المملكة العربية السعودية

أمن المعلومات
(الواجبات والالتزامات الوظيفية)

اعداد المهندس / ماجد بن عيضه الزايدي
مدير المشاريع والشبكات بمركز الحاسب الألي بأمانة الطائف

مقدمة

ان التطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة و مضطردة في أساليب العمل و الميادين كافة إذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية و الدولية و أجهزة الحاسوب من الأمور الروتينية في عصـرنا الحالي و إحدى علامات العصـر المميزة التي لا يمكن الإسـتغناء عنها لتأثيرها الواضـح في تسـهيل متطلبات الحياة العصـرية من خلال تقليل حجم الأعمال و تطوير أسـاليب خزن و توفير المعلومات حيث أن انتشـار أنظمة المعلومات المحوسـبة أدى الى أن تكون عرضـة للإختراق لذلك أصـبحت هذه التقنية سـلاحا ذو حدين تحرص المنظمات على إقتناءه و توفير سبل الحماية له .

ان موضـوع الأمن المعلوماتي يرتبط ارتباطا و ثيقا بأمن الحاسـوب فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسـوب ، و في ظل التطورات المتسـارعة في العالم و التي أثرت على الإمكانات التقنية المتقدمة المتاحة و الرامية الى خرق منظومات الحاسـوب بهدف السـرقة أو تخريب المعلومات أو تدمير أجهزة الحاسـوب ، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية و الوقائية و حسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب ، و كان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء امنية للمعلومات تضمن الحفاظ عليها .

مفهوم الأمن المعلوماتي

تشكل المعلومات لمنظمات البيئة التحتية التي تمكنها من أداء مهامها ، إذ أن نوع المعلومات و كميتها و طريقة عرضـها تعتبر الأسـاس في نجاح عملية صـنع القرارات داخل المنظمات المعاصـرة و عليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لإستخدامها و تداولها و وضع السبل الكفيلة بحيازتها ، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات و إبعادها عن الإستخدام غير المشروع لها .

و من أجل فهم الأمن المعلوماتي Information Security لا بد من تحديد معناه ، حيث عرفه (السـالمي) بأنه مجموعة من الإجراءات و التدابير الوقائية التي تسـتخدم سـواء في المجال التقني أو الوقائي للحفاظ على المعلومات و الأجهزة و البرمجيات إضـافة الى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال ، أما (المشـهداني) فقد عرفه بأنه (الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضـياع و التلف أو من مخاطر الإسـتخدام غير الصـحيح سـواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية ، أما (أنور) فقد عرفه بأنه مجموعة من التدابير الوقائية المسـتخدمة في المجالين الإداري و الفني لحماية مصـادر البيانات من أجهزة و برمجيات و بيانات من التجاوزات أو التداخلات غير المشـروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلسل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية ، فضـلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التيب تؤدي الى فقدان بعض المصـادر كلا أو جزءا ، و من ثم التأثير على نوع و مسـتوى الخدمة المقدمة ، من كل ما سـبق يمكن أن نعرف الأمن المعلوماتي بأنه ذلك الحقل الذي يهتم بدراسـة طرق حماية البيانات المخزونة في أجهزة الحاسـوب إضافة الى الأجهزة الملحقة و شبكات الإتصالات و التصدي للمحاولات الرامية الى الدخول غير المشروع الى قواعد البيانات المخزونة أو تلك التي ترمي الى نقل أو تغيير أو تخريب الخزين المعلوماتي لهذه القواعد .

نظرة عامة على أهم المصطلحات في أمن المعلومات

سنبدأ الحديث عن الأهداف التي من أجلها تقوم المنظمات بإنشاء أنظمة الحماية المختلفة، وهي ثلاثة. السرية، السلامة، الإتاحة أو التوفر.

- **السرية:(Confidentiality)**

السرية هي أشهر الأهداف في مجال أمن المعلومات. إخفاء المعلومات قد يكون مهم جدا، فمثلا المعلومات العسكرية لا يجب أن تصل إلى مخابرات العدوا! حتى في عالم الأعمال، بعض المعلومات سرية ولا يجب أن يطلع عليها المنافسين. سرية المعلومات لا تكون فقط في المعلومات المحفوظة في القرص الصلب، بل أيضا تمتد لتشمل المعلومات المنتقلة عبر الإنترنت.

- **السلامة:(Integrity)**

البيانات تتغير دائما، فمثلا في البنك حينما يقوم أحدهم بسحب نقدي، يجب تغيير ما تبقى له في حسابه بناءً على ما تم سحبه. السلامة تعني أن تبقى البيانات كما هي ولا يستطيع تغييرها إلا الأشخاص المصرح لهم بهذا وبالطريقة الصحيحة. وسلامة البيانات ليست مهددة فقط بفعل هجومي من خارج المؤسسة، انقطاع الكهرباء أو زيادة الشحنة الكهربائية قد تؤثر في البيانات! (تذكر أن كل البينات المنتقلة في الشبكة هي عبارة عن شحنات كهربائية.)

- **الإتاحة:(Availability)**

تعني الإتاحة أن تكون البيانات(أو الخدمات) متاحة للأشخاص المصرح لهم بهذا. ويذكرني هذا الهدف بالمقولة الشهيرة التي تقول: "أكثر الأماكن أمانا للسفن هي الميناء، ولكنها لم تُبن لذلك". لإن حماية البيانات ستكون أكثر سهولة إذا لم تكن متاحة عبر الإنترنت، ولكن ما فائدتها إذن؟

الآن سنتحدث عن أشهر الهجمات التي تستهدف هذه الأهداف.

أولا : الهجمات على السرية:

التجسس:(Snooping)

هي سرقة البيانات المنتقلة من مكان إلى آخر ومعرفة محتواها. على سبيل المثال، إذا تم نقل ملف عبر الإنترنت يحتوي على البيانات سرية، التجسس هو الحصول على هذا الملف ومعرفة ما فيه من بيانات.

التنصت:(Traffic Analysis)

التنصت بعكس التجسس، لا تستطيع الإستفادة من البيانات بشكل مباشر (بسبب أنها مشفرة مثلا). ولكن تستطيع معرفة الكثير من المعلومات الأخرى التي قد تكون مفيدة من خلال مراقبة حزم البيانات المنتقلة من جهاز إلى آخر. على سبيل المثال، تستطيع معرفة وجهة الملف (من خلال معرفة الـــ IP الخاص بالوجهة). ومعلومة واحدة قد لا تكون مفيدة وحدها، ولكن المعلومات الصغيرة قد تفيد إذا ما جمعتهم معًا.

ثانيا : الهجمات على السلامة:

التعديل:(Modification)

التعديل هي خطوة تلي الحصول على حزمة البيانات، فيستطيع المهاجم تغيير البيانات لتكون في صالحه هو. على سبيل المثال، يستطيع المهاجم الإستفادة من رسالة عميل بنك يريد تحويل أمواله إلى حساب آخر من خلال تغيير الحساب المستفيد ليكون حسابه المهاجم.

سرقة الهوية:(Masquerading OR Spoofing)

سرقة الهوية هي ادعاء المهاجم والتظاهر أنه شخصٌ آخر. كادعاء المهاجم أنه عميل بنك معين (من خلال سرقة كلمة المرور الخاصة بهذا العميل مثلا). وتشمل سرقة الهوية إدعاء أنه مؤسسة أيضًا! فقد يدعي المهاجم أنه البنك ليأخذ معلومات حساسة من العميل.

إعادة إرسال:(Replaying)

هذا الهجوم يعتمد على سرقة نسخة من رسالة معينة، ومن ثم إعادة إرسالها في وقت لاحق. على سبيل المثال، ينسخ المهاجم رسالة لعميل أراد تحويل أموال له من البنك لقيامه المهاجم بخدمة معينة للعميل. في وقت لاحق، يرسل المهاجم نفس الرسالة إلى البنك ليتم تحويل المبلغ مرة ثانية وثالثة ورابعة وهكذا..

الإنكار:(Repudiation)

طريقة الهجوم هذه مختلفة تماما عن كل ما سبق. في هذه الطريقة ينكر أحد طرفي الإتصال قيامه بالإتصال. على سبيل المثال، يقوم عميل بنك بطلب تحويل أموال إلى حساب آخر، وبعد فترة يُنكر طلبه هذا الطلب. أو قيام شخص بشراء بضاعة على الإنترنت، وبعد الدفع، يُنكر البائع حصوله على الأموال.

ثالثا : الهجمات على الإتاحة:

الحرمان من الخدمة:(Denial of Service)

من أشهر الهجمات على الإطلاق في عالم أمن المعلومات. لها عدة طرق، منها إرسال طلبات كثيرة إلى الموقع تجعله بطيئا أو تقوم بإيقاعه كليا. قد يشمل أيضا الحصول على الرسائل القادمة من الموقع إلى عميل معين ومسحها، ليُخيل للعميل أن المُخدم قد سقط. أو العكس، يقوم المهاجم بمسح كل الرسائل الموجهة من العميل إلى الموقع.

رابعا : الأربع خدمات التي قدمها معيار (ITU-T) العالمي وكيف يمكن تقديمها.

الخدمات :

الأربع خدمات هم سرية البيانات وتكمالية البيانات والتحقق من الشخصية،و منع الإنكار والتحكم في الوصول. نلاحظ في هذه الخدمات أنها تقوم مجتمعة مقام الأهداف الثلاثة للحماية. وأيضا ستلاحظ أنها تمنع جميع أنواع الأختراق الذي تم ذكره في المقال.

سرية البيانات:(Data Confidentiality)

هي الخدمة المقدمة للحماية من معرفة محتوى البيانات والإستفادة منها بشكل مباشر (من خلال الإطلاع على البيانات مباشرة) أو بشكل غير مباشر (من خلال التنصت على الإتصال)

تكاملية البيانات:(Data Integrity)
هي الخدمة المقدمة لحماية البيانات من التعديل أو المسح أو حتى إعادة الإرسال.

التحقق من الشخصية:(Authentication)
هي الخدمة المقدمة للتحقق من شخصية المستقبل أو المرسل أو كليهما معا.

منع الإنكار:(Nonrepudiation)
هي الخدمة المقدمة للحماية من إنكار أحد طرفي الإتصال قيامة بطلب شئ معين من خلال تمكين المرسل أو المستقبل من إثبات أن من قام بالإتصال هو الطرف الآخر إذا قام الطرف الآخر بالإنكار.

التحكم في الوصول:(Access Control)
هي الخدمة المقدمة للحماية من الوصول إلى البيانات لغير المصرح لهم.

آليات الحماية:
آليات الحماية هي الأدوات التي يتم استخدامها لتقديم الخدمات الأربع التي تم ذكرها آنفا. قد يتم استعمال أكثر من آلية للحصول على خدمة واحدة، وقد تُستعمل الآلية للحصول على أكثر من خدمة أيضًا. سنقوم أولا باستعراض هذه الخدمات، ومن ثم سنستعرض كيف يتم الإستفادة من هذه الخدمات.

التعمية:(Encipherment)
أولى أدوات الحماية، وتعني إخفاء البيانات بطريقة لا يمكن الإستفادة منها إلا من الأشخاص المصرح لهم فقط. أشهر أنواع التعمية اليوم هي التشفير (Encryption) وإخفاء البيانات.(Encipherment)

تكاملية البيانات:(Data Integrity)
هي طريقة لإضافة بيانات إضافية (عبارة عن قيمة معينة) إلى البيانات الأصلية للتحقق منها. يقوم المرسل بحساب هذه القيمة بطريقة معينة ومن ثم يضعها مع البيانات الأصلية. ومن ثم يقوم المستقبل بأخذ البيانات الأصلية ويقوم بعمل نفس الحسابات التي قام بها المرسل ويقوم بعدها بمقارنة النتيجتين للتأكد من تطابقهما.

التوقيع الإلكتروني:(Digital Signature)
التوقيع الإلكتروني هي الطريقة التي يستطيع بها المرسل توقيع البيانات إلكترونيا بحيث يستطيع المستقبل التأكد من صحة التوقيع. الطريقة هي أن يقوم المرسل بعملية تُثبت أنه يمتلك المفتاح السري للمفتاح المُعلن الذي أعلنه من قبل.

تبادل التوثيق:(Authentication Exchange)
هي الطريقة التي يُمكن لطرفي الإتصال من خلالها إثبات هويتهما لبعضهما. على سبيل المثال أحد طرفي الإتصال يستطيع إثبات أنه يمتلك معلومة معينة (كلمة المرور مثلا) هو وحده يعرفها.

حشو حزم البيانات:(Traffic padding)
هي طريقة تستخدم لمنع التجسس، وذلك من خلال إرسال حزم بيانات مزيفة وسط البيانات الحقيقية لتضليل المتنصت.

التحكم بالطريق:(Routing Control)

هي الطريقة التي تقوم على تغيير مسار البيانات بين المرسل والمستقبل بشكل مستمر بحيث يكون من الصعب الحصول على كامل الرسائل المرسلة بينهما.

التوثيق:(Notarization)

وتعني اختيار طرف ثالث موثوق للتحكم بعملية الإتصال بين طرفي الإتصال. هذه الطريقة تستخدم لمنع الإنكار (راجع المقال السابق). يقوم الطرف الثالث بحفظ الطلبات من جهتي الإتصال بحيث لا يستطيع أحدهما إنكار إرسال الطلب.

التحكم في الوصول:(Access Control)

استخدام طريقة للتأكد من أن المستخدم له الحق في الإطلاع على البيانات، استخدام كلمات المرور مثلا.

مراحل تطور مفهوم الأمن المعلوماتي

إن مفهوم الأمن المعلوماتي مر بمراحل تطويرية عدة أدت الى ظهور ما يسمى بأمنية المعلومات ، ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات ، و كان همهم هو كيفية تنفيذ البرامج و الإيعازات و لم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة و كان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة لذلك ظهر مصطلح أمن الحواسيب Computer Security و الذي يعني حماية الحواسيب و قواعد البيانات ، و نتيجة للتوسع في استخدام أجهزة الحاسوب و ما تؤديه من منافع تتعلق بالمعالجة للحجوم الكبيرة من البيانات ، تغير الإهتمام ليمثل السيطرة على البيانات و حمايتها . و في السبعينات تم الانتقال الى مفهوم أمن البيانات (Data Security) و رافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة الى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث و اعتماد خطط لخزن نسخ اضافية من البيانات و البرمجيات بعيدا عن موقع الحاسوب ، و في مرحلة الثمانينات و التسعينات ازدادت أهمية استخدام البيانات ، و ساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات ، كل هذا أدى الى الإنتقال من مفهوم أمن البيانات الى أمن المعلومات ، و أصبح من الضروري المحافظة على المعلومات و تكاملها و توفرها و درجة موثوقيتها ، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة و تقلص اختراق المعلومات و التلاعب بها ، و كانت شركة IBM الأمريكية أول من وضع تعريف لأمن المعلومات ، و كانت تركز على حماية البيانات من حوادث التزوير ، و التدمير أو الدخول غير المشروع على قواعد البيانات و أشارت الشركة الى أن أمنا تام للبيانات لا يمكن تحقيقه و لكن يمكن تحقيق مستوى مناسب من الأمنية ، و السؤال الذي يطرح هنا ماذا سيكون بعد أمن المعلومات ؟ البعض يقول أمن المعرفة (knowledge Security) و ذلك لإنتشار أنظمة الذكاء الإصطناعي و ازدياد معدلات تناقل البيانات بسرعة الضوء أو التفاعل بين المنظومات و الشبكات و صغر حجم أجهزة الحاسوب المستخدمة .

الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات المعتمدة على الحاسب

لقد أصبح اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية خطراً يقلق العديد من المنظمات في السنوات الأخيرة و مع مرور الزمن نجد أن على الرغم من سبل الحماية التي تتبعها المنظمات ، الى أن هناك ارتفاعا واضحا في معدل الإختراقات مع تنوع الوسائل المستخدمة في الإختراق أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة ، فالبعض منها قد يكون مقصود كسرقة المعلومات أو ادخال الفيروسات و غيرها و هي الأشد ضررا على نظم المعلومات و يكون مصدرها أحيانا من داخل أو خارج المنظمة ، و قد يصعب أحيانا التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها ، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية و الكوارث الطبيعية و يمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات الى ثلاث فئات :

أ . الأخطاء البشرية Humane Errors

و هي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو اثناء ادخالها الى النظام ، أو في عمليات تحديد الصلاحيات للمستخدمين ، و تشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات .

ب . الأخطار البيئية Environmental Hazard

و هذه تشمل الزلازل و العواصف و الفيضانات و الأعاصير و المشاكل المتعلقة بأعطال التيار الكهربائي و الحرائق إضافة الى المشاكل القائمة في تعطل أنظمة التكييف و التبريد و غيرها ، و تؤدي هذه الأخطار الى تعطل عمل هذه التجهيزات و توقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة و استرداد البرمجيات و قواعد البيانات .

ج. الجرائم المحوسبة Computer Crime

تمثل هذه تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة و بشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوسبة و هي :

١. سوء الإستخدام لجهاز الحاسوب : و هو الإستخدام المقصود الذي يمكن أن يسبب خسارة للمنظمة أو تخريب لأجهزتنا بشكل منظم .

٢. الجريمة المحوسبة : و هي عبارة عن سوء استخدام لأجهزة الحاسوب بشكل غير قانوني يؤدي الى ارتكاب جريمة يعاقب عليها القانون خاصة بجرائم الحاسوب .

٣. الجرائم المتعلقة بالحواسيب : و هي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة .

و يمكن أن تتم الجرائم المحوسبة سواء من قبل أشخاص خارج المنظمة يقومون باختراق نظام الحاسوب (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول الى النظام و لكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة ، و تشير الدراسات التي أجرتها دائرة المحاسبة العامة و شركة Orkand للإستشارات الى أن الخسائر الناتجة عن جرائم الكمبيوتر تقدر بحدود ١,٥ مليون دولار لشركات المصارف المحوسبة في الولايات المتحدة الأمريكية ، و من ناحية أخرى يقدر المركز الوطني لبيانات جرائم الحاسوب في لوس أنجلوس بأن ٧٠% من جرائم الكمبيوتر المسجلة حدثت من الداخل ، أي من قبل من يعملون داخل المنظمات ، هذا و أن جرائم الحاسوب تزداد بصورة واضحة مما أصبحت تشكل تحديا خطيرا يواجه الإدارات العليا عموما و إدارة نظم المعلومات على وجه الخصوص .

رابعا :الحماية من الأخطار :

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة و الصعبة و التي تتطلب من إدارة نظم المعلومات الكثير من الوقت و الجهد و الموارد المالية و ذلك للأسباب التالية :

أ. العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات .

ب. توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة .

ج. وجود التجهيزات المحوسبة في عهدة أفراد عديدين في المنظمة و أحيانا خارجها .

د. صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية .

ه. التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.

و. التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمنظمة امكانية التعلم من التجربة و الخبرة المتاحة.

ز. تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها .

هذا و تقع مسـؤولية وضـع خطة الحماية للأنشـطة الرئيسـية على مدير نظم المعلومات في المنظمة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي :

- الوقاية من الأخطار غير المتعمدة .
- إعاقة أو صنع الأعمال التخريبية المتعمدة .
- اكتشاف المشاكل بشكل مبكر قدر الإمكان .
- المساعدة في تصحيح الأعطال و استرجاع النظام .

و يمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات و يجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار ، و يمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات و البرمجيات و الشبكات .

تواجه أنظمة المعلومات بعض المشـكلات الشـائعة التي بدأت تغزو أنظمة المعلومات و تسـاهم في تدميرها أو تخريبها أو سرقة الخزين المعلوماتي المحفوظ في أجهزة الحاسوب و من أهم هذه المشاكل هي:

الفيروسات (Virus)

تعتبر من أهم جرائم الحاسـوب و أكثرها انتشـارا في الوقت الحاضـر، و لم يعد يخفى على أحد ما المقصـود بفيروس الحاسـوب حتى من العامة ممن لا يسـتخدموا الحاسـوب و ذلك بسـبب تناقل الصـحف لأخبار خسـائر الشـركات و الحكومات و الأفراد بسـبب تخريب أحدثه فيروس معين ، و لم يعد أحد يخلط بين معنى فيروس الحاسوب و الفيروس البيولوجي الذي يصيب الإنسان كما كان يحدث سابقا بسبب عدم انتشار ثقافة الحاسوب . و يمكن تعريفه على أنه برنامج حاسـوب له أهداف تدميرية يهدف الى إحداث أضـرار جسـيمه بنظام الحاسـوب سـواء البرامج أو الأجهزة و يسـتطيع أن يعدل تركيب البرامج الأخرى حيث يرتبط بها و يعمل على تخريبها ، و هو برنـامج مكتوب بإحدى لغات البرمجة من قبل المبرمجين و هو قادر على التوالد و التناسـخ و يسـتطيع الدخول الى البرامج و على الأفضـلية أكبر من نظم التشـغيل تسـاعده في فحص المكونات المادية مثل الذاكرة الرئيسـية أو القرص المرن أو الليزري ، و قد ظهرت الفيروسـات في نهاية الأربعينات و كان أول من فكر فيها هو اختصـاصـي الكمبيوتر (جون فون تيونان)حيث نشـر مقاله حولها و ظهرت بعد ذلك آثار الفيروس في عام ١٩٥٠ إلا أنها بقيت محدودة الإنتشار حتى عام ١٩٨٣ عندما تفشت الفيروسات في برنامج UNIX و أثار ذلك ضـجة على السـاحة العلمية و العملية ثم ظهرت بعض الحوادث الفردية لصـغار المبرمجين الذين قاموا بزرع الفيروسات في شبكات الكمبيوتر ، فقد قام موريس الذي كان طالبا في جامعة كورنيل بإعداد برنامج مدمر ساهم في تعطيل آلاف من الحواسيب مما كلف الشركات الأمريكية (١٠٠)مليون دولار ، أما كيفية اكتشـاف الفيروس فكان عن طريق مبرمج هندي ، حيث قام بعمل برنـامج خفي من أجل المحـافظة على برنـامجه الذي كان أحدث برنامج للطباعة ، حيث قام بحمايته من النسخ من خلال دخوله على الملفات التشغيلية و هي في حالة النسخ ثم يقوم بتكبير حجم الملفات و من ثم تخريبها (أي الملفات المسـتنسـخة) و اسـتمرت مع التطورات الحاصـلة في مجال تكنولوجيا الحاسوب و البرمجيات تطور كل من برامج الحماية ، مقابل ازدياد حالات ابتكار و اعداد برامج فيروسية .

- الإجراءات الوقائية للحماية من الفيروسات

إن التطورات الحاصلة في مجال إعداد برامج الفيروسات جعلت من الصعوبة ايجاد طريقة مضمونة بدرجة كبيرة للوقاية من الفيروسات ولكن هناك بعض الأساليب الفعالة التي يمكن اتباعها للحماية و هي:

- **تركيب برنامج مضاد للفيروسات ملائم لنظام التشغيل المستخدم في جهاز الحاسوب ويفضل أن يكون نسخة أصلية للاستفادة من الدعم الفني للشركات التي يتم شراء البرامج المضادة منها.**
- **عدم وضع برنامج جديد على جهاز الحاسوب إلا قبل اختباره والتأكد من خله من الفيروسات بواسطة برنامج مضاد للفيروسات.**
- **عدم استقبال أية ملفات من أفراد مجهولي الهوية على الإنترنت.**
- **عمل نسخ احتياطية من الملفات الهامة وحفظها في مكان آمن.**
- **التأكد من نظافة أقراص الليزر التي يحمل منها نظام التشغيل الخاص بجهاز الحاسوب.**

هذه الأساليب إضافة الى العديد منها التي يمكن اتباعها من شأنها أن تساهم في ضمان حماية أجهزة الحاسوب و لكن يجب أن نضع نصب أعيننا و لا نتصور أن وجود برنامج مضاد للفيروسات محدث دائما في أجهزة الحاسوب يعني أننا في مأمن من الفايروسات ، كما أن أي مشكلة في الأجهزة لا تعني دائما أن هناك فيروسا لذا يجب تحديد سبب المشكلة و محاولة إيجاد العلاج لها .

قرصنة المعلومات

قد يسمع الكثير عن ما يسمى بالهاكرز أو مخترقي الأجهزة Hackers و نتسائل كيف يتم ذلك و هل الأمر بسيط الى هذا الحد أم يحتاج لدراسة و جهد ، في الحقيقة أنه مع انتشار برامج القرصنة و وجودها في الكثير من المواقع أصبح من الممكن اختراق أي جهاز حاسوب و بدون عناء فور انزال إحدى برامج القرصنة . و المقصود بالقرصنة هو سرقة المعلومات من برامج و بيانات بصورة غير شرعية و هي مخزونة في دائرة الحاسوب أو نسخ برامج معلوماتية بصورة غير قانونية و تتم هذه العملية إما بالحصول على كلمة السر أو بواسطة التقاط موجات الكهرومغناطيسية بحاسبة خاصة و يمكن إجراء عملية القرصنة بواسطة رشوة العاملين في المنظمات المنافسة . أما عن الهدف من عمليات القرصنة فهو سرقة الأسرار أو المعلومات التجارية أو التسويقية أو التعرف على حسابات المنظمات أو أحيانا بهدف التلاعب بقيود المصارف أو المؤسسات المالية بهدف سرقة الأموال أو يكون الهدف الكشف عن أسرار صناعية (تصاميم منتجات) بهدف إعادة تصنيعها دون إجازة قانونية أو لأهداف سياسية و عسكرية من أجل الحصول على الملفات و الخطط السرية العسكرية أو الحكومية . و الأمثلة على حالات القرصنة عديدة فقد قامت الشركات الصينية بنقل أسرار تكنولوجيا صناعية من الولايات المتحدة و كندا مستخدمة الحاسوب و من ثم القيام بإنتاج سلع على ضوء ذلك و تصديرها لهاتين الدولتين لتباع في أسواقها بثلث الأسعار الأصلية و نفس الشيء قامت به شركة متسوبيشي لبناء السفن و الصناعات التقليدية حيث استخدمت سماسرة للقيام بعملية التجسس الصناعي .

المخاطر التي تهدد خصوصية المعلومات في العصر الرقمي

تمكن تقنية المعلومات الجديدة خزن و استرجاع و تحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات و الدوائر و الوكالات الحكومية و من قبل الشركات الخاصة ، و يعود الفضل في هذا الى مقدرة الحوسبة الرخيصة ، و أكثر من هذا فإنه يمكن مقارنة المعلومات المخزونة في ملف مؤتمت بمعلومات في قاعدة بيانات أخرى ، و يمكن نقلها عبر البلد في ثوان و بتكاليف منخفضة نسبيا ، إن هذا بوضوح يكشف الى أي مدى يمكن أن يكون تهديد الخصوصية .

و تتزايد مخاطر التقنيات الحديثة على حماية الخصوصية ، كتقنيات رقابة (كاميرات الفيديو) و بطاقات الهوية الإلكترونية ، و قواعد البيانات الشخصية ، و وسائل اعتراض و رقابة البريد و الإتصالات ، و رقابة بيئة العمل و غيرها .

امنية نظم المعلومات:

إن موضوع الأمن في النظم الآلية للمعلومات يعتبر من أكثر المواضيع التي تنال اهتمام الباحثين والمتعاملين مع تلك النظم، لاشك إن انتشار الحاسبات الآلية ودخولها المطرد في إدارة نظم المعلومات المختلفة قد اثر تأثيرا مباشـــرا في تطوير ورفع كفاءة تلك النظم، لكن يظل هناك ســـؤالا مطروحا ألا وهو إلى أي مدى يمكن الاعتماد على هذه الحاســـبات الآلية في إدارة تلك النظم بصـــورة دائمة ودقيقة، وعن مدى قدرتها في حماية أســـرارنا وخصوصياتنا من الاعتداء ؟

إن الغرض الأســاســي لهذا الفصــل هو التعرض لهذا الموضــوع الهام وتلخيص آراء ومقترحات بعض ذوي الخبرة في تصميم الطرق العلمية التي تساعد في رفع كفاءة الأمنية، ومن ثم كفاءة النظم الآلية للمعلومات.

تحليل العوامل المهددة لامن الانظمة الالية للمعلومات:

بناء على مسح إحصائي عن حوادث امن المعلومات في النظم الآلية اعد من قبل الحكومة الأمريكية وجد إن العوامل المؤثرة وتأثير كل عامل هي على النحو التالي:

أ: الأفعال غير المقصودة وتمثل ٥٠% من نسبة الحوادث في امن المعلومات.

ب: عدم أمانة العاملين في الحاسب الآلي وتمثل ١٥-٢٠% من نسبة الحوادث.

ج: الابتزاز والضغط ألمطلبي وتمثل ١٠% من الحوادث..

د: المياه والسوائل وعدم الالتزام بالمواصفات البيئية وتمثل ١٠%.

ه: الاعتداء الخارجي لا يتجاوز ٥%

و: الكوارث الطبيعية والحريق ويمثل ١٠%.

من هذا يتضح إن العوامل الثلاثة الأولى أي تلك التي مصدرها الأفراد المتعاملين مع الحاسب الآلي قد تسببت في ٨٠% من جملة الحوادث المهددة لأمن المعلومات في حين إن العوامل التي لا يدخل فيها العامل البشري لا تتعدى ٢٠% وان تأثير العامل البشري الخارجي لا يتجاوز الـــ ٥% مما يشير إلى تركيز المشكلة في الأفراد المتعاملين مع الحاسب الآلي وسينظر إلى كل تلك العوامل نشئ من التفصيل في الأسطر التالية:

أ : افعال المتعاملين غير المقصودة والمهددة لامن المعلومات:

إن الأفعال غير المقصودة التي تؤدي إلى تسرب معلومات إلى جهات غير ذات صلاحية أو فقد ومسح معلومات هامة أو تغير في معلومات أو غير ذلك من مشاكل امن المعلومات تكون في الغالب نتيجة إلى ضغط شديد في العمل أو ضعف في القدرات الذاتية في الانضباط والاهتمام لدى المشغلين والمستخدمين.

فالتسرب غير المقصود للمعلومات يتم مثلا عن طريق إرسال تقارير بالخطأ غير المقصود أو نسيان إغلاق الشاشات فتبقى مفتوحة وهي عارضة لبيانات غير مسموح بعرضها أو استخدام أوراق الحاسب الآلي التالفة والتي تحتوي على بعض المعلومات الهامة في ملف الحاجيات أو وضع كلمة السر في مكان يسهل معرفتها فيه أو نتيجة لمشاكل في الأجهزة أو البرامج.

أما المسح غير المقصود فيتم في الغالب بعمل تنظيم المجاري عن طريق الخطأ لقرص يحتوي على معلومات هامة أو الكتابة على سجلات تحتوي على معلومات أو نقل الملف إلى مساحة تالفة في القرص، أو نتيجة لمشاكل في الأجهزة أو البرامج.

أما تغيير البيانات فاهم مسبباته هو الخطأ غير المقصود عند إدخال وتعديل البيانات.

ب: افعال المتعاملين المقصودة والمهددة لأمن المعلومات:

تشمل الأفعال المقصودة بواسطة المتعاملين مع النظام معالجة محرفة أو تشغيل محرف للبرنامج أو الاطلاع الشخصي، أو إطلاع الآخرين لبيانات غير مسموح الاطلاع عليها، أو نقل بعض البرامج والبيانات الخاصة أو تدمير برنامج أو معلومة أو غير ذلك من الأفعال المقصودة و المهددة لأمن المعلومات.

أما الأفعال ففي الغالب ما يحاول الفاعل فعلها بإدخال ضمن الأفعال غير المقصود حتى تختفي الأغراض الخيانية فيها.

عند تحليل الدوافع التي تؤدي إلى خيانة المتعاملين مع النظام نجدها تتدرج من الخيانة العظمى وخدمة دولة محاربة بدافع اعتقادي أو سياسي أو مادي إلى خدمة مؤسسة أخرى منافسة بدافع مادي أو انتقامي إلى خدمة أفراد بتمليكهم معلومات عن أفراد آخرين منافسين بدافع مادي أو دافع صداقة أو خدمات ذوي القربى أو أصدقاء بتحسين بيانات تخصهم إلى الانتقام من زملاء أو غيرهم بدوافع وهو أدنى درجة من حيث الخطورة.

ج: الابتزاز والضغط المطلبي:

لاشك إن من أهم مميزات الآلية هو تقليص الاعتماد على الإنسان الذي هو معرض للتوقف من العمل لأسباب صحية أو طبيعية أو بدافع تحسين واقعه المعيشي بترك العمل والانتقال إلى جهة أخرى أو عن طريق الوسائل النقابية المعروفة.

وان كنا بالإلية قد تخلصنا لحد كبير من هذا النوع من المشاكل إلا أننا في الجانب الأخر لابد إن نكون في اشد الحذر من أننا سنكون تحت هيمنة تقصير المشرفين على مركز الحاسب الآلي، وربما يكون هذا التقصير مقصود لأحدى الدوافع التي ذكرناها في تحليل الأعمال المقصودة والمؤثرة في امن المعلومات أو غير مقصودة للأسباب التي ذكرناها في إعمال غير العاملين في الحاسب الآلي أي دور في هذه الحوادث كأن يحدث انفجار في مواسير المياه أو نظام مياه وإطفاء الحريق لأسباب مجهولة أو تحت ذبذبة كهربية عالية جدا لعطب مفاجئ في نظام الكهرباء المركزي.

هـ: الاعتداء الخارجي:

ونعني بالاعتداء الخارجي إن يتمكن شخص من غير المتعاملين مع النظام من الإطلاع أو تغيير أو مسح أو سرقة بعض أو كل معلومات النظام، وان كان هذا النوع من الحوادث لا يزيد على ٥% من جملة الحوادث المهددة لأمن أنظمة المعلومات لكن في حالة الحاسبات الشخصية والتي عم انتشارها في هذا العقد فصارت تعتمد عليها كثير من المؤسسات الصغيرة خاصة في نظم الأعمال المكتبية ربما تزيد هذه النسبة كثيرا كما أشارت دراسات أخرى في هذا المجال وذلك لسهولة حملها وتشغيلها.

و: الكوارث الطبيعية والحريق:

إن الكوارث الطبيعية والحريق يمثلان تهديدا امنيا لكل الأنظمة وليس لأنظمة المعلومات وحدها، لكن ذلك التهديد الأمني ربما يكون اقل خطورة وأيسر معالجة في الأنظمة الآلية للمعلومات حيث المرونة في خزن ومناقلة وإمكانية وجود نسخ مسندة للبرامج والبيانات في أماكن بعيدة ومتعددة.

خطط الطوارئ:

لابد من وضع الخطط لاستمرارية عمل النظام في حالة المشاكل الكبيرة كتعطل الحاسب الآلي تعطلا طويلا أو غير ذلك من الحالات الطارئة لابد من قياس المشاكل التي سيواجهها مستخدم النظام في هذه الحالات ووضع البدائل على ضوء ذلك فمثلا في النظم المصرفية أو نظم الحجوزات الجوية حيث لا غنى عن الحاسب الآلي ولو بضع دقائق يستوجب وجود نظام مساند يعمل بطريقة فورية في حالة الطوارئ في حين إن هناك أنظمة أخر يمكنها الاستغناء عن الحاسب الآلي عدة أيام دون إن تتأثر تأثرا كبيرا. هذا من ناحية الاستمرار التشغيلي المباشر للحاسب الآلي أما النواحي الأخرى الهامة غير المباشرة أو المساندة كالكهرباء المستمرة والثابتة أو التبريد الموزون المستمر فهي ضرورية للتشغيل الخالي من الأخطاء إذ إن الزيادة الشديدة في التيار الكهربائي والارتفاع غير المحتمل في درجات الحرارة كلها تؤدي إلى أخطاء في تشغيل ومعالجة البيانات. كذلك يجب مراعاة إن الانقطاع المفاجئ للتيار والإطفاء المباشر للحاسب الآلي كثيرا ما يؤدي إلى فقد بعض المعلومات أو السجلات.

الامن الفيزيائي لمركز المعلومات والحاسب الالي:

يشمل الأمن الفيزيائي بمركز المعلومات والحاسب الآلي حمايته من الحريق والسوائل والغبار والكهرواستاتيكا وكذلك ضمان الكهرباء الكافية والمستلزمات البيئية من حرارة ورطوبة موزونة إضافة إلى التحكم في زيارة ودخول الأفراد إلى المبنى أو المكاتب أو إلى المكاتب الحساسة أو إلى مكتبات المراجع والأشرطة والأقراص ووثائق النظام أو إلى صالة الحاسب الآلي أو إلى طرفية المشغل أو إلى مفاتيح التبريد، كذلك التحكم في الوصول إلى المراكز الفرعية للطرفيات أو خطوط الاتصال أو غيرها من الأشياء المؤثرة في امن النظام الآلي للمعلومات.

د: مراقبة الأفراد:

يمثل الأفراد خط الدفاع الرئيسي في امن المعلومات خاصة المتعاملين مع النظام كما اشرنا سابقا.

فامن الأنظمة الآلية للمعلومات يعتمد أولا وأخيرا على أمانة الأفراد المتعاملين معها فلا يكفي التأكد من أخلاقيات الموظف وأهليته عند تعيينه بل يجب إن تستمر مراقبته لان التغيير السلوكي متوقع في أي وقت كذلك يجب عدم الاعتماد على موظف واحد بأي حال من الأحوال وان كان لابد من ذلك فيجب إن يشمل ذلك الموظف إشرافا ومراقبة دقيقة وتوثيقا دقيقا لأعمال وتدريب مساعدين لهم. عند انتهاء خدمات أي موظف يجب سحب صلاحيته قبل فترة كافية فهناك عدة حوادث انتقام من موظفين أنهيت خدماتهم.

هـ: الصيانة والتامين:

تعتبر الصيانة خط الدفاع الثاني في امن الأنظمة الآلية للمعلومات ووجود الصيانة ضمان للتشغيل المستمر للأنظمة كما إن التامين التجاري يغطي تكلفة إرجاع المعلومات المفقودة وتغطية الخسارة الناتجة عن تعطيل النظام إضافة لتغطية الأجهزة إذا لم تغطى بواسطة عقود الصيانة.

و:- مراقبة المعالجة:

نعني بمراقبة المعالجة التأكد من المعالجة الصحيحة (الابتداء الصحيح للتشغيل) سواء كان إدخال أو تعديل أو استفسار ثم التوثق من إن هذه المعالجة تمت بإذن الجهات ذات الصلاحية (صلاحية التشغيل) ثم التأكد من إدخال الحركة هو الإدخال الصحيح وذلك بتكرار الإدخال مثلا وعمل شاشة مختلفة لكل نوع من الإدخال إضافة لذلك لابد إن يكون للنظام خاصية التعرف على الأخطاء والتعرف على عدم الدقة في المعالجة وعمل تقرير بذلك، وأخيرا يجب إن تخدم التقارير المطبوعة أهداف محددة لإدارات محددة كما يجب تجنب الطباعة الزائدة التي قد تؤدي إلى تسرب المعلومات وضياع الورق. كذلك يجب إن تعكس التقارير المطبوعة الأنشطة المختلفة للأنظمة وتمثل بهذه مراجعة غير مباشرة للبيانات والمعالجة وحركة النظام بصفة عامة.

الخلاصة:

نخلص من الفقرات السابقة إن الكفاءة الأمنية أو امن النظم الآلية للمعلومات تعتمد بدرجة عالية تتجاوز الـــ ٨٠% على الأفراد المتعاملين مع تلك الأنظمة وبصـــفة خاصـــة على مدى التزامهم الأخلاقي، ولما كان الالتزام الأخلاقي من المواضـيع الفلسـفية والنظرية المعقدة التي يصـعب التحكم فيها. يصـبح الحل الواقعي هو تقليص الاعتماد على الأفراد والاتجاه نحو الكفاءة الإدارية.

فالتحكم في الآلية وضـمان اسـتمرارية تشـغيلها وحماية مبانيها وبيئتها وغير ذلك مما يعرف بالحماية الفيزيائية أكثر أمكانا وعملا من مراقبة الأفراد وســـلوكياتهم. بالطبع ليس من المعقول التخلص من العامل البشـــري نهائيا لهذا كان مراجعة التزام العاملين بأخلاقيات المهنة من وقت لأخر والتأكد من وجود أفراد مســاندين لهم عدة بدائل في كل عمل من المتطلبات الأساسية في امن النظم الآلية للمعلومات إضافة إلى المراقبة والمراجعة المنتظمة لكل أنشطة النظام.

من أهم شهادات أمن المعلومات

- **CompTIA Security +**

وهي تعتبر من الشهادات التي ينصح بها للمبتدئين في مجال أمن المعلومات وتقدم من شركة CompTIA العالمية وميزتها أن تعطي الأفكار والمفاهيم الأساسية في مجال أمن المعلومات

- **MCSE Security : Security Vendor: Microsoft**

وهي من الشهادات التي تقدمها شركة مايكروسوفت في مجال أمن وحماية المعلومات وهي من الشهادات المرموقة في مجال برمجيات أمن المعلومات في الأنظمة الخاصة بشركة مايكروسوفت.

- **Cisco Certified Network Professional (CCSP Security)**

وهي من الشهادات التي تقدمها شركة سيسكو العريقة والتي تدرب على كيفية تأمين الشبكات ومراكز البيانات التي يتم إنشاءها بالاعتماد على العتاد الذي تقدمه شركة سيسكو وكيفية تأمينها وبناء دائرة شبكة ذات حماية عالية .

- **Certified Ethical Hacker (CEH) Vendor EC-Council**

وهي من الشهادات الأولية التي تثبت مدى قدرة وخبرة الشخص على استخدام الأنظمة والوسائل التي تستخدم في الاختراق والتهكير وهي شهادة الهدف منها أن يكون لدى المتلقي الخبرة بالبرامج والطرق التي يستخدمها الهكر وكيفية تأمين الشبكة منها .

- **Computer Hacking Forensic Investigation**

وهي شهادة موجهه للتحليل الجنائي الرقمي للبيانات ووسائل استعادتها وتحليلها .

بالإضافة للعديد من الشهادات العالمية في مجال أمن المعلومات مثل CCIE و CISSP وغيرها من الشهادات التي الهدف الرئيسي منها التدريب وتوصيل المفاهيم والخبرات في مجال كيفية وضع سياسات وإجراءات أمن المعلومات وكيفية تأمينها وتحديثها والحفاظ عليها من الاختراقات والتهكير .

كيف تحافظ على حماية وأمن معلوماتك ؟

إليك عدة أساسيات:

- **تحديث نظام التشغيل والبرامج بشكل دائم.**

لا تظن ان تحديث نظام التشغيل والبرامج هي مجرد كماليات فقط من اجل الحصول على بعض المزايا الاضافية. فكثيرا ما تكون هاته التحديثات من اجل سد ثغرات امنية.

لذا فيجب عليك تحديث نظامك والبرامج التي تشتغل عليها، وخصوصا برامج الحماية بصفة دورية.

- **لا تقم بمشاركة الملفات عند استخدامك لشبكة خارجية.**

اختراق الجهاز يكون أسهل عندما يتم عبر شبكة خارجية في اماكن عامة كالمدارس، والمقاهي، وغيرها من الاماكن التي توفر امكانية الاتصال بالأنترنت عبر شبكاتها.

ومشاركتك للملفات في هذه الحالة يعتبر مغامرة منك، فاحرص على عدم مشاركة الملفات بين جهازك وجهاز اخر عند استعمالك للشبكات الخارجية.

- **احذر من الرسائل المجهولة.**

التزم الحذر في التعامل مع الرسائل التي تتلقاها عبر بريدك الالكتروني. فقد تكون ملغمة. لذا تجنبها على قدر المستطاع.

- **ابتعد عن صفحات التحميل المجهولة.**

عندما ترغب في تحميل اي برنامج فابحث اولا عن موقعه الرسمي فان تعذر ذلك ، فقم بتحميله من المواقع المشهورة و الموثوقة.

- **تجنب استخدام الكراكات.**

بالإضافة إلى أن استخدامها غير شرعي وفيه قرصنة ومخالفة لسياسة الخصوصية فإنها غالبا ما يتم ارفاق الكراكات ببرمجيات خبيثة، قد تكتشفها برامج الحماية وقد لا تفعل في حال قام الهاكر بتشفيرها .

المراجع /

منظمة أمن المعلومات الدولية ISSA

الدليل الإرشادي لسياسات وإجراءات أمن المعلومات للجهات الحكومية في المملكة العربية السعودية

كتيب حص المستخدم – اصدار مركز التميز لأمن المعلومات بجامعة الملك سعود

أمن المعلومات بلغة ميسرة – اصدار مركز التميز لأمن المعلومات بجامعة الملك سعود