـت محدودة نسبياً، فيما يتعلق بأمن المعلومات، ولأنه لا يوجد نظـام أمـني رادع لهـؤلاء المخترقـين، فـسوف تزداد المشكلة سوءاً مع ازدياد الاعتماد على الحاسب وشبكة المعلومات الدولية. ومع قرب الانضمام لمنظمة التجارة العالمية تزداد الأهمية الاقتصادية لأنظمة المعلومات والحاسبات، وخـصوصاً مـع الانتـشار الواسـع للتجارة الإلكترونية، مما يستلزم المزيد من العناية بقضايا أمن المعلومات.

مفهوم أمن المعلومات:

أمن المعلومات مصطلح تم استخدامه قديماً، فهو سابق لـولادة وسـائل تكنولوجيـا المعلومـات، إلاّ أنه وجد استخدامه الشائع والفعلي في نطاق أنـشطة معالجـة ونقـل البيانـات بواسـطة وسـائل الحواسـب والاتصال، فمع شيوع الوسائل التقنيـة لمعالجـة وخـزن البيانـات وتـداولها والتفاعـل معهـا عـبر شـبكات المعلومات وتحديداً الإنترنت احتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل وربما أمْسَت أحد الهواجس الـتي تـؤرق مختلـف الجهـات، **فـأمن المعلومات هو**: الطرق والوسائل المعتمدة للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من الـسرقة والتشويه والابتزاز والتلف والضياع والتزويـر والاسـتخدام غـير المـرخّص وغـير القـانوني، وهـو الإحـساس الفعلي أو الافتراضي بعدم وجود أي شكل من أشكال التهديدات لبُنى المؤسسات المعلوماتية، وإتباع كافـة الوسائل والسبل للتأهُّب والعمل الفعلي لمواجهتها٤.

وهناك من يعرِّف أمن المعلومات من زوايا متعددة٥:

- فمن الزاوية الأكاديمية يعتبر أمن المعلومات: هو العلم الـذي يبحـث في نظريـات واسـتراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من كل أنشطة الاعتداء عليها.

(4) محمد منير الجنبيهي، ممدوح محمد الجنبيهي، أمن المعلومات الإلكترونية، ط ١، دارالفكر الجامعي، الإسكندرية، ٢٠٠٥م، ص ١٤.

(٥) http://www.kkmaq.gov.sa/detail.asp?InNewsItemID=164260&InTemplateKey=print

- ومن الزاوية التقنية: هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- وأخيراً يعتبر أمن المعلومات من الزاوية القانونية: هو محل دراسات وتدابير حماية سريّة وسلامة محتوى وتوفّر المعلومات ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها.

ومن الجدير بالذكر أن مصطلح أمن المعلومات يرتبط بمفهوم الأمن المعلوماتي على المستوى الوطني الذي يعني: الإحساس المجتمعي والفعلي والتخيلي بعدم وجود أو تأثير التهديدات الطبيعية أو الافتراضية لبنى المجتمع المعلوماتية وبخاصة الحسّاسة منها في جوانبها المختلفة، سواء أكان مصدرها داخلياً أو خارجياً، وتستدعي التأهُّب أو الفعل الجماعي أو التأهُب الرسمي لمواجهتها[٦].

القصور التشريعي في مجال أمن المعلومات:

يعتبر القصور التقني في مجال أمن المعلومات ليس هو القصور الوحيد، ولكن هناك أيضا قصور تشريعي وتنظيمي من قبل السلطات الأمنية، فالمجرم الذي يسرق أسورة من الذهب أو حفنة من النقود يعامل بأسلوب مختلف عمن يسرق معلومة أو يخترق منظومة أمنية معلوماتية، وفي الحقيقة فإن القصور التشريعي متواجد في جميع أنحاء العالم ليس العالم العربي فقط، ومع ذلك فإن بعض البلدان العربية توجد لديها قوانين تشريعية صارمة جداً في التعامل مع الجرائم المعلوماتية، جرائم لها علاقة بسرقة معلومات خاصة بالكروت البنكية، معلومات لها علاقة بوضع صور مخلة للآداب على مواقع، علاقة شخصيات تم للأسف تصويرها ودمج صورها في صور خارجة، وجدير بالذكر أن الولايات المتحدة الأمريكية تعتبر من الدول التي يمكن القول أنها تتربع على رأس الدول التي توجد فيها تشريعات وقوانين صارمة جدا في مجال أمن المعلومات، ومما لا شك فيه أن ذلك راجعا في المقام الأول لدراية القضاء الأمريكي في التعامل مع الأمور ذات العلاقة بتنقية المعلومات وانتهاكات أمن المعلومات في المنشآت، وتعتبر ولاية كاليفورنيا من أكثر الولايات الأمريكية تقدما في هذا المجال[٧].

(6)http://www.kkmaq.gov.sa/detail.asp?InNewsItemID=164260&InTemplateKey=print

(7) http://www.alarabiya.net/programs/2006/01/15/20304.html

التحديات الأمنية[٨]:

لقد أدت ثورة المعلومات إلى ظهور أنماط جديدة من التحـديات الأمنيـة، ولقـد ظهـرت تحـديات جديدة للأمن بمفهومه التقليدي، وهذه التحديات تتعلق بالاسـتعدادات اللازمـة للتعامـل مـع المـستجدات والمهددات الأمنية والأمن في المجتمع المعلوماتي ما هو إلا النتيجة طبيعية لتطور بـني المجتمـع وانتقالهـا من مجتمع صناعي إلى مجتمع معلوماتي الذي فرض العديد من التحديات على المستوى العالمي والوطني.

أولاً: على المستوى العالمي:

- التحديات السياسية: الحاجة إلى المعلومات قوية . والقوة هذه ذات تـأثير في القـرار الـسياسي في أي مجتمع وهو ما يزيد حاجة السياسي لهذا النوع من القوة.
- التحديات الاقتـصادية: إن نقـص المـوارد الاقتـصادية يعـني الحاجـة إلى المعلومـات الـتي تطـور الاقتصاديات وحاجتها المستقبلية من اجل فرض المنافسة والسيطرة.
- التحديات التقنية: تتمثـل في حاجـة الـدول والمجتمعـات إلى المعـدات والبرمجيـات والى تطـوير الإمكانيات الدالة في هذا المجال .
- التحدي الأمني: ويتمثل في ضعف البناء التحتي المعلوماتي وانكـشافه للتعـديات ووجـود ثغـرات أمنية كبيرة إن تعطيل هذا البناء أو تخريبه أو التعدي يؤدي إلى ظهور اضطراب كبير في عمليات التواصل في مجالات المال والأعمال والعلاقات العامة بين الأفراد .

ثانياً: أهم التحديات الداخلية:

- تحدي التنمية والديمقراطية وحقوق الإنسان: فالفقر والأميـة والجريمـة والمـشكلات الاجتماعيـة المتنوعة والفساد الإداري والسياسي تحد من فرص التطور والانتقال إلى مجتمع المعلومات.

(8) موسوعة الويكيبديا

- التحدي البشري ونقص الكفاءات : نقص الكفاءات علـى المـستوى القيـدة والتقنيـة بـسبب عـدم التأهيل وهجرة العقول .
- التحدي الثقافي: لابد من تماشي الثقافة مع بني مجتمع المعلومات .
- التحديات التربوية : النظام التربوي أكبر تحد في نقل المجتمعات إلى مجتمع المعلومات، فنظـام التعليم لابد أن يبنى على أسس المعلوماتية وتحويله من الاعتماد على الـنظم التقليديـة إلى تكـوين بناء معلوماتي تحتي متكامل يشمل مهارات للتدريس والمنهاج .
- التحدي الأمني: الأمن أساس أي تنمية مستديمة. وعمليات الـتغير الاجتمـاعي تتطلـب اسـتقرار امنيا وأثناء عمليات التحول الاجتماعي لمجتمع المعلومات .

ثالثاً: المهددات المستقبلية الفضائية:

- التهديـد بالاضـطراب في تـدفق الاتـصالات والتحـويلات الماليـة والحمـلات المعلوماتيـة الهامـة. ومحطات الطاقـة والمناقـصات الـسياسية والاضـطرابات في زمـن الحـرب قـد يـؤدي إلى الهزيمـة والخسارة .
- التهديـد باسـتغلال المعلومـات الحـساسة والملكيـة والمعلومـات الـسرية .إن سـرقة المعلومـات أو الاحتيال بها أو الجرائم الفضائية لها آثار سلبية على المستوى الفردي وعلـى المـستوى المؤسـسي وعلى المستوى الوطني .
- التهديد بانتقاء المعلومات لأغراض سياسية أو اقتصادية أو عسكرية واستغلالها أو تدميرها .
- التهديد بتدمير المعلومات : تدمير مكونات البناء المعلوماتي التحتي الحساس .ولهذا نتائج سلبية كبيرة على الاقتصاد والأمن الوطني.

أهم أدوات (وسائل) الحماية:

يتم وضع كلمة سر على جهاز الحاسب الشخصي للولوج إلى الملفات الهامة أو حتى للنظام كلـه، ولا تُعطى هذه الكلمة لأحد، ويوضع برنامج أو أكثر لمقاومة الفيروسات الإلكترونية الـضارة، ويـتم مراعـاة الإجراءات الخاصة بحماية الدخول إلى شبكة الإنترنت والتأكُّـد مـن مـصدر البريـد الإلكترونـي. وإذا كـان الحاسب خاصاً بدائرة أو منشأة ويضم بيانات هامة مصنفة على أنها سـريّة، كـان لزامـاً زيـادة إجـراءات الأمن، فمثلاً يُضاف للنظام جدران نارية تحدّ من دخول أشخاص من الخارج، وتمنع الاعتداءات المنظمـة

التي قد يتعرّض لها النظام أو الموقع المعلوماتي، وإذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الإفشاء، تكون تقنيات التشفير مطلوبة بالقدر المناسب. وفي كل الأحوال لابد من أن تنطلق إجراءات الحماية من احتياجات الحماية الملائمة، لأنها إذا زادت عن حدها أصبحت ذات أثر سلبي على الأداء، إذ يصبح النظام بطيئاً أو غير فاعل في أداء مهامه الطبيعية، كما أن نقص هذه الإجراءات عن الحد المطلوب يزيد نقاط الضعف، ويصبح النظام أكثر عرضة للاختراق الداخلي والخارجي[٩].

ومن أهم وسائل الحماية، والأخطاء الواجب تلافيها:

- التشفير.
- حواجز العبور (جدار النار).
- تلافي الأخطاء.
- اختيار كلمة مرور سيئة.
- الثرثرة.
- ترك الحاسب المحمول.
- تجاهل سياسة أمن المعلومات.
- الفشل في مراقبة الموظفين.

قبل الشروع في شرح وسائل الحماية والأخطاء الذي يجب تلافيها نود أن نعرف الاختراق، فيعرف الاختراق بالقدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف وبطبيعة الحال هي سمة سيئة يتسم بها المخترق لقدرته على دخول أجهزة الآخرين عنوة ودون رغبة منهم وحتى دون علم منهم بغض النظر عن الأضرار الجسيمة التي قد يحدثها سواء بأجهزتهم الشخصية أو بنفسياتهم عند سحبه ملفات وصور تخصهم وحدهم[١٠].

التشفير: هي عملية الحفاظ على سرية المعلومات (الثابت منها و المتحرك) باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول

(9)www.arablaw.org
http://www.kkmaq.gov.sa/detail.asp?InNewsItemID=164260&InTemplateKey=print
(10) http://www.uaeec.com/news.php?action=show&id=3139

لهم بذلك لا يستطيعون فهم أي شيء لأن ما يظهر لهم هو خليط من الرموز والأرقام و الحروف الغير مفهومة[١١].

كما أنه يمكن، تعريف التشفير بأنه عملية تغيير مظهر وشكل المعلومات لإخفاء معناها الحقيقي عن طريق تحويل شكل البيانات لكي تكون غير مفهومة لمن يحاول التلصُّص عليها، أو هي عملية تحويل النص المكتوب أو المفهوم والواضح للناس إلى رموز، وهو وسيلة لاستبدال أي مستند أو وثيقة مقروءة ومفهومة إلى شكل وضعية لا يمكن معرفة وفهم محتواها، لكونها تحوّلت من شكل حرفي مقروء إلى شكل مرمّز يمكن قراءته ولا يمكن فهمه، ويهدف التشفير للتغلُّب على معدات أمن المعلومات، مثل: الاطلاع على المعلومات المحظورة، وتأخير إيصال بعض الرسائل، وتغيير وتسوية محتويات الرسائل المتبادلة، وانتحال شخصية المستخدم الحقيقي، وإدخال رسائل زائفة ضمن الرسائل الحقيقية، وتغيير كلمة السر الخاصة بالمستفيدين وغير ذلك من المخاطر[١٢].

حواجز العبور (جدار النار): هذا الجدار في الواقع هو عبارة عن أسلوب لحماية ومراقبة البيانات والملفات والنظم الداخلية للمؤسسة أو الدائرة وشبكة الإنترنت، أو بين الشبكتين، وهذه الجدران تستخدم للحدّ من دخول المتطفلين والعابثين، أو بالأحرى منعهم من تسريب معلومات غير مرغوب فيها أو برمجيات سيئة. وفي الوقت نفسه تحمي المعلومات المهمة والأساسية المتعلقة بأهداف وعمل وإجراءات وخدمات وأنشطة المؤسسة، وذلك من خلال منع خروجها، فهي جدار سميك ومنظّم للحماية[١٣].

تلافي الأخطاء: يرتكب الموظفون أخطاءً فاحشة وساذجة، وتؤدي في الوقت نفسه إلى كوارث معلوماتية، ومن تلك الأخطاء[١٤]:

- **تعليق كلمات المرور:** فكثيراً ما يقوم المستخدمون بتدمير كل إجراءات أمن المعلومات بلصق كلمات المرور على مقدمة شاشة الحاسب، أو على سطح المكتب، بحيث يمكنهم رؤيتها

(11) http://shkoon.coolfreepage.com/amn/index.htm

(12) http://www.kkmaq.gov.sa/detail.asp?InNewsItemID=164260&InTemplateKey=print

(13) محمد محسن عمر، الإدارة والتقنية: شركاء في مواجهة عصر الإنترنت، ١٩٩٧م، ص ١٦٢ ١٦٤

(14) http://www.kkmaq.gov.sa/detail.asp?InNewsItemID=164260&InTemplateKey=print

بسهولة، هم وكل من حولهم، ثقة منهم فيهم أو لأي سبب آخر، وقد أثبتت دراسة حديثة أن ٢٠٪ من موظفي تكنولوجيا أمن المعلومات يفعلون ذلك.

- **ترك الجهاز مفتوحاً:** والحركة بعيداً عنه للحظات أو لمدة من الوقت، وهو ما يسهِّل مهمة السارق في حصوله على كلمة المرور، وبخاصة إذا كان خبيراً بما يفعل أو عليماً بما يريد.
- **فتح مرفقات البريد الإلكتروني:** فالبعض لا يكلّف نفسه عناء التفكير فيما ورد إليه من رسائل، فإذا كان البعض فوجئ، أو لم تكن لديه خبرة سابقة في كيفية انتشار الفيروس، فلماذا وقعوا في الخطأ نفسه بالنقر على مرفق رسالة البريد الإلكتروني.
- **اختيار كلمة مرور سيئة:** وهذا ما يخيف خبراء أمن المعلومات، حيث يمكن للمقربين التكهّن بهذه الكلمة التي ترتبط باسم الابن، أو فريق الكرة، وكلما طالت الكلمة وتعقدت كلما كان التكهُّن بها أصعب أو مستحيلاً، ولاختيار كلمة المرور قواعد يحسن أن تقوم المؤسسات بإتباعها.
- **الثرثرة:** كأن يجلس الشخص ويقول: لقد غيّرت كلمة المرور إلى كذا، أو أضفت كذا، أو حذفت كذا، ولا يدري أنه قد يكون هناك من يتلقف هذه المعلومة ويسهم مباشرة أو بطريق غير مباشرة في مخاطر جمّة.
- **ترك الحاسب المحمول:** فمن الواجب عدم تركه دون مراقبة، خصوصاً في الأماكن العامة، ولقد قالوا في ذلك: الحاسب المحمول شأنه شأن الهاتف المحمول، وكل شيء (منتج إلكترونياً) محمول خائن، يبغض صاحبه، ويحب سارقه.
- **تجاهل سياسة أمن المعلومات:** فمهما كانت هذه السياسة جيدة، فإن إهمالها يتساوى مع عدم وجودها، فهناك من العاملين من لا يقتنع بهذه القواعد، ويرى أن لديه الأسباب الوجيهة لإهمالها، فمثلاً قد يعطل بعضهم برامج الكشف عن الفيروسات، لأنها تبطِّئ من سرعة الجهاز.
- **الفشل في مراقبة الموظفين:** لأنهم أعلم بأوجه الضرر أكثر من غيرهم. البطء في المواكبة: فالجريمة بشكل عام، وجرائم المعلوماتية بشكل خاص في تطوّر مستمر، وهي في غالب الأحيان تسبق وسائل الأمن والحماية، لذا ينبغي تحديث وسائل وسياسات أمن المعلوماتية بشكل دائم.

دور الجامعات والمعاهد العلمية في تطوير آلية التعامل مع النظم المعلوماتية:

مما لا شك فيه أن المؤسسات التعليمية لها دور أساسي لأنها هي التي تعد الكوادر الأساس في مجال تقنية المعلومات، كما أنها هي التي تقوم بالتوعية العلمية عموماً لقطاعات كبيرة من أبناء المجتمع من خلال طلاب الجامعات والمؤسسات العلمية، وبالتالي فإن الكثير من جامعاتنا تحرص أن يكون هناك دراسات تتعلق ضمن مناهجها، وعلى سبيل المثال جامعة الملك سعود ضمن البرامج الماجستير هناك برامج متخصصة في أمن المعلومات، وضمن البرامج البكالوريوس أيضاً في كليات الحاسب يوجد مقررات في أمن المعلومات، دور الجامعات أيضاً علمية لا يقتصر على الناحية التعليمية هناك إذن جانب الأبحاث جانب التطوير في المجال، لذلك كثير من الجهات العلمية تحرص على أن يكون هناك مؤتمرات علمية في التخصص، ولا يخفى على أحد أن الجانب البحثي مهم أيضاً، لأن الكثير من المشاكل قد تتطلب نوع من الابتكار نوع من الاختراع لحل هذه المشاكل الأمنية المعلوماتية، فبالتالي البحث العلمي في هذا المجال يخدم أيضاً قطاع كبير مستقبلي في التطوير[١٥].

حرج المؤسسات الكبيرة:

قد نجد الكثير من المؤسسات الكبيرة عندما يحدث اختراق لأي نظام معلوماتي خاص بها فتجد حرجا كبيرا في الإفصاح عن تلك الاختراق ولكن كثيرا ما تقوم بإيعاز ذلك إلى الكثير من الأسباب الأخرى مثل انقطاع التيار الكهربائي أو حدوث خلل فني وغيرها من الأسباب الأخرى التي لا تمت بصلة إلى حدوث اختراق أمني، وهذا بالفعل أمرا طبيعيا إذ أن أي اختراق أمني ينتج عنه خسائر اقتصادية، فالمؤسسات المالية أكثر المؤسسات تأثراً بالجانب الاقتصادي، لأنه إذا فقدت الثقة في أسلوب الوصول للمؤسسة والاستفادة من خدماتها ستفقد عملائها، وبالتالي ستفقد مصدر كبير من مواردها[١٦].

(15) http://www.alarabiya.net/programs/2006/01/15/20304.html

(16) http://www.alarabiya.net/programs/2006/01/15/20304.html

اقتراحات في هذا المجال١٧:

- ضرورة تعيين مسئول متخصص في مجال أمن وسرية المعلومات يهتم بتقديم المعلومات الأمنية لكافة مراحل المشروع.
- نقترح ضرورة إجراء تقييم مستمر للتطبيقات للتأكد من توفر أعلى الدرجات للاحتياطات الأمنية.
- ضرورة الاهتمامات بكافة أنواع الأمن المعلوماتي المادي والمنطقي وتطبيق كافة الخطوات الضرورية في كل مرحلة من مراحل المشروع.
- ضرورة الاهتمام بعمل النسخ الاحتياطي اليومي والأسبوعي والشهري مع ضرورة حفظ وسائط التخزين في أماكن آمنة بعيدة عن مراكز المعلومات الوطنية.
- عدم إفشاء أية معلومات شخصية ما لم يتم الموافقة عليها من قبل الأطراف المعنية وهم الأشخاص المستفيدون والإدارة.
- ضرورة تنفيذ الندوات والدورات التدريبية المستمرة لكافة العاملين وذلك لإبقاء معلوماتهم حول المخاطر الأمنية حديثة وفي مواجهة أي مخاطر.
- ضرورة عمل خطط للطوارئ واختبار تلك الخطط في الظروف الاعتيادية.

(17) يحي بابعي ، الفساد الإداري وغياب الشفافية والأمن المعلوماتي تحديات في وجه الحكومة الإلكترونية،٢٠٠٦،ص ٧

http://www.al-jazirah.com.sa/digimag/07122003/agtes20.htm

خاتمة

لقد تحول التسلل الإلكتروني إلى هواية مسلية للمراهقين الأذكياء وفئات أخرى منها مافيا إلكترونية تحاول السيطرة على ساحات الاحتيال الإلكتروني، ويشمل التسلل البيانات الشخصية في أجهزة الكمبيوتر وإتلافها وسرقة كلمات المرور السرية وانتحال أسماء الأشخاص وتجاوزت ذلك إلى ضرب مواقع القطاعات الاقتصادية الهامة مثل السطو على المصارف، وسرقة أرقام البطاقات الائتمانية، والأرقام السرية، والمنشآت التجارية، واستهداف مواقع الحكومات، ورغم دخول تقنية الكمبيوتر متأخرة إلى المنطقة العربية إلا أن مثل هذه الجرائم كلفت خسائر بلغت نحو ٦٠٠ مليون دولار عام ٢٠٠٢ رغم التكتم الشديد على إعلانها من قبل الشركات والبنوك التي تتعرض لها، وتشير التوقعات إلى أن حجم الاستثمارات الموظفة في سوق أمن المعلومات والاتصالات العربية يفوق ٥٠٠ مليون دولار حتى عام ٢٠٠٨ مقارنة بحوالي ٢١ مليار دولار هي حجم الاستثمارات العالمية خلال نفس الفترة، وبالنظر إلى حجم الاستثمارات العربية في المجال خلال السنوات المقبلة فإن الحاجة إلى تأمين هذه الاستثمارات وحمايتها يستدعي البحث عن آليات لذلك من خلال منظومة وطنية عربية وضخ استثمارات كبيرة في مجال أمن المعلومات والاتصالات، لاسيما في ضوء البيانات والإحصاءات التي تشير إلى تنامي هذا القطاع الواعد في العديد من الدول العربية، في مقدمتها مصر والمملكة العربية السعودية والإمارات بنسب تتراوح ما بين ٢٠ و٣٠٪، ويحذر محللون من الإفراط في الاعتماد على استيراد نظم تأمين المعلومات الأجنبية خاصة بالنسبة للمؤسسات الإستراتيجية الحساسة، مؤكدين على أهمية مساندة وتدعيم شركة أمن المعلومات العربية لإنتاج نظم التأمين المعلوماتي.