المحاضرة الثالثة: هيكلة نظم المعلومات

ثانيا: أمن المعلومات

إن موضوع الأمن المعلوماتي يرتبط ارتباطا وثيقا بأمن الحاسوب، فلا يوجد أمن للمعلومات إذا لم يراع أمن الحاسوب. وفي ظل التطورات السريعة في العالم التي أثرت على الإمكانيات التقنية المتقدمة المتاحة الرامية إلى خرق منظومات الحاسوب بهدف السرقة او تخريب المعلومات او تدمير أجهز الحاسوب، كان لابد من التفكير الجدي لتحديد الإجراءات الدفاعية والوقائية حسب الإمكانيات المتوفرة لحمايتها من أي اختراق أو تخريب، وكان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها.

1- مفهوم أمن المعلومات

تشكل المعلومات البنية التحتية للمنظمات حيث تمكنها من أداء مهامها، إذ عن نوع المعلومات وكميتها وطريقة عرضها تعد الأساس في نجاح عملية صنع القرارات وعليه يكون للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها.

لذلك عرف الأمن المعلوماتي بأنه: مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات بالإضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال.

كما عرف أيضا بأنه: الحفاظ على المعلومات المتواجدة في نظام معلوماتي من مخاطر التلف الضياع أو من مخاطر الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية. أي محاولة إبقاء معلوماتك تحت السيطرة المباشرة والكاملة – أي عدم إمكانية الوصول إليها من قبل أي شخص دون إذن منك، وأن تكون على علم بالمخاطر المترتبة لشخص ما بالوصول إلى معلوماتك الخاصة.

مما سبق يمكن تعرف الأمن المعلوماتي بأنه ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزنة في أجهزة الحاسوب إضافة إلى الأجهزة الملحقة وشبكات الاتصال والتصدي لمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزنة أو تلك التي ترمي إلى نقل الخزين المعلوماتي لهذه القواعد أو تغييره أو تخريبه.

2- الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات المحوسبة

لقد أصبح اختراق أنظمة المعلومات ونظم الشبكات والمواقع المعلوماتية خطرا يقلق العديد من المؤسسات في السنوات الأخيرة، ولذلك حاولت هذه الأخيرة تحديد طبيعة الأخطار التي يمكن أن تتعرض لها أنظمة معلوماتها والتي يمكن أن تكون مقصودة كسرقة المعلومات أو ادخال الفيروسات وغيرها (والتي قد يكون مصدرها من داخل المؤسسة أو من خارجها)، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية والكوارث الطبيعية.

أ- الأخطاء البشرية: وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام أو في عمليات تحديد الصلاحيات، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن نظم المعلومات في المؤسسات وسلامتها.

ب- الأخطار البيئية: وتشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق...الخ، وتؤدي هذه الأخطار إلى تعطل عمل التجهيزات وتوقفها لفترة طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات.

ج-الجرائم المحوسبة: تمثل هذه الجرائم تحديا كبيرا لما تسببه من خسارة كبيرة ، ويمكن أن تتم هذه الجرائم من قبل أشخاص خارج المنظمة يقومون باختراق الأنظمة (غالبا من خلال الشبكات) أو من قبل أشخاص داخل المنظمة يملكون صلاحيات الدخول إلى النظام ولكنهم يقومون بإساءة استخدام النظام لدوافع مختلفة. وتشير الدراسات التي أجرتها دائرة المحاسبة العامة وشركةOrkand للاستشارات إلى أن الخسائر الناجمة عن جرائم الكمبيوتر تقدر بحوالي 1.5 مليون دولار لشركات المصارف المحوسبة في الولايات المتحدة الأمريكية. فيما قدر المركز الوطني لبيانات جرائم الحاسوب في لوس أنجلوس بأن 70% من جرائم الكمبيوتر حدثت من الداخل(أي من قبل من يعملون داخل المنظمات).

3- مصادر الإخلال بأمن المعلومات

- ✓ الاعتداء على حق الوصول: ويحدث عند تعدي شخص على الحدود التي وضعت للعمل على نظام المعلومات، مما يؤدي إلى احتمال العبث ولو غير المقصود بملفات النظام.
- ✓ دخول شخص غير مصرح له إلى نظام المعلومات باستخدام كلمة سر مستخدم مشروع: مما يتيح تجاوز الحدود في حق الوصول أو زراعة ملفات تجسسية مثل حصان طراودة[1].
- ✓ خداع بروتكولات النقل عبر الانترنت : أي اعتراض البيانات المنقولة عبر الشبكة باستخدام برامج خاصة مثل برامج الاختراق والقرصنة ليتم تعديلها بما يتوافق مع غرض الاعتداء.

[1] يعد حصان طروادة **نوعًا من البرامج الضارة التي تتسلل إلى جهاز الكمبيوتر متنكرة**، لتسبب الفوضى في نظامك. كل نوع له مهمة محددة ليقوم بها، والتي يمكن أن تكون ما يلي:

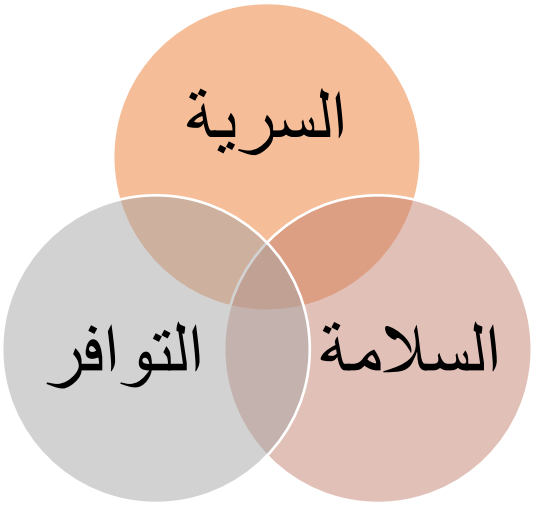
- **التقاط كلمات المرور والتفاصيل الشخصية** للوصول إلى حساباتك.
- **سرقة التفاصيل المصرفية** ومعلومات بطاقة الائتمان.
- **السيطرة على شبكة الكمبيوتر** وإتلاف أو حذف الملفات.
- **جمع المعلومات الشخصية** لسرقة هوية الضحية.
- **فضح التفاصيل السرية** وأسرار حياة الضحية.

- ✓ عدم الإقرار بالقيان بالتصرف: كضياع كلمة السر أو إعطائها لشخص آخر غير مصرح له باستخدام النظام.
- ✓ ارسال كميات كبيرة من الرسائل الالكترونية إلى بريد الموقع المستهدف لإرباك النظام واضعاف برامج الحماية.

4- المبادئ الأساسية لأمن المعلومات:

من أهم مبادئ أمن المعلومات ومنذ أكثر من عشرين عاما هي بالسرية Confidentiality والتكامل Integrity والتوافر Availability (المعروفة باسم الثالوث ((CIA),(أعضاء InfoSec).

الشكل رقم (01) عناصر أمن المعلومات



أ- السرية: وهو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالاطلاع عليها أو الكشف عنها. على سبيل المثال، استعمال بطاقة الائتمان في المعاملات التجارية على شبكة يتطلب إدخال رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الوصول إلى أماكن تخزين أو ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها. أما إذا كان الطرف غير المصرح له قد حصل على رقم البطاقة بأي شكل من الأشكال فإن ذلك يعد انتهاكا لمبدأ السرية في حفظ وتخزين البيانات.

خرق السرية يتخذ أشكالا عديدة. تجسس شخص ما على شاشة الحاسوب لسرقة كلمات سر الدخول، أو رؤية بيانات سرية بدون علم مالكها، يمكن أن يكون خرقا للسرية. إذا كان الحاسوب المحمول

يحتوي على معلومات حساسة عن موظفي المؤسسة، فإن سرقته أو بيعه يمكن أن يسفر عن انتهاك لمبدأ السرية.

ب- التكامل (السلامة): في مجال أمن المعلومات، التكامل (السلامة) يعني الحفاظ على البيانات من التغيير أو التعديل من الأشخاص غير المخولين بالوصول اليها. عندما يقوم شخص، بقصد أو بغير قصد، بحذف أو انتهاك سلامة ملفات البيانات الهامة أو الإضرار بها، وهو غير مخول بذلك، يعد هذا انتهاكا لسلامة البيانات. وعندما يصيب فيروس حاسوبا ويقوم بتعديل بياناته أو يتلفها يعد هذا انتهاكا لسلامة البيانات، وكذلك عندما يكون الموظف (غير المخول) قادرا على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم (غير مصرح له) بتخريب موقع على شبكة الإنترنت. وتعني سلامة البيانات كذلك، أن تكون التغيرات في البيانات مطردة، فعندما يقوم عميل البنك بسحب أو إيداع، ينبغي أن ينعكس ذلك على رصيده في البنك.

إن الإخلال بسلامة البيانات ليس بالضرورة نتيجة عمل تخريبي، فمثلاً الانقطاع في النظام قد ينشئ عنه تغيرات غير مقصودة أو لا تحفظ تغيرات قد تمت فعلاً.

ج- توفر البيانات: يهدف أي نظام للمعلومات لخدمة غرضه، أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن تعمل عناصر النظام الآتية بشكل صحيح ومستمر:

- ✓ الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات.
- ✓ الضوابط الأمنية المستخدمة لحماية النظام.
- ✓ قنوات الاتصال المستخدمة للوصول.
- ✓ نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات.
- ✓ منع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، أو نظام الترقيات والتحديث.
- ✓ ضمان منع هجمات الحرمان من الخدمة.

5- أساليب حماية وأمن المعلومات:

أ- التغلب على المشاكل المرتبطة بالتغذية الكهربائية: مثل استخدام تطبيقات الحفظ التلقائي، تزويد الحاسوب بمنظم التغذية الكهربائية، المولدات الكهربائية.....

ب- التحكم بالوصول: أبسط أنواع الحماية هي استخدام نظام التعريف بشخص المستخدم، موثوقية الاستخدام، ومشروعيته. هذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بالاستخدام. وتضم:

- ✓ كلمات السر بأنواعها.
- ✓ البطاقات الذكية المستخدمة للتعريف.
- ✓ وسائل التعريف البيولوجية والتي تعتمد على سمات الشخص المستخدم المتصلة ببنائه البيولوجي كالبصمة.

- ✓ المفاتيح المشفرة ويمكن أن تشمل ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

ج- جدران النار: وهو برنامج أو جهاز حاسوب يسمح لمستخدمي الحاسوب في المؤسسة بالوصول إلى الانترنت ولكنه يحدد بصرامة إمكانية الغرباء من الوصول إلى البيانات الداخلية، ويمكن بناؤه من خلال البرمجيات أو العتاد الصلب أو بتركيبة من الاثنين معا. (جدار النار لا يحمي من الأخطار الداخلية).

د-التشفير وفك التشفير: وهو عملية تحويل المعلومات إلى نص مخفي لا يمكن فهمه عند نقله على الشبكة، وعملية فك التشفير هي العملية العكسية.

د- الحماية من المخترقين: hachers ، يعدل المخترق الأنظمة للحصول على أعظم أداء ممكن، وأحيانا يحاولون تتبع الضعف والثغرات في أمن النظام.(نادرا ما يخربون البيانات أو يسرقونها لكن تكرار الهجمات يعد مصدر ازعاج للمؤسسة). وللحماية من المخترقين ينصح بـ:

- ✓ إنشاء قاعدة بينات بأسماء احصنة طراودة.
- ✓ تثبيت برنامج مكافحة الفيروسات على الحاسب.
- ✓ إدخال كلمات سر قوية متضمنة تركيبة من الأحرف والأرقام والرموز.
- ✓ تجنب استخدام نفس كلمة المرور لجميع الحسابات.
- ✓ جعل الشبكة اللاسلكية آمنة مما يتطلب ادخال اسم المستخدم وكلمة المرور.

هـ- تثبيت برامج الحماية والأمان: برامج مكافحة الفيروسات[2] بأنها مجموعة البرامج التي صممت خصيصاً للكشف عن الفيروسات وإزالتها من أجهزة الحاسوب، بالإضافة إلى قدرتها على حماية أجهزة الحاسوب من مجموعة متنوعة من التهديدات كبرامج التجسس وبرامج أحصنة طروادة وغيرها من البرامج التي تعرف بالفيروسات، وقد طور العلماء برامج مكافحة الفيروسات في أواخر الثمانينات من القرن المنصرم وقد ازداد هذا التطور نتيجة لزيادة حجم المخاطر التي تهدد الحواسيب، وبعض هذه البرامج مجانية في حين أنّ بعضها الآخر مدفوع الثمن، ولكن تجدر الإشارة إلى أنّ البرامج المدفوعة الثمن من برامج مكافحة الفيروسات هي أكثر فعالية في وقاية الأجهزة وحمايتها. تنتقل الفيروسات إلى أجهزة الحاسوب من خلال عدة طرق:

- ✓ من خلال الإنترنت، حيث يمكن أن يُحمّل المستخدم بعض الملفات التي تحوي الفيروسات.
- ✓ من خلال بعض أجزاء التخزين التي تحتوي على الفيروسات.

---

[2]الفيروس هو برنامج صغير مكتوب بأحد لغات الحاسب ويقوم بإحداث أضرار في الحاسب والمعلومات الموجودة على الحاسب بمعني انه يتركز علي ثلاث خواص وهي التخفي، التضاعف، وإلحاق الأذى. مصادر الفيروس يكمن مصادر الفيروس من خلال الرسائل الإلكترونية المجهولة، صفحات الإنترنت المشبوهة، نسخ البرامج المقلدة، استخدام برامج غير موثقة، كذلك تبادل وسائل التخزين دون عمل فحص مسبق مثل الأقراص والذاكرة المتنقلة وارسال الملفات داخل الشبكة المحلية. للفيروس ثلاث خواص مؤثرة وهي: التضاعف: تتم عملية تضاعف الفيروس عند التحاق الفيروس بأحد الملفات وهنا تتم عملية زيادة عدد العمليات التي تتم إلى ملاين العمليات مما يسبب البطء في العمل أو توقف الحاسب عن العمل. التخفي: لابد للفيروس من التخفي حتى لا ينكشف ويصبح غير فعال، ولكي يتخفى فإنه يقوم بعدة أساليب منها على سبيل المثال، صغر حجم الفيروس لكي سيناله الاختباء بنجاح في الذاكرة أو ملف آخر. إلحاق الأذى: قد يتراوح الأذى الذي يسببه الفيروس بالاكتفاء بإصدار صوت موسيقي أو مسح جميع المعلومات المخزنة لديك، ومن الأمثلة الأخرى في إلحاق الأذى: إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلا أو إلغاء البرنامج المكتوب علىBIOS .

- ✓ من خلال العدوى من أجهزة أخرى حيث يمكن أن تنتقل الفيروسات من جهاز لآخر عبر الشبكات المحلية التي تربط الأجهزة.