قضايا أخلاقية ومهنية واجتماعية
(7)
أمـــن السايبر
Security in Cyberspace

مقدمة

يختلط مفهوم تأمين نظم الحاسوب كثيراً بمفهوم السلامة safety أو بمفهوم الخصوصية Privacy او السرية Confidentiality أو الصحة والتكامل Integrity .

ويمكن أن نعرف الأمن بأنه الوقاية ضد :

1-الوصول (النفاذ) الغير مأذون للأنظمة.

2-تغيير البيانات المخزونة أو المرسلة عبر نظم الحاسوب.

3-تعطيل disruption او تخريب sabotage أو نهب vandalism نظم الحاسوب وشبكاته.

ويمكن أن نعتبر أن هذا تعريف لأمن الحاسوب.

تعريفات أخرى:

1-يكون نظام الحاسوب مؤمناً حينما يتحقق شرطان :

حينما نعتمد على النظام وحينما نعمل برمجياته كما نتوقعها.

2-النظام مؤمن اذا توفرت فيه الشروط الثلاثة:

السرية والصحة والتكامل فى الإتاحة (التواجد) availability وذلك يعنى ان النظام لا يسمح بتوصيل أو تعديل معلومات لجهة غير مأذونة كما إنه يضمن إتاحة المعلومات للشخص- الجهة المأذون الذي يطلبها.

3-كما يرى آخرون أهمية ثبات المعلومات وتجانسها consistency وضبط الوصول (النفاذ) لها Access control.

أمن الحاسوب و جرائم الحاسوب:

أمن النظم هي جزء من جرائم الحاسوب فجرائم الحاسوب ليس بالضرورة ان تنتج من عدم كفاءة أمن النظام و لكنها ربما تحدث لأسباب ليست لها علاقة بكفاءة أمن النظام. و مثال ذلك الجرائم المتعلقة بالملكية الفردية (بيع برامجيات غير مأذونة) او استخدام مادة (ملفات) ذات محتوى يحرمه القانون..الخ.

تداخل الخصوصية و التأمين:

هناك تداخل بين حفظ المعلومات بطريقة مأمونة و الخصوصية:

1. هنالك جهات مأذون لها أن تبحث المعلومات و تطلّع على تفاصيل و محتويات النظام (مثال: مديري النظام, مشرفي الأمن في الشبكة..الخ). هذه الجهات عادة يكون التخوف منها ان تخرق الخصوصية.
2. المستخدم المباشر / الفوري on-line user يتخوف من وصول اشخاص او مؤسسات غير مأذونة للمعلومات او تغييرهم للمعلومات.

و يمكن ان نقول ان تأمين المعلومات شرط لازم لتحقيق الخصوصية[نحن نريد التأمين لأن ذلك يحمي الخصوصية و لكننا نخشى التأمين لأنه قد يطغى على الخصوصية و يخترقها] .

نقاش: تقوية التأمين و الخصوصية يتعاضدان في كثير من الأحيان و لكنهما يتناقضان في بعض الاحيان (في الإنترنت مثلاً).

- التأمين يحافظ على المعلومات من المتطفلين و هو بذلك يُمكن من تحقيق الخصوصية.
- إمعاناً في الخصوصية نستخدم وسائل التخفي(إخفاء الشخصية) في الإنترنت و ذلك يجعل مهمة التأمين صعبة.

هل يؤدي تأمين السايبر لعمليات غير أخلاقية:

هنالك من يستخدمون وسائل إخفاء الهوية anonymity فيدخلون بعض المواقع و قواعد المعلومات و ربما كشفوا بعض المعلومات مما يسبب خسائر لأصحابها.فوسائل إخفاء الشخصية تساعد على الخصوصية لكنها قد تستغل لإستخدام خاطئ فتهزم أمن النظام.

تأمين السايبر:

يتكون تأمين السايبر من جزئين:

الجزء الأول: خرق النظام (نقصد النظام نفسه و ليس محتوياته من قواعد بيانات و معلومات..الخ):

حماية النظام من الثغرات و قابلية الاختراق من البرامج المعتدية و الفيروسات و غيرها.

الجزء الثاني: تأمين المعلومات:حماية النظم من الوصول غير المأذون و يشمل ذلك المعلومات المخزونة و المرسلة.

مقتحمو نظم الحاسوبcomputer hacker:

هي مجموعات تربطهم علاقة قوية و قواعد تحكم تصرفاتهم و يدعون بأنهم يؤمنون بإزالة الحواجز و بالحرية المطلقة و انهم يقدمون خدمات للمجتمع باكتشافهم ثغرات النظام و باختراقها و انهم لا يؤذون احداً. و لكنهم يعملون ضد القانون و ضد قوانين حقوق الملكية الفكرية. كما و يتسببون في إيذاء جمهور المستخدمين و يتسببون في خسائر لا شخاص و مؤسسات. وبناء على ذلك فتصرفاتهم غير أخلاقية.

هل يمكن تحقيق التأمين الكامل:؟

- زيادة التأمين ربما تجلب مزيداً من الإجراءات التى قد تجعل استخدام النظم صعباً و غير سهل للمستخدمين.
- التجارة الالكترونية تحبذ زيادة التأمين و لكنها تخشى ان تسبب صعوبة الاستخدام في صد الزبائن المبتدئين في تعلم الحاسوب.

وهذا الموضوع لايزال قيد البحث إذ لا يوجد نموذج لتحديد التأمين الأكثر كفاءة. كما لا توجد دراسة تحدد على من تقع المسئولية الأخلاقية في تأمين نظم الحاسوب.

التأمين في المؤسسات:-

مقدمة:

بما إن النظام يتكون من سلسلة من الوحدات والحلقات والعناصر المرتبطة فإن درجة تأمين آي نظام تساوى درجة تأمين أضعف حلقاته. وتتكون معظم نظم معلوماتنا من أفراد موظفين ومعدات وبرامجيات .... الخ. فإذا انخفضت درجة تأمين/ انضباط البشر (الموظفين) المتعاملين مع النظام فلن ترتقي درجة تأمين النظام مهما بذلنّا في تأمين المعدات والبرامجيات ....الخ.

ومعلوم أن 80% من خروقات الأنظمة الحاسوبية يعود لمشاكل أو إهمال في التأمين سببه البشر المتعاملين مع النظام ولذلك فإن سد هذه الثغرة هو أهم عناصر تأمين النظام.

وتحتوى النظم الحديثة على مكونات شتى قد يكون بعضها ليس معروفاً لمصمم النظام أو لمطبقه أو لمستخدمه. ولذلك قد يبقى التأمين هاجساً ما بقى النظام. ويشمل التأمين عدداً من العمليات المتعاضدة من إجراءات وتقنيات لمنع وقوع الخروقات وعمليات لاكتشافها وصدها ثم نظام للتحقق منها ومقاضاة ومعاقبة من ارتكبها.

الاجراءات المقترحة:

تقوم كل مؤسسة بتحديد نظام للتأمين (سياسة التأمين Security Policy) توضح فيه الاجراءات المطلوب اتباعها من كل منسوبى المؤسسة خاصة في استخدام نظام المعلومات والأجهزة وكلمات المرور.

جرائم الحاسوب والجرائم ذات الصله بالحاسوب

القوانين قديمة وتطورت وتكيفت مع المجتمعات والثقافات. اما الحاسوب والسايبر فهما امران جديدان ولذلك فان القوانين التي ابتدعت لازالت جديده ومتغيره ولم تستقر بعد.

وتدور كثير من جرائم الحاسوب حول التزوير fraud وسوء استغلال نظم الحاسوب abuse.

التزوير: هو تغير البيانات او المعلومات عمدا للمنفعة.

سوء الاستغلال: (وهو اوسع ويشمل التزوير) النشاط الغير مأذون الذي يؤثر (قصدا او إهمالا)على تواجد النظام او السرية او الصحة والتكامل لموارد النظام .وسوء الإستخدام الجنائي يشمل التزوير والإختلاس والسرقه وتوقيف الخدمه Denial of service… الخ.

جرائم الحاسوب:

هي الجرائم التي يكون فيها الحاسوب اداة اساسية في ارتكاب الجريمة.

ولذلك فان سرقة جهاز حاسوب او اقتحام معمل حاسوب لا تعتبر جريمة حاسوب بل هي جريمة عادية.

جرائم الحاسوب الاصيلة:

الجرائم التي لا يمكن ان ترتكب الا باستخدام الحاسوب او التي لا يمكن ان تحدث الا في بيئة (دنيا) الحاسوب.

انواع جرائم الحاسوب:

a) القرصنة Cyber piracy:

استخدام تكنولوجيا السايبر دون إذن:

- لانتاج نسخ من برامجيات او معلومات مملوكة للغير.
- توزيع معلومات مملوكة للغير(رقمية) عبر شبكة حاسوب.

b) التعدي Cyber trespass:

استخدام التكنولوجيا للوصول(النفاذ) دون إذن لـ:

- لنظام حاسوب يخص شخصاً آخر او منظمة .
- لموقع محمي بكلمة مرور.

c) التخريب / النهب Cyber vandalism:

استخدام التكنولوجيا لاطلاق برنامج او اكثر.

- لتعطيل ارسال المعلومات الكترونياً عبر شبكة او شبكات اتصالات والانترنت.
- لإتلاف بيانات مخزونة في حاسوب او الاضرار بموارد نظام حاسوب او ارتكاب الاثنين معاً.

وتعتبر اي من الافعال الثلاثه اعلاه جريمة بغض النظر عن الدوافع سواء احدثت من المتعدين hackers او الناشطين او غيرهم.

الجرائم ذات الصلة : الجرائم ذات الصلة يمكن ان نقسمها لاثنين:

- **جرائم بمساعدة السايبر:** مثل الغش في نماذج الضرائب والغش في اختبار مادة اخلاقيات السايبر.

- **جرائم بدفع السايبر** :جرائم تضخمت وتأججت وتعاظمت بالسايبر مثل القمار عبر الإنترنت.

الجرائم الأصلية :

هي جرائم السايبر تحديدا (التي ذكرناها آنفا:القرصنة والتعدي والتخريب).

الجرائم المنظمة باستخدام الانترنت:

- التغرير بالصغار.
- جرائم الجنس.
- الاحتيال (المالي).
- الصور الخليعة.

التجسس المؤسسي:

التجسس المؤسسي لسرقة المخترعات Corporate Espionage والأفكار والبرامج و يعد مثل جرائم التجسس والسرقة الاخرى.

مشاكل في محاربة جرائم الحاسوب:

سنت القوانين الوطنية لدول ذات سيادة على رقعة جغرافية معلومة يسود فيها قانون الدولة,لكن الانترنت جعلت الموضوع معقدا فقد يرتكب المجرم جريمة من بلد ما فيؤذي آخرين في عدة بلاد اخرى وتثار عدة مشاكل اين ارتكبت الجريمة؟ اين يحاكم؟ وبأي قانون .

هنالك عدة مشاكل في هذا الجانب كما ان هنالك عدد من مشاكل قوانين الحاسوب لازالت قيد البحث ولازالت هنالك حاجة لقوانين وطنية واقليمية ودولية لمعالجة هذا الامر.ومن مشاكل القوانين التي وضعت في بعض البلدان انها تتعدل بسرعة لمواكبة المتغيرات السريعة في التكنولجيا.ويشكو الكثيرون من عدم مواكبتهم للقوانين بسبب كثرة التعديلات.

وهنالك اتفاقيات بين مجموعات من الدول كمجموعة الثمانية تعالج جرائم الحاسوب والجرائم ذات الصلة والمحتوى المؤذي والجرائم المتعلقة بحقوق الطبع.

الاطفال والانترنت:-

(انظر الموقع http://www.cybercrime.gov وهو موقع تابع للحكومة الامريكية .وتصفح الارشادات للمدارس الابتدائية التي تنصح التلميذ وتوجهه ليتفادى مشاكل و جرائم الانترنت).

ونرى أننا يجب أن نحمى الأطفال من مضار استخدام الحاسوب والانترنت من النواحى التالية:

(i) الصحة: تفادى الجلوس أمام الحاسوب لمدة طويلة (تزيد عن الساعتين) لما في ذلك من مضار محتملة على العينين واليدين... كما وأن طول الجلوس يؤدى لزيادة الوزن.

(ii) التغرير: الانترنت ... طلب رقم الهاتف، العنوان، الاغراء بالجوائز.

(iii) المحتوى: التأكد من أن الطفل يطلع على المحتوى المحترم والملائم.