الأكاديمية العربية الدولية
Arab International Academy

إسم المادة: إدارة أمن المعلومات ومعاييرها

إسم المحاضِر: م.خليل المحمد

الأكاديمية العربية الدولية – منصة أعد

التعريف بأمن المعلومات

ان علم امن المعلومات هو العلم الذي يعنى بحماية المعلومات من المخاطر التي قد تتعرض لها ويمكن تعريف امن المعلومات بشكل مختصر بانه: حماية المعلومات من الوصول غير المسموح به ويمكن تعريفه بتفصيل اكثر بانه المفاهيم والتقنيات والتدابيرالتقنيه والادارية المستخمة لحماية اصول المعلومات من الوصول غير الماذون به عمدا أو سهوا او حيازتها او الاضرار بها او كشفها او التلاعب او تعديلها او فقدها او اساءة استخدامها وبهذا يتسع مفهوم امن المعلومات ليشمل المحاور التالية:

- حماية المعلومات من الضرر باشكاله كافة سواء اكان المصدر اشخاص كالمخترقين ام برامج كفيروسات الحاسب الالي وسواء اكان متعمدا او عن طريق الخطا.
- حماية المعلومات من الوصول غير المصرح به او السرقه او الالتقاط او تغييراواعاده التوجيه او سوء الاستخدام.
- حماية قدرة المنشاة على الاستمرار واداء اعمالها على احسن وجه.
- تمكين انظمة تقنية المعلومات والبرامج التطبيقيه لدى المنشاة من العمل بشكل امن.

الحاجة لأمن المعلومات

1- حماية الأصول المعلوماتية الحرجو اذ لا تقوم تقنية المعلومات في المنشاة ولا الخدمات التي تقدمها تلك المنشاة الا على الا على أصول معلوماتية مهمة وحرجة يجب حمايتها من أي اخطار تهددها ويجب المحافظة على استمراريتها وبقائهامتاحه متوافرة في جميع الاوقات فالحاجه لحماية هذه الأصول عاملة متاحة امنة والوجه الاخر ان توفير هذه الأصول كلف مبالغ وجهودا كبيرة تستحق ان يبذل من اجلها الوقت والجهد والمال لحمايتها ومن الأمثلة على الأصول المعلوماتية الحرجة ما يلي : أنظمة التشغيل operating System البرامج التطبيقية Application programs أجهزة تخزين المعلومات , المواقع والبوابات الالكترونية سواء داخليه او على شبكة الانترنت مراكز البيانات data centres قواعد البيانات Databases أجهزة الخوادم الرئيسية, البرامج التطبيقية application programs , شبكات المعلومات المحلية Lan والواسعة Wan

الحاجة لأمن المعلومات

2- حاجة اعمال المنشات وانشطتها الى ذلك حيث أصبحت المعلومات تشكل ثروة حقيقية للمنشات ومواردا مهما من مواردها بل ان - المعلومات في بعض المنشاة هي مصدر الدخل الأول لها ويقوم عليها نشاط المنشاة الأساسي والتجارة الالكترونية خير مثال لذلك

3- حاجه المستفيدين من الخدامات الالكترونية الى ذلك ومعنى ذلك ان المستفيدين من الخدمات الاكترونية بحاجة الى حماية معلوماتهم من كل ما يضر بها

4- انتشار الخدامات الالكترونية عن بعد مثل خدمات الحكومات الالكترونية والتعليم عن بعد لدرجة ان المواطن يستطيع ان ينهي جل او جميع اجراءته وان يحصل على درجته العلمية المناسبه من منزله

5- الحاجة الى معرفة إمكانيات المنشات ومدى قدرتها على حماية معلوماتها ومعرفة التهديدات التي تواجهها فلكي تكون امنا فلا بد ان تعرف نفسك وتعرف التهديدات التي تواجهك.

6- كثرة التهديدات وتنوعها وتعدد مصادرها والخطورة في ذلك انه قد توجد جملة من التهديدات داخل المنشاة في أنظمتها المعلوماتية او في موظفيها.

تهديدات أمن المعلومات

1- تهديدات فنية:

وهي التهديدات الناجمة عن القصور والاخطاء الفنية في مختلف أنظمة امن الملومات والتي يغلب عليها الطابع الفني دون ان يكون هناك أي تدخل بشري او ان تكون بسبب كارثة طبيعية ومنها

- **تهديدات عيوب التصميم والتشغيل**

وتشمل عيوب التصميم في الأجهزة والبرامج والشبكات وأدوات الربط والتخزين او أي مكون اخر من مكونات الأنظمة المعلوماتية وهنا تبرز أهمية تصميم البنية التحتية التقنية عيوب التشغيل عن اخطار التصميم في إمكانية النفوذ الى المعلومات بصفة غير شرعية او التسبب في فقدها بسبب خطا تشغيلي قد يكون بسيطا من الأمثلة على ذلك فتح منافذ اتصال بدلا من اغلاقها او نسخ المعلمات الى أماكن خاطئة او توجيهها الى غير وجهتها الصيخية ناهيك عن التهديدات المتعلقة باخطاء النسخ الاحتياطي التشغيلية كاخذ نسخة احتياطية لجزء من المعلومات فقط او استعادة معلوماتقديمة بدلا من المعلومات الحديثة عند اجراء عملية الاستعادة للمعلومات التي سبق اخذ نسخه احتياطية لها.

تهديدات أمن المعلومات

- **تهديد تشتت المعلومات**

اذا كانت معلومات المنشاة متشتتة ومخزنة في أماكن كثيرة ويجري التعامل معها من خلال شبكات متعدده فان هذا التشتت يحتم تطبيق أنظمة امن المعلومات وتشتتها وكذلك زيادةتكاليف توفيرها وادارتها والسيطرة عليها

2- تهديدات بشرية:

ويقصد بها التهديدات الناجمة عن العنصر البشري مباشرة فقد يتسبب العنصر البشري عمدا او عن طريق الخطا في الضرر او وصول الى معلومات والاطلاع عليهادون ان يكون له صلاحيه ذلك او اتلافها او تسريبها الى جهات خارجية

تهديدات أمن المعلومات

3- تهديدات طبيعية

يقصد بها الكوارث الطبيعية التي ليس للإنسان او التجهيزات الفنية دخل في حدوثها كلزلازل والبراكين والفيضانات والصواعق والحرائق وموجات الغبار العاتية. وقد تلحق مثل هذه الكوارث الضرار كبيرة بانظمة المعلومات وقد تودي الى انقطاع الخدمات الالكترونية نهائيا في حال اصابت المراكز الرئيسية لتقديم تلك الخدمات.

هجمات البرامج او الاكواد الخبيثة Malicious Code Attack

تشمل هجمات البرامج الخبيثة بشكل أساسي هجمات فيروسات وديدان الحاسب الالي وبرامج احصنة طروادة وبرامج الاختراق وبرامج التجسس الالكتروني

الهجمات الالكترونية والحماية منها

هجمات الأبواب الخلفية Back Door Attacks

في بعض الأحيان يترك المصممون او المبرموجون او فتيو الصيانة طرقا خفية تسمى الأبواب الخلفية للوصول الى الأجهزة والشبكات من اجل استخدامها لاحقا لاعمال التطوير والصيانة عن بعد ويستغل المهاجمون هذه الطرق عند اكتشافها كابواب خلفية للدخول الى الاجهزه والشبكات بطرق غير شرعية

الهجوم الاعمى الاستقصائي Brute Force Attack

يسمى الهجوم الذي يحث عن طريق تجريب جميع لاحتمالات الممكنه لكلمات المرور او الأرقام السرية او أي معلومة يحتاج اليها المهاجم في عملية الهجوم بالهجوم الاعمى او الاستقصائي وسمي بهذا الاسم لانه لا يعتمد على أي عملية حسابية او أي عملية لتسريع الهجوم او اختصار الوقت الازم لتنفيذه وانما يحصل بمحالوة الدخول مرة تلو الأخرى واستقصاء جميع الاحتمالات الممكنه.

الهجمات الالكترونية والحماية منها

كسر كلمات المرور Password Crack

نعنى بكسر كلمات المرور هنا عملية إعادة حساب كلمات المرور من البصمات الرقمية لهذه الكلمات التي تحفظ عادة في ملفات خاصة بذلك ويمكن تنفيذ هذا النوع من الهجوم اما بإعادة حساب البصمة الرقمية لكلمات المرور بطرق رياضية معقدة او منخلال الجميع بين هذه الطريقة **وهجمات المعجم Dictionary Attack**

الهجوم الاعمى الاستقصائي Brute Force Attack

يسمى الهجوم الذي يحث عن طريق تجريب جميع لاحتمالات الممكنه لكلمات المرور او الأرقام السرية او أي معلومة يحتاج اليها المهاجم في عملية الهجوم بالهجوم الاعمى او الاستقصائي

هجمات المعجم Dictionary Attacks

تعد هجمات المعجم نوعا من أنواع الهجوم الاعمى خاصة عند تخمين كلمات المرور.

الهجمات الالكترونية والحماية منها

هجوم تعطيل الخدمة Denial of Service Attacks DoS

في هذا النوع من الهجوم يرسل عدد هائل من طلبات الاتصال او أوامر بروتوكولات الشبكات مثل امر ping الى الجهاز الضحية من اجل اغراقه في معالجة هذا الطلبات وتحميله اكثر من طاقته حتى وصوله لدرجة عدم الاستجابة.

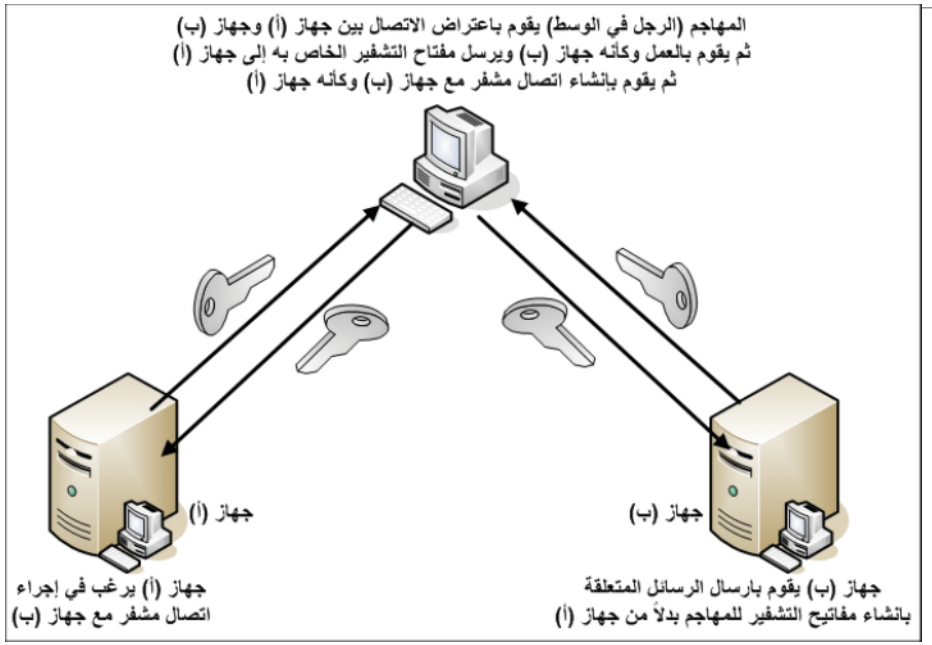
هجمات الخداع Spoofing Attacks

هي طريقة للتمكن من الوصول الى الاجهزه بطريقة غير شرعية عن طريق خداع هذه الاجهزه بارسال رسائل مخادعة تحتوي عنوان انترنت IP يجعل الرسالة تبدو كانها قادمة من جهة موثوقة.

الرسال غير المرغوب فيها او المزعجة Spam

يرد الى صناديق البريد الالكترونيالكثير من الرسائل المزعجة و يعتبر كثير من الناس أن هذه الرسائل ليست هجمات الكترونية لكن واقع الحال يقول ان كثير منها يحتوي ملفات بها برامج او اكواد خبيثة.

الهجمات الالكترونية والحماية منها



هجمات الرجل في الوسط Man in the Middle Attacks

يطلق على هذا الهجوم أيضا هجوم اختطاف بروتوكل النقل TCP Hijacking Attack

ويحث في هذا الهجوم التقاط حزم البيانات Data Packets المارة في الشبكة ثم تغييرها ثم اعادتها مرة أخرى الى الشبكة لتكمل مسارها لكن بمعلومات معدلة.

تفجير البريد الالكتروني Mail Bombing

وهذا أيضا هجوم على البريد الالكتروني لكن بنوع من أنواع هجوم تعطيل الخدمة وهو هجوم تفجير البريد الالكتروني او فنبلة البريد الالكتروني وما يحدث في هذا الهجوم هو ان المهاجم يوجه عددا هائلا من الرسائل الالكترونية الى الضحية.

الهجمات الالكترونية والحماية منها

هجمات التشمم او الالتقاط Sniffer Attacks

التشمم هو برنامج او جهاز يراقب البيانات المارة عبر الشركة ويلتقطها ويمكن ان يكون هناك تشمم او التقاط غير شرعي لمراقبة الشبكة ومتابعها وادارتها ويكن ان يكون غير شرعي لسرقة البيانات.

هجوم تصفح الكتف Shoulder Surfing Attack

يعني هجوم تصفح الكتف ان يطلع المهاجم على المعلومات المهمة والحساسية كما لو كان ينظر اليها من فوق كتف الضحية ويرى لوحة المفاتيح وما يقوم بضغطه من ازرار وما يعرض عل الشاشة من معلومات

الهجمات الالكترونية والحماية منها

هجمات الهندسة الاجتماعية Social Engineering Attacks

يخلط هذا النوع من الهجوم بين النواحي الاجتماعية واهتمامات الناس وبين المهارات الفنية في خداع الضحايا وكسب ثقتهم للادلاء بمعلومات سرية يتم استغلالها لسرقة المعلومات والأموال الكترونيا

هجمات المعلومات الجانبية Side Channel Attacks

ظهر نوع حديث نسبيا وخطير جدا من الهجمات الالكترونية يعتمد على المعلومات الجانبية التي يجمعها المخترق من أجهزة التشفير خاصة أجهزة التشفير التي تعمل بانظمة التشفير بلمفتاح العام ثم يحللها للحصول على المعلومات السرية كمفاتيح التشفير

عناصر أمن المعلومات

لقدد حدد بعض المؤلفين ثلاث ركائز أساسية لامن المعلومات هي السرية Confidentiality وسلامة المعلومة وتكاملها Integrityوالتوفر Availability واطلق على ذلك مثلث CIA Triangle الا ان الاتحاد العالمي للاتصالات في تصويته X800 قد حدد عناصر أساسية لامن المعلومات يمكن حصرها في سبعة عناصر رئيسية هي التحقق من الهوية والتحكم بلوصول والسرية وسلامة المعلومة وتكاملها وعدم الانكار وتوافر او ديمومة المعلومة والمتابعة او التدقيق.

ماهية عناصر امن المعلومات

يمكن تعريف عناصر امن المعلومات بانها مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة بحيث يغطي كل عنصر من هذه العناصر جانبا من جوانب الحماية المطلوبة ومعنى ذلك هة ان تتكامل هذه العناصر حتى توفر الحماية المطلوبة وفي حال فقد أي منها خلل امني في الجانب الذي يغطيه هذا العنصر لتوضيح ما نقصده بعناصر امن المعلومات سوف نشرح ذلك من خلالمثال ارسال رسالة من شخص الى اخر باستخدام الطريقة التقليديه البريد العادي ومقارنة ذلك بالطرق الحديثة التي يجري فيها ارسال الرسالة الالكترونيا والسبب في اختيار هذا المثال هو أولا لتقريب مفهوم عناصر امن المعلومات وثانيا اغلب ان اغلب طرق الحصول على المعلومات وتبادلها يكون عن طريق طرفين احدهما مرسل والأخر مستقبل او عن طريق تقنية الخادم والعميل او تطبيقات شبكة الانترنت شبكة التي لا تخلو من تبادل المعلومات بين طرفين او جهتين قد تكون جهازين يعملان بشكل الي

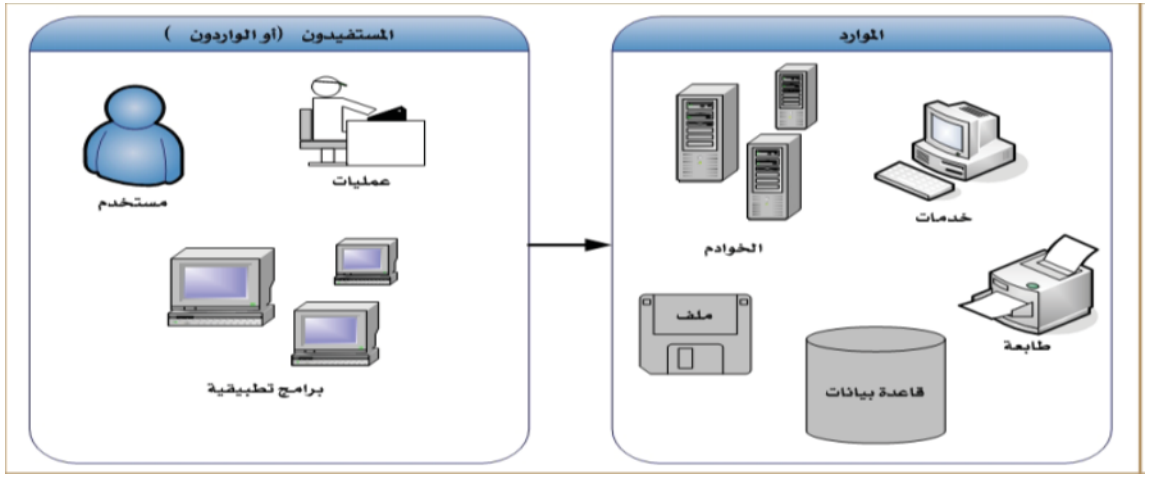
التحقق من الهوية Authentication

تعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص او الجهة وانه الشخص المعني لاغيره فعند اتصال شخصين او جهتين بعضهما ببعض فلا بد ان يتعرف كل منها الى الاخر لضمان ان يتخاطب كل منهما مع الشخص او الجهة المعينة وليس مع غيرها بعبارة أخرى فان التحقق من الهوية هو التحقق من ان المستخدم لنظام ما هو بالفعل من ادعى انه ذلك المستخدم وفي حال نقل المعلومات فانه يجب التحقق من هوية المستلم لضمان ان المعلومة ذاهبة الى وجهتها الصحيحة.

تبدأ عملية التحقق من الهوية بالتعريف بالهوية او تحديد الهوية Identification ويمكن تحقيق ذلك من خلال اسم المستخدم او رقم الحساب مثلا ان تحديد هوية الشخص او التعريف به رقميا الكترونيا امر مهم وقد يكون صعبا في بعض الأحيان اذ ان الشخص الواحد نفسه قد يكون لديه اكثر من هوية رقمية لذا يجب ان تتوفر في طريقة تحديد الهوية المعايير الاتية:

- ان تكون الهوية فريدة ومعنى ذلك ان تكون غير قابلة للتكرار ومثال ذلك ان يكون للشخص رقم هوية فريد خاص به لا يشترك معه غيره فيه ومثال اخر هو استخدام الخصائص الحيوية للإنسان غير قابلة للتكرار كبصمات الأصابع وبصمات العين.
- ان تكون غير مصفحه عن معلومات المستخدم و ظيفته والغرض من وصوله الى المعلوة ومثال ذلك ان لا ينم اسم المستخدم لمدير النظام مثل استخدام عبارة مدير Administrator او عبارة Backup Operator وهكذا.

التحكم بالوصول Access Control

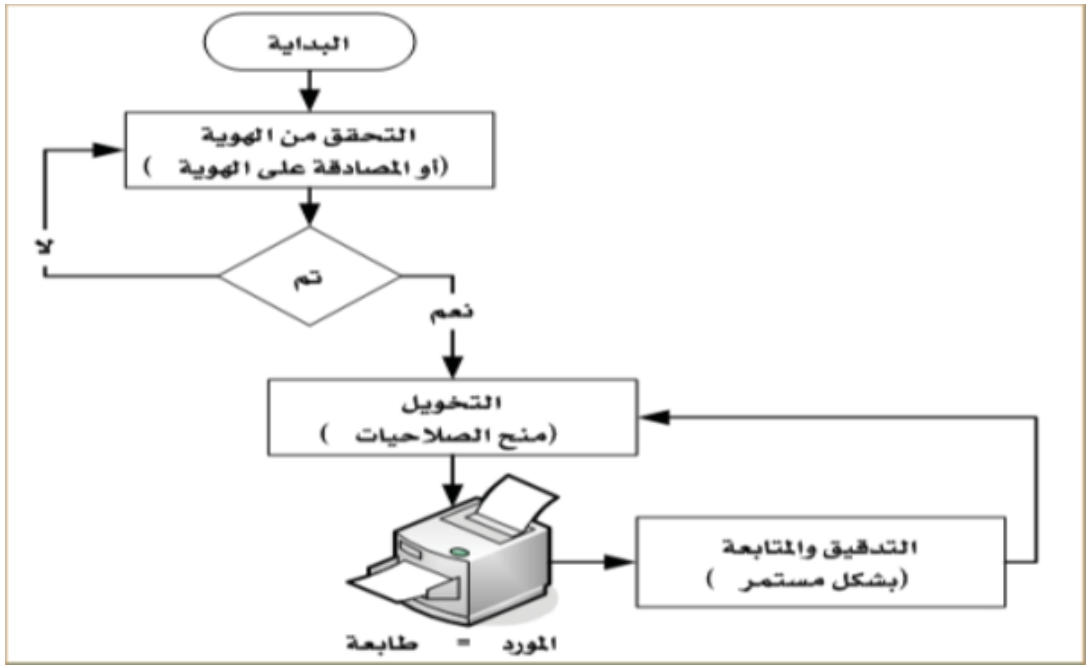


- ان لا تكون مشتركة بين المستخدمين كاعطاء قسم كامل به عدد من الموظفين اسم المستخدم نفسه.
- اتباع معايير التسمية المعتمدة عند المنشاة عند انشاء الحساب كاستخدام اول حرف من اسم المستخدم الحقيقي متبوعا برقم الهوية او غير ذلك من التسميات التي قد يستفاد منها في تحديد الشخص بسهولة عند اجراء عمليات التدقيق والمتابعة.

Access Controlالتحكم بالوصول:

التحكم بالوصول هو طرق او وظائف الحماية التي تتحكم بوصول المستخدمين او الأنظمة الى موارد المنشاة كالاجهزة الرئيسية والبيانات المركزية او بعبارة أخرى منع الاستخدام غير المرخص به للموارد فتلك الطرق هي التي تحمي الأنظمة وموارد المنشاة المختلفة من الوصول الغير شرعي كما انها تساعد في تحديد مستوى التخويل Authorization المصرح به بعد نجاح عملية التحقق من الهوية.

التحكم بالوصول Access Control



يأتي عنصر التحكم بالوصول بعد عنصر التحقق من الهوية فعندما يتم التحقق من هويةالشخص ويسمح له بالدخول الى شبكة الحاسب الالي مثلا فانه يجري التحكم باستخدامه لموارد محددة من الشبكة وليس جميع الموارد عن طريق التحكم بالوصول Access Control List ACLمن اجل ذلك تحدد الأشخاص المصرح لهم فقط باستخدامها وان كان مصرحا لهم بالدخول الى الشبكة عموما ويشمل ذلك منع الاستخدام غير المرخص به لاي معلومة وكذلك تحديد صلاحيات محددة للأشخاص المصرح لهم بالوصول الى المعلومات لاستخدامها والاطلاع عليها تحت شروط محددة

السرية Confidentiality

يمكن ان يطلق على هذا العنصر أيضا الخصوصية Privacy وتعني الحفاظ على المعلومات من ان يطلع عليها يقراها ويفهمها غير الأشخاص المصرح لهم فقط او بعبارة أخرى منع الكشف غير المصرح به فعندما ترسل رسالة سرية فان ذلك يتطلب ان لا يراها الاالمرسل والمرسل اليه فقط فان استطاع احد الاطلاع عليها فانه لا يستطيع ان يفهم محتواها أي يجب ان تكون غير مفهومة له.

هناك العديد من الطرق لتوفير السرة تتراوح بين حجب المعلومة يدويا وعدم تسليمها الا للأشخاص المصرح لهم فقط الى طرق التشفير الحديثة التي تعتمد على خوارزميات رياضية معقدة يصعب فكها ان لميكن مستحيلا من هنا يمكن القول انه يمكن توفير عنصر السرية من خلال تشفير البيانات سواء الثابتة منها او منقولة وتطبي سياسة صارمة للتحكم بالوصول وتصنيف المعلومات وتدريب العاملين على أنظمة وسياسات امن المعلومات تدريبا جيدا قد يتبادر الى ذهن بعضهم بانه عندما يتوافر عنصر السرية للمعلومة فانها بذلك تصبح معلومة امنة او بعبارة اخرة ان التشفير كوصيلة لتحقيق عنصر السرية يضمن امن المعلومة بشكل كامل وهذا مفهوم خاطئ والصحيحان السرية ماهي الا عنصر واحد من عدة عناصر رئيسية يجب توافرها جميعا لتصبح المعلومة امنة فتوفر عنصر السرية لا يضمن كشف تعديل البيانات اثناء النقل مثلا فقد يتم تغيير تاريخ معين في الرسالة المشفرة وعندما يفك المستقبل شيفرة الرسالة يحصل على تاريخ مقبول ظاهريا له لكنه غير التاريخ الحقيقي وكذلك فان توافر عنصر السرية لا يغني عن عنصري التحقق من الهوية وعدم الانكار.

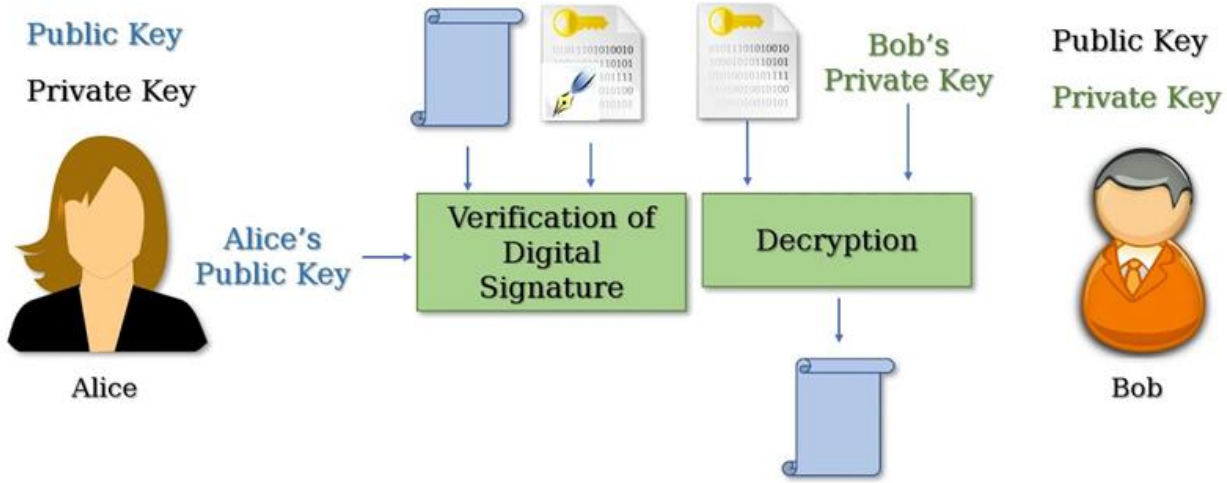
سلامة المعلومة وتكاملها Data Integrity

تعني الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة المعلومة من التعديل او الحذف او الإضافة او إعادة التركيب او إعادة التوجيه وهذا امر مهم جدا لضمان الثقة في المعلومة وانها هي المعلومة الاصلية دون زيادة او نقصان فقد تكون المعلومة مشفرة وسريتها مضمونة لكن قد تتعرض لتغيير طالما انها معلومة الكترونية هذا التغيير لا بد من إيجاد طريقة لاكتشافه وهو ما يوفره هذا العنصر وقد يترتب على ذلك الغاء المعلومة وعدم الاعتماد عليها بالكلية لا يهتم عنصر السلامة المعلومة وتكاملها بضمان دقة الأنظمة المعالجة لها وسلامتها من التلاعب او التغيير غير المصرح به ويتطلب ذلك ان تعمل الأجهزة ةالبرامج وأنظمة الشبكات بانسجام تام للمحافظة على المعلومة ومعالجتها ونقلها الى وجهتها الصحيحة دون أي تغيير او تعديل غيرمتوقع ويشمل كذلك الحفاظ على البيانات من أي تلوث خارجي او تداخل او تضلرب او تشويش مع بيانات أخرى من الأمثلة على الخروقات الممكنة لامن المعلومات التي يمكن ان تتم في حال عدم توفر عنصر سلامة المعلومة او الأنظمة المعالجة لها فعلى سبيل المثال من الممكن ان يحذف المستخدم الذي لديه صلاحية كاملة على محرك القرص الصلب ملفا من ملفات التهيئة من غير قصد ظنا منه انه ملف غير مهم لانه لم يستخدمه مطلقا ومثال اخر هو ان ادخال 50000دولار بدلا من 5000دولار بلاضافة الى أخطاء المستخمينالعاديين فهنالك مجال مهم اخر عرضة الأخطاء المبرمجين ومديري قواعد البيانات وهو تغيير البيانات المخزنة في قواعد البيانات او اتلافها.

عدم الإنكار Non Repudiation

عدم الانكار Non Repudiation

هي الخدمة التي من خلالها يمكن منع أي شخص او جهة من انكار أي عملية قاموا بها وكشفهم فعلى سبيل المثال اذا منحت جهة معينة الصلاحية لتلك الجهة فان خدمة عدم الانكار ستكشف ذلك, في حالة ارسال رسالة بين طرفين فان عدم الانكار يثبت ارسال المرسل لها ويثبت استقبال المستقبل لها بحيث لا يمكن لاي منهما انكار ذلك وتزداد أهمية هذا الاثبات بازدياد أهمية الرسالة نفسها



يلعب عنصر عدم الانكار دورا رئيسيا في اثبات وقوع التفاعلية بين طرفين اخد وعطاء كالعمليات الحكومة الالكترونية.

تشمل خدمة عدم الانكار أيضا اثبات وقوع العمليات والإجراءات الالكترونية في أوقات وتواريخ معينه عن طريق الحاق بصمة التاريخ والوقت بالعملية نفسها Time Stamping .

توافر المعلومة Availability

توافر المعلومة Availability

يقصد بتوافر المعلومة ان تكون قابلة للوصول اليها واستخدامها حين الطلب من قبل أي شخص او أي جهة معروفة ومحددة وفي أي وقت مصرح به ويمكن القول ان خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحا دائما ومن هنا يطلق عليها أحيانا الديمومة وهي موجهة خصيصا الى أي خلل او هجوم يمكن ان يؤدي الى عدم توفر الخدمات ومن امثلة ذلك هجوم الفيروسات وهجوم حجب الخدمه او منعها Denial of Service DoS ويتطلب هذا الامر في غالب الأحيان حماية مادة تقنية كتقنيات توفير نظم احتياطية للمعلومات والطاقة الكهربائية ان الهدف العام من عنصر توافر المعلومة ان تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج اليها المستخدم وان توفر الحماية لها مما قدر يتسبب في عطل او عدم توفر أي منها وفي حال حدوث الأعطال او الكوارث المعلوماتية يجب ان تكون هناك شبكة وأجهزة وأنظمة وبرامج بديلة يجري احلالها اليا وبسرعة فائقة محل تلك التي تعرضت للعطل او الكارثة وفق خطة تشغيل للطوارئ يتم إقرارها والتدريب عليها جيدا قبل ذلك من الأمثلة على الخروقات الممكنة لامن المعلومات التي يمكن ان تتم في حال عدم توافر عنصر توافر المعلومة: إمكانية تدمير أنظمة المنشاة باستخدام برنامج تدميري او فيروسات تدميري حديث الإنتاج لا يوجد له برامج حماية او تحديثا Patches تلغي توافر المعلومة فسيكون هناك توقف تام في عمل المنشاة ولو لوقت محدود والسبب في ذلك هو ان توفير التحديثات اللازمة المضادة لها ونشرها من قبل الجهات المنتجة للبرامج التطبيقية وأنظمة التشغيل.

المتابعة والتدقيق Auditing

المتابعة والتدقيق Auditing

تهدف المتابعة ويطلق عليها أحيانا المحاسبة Accountability الى متابعة عمليات المستخدمين والتحقق من فرض سياسات امن المعلومات وانها تطبق بشكل صحيح ودقيق كما يكن استخدام نتائج المتابعة كاداوات تحقيق Investigation Tools في حالة خرق أنظمة امن المعلومات لاثبات وقوع بعض الاحداث واثبات ادانة المستخدم او المتهم او براءته من القيام بذلك الحدث وهناك أسباب عديدة وراء ضرورة اجراء عمليات التدقيقوالمتابعة على موارد الشبكة ومستخدميها نجملها في ما يلي:

1- التحقق من ان الأجهزة والأنظمة والبرامج تعمل بشكل طبيعي صحي من خلال مراجعة سجلات الاحداث Log Files ثم اتخاذ الإجراءات المناسبة بناء على المعلومات المتوافرة في تلك السجلات ومن ذلك:

a. معرفة أي خطأ Error يقع حيث سيكون هناك رسالة خطأ في سجل الأحداث تشرح الخطأو السبب المتوقع له أو الأنظمة أو الصلاحيات المتعلقة بهذا الخطأ.

المتابعة والتدقيق Auditing

b. معرفة رسائل التحذير Alerts التي تنبئ عن إمكانية حدوث مشكلة ما ويستخدم هذا النوع من الرسائل التحذيرية لمعرفة تاريخ المشكلة ومتى بدأت والظروف التي بدأت فيها ومتى تحولت الى مشكلة

c. توفير المعلومات Information عن الاحداث التي تتم لمجرد الإخبار عنها فقط وتستخدم هذه المعلومات في معرفة سلسلة الأحداث سواء أكانت طبيعية وخاضعة لسياسات أمن المعلومات أم كانت مخالفة لها ويمكن ان تستخدم هذه المعلومات لأغراض التحقيق الجنائي في جرائم المعلوماتية.

2- مراقبة العمليات الضارة التي قد يقوم بها المستخدمون عمداً أو خطأً.

3- الكشف عن عمليات التطفل والاختراقات.

4- المساعدة على استعادة الأحداث ومعرفة متطلبات الأنظمة واعداداتها, لاستعادتها قبل وقوع أي مشكلة.

المعايير العالمية لأمن المعلومات (الأيزو)

المنظمة الدولية للتوحيد القياسي ايزو ISO الذي أنشئ في عام 1947 هو هيئة غير حكومية تتعاون مع اللجنة الدولية الكهرتقنية IEC والاتحاد للاتصالات ITU على تكنلوجيا المعلومات والاتصالات ICT وهنا اشهر المعايير التابعة لها:

1- ايزو27002 : هذا المعيار يتضمن بعض السياسات والتوجيهات منها: السياسة الأمنية Security policy تنظيم امن المعلومات organization of information
امن الموارد البشرية human resources security الامن البيني physical and environmental security الاتصالات وإدارة العمليات communications and operation management التحكم في الوصول access control اقتناء نظم المعلومات وتطويرها وصيانتها Information system acquisition development إدارة الحوادث الأمنية للمعلومات Information security incident management

2- ايزو 27001: هذا المعيار يقدم نموذج دورس يعرف ب PDCA وهو اختصار ل Plan Do check act وهو يهدف الى تحديد الاحتياجات الازمة لاقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة امن المعلومات داخل المنظمة وعادة ما ينطبق على جميع أنواع المنظمات بما في ذلك المؤسسات التجارية والوكلات الحكومية وغيرها : الخطة Plan, تأسيس نظام لادارة امن المعلومات , التنفيذ DO البدء في تنفيذ الخطط وتشغيلها التحقق check مراجعة النظام بعد تنفيذه العمل Act صيانة وتحسين النظام.

3- ايزو 15408: يساعد هذا المعيار على التقييم والتحقق والتصديق على الضمانات الأمنية للمنتجات التكنولوجية وكذلك يمكن تقييم الأجهزة وابرمجيات لمكافحة تغير المناخ في مختبرات متعمدة للتصديق.

المعايير العالمية لأمن المعلومات (الكوبيت)

معايار الكوبيت COBIT: The Control objectives for information Related technology

هو عبارة عن اطار للسيطرة او التحكم تربط تقنية المعلومات بمتطلبات العمل وتنظيم لانشطة تكنولوجيا المعلومات في نموذج العملية المقبولة وتحديد الموارد الرئيسية لتكنوجيا المعلومات واهداف القابة الإدارية التي سينظهر فيها وقد تم بناء هذا المعيار من قبل معهد حوكمة تقنية المعلومات ITIG: IT Governance Institute في عام 1995م.

والكوبيت هو مجموعة من المواد التوجيهية الدولية تستخدم لحكومة تفنية المعلوماتوكذلك تتيح للمديرين سد الفجوة بين متطلبات الرقابة والقضايا التقنية والمخاطر التجارية واستنادا الى ابرز النقاط في كوبيت تبين انه يركز على مخاطر محددة حول امن تكنولوجيا المعلومات بطريقة بسيطة لمتابعة وتنفيذ المنظمات الصغيرة والكبيرة .

وهو الان في النسخة الرابعة وتتكون من سبعة أجزاء رئيسية : النظرة التنفيذية executive Overview اطار الكوبيت COBIT framework

التخطيط والتنظيم Plan and organize الاكتساب والتنفيذ Acquire and implement التسليم والدعم deliver and support

الرصد والتقييم monitor and evaluate الملاحق بما في ذلك المعجم او المصطلحات Appendices

المعايير العالمية لأمن المعلومات (ITIL)

هو اختصار ل The Information Technology Infrastructure ويسمى أيضا ايزو 20000

هو عبارة عن مجموعة من افضل الممارسات في مجال إدارة خدمات تقنية المعلومات ITSM ويركز على خدمة عمليات تقنية المعلومات ويعتبر الدور الرئيسي للمستخدم. وقد تم بناؤه بواسطة مكتب المماكة المتحدة لتجارة الحكومة OGC وإدارة خدمة التقييم الذاتي يتم العمل بها عن طريق وضع استبيانات على الانترنت استبيان التقييم الذاتي يساعد على تقييم إدارة المناطق التالية:

إدارة مستوى الخدمة Service Level Management الإدارة المالية Financial Management إدارة بناء القدرات Capacity Management

إدارة استمرارية خدمة Service Continuity Management إدارة التوفر Availability Management مكتب الخدمات Service Management

إدارة الخدمات Incident Management إدارة المشكلة Problem Management إدارة التكوين Configuration Management

إدارة التغيير Change Management إدارة الإصدار Release Management

اللوائح والقوانين المتعلقة بأمن المعلومات

1- قانون SOX: هو اختصار ل Sarbanes Oxley Act

بعد ارتفاع عدد الفضائح العالية في الولايات المتحدة بما في ذلك شركة انرون و وورلدكوم صدر قانون ساربانيس اوكسلي Sarbanes Oxley Act في عام 2002 والغرض من ذلك هو لحماية المستثمرين عن طريق تحسين دقة وموثقية نظام الإفصاح او التعريف المقدمة عملا لقوانين الأوراق المالية ولاغراض أخرى و هذا النظام يؤثر على جميع الشركات المدرجة في اسواق الورق المالية في الولايات المتحدة وقانون SOX يتطلب كل تقرير للرقابة الداخلية.

2- قانون COSO: وهو اختصار ل committee of sponsoring organizations of the tread way commission

هو اطار يبدا من عملية الضوابط الداخلية كما انها تساعد على تحسين وسائل السيطرة على الشركات من خلال تقييم فاعلية الضوابط الداخلية ويحتوي على خمسة مكونات رئيسية:

1. مراقبة البيئة بما في ذلك عوامل مثل السلامة من الناس داخل المنظمة وإدارة السلطة والمسؤوليات.
2. تقييم المخاطر وتهدف الى تحديد وتقييم المخاطر التي يتعرض لها قطاع الاعمال
3. مراقبة الانشطة بما في ذلك سياسات وإجراءات لتنظيم.
4. المعلومات والاتصالات بما في ذلك تحديد المعلومات المهمة لرجال الاعمال وقنوات الاتصال لتقديم قنوات الرقابة من جانب الإدارة للموظفين
5. الرصد بما في ذلك عملية استخدامها لرصد وتقييم جودة جميع نظم الرقابة الداخلية على مر الزمن

اللوائح والقوانين المتعلقة بأمن المعلومات

3- قانون HIPAA : the health insurance portability and accountability ويعني قابلية التامين الصحي وقانون المحاسبة هو قانون للولايات المتحدة تهدف الى تحسين قابلية واستمرار تغطية التامين الصحي في المجموعة على حد سواء والأسواق الفردية ومكافحة الهدر والاحتيال وسوء المعاملة في التامين الصحي والرعاية الصحية.

4- قانون FISMA: federal information security management ويعني قانون إدارة امن المعلومات الفيدرالي وهي تتطلب وكالات اتحادية أمريكية لتطوير وتوثيق وتنفيذ برنامج على نطاق الوكالة لتوفير امن معلومات عن المعلومات ونظم المعلومات التي تدعم عمليات الأصول للوكالة بعض الاحتياجات مثل تقييم المخاطر الدوري للمعلومات ونظم المعلومات التي تدعم عمليات واصول المنظمة

5- قانون FIPS: The Federal Information Processing Standards قانون معالجة المعلومات الفيديرالية.و هو عبارة عن سلسلة من المنشورات الرسمية المتعلقة بالمعايير والمبادئ التوجيهية المعتمدة والمتاحة.

نهاية المحاضرة

شكراً للمتابعة..... آمل أن تكونوا قد حققتم الفائدة