مـا المقصـود بأمــن المعلومات Information Security

أمن المعلومات هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن انشطة الاعتداء عليها . ومن زاوية تقنية ، هو الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية .

واستخدام اصطلاح أمن المعلومات في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال ، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات- وتحديدا الإنترنت – احتلت ابحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة .

عناصر أمن المعلومات

1- **السرية أو الموثوقية CONFIDENTIALITY** :
وتعني التأكد من ان المعلومات لا تكشف ولا يطلع عليها من قبل اشخاص غير مخولين بذلك .

2- **التكاملية وسلامة المحتوى INTEGRITY :**
التأكد من ان محتوى المعلومات صحيح ولم يتم تعديله او العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او العبث به في اية مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع .

3- **استمرارية توفر المعلومات او الخدمة AVAILABILITY** :
التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض الى منع استخدامه لها او دخوله اليها .

4- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation :**
ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل بالمعلومات او مواقعها انكار انه هو الذي قام بهذا التصرف ، بحيث تتوفر قدرة اثبات ان تصرفا ما قد تم من شخص ما في وقت معين .

هل تحتاج اية معلومات عناصر الحماية ذاتها وبذات القدر ؟؟

ليس كل المعلومات تتطلب السرية وضمان عدم الافشاء ، وليس كل المعلومات في منشأة واحدة بذات الاهمية من حيث الوصول لها او ضمان عدم العبث بها ، لهذا تنطلق خطط أمن المعلومات من معرفة :-

ما الذي نريد ان نحميه - بجب تصنيف البيانات والمعلومات من حيث اهمية الحماية ، اذ تصنف المعلومات تبعا لكل حالة على حده ، من معلومات لا تتطلب الحماية ، الى معلومات تتطلب حماية قصوى

ما هي المخاطر التي تتطلب هكذا حماية- وتبدا عملية تحديد المخاطر بتصور كل خطر قد يمس المعلومات محل الحماية او يهدد امنها ، ابتداء من قطع مصدر الكهرباء عن الكمبيوتر وحتى مخاطر اختراق النظام من الخارج بواحد او اكثر من وسائل الاختراق عبر نقاط الضعف ، مرورا باساءة الموظفين استخدام كلمات السر العائدة لهم ، ويصار الى تصنيف هذه المخاطر ضمن قوائم تبعا لاساس التصنيف ، فتصنف كمخاطر من حيث مصدرها ومن حيث وسائل تنفيذها ، ومن حيث غرض المتسببين بهذه المخاطر ، ومن حيث اثرها على نظام الحماية وعلى المعلومات محل الحماية. وهو ما سنقف لاحقا عليه بشكل تفصيلي . ومتى ما تم الانتهاء من هذا التحديد يجري الانتقال الى التساؤل التالي .

وسائل الحماية - كل منشاة وكل هيئة طريقتها الخاصة في توفير الأمن من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات المخصوصة التي تم تحديدها وبحدود امكاناتها المادية والميزانية المخصصة للحماية ، فلا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغا بها الى حد يؤثر على عنصر الأداء في النظام محل الحماية ، اذ لو تصورنا شخصا أراد حماية النقود الموجودة في منزله ، فانه من المقبول وضعها مثلا في قاصة حديدية ووضع حديد حماية مثلا على نوافذ المنزل ، او وضع جرس إنذار لأي اقتحام للمنزل وربما يمكن قبول هذه الوسائل الثلاث لتوفير الأمن من انشطة سرقة هذا المال . لكن ليس منطقيا بل مبالغا فيه ان يحمي هذا الشخص ماله بان يضع حراسا (أشخاصا) على منزله ، ويضع صواعق كهربائية على الأسوار الخارجية ، ومن ثم يضع حديد حماية على الأبواب والنوافذ ، ويضيف الى ذلك جرس إنذار لكل نقطة في المنزل ، فإذا ما دخلنا الى المنزل وجدنا كاميرات مراقبة عند كل نقطة ، ووجدنا بعدها ان الغرفة التي تحتوي القاصة الحديدية لا يسمح بالدخول اليها الا بعد تجاوز إجراءات تعريف خاصة كبطاقة تعريف او رقم سري على الأقفال او غير ذلك ، فإذا ما دخلنا الغرفة وجدنا اننا لسنا امام قاصة حديدية عادية ، وانما خزانة حفظ تفتح بقفل وقتي او ساعة وقتية ، او تفتح بمفتاحين او اكثر وبارقام سرية متعددة او غير ذلك من انماط القاصات المعقدة بل ووجدنا ان فتحها يتطلب ابتداء إلغاء جرس إنذار خاص بالقاصة نفسها . ان هكذا حماية لا يمكن ان تكون مقبولة ، لأنها ببساطة تجعل عملية حصول الشخص نفسه على بعض المال من بين نقوده عملية معقدة قد تدفعه لاحقا الى إهمال كل إجراءات الأمن هذه فيكون اكثر عرضة للسرقة من غيره ، وهذا ما نسميه التأثير على صحة الأداء وفعاليته . وفي بيئة المعلومات ، فمن الطبيعي مثلا ان نضع على جهاز الكمبيوتر الشخصي كلمة سر للولوج الى الملفات الهامة او حتى للنظام كله وان لا نعطي الكلمة لاحد ، وان نضع برنامجا او اكثر لمقاومة الفيروسات الإلكترونية الضارة ، ونراعي إجراءات مقبولة في حماية الدخول الى شبكة الإنترنت والتأكد من مصدر البريد الإلكتروني مثلا . فإذا كان الكمبيوتر خاص بدائرة او منشاة ويضم بيانات هامة ومصنف انها سرية ، كان لزاما زيادة إجراءات الأمن ، فمثلا يضاف للنظام جدران نارية تحد من دخول اشخاص من الخارج وتمنع اعتداءات منظمة قد يتعرض لها النظام او الموقع المعلوماتي ، واذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الافشاء ، تكون تقنيات التشفير مطلوبة بالقدر المناسب . لكن لا يقبل مثلا على جهاز كمبيوتر خاص غير مرتبط بشبكة عامة ان توضع أنواع متعددة من الجدران النارية ، او ان يوضع على أحد مواقع الإنترنت وسائل تعريف متعددة لشخص المستخدم ، ككلمة السر والبصمة الإلكترونية والبصمة الصوتية ، وان يخضع نظام الموقع الى عدد مبالغ به من الفلترات والجدران النارية ، وتشفير طويل المدى لكافة البيانات الموجودة عليه والمتبادلة عبره ، وأيضا لا يقبل موقع أمني يضم بيانات سرية للغاية مجرد الاقتصار على كلمة سر للدخول للنظام . بمعنى ان إجراءات الحماية تنطلق من احتياجات الحماية الملاءمة ، فان زادت عن حدها أمست ذات اثر سلبي على الأداء ، فاصبح الموقع او النظام بطيئا وغير فاعل في أداء مهامه الطبيعية ، وان نقصت عن الحد المطلوب ، ازدادت نقاط الضعف واصبح اكثر عرضة للاختراق الداخلي والخارجي . فإذا فرغنا من اختيار وسائل الحماية التقنية واستراتيجياتها الإدارية والادائية الملائمة ، انتقلنا بعدئذ الى التساؤل الاخير.

مواطف المخاطر والاعتداءات في بيئة المعلومات

1 - **الأجهـــزة** :- وهي كافة المعدات والادوات المادية التي تتكون منها النظم ، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها .

2 - **البرامـــج :-** وهي الاوامر المرتبة في نسق معين لانجاز الاعمال ، وهي اما مستقلة عن النظام او مخزنة فيه .

3 - **المعطيـات :-** ا وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها ، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم . والمعطيات قد تكون في طور الادخال او الاخراج او التخزين او التبادل بين النظم عبر الشبكات ، وقد تخزن داخل النظم او على وسائط التخزين خارجه .

4 - **الاتصـالات :-** وتشمل شبكات الاتصال التي تربط اجهزة التقنية بعضها بعض محليا ونطاقيا ودوليا ، وتتيح فرصة اختراق النظم عبرها كما انها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي.

ومحور الخطر ، الانسان ، سواء المستخدم او الشخص المناط به مهام تقنية معينة تتصل بالنظام ، فادراك هذا الشخص حدود صلاحياته ، وادراكه اليات التعامل مع الخطر ، وسلامة الرقابة على انشطته في حدود احترام حقوقه القانونية ، مسائل رئيسة يعنى بها نظام الأمن الشامل ، تحديدا في بيئة العمل المرتكزة على نظم الكمبيوتر وقواعد البيانات

عمليات متصلة بأمن المعلومات

تصنيف المعلومات Information classification :-

وهي عملية اساسية لدى بناء أي نظام او في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشاة مدار البحث ، فمثلا قد تصنف المعلومات الى معلومات متاحة ، وموثوقة ، وسرية ، وسرية للغاية او قد تكون معلومات متاح الوصول اليها واخرى محظور التوصل اليها وهكذا .

التوثيق Documentation :-

وتتطلب عمليات المعلومات اساسا اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها . وبشكل رئيس فان التوثيق لازم وضروري لنظام التعريف والتخويل ، وتصنيف المعلومات ، والانظمة التطبيقية . وفي اطار الأمن ، فان التوثيق يتطلب ان تكون استراتيجية او سياسة الأمن موثقة ومكتوبة وان تكون إجراءاتها ومكوناتها كاملة محل توثيق ، اضافة الى خطط التعامل مع المخاطر والحوادث ، والجهات المسؤولة ومسؤولياتها وخطط التعافي وادارة الازمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر .

المهام والواجبات الإدارية والشخصية Administration and Personnel Responsibilities :-

ان مهام المتصلين بنظام أمن المعلومات تبدأ في الاساس من حسن اختيار الافراد المؤهلين وعمق معارفهم النظرية والعملية ، على ان يكون مدركا ان التأهيل العملي يتطلب تدريبا متواصلا ولا يقف عند حدود معرفة وخبرة هؤلاء لدى تعيينهم ، وبشكل رئيس فان المهام الإدارية او التنظيمية تتكون من خمسة عناصر او مجموعات رئيسة :- تحليل المخاطر ، وضع السياسة او الاستراتيجية ، وضع خطة الأمن ، وضع البناء التقني الامني – توظيف الاجهزة والمعدات والوسائل ، واخيرا تنفيذ الخطط والسياسات .

وسائل التعريف والتوثق من المستخدمين وحدود صلاحيات الاستخدام
Identification and Authorization :-

ان الدخول الى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية عموما ، يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام ، وهو ما يعرف بأنظمة التعريف والتخويل Identification and Authorization systems. والتعريف او الهوية مسالة تتكون من خطوتين ، الأولى وسيلة التعريف على شخص المستخدم ، والثانية قبول وسيلة التعريف او ما يسمى التوثق من صحة الهوية المقدمة .

ووسائل التعريف تختلف تبعا للتقنية المستخدمة ، وهي نفسها وسائل أمن الوصول الى المعلومات او الخدمات في قطاعات استخدام النظم او الشبكات أو قطاعات الاعمال الإلكترونية ، وبشكل عام ، فان هذه الوسائل تتوزع الى ثلاثة أنواع :-

1 - شئ ما يملكه الشخص مثل البطاقة البلاستيكية او غير ذلك .
2 – شئ ما يعرفه الشخص مثل كلمات السر او الرمز او الرقم الشخصي غير ذلك
3– شيء ما يرتبط بذات الشخص او موجود فيه مثل بصمة الاصبع او بصمة العين والصوت وغيرها .

وتعد وسائل التعريف والتوثق الاقوى ، تلك الوسائل التي تجمع بين هذه الوسائل جميعا على نحو لا يؤثر على سهولة التعريف وفعاليته في ذات الوقت .

وايا كانت وسيلة التعريف التي سيستتبعها توثق من قبل النظام authentication ، فانها بذاتها وبما ستصل باستخدامها تخضع لنظام أمن وارشادات امنية يتعين مراعاتها ، فكلمات السر على سبيل المثال ، وهي الاكثر شيوعا من غيرها من النظم ، تتطلب ان تخضع لسياسة مدروسة من حيث طولها ومكوناتها والابتعاد عن تلك الكلمات التي يسهل تخمينها او تحريها وكذلك خضوع الاستخدام لقواعد عدم الاطلاع وعدم الافشاء والحفاظ عليها.
ومتى ما استخدمت وسائل تعريف ملائمة لاتاحة الوصول للنظام ، ومتى ما تحققت عملية التوثق والمطابقة والتأكد من صحة التعريف (الهوية) فان المرحلة التي تلي ذلك هي تحديد نطاق الاستخدام Authorization وهو ما يعرف بالتخويل او التصريح باستخدام قطاع ما من المعلومات في النظام ، وهذه المسالة تتصل بالتحكم بالدخول او التحكم بالوصول الى المعلومات او اجزاء النظام Access Control system .

عمليات الحفظ Back-up :-
وعمليات الحفظ تتعلق بعمل نسخة إضافية من المواد المخزنة على إحدى وسائط التخزين سواء داخل النظام او خارجه ، وتخضع عمليات الحفظ لقواعد يتعين ان تكون محددة سلفا وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية .

ويمثل وقت الحفظ ، وحماية النسخة الاحتياط ، ونظام الترقيم والتبويب ، وآلية الاسترجاع والاستخدام ، ومكان الحفظ وامنه ، وتشفير النسخ التي تحتوي معطيات خاصة وسرية ، مسائل رئيسة يتعين اتخاذ معايير واضحة ومحددة بشأنها .

وسائل الأمن الفنية ونظام منع الاختراق :-
تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة الكمبيوتر والإنترنت ، كما تتعدد أغراضها ونطاقات الاستخدام ، وقد تناولنا فيما تقدم مسائل التعريف والتوثيق وتحديدا كلمات السر ووسائل التعريف الأخرى . وتتخذ الجدران النارية **Firewalls** ، اضافة للتشفير **cryptography** ، وكذلك نظم التحكم في الدخول و نظام تحري الاختراق ، وأنظمة وبرمجيات مقاومة الفيروسات اهمية متزايدة ، لكنها لا تمثل جميعها وسائل الأمن المستخدمة ، بل هي اضافة لوسائل التعريف والتوثيق المتقدم الاشارة اليها تمثل اهم وسائل الأمن التقنية في الوقت الحاضر ،

التهديد Threats : ويعني الخطر المحتمل الذي يمكن ان يتعرض له نظام المعلومات وقد يكون شخصا ، كالمتجسس او المجرم المحترف او الهاكرز المخترق ، او شيئا يهدد الاجهزة او البرامج او المعطيات ، او حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية .

نقاط الضعف او الثغرات Vulnerabilities : وتعني عنصر او نقطة او موقع في النظام يحتمل ان ينفذ من خلاله المعتدي او يتحقق بسببه الاختراق فمثلا يعد الأشخاص الذين يستخدمون النظام نقطة ضعف اذا لم يكن تدريبهم كافيا لاستخدام النظام وحمايته ، وقد يكون الاتصال بالإنترنت نقطة ضعف مثلا اذا لم يكن مشفرا . وقد يكون الموقع المكاني للنظام نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية والحماية ، وبالعموم فان نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات او المخاطر . ويرتبط بهذا الاصطلاح اصطلاح **وسائل الوقاية Countermeasures :** وتعني التكنيك المتبع لحماية النظام ككلمات السر والأقفال ووسائل الرقابة والجدران النارية وغيرها .

المخاطر Risks : فانها تستخدم بشكل مترادف مع تعبير التهديد ، مع انها حقيقة تتصل بأثر التهديدات عند حصولها ، وتقوم استراتيجية أمن المعلومات الناجحة على **تحليل المخاطر Risk analysis** ، **وتحليل المخاطر هي عملية Process** وليست مجرد خطة محصورة ، وهي تبدأ من التساؤل حول التهديدات ثم نقاط الضعف واخيرا وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف .