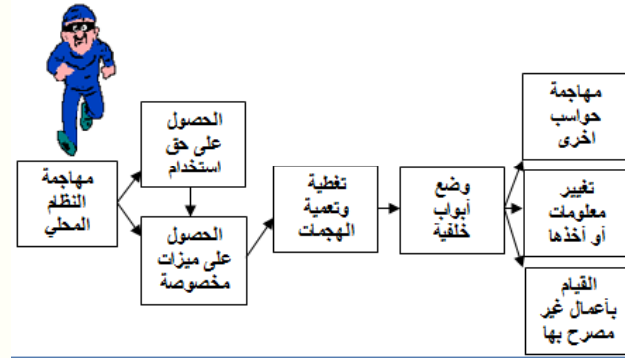


الهجمات علي البنية التحتية لتكنولوجيا المعلومات

هناك ثلاثة أنواع للهجمات:

هجمات تقنية: Technical تم حل حوالي ٨٠% منها ولكن الصعوبة في ال ٢٠% الباقية (متمثلة في أعمال القرصنة والهجمات المؤتمتة وكذلك البرمجيات المخربة لبرامج الغير).



هجمات مادية: Physical وضع بعض المكونات المادية تنقل لاسلكيا ما يتم على الحواسيب المهمة مثل:



هجمات اجتماعية: Social هذا يعتبر أخطر أنواع الهجمات حيث أنه يتم اختيار اشخاص من داخل النظام لتجنيدهم ، وتأثيرهم يكون أكثر ضررا.

الجوانب القانونية لتأمين تكنولوجيا المعلومات:

لا جريمة دون أن يكون هناك نص قانوني يحدد أركانها ونموذج وقوعها ولا عقاب ولا مساءلة عند انتقاء النص. لذلك وجب علينا معرفة

التشريعات القانونية للجرائم المعلوماتية (في مصر):

○ قانون الأحوال المدنية رقم ١٤٣ لسنة ١٩٩٤.

○ القانون رقم ٨٢ لسنة ٢٠٠٢ ولائحته التنفيذية والخاص بحماية حقوق الملكية الفكرية.

○ قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣.

○ إنشاء إدارة متخصصة لمكافحة جرائم الحاسبات والشبكات بوزارة الداخلية تسمى " إدارة مباحث مكافحة جرائم الحاسبات الإنترنت".

○ القانون رقم ١٥ لسنة ٢٠٠٤ لتنظيم التوقيع الالكتروني ولائحته التنفيذية.

○ صدر القرار الوزاري رقم ٣٢٧ لسنة ٢٠٠٥ بتشكيل لجنة لإعداد مشروع قانون أمن المعلومات ومكافحة الجرائم المعلوماتية. فتم إنشاء هيئة تنمية صناعة تكنولوجيا المعلومات والتي تأخذ على عاتقها إعداد اللجان الفنية والقانونية لإعداد مشروع قانون يتناول الجرائم المعلوماتية بنصوص تشريعية تحمي المجتمع من أضرارها.

أما بالنسبة للنشر على الانترنت فإنه وفقا للقانون المصري فإنه يخضع النشر عن طريق الإنترنت للقواعد العامة في المسؤولية الجنائية إذا ما تعلق النشر بإحدى جرائم الصحافة المنصوص عليها في الباب الرابع عشر من الكتاب الثاني من قانون العقوبات.

أهم طرق الاتصال بوزارة الداخلية المصرية:

موقع معلومات وزارة الداخلية: www.moiegypt.gov.eg

البريد الإلكتروني لوزارة الداخلية: center@iscmi.gov.eg

رقم تليفون مركز اتصالات الحكومة المصرية: ١٩٤٦٨

شرطة النجدة ١٢٢ مصلحة الأمن العام ١١٥

تليفونات مكافحة : الجرائم الالكترونية : ٢٧٩٢١٤٩٠ جرائم الشبكات: ٢٧٩٢٨٤٨٤

جرائم الأموال العامة: ٢٧٩٢٩٩٨٨ جرائم المصنقات الفنية: ٢٧٩٤٣٢٩١

جرائم حقوق الملكية الفكرية: ٢٧٩٤٧٦٠٤

المراجع منها :

مقالات للدكتور هشام بالاضافة إلى <http://www.itida.gov.eg/>

<http://alquds.masrawy.com/01082003/179165news.htm>

الشكر واجب لكل الزملاء المراجعين



تأمين تكنولوجيا المعلومات

إعداد

دكتور مهندس / هشام نبيه المهدي محمد

استاذ تكنولوجيا المعلومات المساعد

بكلية الحاسبات والمعلومات - جامعة القاهرة

رائد الجمعية العلمية بالكلية

<http://www.h-elmahdy.net/>

أمن المعلومات ليس تكنولوجيا وأدوات فنية يجرى شراؤها وتركيبها وحسب، ولكنها منظومة ثقافية ووعي وثقة وانتماء تشكل أرضية مناسبة تزرع فيها سياسات تأمين فعالة ومتوازنة تخدمها تقنيات يتم اختيارها بذكاء. هذا العدد من النشرة تم تخصيصه لإلقاء الضوء على تأمين تكنولوجيا المعلومات. ذلك لعلنا نسمى الأمور بمسمياتها ونذكر حجم المشكلة الحقيقي.

العدد السادس - مايو ٢٠٠٨

في احتفالية بمناسبة تكريم كين تومبسون (الأب الرسمي لنظام التشغيل يونيكس) بمناسبة منحه أعلى الأوسمة بعد مرور ٣٥ عام على اختراعه نظام التشغيل المذكور، تمت دعوة مستر تومبسون لإلقاء محاضرة تحت عنوان: "الثقة في الثقة. Trust on Trust. ..."

استهل مستر تومبسون محاضرتة بالدعاية الآتية: يجب على أي شركة تكنولوجيا معلومات محترمة أن لا تقوم بتوظيف أي متخصص مثل كين تومبسون .. وبعد أن هدأ ضحك الحاضرين بدأ يحكي لماذا يقول هذا ؟

قال لهم هذه القصة: حينما أن أنهيت تصميم المكونات الرئيسية لنظام التشغيل يونيكس أحسست أنه سوف يستخدم في مؤسسات وشركات كبيرة. فحدثتني نفسي أن أضع بابا خلفيا يمكنني من الدخول لأي نظام. كانت هناك مشكلة بسيطة وهي أن نظام التشغيل هذا يتم توزيعه مفتوح المصدر (أي يمكن لأي مبرمج مبتدئ أن يتعرف على مكونات البرامج ويغلق ذلك الباب). فوضعت موديول مستقل كصندوق مغلق لا يستطيع أحدا أن يعرف وظائفه ولكنه ضروري للتشغيل. وظيفة هذا الموديول هو السماح لي بالدخول الخفي لأي نظام.

هناك العديد من القصص الحقيقية للاختراقات الأمنية المشابهة لهذه الحالة. طبعا الغرض ليس للتسلية ومصممة الشفافيف أو زيادة الإحباط خاصة لمن يؤمنون بنظرية المؤامرة ، ولكن الغرض الرئيس أولا: هو تسمية الأمور بمسمياتها ، ثانيا: لوضع الحجم الحقيقي للمشكلة أمام القارئ عسى أن تتال اهتمام متخذي القرار لوضعها في الرؤية الاستراتيجية العربية والمصرية.

إن الحديث عن أمن المعلومات التي ننتجها جميعًا – كأفراد وشركات ومؤسسات – لم يعد ترفاً أو من قبيل الأشياء الكمالية، فالبيانات والمعلومات هي الثروة الحقيقية التي لا تقدر بثمن، وتتجاوز قيمة الأجهزة والبرامج، فكل الأجهزة والبرمجيات قابلة للتعويض والإحلال، أما البيانات والمعلومات فلا يمكن تعويضها بسهولة إذا تعرضت للسطو أو الفقد، علاوة على أن الأمر ليس فقط تأمين للمعلومات بغرض الحماية من السرقة والفقد، فهناك حماية الخصوصية، وضبط العلاقة بين المتعاملين بالمعلومات وغيرها من أمور كثيرة تدرج تحت مظلة أمن المعلومات.

وحتى الآن لا تزال هناك تساؤلات عديدة مثارة حول ما إذا كنا – كأفراد وهيئات ومجتمع ككل – جاهزين فعلا لتأمين القدر الكبير من المعلومات الذي نتعامل معها وتتعاظم بمرور الوقت، وتستمد هذه التساؤلات أهميتها من ازدياد التوجه داخل المجتمع بكل قطاعاته – حكومة وهيئات عامة وقطاع خاص وأفراد – نحو تكنولوجيا المعلومات وتطبيقاتها المختلفة.

ولا بد من الاعتراف بأن التعامل مع قضية أمن المعلومات بالعديد من دول العالم – ومنها مصر والمنطقة العربية – يتخذ صورتين بعيدتين عن الفهم السليم، الأولى تتبع منطق التهوين وفيها ينشئ البعض المواقع وقواعد البيانات والشبكات ويحملونها بكم ضخم من البيانات والمعلومات ثم لا يلقون بالا لعيلة التأمين من الأصل، لكنهم لا يؤمنون بقيمة المعلومة التي يمتلكونها، ومن ثم لا يوجد لديهم دافع يحثهم على تأمينها، والبعض الآخر لديه إحساس عفوى عشوائي بأنه لا يوجد خطر يهدد هذه المعلومات، فلا يرتاحون إلى الإنفاق على تأمينها، والنتيجة أنهم عند أول تهديد جدى يجدون أنفسهم أمام وضع مؤسف ضاع فيه كل شيء.

نبدأ ببعض التعريفات ليمكننا معرفة حدود الموضوع:

- عناصر تأمين المعلوماتية:
- تأمين العنصر البشرى.
- تأمين المكونات المادية للحاسبات.
- تأمين البرامج ونظم التشغيل والوسائط التخزينية.
- تأمين وسائل الاتصالات التي تربط بين الشبكات.
- التعريف القانوني الدقيق للجريمة المعلوماتية.

الجريمة المعلوماتية:

جريمة الكترونية غير مادية تظهر وتختفى فى ثوان. ومرتكبي هذه الجرائم لهم صفات مميزة من حيث الثقافة والعلم التكنولوجى. قد تمتد إلى خارج حدود مرتكبيها إلى دولة اخرى وهنا تثار مشاكل الاختصاص والإجراءات والتحرى والتفتيش. وقد تكون مواجهتها بنفس أساليب وإجراءات أرتكابها حتى وإن كانت غير مشروعة.

التعريف القانوني للجريمة المعلوماتية:

- نشاط غير مشروع تم توجيهه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي يتم تحويلها عن طريقه.
- كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات.
- نمط من أنماط الجرائم المعروفة فى قانون العقوبات طالما مرتبطة بتقنية المعلومات.
- الجريمة الناجمة عن إدخال بيانات مزورة فى الأنظمة وأساءة استخدام المخرجات.
- فعل أجرامى يستخدم الكمبيوتر فى أرتكابه كأداة رئيسة.
- هى الجريمة التى تلعب فيها البيانات والبرامج المعلوماتية دوراً.
- كل أشكال السلوك غير المشروع الذى يرتكب باستخدام الحاسب.

بعض صور جرائم الانترنت:

- الاختراقات والتجسس بغرض الحصول على المعلومات الهامة ذات الطبيعة السرية (مثل بيانات كروت الائتمان).
- انتحال الشخصيات والمضايقة والملاحقة.
- التخريب والاستدراج وتشويه السمعة.
- انتاج ونشر الإباحية.
- النصب والاحتيال والاعتداء على الآخرين.
- الإرهاب و تقنياته.
- جرائم البنوك وغسيل الأموال.