

**أمن المعلومات**



**إعداد الطالب:**

**أمن المعلومات**

أمن المعلومات علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجيا ويرتكز أمن المعلومات إلى:-

أنظمة حماية نظم التشغيل

أنظمة حماية البرامج والتطبيقات.

أنظمة حماية قواعد البيانات.

أنظمة حماية الولوج أو الدخول إلى الأنظمة.

**المبادئ الأساسية**

من أهم المفاهيم, ومنذ أكثر من عشرين عاما، وأمن المعلومات قد حددت بالسرية سرية (مبدأ) والتكامل سلامة البيانات والتوافر تواجدية(المعروفة باسم الثالوث (سي آي ايه)(CIA),(أعضاء InfoSec التقليديون الثالوث -السرية والتكامل والتوافر - ويشار إليها بالتبادل في الأدبيات على أنها, سمات أمان، خصائص وأهداف أمنية, جوانب أساسية، معايير معلومات، خصائص معلومات هامة, واللبنات الأساسية.) والمبادئ الأساسية لأمن المعلومات. العديد من المتخصصين في مجال أمن المعلومات يؤمنون إيمانا راسخا بأن المساءلة ينبغي أن تضاف كمبدأ أساسي لأمن المعلومات.

في عام 2002، اقترح دون باركر نموذجا بديلا للثالوث التقليدي (CIA). يتكون نموذج باركر من ستة عناصر من أمن المعلومات. العناصر هي السرية، الحيازة، السلامة، الأصالة، التوفر والأداة. إن سداسي باركر هو موضع نقاش بين المتخصصين في مجال الأمن.

أبسط أنواع الحماية هي استخدام نظام التعريف بشخص المستخدم, وثوقية الاستخدام, ومشروعيته. هذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بالاستخدام. وتضم هذه الطائفة:

كلمات السر بأنواعها.

البطاقات الذكية المستخدمة للتعريف.

وسائل التعريف البيولوجية والتي تعتمد على سمات الشخص المستخدم المتصلة ببنائه البيولوجي.

المفاتيح المشفرة ويمكن ان تشمل ما يعرف بالاقفال الإلكترونية التي تحدد مناطق النفاذ.

إن كل التقنيات التي وصل إليها العالم لا يمكن ان تعيش من دون أمن المعلومات. فعلى سبيل المثال, نظام البنوك لو لم يكن هناك أمن المعلومات لاستطاع أي شخص ان يدخل على النظام ويغير حسابه ويصبح مليونير من لا شيء.

**السرية**

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالأطلاع 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. اماإذا 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 الشركة, فإن سرقته أو بيعه يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر اتصال هاتفي هو انتهاك لمبدأ السرية إذا كان طالب الاتصال غير مخول بأن يحصل على المعلومات.

السرية أمر ضروري (لكنها غير كافية) للحفاظ على خصوصية الناس الذين تحتوي الأنظمة معلوماتهم الشخصية.

**التكامل (السلامة)**

في مجال أمن المعلومات، التكامل (السلامة) يعني الحفاظ على البيانات من التغيير أوالتعديل 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 ، كل ذلك يعد انتهاكا لسلامة البيانات. و تعني 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 مقصودةأو لا تحفظ تغيرات قد تمت فعلاً.

**توفر البيانات**

يهدف أي نظام للمعلومات لخدمة غرضه، أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن تعمل عناصر النظام الآتية بشكل صحيح و مستمر:

الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات.

الضوابط الأمنية المستخدمة لحمايتة 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، اونظام الترقيات والتحديث.

ضمان منع هجمات الحرمان من الخدمة.

**إدارة المخاطر**

والمعالجة الشاملة لموضوع إدارة المخاطر هو خارج عن نطاق هذا المقال. ومع ذلك، سوف تقدم تعريفا مفيدا لإدارة المخاطر تكون كذلك بعض المصطلحات الأساسية ويشيع استخدامه في عملية إدارة المخاطر.

ينص التعريف التالي لإدارة المخاطر : "إدارة المخاطر هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المنظمة أو الشبكة المعلوماتية في تحقيق الأهداف التجارية أو الاخرى، والحد والتقليل من نقاط الضعف إن وجدت، لتأخذ في الحد من المخاطر إلى مستوى مقبول، على أساس قيمة موارد المعلومات إلى المنظمة. "

هناك أمران في هذا التعريف قد يحتاجان إلى بعض التوضيح. أولا، عملية إدارة المخاطر هي تكرار العمليات الجارية ويجب أن يتكرر إلى ما لا نهاية لان بيئة العمل المتغيرة باستمرار، والتهديدات الجديدة والضعف تظهر كل يوم. والثانية اختيار التدابير المضادة (الرقابة) المستخدمة لإدارة المخاطر يجب أن توازن بين الإنتاجية، والتكلفة، وفعالية التدابير المضادة، وقيمة الموجودات وحماية البيانات.

الخطر هو احتمال أن شيئا ما سيئا سيحدث يسبب الأذى لأحد الأصول المعلوماتية (أو الخسارة في الأصول). الضعف هو الضعف الذي يمكن أن يستخدم لتعريضها للخطر أو التسبب في ضرر لأحد الأصول المعلوماتية. التهديد أي شيء فعل (من صنع الإنسان او فعل من أفعال الطبيعة) لديه القدرة على التسبب في ضرر.

احتمال أن يشكل تهديدا سوف تستخدم من التعرض للضرر يتسبب في خطر. عندما لا يشكل تهديدا استخدام الضعف لإلحاق الاذى، لما له من أثر. في سياق أمن المعلومات، وأثر هو خسارة لتوافر والنزاهة والسرية، وربما غيرها من الخسائر (الدخل المفقود، والخسائر في الأرواح وخسائر في الممتلكات العقارية). وتجدر الإشارة إلى أنه ليس من الممكن تحديد جميع المخاطر، ولا هو ممكن القضاء على جميع المخاطر. المخاطر المتبقية تسمى المخاطر المتبقيه.

**تقييم المخاطر**

السياسة الأمنية.

تنظيم أمن المعلومات،

إدارة الأصول.

امن الموارد البشرية.

الجسدية الأمن البيئي.

الاتصالات وإدارة العمليات،

التحكم في الوصول.

اقتناء نظم المعلومات وتطويرها وصيانتها أو ما يسمى ب التحديث،

أمن المعلومات إدارة الحادث.

إدارة استمرارية الأعمال

التوافق التنظيمي.

**إدارة المخاطر**

تتألف عملية إدارة المخاطر من:

.تحديد الموجودات وتقدير قيمتها. تشمل ما يلي: الأفراد والمباني والأجهزة والبرامج والبيانات (الإلكترونية والمطبوعة وغيرها)، واللوازم.

.إجراء تقييم التهديد. وتشمل: أفعال الطبيعة، أعمال الحرب والحوادث والأفعال الضارة القادمة من داخل أو خارج المنظمة.

.إجراء تقييم الضعف، ولكل الضعف، وحساب احتمال أن يكون للاستغلال. تقييم السياسات والإجراءات والمعايير، والتدريب، الأمن المادي، مراقبة الجودة والأمن التقني.

.في حسبانها تأثير كل ذلك من شأنه أن يكون خطرا على كل الموجودات. استخدام التحليل النوعي أو التحليل الكمي.

.تحديد واختيار وتطبيق الضوابط المناسبة. تقدم ردا متناسبا. النظر في الإنتاجية، وفعالية التكاليف، وقيمة الموجودات.

.تقييم فعالية تدابير المكافحة. ضمان توفير الضوابط اللازمة لحماية فعالة من حيث التكلفة دون فقدان ملحوظ في الإنتاجية.

عند أي خطر معين، يمكن أن تختار الإدارة التنفيذية قبول المخاطرة استنادا إلى انخفاض القيمة النسبية للموجودات، وتواتر حدوث منخفضة نسبيا، وأثر انخفاض نسبي على الأعمال التجارية. أو، قد تختار القيادة التخفيف من المخاطر من خلال تحديد وتنفيذ تدابير الرقابة المناسبة للحد من المخاطر. في بعض الحالات، يمكن أن يكون خطر نقل إلى آخر أعمال التأمين عن طريق شراء أو التسنيد إلى آخر الأعمال. قد واقع بعض المخاطر يمكن الجدال فيها. في مثل هذه الحالات قد تختار القيادة إنكار المخاطر. هذا هو في حد ذاته يشكل خطرا محتملا

**اعتماد وتدقيق أمن المعلومات**

أصبحت النظم المعلوماتية وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات. حيث أصبح من المهم الحفاظ على أمن المعلومات بعناصره الرئيسية الثلاث: السرية والصوابية والاستمرارية. وعلى المستوى العالمي يبرز نظام الأيزو للاعتماد والتقييم والتقييس 27001 لضمان أمن المعلومات. كما يوجد نظام HIPAA في الولايات المتحدة الأمريكية لضمان أمن المعلومات الصحية ونظام COBIT من ISACA لأمن المعلومات.

**الضوابط**

عندما تختار الإدارة للتخفيف من المخاطر، فإنها تفعل ذلك من خلال تنفيذ واحد أو أكثر من ثلاثة أنواع مختلفة من الضوابط.

**الإدارية**

الرقابة الإدارية (وتسمى أيضا الضوابط الإجرائية) تتألف من الموافقة الخطية والسياسات والإجراءات والمعايير والمبادئ التوجيهية. الرقابة الإدارية تشكل إطارا لإدارة الأعمال التجارية وإدارة الأفراد. إنها إطلاع الناس على كيفية عمل ما وهو كيفية تشغيل العمليات اليومية وكيف يجب أن تجرى. القوانين واللوائح التي أنشأتها الهيئات الحكومية هي أيضا نوع من الرقابة الإدارية لأنها أبلغ الأعمال. بعض قطاعات الصناعة والسياسات والإجراءات والمعايير والمبادئ التوجيهية التي يجب اتباعها—الدفع صناعة بطاقات) معيار أمن البيانات المطلوبة من قبل تأشيرة الدخول وماستر كارد هو مثال على ذلك. ومن الأمثلة الأخرى على ضوابط إدارية وتشمل الشركات السياسة الأمنية، سياسة كلمة السر، سياسات التوظيف، والسياسات التأديبية.

الرقابة الإدارية تشكل أساسا للاختيار وتنفيذ الضوابط المنطقية والفيزيائية. الضوابط المنطقية والفيزيائية هي مظاهر الرقابة الإدارية. الضوابط الإدارية لها أهمية قصوى.

**منطقي**

الضوابط المنطقية (وتسمى أيضا الضوابط التقنية) استخدام البرمجيات والبيانات لرصد ومراقبة الوصول إلى نظم المعلومات والحوسبة. على سبيل المثال :كلمات السر، والجدران النارية، وكشف التسلل، قوائم التحكم بالولوج، وتشفير البيانات والضوابط المنطقية.

رقابة هامة من المنطقي أن يتم التغاضي عن كثير من الأحيان هو مبدأ الامتيازات الأقل. مبدأ الامتيازات الأقل يتطلب أن الفرد أو برنامج أو عملية النظام لا يتم منح أي امتيازات وصول أكثر من ضرورية لأداء المهمة. وثمة مثال صارخ على عدم التقيد بمبدأ الأقل امتياز هو تسجيل الدخول إلى ويندوز المستخدم المسؤول لقراءة البريد الإلكتروني وتصفح الإنترنت. انتهاكات من هذا المبدأ يمكن أن يحدث أيضا عند الفرد بجمع امتيازات الوصول إضافية بمرور الوقت. هذا يحدث عندما العمال تغيير واجبات العمل، أو أنهم ترقيته إلى منصب جديد، أو أنهم نقل إلى قسم آخر. امتيازات الوصول التي تتطلبها مهامهم الجديدة كثيرا ما أضيف على امتيازاتها وصول القائمة بالفعل والتي قد لا تكون ضرورية أو مناسبة.

**المادية**

الضوابط المادية رصد ومراقبة البيئة في مكان العمل ومرافق الحوسبة. كما رصد ومراقبة الدخول والخروج من هذه المرافق. على سبيل المثال الأبواب والأقفال، والتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق ونظم إخماد الحريق، والكاميرات، ووضع المتاريس، والمبارزة، وحراس الأمن، وتأمين الكابلات، وما إلى ذلك فصل الشبكة، ومكان العمل في مجالات وظيفية هي أيضا الضوابط المادية.

رقابة هامة المادية التي كثيرا ما يتم تجاهلها في الفصل بين الواجبات. الفصل بين الواجبات ويضمن أن الفرد لا يستطيع إكمال المهمة الحاسمة بنفسه. على سبيل المثال : الموظف الذي يقدم طلبا لسداد لا ينبغي أيضا أن يكون قادرا على أن يأذن بدفع أو طباعة الشيك. مبرمج تطبيقات لا ينبغي أن يكون أيضا مسؤول الملقم أو مدير قاعدة البيانات—هذه الأدوار والمسؤوليات يجب أن تكون مفصولة عن بعضها البعض

**شهادات لخبراء أمن المعلومات**

تعد CISA مدقق نظم المعلومات المعتمد أحد أبرز الشهادات في إدارة وتدقييق النظم المعلوماتية. كما تعتبر شهادة CISSP خبير أمن معلومات معتمد شهادة مهمة في أمن المعلومات. كما توجد شهادات متخصصة في أغلب الشركات الكبيرة لتخصص أمن المعلومات مثل ميكرسوفت وسن وسيسكو وغيرها من الشركات.

**مهددات امن المعلومات**

الفيروسات

الفيروس هو برنامج صغير مكتوب بأحد للغات 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، كذالك 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 يتخفي فأنة يقوم بعدة أساليب منها علي 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 الاخري في إلحاق الأذى: إلغاء بعض ملفات النظام، إغلاق الحاسب من تلقاء نفسه عند الدخول على الإنترنت مثلا أو إلغاء البرنامج المكتوب على BIOS.

**هجوم تعطيل الخدمة**

هذا النوع من الخدمة يقوم فيه القرصان أو المعتدي بإجراء أعمال خاصة تؤدي إلى تعطيل الأجهزة التي تقدم الخدمة Server في الشبكات.

**مهاجمه المعلومات المرسلة**

هو اعتراض المعلومات عند ارسالها من جهة إلى أخرى، ويحدث هذا التعامل غالباً أثناء تبادل الرسائل خلال الشبكات:

الإنترنت

الشبكات التي تستخدم شبكة الهاتف العامة

**هجوم السيطرة الكاملة**

في هذا النوع يقوم القرصان بالسيطرة الكاملة على جهاز الضحية والتحكم في جميع ملفاته كما لو كانت في جهازه هو ويمكن للقرصان مراقبة الضحية بصورة كاملة. يتم الهجوم بعد أن يضع القرصان ملف صغير على جهاز الضحية (عن طريق البريد الإلكتروني أو أي وسيلة أخرى) أو عن طريق استغلال نقاط الضعف في أنظمة التشغيل.

**هجوم التضليل**

وفيه يقوم القرصان بانتحال شخصية موقع عام. كما يمكن للقرصان أن ينتحل شخصية مستخدم موثوق به للحصول على معلومات غير مصرّحة له.

**الوصول المباشر لكوابل التوصيل**

يقوم المهاجم بالوصول المباشر لأسلاك التوصيل والتجسس على المعلومات المارة. ولكنه هجوم صعب ويتطلب عتاد خاص.

**طرق وأدوات لحماية أمن المعلومات**

التأمين المادي للأجهزة والمعدات.

تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.

تركيب أنظمة كشف الاختراق وتحديثها.

تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.

عمل سياسة للنسخ الاحتياطي.

استخدام أنظمة قوية لتشفير المعلومات المرسلة.

دعم أجهزة عدم انقطاع التيار.

نشر التعليم والوعي الأمني.