جامعة ديالى
كلية التربية الأساسية
قسم الحاسبات

إدارة تأمين نظم وشبكات المعلومات

بحث تخرج تقدم به الطالبان

حسام قاسم حسين
محمد جواد عبد

وهو من متطلبات الحصول على شهادة البكالوريوس في الحاسبات

اشراف محاضر مادة الشبكات

عصام سرحان ذياب

الفهرس

الفـــصـــل الاول

–المقدمة –

إدارة تأمين نظم وشبكات المعلومات تعني مجموعة من مراكز ومؤسسات المعلومات المتجانسة أو غير المتجانسة تتفق فيما بينها على تشاطر المصادر المستخدمة في الحواسيب ووسائل الاتصالات الحديثة التي تؤدي إلى توفير فرص لكافة المشاركين عن طريق التوزيع أو البث من خلال وسائل الاتصال عن بعد من خدمات المعلومات .

تتطور تقنيات الحاسوب والاتصالات بصورة كبيرة بسبب زيادة التطبيقات تعقيدا نظرا للمتطلبات الكثيرة والمتجددة من قبل المستفدين ،فأدى الى زيادة اعتماد المجتمعات عليها بحيث وضعت جميع حاجاتها وامتيازاتها في هذه التطبيقات ، ومن ضمنها تطبيق الحكومة الالكترونية والتي تتجه اليها بسرعة جميع الدول والتي بدات قسم منها بتطبيقها والقسم الاخر في تهيئه البنية التحتية لها من انظمة واجهزه واتصالات وتطبيقات فرعية .

فان في هذا التطبيق يصبح المستفيد هو الانسان ، وان مثل هذه التطبيقات المهمة والتي تكون مادتها الخام والمعلومات هي ناتجها بالتأكيد سوف تكون عرضة للكثير من الاخطار سواء كانت الطبيعية او من صنع البشر.

مما ادى الى ايجاد الحماية للتطبيقات والمعلومات التي تحتويها واعطاء الصلاحيات حسب المسؤوليات والتحقيق من المستفدين ومكافحة الفيروسات والكثير من المهام الكبيرة التي يجب توفرها لخدمة هذه الانظمة.

وازداد ابتكار المتطفلين لايجاد تهديدات متنوعة حسب الاجهزه المستخدمة وقد تراوحت هذه التهديدات من التصنت على خطوط الاتصالات الى الوصول الى الحواسيب وسرقة المعلومات المخزونة فيها ، بالاضافة الى الاطلاع على رسائل البريد الالكتروني ، فيؤدي الى ايجاد سياسة امنية لتضمين وتنفيذ المضمون لامن وحماية نظام المعلومات والشبكات شاملا عن طريق تحديد اهم المخاطر التي قد يتعرض لها النظام في أي مرحلة من مراحلة .

وفي الوقت الذي تهتم اغلب الدول والمؤسسات بتطوير البنية الاساسية لمجتمع المعلومات بهدف بناء صناعة قومية تعتمد على التكنولوجيات المتقدمة مع اعداد اجيال جديدة من القادة والمديرين القادرين

على التعامل أكثر مع التقنيات الحديثة وتطويعها لخدمة كافة المجالات فانها تتناسى احيانا أهمية تامين هذه البنية المعلوماتية ونحن نشهد بدايات عصر أو ثورة أو فورة المعلومات والمعرفة وسيتم بناء المزيد من نظم وشبكات المعلومات في الأعوام القليلة المقبلة أكثر كثيرا مما تم بناءة في السنوات السابقة .

ستكون هذه الأجيال الضخمة من البيانات والمعلومات معرضة للخطر إذا لم يتم تخزينها وإدارتها وتداولها بأمان وسرية تامة.

لذلك يجب توفر درجة الأمان ومواجهة ومعالجة مشاكل الحماية والتامين وخاصة إننا سوف نشهد في السنوات القادمة بناء الكثير من نظم وشبكات المعلومات.

أهمية البحث

يستمد هذا البحث أهميته من خلال دراسة إدارة تامين نظم وشبكات المعلومات التي لها أهمية كبيرة في مختلف مجالات الحياة حيث أصبحت التقنيات المعتمدة على الحاسبات وشبكات المعلومات والاتصالات هي الوسيلة الرئيسية لتجميع وإدارة ومعالجة ونقل البيانات داخل وخارج معظم المؤسسات .

فظهرت أهمية امن البيانات والشبكات كأحد العناصر الرئيسية المكونة لنظام المعلومات الحديث ، كما ظهرت ضرورة دراسة الأساليب التي تودي إلى حماية فعالة لنظام المعلومات ضد جميع الانتهاكات والتداخلات والمخاطر المقصودة وغير المقصودة التي قد تؤدي إلى فقد النظام أو فقد تكامله ونزاهته وكذلك تميز تكنولوجيا المعلومات في سرعة الاستجابة إلى طلبات المستخدمين وتامين نقل المعلومات المطلوبة بدقة واستلام المعلومات والإجابات وتكون المعلومات فيها محصنة من التداخلات والتأثيرات وتتصف بسهولة الاستخدام من قبل الجهات المشاركة ومعرفة ادارتها بسهولة ويسر وكيفية .

وان أهمية البحث فيما عداماسبق هو القيام بتوضيح امنية الشبكات والمعلومات والسياسات الأمنية وكيفية تامين الدخول على نظم المعلومات والتعرف على نظام المعلومات في الشبكة وتصنيف أصول وممتلكات نظم المعلومات.

مشكلة البحث

إن اغلب المشاكل المتعلقة في إدارة تامين نظم وشبكات المعلومات لاتحضى بالاهتمام الكافي اذ تبدو انها لم تحتل حيزا ذا اهمية فالدراسات التي بحثت في هذا الموضوع وجدت ان هنالك حاجة لادوات مؤتمنة لحماية الملفات والمعلومات المخزونة وكثرة الانظمة الموزعة واستخدام وتسهيل الشبكات لنقل البيانات بين محطة المستخدم والحاسوب وبين حاسوب وحاسوب اخر .

لهذا يؤدي الى بطا في نقل المعلومات وادارتها وهنالك حاجة الى ايجاد طرق تساعد على ادارة اكثر كفاءه وامنا وسهولة في النقل وتبادل المعلومات .

ومن المشاكل التي قد يتعرض لها للخطر بطريقة او باخرى انشطة التشغيل والاستمرارية لنظام المعلومات هو عدم قدرة ادارة تامين نظم وشبكات المعلومات على تحقيق اهدافها وبذلك يؤدي الى عدم الثقة وانعدام اعتمادية المسؤوليين على كافة المستويات على نظام المعلومات عند اتخاذ القرارات .

أهداف البحث

اولا/تحديد الاجراءات ووسائل الادارة والتحكم في سرية المعلومات واجراءات الحماية والتشغيل والاتصالات وكيفية الاستفادة من المعايير العالمية في امن ادارة وسرية المعلومات .

ثانيا/ التامين والتحكم في نظم وشبكات المعلومات من خلال تطوير ومراجعة نظام الامن عن طريق تحليل الاخطار ووضع خطط الطوارئ التي تتضمن استمرارية عمل النظام تحت كافة ظروف المخاطر .

ثالثا/ يهدف الى تضمين وتنفيذ المفهوم الشامل لامن وحماية نظام المعلومات وتحديد اهم المخاطر التي يتعرض لها النظام .

رابعا/ يهدف الى افضل ادارة وتامين لنظم شبكات المعلومات وذلك من اجل امن وسرية المعلومات .

خامسا/ يهدف الى الهيكل التنظيمي المساند للحماية والتامين والسرية ودور الافراد في الامن .

مجالات البحث

أولا/ يناقش أفضل الممارسات القابلة للتطبيق التي تتعلق بالحماية ضد التهديدات المختلفة لامن المعلومات وبعض مخاطر التامين المقصودة وغير المقصودة التي يواجها بعض الاشخاص والمستخدمين للحاسوب بسبب التطور الحاصل في مجالات تهديد وانتهاكات واختراقات السياسات الامنية لنظم المعلومات.

ثانيا/ يقوم بدراسة ادارة امنية الحواسيب الشخصية (personal computer) .

ثالثا / ادارة امنية الشبكة وكيفية تحليل الخطر والخطط الامنية والسياسات الازمة لذلك .

رابعا/ المشاكل التي يواجه أمنية وادارة شبكات المعلومات وقسم معالجة البيانات .

خامسا / حماية الملفات والاجراءات الامنية التي تكون لها حق الوصول الى الملف باكملة او لايكون لها حق الوصول.

الـفصـــل الثانى

أولا/تأمين نظم المعلومات:-

أصدرت المؤسسات العلمية للتوحيد القياسي عدة معايير وتوصيات خاصة بتامين نظم المعلومات تشمل التوصيات احدث وسائل التامين والحماية التي تتمشى مع التطور التكنولوجي طبقا لتجارب الدول المتقدمة [1].

فظهر ما يسمى بعصرالمعلومات ومن ابرز ما فيه هو شبكة الانترنت واستخدمتها الحديثة كالتجارة والإعمال الاخرى فتعرضت هذه الشبكات للانتهاكات عدة ومن اساليب انتهاك المعلومات نذكر منها :-

١ـ التصنت :-هو قيام المهاجم والمقتحم بمراقبة مايدور في الشبكة وما يتم تبادلة فيها من وسائل وبأبقائها في طي الكتمان وهناك نوعان من التصنت :-

أـ هو مراقبة الرسائل (packet sniffing).

بـ هو اعادة ارسال الرسائل (Replay).

٢ـ دوافع اختراق نظم المعلومات :-

بالرغم من المخاطر الكبيرة الناتجة من الهفوات الأمنية تصر العديد من المؤسسات على صرف القليل من تكنولوجيا المعلومات والشبكات على مقاييس ووسائل التامين والسرية لكافة المستويات يرجع سبب ذلك إلى إن مثل هذه المقاييس لا تتهتم مباشرة في النتيجة ومخاطر الانتهاكات الأمنية غالبا لاتظهر سريعا ،فمن مصلحة المنتهك والمتلصص على نظام المعلومات استمرار النظام في العمل ليتسنى له سرقة المعلومات ومن تلك الدوافع اختراق نظم المعلومات الاتي :-

أـ تزايد أهمية المعلومات والاعتماد الدائم عليها .

---

١)أدارة تامين نظم وشبكات المعلومات ،د.احمد الشربيني ود.وفائي بغدادي محمد ،مكتبة الاسرة ٢٠٠٨،ص٢٨ـ٢٩.

٢)تحليل وتصميم نظم المعلومات ،اروى يحيى عبد الرحمن الارياني ماجستير تحليل وتصميم نظم المعلومات ،جامعة سيتي ـلندن ،الطبعة الاولى ١٩٩٨،ص٩٤ .

ب- أهداف مشبوهة[٢].

ج- الفضول وحب الاستطلاع .

د- من غير قصد .

ز- حرب المعلومات .

هـ- الدفاع عن حقوق الملكية [١].

ثانيا / تصنيف أصول وممتلكات نظم المعلومات :-

١ - مطالب نظم إدارة تامين المعلومات:-

هو ضمان استمرار التامين والحماية الملائمة للاصول التشغيلية والتنظيمية بالمؤسسة ومن الضروري اخذ كل أصول المعلومات الرئيسية في الحسبان عند اختيار وسائل التامين على إن يكون لكل مصدر مالك مرشح من قبل الجهة الإدارية بالمؤسسة حيث إن توفير الحماية الملائمة للأصول يضمن لها البقاء والاستمرارية.

ويجب ان يميز مديرو المؤسسة كل الاصول الرئيسية لها ويتم تخصيص وسائل التحكم والمسؤولية الدائمة للاصول ،قد يتم تفويض مسؤولية تطبيق التحكم من المالك لاحد المستخدمين لتلك الأصول ولكن تبقى المسؤولية الإجمالية للتامين والتحكم مع المالك المسؤل بالمؤسسة [٢] .

٢ - تصنيف المعلومات:-

يعني ضمان حصول أصول المعلومات على المستوى الملائم من الحماية ،ويلزم تصنيف المعلومات للإشارة إليها عند الحاجة وبأولويات ودرجة الحماية الخاصة بكل منها ،وتكون المعلومات درجات مختلفة من الحساسية والخصوصية بعض الأصول قد تتطلب مستوى إضافي من الحماية والمعالجة الخاصة ،ويلزم استخدام نظام تصنيف مستويات المعلومات لتعريف مجموعة ملائمة من مستويات الحماية لها وبالتالي الإبلاغ عن الحاجة لاجراء المعالجة الخاصة بها [٣].

---

١)تحليل وتصميم نظم المعلومات ،المصدر السابق ، ص٩٤ .
٢) ادارة تامين نظم وشبكات المعلومات ،المصدر السابق ،ص٧٧.
٣) تكنولوجيا أمنية المعلومات وأنظمة الحماية ،أ.د علاء حسن الحمامي جامعة عمان العربية للدراسات العليا ود.سعد عبد العزيز العاني جامعة عمان الاهلية ،الطبعة الاولى ٢٠٠٧،دار وائل للنشر،ص٨٢ .

٣- تميز التصنيف والتعامل معة :-

لابد من وضع وتعريف خطة التصنيف والمجموعة الملائمة من الاجراءات التي تتبناها المؤسسة لتغطية اصول المعلومات في اشكالها الطبيعية والالكترونية ،وتعريف التصنيف لكل اصل يهدف الى تغطية الانواع التاليةمن انشطة اعداد المعلومات :-

أ- النسخ .

ب- التخزين .

ج- الارسال بالبريد –الفاكس –والبريد الالكتروني .

هـ- الارسال بالكلمة المنطوقة ويشمل الهاتف المحمول – البريد الصوتي [١].

٤- قائمة جرد الأصول :-

تساعد عملية جرد الاصول على ضمان الحماية المتميزة والفعالة لها ويتم جرد الاصول لاغراض العمل مثل (الصحة و السلامة) أو عند تقدير القيمة المالية للاصول ((إدارة الأصول)) وان عملية جرد جميع الأصول سمة مهمة من إدارة المخاطر ومن المهم إن تكون المؤسسة قادرة على تميز أصولها والقيمة النسبية لها واهميتهاوتسطيع المؤسسة تزويد مستويات الحماية مستندة على هذه المعلومات حيث تكون الحماية متوافقة مع القيمة واهمية الاصول . وما يميز جرد الاصول المهمة هو ارتباطها بكل نظام المعلومات ويكون التميز بشكل واضح ويحددملكية الاصل وتصنيفة الامني ،وان يتم توثيق ذلك بالإضافة لموقع الأصول الحالي (مهمة عندما يتم محاولة التعويض من الفقد او الضرر).

أمثلة الأصول المرتبطة بأنظمة المعلومات :-

أ)أصول معلوماتية :-ملفات البيانات وقواعد البيانات – وثائق النظام – أدله المستعمل –برامج تدريبيه فعالة أو إجراءات دعم فني- خطط الاستمرارية –إجراءات الاحتياطي – أرشيف المعلومات .

ب)أصول برمجيات:-برامج تطبيقية وبرمجيات ونظم وأدوات التطوير ومرفقاتها[٢].

---

١) حماية وامن شبكات المعلومات ،أ.دعامر تحسين سهيل الصميدعي ،جامعة قطر الطبعة الثانية ١٩٩٩،دار الروائع للنشر ص٨١ .

٢) www.c4arab.com .

ج)أصول طبيعية :-أجهزة الحاسبات والمعالجات – أجهزة تحويل وتوجيه –حاسبات محمولة – وأجهزة اتصالات نقل البيانات مثل المودم وخلافة –أجهزة اتصالات تليفونية (مسارات –سنترال داخلي –أجهزة فاكس)- أجهزة تخزين مغناطيسية(أشرطة وأقراص) أجهزة تقنية (تجهيزات طاقة تكييف) أثاث –وخلافة .

هـ) الخدمات:- خدمات الاتصالات واستعمال الحاسبات – مرافق عامة –ومثال ذلك –تدفئة – اضاءة- قوة تيار كهربائي –تكييف[1].

ثالثا:- التامين الطبيعي لنظم المعلومات:-

١-مطالب التامين الطبيعي لاماكن الحاسبات :- يجب استخدام نظم التحكم في الوصول لاماكن الحاسبات باعتبارها مناطق أمنية تسمح نظم التحكم في الدخول للمصرح لهم فقط بالتواجد في المناطق الأمنية وتمنع الآخرين غير المصرح لهم ولزيادة فعالية نظام التحكم في الوصول يلزم قدر الإمكان تقليل وتقييد عدد المترددين أو الزائرين للمناطق .

تؤسس نظم التحكم في الدخول على تقسيم المكان الطبيعي لنظام المعلومات الى مناطق ذات درجات امنية متدرجة- اصدار تصاريح مرور بالوان مختلفة مع تزويد التصاريح اذا امكن بوسائل تحديد العمل – تحديد وسائل تامين كل منطقة مؤمنة .

تنقسم نظام التحكم في الدخول الى أربعة أقسام هي :- ((Authorization, Auditing, (Authentication, Accounting,

أ) وسائل التعرف والتحقق من الهوية شاملا :- استخدام الخصائص الطبيعية مثل الصوت وبصمة اليد وبصمة العين – استخدام اشياء يملكها الفرد مثل العملات الالكترونية والكروت المغناطيسية والمفاتيح – استخدام كلمات المرور مثل الاسم كلمة المرور والأدلة والمصافحة [2].

---

١) www.c4arab.com .
٢) شبكات المعلومات والاتصالات ، أ.د عامر ابراهيم جامعة قطر ، والدكتورة ايمان فاضل السامرائي جامعة قطر ، ص ١٠١.

ب) احقيات اوصلاحيات الدخول للبيانات والبرامج والتعامل مع وسائل أعداد البيانات شاملا :-
القراءة والكتابة – الإضافة – التعديل- الحذف – طباعة التقارير من خلال تصميم الدخول .
ج) تدقيق ماتم من تفاعلات على النظام .
هـ) مراقبة الحسابات اليومية والختامية[١] .
ويتم حماية المناطق الأمنية بوسائل مناسبة للسيطرة على الدخول لضمان إن الموظفين المصرح لهم هم الوحدين الموجودين داخل مكان الحاسبات الالية – ولابد الاخذ بنظر الاعتبار وسائل التحكم التالية :-

١- الإشراف على زوار المناطق الامنية حتى يتم خروجهم مع تسجيل وقت دخولهم ووقت خروجهم ومن الضروري السماح لهم فقط بالزيارة في حالات معينة مصرح بها وفي اماكن محدده ويتم احضارهم والحصول على موافقتهم على تعليمات تامين المنطقة وعلى اجراءات الطواريء .
٢- التحكم في الدخول للمعلومات الحساسة واستخدام وسائل اعداد المعلومات يكون مقصورا فقط على المصرح لهم مع الاستعانة بوسائل تحديد الهوية مثل البطاقات الشخصية والكروت ذات الرقم الكودي الشخصي ([personel identification number]PIN)
لتسجيل جميع حالات الدخول والخروج للمناطق الامنية .
٣- ان يطلب من كل الموظفون لبس زي مميز مع اظهار بطاقات الهوية ومن الضروري ان يتشجعوا لتحدي الغرباء غير المرافقين واي فرد لايلبس الزي المميز ولايضع بطاقة الهوية الظاهرة .
٤- استمرار تسجيل ومراجعة حالات الدخول والخروج للمناطق الامنية [٢].

٢-تامين الأجهزة :- يعني الفقد أو الضرر أو التعديلات في الاصول مما يؤدي الى توقف الأنشطة التشغيلية للمؤسسة .ولابد من حماية الاجهزة طبيعيا من اخطار البئية والتهديدات الامنية لمنع خطر الوصول غير المصرح به الى البيانات وللحماية ضد الفقد او الضرر واتباع وسائل[٣].

---

١) شبكات المعلومات والاتصالات ،المصدر السابق ،ص١٠١ .
٢)ادارة تامين نظم وشبكات المعلومات ،المصدر السابق ،ص١٠٦.
٣)شبكات المعلومات والاتصالات ،المصدر السابق ،ص١١٠.

التحكم الخاصة بالحماية ضد المخاطر او الوصول غير المصرح به – وحماية وسائل المساندة مثل التجهيز الكهربائي وشبكات البنية الاساسية [١].

٣-صيانة الأجهزة :-

الأجهزة تبقى بالشكل الصالح لضمان توافرها المستمر وتكاملها ونزاهتهاووسائل التحكم التالية تؤخذ في الاعتبار :-

ا)صيانة الاجهزة وفقا للفترات والمواصفات التي تحددها الشركة المنتجة .

ب)ان يتم تنفيذ اعمال الصيانة والاصلاح بواسطة الفنيين المصرح لهم فقط .

ج)الاحتفاظ بوثائق الدعم الفني لكل جهاز يدون بها الاعطال المثبتة بها والاعطال الفعلية وتفاصيل كل اعمال الصيانة الوقائية والتصحيحية التي تمت على كل الجهازبتوقيت حدوثها.

هـ) تنفيذ وسائل سيطرة خاصة للاجهزة التي يتم اصلاحها خارج المؤسسة ويتم الالتزام بكل المطالب التي تفرضها وثائق التامين على الاجهزة [٢].

رابعا:- نظم تامين الدخول على معدات نظم المعلومات :-

١- مطالب التحكم في احقية الدخول :- يعني التحكم في أحقية الدخول للمصادر التشغيلية للنظام والحصول على المعلومات وتنقسم تأمين الدخول على معدات نظم المعلومات إلى قسمين :-

أ- وسائل التعرف على المستخدم:- يشمل التعرف على المستخدم (Identification) بتحديد الاسم يليها التحقق من الشخصية (Authentication) للتأكد من أن المستخدم الذي حدد اسمه هو نفس المستخدم. ويتم التعرف على المستخدم من خلال مزيج من الوسائل هي :-

١- اسم المستخدم.

٢- شيء يميز المستخدم ذاته مثل الصورة والبصمة او الصوت وشبكة العين .

٣- وسيلة خاصة مميزة توجد لدى الشخص ولاتوجد لدى غيره هي المفاتيح والبطاقات (الشخصية ، مغناطيسية، الكترونية) [٣].

---

١) شبكات المعلومات والاتصالات ،المصدر السابق ،ص١١٠.
٢) المصدرنفسة، ص١١٤.
٣) نظم المعلومات المحوسبة ، الاستاذ الدكتور عامر قنديلجي والدكتور علاء الدين الجنابي ، ص١٤٧.

٤ـ معلومة سرية يعرفها الاشخاص المصرح لهم فقط مثل كلمة المرور والرقم السري .

٥ـ المصافحة وفيها يتم اعطاء المستخدم عملية سرية او دالة سرية تكون معروفة للحاسب وعندما يريد المستخدم الدخول للنظام فان الحاسب يعطيه رقماً عشوائيا وينتظر أجابته يقوم المستخدم بحساب القيمة طبقا للعملية السرية أو الدالة السرية ويدخلها للحاسب ليسمح له بالدخول الى النظام .

ب- وسائل احقيات او متيازات الدخول الى البيانات :- ويتم فيها استخدام مصفوفة الدخول التي تنظم علاقة ثلاثية بين المستخدم – والمصادر العملياتية التي من حق المستخدم الدخول اليها (تسمى الاقفال) وامتيازات دخول المستخدم المعين على المصادر الخاصه به (تسمى المفاتيح) وتشمل تفاعلات التعامل مثل القراءه فقط – القراءه والكتابة – (التعديل – الاضافة –الحذف) ويجب ان يتم التحكم في احقية الدخول على المعلومات وعلى عمليات التشغيل للنظام على اساس مطالب التأمين والسرية [١].

٢ـ قواعد التحكم في احقية الدخول :- يجب مراعاه العوامل التالية عند تحديد قواعد التحكم في احقية الدخول :-

أ- التمييز بين قواعد التي يمكن ان تكون اجبارية والقواعد الاختيارية .

ب- تاسيس قواعد التحكم اما على اساس القاعده الحذرة :- (عموما كل شيء غير مصرح به مالم يسمح به بشكل واضح).

او القاعده المرنة :- (كل شيء مسموح به طالما لم يتم تحريمه).

ج- عند اعداد المعلومات يتم مراعاة التغير في تصنيف وترقيم المعلومات التي تتم بوسائل الية وذلك الترقيم المحدد بواسطة تقدير المستخدم .

هـ - مراعاه التغير في احقية الدخول الممنوحة للمستخدم التي تتم بوسائل الية وتلك المعطاه له من قبل الادارة .

و- التميز بين القواعد التي تتطلب لموافقة اضافية من المدير وتلك التي لاتحتاج موافقات اضافية [٢].

---

١) نظم المعلومات المحوسبة، المصدر السابق ،ص١٤٧ .
٢) تكنولوجيا أمنية المعلومات وأنظمة الحماية ، المصدر السابق ، ص١٤٩ .

٣- سياسة أحقية الدخول الى الشبكات :- يعني تامين وحماية خدمات الشبكات والذي يلزم احكام التحكم في الدخول على خدمات الشبكات الداخلية والخارجية – وسائل التحكم هذه ضرورية لضمان المستخدمين الذين لديهم احقية الدخول على الشبكات لايعرضوا تامين خدمات الشبكات للخطر ، من الضروري التاكد من اجراءات التحكم التالية :-

أ- وجود وصلات ربط ملائمة ومؤمنة بين شبكة المؤسسة والشبكات المملوكة للمؤسسات الاخرى والشبكات العامة .

ب – تنفيذ اليات مناسبة للتحقق من هوية مستخدمي الشبكات والأجهزة .

ج- وجود وسائل سيطرة لاحقية وصلاحيات دخول المستخدم للحصول على المعلومات .[١]

١)تكنولوجيا أمنية المعلومات وأنظمة الحماية،المصدر السابق ،ص١٥٧ .

الفصل الثالث

أولا:-أمنية الشبكات (Network security)

منذ بداية استخدام الحاسوب كانت هناك حاجة لأدوات مؤتمنة كحماية الملفات الاخرى المخزونة في الحاسوب .

إن هذه الحاجة واضحة في النظام المشترك (Shared system) مثل نظام المشاركة الزمنية (Time – sharing system) وقد أصبحت الحاجة أكثر لأنظمة يمكن الوصول إليها من خلال الهاتف الوطني أو شبكة البيانات ، إن الاسم العام لمجموعة الأدوات المصممة كحماية البيانات ومقاومة التطفل هو أمنية الحاسوب (Computer security) .

كان التغير الكبير الثاني الذي اثر على الأمنية هو بداية استخدام الأنظمة الموزعة واستخدام تسهيلات الشبكات والاتصالات لنقل البيانات بين محطة المستخدم والحاسوب وحاسوب أخر، وهناك حاجة مطلوبة لإجراءات حماية الشبكة من اجل حماية البيانات خلال إرسالها وبالحقيقة إن مصطلح أمنية الشبكة (Network security) هو بصورة افتراضية يربط جميع الإعمال والحكومة والتنظيمات الأكاديمية ببياناتها وأجهزة معالجاتها مع مجموعة من الشبكات المترابطة داخليا مثل هذا التجمع يشار له عادة على أنة انترنت (Internet)[1] .

ولإدارة ملائمة للشبكات ومواقع الشبكات هي شبكات المنطقة الواسعة و الانترنت (Wide area network and internet)، وان أمنية شبكات المنطقة الواسعة هي معقدة وذلك بسب المسافة والحجم لان هناك حاجة لكل مضيف وكل شبكة موقعيه (Local area network [LAN]) مرتبطة بالانترنت:-

أولا:- المسافة والحجم (Distance and size):-

من الممكن تفيذ امنية شبكة تتمتلك عقد في مناطق متعددة ومن الأمثلة عليها هي التنظيمات العسكرية فلها شبكات كبيرة جدا وهي أمينة تماما.[2]

---

١) تكنولوجيا أمنية المعلومات وأنظمة الحماية، المصدر السابق، ص٢٢.
٢) شبكات المعلومات والاتصالات، المصدر السابق، ص٤٢٧.

وشركات متعددة الجنسية كبيرة مثل مقدمي الاتصالات السلكية والشركات المصنعة لها وشبكات أمنية مشابهة فالمسافة والحجم تؤثر على أمنية إذا كانت الشبكة هي غير مدارة بطريقة واضحة ومتناغمة .

ثانيا:- الداخلين والخارجين (Insiders and outsiders):- يستخدم لوصف سياج افتراضي يفصل الموارد الخارجة عن الموارد الداخلية فكلما يرتفع عدد المضيفات المنفصلة تزداد المسافة بينهما.

ثالثا:- الملكية والمسؤولية (ownership and responsibility):-

يختلف الانترنت عن بقية الشبكات الاخرى بشئ واحد مهم فإنها مازالت مملوكة أو مسيطر عليها من قبل سلطة واحدة.كانت نوعيات أريا /انترنت مازالت مفتوحة وخاضعة للتجربة ومرنة، إن الجانب المشرق هو التقدم المثير في تكنولوجيا الشبكة الذي تم تحقيقه بفترة قصيرة إما الجانب السلبي فقدت روح الجماعة والديمقراطية والشعبية بسب الرسميات في الارتباط بالانترنت [1].

ثانيا:- أمنية المعلومات (Information security):-

لحصر احتياجات الأمنية لأي مؤسسة بصورة كفوءة ولتقيم واختيار السياسات والمنتجات الأمنية المختلفة ،فأن المدير المسؤل عن الأمنية يحتاج إلى طريقة نظامية لتحديد المتطلبات الأمنية ورسم الطرق الخاصة بتحقيق هذه المتطلبات ويتم ذلك بتحديد ثلاث مواضيع أمنية للمعلومات وهي :-

أ)الهجوم الأمني (Security attack):- هو أي عمل يخترق أمنية المعلومات العائدة لأي مؤسسة

ب) الإلية الأمنية (security mechanism):- إلية صممت للكشف اوالمنع أو النقاهة من الهجوم الأمني .

ج) الخدمة الأمنية (security service):- خدمة تضيف الأمنية إلى أنظمة معالجة البيانات ونقل المعلومات لأي مؤسسة هدف الخدمات هو احتواء ومجابهة الهجومات الأمنية باستخدام إلية أمنية واحدة أو أكثر لتأمين الخدمة[2].

---

١)شبكات المعلومات والاتصالات، المصدر السابق، ص٤٢٧- ٤٢٨.

٢)مدخل إلى امن المعلومات ،د.بدرخان والدكتور محمد ميثم ،الطبعة الأولى ٢٠٠٢ ،جامعة القاهرة –مصر، ص٣٢ .

ثالثا :- السياسة الأمنية لنظم المعلومات :-

السياسة الأمنية تعني تضمين وتنفيذ المفهوم الشامل لأمن وحماية نظام المعلومات والشبكات شاملا ذلك تحديد أهم المخاطر التي قد يتعرض لها النظام من مرحلة التصميم إلى مرحلة التشغيل الفعلي وكذلك الوسائل المختلفة للحماية بدءا من التحكم في الدخول لمصادر المعلومات والشبكات وامتيازات التعامل مع المصادر وتصنيف المصادر التشغيلية والتحكم في تدفق البيانات والتحكم في جميع مصادر تشغيل النظام ومنتهيا باستغلال وسائل التشفير إثناء استخدام الشبكات وعند تخزين المعلومات .ويتم تفصيل وتدعيم توجيهات الإدارة فيما يخص تامين المعلومات حيث تضع إدارة المؤسسة من خلالها اتجاه واضح وتدعيم التزامات وصيانة لسياسة تامين المعلومات عبر المؤسسة[1].

وثيقة السياسة الأمنية لنظم المعلومات :-

يجب إن تصدق إدارة المؤسسة على وثيقة السياسة الأمنية وتعمل على نشرها وتوجيهها إلى كل المستفدين من نظام المعلومات ومن المهم إن تعكس الوثيقة نظرة الإدارة إلى تامين المعلومات ومن أهم تلك التوجيهات :-

١)تعريف تامين المعلومات:- أهدافه العامة ومجاله وأهمية التامين كإلية للمشاركة المؤمنة في البيانات ومصادر المعلومات.

٢)بيان يوضح نية الإدارة ويدعم الأهداف ومبادئ تامين المعلومات.

٣)تفسير قصير عن السياسة الأمنية:-مبادئها ومطالب الالتزام بها ومعايير الأهمية المعنية للمؤسسة- ومثال ذلك:-

أ)التزام بالمطالب التشريعية والتعاقدية. ب)مطالب التدريب على التامين والسرية .

ج) منع وكشف الفيروسات الخبيثة الاخرى. د)إدارة استمرارية العمل.

٤)علامات وإشارات انتهاكات سياسة الأمن.

٥)تعريف المسؤوليات العامة والمعنية بإدارة تامين المعلومات ويتضمن كتابة تقارير حوادث الأمن[2].

---

١)إدارة تامين نظم وشبكات المعلومات، المصدر السابق، ص٥٥.

٢)حماية وامن الشبكات المعلومات ،المصدر السابق ،ص١٦١.

٦)المرجع الوثائقي الذي يؤيد السياسة الأمنية :- مثال على ذلك سياسات وإجراءات الأمن الأكثر تفصيلا لأجزاء معنية من نظام المعلومات الذي يلزم إن يمثل بة مستعملي النظام .

ويتم نشر السياسة الأمنية وشرحها في كافة إنحاء المؤسسة إلى المستفدين ومن له علاقة بنظام المعلومات في الشكل المفهوم لديهم وبطريقة سهل الوصول إليها .

وتتضمن وثيقة السياسة الأمنية المعلومات التالية :-

١)التعريف بالسياسة الأمنية :-هي خطة تحدد ماهي أصول المؤسسة الحرجة وكيف يمكن حمايتها كما تزود السياسة الموظفين بصلاحيات التعامل مع أصول المؤسسة و بالتالي يصبح الموظفين مسؤولين عن حماية المعلومات .

٢)التعرف بأهداف السياسة الأمنية :-

أ)تحديد كيفية معالجة المعلومات ذات درجات السرية العالية.

ب)تحديد كيفية الاحتفاظ بشكل امن بهوية كل موظف وكلمة السر بالإضافة إلى أي بيانات ذات خصوصية أخرى .

ج)تحديد كيفية التعامل مع حادثة امن محتملة أو محاولة تداخل أو اختراق – الخ .

د)تحديد كيفية استعمال الربط مع الانترنت وأجهزة العمل بطريقة أمنة.

هـ)تحديد كيفية استعمال نظام البريد الالكتروني للمؤسسات بشكل صحيح .

٣)كيفية التخطيط لبناء السياسة الأمنية .

٤)استكشاف تام للمصادر التشغيلية للمؤسسة .

٥)كيفية تحليل المخاطر المحتملة على تلك المصادر .

٦)كيفية تطوير أساليب السرية والتامين والحماية.

٧)كيفية تطوير أساليب الاكتشاف السريع للانتهاكات والمخاطر على النظام الأمني .

٨)كيفية تدريب الموظفين على الإجراءات الأمنية .

٩)كيفية اختبار كفاءة النظام الأمني.

١٠)كيفية التغلب على الانتهاكات والمخاطر واسترجاع النظام لحالته الأولية .[1]

---

١)حماية وامن المعلومات ،المصدر السابق ،ص١٦١ – ١٦٢ .

رابعا:- تصميم النظام الأمني (security system design):-

هناك الكثير من الحوادث والكوارث التي أدت إلى فقدان بعض المؤسسات لمعلوماتها وأنظمتها المعلوماتية بصورة عامة مما أدى إلى فقدانها لسوق العمل بينما هناك مؤسسات أخرى جابهت هذه الإخطار من خلال إحساسها الأمني واتخاذها الإجراءات المناسبة للحيلولة دون حدوث الكوارث .ومازالت الحماية في معظم المؤسسات بعيدة عن الجدية وذلك للأسباب التالية :-

أ)الأمنية غير ملائمة:-معظم التقنيات المستخدمة التي تميز المستخدمين المخولين هي نفسها متعادلة التأثير على إعاقة (Hindering) المستخدمين المخولين.

ب)تحميل التقنية لمشكلة الأمنية:-يحب إن يعرف دائما إن الأمن هي مشكلة إنسانية وليست تقنية.

ج)تباهي المؤسسات بأنها محمية :-إن العديد من جرائم الحواسيب هي غير معلنة لان المدراء يخفون هذه الجرائم عن زبائنهم حتى لاتتشوة صورة مؤسساتهم .

هـ)الحذر من المشكلة فقط غير كافي ولذلك يكون من الضروري كما هو دائما التقدم بخطوة واحدة تجاة الحل ويجب ان لاتكون هي الخطوة الأخيرة .

ز)هناك دائماشخاص (المدراء –المسؤولين –الخ) يعتقدون بعدم وجود مشكلة اسمها أمنية .[1]

تعتبر أمنية الحاسوب مهنة خاصة بالخبراء محترفي أنظمة المعلومات ،خبراء الأمنية والموظفين الكبار و كان للحواسيب الشخصية دور في نشر قدرة المعالجة إلى الموظفين على مختلف طبيعة إعمالهم فان مسؤولية الأمن قد توزعت على هؤلاء الموظفين ومشرفيهم ومدراهم ،حيث يبقى المدير هو المسؤول الرئيسي للأمن .

ولكن مازال يتمتع بعض المحترفون بمسؤولية مهمة لأنة يجب عليهم تحديد طبيعة بيانات مؤسساتهم وأنواع التهديدات التي تجابهها ،ويجب عليهم وضع وتنفيذ الخطط لحماية لبيانات من هذه التهديدات ودائما يحتاج المحترفون إلى درجة عالية من المعرفة التقنية .[2]

---

١) أسس تصميم الشبكات الحاسوبية ، د. المهندس بسام محمد عضو هيئة التدريسية في قسم الهندسة الالكترونية /كلية الهندسة الميكانيكية والكهربائية ، جامعة دمشق ،ص ٤٠ .

٢) تكنولوجيا المعلومات وأنظمة الحماية ، المصدر السابق ،ص٤٣٠.

في عالم الحاسوب ،حتى تكملة هذه الأهداف ذات التخصيصة العالية فإنها لاتكفي للحفاظ على أمنية الحواسيب في الحقيقة ،يمكن القول هذه الأيام بان عمل محترفي الأمنية بصورة رئيسة إسناد الجهود المبذولة من المدراء غير المتخصصين .[١]

المبادئ الأساسية في تصميم النظام الأمني (Basic principles) أهم تلك المبادئ هي:-

١)يجب إن تكون كلفة الوصول إلى المعلومات من قبل المتطفل هي اعلي من قيمة المعلومات نفسها.

٢)يجب إن ترسخ في الأذهان فكرة عدم وجود نظام امني متكامل وهناك ثغرات موجودة يجب ردمها من خلال اخذ كل الاحتمالات عند التصميم ووضع أسس لمراجعة النظام الأمني عند تنفيذه .

٣)كلفة النظام الأمني:- يجب إن تكون كلفة النظام الأمني وتعقيده متوازية مع قيمة المعلومات التي يحميها فكلما كانت قيمة المعلومات كبيرة كلما كان النظام الأمني أكثر تعقيدا والعكس صحيح.

٤)المعلومات لمن يحتاجها :-من الضروري إظهار اقل مايمكن من المعلومات المطلوبة إلى الأشخاص المخولين عند إرسال هذه المعلومات من حاسوب إلى أخر .

٥)يجب إن يكون النظام الأمني قادرا على حماية نفسه ضد المتطفلين.

٦)اعرف عدوك :- يتميز المتطفلون في مجال المعلوماتية بكونهم خبراء في مجال الحاسوب ولديهم الإمكانيات المتقدمة والخبرة في اختراق أنظمة الحواسيب والشبكات لذلك يجب إن تكون أنظمة الحماية معتمدة على أخر التقنيات الحديثة في تصميمها لتجابه هذا التحدي .

٧)أسبقيات الحماية :- ضع الأسبقيات للبيانات الواجب حمايتها أولا ووسائل الحماية التي يجب وضعها لاتكن قصير النظر بحيث تفكر بالبيانات المخزونة في مؤسستك فقط بل فكر بالبيانات التي ترسل من والى مؤسستك .[٢]

---

١)تكنولوجيا أمنية المعلومات وأنظمة الحماية، المصدر السابق، ص٤٣٠.

٢)أسس تصميم الشبكات الحاسوبية ،المصدر السابق ،ص٥٧ ــ ٥٨ .

الفصل الرابع

أولا:- السياسات الأمنية:-

إن العنصر الرئيسي في أي خطة يجب إن تكون سياسة أمنية مؤثره. ويلزم إن يكون هناك مالك أو صاحب للسياسة الأمنية ويكون مسؤلا عن صيانتها ومراجعتها طبقا للخطة الموضوعة للمراجعة . وتضمن هذه العملية بأن تكون ذا اثر فعال على أي متغيرات تؤثر على أسس تقدير المخاطر الأمنية من حيث أهميتها وتأثيرها ومثال ذلك :- تحليل للحوادث الأمنية الهامة –نقاط الضعف والمتغيرات الجديدة في البنية التنظيمية أو التقنية لنظام معلومات والسياسات الأمنية .[1]

ولابد من تقيم ومراجعة السياسات الأمنية بشكل دوري ويتم ذلك كالأتي:-

١)تأثير السياسة الأمنية على عدد ونوعية حوادث الأمن المسجلة وتأثيرها على كفاءة نظام المعلومات .

٢)تكلفة وتأثير وسائل التحكم الأمنية على كفاءة العمل.

٣)تأثيرات التقنية على المتغيرات في وسائل السياسة الأمنية .

ويهدف بناء السياسة الأمنية الجيدة بالمؤسسات إلى التطبيق الناجح لأمن النظم الحالية وما يتعلق بالمشاريع المستقبلية ،إن الخطوة الأولى الإلزامية نحو تحسين امن المؤسسة هو إعلام وإلزام الموظفين بالسياسة الأمنية وعلاقتها بمسؤلياتهم تجاه تامين خصوصة معلومات ومصادر المؤسسة مايؤدي لسرعة الاكتشاف والتسجيل والتغلب على الأنشطة الممنوعة .

إن التطوير والتطبيق الصحيح للسياسة الأمنية سوف يحول الموظفين إلى مشاركون في جهد المؤسسة ويضمن المساعدة في تخفيض خطر الاختراقات الأمنية التي تنشأ من أخطاء العامل البشري مثل الاستعمال غير الأمن أو غير الصحيح لشبكة الانترنت والعديد من الأنشطة الخطرة الاخرى ، وتساعد عملية بناء السياسة الأمنية على التعريف بأصول المؤسسة الحرجة التي يلزم إن تكون بعيده

---

١) نظم المعلومات المحوسبة ، المصدر السابق ، ص١٦٨.

٢) مدخل إلى امن المعلومات ، المصدر السابق ، ص١٤١.

قدر الإمكان عن جميع أنواع المخاطر باستخدام وسائل التامين والحماية وإجراءات السياسة الأمنية [٢].

ثانيا/ الجرائم عبر الشبكة :-

هنالك العديد من الجرائم والتجاوزات وأساءه الاستخدام عبر النظم الحاسوبية والشبكات وهي في تزايد مستمر ومن هذه الجرائم :-

أ- القرصنة والاختراق(Hacking).

حيث يستغل القراصنة نقاط الضعف في الجوانب الأمنية لمواقع الشبكة العنكبوتية (الويب) فيحصلوا على فرص للدخول إلى البيانات الخاصة بهم ، مثل المعلومات الخاصة عن الزبائن ، وكلمات المرور . وقد يستخدم هؤلاء القراصنة أنواع من الفيروسات.

والقراصنة أو الهاكرز (Hackers) يعمدون عادة الدخول إلى نظام التشغيل في أجهزة المستخدمين الآخرين بطريقة غير مشروعة ، لإغراض غير مشروعة كالسرقة والتخريب عن طريق نقل أو مسح ملفات وبرامج أو إضافة ملفات وبرامج وباستطاعة القرصان المخترق إن يسيطر على جهاز التشغيل ويتحكم به فيصدر أوامر التصوير والطباعة والتخزين . وهنالك عدة جوانب تساعد الشخص على الدخول إلى جهاز ونظام الحاسوب :-

١)ارتباط جهاز أو نظام الحاسوب بالانترنيت والشبكة العنكبوتية حيث انه لايستطيع المخترق الدخول إلى نظام أو جهاز الحاسوب غير المرتبط بالشبكة .

٢)وجود مايسمى بملف (Patch) أو ملف (Trojan) في جهاز الحاسوب المعني بالارتباط وهذه الملفات يحتاجها مستخدم الحاسوب في عمليات ارتباطه بالحواسيب الاخرى وتعامله معها ففي هذا النوع من الملفات يستطيع المخترق وضع اسم مستخدم (User Name) ورمز سري (Password) تخوله بان يدخل إلى حاسوب المستخدم .

٣)استخدام احد برامج القرصنة المعروفة مثل:- (Girlfriend, Hackers Utility, NetBuster, Busscang) [١].

---

١)حماية وامن شبكات المعلومات ، المصدر السابق ،ص١٧٨.

ب- الجرائم المالية والاقتصادية :-

تشمل جرائم السطو على أرقام البطاقات الائتمانية (Credit Cards) ولعب القمار، التزوير، وغسيل الأموال وهي من الجرائم التي اشتهر محاربتها جنائيا.فجرائم السطو على أرقام البطاقات الائتمانية تعتبر من أشهر الجرائم المالية، وأكثرها تأثيرا على الإفراد والمؤسسات المالية والمصرفية. فمنذ إن بدا مفهوم التجارة الالكترونية ينتشر في السبعينات من القرن الماضي ، وفي ضوء عدد من العوامل المشجعة لعملية التبادل التجاري والشراء والبيع الكترونيا فمن هذه العوامل مثل إمكانية اختزال العمليات الورقية والبشرية ،والسرعة في إرسال البيانات ،وتخفيض تكلفة التشغيل ،تحولت العديد من الشركات الإعمال إلى استخدام الشبكات الحاسوبية والانترنت والاستفادة من مزايا التجارة الالكترونية .حيث أصبح الاستيلاء على بطاقات الائتمان عبر الانترنت ممكنا وأصبح لصوص بطاقات الائتمان يستطيعون سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم يبيع هذه المعلومات للآخرين، بغرض الاستفادة منها في سرقة أموال الآخرين.[١]

ثالثا:- أمثلة على الاختراقات والتسلل:-

هناك العديد من الاختراقات والتسلل والاقتحام للمواقع الرسمية أو الشخصية:-

١) تسلل إلى وزارات الدفاع والعدل والمخابرات المركزية والقوات الجوية في الولايات المتحدة الأمريكية

٢) قيام قراصنة اسرائيلين باقتحام صفحة الانترنت الإعلامية الخاصة ببنك فلسطين المحدود ووضعوا بها صورا وشعارات معادية مما اضطر البنك إلى إلغاء الصفحة ومحوها كليا .

٣)في عام (١٩٩٧) قدرت وكاله المباحث الفيدرالية الأمريكية (FBI) تعرض (٤٣؟) من الشركات التي تستخدم شبكة الانترنت المحولة لعمليات تسلل تتراوح مابين (١- ٥) مرات خلال سنة واحدة.

٤)وكذلك هناك بعض الهواة محاوله منهم ملا أوقات الفراغ ومنهم هناك فتاة مراهقة في الخامسة عشر من عمرها قامت بمحاولة التسلل إلى الصفحة العنكبوتية الخاصة بقاعدة عسكرية للغواصات الحربية بسنغافورة .[٢]

٥)في عام (١٩٩٧)قام مراهق بالتسلل إلى نظام مراقبة حركة الملاحة الجوية في مطار ماشيتيوس (Massachusetts) مما أدى إلى تعطيل نظام الملاحة الجويةوانظمة أخرى حيوية لمدة ستة ساعات .

٦)وكذلك في حرب الخليج الأولى عندما اجروا تحقيقا حول تسلل أشخاص إلى صفحة الانترنت العنكبوتية الخاصة بإحدى القواعد العسكرية الأمريكية وقد اتضح إن المتسللين هما مراهقان كان يبعثان بجهاز الحاسب الآلي في منزلهما .[1]

رابعا :- الإجراءات الأمنية للشبكات المعلومات :-

لابد إن يتم إجراءات أمنية للشبكات المعلومات ليتم السيطرة بواسطة طرق إدارية وتقليص الخطر المرتبط بالأجهزة والنظم الحاسوبية فيتم ذلك عن طريق الاهتمام بالأوساط الخزينة ،الإسناد البيئة ،المخازن المغناطيسية وفصل الواجبات .وهناك العديد من الإجراءات التي يتم بها تحسن استخدام أمنية الحواسيب:-

أ)لاتترك الحواسيب الشخصية اوغيرها بدون رقابة في بيئة مكشوفة إذا كانت تحتوي على معلومات حساسة أو تنفذ حسابات مهمة .لقد جعلت سهولة الاستخدام للبرمجيات بساطة للمستخدمين غير الماهرين تعلم كيفية الاستخدام للحزم الجديدة.

ب)لاتترك الطابعات بدون رقابة إذا كانت تطبع تقارير سرية هذا التحديد مهم بصورة خاصة إذا كانت الطابعة مشتركة من قبل حاسوبين أو أكثر إذا كان موقع الطابعة هو مكان عام .

ج)امن الوسائط الخزينة بعناية وبصورة مكافئة للتقارير السرية .تحتوي الأقراص على معلومات سرية يجب المحافظة عليها والحواسيب ذات الأقراص الصلبة المحتوية على معلومات سرية يجب المحافظة عليها .

---

١)مدخل إلى امن المعلومات ،المصدر السابق ،ص١٧٨- ١٧٩ .
٢)نظم المعلومات المحوسبة ،المصدر السابق ،ص.١٤٠ .

هـ) استخدام نسخ الإسناد بفترات زمنية:- اعتماد على أهمية التطبيقات فان الاستنساخ اليومي للملفات المتغيرة من القرص الصلب إلى أقراص أو أجهزة.[٢]

قد يكون من الأفضل استنساخ الملف كل مرة يتغير فيها.

ز)طبق فصل الصلاحيات :- صمم طرق أمنية حتى لايكون شخص واحد يمتلك صلاحية التأثير على البيانات السرية . مثلا صمم أنظمة محاسبة حتى يتم إدامة البيانات على نظامين من قبل شخصين حتى يمكن موازنة الأرقام النهائية بين النظامين بهذه الطريقة فأن التزييف يحتاج آلة تعاون الفريقين.[١]

خامسا :- نظام المعلومات في الشبكة :-

يقوم بتزويد المنظمة بالمعلومات الضرورية اللازمة لصناعة واتخاذ القرارات وذلك في الوقت المناسب وعند المستوى الإداري الملائم ومثل ذلك النظام يقوم باستقبال البيانات ونقلها وتخزينها ومعالجتها واسترجاعها ثم توصليها بذاتها أو بعد تشغيلها إلى مستخدميها في الوقت المناسب والمكان المناسب .

ومن أهم خصائص نظام المعلومات في الشبكة الأتي :-

أ) الرسالة (Message):- هي مجموعة من الحروف والرموز يمكن نقلها وتخزينها ومعالجتها من خلال نظام للمعلومات بالمنظمة ومحتوى وقيمة الرسالة يختلفان من مستوى إداري إلى أخر بل إنهما قد يختلفان من شخص إلى أخر في المستوى الإداري نفسه وعند الشخص نفسه من وقت إلى أخر فالرسالة قد تمثل بيانات (... Data) عند مستوى معين أو في وقت معين وقد تمثل معلومات عند مستوى أخر أو في وقت مختلف .

ب)البيانات والمعلومات:-

البيانات هي مجموعة من الحروف والرموز تعبر عن الحقائق والمواقف الحالات والآراء المتعلقة بالإحداث التي يمكن التعرف عليها وقياسها وغالبا ماتكون البيانات مستقلة عن بعضها البعض إلا أنها قابلة للنقل والتخزين والمعالجة من خلال نظام للمعلومات بالمنظمة وعلى الرغم من إن شيوع

---

١)نظم المعلومات المحوسبة ،المصدر السابق ،ص١٤٠ .

٢) www.pdffactory.com .

استخدام اصطلاح (بيانات Data) كمرادف لاصطلاح معلومات (Information) فأنة يمكن القول بان البيانات هي المادة الخام للمعلومات فالثانية هي نتاج تشغيل أو معالجة الأولى سواء بإجراء بعض العمليات عليها أو تخزينها .[٢]

ج)التشغيل والمعالجة الفعالة للبيانات من خلال استخدام معدات (Hardware) وبرمجيات (Software) فاعلة من اجل الحصول على المعلومات.

هـ)إدارة فعالة للمعلومات مع التركيز على عملية إدارة ملفات المعلومات وعمليات ضمان وامن وسلامة هذه الملفات .

ز) المرونة بحيث يمكن للنظام إن يعالج عمليات متنوعة تتعلق بالبيانات والمعلومات.

د)تحقيق متطلبات المستفدين من النظام .[١]

وفي الحقيقة إن تدفق وتوفر المعلومات الذي يواجه المديرين ومتخذي القرار حاليا قد يكون سلاحا ذا حدين، ذلك إن متخذي القرار إذا أمكنة السيطرة على هذه المعلومات فإنها ذات اثر فاعل في اتخاذه للقرار السليم في الوقت المناسب.

إما إذا عجز عن ذلك فان الطوفان من المعلومات قد يجرفه إلى اتخاذ قرارات خاطئة فنشأت الحاجة إلى مستويات متعددة من نظم المعلومات قد تتوفر كلها أو بعضها في المنطقة حسب حجمها ودرجة اعتمادها على الأساليب المتطورة في الإدارة .[٢]

ويمكن القول بصفة عامة بان كل فعل (Action) يسبقه قرار (Decision) وفي نطاق منظمات الإعمال (Bussiness organization) نجد إن هناك من يعرف القرار في نظم المعلومات ((تخصيص غير مردود للموارد)) وفي رأينا إن العملية القرارية لاتقف عند نقطة واحدة في نظم المعلومات بل تشمل عدة نقاط ومراحل مهمة هي :-

ا) صناعة القرار.

ب)اتخاذ القرار وإصدار تعليمات تنفيذه.

ج) تنفيذ القرار (إجراءات الأفعال).

د)متابعة تنفيذ القرار.

---

١) www. Pdffactory.com .

٢)أسس تصميم الشبكات الحاسوبية ،المصدر السابق ،ص١١٥ .

فيتم صنع القرار في نظم المعلومات بتجميع البيانات ومعالجتها واستخلاص المعلومات التي تم البناء عليها ليتم اتخاذ القرار.[٣]

١)أسس تصميم الشبكات الحاسوبية ،المصدر السابق ،ص١١٥ .
٢)تحليل وتصميم نظم المعلومات، المصدر السابق، ص٨٨.
٣) المصدر نفسة ، ص٨٩ .

الاستنتاجات

١)إن الجبال الضخمة من البيانات والمعلومات المتوفرة في شبكات المعلومات معرضة للخطر إذا ليتم تخزينها وإدارتها وتداولها بأمان وسرية تامة.

٢)عدم قدرة نظم وشبكات المعلومات على تحقيق أهدافها يؤدي إلى عدم الثقة وانعدام اعتمادية المسؤولين على كافة مستويات نظام المعلومات عند اتخاذ القرارات .

٣)يجب استخدام نظم التحكم في الأصول لاماكن الحاسبات باعتبارها مناطق أمنية تسمح نظم التحكم في الدخول للمصرح لهم فقط بالتواجد في المناطق الأمنية وتمنع الآخرين غير المصرح لهم.

٤)إن التغير الكبير الذي اثر على الأمنية هو استخدام الأنظمة الموزعة واستخدام تسهيلات الشبكات والاتصالات لنقل البيانات بين محطة المستخدم والحاسوب وبين حاسوب أخر.

٥)يجب إن تصدق إدارة المؤسسة على الوثيقة السياسة الأمنية وتعمل على نشرها وتوجيهها إلى كل المستفدين من نظام المعلومات ومن المهم إن تعكس الوثيقة نظرة الإدارة إلى تامين المعلومات .

٦)يجب أن تكون كلفة الوصول إلى المعلومات من قبل المتطفل اعلي من قيمة المعلومات نفسها.

٧)أن الهاكرز دائما يعمدون الدخول إلى نظام التشغيل في أجهزة المستخدمين بطريقة غير مشروعة كالسرقة والتخريب وغيرها .

٨) يصمم أنظمة محاسبة حتى يتم إدامة البيانات على نظامين من قبل شخصين وبهذه الطريقة فان التزييف يحتاج إلى تعاون الفريقين.

١) يوصى مناقشة أفضل الممارسات القابلة للتطبيق التي تتعلق بالحماية ضد التهديدات لأمن المعلومات .

٢)يلزم قدر الإمكان تقليل وتقيد عدد المترددين أو الزائرين للمناطق الأمنية لشبكات المعلومات وبهذا يزداد فعالية نظام التحكم في الوصول .

٣)يوصى بتوفير درجة من الأمان لشبكات المعلومات ومواجهة ومعالجة مشاكل الحماية والتامين وخاصة إننا سوف نشهد في السنوات القادمة بناء الكثير من نظم وشبكات المعلومات.

٤) يوصى صيانة الاجهزه وفقا للفترات و المواصفات التي تحددها الشركة المنتجة وبواسطة الفنين المصرح لهم فقط .

٥)يوصى التعرف على المستخدم لاماكن الحاسبات الأمنية الخاصة للشبكات المعلومات وذلك بتحديد الاسم يليها التحقق من الشخصية للتأكد من إن المستخدم الذي حدد أسمة هو نفس المستخدم.

٦)يوصى بوضع الإدارة الأمنية لشبكات المعلومات بوضع بيان يوضح بيه الإدارة ويدعم الأهداف ومبادئ تامين المعلومات .

٧)يوصى بترسيخ في الأذهان فكرة عدم وجود نظام امني متكامل وهناك ثغرات موجودة يجب ردمها من خلال أخد كل الاحتمالات عند التصميم ووضع أسس لمراجعة النظام عند تنفيذه .

٨)لاتترك الحواسيب الشخصية أو غيرها بدون رقابة في بيئة مكشوفة إذا كانت تحتوي على معلومات أو تنفذ حسابات مهمة .

المصادر

أولا:- الكتب

١) أسس تصميم الشبكات الحاسوبية ،الدكتور المهندس بسام محمد ،عضو الهيئة التدريسية في قسم الالكترونية ،كلية الهندسة الميكانيكية والكهربائية ،جامعة دمشق .

٢) إدارة تامين نظم وشبكات المعلومات، دكتور احمد شربيني والدكتور وفائي بغدادي محمد، مكتبة الأسرة، ٢٠٠٨.

٣) تحليل وتصميم نظم المعلومات ، اروي عبد الرحمن الارياني ،ماجستير تحليل وتصميم نظم المعلومات ، جامعة سيتي –لندن ،الطبعة الأولى ،١٩٩٨ .

٤) تكنولوجيا أمنية المعلومات وأنظمة الحماية ، الأستاذ علاء حسين الحمامي والدكتور سعد عبد العزيز العاني ،جامعة عمان العربية للدراسات العليا –جامعة عمان الأهلي ،الطبعة الأولى ،دار النشر .

٥) حماية وامن شبكات المعلومات ،أ.د عامر تحسين سهيل الصميدعي ،جامعة قطر ،الطبعة الثانية ،١٩٩٩،دار الروائع للنشر .

٦) شبكات المعلومات والاتصالات ،الأستاذ عامر إبراهيم قنديلجي ،جامعة قطر – الدكتورة إيمان فاضل السامرائي ،جامعة قطر .

٧) مدخل إلى امن المعلومات ، د.بدر خان ودكتور محمد ميثم ، الطبعة الأولى ،٢٠٠٢ ،جامعة القاهرة –مصر .

٨) نظم المعلومات المحوسبة ،الأستاذ الدكتور عامر قنديلجي ،الدكتور علاء الدين الجنابي .

ثانيا:-الانترنت

١) www.C4arab.com .

٢) www.pdffactory.com .