الاتحاد الدولي للاتصالات

تأمين الانترنت وشبكات المعلومات

أ.د/ أحمد مصطفى الشربينى

أستاذ نظم الاتصالات والشبكات
بكلية الهندسة جامعة القاهرة

أ.م.د/وفائى بغدادى محمد

استشارى نظم وشبكات المعلومات

تقـــــديـــم

تعتمد الحكومات والمؤسسات والأفراد فى الوقت الراهن بصورة متزايدة على المعلومات التي يجرى تداولها عبر شبكات الاتصالات المتقدمة خاصة الإنترنت – ومع زيادة استخدامات شبكات المعلومات والإنترنت، تزداد أهمية نظم التأمين والحماية للحفاظ على سرية البيانات والمعلومات ومكونات الشبكة.

ويعمل المكتب الإقليمي العربي للاتحاد الدولي للاتصالات جاهداً من أجل التصدي للتحديات المرتبطة بمجتمع المعلومات والاتصالات خاصة فى الدول العربية. ومن أبرز التحديات التي تواجه أمن وسلامة مجتمع المعلومات والاتصالات، الاختراقات الأمنية والدخول غير المشروع على البيانات والرسائل الاقتحامية والجرائم الأمنية وزرع الفيروسات وهجمات منع الخدمة.

ويتصدى الاتحاد الدولي للاتصالات لهذة التحديات من خلال عدة محاور – من أهمها:

1- وضع المعايير القياسية الأمنية التى تحدد مستويات الأداء والأمن في مجالات التكنولوجيات والأنظمة والمنتجات على نحو يحافظ على كفاءة الشبكات ويعزز بناء الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

2- تقديم المساعدة التقنية المباشرة من خلال المكاتب الإقليمية للاتحاد من أجل بناء قدرات الدول الأعضاء على تنسيق الاستراتيجيات الوطنية وحماية البنية التحتية للشبكات ضد المخاطر.

3- إصدار المراجع والوثائق الخاصة بتعزيز ثقافة أمن المعلومات والشبكات وتوعية المجتمع المعلوماتي لمواطن الضعف المتعلقة بأمن استخدام الشبكات وخاصة الإنترنت.

ومن هذا المنطلق يقدم الاتحاد الدولي للاتصالات هذا الكتاب بعنوان "تأمين الإنترنت وشبكات المعلومات" والذي يعتبر أول كتاب متخصص من نوعه باللغة العربية يتعرض لوسائل التغلب على مخاطر اقتحام الشبكات والإنترنت ويوضح استخدام المعدات والبرامج التقنية ووضع الاشتراطات الأمنية للشبكات وبناء السياسة الأمنية وتطوير الهيكل التنظيمي المساند وأمن اتصالات الطوارئ.

ويأمل الاتحاد الدولي للاتصالات أن يلاقي هذا الكتاب قبول القارئ العربي المتخصص والمؤسسات والهيئات المستخدمة لشبكات الاتصال والإنترنت وأن يساهم فى رفع المستوى المعرفي والتقني للعاملين في قطاع الاتصالات وتكنولوجيا المعلومات من أجل بناء واستخدام شبكات أكثر أمنا وأكثر اعتمادية.

سامي البشير المرشد

مدير قطاع تنمية الاتصالات

محتويات الكتاب

الفصل السادس: تأمين الإنترنت

الفصل الأول

المقدمة

بدأت الطفرة الهائلة في عالم الحاسبات والإنترنت بربط نظم المعلومات بعضها ببعض من خلال الشبكات وكان هذا إيذاناً بظهور "نظم شبكات المعلومات الموزعة" وأصبح بمقدور المستخدمين أن يتبادلوا البيانات دون استخدام التقارير المطبوعة وكانت النتيجة طفرة هائلة في مستوى الاستغلال الأمثل لمصادر شبكات المعلومات وفى معدل إنتاجية النظم حيث حلت النظم الموزعة محل النظم المركزية وأصبح المستخدمون يمتلكون الآن هذه القوة الهائلة رهن أصابعهم وأصبح لديهم البرامج الخاصة بالمعالجة الموزعة وحلت الحاسبات الشخصية وحاسبات الميكرو زهيدة التكلفة محل الحاسبات السوبر والعملاقة. والآن ومع تزايد قوة وطاقة نظم المعلومات والشبكات أصبح ممكناً ميكنة المكاتب والفروع. وظهر أيضاً مجتمع الحكومات الإلكترونية ونظم المدفوعات الإلكترونية حيث تتم أعمال البيع والشراء وعقد كافة أنواع الصفقات بواسطة البنوك والشركات بأوامر من عملاءهم وباستخدام الإنترنت.

ويتجه العالم المعاصر بخطى حثيثة ومتأنية نحو مجتمع المعلومات الذي يتسم بأنه مجتمع لا حدود له غير متأثر بالمسافة أو الوقت. كما تعتبر اقتصاديات وسياسات ومجتمعات اليوم مبنية أقل على البنية الأساسية الجغرافية والطبيعية عما كانت عليه في الماضي وصارت حالياً تعتمد بزيادة مطردة على البنية الأساسية لنظم وتطبيقات المعلومات في البيئة الرقمية التي أصبحت تفيد الحكومات والمنظمات والمؤسسات والأفراد على حد سواء. وصارت هذه النظم والتطبيقات المعلوماتية تمثل جزءاً مكملاً وأساسياً لأنشطة الشؤون المالية والصناعة والإدارة والتجارة وكافة تطبيقات الأعمال على المستوى القومي والدولي. وعلى هذا الأساس صارت هذه النظم والتطبيقات الرقمية تستخدم في أداء كثير من الخدمات والأنشطة الحكومية من خلال الحكومات الإلكترونية (E-Government) والتعلم الإلكتروني (E-Learning) وإدارة الأعمال عن بعد والتجارة الإلكترونية والطب البعيد ... الخ. وتقدم استخدامات تطبيقات وخدمات شبكات المعلومات مدى واسع وممتد من الإمكانيات في الوصول الأعظم للموارد والخبرة والتعلم والمشاركة في الحياة المدنية والثقافية للمواطن العادي.

أمن شبكات المعلومات من زاوية أكاديمية هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للبيانات ومصادر المعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. ومن زاوية قانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفير المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الحاسب والإنترنت).

واستخدام اصطلاح أمن شبكات المعلومات (Information Network Security) ولد مع الاستخدامات الهائلة لتكنولوجيا المعلومات والاتصالات وأصبح استخدامه الشائع بل والفعلي في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحاسبات الآلية والاتصالات. إذ مع شيوع الوسائل التقنية لمعالجة وتخزين البيانات وتداولها والتفاعل معها عبر شبكات المعلومات وتحديداً الإنترنت. واحتلت أبحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.

إذن الهدف الأساسي من تأمين وحماية الإنترنت وشبكات المعلومات هو استخدام الوسائل التي تحقق توفير أقصى مستوى من التأمين والحماية بدون أن يكون هناك تأثير ملحوظ على كفاءة دخول المستخدمين على موارد النظام (الحاسبات – الشبكات – التطبيقات – قواعد البيانات) وعلى كفاءة عمل هذه الموارد.

يشمل التأمين كل عناصر النظام المعرضة للمخاطر وللتهديد شاملاً أمن الأفراد والبيانات والبرمجيات وتطبيقات العمل ومصادر النظام الآلية وأساليب العمل. كما يشمل الأمن ضد اختراقات الشبكات المحلية والواسعة والإنترنت. ويتم التأمين باستخدام تقنيات مثل حق الدخول (للتعرف والتحقق والتصريح للمستخدمين) والتشفير والجدران النارية واكتشاف ومنع التداخلات ومنع زرع الفيروسات والبرامج الخبيثة الأخرى.

وتشمل الحماية الأمن الطبيعي لمكان الحاسبات والأمن المادي للحاسبات واستخدام النسخ الاحتياطية من البرامج والبيانات والتحصين لمنع الإشعاع الصادر من شبكات الاتصال. ولكي تكون وسائل التأمين والحماية فعالة فإنه يلزم وجود "كيان أو عناصر أمن" ضمن الهيكل التنظيمي للمؤسسة مهمته التنفيذ المستمر ومتابعة سلسلة متصلة من المراحل المتتالية أو ما يعرف "بالسياسة الأمنية لمواجهة الأخطار" تبدأ من مرحلة الإجراءات التقنية والإدارية والقانونية اللازمة ثم مرحلة إجراءات التحليل لطبيعة المخاطر التي حدثت وسبب حدوثها وكيفية منع حدوثها في المستقبل. وأخيراً إجراءات التعافي والعودة إلى الوضع الطبيعي قبل حدوث الخطر مع مراعاة تنفيذ ما أظهره نتائج التحليل فيما يخص كيفية حدوث المخاطر والإجراءات التي تضمن عدم حدوثها مرة أخرى. المراجع أرقام (1 و24 و25 و26 و27)].

في دراسات هامة يقدمها مكتب الإحصائيات العام الأمريكي (U.S. General Accounting Office GAO) منذ عام 1996 أوضحت أن شبكة حاسبات وزارة الدفاع الأمريكية قابلة للاختراقات الأمنية بنسبة ليست بسيطة [المراجع أرقام (43 و67)]. وقد تضمنت الدراسات أن وكالة أمن نظام المعلومات (Defense Information System Agency DISA) قد وجهت في فترة زمنية عدة هجمات أمنية لقياس مدى مقاومة شبكة وزارة الدفاع الأمريكية للمخاطر والاختراقات الأمنية. وقد نجح منها 38000 هجمة في اختراق شبكة وزارة الدفاع الأمريكية وتم الدخول على حواسب الشبكة لفترة تقدر بـــ 65% من إجمالي وقت عمل المستخدمين المصرح لهم. ونجحت "تقنيات التأمين والحماية" المزود به شبكة حواسب وزارة الدفاع الأمريكية في اكتشاف نسبة 4% فقط من الاختراقات الأمنية الناجحة (حوالي 988 اختراق). ورغم ذلك اتضح أن نسبة 27% منها (حوالي 267 اختراق) قد تم الإبلاغ عنها بتقارير إلى مدير النظام وإلى "كيان الأمن" تنفيذاً لإجراءات "السياسة الأمنية".

ولو أخذنا في الاعتبار أن شبكة وزارة الدفاع الأمريكية هي أكثر شبكات المعلومات أمناً وتعقيداً على مستوى العالم فإنه يمكن استخلاص عدة نتائج من هذه الدراسات من أهمها:

1) نظام التأمين والحماية الشامل هو تكامل بين نظامين فرعيين هما "تقنيات التأمين والحماية" و"السياسة الأمنية".

2) لا توجد شبكة معلومات مؤمنة ومحمية بنسبة 100% ولكن تختلف نسبة التأمين والحماية طبقاً للوسائل الخاصة بالوقاية. سرعة اكتشاف الاختراقات الأمنية – سرعة استرجاع حالة النظام – الردع حتى لا تتكرر نفس حالات الاختراق – ثم سياسة استمرارية العمل تحت مختلف الظروف من خلال وجود مواقع بديلة (Disaster Recovery Sites).

3) مع كل يوم جديد ثمة جديد في ميدان المخاطر والاختراقات الأمنية لأنه في كل يوم يوجد الجديد من التقنيات والبرمجيات والبروتوكولات. وفي كل يوم البشرية أمام مبرمج يتفتق ذهنه عن ابتكار أو اختراع جديد في عالم الإنترنت وشبكات المعلومات وهو إما ابتكار جديد مفيد وإيجابي يستخدم في رخاء البشرية وضمن الاستخدام الإيجابي للإبداع العقلي أو جديد مدمر وسلبي يستثمر في تحقيق أغراض غير مشروعة أو في ارتكاب أفعال مجرمة أو أفعال يأباها السلوك الأخلاقي القويم. وبالتالي فإن تحديد ومجابهة التهديدات والثغرات والاعتداءات عملية مستمرة، يوماً بعد يوم وهي من أهم ما يميز خطط الأمن بعضها عن بعض.

4) خطط الأمن الفعالة يجب تطويرها باستمرار لملاحقة كل ما هو جديد في الاختراقات الأمنية ووسائل التأمين المضادة من نواحي عديدة منها: اقتناء أحدث تقنيات التأمين – التدريب والوعي المستمر – تفعيل إجراءات السياسة الأمنية خاصة إدارة المخاطر إلى تضمن سرعة الإبلاغ عن الحوادث الأمنية.

وفى عالم اليوم تلعب تكنولوجيا المعلومات والشبكات دوراً هاماً وأساسياً في جميع المؤسسات حيث يتم من خلال نظم المعلومات التعامل مع البيانات للحصول على المعلومات التي تعتبر مورداً أساسياً تعتمد عليه كل المستويات الإدارية لتحقيق العديد من أهداف المؤسسات. كما أن الاتجاه الحالي في مجال تكنولوجيا المعلومات هو تعميق مفهوم زيادة الاعتماد على الشبكات وعلى رأسها الشبكة الدولية للمعلومات "الإنترنت" حيث تتيح الشبكات تحقيق الاتصال بين الحاسبات لتخاطب بعضها البعض في سهولة ويسر الأمر الذي سينعكس بشكل إيجابي على تحسين مستوى الخدمة والأداء وسهولة اتخاذ القرار بناء على توافر المعلومات والقدرة على تحليلها.

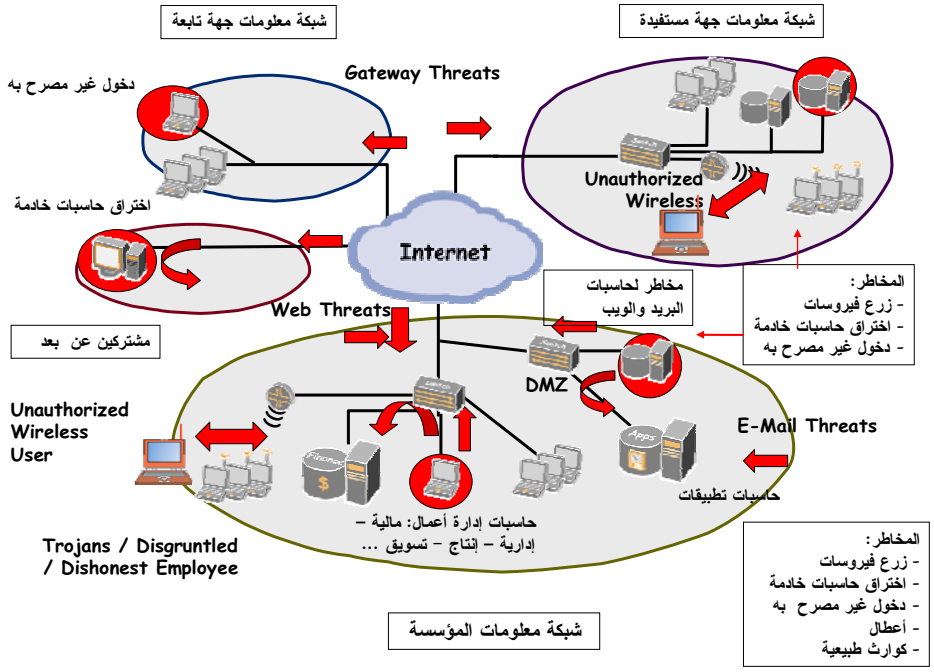
ونتيجة لسرعة انتشار شبكات المعلومات زادت مطالب المستفيدين من الشركات المنتجة لكي تصنع معدات وتطور تقنيات تحقق سهولة التعامل مع الشبكات باستخدام واجهات برامج تطبيقات (Application Program Interfaces) ذات أوامر وتعليمات تتيح لأي فرد استخدامها مما يكون له تأثير سلبي على تأمين الشبكات.

ومع دخولنا "عصر الإنترنت" زادت مشاكل السطو والسرقات المعلوماتية حيث تستخدم بروتوكولات الشبكة في تداول البيانات عبر شبكات اتصال مختلفة قد لا يعلم مستخدمي الشبكة خاصة من العالم الثالث الكثير عنها لذلك كان من الطبيعي أن تتعرض شبكات المعلومات للعديد من التهديدات على هيئة اختراقات وانتهاكات وتدمير وسرقة للمعلومات وحرمان من استغلال موارد الشبكة أو كجزء من حرب المعلومات.

والشكل رقم (1) يوضح التهديدات التي يمكن أن تتعرض لها شبكة معلومات مؤسسة ما تستخدم نظام المعلومات في تنفيذ تطبيقات العمل (Business Applications) الخاصة بالمؤسسة

والتي قد تشمل النظم الإدارية والنظم المالية ونظم الإنتاج ونظم التسويق بالإضافة إلى النظم المكتبية والبريد الإلكتروني وموقع المؤسسة على شبكة الإنترنت وباقي النظم الإلكترونية الحديثة. ولكي يؤدي نظام المعلومات مهامه يتم ربطه من خلال الشبكات العامة أو الإنترنت بالجهات التابعة للمؤسسة وبالجهات المستفيدة من نظام المعلومات كما يرتبط بها المشتركون عن بعد باستخدام وسائل الاتصال السلكية واللاسلكية.

1



الشكل رقم (1): التهديدات التي يمكن أن تتعرض لها شبكة معلومات مؤسسة

وبالرجوع إلى شكل رقم (1) يمكن حصر بعض التهديدات الشائعة التي قد تهدد شبكة معلومات المؤسسة ومنها: الاختراقات الأمنية للوصول إلى البيانات والمعلومات وحاسبات تطبيقات العمل مثل البريد الإلكتروني وموقع الويب للمؤسسة – زرع الفيروسات – سرقة البيانات والخدمات والأجهزة – أعطال في أجهزة ومعدات الحاسب – أعطال أو أخطاء في البرامج – أخطاء في استخدام الأنظمة ... الخ

والمعروف أن زيادة عدد الدخلاء والقراصنة والمتطفلين والمهاجمين والمتسللين (الهاكرز) (Hackers) والمتلصصين واللصوص (Message Tapping/ Eavesdroppers) على شبكات المعلومات يرجع إلى أسباب عديدة من أهمها:

1) سهولة بروتوكولات الربط (TCP/IP) ولغة التعامل مع الشبكة HTML والمتصفحات؛
2) الأخطاء البرمجية والعيوب في تصميم التطبيقات خاصة التي يتم نشرها للعامة؛
3) زيادة الاعتماد على المعلومات ذات القيمة العالية واعتبارها "ثروة" وزيادة عدد المتصلين بها عبر شبكات الاتصال مما أغرى الدخلاء والقراصنة والمتطفلين والمتلصصين؛
4) وجود برامج جاهزة تساعد على الاختراقات الأمنية ووجود وثائق على مواقع الإنترنت يؤلفها الهاكرز وتحتوى على خبراتهم في اختراق النظم.

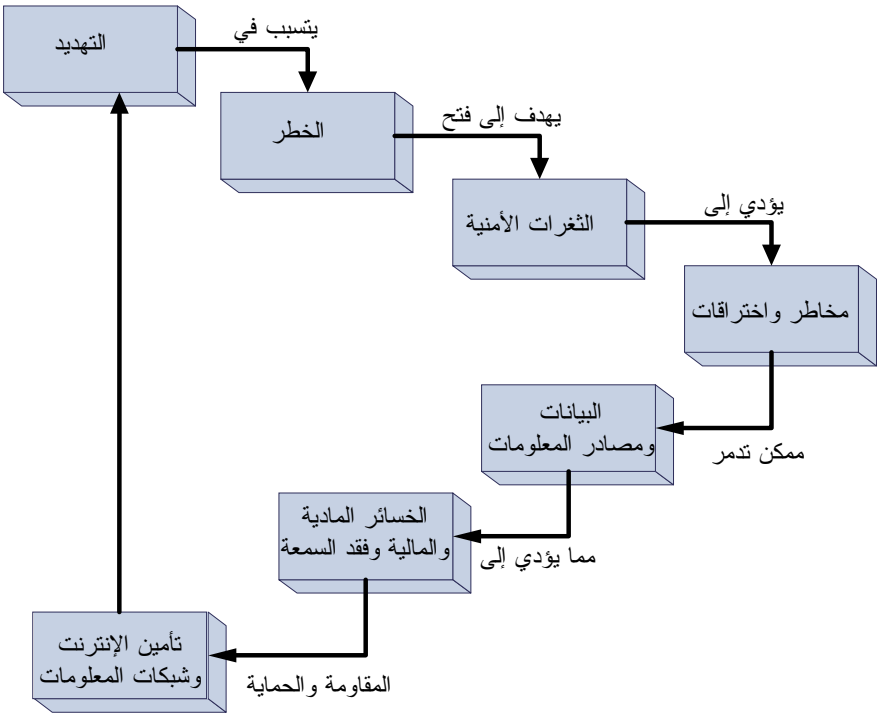
لذا يشكل أمن الإنترنت وشبكات المعلومات هاجساً لكل من يتعامل مع الحاسب الآلي والبيانات والمعلومات والشبكات وأصبح هناك عبء كبير على وسائل التأمين والحماية وعلى الأفراد العاملين في مجال تأمين شبكات المعلومات.

وكان من الطبيعي مع التوسع المستمر في استخدام الإنترنت وتزايد تطبيقاتها وخدماتها يوماً بعد يوم إلى طرح تساؤلات عديدة من قبل المستخدمين مثل: هل المعلومات خاصة الشخصية بمأمن من المتطفلين؟ وهل يمكن أن تنكشف معلومات حساب شخص ما للآخرين عندما يستعلم بواسطة الإنترنت؟ وهل من الممكن أن يسرق أحد رقم بطاقة الائتمان عند التسوق عبر الإنترنت؟ هل يمكن سرقة ابتكار أو اختراع جديد لشركة صرفت عليه أثناء البحث والتطوير وكانت ستجني من خلاله أرباحاً إذا تم تطبيقه؟

1-1 أهم المصطلحات المستخدمة في تأمين شبكات المعلومات

إن من المفيد في هذه المقدمة تقديم تعريفات للمصطلحات الشائعة المستخدمة في عالم التأمين والحماية ضد جرائم الإنترنت وشبكات المعلومات بهدف التمييز بين العديد من هذه المصطلحات التي قد يتم الخلط بينها فثمة فرق بين الجريمة الإلكترونية والإرهاب الإلكتروني وحرب المعلومات والتهديدات ونقاط الضعف والثغرات الأمنية والحوادث والكوارث الطبيعية وأخطاء التشغيل أو البرمجة وغيرها. والشكل رقم (2) يوضح الفروق بين التهديد والخطر والثغرات الأمنية.

2



الشكل رقم (2): الفروق بين التهديد والخطر والثغرات الأمنية

- التهديد Threats يعني الخطر المحتمل الذي يمكن أن تتعرض له الإنترنت وشبكات المعلومات وقد يكون مصدره شخصاً كالمتجسس أو المجرم المحترف أو الهاكرز المخترق. أو يكون شيئاً يهدد الأجهزة أو البرامج أو المعلومات أو حدثاً كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية.
- نقاط الضعف أو الثغرات الأمنية (Vulnerabilities) تعني عنصر أو منفذ أو بوابة أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق فمثلاً يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافياً لاستخدام النظام وحمايته – وقد يكون الاتصال بالإنترنت نقطة ضعف مثلاً إذا لم يكن مشفراً. وقد يكون الموقع المكاني للنظام نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية والحماية – وبالعموم فإن نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات أو المخاطر.
- يرتبط باصطلاح نقاط الضعف اصطلاح وسائل الوقاية (Countermeasures): وتعني التقنية المتبعة لحماية النظام ككلمات المرور والأقفال الإلكترونية ووسائل الرقابة والجدران النارية وغيرها.
- أما المخاطر (Risks) فإنها تستخدم بشكل مترادف مع تعبير التهديد مع إنها 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 وأخيراً وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف.

- أما الحوادث (Incident) فهو اصطلاح متسع يشمل المخاطر ويشمل الأخطاء وهو بالمعنى المستخدم في دراسات أمن المعلومات التقنية يشير إلى الأفعال المقصودة أو غير المقصودة ويغطي الاعتداءات والأخطاء الفنية.
- أما الهجمات (Attacks) فهو اصطلاح لوصف الاعتداءات بنتائجها أو بموضع الاستهداف فنقول هجمات إنكار الخدمة أو هجمات إرهابية أو هجمات البرمجيات أو هجمات الموظفين الحاقدين أو الهجمات المزاحية. ويستخدم كاصطلاح مرادف لاصطلاح الاختراقات (Penetrations) أو الثغرات (Vulnerabilities) أو الانتهاكات أو الإخلالات (Breaches) وهو اصطلاح توصف به مختلف أنماط الاعتداءات التقنية وبالتالي يكون مرادفاً أيضاً للاعتداءات.
- يستخدم مصطلح اللصوصية (Phishing) للتعبير عن سرقة الهوية وهو عمل إجرامي حيث يقوم شخص أو شركة بالتحايل والغش من خلال إرسال رسالة بريد إلكتروني مدعياً أنه من شركة مشهورة ويطلب الحصول من مستلم الرسالة على المعلومات الشخصية مثل تفاصيل الحسابات البنكية وكلمات المرور وتفاصيل البطاقة الائتمانية. وتستخدم هذه المعلومات للدخول إلى الحسابات البنكية عبر الإنترنت والدخول إلى مواقع الشركات التي تطلب البيانات الشخصية للدخول إلى الموقع.

أما في إطار الاصطلاحات الأكاديمية فإنه من المهم في هذا المقام تحديد الفرق بين ثلاث اصطلاحات تستخدم في ميدان الدراسات الأكاديمية:

- الأول وهو اصطلاح الجرائم الإلكترونية (Cyber crime) وهو الدال على مختلف جرائم الحاسب والإنترنت في الوقت الحاضر بالرغم من أن استخدامه ابتداء كان محصوراً بجرائم شبكة الإنترنت وحدها.
- أما الثاني فهو إرهاب السيبر أو إرهاب العالم الإلكتروني (Cyber Terrorism) وهي هجمات تستهدف نظم الحاسب والمعلومات لأغراض سياسية أو فكرية أو تنافسية وفي حقيقتها جزء من "الجرائم السيبرية" "السيبر كرايم" (Cyber crime) باعتبارها جرائم إتلاف للنظم والمعلومات أو جرائم تعطيل للمواقع وعمل الأنظمة لكنها تتميز عنها بسمات عديدة سنقف عليها لدى بحثنا لأنماط جرائم الحاسب ومن أبرزها إنها ممارسة لذات مفهوم الأفعال الإرهابية لكن في بيئة الحاسب والإنترنت وعبر الاستفادة من خبرات مجرمي الحاسب الحاقدين والمخربين والدخلاء.
- أما الاصطلاح الثالث فهو اصطلاح حرب المعلومات (Information warfare) وهو اصطلاح ظهر في بيئة الإنترنت للتعبير عن اعتداءات تعطيل المواقع وإنكار الخدمة والاستيلاء على المعلومات. وكما يشير الاصطلاح فإن الهجمات والهجمات المقابلة هي التي تدل على وجود حرب حقيقية. وبما أنها حرب فهي حرب بين جهات تتناقض مصالحها وتتعارض مواقفها لهذا تكون في الغالب هجمات ذات بعد سياسي أو هجمات منافسين حاقدين في قطاع الأعمال وهو ما يجعلها مترادفة هنا مع أعمال "الجرائم السيبرية" "السيبر كرايم" (Cyber crime). وهذا الاصطلاح في حقيقته اصطلاح إعلامي أكثر منه أكاديمي ويستخدم مرادفاً في غالبية التقارير لاصطلاح الهجمات الإرهابية الإلكترونية. ونجده لدى الكثيرين اصطلاح واسع الدلالة لشمول كل أنماط مخاطر وتهديدات واعتداءات وجرائم البيئة الإلكترونية. ونرى ضرورة قصر استخدامه على الهجمات والهجمات المضادة في ضوء حروب الرأي والمعتقد لتمييزه عن بقية أنشطة تعطيل المواقع التي لا تنطلق من مثل هذه الأغراض.

والجدير بالذكر أن جميع الشركات المنتجة لأجهزة الحاسب أو البرامج والتطبيقات وحلول نظم المعلومات تتبنى مفهوم الشبكات باعتباره هو مستقبل التكنولوجيا كما أنه لا بقاء للمؤسسات التي ما زالت مترددة في الاقتناع بهذا المفهوم الجديد وبالتالي فإن أمن شبكات المعلومات لم يعد خياراً وإنما واجباً لمن يبحث عن البقاء والاستمرار وزيادة الاعتماد على الأرشفة الإلكترونية للبيانات والمعلومات ودخول عالم الأعمال الإلكترونية رغم التخوف من تعرضه لبعض عمليات السرقة والاختراق والقرصنة والاحتيال.

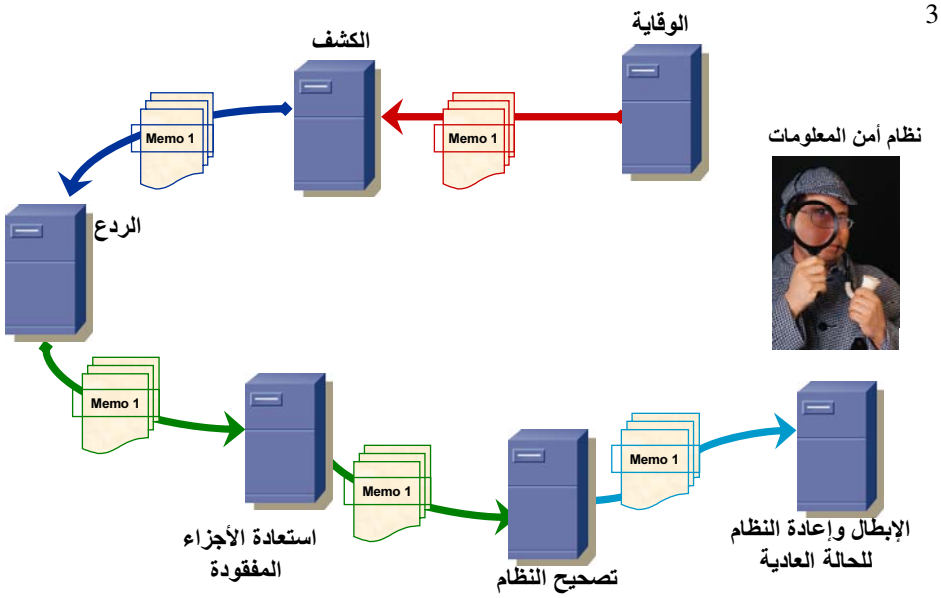
ومن هنا تظهر أهمية أمن الإنترنت وشبكات المعلومات حيث تمثل عمليات القرصنة على برامج الحاسب عبر الإنترنت خطورة بالغة على نظم المعلومات مما يستوجب دراسة وتطبيق الأساليب التي تؤدي إلى حماية مؤثرة لها من أي مشاكل أو مخاطر أو تهديدات قد تؤدي إلى فقد نظام المعلومات أو فقد تكامل البيانات أو قد تؤثر على كفاءة الأداء أو كفاءة مستويات السرية به.

كما يلزم وجود التشريعات القانونية لحماية برامج الحاسب الآلي وكذلك بحث الآثار السلبية لعمليات الاختراق التي يقوم بها المتطفلين والمتلصصين والقراصنة وزارعي الفيروسات والبرامج الخبيثة الأخرى على شبكات المعلومات بالمؤسسات سواء من داخل أو خارج المؤسسة مستخدمين الشبكات المحلية أو الواسعة أو عن طريق الإنترنت أو بطرق أخرى مختلفة.

يشمل تأمين الإنترنت وشبكات المعلومات كل العناصر المعرضة للمخاطر وللتهديد شاملاً ذلك الأمن الطبيعي لمكان الحاسبات والأمن المادي للحاسبات وأمن البرمجيات وأمن البيانات وأمن الأفراد وأمن التطبيقات والنظم الآلية والأمن ضد اختراقات الشبكات المحلية والواسعة والإنترنت بمنع زرع الفيروسات والبرامج الخبيثة الأخرى.

ويشمل التأمين الفعال وجود كيان بالمؤسسة خاص بالتأمين مهمته التنفيذ المستمر ومتابعة سلسلة متصلة من الأعمال الرئيسية (كما في الشكل رقم (3)) هي:

3



تصميم نظام المعلومات المؤمن

الشكل رقم (3): الأعمال الرئيسية لتصميم نظام المعلومات المؤمن

(1) الوقاية:

من الناحية النظرية فإن عدد كبير جداً من الوسائل والإجراءات الأمنية يمكن أن تؤدي إلى الوقاية الكاملة من كافة أنواع المخاطر والتهديدات المتوقعة وغير المتوقعة على نظام المعلومات والشبكات. ولكن من الناحية العملية يعتبر من غير المفيد حشد موارد لا نهائية للوصول إلى الوقاية الكاملة للنظام على حساب التكلفة الباهظة أو مستويات الأداء. ويفضل في هذه الحالة تنفيذ سياسة "إدارة المخاطر" التي تبدأ بتحديد موارد النظام ثم المخاطر التي قد تتعرض لها هذه الموارد وتأثير ذلك على مستويات الأداء يليها تحديد تكلفة تنفيذ تقنيات التأمين التي تحقق الوقاية من المخاطر.

وبصفة عامة لا يوجد نظام معلومات يحقق الوقاية التامة من كافة أنواع المخاطر والتهديدات المتوقعة وغير المتوقعة ورغم ذلك تعتبر الوقاية هدف أساسي تتمنى المؤسسات تحقيقه لنظام المعلومات الخاص بها.

(2) سرعة الكشف:

تتم سرعة الكشف عن المخاطر من خلال وسائل تقوم بمسح المكونات الرئيسية لنظام المعلومات والشبكات بواسطة مجسات أو مستشعرات. كما تقوم بتسجيل الاختراقات الأمنية ومحاولات الدخول غير المشروع وزرع البرامج الخبيثة سواء من داخل أو خارج المؤسسة. ومن الضروري أن تحقق هذه الوسائل إمكانية تحديد مصدر التهديد المشتبه فيه أو الفعلي حتى يمكن استكمال المراحل التالية من نظام التأمين.

(3) الردع:

تتضمن "السياسة الأمنية" وسائل الردع وإجراءات الحماية من المخاطر والاختراقات الأمنية شاملاً ذلك محاسبة الأفراد من داخل المؤسسة المتسببين بقصد أو بدون قصد في الاختراقات الأمنية كما تعتبر الإجراءات والقوانين الخاصة بسرية نظم المعلومات التي تصدرها الدولة وسيلة لتخويف المخربين من خارج المؤسسة من انكشاف أمرهم ومحاسبتهم.

(4) استعادة المعدات والبرامج والشبكات التي تعرضت للمخاطر:

تتم سرعة استعادة المعدات والبرامج والشبكات التي تعرضت للمخاطر من خلال:

أ) تنفيذ سياسة فعالة لتحقيق "استمرارية العمل" تحت مختلف الظروف.

ب) النقل والتحميل الدوري 'Backup' للمعلومات الموجودة في أوساط التخزين العاملة وذلك على وحدات تخزين منفصلة لاستخدامها عند حدوث أي عطل أو خطر يؤدي إلى الفقدان الكلي أو الجزئي لكفاءة نظام المعلومات.

ج) ازدواجية معدات الحاسبات (Fault tolerant- redundant- clustered) والشبكات.

د) وجود عدد احتياطي من المعدات والبرامج في الموقع العامل.

هـ) إنشاء موقع احتياطي للطوارئ "Disaster Recovery D/R site" ويفضل أن يكون الموقع الاحتياطي على مسافة حوالي 100 كم من الموقع العامل.

(5) تصحيح النظام:

توفر وسائل تصحيح النظام سرعة الإبلاغ عن حالات الاختراق والثغرات الأمنية ومواطن الضعف الأمني التي تم اكتشافها في أي من عناصر النظام (الأفراد – المكان – المعدات – البرامج – الأفراد – الشبكات المحلية والواسعة – الإنترنت – أساليب العمل) لغلق الثغرات الأمنية وتصحيحها بصفة مستمرة. كما يشمل ذلك التحصين المستمر للحاسبات الخادمة والشخصية من خلال التعديل المستمر بالمستحدثات Service Packs التي تصدرها الشركات المنتجة للبرمجيات بمجرد اكتشافها لثغرات أمنية في منتجاتها.

(6) الإبطال وإعادة النظام لتنفيذ تطبيقاته التي صمم من أجلها:

عندما تفشل جميع إجراءات التغلب على المخاطر الأمنية فإن الوسيلة الوحيدة الباقية هي إعادة تصميم عناصر النظام مرة أخرى بهدف وضع الإجراءات الأمنية في المراحل المختلفة من التصميم بدءاً من دراسة الجدوى ومارا بتحليل وتصميم وبرمجة وتشغيل وصيانة النظام. وقد يشمل ذلك إعادة تصميم الهيكل التنظيمي واختيار أفراد جديدة مؤهلة فنياً وامنياً.

مع الانتشار الكبير لشبكة الإنترنت واستخدامها من جانب المؤسسات والشركات في كثير من أعمالها كعقد الصفقات وتحويل الأموال وتبادل الرسائل ونقل المعلومات تواكب مع ذلك انتشار جرائم المعلوماتية مثل بناء ونشر برامج الفيروسات والدخول غير المشروع على شبكة الحاسبات وقرصنة المعلومات والتحايل على نظام المعالجة الآلية للبيانات لإتلاف البرامج وتزوير المستندات المعالجة إلكترونياً حيث يتم ذلك عن طريق قراصنة المعلومات المحترفين بجانب الشركات المنافسة أو الموظفين من داخل المؤسسات نفسها وهذه الفئة هي الأخطر والأقدر على اختراق الشبكات حيث تقدر الدراسات الحديثة أن النسبة الأكبر من الاختراقات تتم من خلال الإنترنت يليها ما يتم من خلال موظفي المؤسسات.

وتبرز أهمية وجود سياسة واضحة المعالم لتأمين نظم المعلومات بالمؤسسات ترتكز على مجموعة من المحاور المتكاملة والتي يجب تنفيذها بالتزامن هي:

1) التحكم في بداية التشغيل للحاسبات باستعمال كلمات المرور أو بطاقات الهوية أو الوسائل الحيوية الأكثر أمناً مثل بصمات الأصابع أو قاع العين أو الشبكية أو الصوت أو حرارة الجسم.
2) إضفاء شرعية توثيقية على هوية المستخدم 'Authentication' من خلال تكاملها مع تكنولوجيا توثيق الشرعية 'Authorization' والتي تعمل على تحديد الصلاحيات المتاحة للمستخدمين للشبكة الداخلية للمؤسسة وللإنترنت من حيث الاتصال والحصول على المعلومات والتعامل معها.
3) استغلال خوارزميات التشفير سواء على مستوى الملفات أو مستخدمي الحاسب أو تبادل الرسائل وهنا يمكن الاعتماد على حلول التشفير القومية التي تستخدم لتشفير الرسائل الإلكترونية ولا يسمح لأحد بقراءته إلا المرسل إليه فقط كما تستخدم وسائل أخرى مثل التوقيع الإلكتروني وشهادات التوثيق لحماية وتشفير الملفات أثناء تخزينها أو إرسالها بالإنترنت.

4) استخدام معدات وبرامج الجدران النارية (Firewall) وهو الدرع الأول في مواجهة الدخلاء من داخل أو خارج المؤسسة بدون أن يكون مصرح لهم بذلك مع إضافة حجب أو منع أو تصفية أو فلتر المواقع (Sites Filter) لمنع تعرض المستخدمين للمواقع غير المرغوب فيها.

5) استخدام وسائل نظام تأمين شبكات الحاسب ذات الطابع التكيفي شاملاً ذلك البحث الأمني 'Scanning Security' لإظهار نقاط الضعف التي يمكن من خلالها الاختراق إلى أي حاسب شخصي أو حاسب مركزي سواء من داخل الشبكة أو من خارجها ولضمان التأمين ضد أي محاولة.

6) ضرورة وجود ماسحات اكتشاف ومضادات للفيروسات 'Anti Virus Scanning' لحماية الحاسب والشبكات الإلكترونية والملفات التي يتم تحميلها من شبكة الإنترنت أو بواسطة أي مستخدم داخل الشبكة الداخلية بجانب 'URL Filtering' لتنقية المعلومات المستقبلة من أي موقع من البرامج غير المرغوب فيها علاوة على استخدام أكواد تأمين متنقلة "Mobile Security Code" لإيقاف عمل البرامج الضارة التي قد تنتقل أثناء التجوال على الإنترنت والشبكات.

7) التخزين الاحتياطي والتحميل الدوري "Backup" للمعلومات الموجودة في أوساط التخزين العاملة على وحدات تخزين منفصلة لتفادي حدوث أي عطل يؤدي إلى فقدان هذه المعلومات.

تشكل هذه المحاور منظومة متكاملة وسلسلة إجراءات متصلة تهدف إلى التأمين الشامل لنظام المعلومات بالمؤسسة مع الأخذ في الاعتبار أن تطبيق محور دون المحاور الأخرى يجعل سرية نظم المعلومات هشاً ضعيفاً ومعرض لانتشار الجرائم المعلوماتية من تجسس أو مسح أو تعديل للبيانات السرية الخاصة بتطبيقات العمل. ولضمان فعاليات تقنيات التأمين والسياسة الأمنية للإنترنت وشبكات المعلومات يجب الاستعانة بالخبراء المتخصصين لتقديم الاستشارات الفنية ورفع مستوى التوعية الأمنية والتدريب الفعال للعاملين.

تم تحديد معايير ووسائل أمن شبكات المعلومات ضمن توصيات إدارة أمن نظم وشبكات المعلومات التي من أهمها ما أصدرته كلاً من المنظمة الدولية للتوحيد القياسي International Standardization Organization (ISO) 7001 standard [المراجع أرقام (14 و23 و36 و37 و38)] والاتحاد الدولي للاتصالات International Telecommunication Union (ITU) [المراجع أرقام (10 و40 و41 و42)].

واشتملت التوصيات على معايير أمن شبكات المعلومات وعلى سياسة التأمين وإدارة المخاطر وتصنيف الأصول ورقابتها وأمن الأفراد والتأمين الطبيعي والبيئي لموقع المعدات والرقابة على الوصول وتطوير النظم وصيانتها وإدارة استمرارية الأعمال. وهذا ما ستتناوله بالتفصيل فصول هذا الكتاب.

ولقد استخدمنا في هذا الكتاب اصطلاح "مؤسسة" ليدل على أي جهة حكومية أو غير حكومية أو شركة أو منشأة أو ما شابه تستخدم الإنترنت وشبكات المعلومات في تنفيذ تطبيقات العمل الخاصة بها. كما راعينا كتابة المصطلحات التقنية باللغتين العربية والإنجليزية ليتيح للقارئ الحصول على فهم أكبر للفكرة المطروحة.

2-1 أهم الموضوعات التي يتناولها هذا الكتاب

يهدف هذا الكتاب إلى إلقاء الضوء على المخاطر والتهديدات التي قد تتعرض لها المؤسسات التي تعتمد على الإنترنت وشبكات المعلومات مع التركيز على كيفية توفير التأمين والحماية لها بالتقنيات وبالسياسة الأمنية.

وتعطى المعلومات الموجودة بالكتاب القارئ فكرة جيدة عن كل ما يتعلق بوسائل تأمين عناصر النظام من الأفراد وأساليب العمل ومصادر المعلومات والحاسبات والبرمجيات والشبكات وكافة التقنيات والإجراءات التي تحقق أفضل ممارسات تأمين للإنترنت ولشبكات المعلومات.

ويلزم التنويه على أنه نظراً للتطوير المستمر في أنواع الفيروسات والبرامج الخبيثة وأساليب زرعها في النظم وكذلك في طرق الاختراقات الأمنية التي قد تتغلب على تقنيات وإجراءات التأمين والحماية وفى المخاطر الأخرى بصفة عامة فإنه لا يمكن الوصول إلى النظام المؤمن بنسبة 100% مما يستلزم استمرارية بذل المؤسسات للجهود الخاصة بتأمين النظم واختيار أفضل الأفراد والمعدات والبرامج وأساليب العمل والشبكات التي تحمي قدر الإمكان من التهديدات التي قد تتعرض لها النظم حالياً ومستقبلاً. ونظراً لأن التقنيات التي سيتناولها الكتاب بالشرح مثل النظم الشفرية والجدران النارية ومنع الاختراقات ومضادات الفيروسات يتم تعديلها باستمرار كلما ظهرت تقنيات جديدة لمواجهة ما يستجد من مخاطر فإن مؤلفي الكتاب يعدون القارئ بإمداده بالمعلومات عن أحدث التقنيات في الإصدارات الجديدة للكتاب.

يناقش الكتاب الإطار الشامل لأمن الإنترنت وشبكات المعلومات حيث يوضح مراحل تصميم نظام التأمين والحماية للإنترنت ولشبكات المعلومات والوسائل والتقنيات الفنية والسياسات الأمنية التي تحقق التأمين لها شاملاً ذلك التأمين الطبيعي لمكان المعدات والتحكم في الدخول إلى البيانات ومصادر المعلومات وكذلك التحكم في تدفق البيانات والتحكم في محاولات الاستنتاج والتشفير. كما يوضح الكتاب كيفية تصنيف المعلومات ودور الأفراد في الأمن سواء كانوا مصدر للتأمين أو سواء كانوا مصدراً للمخاطر والاختراقات الأمنية من داخل أو من خارج المؤسسات. يناقش الكتاب أيضاً وسائل تطوير ومراجعة نظام الأمن عن طريق إدارة وتحليل المخاطر الأمنية ووضع خطط الطوارئ التي تضمن استمرارية عمل النظام تحت مختلف الظروف.

يتطرق الكتاب أيضاً إلى تفاصيل فنية عن الوسائل التقنية لتأمين شبكات المعلومات شاملاً ذلك: الجدران النارية – ترجمة العناوين – النطاقات الأمنية – التحقق من الهوية – التشفير – الشبكات الافتراضية المؤمنة – التوقيع الإلكتروني وشهادات التوثيق الخ.

كما يتضمن الكتاب العديد من جوانب المعرفة المتعلقة بأمن الإنترنت وشبكات المعلومات لأن التهديدات تتعاظم باستمرار خاصة مع استخدام وسائل الاختراقات والكشف غير المشروع والمعالجة التقنية المتاحة الآن على شبكة الإنترنت.

يمكّن الكتاب القارئ من معرفة كل ما يتعلق بهذه التقنيات ويساعده على تحديد أبعاد مشكلة التأمين بهدف الوصول إلى اتخاذ قرارات فعالة قابلة للتنفيذ بشأن تحقيق مستويات محددة من التأمين بقدر محدود من الموارد المالية والبشرية والمعدات والبرامج بحيث لا يعرض نظام المعلومات للمخاطر الأمنية من جهة ولا يرهق الموارد المالية للمؤسسة من الجهة الأخرى.

ولأنه كان لزاماً أن تظهر وسائل تقنية حديثة لمواجهة ما يستجد من التهديدات والاختراقات الأمنية سنبقى نؤكد ما ركزنا عليه في هذا الكتاب من أن التأمين والحماية عبر الوسائل التقنية تجيء لاحقة على التهديدات والاختراقات التقنية لهذا تظل التهديدات أسبق في الحدوث وتظل الحماية في موضع متأخر عنها. من هنا تظهر أهمية أن تكون بالمؤسسات "سياسة أمنية" فعالة يتابع تنفيذها "كيان أو إدارة أو قسم خاص بالأمن" ضمن الهيكل التنظيمي للمؤسسة ويتبع مباشرة الإدارات العليا بالمؤسسة بما يكفل التنفيذ المستمر والمتابعة لسلسلة متصلة من الأعمال الرئيسية التي تشارك تقنيات التأمين والأفراد في تنفيذها وهي: الوقاية – سرعة الكشف – الردع – استعادة المعدات والبرامج والشبكات التي تعرضت للمخاطر – وأخيراً الإبطال وإعادة النظام لتنفيذ تطبيقاته التي صمم من أجلها.

الفصل الثاني

شبكة الإنترنت

1-2 مقدمة

الإنترنت هي شبكة الشبكات وهى الشبكة التي تجمع مجموعة هائلة متصلة من شبكات الحاسب التي تضم كل الحاسبات الخادمة للتطبيقات وقواعد البيانات بالإضافة للموجهات (Routers) المرتبطة فيما بينها حول العالم. وتقوم الإنترنت بتبادل حزم البيانات بواسطة بروتوكول الإنترنت الموحد (IP) وتوفر الإنترنت العديد من الخدمات مثل الشبكة العنكبوتية العالمية (الويب www) وتقنيات البريد الإلكتروني (E-Mail) والتخاطب (Chat) ونقل الملفات FTP والمجموعات الإعلامية Usenet والاتصالات التليفونية والتعليم عن بعد والتجارة الإلكترونية. وأخيراً دخلت في العلاقات الإنسانية الاجتماعية (Social Relationship) من خلال مواقع حديثة أشهرها Face book. وتمثل الإنترنت اليوم ظاهرة لها تأثيرها الاجتماعي والثقافي في جميع بقاع العالم حيث أدت إلى تغيير المفاهيم التقليدية للعديد من المجالات منها على سبيل المثال إدارة الأعمال والتعليم والتجارة والصناعة والإعلام والمجتمع المدني والعلاقة بين الحكومة والأفراد وشكلت الإنترنت ما نراه يومياً من تطوير هائل لمجتمع المعلومات.

ولقد حدث تطور مذهل في عدد مستخدمي الإنترنت حيث زاد من 95 مليون شخص عام 1995 إلى 130 مليون عام 1998 وزاد العدد إلى 350 مليون عام 2003 ووصل العدد إلى 500 مليون عام 2005. والآن فقد بلغ عدد مستخدمي الإنترنت في العالم 1,319 بليون شخص. وتعد الصين أولى دول العالم في الزيادة السنوية لعدد مستخدمي الإنترنت الذين ارتفع ليبلغ 221 مليون شخص في شهر فبراير 2008 وبذلك احتلت الصين المرتبة الثالثة في استخدام الإنترنت بعد أمريكا ودول أوروبا وتخدم الإنترنت هذا العدد الضخم وتنمو بشكل سريع للغاية يصل إلى نسبة تصل إلى أكبر من 250% سنوياً [المراجع أرقام (34 و46)].

وقد بدأت فكرة الإنترنت أصلاً كفكرة شبكة حكومية عسكرية وامتدت إلى قطاع التعليم والأبحاث ثم التجارة حتى أصبحت الآن بعد ما حدث فيها من تطوير يهدف إلى انتشارها وسهولة التعامل معها في متناول جميع الفئات السنية والتعليمية. والإنترنت عالم مختلف تماماً عن علوم الحاسب. عالم يمكن لطفل في العاشرة أو لشخص متوسط التعليم الإبحار فيه والاستفادة بما يحتويه من معلومات هائلة ومتنوعة.

في البداية كان على مستخدم الإنترنت أن يكون على معرفة ببروتوكولات ونظم تشغيل معقدة كبروتوكول TCP/IP وكنظام التشغيل Unix أما الآن فلا يلزم سوى معرفة بسيطة بالحاسب لكي يتم الدخول إلى عالم الإنترنت. كما كان من الصعب في الماضي الدخول للإنترنت من خلال الشبكة التليفونية باستخدام حاسب المودم ولكن مع ظهور وسائل الاتصال الأخرى مثل قنوات الشبكات متكاملة الخدمات ISDN وقنوات ADSL والقنوات اللاسلكية ومع انتشار شركات توفير الخدمة (Internet Service Providers ISP) تبددت هذه الصعوبات.

وقد بدأ التغلب على هذه الصعوبة منذ أن بدأت المؤسسة الأمريكية CompuServe في توفير خدمة الدخول على الإنترنت عبر بروتوكولات Point-to-Point عام 1995 ومنذ هذا التاريخ لم يعد الدخول في الإنترنت أمراً صعباً.

في البداية اعتمدت اللغة الانجليزية كلغة أولية رسمية يفهمها مستخدمي ومطوري الإنترنت مما يستوجب معرفة بعض المصطلحات العلمية والقوائم بهذه اللغة. أما الآن فتوفر الإنترنت إمكانية التعامل مع كافة لغات العالم طبقاً للمطالب وأصبح الإبحار في الإنترنت مجاني تماماً ولكن الثمن الذي يتم دفعه هو مقابل توفير خدمة الاتصال.

2-2 نشأة الإنترنت

تعتبر الإنترنت ثورة جديدة في مجال الاتصالات والإعلام فإذا كانت الثورة الأولى في مجال الإعلام بدأت مع ظهور الطباعة ثم تلتها الصحافة فالسينما والراديو والتليفزيون وأخيراً البث الفضائي عبر الأقمار الصناعية. فإن الإنترنت استطاعت أن تجمع بين مختلف الوسائل الإعلامية في وسيلة واحدة حيث يستطيع المستخدم أن يقرأ ويسمع ويشاهد وأن يتفاعل مع هذه الشبكة العجيبة ويستطيع أن يتجول من بلد إلى بلد ومن شبكة إلى شبكة من القاهرة إلى سيدنى بأستراليا إلى طوكيو باليابان أو إلى لندن وبون أو واشنطن أو إلى أي مكان في العالم وهو في مقر عمله أو مكتبه أو غرفته شريطة أن يكون لديه حاسب مرتبط عبر التليفون أو لاسلكياً أو بواسطة الأقمار الصناعية بالشبكة الدولية للمعلومات الإنترنت.

كلمة الإنترنت جديدة في القاموس اللغوي لمختلف اللغات العالمية فهي مشتقة من الحروف الأولى من جملة INTERnational NETwork أو من تقنية INTERNETworking أو من جملة شبكة الشبكات (Network of Networks) أو أم الشبكات (Mother of Networks) – وهى تدل على أنها مجموعة هائلة من المعدات والبرامج والتطبيقات التي تستخدم تكنولوجيا المعلومات والاتصالات وهي أيضاً نظام معلومات عالمي. وباختصار شديد يمكن التعبير عنها بأنها شبكة عالمية تربط بين مختلف شبكات الحاسب على النطاق المحلي والعالمي لتجعلها منظومة متكاملة تساعد على التنقل في الفضاء الكوني الإلكتروني لهذه المنظومة العالمية المعقدة المرتبطة ببعضها عبر خطوط الهاتف والأقمار الصناعية وأجهزة الحاسب الآلي.

وأبسط ما يمكن القول عنها إنها شبكة عالمية من الحاسبات الآلية (Computer Networks) المتصلة مع بعضها البعض حول العالم.

وتحتوي الشبكة على مجموعة من الشبكات المحلية والشبكات داخل نفس الدولة المتصلة بباقي الشبكات الدولية عن طريق بوابات اتصال (Gateways) تربط الشبكات الدولية بعضها البعض على مستوى العالم مما يعطي المستخدم إمكانية الاتصال أو الارتباط بالشبكات البعيدة عنه عبر شبكات دولية في الدول الأخرى.

والإنترنت مصطلح جديد في القاموس اللغوي. وقد استخدم هذا المصطلح لأول مرة في (1973) في أوساط المختصين بهذه الشبكة وصناعتها والمعنيين ببرامج البحوث في مجال علم الحاسب الآلي في الولايات المتحدة الأمريكية.

استخدم هذا المصطلح في عام (1983) للتعبير عن مصطلح interconnecting of networks أي الشبكات المرتبطة ببعضها وكل منها يتكون من مجموعة من الحاسبات الآلية الكبيرة – وفي التسعينات استخدم هذا المصطلح وانتشر بشكل واسع وتم تحديده ليعني

الارتباط عبر مجموعة من شبكات الحاسب الآلي بشبكة الجمعية الوطنية للعلوم الأمريكية (NSF-NET National Science Foundation Network).

وتعتبر الإنترنت أضخم شبكة حاسبات في العالم وتضم داخلها الملايين من نظم الحاسب وشبكاتها في مختلف بلدان العالم وتعمل على اتصال مختلف أجهزة الحاسبات الآلية وشبكاتها مع بعضها البعض بواسطة خطوط اتصال ذات سرعات فائقة مكرسة على مدار الساعة لتأمين الاتصالات بين مختلف أطراف الشبكة. ويمكن لهذه المنظومة المعقدة من شبكات الحاسب الآلي القيام بالكثير من الأعمال التي تهم المشترك فهي تسهل له التواصل والارتباط بالعالم الخارجي عبر الإنترنت وبأقل التكاليف وذلك عبر استخدام تطبيقات وخدمات الشبكة مثل البريد الإلكتروني. كما تساعده على تصفح الوثائق والمستندات في أي مكان من العالم شريطة أن يكون مرتبطاً بالشبكة. وتعمل الشبكة على نقل المعلومات من حاسب عملاق كبير Mainframe and Super Computer إلى آخر أصغر أو حاسب شخصي PC وتحديث البيانات الموجودة به باستخدام أسلوب التحميل (down load) أو العكس أي نقل المعلومات والبرامج من الحاسبات الصغيرة للحاسبات العملاقة عبر أسلوب (up load). وكما تحقق المشاركة في مجموعات الحوارات والنقاش. وأخيراً توفير كافة أنواع المعلومات والخدمات.

3-2 خلفية تاريخية عن فكرة الإنترنت

تاريخياً بدأت شبكة الإنترنت في (1969) داخل مراكز البحوث ومختبرات وزارة الدفاع الأمريكية والأجهزة الحكومية ومراكز الأبحاث التابعة لها. وكان الهدف الأساسي لهذه الشبكة تأمين وسرعة الاتصال بين مختلف هذه الجهات لحماية الولايات المتحدة الأمريكية من خطر الحرب النووية نتيجة التهديد السوفيتي لها. حيث كانت فترة الستينات هي ذروة سنوات الحرب الباردة بين المعسكرين الشرقي بزعامة الاتحاد السوفييتي والغربي الذي تتزعمه الولايات المتحدة الأمريكية حيث شهدت هذه الفترة أزمة نشر الصواريخ السوفييتية في كوبا بتحريض من الرئيس كاسترو وإطلاق أول أقمار التجسس الروسية SpotnecII على تحركات الجيش الأمريكي وأصبح العالم على حافة حرب عالمية نووية بين المعسكرين.

وحيث إن كوبا على مرمى حجر من المدن الأمريكية وفي حالة نشوب حرب عالمية ستتأثر المدن الأمريكية بشكل فعال وستؤدي إلى تدمير كافة مرافق الاتصالات العسكرية والمدنية في الولايات المتحدة الأمريكية. فمن هذا المنطلق سعت وزارة الدفاع الأمريكية إلى ربط مختلف الجهات التابعة لوزارة الدفاع والمنتشرة بالولايات الأمريكية بشبكة اتصالات قوية وآمنة وقادرة على العمل في أشد وأصعب الظروف. شبكة قادرة على أن تعمل في حال نشوب حرب نووية وقادرة على أن تعمل في حالة تدمير شبكات الاتصالات الرئيسية وقادرة على ربط مختلف الولايات الأمريكية بعضها بالبعض وربط مراكز القيادة العسكرية والمدنية الأمريكية. ومن هنا جاءت أهمية إنشاء شبكة لوزارة الدفاع الأمريكية للربط بين نظم الحاسبات الآلية التي تنتجها شركات الحاسب الآلي الأمريكية IBM، DEC، Cray والمنتشرة في مراكز الأبحاث العسكرية والجامعات والمؤسسات الأمريكية المدنية والعسكرية.

وقد بدأ المشروع مع خطط وكالة مشروعات الأبحاث العسكرية المتقدمة Defense Advanced Research Projects Agency (DARPA) تحت مسمى شبكة مصادر الحاسبات المشتركة (Resource Sharing Computers Networks (RSCN)) وأطلق على الشبكة اسم "أربانت" Advanced Project Agency Network (ARPANET). ومنذ عام (1969) إلى اليوم حصل الكثير من التطور والتقدم في مجال ربط الحاسبات والشبكات الدولية بعضها بالبعض بفضل

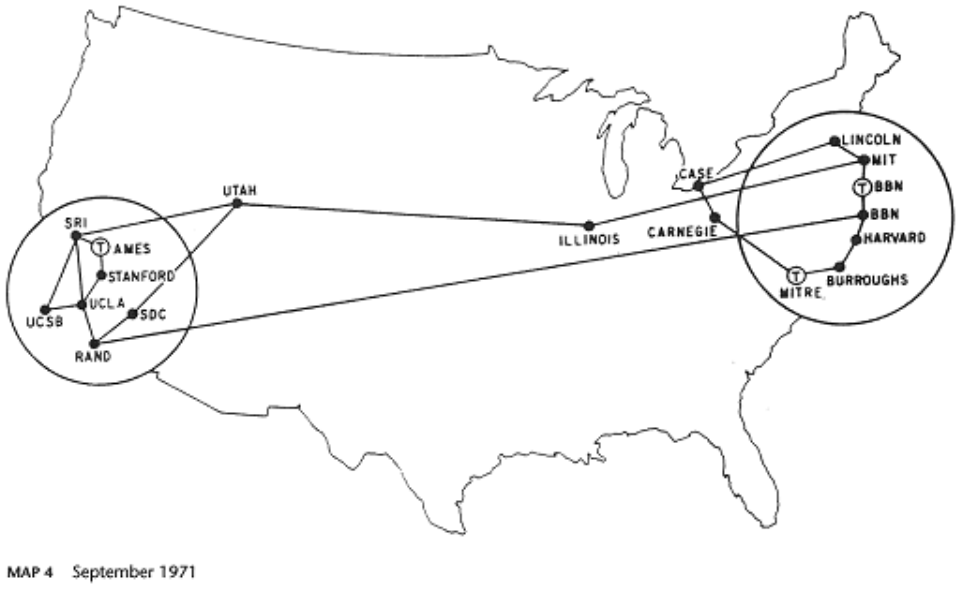
مشروع شبكة "أربانت" وما تلتها من شبكات مبنية على نفس تقنياتها وعلى رأسها الإنترنت. [المراجع أرقام (34 و65)].

4-2 تطوير الإنترنت

كما ذكرنا بدأت فكرة الإنترنت من خلال مشروع "أربانت" لربط مجموعة من الحاسبات الإلكترونية العملاقة (Mainframe and Super Computers) مع بعضها البعض لتمرير الرسائل والملفات والوثائق بين مختلف الشبكات. وكانت أهم الأهداف من إنشاء شبكة وزارة الدفاع الأمريكية ARPANET تحقيق التطبيقات العسكرية للجيش الأمريكي ومنها الآتي:

1) تأمين وسرعة الاتصال بين الجهات الأمنية والعسكرية الأمريكية.
2) ربط مختلف مناطق الولايات الأمريكية بشبكة اتصالات قوية وآمنة وقادرة على العمل في أشد وأصعب الظروف حتى في حالة نشوب حرب نووية وتدمير شبكات الاتصالات الرئيسية.
3) ربط مختلف الولايات الأمريكية بعضها ببعض لتبادل البيانات الحضارية الخاصة بكل ولاية.
4) ربط مراكز القيادة العسكرية والمدنية الأمريكية لتبادل المعلومات الخاصة بالأبحاث العسكرية.

الشكل رقم (1) يوضح شبكة ARPANET التي ربطت بين مراكز البحوث العسكرية للجيش الأمريكي. [المراجع أرقام (46 و65)].



الشكل رقم (1): شبكة ARPANET عام 1971
للربط بين مراكز البحوث العسكرية الأمريكية

في بداية تنفيذ الشبكة فشلت جميع محاولات ربط الحاسبات ببعضها نظراً لأن تصميم الحاسبات لم يأخذ في الاعتبار إمكانيات ووسائل الربط بينها. مما دعى وزارة الدفاع الأمريكية إلى تكليف شركة IBM بصفتها أكبر شركة في مجال حاسبات تنفيذ الأعمال International Business Machines لتطوير بروتوكول يحقق الربط بين مختلف أنظمة الحاسبات الآلية ويحقق تنفيذ تطبيقات الشبكات مثل البريد الإلكتروني ونقل الملفات والبحث في قواعد البيانات. ولقد طلبت وزارة الدفاع الأمريكية من الشركة الاستعانة بمراكز الأبحاث العسكرية والجامعات والمؤسسات الأمريكية العسكرية والمدنية (مثل Harvard وMIT وPoston). وخلال فترة نهاية الستينات والسبعينات بدأت الشبكة بالعمل كحقل تجريبي بين المعاهد ومراكز الأبحاث الأمريكية وخلال تلك الفترة إلى عام (1983) نجحت وزارة الدفاع الأمريكية في تطوير بروتوكول التحكم في الإرسال/بروتوكول الإنترنت (TCP/IP) ونما في أحضان شبكة وكالة مشروعات الأبحاث المتقدمة ARPANET. واعتبر يناير 1983 هو التاريخ الفعلي لميلاد عصر الحاسبات الآلية والشبكات والإنترنت.

ولقد تم إجراء العديد من التجارب على شبكة ARPANET ببروتوكول الاتصال TCP/IP ونفذ الكثير من الخطط والمشروعات لتحسين الشبكة وربطها جيداً بين مختلف مراكز البحوث للجيش الأمريكي حيث تم خلال السبعينات تطوير عمل هذا النظام ليشمل التحكم في مختلف وسائل الاتصال اللاسلكية (الأقمار الصناعية والميكروويف وموجات الراديو) والسلكية الأرضية والبحرية (الكوابل النحاسية وكوابل الألياف الضوئية التي تمثل حالياً البنية التحتية للاتصالات على مستوى كل دولة وعلى مستوى العالم) وقد تم تحقيق الترابط والاتصال بين مختلف وسائل الاتصال عبر استخدام عدد رهيب من مبدلات أو مقسمات أو محولات البيانات (Switches) والموجهات (Routers) وبوابات الربط (Gateways) التي تستطيع أن تتعامل مع كافة أنواع نظم التشغيل لمراكز الحاسبات الآلية والشبكات المتواجدة في الجامعات والمعاهد ومراكز الأبحاث.

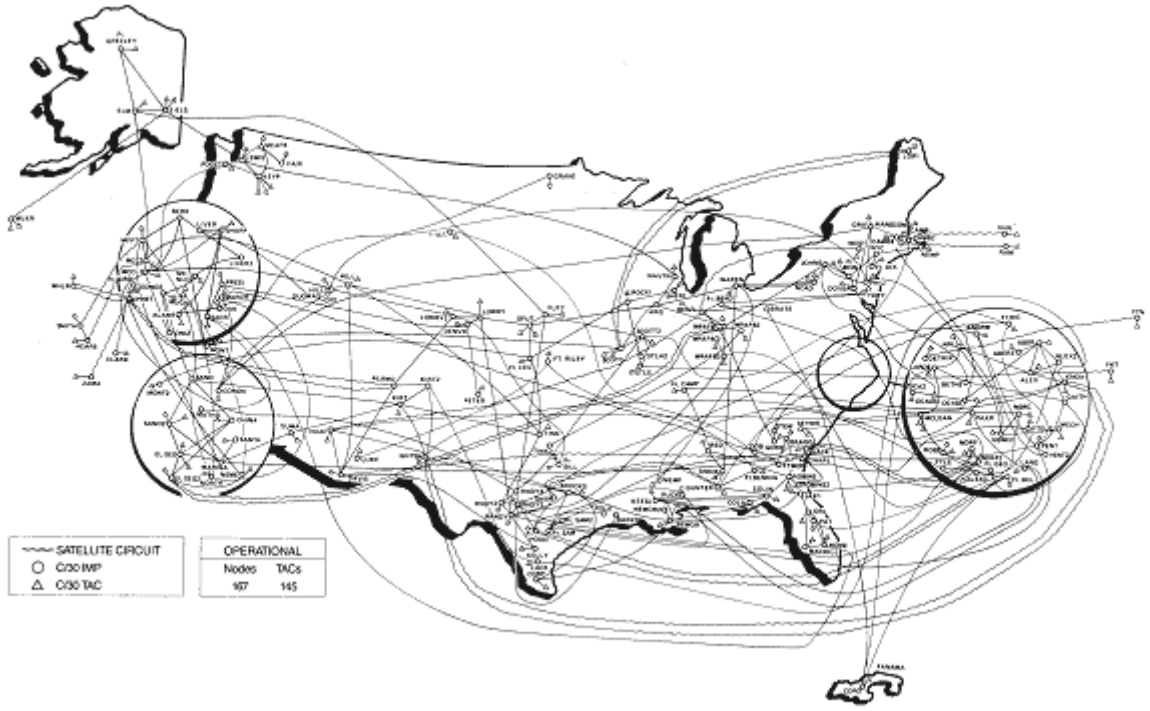
منذ عام 1983 وحتى يومنا هذا لا تستطيع أي شبكة أن تعمل إلا باستخدام نظام التحكم في الإرسال أو نظام الإنترنت (TCP/IP) للارتباط بالشبكة الأم أو للتوصيل إلى الشبكة المعلوماتية. وخلال هذه الفترة استطاعت مجموعة البحوث الخاصة بنظم تشغيل أجهزة الحاسب في جامعة كاليفورنيا بركلي (Berkeley) أن تخترع نظام تشغيل عسكري حر مبني على برامج التشغيل "يونكس" أطلق عليه اسم (MILSTD. BSD. UNIX) حيث ضمن هذا النظام الاستخدام الواسع للبروتوكول (TCP/IP). وعملياً بدأ التكامل بين نظام UNIX وبروتوكول الإنترنت من خلال تطبيقات البريد الإلكتروني والدخول عن بعد ونقل الملفات ليمثل هذا ما نراه ونحس به الآن من "ثورة تكنولوجيا شبكات المعلومات".

ومنذ يناير 1983 (وحتى الآن) دخلت الشبكة العسكرية (ARPANET) الخدمة الفعلية في الجيش الأمريكي لأول مرة كشبكة حقيقية واستطاعت أن تفتح أبوابها عبر وكالة الاتصالات الدفاعية الأمريكية لمختلف المراكز والجامعات التي تتعامل مع وزارة الدفاع الأمريكية.

وقد بدأت وزارة الدفاع الأمريكية بإنشاء شبكات منفصلة عن شبكة ARPANET وتستخدم نفس التقنيات والبروتوكولات الناجحة من أهمها:

شبكة للبريد الإلكتروني العسكري "ميل نت" (Mil net) تتبع وزارة الدفاع الأمريكية. والشكل رقم (2) يوضح شبكة (Mil net) للبريد الإلكتروني العسكري [المرجع رقم (65)].

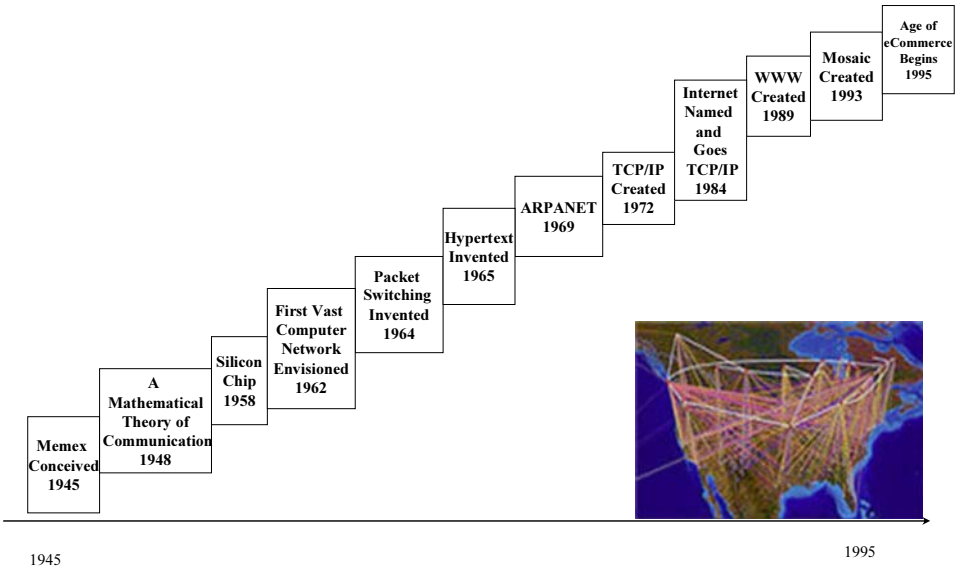
شبكة مدنية تجارية لصالح الشركات المدنية التي تتعامل مع وزارة الدفاع الأمريكية والتي أطلق عليها "شبكة الإنترنت" وكان هذا الاسم نابع من دور الشبكة وهو الربط INTERNETWORKING.



الشكل رقم (2): شبكة (Mil net) للبريد الإلكتروني العسكري

الفرق الجوهري بين شبكة "أربانت" وشبكة "ميل نت" وشبكة "الإنترنت" أن الشبكتين الأولى والثانية "عسكرية" لذلك فهما مؤمنين بنسبة 100% – أما الشبكة الثالثة (الإنترنت) فهي شبكة "مدنية تجارية" لذلك فهي بطبيعتها وبالهدف من إنشاؤها غير مؤمنة وعلى من يستخدمها أن يوفر لنظام معلوماته كافة وسائل وإجراءات وسياسات التأمين (التي سيتم ذكرها بالتفصيل في هذا الكتاب) وإلا سيتعرض للمخاطر والاختراقات الأمنية الموجودة في الشبكة. الشكل رقم (3) يوضح تاريخ تطوير شبكة ARPANET وخليفتها شبكة الإنترنت [المرجع رقم (46)].

ملخص تاريخ الإنترنت



الشكل رقم (3): تاريخ تطوير شبكة ARPANET
وخليفتها شبكة الإنترنت حتى عام 1995

ومن خلال الشكل رقم (3) وهذا التحليل المختصر لتطور الشبكة نستطيع القول إن تكنولوجيا الربط INTERNETWORKING أو تكنولوجيا الإنترنت استغرقت 14 سنة لتخرج من دهاليز وزارة الدفاع الأمريكية ومراكز الأبحاث التابعة لها إلى العالم الخارجي وإلى جمهور المستخدمين. كما يعتبر عام 1983 هو عام الميلاد الحقيقي لشبكة ARPANET كشبكة فعالة حقيقية وأساسية في الولايات المتحدة الأمريكية رغم أنها ما زالت شبكة تخدم الأغراض العسكرية أكثر من الأهداف المدنية التجارية وتربط بين مختلف الهيئات ومراكز البحوث والدوائر التي تدور في خدمة المصالح العسكرية الأمريكية.

انتشرت شبكة ARPANET لتغطي دول حلف الناتو في أوروبا. وطلبت الشركات المدنية الأمريكية من وزارة الدفاع عمل شبكة خاصة بهم لمعرفة مطالب الجيش الأمريكي غير العسكرية (معدات – أغذية – مواد بناء – الخ) فاستقر الرأي على استخدام الشبكة المدنية التجارية "الإنترنت" كشبكة وليدة أو كانبعاج صغير من شبكة ARPANET واعتمد إنشاء هذه الشبكة الوليدة على نفس النجاحات التي تم تطبيقها في شبكة ARPANET شاملاً ذلك استخدام بروتوكول التحكم في الإرسال (Transmission Control Protocol) نظام الإنترنت (Internet Protocol) (TCP/IP) ونظم التشغيل يونكس. وحيث إن القانون الأمريكي يلزم الفصل طبيعياً وإدارياً بين الشبكات العسكرية والشبكات المدنية فقد انفصلت شبكة الإنترنت الجديدة عن الشبكة (ARPANET) .

وإلى عام 1984 لم تكن الإنترنت مفتوحة للأفراد من خارج العاملين بالمؤسسات العسكرية والشركات ومراكز الأبحاث المتعاملة مع وزارة الدفاع ولكن ونتيجة لضغط من مراكز البحوث والجامعات غير المتعاملة مع وزارة الدفاع سعت جمعية العلوم الوطنية الأمريكية (NSFNET) - National Science Foundation Network إلى تبني شبكة الإنترنت

واستخدامها على نطاق محدود لربط بعض مراكز البحث العلمي والجامعات والمؤسسات الأكاديمية العلمية الأمريكية بعضها بالبعض.

وفي 1985 أسست الجمعية مجموعة من مراكز أجهزة الحاسبات الآلية العملاقة Supercomputers حيث استطاعت أن تبني 6 مراكز من الحاسبات العملاقة في ست جامعات ومراكز في مختلف أنحاء الولايات الأمريكية داخل مراكز البحوث التابعة للجامعات وهدفت (NSFNET) من هذا المشروع إعطاء الإمكانية والفرص لمجتمع الأبحاث في الجامعات والمراكز العلمية عبر مختلف الولايات الأمريكية إلى ربط بعضها بالبعض لتسهيل تداول المعلومات والأبحاث العلمية عبر هذه الأجهزة العملاقة. وقد عرضت الجمعية الوطنية للعلوم (NSFNET) الإمكانية لمختلف المؤسسات الأكاديمية للربط بالشبكة والمساعدة على إنشاء وتطوير بروتوكول TCP/IP الذي يربط الشبكة المحلية بالشبكات المحلية الأخرى في المراكز المذكورة. وقد قامت الجمعية بربط كل الشبكات المحلية ومراكز الحاسب التي تستطيع أن تتصل بالشبكة الرئيسية بشكل طبيعي والذي أدى لاحقاً إلى ما يعرف اليوم بمجتمع الإنترنت.

وفي عام 1986 عرضت الجمعية شبكة جديدة تعمل بسرعة 56 ألف ب/ث (وهى أقصى سرعة ربط حاسبات في ذلك الوقت) وسميت (NSF net). وعام 1987 عقدت الجمعية اتفاقية مع مؤسسة (MERIT) وهي مؤسسة أمريكية لا تسعى إلى الربحية مكونة من 11 جامعة في ولاية ميتشجن لبناء شبكة وطنية عبر استخدام سرعة الربط بالمواصفات القياسية T1 وبقيمة 1544 ألف ب/ث لتربط بين 11 مدينة أمريكية وأعطت الجمعية المشروع إلى كل من شركتي IBM وMCI حيث تم إنشاء مؤسسة موحدة من الشركتين المذكورتين تحت اسم مؤسسة خدمات الشبكة المتطورة (Advanced Network Services) وهكذا استطاعت الكثير من الجامعات ومراكز البحوث الارتباط بالشبكة. وتطورت شبكة (NSF net) واستطاعت أن تربط بين الحاسبات الشخصية للأفراد بالمعاهد والجامعات التي تريد أن تنضم إلى الشبكة والتي تريد أن تستخدم معلومات الشبكة. وقد تم تمويل الشبكة بواسطة الحكومة الأمريكية وأصبح الدخول إليها محدداً فقط للأبحاث غير التجارية وللاستخدامات العلمية الأكاديمية.

ومن خلال التعامل مع الإنترنت وجدت فائدة كبيرة في استخدام خدمات نقل الملفات والوثائق الإلكترونية وتبادل الرسائل عبر البريد الإلكتروني وكذلك لتكوين مجموعات نقاش في مختلف مجالات الحياة. وبعد عدة أشهر تم إكمال البرنامج واستطاعت الشبكة أن يتم من خلالها تداول أكثر من 152 مليوناً من الملفات والوثائق خلال عدة أشهر فقط من خلال ربط 170 شبكة محلية (Local Area Network LAN) داخل في الولايات المتحدة الأمريكية ودول حلف الناتو.

وفى عام 1990 وبعد انتهاء الحرب الباردة وانهيار الاتحاد السوفييتي وغياب التهديد النووي وما يفرضه من ضغوط على الولايات المتحدة الأمريكية انتهى الغرض العسكري وشملت الإنترنت خدمات خاصة بالنواحي المدنية والتجارية وتم الفصل الكامل بين شبكة ARPANET العسكرية والإنترنت وتم نشر الإنترنت لتغطي جميع الولايات المتحدة الأمريكية ودول حلف الأطلنطي ثم أوروبا ثم انتشرت الشبكة لتشمل جميع أنحاء العالم وتم تطويرها لتتعامل مع جميع أنواع المعلومات (بيانات وصوت وصورة).

وفي عام 1993 طورت مجموعة صغيرة من الباحثين في جامعة الينويز Illinois واجهة نوافذ جديدة (Windows) للشبكة العنكبوتية العالمية وسميت الفسيفساء "موزايك" (Mosaic) وخلال هذه الفترة استطاعت الجمعية الوطنية للعلوم الأمريكية أن تؤسس وتطور نسخة موزايك لتعمل على أنظمة أبل ماكنتوش ومايكروسوفت. وظهرت النسخة الأولى من نوافذ مايكروسوفت على

واجهة موزايك في نوفمبر 1993. ويعتبر متصفح موزايك (Browser) للشبكة العنكبوتية العالمية الواجهة الجميلة للإنترنت حيث يستطيع أي مشترك من خلالها أن يبحر في شبكة نسيج العنكبوت العالمية ويستفيد بكافة تطبيقات الإنترنت عبر استخدام الفأرة (Mouse) والضغط على أماكن ربط المواقع. وهذا المتصفح سهلاً للغاية حيث إنه قابل للامتداد والبسط ويستطيع إضافة مناظر وصور عبر نظام (GIF) وكذلك استدعاء كافة أنواع الملفات ومشاهدتها كما هي. ويسمح المد والبسط في المتصفح كذلك للمستخدم إضافة ميزة تشغيل الصوت والصورة لاستخدام الفيديو متعدد الأوساط (Audio and video players for video clips) واستطاعت شركات الحاسب أن تطور هذا المتصفح ليشمل كل ما هو موجود في الإنترنت.

وكانت متصفحات موزايك الواجهة الأمامية المصورة لشبكة الإنترنت حيث استطاعت أن تحتل قلوب المتصفحين والمستخدمين للشبكة في فترة قصيرة من عمر الواجهة والتي لا تزيد على 4 أو 5 سنوات قبل أن يتم تطوير واجهات أو متصفحات أحدث.

ويعتبر واجهة أو جوال أو بحار شركة Netscape أحد أفضل المتصفحات المتطورة خاصة مع إضافة إمكانيات التأمين والتوقيع الإلكتروني وتشفير أعمال التجارة الإلكترونية له (تشفير SSL) وقد احتلت المتصفحات أسواق الإنترنت بأسرع وقت ممكن وقد استطاعت إضافة وظائف أخرى لنسيج العنكبوت العالمية مثل إمكانيات FTP لنقل الملفات وTelnet وe-mail للبريد الإلكتروني وUser net للمجموعات الإخبارية ويستطيع المستخدم أن يعمل عبر هذه الوظائف أي شيء يخطر في باله داخل الشبكة. ودخلت شركة ميكروسوفت المنافسة في مجال تطوير المتصفحات بإنتاج Internet Explorer الذي وصل الآن إلى الإصدار السابع. أما المتصفح الأكثر استخداماً وانتشاراً الآن فهو Mozilla Firefox حيث إنه طبقاً للإحصائيات والدراسات الأكثر كفاءة وسرعة في عرض صفحات المواقع وفى تحميل الملفات من الإنترنت. [المرجع رقم (44)].

وعلى ذكر التأمين والسرية فمن المهم أن نوضح أن التصفح والتجول عبر الإنترنت يترك لدى الموقع المزار كمية واسعة من المعلومات على الرغم من أن جزءاً من هذه المعلومات لازم لإتاحة الربط بالإنترنت والتصفح. وبمجرد الدخول إلى صفحة الموقع فإن معلومات معينة تتوفر عن المشترك وهي ما يعرف بمعلومات رأس الصفحة (header information) وهي التي يزودها الحاسب المستخدم للحاسب الخادم الذي يستضيف مواقع الإنترنت وهذه المعلومات قد يستغلها الدخلاء في أعمال الاختراقات الأمنية حيث إنها تتضمن:

1) عنوان بروتوكول الإنترنت للمشترك (IP Destination) ومن خلاله يمكن تحديد اسم النطاق وتبعاً له تحديد اسم الشركة أو الجهة التي قامت بتسجيل النطاق عن طريق نظام أسماء المنظمات وتحديد موقعها.
2) المعلومات الأساسية عن المتصفح ونظام التشغيل وتجهيزات النظام المادية المستخدمة من قبل المشترك.
3) وقت وتاريخ زيارة الموقع.
4) مواقع الإنترنت وعنوان الصفحات السابقة التي زارها المستخدم قبل دخوله الصفحة في كل الزيارة.
5) وقد تتضمن أيضاً معلومات محرك البحث الذي زاره المستخدم للوصول إلي الصفحة وتبعاً لنوع المتصفح قد يظهر عنوان البريد الإلكتروني للمستخدم.

6) وأيضاً تبعاً لنظام تشغيل حاسب المستخدم ووجود الأوامر الخاصة بإدارة التعامل مع الشبكة قد تظهر معلومات حول الوقت الذي تم قضاؤه في كل صفحة وبيان المعلومات التي أرسلت واستقبلت.

في 30 أبريل 1995 أنتجت عمليات التشغيل والتطوير المستمرة على شبكة الجمعية الوطنية للعلوم الأمريكية (NSFNET) شبكة خاصة جديدة منبثقة ومرتبطة بالإنترنت وهي Network Access Points (NAPs) وهذه الشبكة الجديدة تم تأسيسها من قبل الحكومة الأمريكية بالفعل. وتتكون من أربع شبكات وتم إدارة هذه الشبكات من قبل القطاع الخاص وأي مؤسسة أو شخص يريد استخدام الإنترنت الخاصة عليه أن يدفع مقابل الخدمات التي يحصل عليها من قبل الشركات المالكة لها. كما تم إنشاء شبكات عالمية تتصل بالإنترنت وخاصة بمجال أعمال معينة مثل شبكة البحوث العلمية STAR وشبكة الربط بين البنوك للمدفوعات المالية SWIFT وشبكة شركات الطيران CITA وشبكة نقل مانيفستو النقل البري والبحري والجوي EDI Electronic Data Interchange

5-2 أسلوب عمل بروتوكول الإنترنت

تضم الإنترنت مجموعة هائلة من ملايين نظم الحاسبات وشبكاتها المنتشرة في مختلف أرجاء العالم وتتصل هذه النظم والشبكات مع بعضها بواسطة شبكات من الموجهات Routers وبوابات الربط Gateways وخطوط الاتصالات فائقة السرعة. ويمكن أن نشبه الإنترنت بشبكات الطرق البرية حيث توجد محاور رئيسية (highway) تربط الدول والمدن الكبرى وتتم الحركة عبرها بسرعات فائقة وبها مخارج تتفرع منها طرق وشوارع رئيسية وفرعية تربط المدن الصغيرة والقرى تليها شوارع داخلية في المدينة الواحدة تكون الحركة داخلها أقل سرعة. وتوجد في الإنترنت الشبكات فائقة السرعة التي تتصل من خلال شبكات الأقمار الصناعية وشبكات الألياف الضوئية بين القارات (التي تبلغ سرعتها 2 جيجا ب/ث) وتسمى العمود الفقري (backbone) أو الطريق السريع للاتصالات وتبلغ أقل سرعة لتفريعات هذه الشبكات عند كل بلد 45 مليون ب/ث وهذا يشمل خطوط ربط قياسية من الفئة T3 بالنظام الأمريكي وتتفرع منها شبكات أقل بسرعات تبلغ أقلها 1544 ألف ب/ث وهذا يشمل خطوط الربط القياسية من الفئة T1. وتنتهي حلقة الاتصال بخطوط ربط المشتركين (السلكية ADSL – واللاسلكية) والتي تبلغ سرعتها في المتوسط 256 ألف ب/ث في اتجاه و1500 ألف ب/ث في الاتجاه المقابل.

بروتوكول التحكم في الإرسال/نظام الإنترنت (TCP/IP) هو البروتوكول القياسي التجاري (Commercial Standard Protocol) الذي يقدم حلولاً في مجال ربط الحاسبات بالشبكات وفي تحقيق الاتصال فيما بين الشبكات المحلية والقومية والعالمية (Global Internetworking).

بمعنى أن الحاسبات والشبكات الحالية يجب أن تتوافق مع وتستخدم هذا البروتوكول لتكون ضمن مجتمع الشبكات والإنترنت. وقد تم بناء نموذج هذا البروتوكول من عدة طبقات لتحقيق الاتصال الناجح بين الحاسبات المتصلة من خلال الشبكات. وكل طبقة مسؤولة عن تنفيذ مهمة أو عدة مهام تساعد على تحضير البيانات من أجل الإرسال والاستقبال – وتتفاعل كل طبقة مع الطبقات المجاورة لها إذ تقدم الطبقة خدماتها إلى الطبقة الموجودة تحتها وتطلب الخدمة من الطبقة التي أعلاها.

ويتضمن بروتوكول TCP/IP أربعة مستويات أو طبقات أو بروتوكولات أساسية طبقاً للجدول التالي:

مستوى الطبقة	البروتوكول الأساسي	ملاحظات
الرابعة	التطبيقات (Applications)	
الثالثة	التحكم في الإرسال Transmission Control Protocol (TCP)	
الثانية	بروتوكول الإنترنت (Internet Protocol (IP))	
الأولى	الربط فيما بين الشبكات Subnet	التحكم في المحور Data Link Layer والربط المادي Physical Layer

وتشتمل المهام الأساسية التي تنفذها كل طبقة من طبقات البروتوكول الآتي: تقسيم وتجميع حزم البيانات – التغليف (التهيئة على هيئة إطارات Frames) – التحكم في الربط بفتح وغلق الدوائر – ترتيب الوصول – التحكم في حركة البيانات – معالجة الأخطاء وضمان سلامة تداول البيانات أو الاعتمادية – العنونة – المزج أو التجميع Multiplexing – الإرسال – والاستقبال. وقد تشتمل على مهام إضافية أخرى مثل الأولوية في تداول بعض أنواع حزم البيانات وتأمين البيانات طبقاً لمستوى الطبقة ونوع التطبيق.

- من البروتوكولات المستخدمة في الطبقة الرابعة (التطبيقات) وتسمح بتبادل المعلومات بغض النظر عن نظام التشغيل المستخدم الآتي:

أ. HTTP: ويستخدم مع الشبكة العنكبوتية لعرض مختلف أنواع المعلومات بشكل مقروء أو ما يسمى بالنصوص التشعبية (Hypertext Transfer Protocol).

ب. FTP: ويُستخدم لنقل الملفات من حاسب لآخر (File Transfer Protocol) وهو الذي يستخدم عادة عندما يتم تحميل لبرنامج أو وثيقة من الإنترنت.

ج. NNTP: ويُستخدم في خدمة مجموعات الإعلام Network News Transfer Protocol.

د. SMTP: ويُستخدم لإرسال البريد الإلكتروني Simple Mail Transport Protocol.

هـ. POP: ويُستخدم للحصول على البريد الإلكتروني من خادم البريد Post Office Protocol.

و. SNMP: وهو يستخدم للتحكم في الشبكة وإدارتها Simple Network Management Protocol.

- يوجد بالطبقة الثالثة بروتوكول التحكم في الإرسال TCP الذي يحقق الاتصال وتداول البيانات بين أي حاسبين متصلاً عبر الإنترنت. حيث يتم في الإرسال تقسيم الرسائل إلى مجموعة من حزم البيانات ويتم ترقيم كل حزمة لإعادة تجميعها عند الاستقبال. وطبقاً لبروتوكول التحكم في الإرسال TCP يتم إرسال عدد محدود أو "نافذة" من حزم البيانات (Window Size) ثم التوقف انتظاراً للرد العكسي باستلام هذه الحزم. فإذا لم يتم الحصول على الرد العكسي لحزمة بيانات ما أو لمجموعة من الحزم بعد فترة معينة – فإن الحاسب المرسل يعيد إرسالها مرة أخرى وهكذا حتى يتم إرسال جميع حزم البيانات. وتسمى هذه الخاصية "تدقيق تدوال حزم البيانات بالتغلب على الأخطاء وإعادة الإرسال" (Error Detection and Correction by Retransmission) أو خاصية "الاعتمادية

Reliability". وتوجد خاصية أخرى لهذا البروتوكول وهى تحقيق الاتصال Connection بفتح وتهيئة وغلق دوائر الربط أثناء جلسات العمل بين الحاسبات حيث يتم مع بدء الإرسال تكوين دائرة افتراضية (virtual circuit) مع TCP بين الحاسب المرسل والمستقبل. والخاصية الثالثة هي التحكم في تدفق حزم البيانات (Flow Control) حيث مع بدء عملية الإرسال يقوم TCP للحاسب المرسل بإرسال رسالة إلى TCP الحاسب المستقبل مستفسراً عن إمكانية إرسال حزم بيانات الآن. وإن كانت الإجابة "لا" فإن TCP المرسل ينتظر قليلاً قبل أن يرسل رسالة استفسار مرة أخرى. وعندما تأتي رسالة الإيجاب فإنه يقوم بإرسال حزم البيانات المرقمة كما ذكرنا. ويتفق TCP المرسل مع TCP المستقبل على كمية حزم البيانات المرسلة قبل الحصول على رسالة تأكيد وصول أخرى من الحاسب المستقبل. كما أن البروتوكول TCP هو بروتوكول نهاية لنهاية أي أن المصدر سيكون حاسب واحد فقط والهدف أيضاً سيكون حاسب واحد. أي أن TCP موجه للاتصال بين نقطتين فقط وهو غير قادر على بث البيانات التي ينقلها بشكل مشاع لجميع الأجهزة الموجودة وفي وقت واحد. بل عليه أن يعيد إرسال هذه البيانات من أجل كل حاسب على حدة وذلك لأن حقل العنونة في بنية البروتوكول TCP لا يتسع إلا لوجهة واحدة فقط. الخلاصة أن البروتوكول TCP هو بروتوكول موثوق بدرجة عالية بحيث يضمن وصول حزم البيانات إلى الحاسب المستهدف بشكل صحيح وبالترتيب الذي أرسلت به. وفي حال فقدان إحدى الحزم فإن البروتوكول TCP يعاود الاتصال بالحاسب المرسل لكي يعيد إرسال الحزمة الضائعة مرة أخرى كما ذكرنا. وبالتالي فإن تنفيذ هذا البروتوكول لمهامه يسبب حملاً زائداً على الإنترنت خاصة عند إرسال كمية كبيرة من حزم البيانات.

- يوجد في نفس الطبقة الثالثة بروتوكول حزم بيانات المشترك User Datagram Protocol (UDP) وهذا البروتوكول لا يحقق الاتصال ودقة تداول البيانات. بمعنى أنه لا ينشئ جلسات العمل بين الحاسبات أثناء الاتصال. كما أنه لا يضمن الوصول السليم لحزم البيانات على الحالة التي أرسلت بها. وهو بذلك يعتبر غير اعتمادي وغير موصل (Unreliable and Connectionless) على خلاف البروتوكول TCP. لبروتوكول النقل UDP ميزات تجعل من المستحب استخدامه في بعض الحالات مثل إرسال بيانات مجمعة عامة وعند الحاجة إلى السرعة في تداول البيانات حيث إن السرعة ناتجة من عدم حاجته إلى التحقق من دقة الإرسال. ويستخدم UDP في نقل ملفات الوسائط المتعددة مثل الصوت والفيديو لأن الوسائط لا تحتاج إلى دقة التداول.

- يوجد بالطبقة الثانية بروتوكول الإنترنت (IP) وهو الذي يتحكم في توجيه أو تسيير حزم البيانات (data routing) من المرسل إلى المستقبل عبر الشبكات. وينظر بروتوكول الإنترنت (IP) إلى عنوان كل حزمة ثم باستخدام جدول يسمى جدول التوجيه يقرر من هي أفضل محطة تالية (موجه (Router) أو بوابة ربط (Gateway)) لتلك الحزمة وللحزم التالية. وللوصول إلى حاسب معين على الشبكة يلزم معلومتين هما: على أي شبكة يوجد هذا الحاسب NET Address؟ وما هو رقم التعريف للحاسب على الشبكة Host Address؟ – وهما ضمن مكونات عنوان IP للحاسب وللشبكة. لا يتضمن بروتوكول الإنترنت خاصية الربط والاعتمادية في تداول حزم البيانات لأنه عندما يكتشف خطأ يقوم بحذف حزم البيانات دون محاولة التصحيح أو إعادة طلب حزم البيانات مرة أخرى وبالتالي يعتبر بروتوكول عديم التوصيل (Connectionless) وعديم الاعتمادية (Un Reliable). فقد يضمن أن كل حزم البيانات المستقبلة بياناتها صحيحة ولكنه لا يضمن أن الحزم وصلت كاملة أو بالترتيب الصحيح. كما لا يتضمن بروتوكول الإنترنت خاصية التحكم في فتح وغلق الدوائر والسبب الرئيسي في عدم تضمين بروتوكول الإنترنت (IP) للاعتمادية

والتوصيل أنه يعتمد على تلك الخصائص الموجودة في الطبقة الأعلى TCP (إذا تم استخدامها) ولتوفير السرعة العالية في تداول حزم البيانات دون تأخير.

تتكون العناوين في الإصدار الرابع من بروتوكول الإنترنت من 32 نبضة وتُكتب كأربع مجموعات من الأرقام تفصلها نقاط (A.B.C.D). حيث إن كل مجموعة بها 8 نبضات وتتراوح قيمتها النظرية بين (0 و255) بإجمالي 82. وتنقسم العناوين في هذا الإصدار إلى أربعة فصول IP Classes طبقاً للشكل رقم (4) هي:

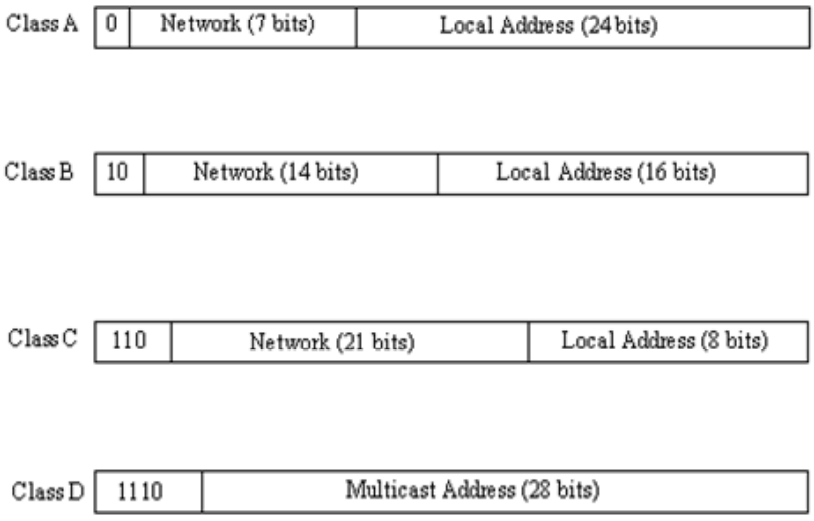
أ. الفصل "أ" (Class A) ويتكون من حقل لعنوان الشبكة (7 نبضات) وثلاثة حقول لعنوان الحاسب (24 نبضة) بالترتيب (NET.HOST.HOST.HOST).

ب. الفصل "ب" (Class B) ويتكون من حقلين لعنوان الشبكة (14 نبضة) وحقلين لعنوان الحاسب (16 نبضة) بالترتيب (NET.NET.HOST.HOST).

ج. الفصل "ج" (Class C) ويتكون من ثلاثة حقول لعنوان الشبكة (21 نبضة) وحقل لعنوان الحاسب (8 نبضة) بالترتيب ((NET. NET. NET. HOST).

د. الفصل "د" (Class D) ويتكون من 4 نبضات لعنوان الشبكة و28 نبضة لتحقيق الاتصال بين مجموعة من الحاسبات Multicast.

IP Classes



الشكل رقم (4): فصول عناوين الإنترنت IP CLASSES

باستخدام الإصدار الرابع لبروتوكول الإنترنت فإن عدد العناوين المتاحة تتجاوز قليلاً أربعة بلايين (2^{32}). هذا الرقم يبدو عالياً جداً خصوصاً وإن عدد الحاسبات والشبكات الموجودة حالياً في العالم تعد في الملايين فقط. ولكن المشكلة تكمن في أن توزيع العناوين لا يتم بصورة فردية ولكن بصورة جماعية. فعندما تطلب مؤسسة (هيئة حكومية أو مدنية أو شركة) عنوان IP لها يتم إعطائها مجموعة من العناوين تصل إلى الملايين والمؤسسة حرة في أن تستخدم منها ما تريد حالياً ومستقبلاً مما يعد استغلال غير اقتصادي للعناوين ويستهلك فضاء العناوين المتاح IP Address Space. وبالتالي تقل عدد العناوين المتوافرة في السنوات القادمة.

ولهذا السبب فإن الكثير من الهيئات والمنظمات والشركات المسؤولة عن إدارة الإنترنت بدأوا بتصميم "الجيل التالي من بروتوكول الإنترنت .Next Generation Internet Protocol IP NG. وهذا البروتوكول – والذي تمت تسميته ببروتوكول الإنترنت الإصدار السادس IPV6 يستعمل 128 بت من أجل صياغة العناوين أي أنه يتيح أربعة أضعاف عناوين الإصدار الرابع. وهذا سيسمح بوجود أكثر من 16 مليار عنوان لحاسب وشبكة (2^{128}) على الإنترنت. وسيحقق IPV6 مزايا عديدة منها:

- التعامل مع بلايين الحاسبات والشبكات وبالتالي المشتركين.
- اختصار حجم جداول التوجيه.
- تبسيط البروتوكول للسماح للموجهات بمعالجة حزم البيانات بشكل أسرع.
- تقديم أمن أفضل للمعلومات بتوفير المصداقية والخصوصية والتكامل للبيانات.
- إعطاء اهتمام أكبر لنوع الخدمة المقدمة وخاصة لمعلومات خدمات الزمن الحقيقي مثل الهاتف بالإنترنت والفيديو.
- السماح للحاسبات بالتنقل دون تغيير عنوانها (خاصية الترقيم الثابت وليس الجغرافي).
- السماح للبروتوكول بالتطور في المستقبل.
- إمكانية تواجد البروتوكولات القديمة والجديدة معاً لسنوات قادمة.

التحول من بروتوكول الإنترنت IPV4 إلى بروتوكول IPV6 فجأة أمر غير ممكن وذلك بسبب الحجم الكبير لشبكة الإنترنت بالإضافة إلى أن الكثير من المؤسسات صارت أكثر اعتماداً على الإنترنت في عملها اليومي وهي بهذه الصفة لا تتحمل التغيير الفوري لنظام بروتوكول الانترنت. ونتيجة لذلك لن يكون هنالك وقت محدد يتم فيه إيقاف بروتوكول IPV4 وإحلال بروتوكول IPV6 محله وذلك لأنهما يمكن أن يتعايشا مع بعض بدون أي مشاكل. بالتالي يستطيع المستخدمين الاستفادة من ميزات بروتوكول IPV6 وفي نفس الوقت يمكنهم من استخدام برامج بروتوكول IPV4 وملحقاته. بعض خواص بروتوكول IPV6 قد صممت خصيصاً لتبسط التحول بمعنى أنه يمكن استخلاص عناوين IPV6 آلياً من عناوين IPV4. كما يمكن بناء أنفاق مؤمنة لبروتوكول IPV6 (Tunnels) على شبكات بروتوكول IPV4.

يساعد نظام أسماء المواقع (DNS) مستخدمي الإنترنت على الوصول إلى ما يبحثون عنه في رحاب الإنترنت حيث يوجد لكل حاسب متصل بالإنترنت عنوان مستقل يسمى "عنوان بروتوكول الإنترنت (Address IP)". وهو ينقسم إلى قسمين بينهما علاقة هما: عنوان IP بالأرقام على هيئة A.B.C.D والقسم الثاني هو عنوان IP بالاسم أو Domain Name System (DNS) الذي استخدم نظراً لصعوبة تذكر أرقام عناوين بروتوكول الإنترنت من القسم الأول. فقد استبدل نظام أسماء المواقع DNS الأرقام بمجموعات من الحروف المألوفة (التي تشكل "أسماء المواقع") حيث يظهر فيها اسم الدولة (المستوى العلوي – القسم الثاني الذي يتكون من حرفين) والنشاط الرئيسي (المستوى العلوي – القسم الأول الذي يتكون من حرفين أو أكثر) والأنشطة الفرعية للموقع (نطاقات المستوى الثاني). فعوضاً عن كتابة الرقم: "192.0.34.65" يمكن كتابة اسم مثل www.icann.org.

ويحتل نظام أسماء المواقع DNS الأساس في تحديد هوية الوجود على إنترنت إذ يمكن بواسطته إيجاد مواقع الشركات والمنظمات على الويب. ويقوم نظام أسماء المواقع DNS بترجمة الاسم الذي يتم كتابته إلى عنوان بروتوكول الإنترنت المقابل (من IP الاسم إلى IP الرقم) ثم يتم الاتصال بالموقع الذي يرغب المشترك في زيارته. كما يساعد نظام أسماء المواقع على تشغيل البريد الإلكتروني بالشكل الصحيح بحيث تصل الرسائل إلى المرسل إليه المقصود.

تدور المسألة الرئيسية في أسماء النطاقات DNS حول نطاقات المستوى العلوي (Top-Level Domains, (TLD)) ونطاقات المستوى الثاني ((Second-Level Domains (SLD). وتوجد مجموعتان رئيستان من أسماء نطاقات المستوى العلوي هما :النطاقات العامة (generic, gTLD)، ونطاقات شفرة البلد (country code, ccTLD). وتغطي مجموعة أسماء النطاقات الأولى مختلف الأنشطة الرئيسية مثل: com. للشركات التجارية وorg. للمنظمات وgov. للجهات الحكومية وint. للمنظمات العالمية وedu.sci. للمواقع التعليمية.

بينما تغطي أسماء نطاقات شفرة البلد كود البلد من حرفين مثل: eg. لمصر وfr. لفرنسا وmx. للمكسيك وde. لألمانيا. وتأتي النطاقات العامة gTLD بعد نطاقات شفرة البلد ccTLD مثل gov.eg بمعنى موقع حكومي في مصر.

وتأتي أسماء نطاقات المستوى الثاني قبل أسماء نطاقات المستوى العلوي مثل: وnti.sci. وitu.int وMicrosoft.com وharvard.edu. وبالتالي يكون موقع المعهد القومي للاتصالات على شبكة النسيج العنكبوتية هو: www.nti.sci.gov.eg ومعناه موقع المعهد القومي للاتصالات ذو النشاط العلمي والتابع للحكومة المصرية. ومن الممكن إضافة أسماء نطاقات من المستوى الثاني.

كانت إدارة العديد من الوظائف المهمة في أمور التنسيق المتعلق بتقنيات الإنترنت تتم من قبل وكالة العلوم والبحوث الأمريكية National Science Foundation والهيئات الخاصة المخولة بذلك إضافة إلى شبكة واسعة من المتطوعين. إن وجود هذه البنية الغير رسمية كان يعكس روح وثقافة مجتمع الدراسات والبحوث الذي قام بتطوير الإنترنت في الأصل. كانت الطريقة الوحيدة – حتى وقت قريب – للحصول على اسم نطاق من النوع الذي ترغب فيه معظم الجهات، تسجيل الاسم من خلال شركة Network Solution Inc. (http://www.nsi.com) التي تعاقدت عام 1993 مع الحكومة الأمريكية ومع وكالة البحوث National Science Foundation كي تعمل كموزع لأسماء النطاقات.

وأوكلت ذلك لمنظمة تابعة لها خاصة بتعيين أرقام الإنترنت والمعروفة بالاختصار IANA (Internet Assigned Numbers Authority) وعنوانها www.iana.org. إلا أن تطور الأهمية العالمية المدنية والتجارية للإنترنت أدى إلى خلق منظمة خاصة بإدارة التقنيات وتطوير سياسة خاصة بالإنترنت وهي منظمة تحديد الأسماء والأرقام على الإنترنت ICANN (The Internet Corporation for Assigned Names and Numbers).

وقد تم إعطاء منظمة "الايكان" بنية رسمية ذات مسؤولية قانونية وهيكلية أكثر شفافية لتعكس بوضوح كامل كافة المجتمعات الموجودة على الإنترنت. في عام 2002 كان لدى المنظمة أربعة عشر موظفاً فقط بينما كان هناك تسعة عشر عضواً يتبرعون للعمل في مجلس الإدارة. وكان "د. فينتون سيرف" الذي يعتبره الكثيرون "والد الإنترنت" رئيساً لهذا المجلس. وقد كان تمويل هذه المنظمة يأتي عن طريق الأجور المستحقة من الشركات التجارية لقاء تسجيل الملكيات والمواقع.

وتعتبر شبكة الإنترنت حالياً حصيلة جهود مشتركة لعدد كبير من المنظمات والمؤسسات والمعاهد العالمية. وكانت ولا زالت تلك الجهات تسهم ببحوثها وأنظمتها ومواردها في خدمة وصيانة وتحديث هذه الشبكة. وبناء على ذلك لا تستطيع أي جهة أن تدعي ملكية الإنترنت أو السيطرة الكاملة عليها.

أما عملياً فهنالك هيئات وشركات رائدة في قطاع تكنولوجيا المعلومات والاتصال تمارس نفوذها عبر وضع معايير تتوافق مع أنظمة الأجهزة والبرمجيات. إلى جانب ذلك شرعت عديد من الدول في سن نصوص خاصة بالإنترنت وتنظيم حركة حزم البيانات التي تتم عبرها.

ومن أهم الهيئات والمؤسسات التي تلعب دوراً هاماً في تطوير وتنظيم انتشار شبكة الإنترنت هي:

1) (IETF) وهي اختصار لكلمات (The Internet Engineering Task Force): وهى هيئة عالمية تفتح باب الاشتراك فيها لجميع مصممي الشبكات. وتلعب دوراً رئيسياً في تطوير الإنترنت وذلك بتقديم حلول للمشاكل التقنية التي قد تواجهها الشبكة.

2) (IESG) وهي اختصار لكلمات (The Internet Engineering Steering Group): وهي هيئة تقوم بإدارة ومتابعة أنشطة IETF ومراجعة المعايير التي تضعها بعض الهيئات المختصة على غرار مختلف البروتوكولات التي تخص الشبكة. وتنشر الهيئة وثائق الإنترنت مجاناً على هيئة "طلب تعقيب أو توصيف" ((Request For Comments (RFC)).

3) (W3C) وهي اختصار لكلمات (World Wide Web Consortium): وهى هيئة تشجع وتصادق على تطوير المعايير المفتوحة لإعداد صفحات الشبكة العنكبوتية مثل HTML وXML وغيرها.

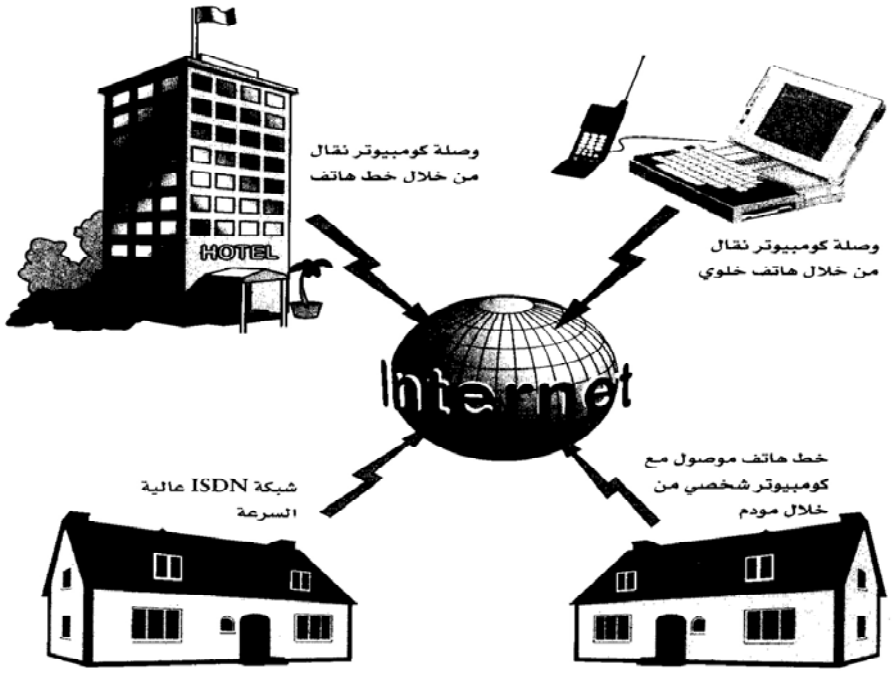
4) (IAB) وهي اختصار لكلمات (Architecture Board Internet): وهى هيئة للاستشارات التكنولوجية تقدم استشاراتها وتوجيهاتها لهيئة IETF كما تحدد الهيكلية العامة للإنترنت وعمودها الفقري Backbone.

5) (ISOC) وهي اختصار لكلمات (Internet Society): وهي جمعية متخصصة تضم في عضويتها عدة جهات وأفراد وإدارات حكومية وشركات ومؤسسات وهيئات غير ربحية تبدي آراءها في السياسات والممارَسات المتعلقة بالإنترنت. كما تسعى إلى تعزيز ورفع مستوى استخدام وتطوير وصيانة الإنترنت.

6) (ICANN) وهي اختصار لكلمات (The Internet Corporation for Assigned Names and Numbers): وهي كما ذكرنا مؤسسة غير ربحية تتولى إدارة عناوين الإنترنت الرقمية (IP addresses) وأسماء المجالات (Domain names) التي تعد أساسية في تشغيل شبكة الإنترنت وتأمين عملها المستقر والآمن. بالإضافة إلى ذلك تعمل على تنسيق تطوير السياسة المتعلقة بهذه المهام الفنية.

7) يضاف إلى هذه الجهات توجد المنظمات العالمية الدولية مثل الاتحاد الدولي للاتصالات (ITU) والمنظمة العالمية للقياسيات (ISO) بالإضافة للشركات العالمية التي تنتج معدات تكنولوجيا المعلومات والاتصالات التي تساهم بالبحوث والدراسات في تطوير وانتشار الإنترنت على المستوى العالمي كما تساهم في تامين خدمات الشبكة مثل الاتصال الهاتفي ببروتوكول الإنترنت والتجارة الإلكترونية بوسائل من أهمها التشفير والتوقيع الإلكتروني وشهادات التوثيق كما سيتم تناوله بالتفصيل في الباب الخامس.

ويتم حالياً الربط بالإنترنت باستئجار خطوط الاتصال من شركات "تقديم خدمة الإنترنت" المحلية العاملة في البلد أو المنطقة التي يوجد بها الحاسب المضيف. وتتكون شبكة مقدم الخدمة من عقد اتصال وموجهات ترتبط فيما بينها بشبكة الاتصالات القومية. فعلى سبيل المثال في مصر توفر الشركة المصرية للاتصالات العمود الفقري لربط شبكات مقدمي خدمة الإنترنت. بمعنى أن الشبكة تربط فيما بين الثلاثة عناصر للربط وهم: الشبكات الدولية (من خلال قنوات الأقمار الصناعية والألياف الضوئية) ومزودي خدمة الإنترنت والمشتركين في منازلهم والشكل رقم (5) يوضح بعض وسائل الربط مع شبكة الإنترنت



الشكل رقم (5): بعض وسائل الربط مع شبكة الإنترنت

6-2 انتشار الإنترنت عالمياً

الإنترنت معروفة منذ سنين تعود إلى السبعينات إلا أن الكثير من مستخدمي الإنترنت اليوم يعرفها على إنها شبكة نسيج العنكبوت العالمية (World Wide Web) (www) وقد بدأت هذه الشبكة العنكبوتية على يد عالم سويسري يدعى Tim-Berners-Lee الذي يعمل في مختبرات المركز الأوروبي لبحوث الطاقة النووية (CERN) في جنيف بسويسرا عام 1989 – حيث استطاع أن يطور برامج لتسهيل عملية تبادل وإشراك الباحثين والمختصين في الطاقة العالية وخاصة الفيزياء وحصولهم على المعلومات الخاصة بأبحاث الطاقة والطب والفيزياء الموجودة بالحاسب الآلي باستخدام لغة إضافة النص الوافر (Hypertext HTML-Markup Language). حيث يتم استخدام النص الوافر ليس فقط داخل الوثيقة الواحدة أو بين مختلف الملفات والوثائق بل وبين مختلف مواقع شبكات الحاسب الآلي التي ترتبط بعضها البعض عبر الإنترنت. وقد وفر الباحث طريقة سهلة لربط المعلومات الموزعة على امتداد شبكة الإنترنت. وبذلك يستطيع أي مشترك أن يتصل من خلال تطبيقات البروتوكول TCP/IP وعلى الأخص بروتوكول الربط Telnet إلى الحاسب الخادم بالموقع الذي يتعامل مع الشبكة العنكبوتية وأن يدخل إلى الشبكة ولكن كل ذلك عبر استخدام النص فقط (Text).

وتشير الإحصائيات إلى أن الإنترنت توسعت بشكل سريع خلال السنوات الماضية. وقد تضاعف عدد المشتركين والمستخدمين للشبكة إلى أكثر من 4-5 مرات بين عامي 1993 و1999 فقط. والجدول التالي يوضح عدد الحاسبات المضيفة Hosts المرتبطة على الإنترنت منذ عام 1977 وحتى عام 2010. [المراجع أرقام (34 و44)].

العام	1977	1983	1986	1989	1992	2001	2002	2008
عدد الحاسبات	111	562	5000	100 ألف	1 مليون	175 مليون	200 مليون	600 مليون

وأدى إنشاء شبكة ويب العالمية (www) (World Wide Web) وظهور الواجهات أو المتصفحات Browsers ذات الاستخدامات الرسومية والمتوافقة مع مختلف أنواع نظم التشغيل إلى اتساع هائل في الشبكة العالمية فحتى وقت قريب اقتصرت خدمات الإنترنت على البلدان المتقدمة على جانبي شمال المحيط الأطلسي واليابان وأستراليا. ولكنها تتوسع اليوم لتشمل غالبية بلدان العالم بما في ذلك البلدان العربية ولن يمضي وقت طويل قبل أن يعم استخدام الشبكة وانتشارها مثل انتشار خدمات البنية الأساسية أو الطريق السريع للاتصالات التي تستعملها البشرية اليوم مثل شبكات الهاتف الثابت والمحمول والكهرباء والمياه والطرق السريعة والطيران المدني.

وبتوسع الإنترنت في مختلف بلدان العالم زادت الطلبات على استخدام خدماتها ومع زيادة هذه الطلبات زاد أيضاً عدد المشتركين (الأفراد والجهات المتعاقدة على الشبكة) والمستخدمين (الذين يستخدمون الشبكة من خلال المشتركين) لها. إلا أنه من الصعب بمكان تحديد عدد المستخدمين الفعليين للشبكة. والصعوبة في ذلك تكمن في أن عدد المستخدمين يزيد بكثير عن عدد المشتركين حيث إنه يتم استخدام الشبكة من قبل عشرة مستخدمين على الأقل لكل مشترك منزلي واحد وتتضاعف هذه النسبة مع المشتركين من الجهات العلمية والحكومية والشركات والمؤسسات كما ترتفع هذه النسبة إلى أكثر من ذلك في البلدان العربية والنامية. وذلك بسبب زيادة عدد أفراد الأسرة وعدد الشقق في العمارات ووجود عدد كبير من الطلاب يستخدمون عدداً قليلاً من الاشتراكات. ولكن في مقابل زيادة المستخدمين لكل اشتراك في البلدان العربية والنامية تنقص هذه الأعداد في مختلف بلدان العالم الأخرى مثل الولايات المتحدة الأمريكية والسويد.

وتشير الإحصائيات الأخيرة إلى أن عدد مشتركي الإنترنت وصل 500 مليون عام 2005 منهم حوالي 210 مليون في أمريكا وحدها و150 مليون في أوروبا والباقي مقسم على باقي بلدان العالم والآن بلغ عدد مستخدمي الإنترنت في العالم 1,319 بليون شخص في ديسمبر 2007. وتعد الصين أولى دول العالم في الزيادة السنوية لعدد مستخدمي الإنترنت الذين بلغ عددهم 221 مليون شخص في فبراير 2008 وتفوقت بذلك على أمريكا التي وصل العدد الحالي للمشتركين 220 مليون [المراجع أرقام (34 و39 و44)].

وتشير الدراسات والبحوث إلى نمو مستخدمي الإنترنت على المستوى العالمي حيث زادت بنسبة قياسية منذ عام 1996. وتشير البحوث في مجال الإنترنت إلى زيادة عدد الدول التي دخلتها الإنترنت لأكثر من 218 دولة من أصل 246. ويوجد أكثر من 32 مليون اسم نطاق (Domain Name). ويوجد بالشبكة أكثر من 100 تيرابايت من البيانات متاحة من أكثر من 200 مليون موقع. ومع الزيادة في أعداد مستخدمي الإنترنت على المستوى العالمي زادت أيضاً أعداد مواقع الشبكة ويتم يومياً إضافة العديد من المواقع الهامة وزاد العدد السنوي للمواقع الجديدة بنسبة 100 بالمائة في دول مثل كندا وبريطانيا [المراجع أرقام (34 و44)].

كما زادت أعداد المواقع العربية منذ عام 1997 حيث تراوحت زيادة عدد المواقع ما بين 150 و250 بالمائة. [المراجع أرقام (28 و34 و39)]. وقد ترافق مع هذا الانتشار العالمي للإنترنت زيادة في الخدمات وتحسين في الجودة.

ويتمثل التطوير المستقبلي للإنترنت في مشروعين رئيسين هما الإنترنت 2 وإنترنت المستقبل (New Generation Internet (NGI)) التي تختلف عن الإنترنت الحالية في عدة محاور رئيسية هي:

1) رفع درجة الخدمة Quality Of Services (QOS): ومعناها زيادة قدرة الشبكة على استيعاب جميع أنواع المعلومات (بيانات وهاتف وصورة) بنفس الكفاءة ويتم ذلك من خلال زيادة سعة شبكات الاتصال وسرعة وصول المشترك للتغلب على التراكم في حجم البيانات وتقليل التأخير في تداول البيانات وزيادة معدل تدفق البيانات.

2) زيادة القدرة على البقاء (Reliability): ويتم ذلك من خلال إتاحة أكبر عدد ممكن من الحاسبات والشبكات والمواقع الرئيسية والتبادلية وكذلك وجود وسائل التغلب على الأخطاء في تداول البيانات.

3) التأمين والسرية (Security): من خلال تقنيات التأمين والحماية التي يتناولها بالتفصيل هذا الكتاب ومن أهمها الجدران النارية والنظم الشفرية والتعرف على الهوية والتحكم في الدخول.

4) التوافق والتمهيد لإدخال النسخة 6 من بروتوكول إنترنت (IPV6): لحل مشكلة قلة العناوين المتاحة على النسخة 4 من بروتوكول إنترنت (IPV4) حيث يتم حالياً تحديد خطط الانتقال وإجراءاته.

5) التوسع في استخدام خدمة "الهاتف بواسطة بروتوكول الإنترنت" (Voice Over IP) أو (IP telephony): التي سيتم الإشارة إليها في البند التالي (رقم 2-9). ولأهمية انتشار هذه الخدمة من خلال وضع المواصفات القياسية بواسطة الاتحاد الدولي للاتصالات (ITU) والمعهد الأوروبي لمعايير الاتصالات ورابطة صناعة الاتصالات والقواعد التنظيمية للهاتف التماثلي. وقد شكل الاتحاد الدولي للاتصالات لجنة لدراسة تعزيز انتشار هواتف بروتوكول إنترنت وإدخال شبكات بروتوكول إنترنت على نحو منسق. وطبقاً لخطاب مدير مكتب تنمية الاتصالات في المؤتمر العالمي لتنمية الاتصالات الذي نظمه الاتحاد الدولي للاتصالات (ITU) في اسطنبول بتركيا في مارس 2002 فإن الدراسات تهدف إلى تحديد الآتي:

أ- نوعية خدمة الهاتف باستعمال بروتوكول إنترنت وتصنيف نوعية الخدمة من طرف إلى طرف إلى ثلاث فئات على النحو التالي: الفئة (أ) (توصيل الخدمة إلى مستوى الهواتف الثابتة) والفئة (ب) (توصيل الخدمة إلى مستوى الهواتف المحمولة) والفئة (ج) (توصيل الخدمة للمستويات الأخرى وهى نوعية أقل من نوعية الفئة (ب) لكنها مقبولة للاتصال الصوتي). وينبغي على مقدمي خدمة هواتف بروتوكول إنترنت وبائعي الأجهزة الطرفية لهذه الخدمة توضيح النوعية وفق هذا التصنيف.

ب- أسلوب تقدير نوعية الخدمة من خلال وضع هيئات التوحيد القياسي لمعايير أساليب وشروط تقدير نوعية خدمة هواتف بروتوكول إنترنت.

ج- وضع القواعد التنظيمية التقنية لنوعية هواتف بروتوكول إنترنت لكي تناظر مختلف خدمات الهاتف الأخرى. وينبغي على مقدم الخدمة أن يحدد بنفسه مستوى النوعية المستهدف وأن يسعى للمحافظة على هذا المستوى.

د- خطة ترقيم هواتف بروتوكول إنترنت: من خلال تخصيص الأرقام لهواتف بروتوكول إنترنت وهي الأرقام التي يتم طلبها من الشبكة القومية للوصول إلى الأجهزة الطرفية المتصلة فيما بينها من خلال شبكة بروتوكول إنترنت سواء من خلال خط المشترك الرقمي أو نظام الاستقبال التلفزيوني بهوائي جماعي (CATV) أو أي وسيلة ربط سلكية أو لاسلكية مماثلة.

هـ- وضع معايير الفحص المتصلة بالأرقام الهاتفية بهدف كفالة تخصيص الأرقام الهاتفية بطريقة عادلة وفعالة.

و- تنظيم أرقام هواتف بروتوكول إنترنت والاستعداد لها من خلال دراسة التدابير لرسم الحدود الفاصلة بين الرقم الهاتفي وعنوان بروتوكول الإنترنت على شبكات الربط.

ز- تعزيز التوصيل البيني: نظراً لحالات التوصيل البيني بين مختلف الشبكات سيكون من الضروري وضع شروط تقنية لهذه التوصيلات البينية بالتعاون مع منظمة التوحيد القياسي وشركات تقديم الخدمة.

ح- أساليب تأمين خدمة الهواتف ببروتوكول الإنترنت: لحماية شبكات بروتوكول إنترنت من خطر الإرهاب التقني حيث يلزم تعزيز البحث والتطوير الخاص بوسائل الأمن وإقامة نظام للاتصال والتنسيق بين الإدارات والقطاع الخاص وتشجيع المستعملين على تطبيق تدابير كافية للأمن.

ط- كفالة الاتصالات في حالات الطوارئ: لكفالة الاتصالات في حالات الطوارئ فيما يتعلق بهواتف بروتوكول إنترنت يلزم بذل الجهود للشروع في أعمال البحث والتطوير وهي لا تقتصر على شركات نقل الاتصالات بل تتعداها إلى الحكومات أيضاً.

والإنترنت2 هو مشروع طموح يهدف إلى تطوير البنية التحتية لشبكات الاتصال وشبكات الحاسب على مستوى الدول بالتوسع في استخدام نظم كوابل الألياف الضوئية والبث التلفزيوني والأقمار الصناعية. والهدف من التطوير تحقيق تداول المعلومات بسرعات فائقة (جيجا إلى تيرا بت/ث) والقدرة على تداول جميع أنواع المعلومات بنفس درجة الجودة وذلك تمهيداً لقدوم إنترنت2 المستقبلية. وقد أُطلِق هذا المشروع عام 1999 في جامعة UCAID (University Corporation for Advanced Internet Development).

وتعمل حالياً أكثر من 170 جامعة على تطوير وتنفيذ ما تتطلَّبه إنترنت2 من تطبيقات وتقنيات شبكية متقدمة وذلك بتمويل من الحكومة الأمريكية وبمشاركة أكثر من 60 شركة رائدة عالمياً في قطاع تكنولوجيا الاتصالات والمعلومات. ولن يقتصر استخدامات هذه التطبيقات والتقنيات على الأبحاث والتعليم بل سيشمل أيضاً أغراضاً مدنية وتجارية. ولن تكون إنترنت2 منفصِلة عن الإنترنت الحالية ولن تكون بديلاً عنها.

أما إنترنت الجيل المُقبل (Next Generation Internet-NGI) فهو مشروع تشترك فيه عدة هيئات ومؤسسات سعياً لمضاعفة السرعة الحالية للإنترنت من 100 إلى 1000 مرة ولإيجاد تقنيات تشبيك أقوى كثيراً من تلك الموجودة حالياً على الإنترنت.

ومن الإدارات الفيدرالية الأمريكية المشاركة في هذا المشروع: وكالة NASA (National Aeronautics Space Administration) ووكالة DARPA (Defense Advanced Research Projects Agency) ومؤسسة NSF (National Science Foundation) بإضافة إلى وزارة الطاقة الأمريكية (Department of Energy). ويهدف مشروع إنترنت الجيل المقبل (NGI) إلى تطوير تقنيات تشبيك شاملة متقدِّمة تُحفز على تطوير تطبيقات ستستَخدم في الشركات وإدارة الأعمال والجامعات والمدارس كما سيستخدمها أيضاً عموم الناس.

وبخلاف ما عليه الحال في مشروع إنترنت2 الذي تقوده الجامعات فإن الحكومة الأمريكية هي التي تقود وتموِّل مشروع (NGI).

ومن أهم التطبيقات التي ستحققها إنترنت2 وإنترنت الجيل المُقبل: المكتبات الرقمية (digital libraries) والهاتف ببروتوكول الإنترنت IPV6 والتليفزيون التفاعلي ومؤتمرات الفيديو والأوساط المتعددة والطب العلاجي وتطبيقات إلكترونية متقدِّمة للتعليم والرعاية الصحية والحكومات الإلكترونية والتأمين والخصوصية إضافة إلى تطبيقات تجارية وصناعية وبيئية. وحالياً يتقدم المشروعين بشكل متوازٍ ويكمِّل كل منهما الآخر.

7-2 الإنترنت في متناول الجميع

إذا كانت بدايات استخدامات الإنترنت مقتصرة على العاملين بالمؤسسات المدنية والتجارية المتعاملة مع وزارة الدفاع الأمريكية عام 1990 فإن استخدامها اليوم انتشر ليشمل الكبير والصغير العالم والطالب التاجر والمشتري والرجل والمرأة مهما اختلفت درجات التعليم من المتوسط إلى العالي فكل يجد في الشبكة ما يريد من المعلومات والخدمات. ففي دراسة نصف سنوية يجريها معهد جورجيا للتكنولوجيا في أتلانتا بالولايات المتحدة الأمريكية منذ عام 1994 تشير إلى ارتفاع معدل مستخدمي الإنترنت على المستوى العالمي وإلى ارتفاع مستوى مختلف الفئات والشرائح الاجتماعية التي تستخدم الشبكة وكذلك إلى ازدياد نسبة مستخدمي الإنترنت خارج الولايات المتحدة الأمريكية. ولقد توصلت الدراسات على عينة من مستخدمي الإنترنت إلى الحقائق الآتية [المرجع رقم (34)]:

1) ارتفاع نسبة النساء المستخدمات للشبكة من 5% إلى 38% مقابل 62% للرجال.
2) ارتفاع بنسبة (11%) للنساء الشابات (سن 16-20 سنة) المستخدمات للشبكة أكثر من الرجال (8%) في نفس الفئة العمرية.
3) انخفاض مستوى المستخدمين المتعلمين للشبكة الذين يحملون شهادات جامعية وما فوقها من 66% إلى 47%.
4) ارتفاع مستوى المستخدمين الذين يمتلكون خبرة طويلة في استخدام الشبكة حيث أظهرت الدراسة أن 37% من العينة تحت الدراسة يمتلكون خبرة أقل من سنة في استخدام الإنترنت بينما يشكل ذوى الخبرة نسبة 63%.
5) ذكرت 84% من العينة أن خدمة الإنترنت أصبحت ضرورية ولا غنى عنها في حياتهم.

6) تسوق من الإنترنت نسبة 84% من العينة من المستخدمين القدامى مقارنة بنسبة 54% من المستخدمين الجدد.

7) انخفاض نسبة المستخدمين العاملين في شركات ومؤسسات الحاسب عن السنوات السابقة حيث أظهرت الدراسات أن 21% من المستخدمين المشاركين في الدراسة يعملون في مجالات الحاسب الآلية.

8) يدخل الشبكة 41% من المستخدمين من بيوتهم .

9) يستخدم 49% من الفئة العمرية (19-25 سنة) الشبكة في الأغراض التعليمية.

10)ارتفعت نسبة العينة في الفئة العمرية (50 سنة وما فوق) إلى 30%.

11)ذكر 41% من نفس الفئة العمرية (50 سنة) إن الشبكة ربطتهم أكثر مع أفراد عائلاتهم.

12)بلغ متوسط معدل الزيادة العالمية في استخدام الإنترنت ما بين 6-10% شهرياً.

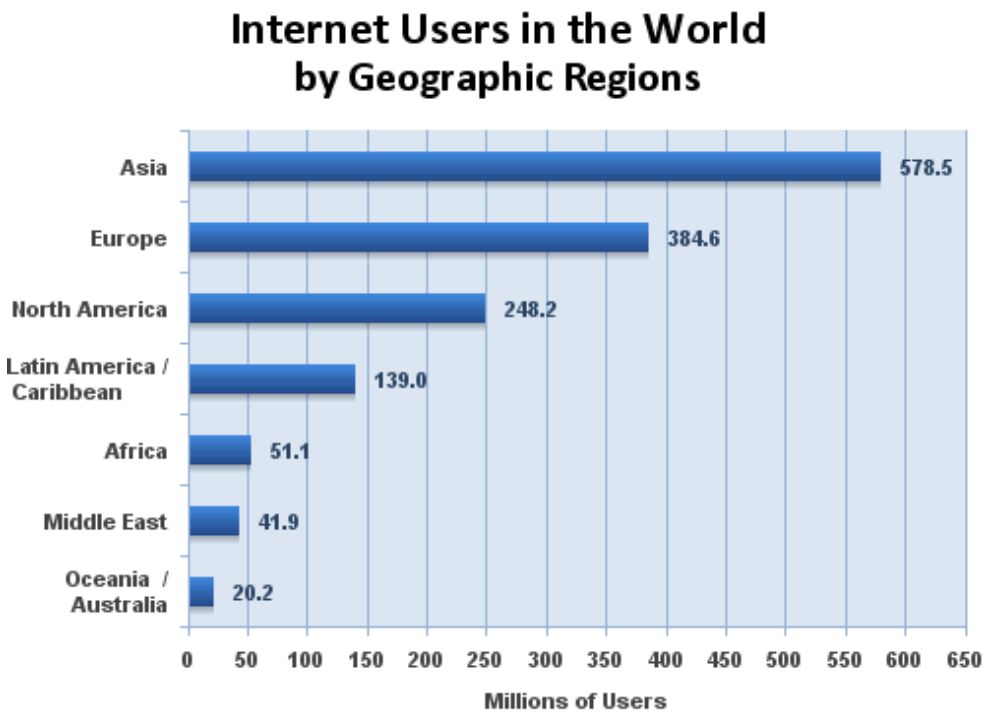
13)تلاحظ حالياً زيادة عالية في عدد مستخدمي الشبكة بنسبة قياسية حيث تتراوح هذه الزيادة ما بين 100% إلى 250%.

14)تمثل مواقع الاتصالات الهاتفية نسبة 22% من المستخدمين تليها مواقع الاتصالات الاجتماعية بنسبة 16% ثم مواقع الترفيه بنسبة 14% فمواقع التسوق بنسبة 8% يليها التعليم والأعمال بصفة عامة 6% بينما تحتل باقي المواقع نسبة 35%.

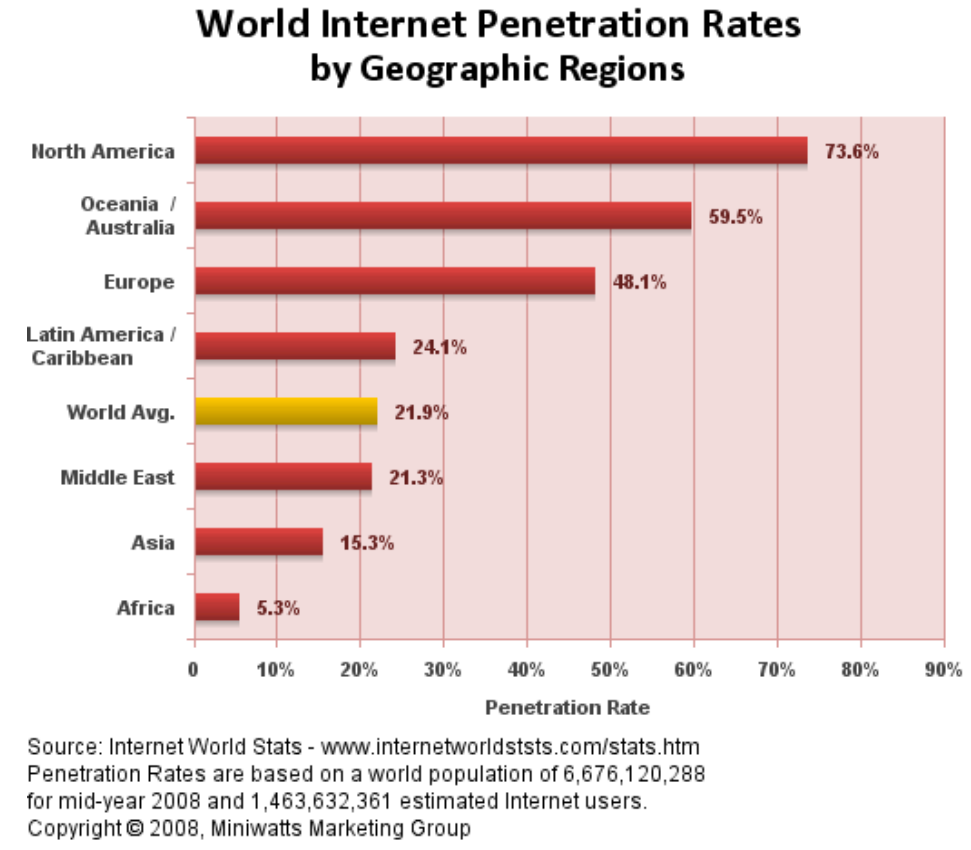
15)مواقع ياهوو (Yahoo) وجوجل وأمريكان أون لاين الأكثر انتشاراً كخادم بريد. والمواقع "س ن ن" و"ب ب سي" و"تايمز" الأكثر انتشاراً في الإعلام – وموقع E-Pay وأمازون وديل الأكثر انتشاراً في التسوق. وحيث انتشرت كالطوفان وفي زمن قياسي المواقع الاجتماعية: أي فون– بادو– فاسبوك– دايلى موشن– سكاى باى– ويبكينز– ويو تيوب واحتلت المرتبة الخامسة بين المواقع الأكثر انتشاراً عالمياً.

16)أكثر 4 مواقع انتشاراً يوتيوب حيث يزوره يومياً 258 مليون زائر بمعدل زيادة سنوية 94% يليه فايسبوك بعدد 101 مليون زائر بمعدل زيادة سنوية 305% ثم سكاي باي حيث يزوره 276 مليون زائر بمعدل زيادة سنوية 61% وأخيراً موقع بأي بال حيث يزوره 57 مليون زائر بمعدل زيادة 16%.

وتؤكد الإحصائيات التي نشرتها مؤسسة Internetworldstats [المرجع رقم (68)] ومركز International Data Center (IDC) [المرجع رقم (34)] وكذلك ووفقاً لإحصائيات الاتحاد الدولي للاتصالات ITU [المراجع أرقام (39 و68)] أن قارة أمريكا الشمالية (الولايات المتحدة الأمريكية وكندا) ما زالت تتقدم على القارات في نسبة استخدام الإنترنت حيث يستخدم الشبكة 248 مليون من أصل 337 مليون لتصل النسبة إلى 73,6% – تليها أستراليا حيث يستخدم الشبكة 20 مليون من أصل 34 مليون لتصل النسبة إلى 59,5% – ثم أوروبا حيث يستخدم الشبكة 384 مليون من أصل 800 مليون لتصل النسبة إلى 48,1% – ثم أمريكا اللاتينية حيث يستخدم الشبكة 139 مليون من أصل 576 مليون لتصل النسبة إلى 24,1% – يلي ذلك منطقة الشرق الأوسط حيث يستخدم الشبكة 41 مليون من أصل 197 مليون لتصل النسبة إلى 21,3% – ثم آسيا حيث يستخدم الشبكة 578 مليون من أصل 3776 مليون لتصل النسبة إلى 15,3% – وأخيراً أفريقيا حيث يستخدم الشبكة 51 مليون من أصل 955 مليون لتصل النسبة إلى 5,3%. والأشكال أرقام (6 و7) توضح إحصائيات استخدام الإنترنت على مستوى العالم (طبقاً للمراجع أرقام 30 و34 و39 و68).



الشكل رقم (6): أعداد مستخدمي الإنترنت طبقاً للتوزيع الجغرافي العالمي



الشكل رقم (7): نسبة مستخدمي الإنترنت لعدد السكان طبقاً للتوزيع الجغرافي العالمي

وتتوقع الدراسات أن الإنترنت ستشهد "انفجاراً سكانياً" في السنوات القليلة القادمة حيث تتوقع أن يصل عدد مستخدمي الشبكة إلى أكثر من مليار ونصف مستخدم عام 2010. وستنخفض نسبة الأمريكيين بين مستخدمي الإنترنت إلى 54% ليحتل مكانها دول جديدة مثل الصين حيث تتوقع مؤسسة IDC أن تتفوق بلدان قارة آسيا على بلدان أستراليا وأوروبا الغربية (التي تحتل حالياً المركز الثاني والثالث بعد أمريكا في نسبة المستخدمين).

يطلب مستخدمو الإنترنت على مستوى الدول المزيد من الخدمات والتوسعات في بوابات الربط مع الإنترنت على مستوى الدول وبالتالي على مستوى سرعات ربط المشتركين.

وعندما يتحدث مجتمع الإنترنت العالمي عن البليون القادم من مستخدمي الإنترنت فهم يتحدثون عن آسيا ومنطقة الشرق الأوسط وإفريقيا. فعلى سبيل المثال ووفقاً لإحصائيات الاتحاد الدولي للاتصالات ITU والمراجع أرقام (39 و68) يبلغ عدد سكان الهند 1,13 بليون نسمة ونسبة دخول إلى الإنترنت تصل إلى 5,3% ويبلغ عدد سكان الصين 1,3 بليون نسمة ونسبة دخول إلى الإنترنت تصل إلى 12,3%. وبالمثل في دول الشرق الأوسط التي يبلغ عدد سكانها 195 مليون نسمة تقريباً يوجد حالياً 33,5 مليون مستخدم للإنترنت وعلى سبيل المثال يوجد بإيران 18 مليون مستخدم مع نسبة دخول تصل إلى 25,6%. وبالمقارنة ببلدان أوروبا وأستراليا حيث تصل نسبة الدخول إلى الإنترنت فيهما ما يقرب من 70% فالمطلوب تساوي نسب مشتركي الإنترنت على مستوى العالم.

ولتسهيل استخدام شبكة الإنترنت وجعلها في متناول الجميع في أي مكان – عمدت بعض الشركات المتخصصة إلى نشر مقاهي أو أكشاك الإنترنت (Internet Kiosks or Café) في الشوارع العامة والمطارات والمتاجر ومحطات السيارات والقطارات والفنادق والمنتجعات والسوبر ماركت والقرى والأماكن السياحية. وتوجد هذه الأكشاك على ثلاثة أنواع:

1) مكاتب لرجال الأعمال والمسافرين: حيث أخذت الشركات تنشر هذه المكاتب في المطارات ومحطات السفر والفنادق وتتيح للمسافر فتح بريده الإلكتروني وإرسال الفاكسات وقضاء أعمال معينة مقابل رسوم خدمة.

2) تليفونات وحاسبات شخصية متعددة الوسائط والمهام: حيث وفرت شركات الاتصالات هذه المعدات المؤهلة للإنترنت لتوفر الأنباء والخرائط المحلية والأماكن السياحية، فضلاً عن المكالمات وتتيح الدفع بواسطة بطاقات الائتمان أو البطاقات الذكية.

3) أكشاك التجارة الإلكترونية ذات الشاشات اللمسة والشبيهة بالحاسبات Hand Held PC التي تعتمد في استخدامها على لغة HTML تمهيداً لربطها بالإنترنت. وقد بدأ الكثير من الشركات استخدام هذه الأكشاك ضمن تطبيقات الحكومات الإلكترونية شاملاً ذلك حجز تذاكر السفر والسياحة والفنادق والمتاجر العامة وانتشرت في الولايات المتحدة وكندا وهونغ كونغ وغيرها من البلدان الغربية والعربية.

8-2 الإنترنت في العالم العربي

كما ذكرنا آنفاً فقد بلغ عدد مستخدمي الإنترنت في العالم 1,319 بليون شخص في ديسمبر 2007 ووفقاً لإحصائيات الاتحاد الدولي للاتصالات (ITU) يوجد في الإمارات العربية المتحدة ما يزيد قليلاً على 1,7 مليون شخص متصلون بالإنترنت مع نسبة دخول إلى الإنترنت تصل إلى 42,9%. ويوجد في المملكة العربية السعودية 4,7 مليون مستخدم للإنترنت مع نسبة دخول تصل إلى 19,5%.

ويوجد في مصر 6,9 مليون مستخدم بنسبة دخول 8,8%. وفى سوريا 1,5 مليون مستخدم بنسبة دخول تصل إلى 7,7%. وتعد مصر أولى دول الدول العربية في عدد مستخدمي الإنترنت.

والجدول رقم (1) يوضح عدد مستخدمي الإنترنت في العالم العربي ونسبة عدد المستخدمين إلى نسبة عدد السكان وذلك طبقاً لإحصائيات الاتحاد الدولي للاتصالات والمراجع أرقام 34 و68.

الجدول رقم (1): الإنترنت في العالم العربي

الترتيب	الدولة	العدد التقريبي لمستخدمي الإنترنت	النسبة المئوية لعدد المستخدمين بالنسبة لعدد السكان
1	مصر	6,9 ملايين	8,8
2	المغرب	4,6 مليون	15,1
3	السودان	2,8 ملايين	8,8
4	السعودية	4,7 مليون	19,5
5	العراق	2,53 مليون	10
6	الجزائر	1,92 مليون	5,7
7	الإمارات	1,7 مليون	42,9
8	سورية	1,5 مليون	7,7
9	تونس	953 ألف	9,2
10	الكويت	700 ألف	25,6
11	الأردن	2 مليون	52
12	لبنان	600 ألف	15,4
13	اليمن	330 ألف	1
14	عمان	285 ألف	10
15	فلسطين	243 ألف	7,9
16	قطر	219 ألف	26,6
17	ليبيا	205 آلاف	3,3
18	البحرين	155 ألف	20
19	الصومال	90 ألف	0,7
20	موريتانيا	20 ألف	0,5
21	جيبوتي	10 آلاف	1,1

ويقدّر عدد مستخدمي الإنترنت المتكلمين باللغة العربية حوالي 28 مليوناً ونصف المليون. أي حوالي 2,5% من تعداد المستخدمين في العالم وهي المرتبة العاشرة في العالم بعد اللغة الإنجليزيّة 28,9% والصينيّة 14,7% والإسبانيّة 8,9% واليابانيّة 7,6% والألمانيّة 5,2% والفرنسيّة 5% والبرتغاليّة 3,6% والكوريّة 3% والإيطاليّة 2,7%.

وعلى سبيل المثال بدأ استخدام الإنترنت في مصر في عام 1992 حيث تمّ تمديد بنية اتصالات تحتيّة بين شبكة الجامعات المصريّة FRCU وشبكة "بت نت" الفرنسيّة التي عملت كبوابة ربط Gateway بين مصر والعالم الخارجي في مجال البحوث العلمية إلى جانب ذلك بدء استخدام شبكة الإنترنت في المجال التجاري والمدني حيث اقتصرت هذه الخدمة وقتها على جهتين حكوميتين فقط هما مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء IDSC وشبكة مركز تكنولوجيا المعلومات الإقليمية RITSEC. ومع بداية عام 1994 بدأ مركز IDSC في إدخال خدمة الإنترنت للوزارات والهيئات الحكومية والمحافظات. وتخصصت شبكة الجامعات في إمداد المعاهد الأكاديمية والجامعات بخدمة البحث العلمي. وبداية من عام 1997 بدأ المركز في خصخصة خدمات الإنترنت من خلال إتاحة الخدمات لعدد من الشركات الخاصة كمزودين للخدمة ISPs والذين يقومون بدورهم ببيع الخدمة للمواطنين والشركات.

وفى عام 1997 تواجد بالسوق المصري 16 شركة خاصة لتقديم خدمات الإنترنت ارتبطت من خلال قنوات الشركة المصرية للاتصالات ووصل عدد الشركات العاملة في هذا المجال إلى حوالي 68 شركة بحلول عام 2000 وفي عام 2002 بدأت الحكومة المصرية في مبادرة الإنترنت المجاني وهى عبارة عن مشروع تبنته وزارة الاتصالات والمعلومات بعقد شراكة بين الشركة المصرية للاتصالات وشركات مزودي خدمة الإنترنت لتقديم خدمة الاتصال بالإنترنت بتكلفة المكالمة العادية. وفي عام 2004 أطلقت الحكومة المصرية مبادرة الإنترنت فائق السرعة ADSL لسرعة التحميل 256 ك ب/ث في اتجاه وسرعة 2 ميجاب/ث في الاتجاه المقابل.

في يوليو 2007 أعلن وزير الاتصالات وتكنولوجيا المعلومات المصري عن تطبيق نظام جديد حيث تم تحديد كمية التحميل حسب سرعة الاشتراك. وفي أبريل 2008 ظهرت خدمة ADSL+2 التي تصل السرعات بها إلى 24 ميجا/الثانية.

وطبقاً لإحصائيات وزارة الاتصالات وتكنولوجيا المعلومات المصرية المنشورة في "الكتاب الذهبي للوزارة إصدار عام Egypt ICT Golden Book 2007" بلغ عدد مستخدمي الإنترنت عام 2007 في مصر حوالي 6 ملايين و990 ألف مشترك مما يجعلها أول الدول العربية استخداماً للإنترنت (طبقاً للجدول رقم 1). ويبلغ عدد مزودي خدمة الإنترنت في مصر 220 شركة وتنقسم هذه الشركات إلى 3 مستويات (أ، ب، ج) والمستوى «أ» يضمّ أربع شركات فقط وهي (تي إي داتا - ولينك دوت نت ونايل أون لاين وإيجي نت) وهي الشركات التي تملك البنية التحتية للإنترنت في مصر. وتعتبر تي إي داتا هي أكبر مزود لخدمة الإنترنت في مصر – أما المستوى «ب» فيضم الشركات التي تقدم خدمة الإنترنت من خلال الشراء من الشركات التي في المستوى «أ». أما المستوى «ج» فيضم الشركات التي تقدم الخدمات للجمهور من خلال الشراء من المستويين (أ) و(ب).

وأكثر المواقع زيارة في مصر هي: فور اسلام – فور أراب– اي سي كيو– ياهوو – جوجل – فيسبوك – ويندوز لايف – يوتيوب – رابيدشير– إم.إس.إن – الجزيرة– مصراوي – عجيب – وأخيراً مكتوب.

9-2 الخدمات التي تقدمها الإنترنت

يمكن تقسيم خدمات الإنترنت إلى خدمات رئيسية وخدمات فرعية كالتالي:

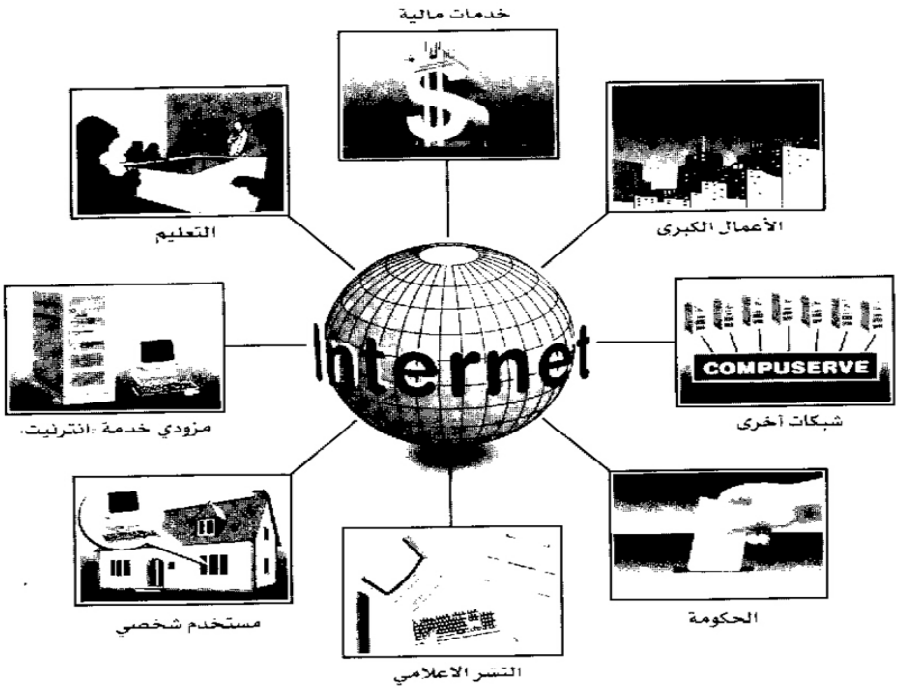
* خدمة تداول الرسائل وينبثق منها الخدمات الفرعية التالية:
  1) البريد الإلكتروني.
  2) المجموعات الإعلامية التخصصية.
  3) استخدام الشبكة.
  4) المحادثة أو الدردشة الفورية بالكتابة (النصوص).
  5) المؤتمرات المرئية (صورة وصوت).

* خدمة البحث وتداول الملفات وينبثق منها الخدمات الفرعية التالية:
  1) البحث باستخدام البروتوكول TCP/IP باستخدام نقل الملفات FTP.
  2) البحث باستخدام قوائم جوفر.
  3) البحث باستخدام الشبكة العنكبوتية www.
  4) البحث بواسطة محركات البحث : ياهوو – التافيستا – ليكوس – ...
  5) البحث عن الملفات التاريخية بواسطة أرشي – فيرونيكا – ...

* خدمات الدخول عن بعد على حاسب الشبكة:
  خدمة Telnet

* الخدمات التخصصية ذات التقنية العالية وتشمل:
  1) التجارة الإلكترونية.
  2) التعليم الإلكتروني عن بعد.
  3) الأعمال الإلكترونية: حجز التذاكر – الفنادق – البورصة – ....الخ
  4) الدخول المباشر في الوقت الحقيقي على البنوك – البنك المنزلي.
  5) الاتصالات التليفونية باستخدام الإنترنت (Voice Over IP or Internet Telephony).
  6) استخدام المحمول في الاتصال بخدمات الإنترنت.
  7) الترجمة الفورية.
  8) الفاكس بالإنترنت.
  9) الحكومة الإلكترونية.

الشكل رقم (8) يوضح أهم الخدمات التي توفرها شبكة الإنترنت.



الشكل رقم (8): أهم الخدمات التي توفرها شبكة الإنترنت

يتضح من سرد خدمات الإنترنت أن المستفيد منها يستطيع بصفة عامة تحقيق الآتي:

1) التواصل والارتباط بالعالم الخارجي عبر الإنترنت وبأقل التكاليف وذلك عبر استخدام البريد الإلكتروني والدردشة بالصوت والصورة والمؤتمرات التليفزيونية التي تنقل بواسطة الكاميرات WEB CAM المزود بها حالياً جميع أجهزة الحاسبات الشخصية الثابتة والمحمولة والتلفونات المحمولة.
2) تصفح الوثائق والمستندات والكتب في أي مكان من العالم إما مجاناً أو بتكلفة شريطة أن يكون مشترك في شبكة المعلومات أو المكتبات التي بها الوثائق والمستندات والكتب.
3) نقل الملفات وكافة أنواع المعلومات من حاسب آلي كبير إلى آخر أصغر وتحديث البيانات المستخدمة.
4) نقل المعلومات والبرامج بين مختلف الأجهزة.
5) المشاركة في مجموعات النقاش أو المنتديات.
6) تقديم المعلومات والخدمات الحكومية والبنكية والمالية والتسوقية ...الخ.
7) الخدمات الإعلامية.
8) الهاتف عبر الإنترنت.
9) التعليم وإدارة الأعمال عن بعد.
10) التجارة الإلكترونية.
11) البنك المنزلي الإلكتروني (Home Banking- Internet Banking).

11)كافة تطبيقات الحكومة الإلكترونية (استخراج شهادات الميلاد ورخص القيادة وتجديد رخص السيارات والإقرارات الضريبية ودفع الجمارك والتطبيقات المماثلة).

سنقدم في هذا الفصل خصائص أهم خدمات الإنترنت:

1) البريد الإلكتروني (E-Mail)

هي إحدى أهم المميزات والخدمات الأساسية التي تقدمها الإنترنت وأكثرها انتشاراً حيث تمثل حوالي 90% من حركة بيانات الشبكة. ظهر البريد الإلكتروني بشكل عملي وفعال في عالم الإنترنت في عام 1988. وميزة البريد الإلكتروني أنه باستطاعة شخص أن يتبادل البريد ويخاطب أو يراسل أي شخص آخر يعرف بريده الإلكتروني في أي مكان في العالم خلال ثوان وبأقل التكاليف. ومقارنة مع البريد العادي أو التليفون أو الفاكس فإن البريد الإلكتروني يعتبر أكثر سرعة وفاعلية وأقل تكلفة. فالبريد العادي على سبيل المثال يأخذ أياماً أو أسابيع حتى يصل إلى المرسل إليه. أما التليفون فإنه سريع وميزته يعطي الصوت إلا أنه أكثر سعراً.

وكذلك الفاكس سريع إلا أنه أقل وضوحاً.

يجمع البريد الإلكتروني بين أغلبية هذه الأشياء المذكورة عالية ويعتبر أكثر وضوحاً وأسرع وممكن أن يتم تبادل الرسائل أو التخاطب مع الجانب الآخر من الخط بكل سهولة وبتكلفة زهيدة لكن يشترط لتنفيذ كل ذلك أن يكون لدى الشخص الآخر حساب بريد إلكتروني.

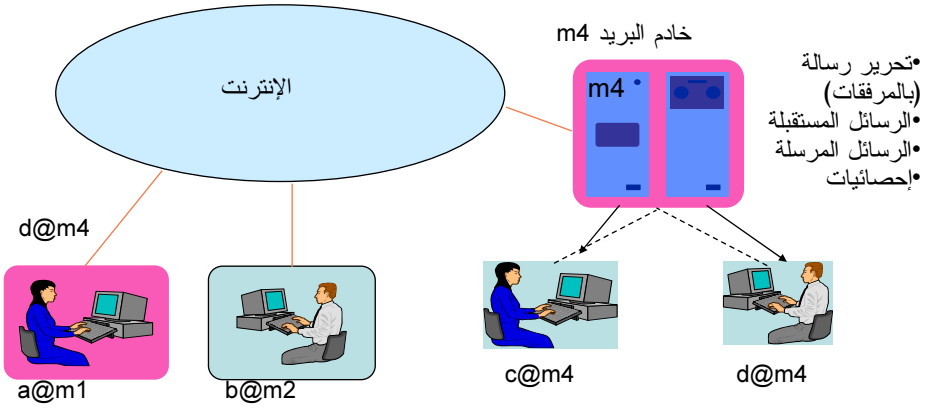
في السنوات الأولى لاستخدام البريد الإلكتروني حدث الكثير من الصعوبات والمشاكل بين الشركات التي تسيطر على سوق الإنترنت. ففي السنوات الأولى كان لا بد من الاشتراك في شبكة NSF net واستخدام البريد الإلكتروني من خلالها. فكان المشترك مثلاً يبيع استخدام البريد إلى شخص آخر وكذلك يبيع ذلك المشترك الجديد الاستخدام إلى عدة مشتركين جدد (1 أو 2 أو أكثر) وهؤلاء يبيعون إلى مجموعة أخرى فكان المشترك الأول هو الذي يحدد شروط وأسعار استخدام الشبكة. وبتوسع الشبكة وإيجاد شبكات محلية في مناطق معينة وانتشار الشبكة تواجدت مجموعة من الشركات التي توفر خدمات البريد في الإنترنت. ووضعت الشركات شروطاً مجحفة بحق المستخدمين. فكان المستخدم لا يستطيع الاتصال إلا بالمشتركين في الشبكة التي هو مسجل بها. وعند توسع الشبكات وزيادة عددها أصبحت هذه الشبكات مثل الجزر المنفصلة في المحيط. وتزايد الصراع والتنافس بينها في سبيل من يدفع للآخر وأي شبكة أقوى وأمور تجارية أخرى مما أثر سلبياً على مشتركي الشبكة.

وفي التسعينات بدأ الكثير من الجامعات في العالم في تأسيس أقسام بها خاصة بعلوم الحاسب وبدأت كذلك في توزيع البريد الإلكتروني للعاملين فيها من أساتذة وطلاب وموظفين بالمجان. فأصبح من السهولة بمكان الحصول على بريد إلكتروني مجاني من جامعة واستخدامه ومراسلة الأصدقاء على أي شبكة كانت. ومن هنا انطلقت فكرة البريد الإلكتروني المجاني في كل الشبكات العالمية. واستطاع المستخدم أن يخاطب أي عنوان بريد إلكتروني على أي شبكة كانت في أمريكا وأوروبا وآسيا وإفريقيا. والشكل رقم (9) يوضح الشكل العام للبريد الإلكتروني.

البريد الإلكتروني

يوفر خادم البريد صندوق إرسال وصندوق استقبال لكل مشترك مسجل به.

من خلال الحاسب خادم البريد يتم تبادل الرسائل فيما بين المشتركين.



الشكل رقم (9): يوضح الشكل العام للبريد الإلكتروني

من أهم استخدامات البريد الإلكتروني: إرسال البريد الإلكتروني إلى شخص معين أو إلى مجموعة من الأشخاص – قراءة البريد والرد عليه – حذف وتخزين الرسائل البريدية – تمرير البريد وإرساله إلى اتجاهات مختلفة – إرسال الملاحق مع الرسائل – عمل إحصائيات للبريد المرسل أو المستقبل – البحث بالكلمات عن رسالة أو موضوع معين ... الخ.

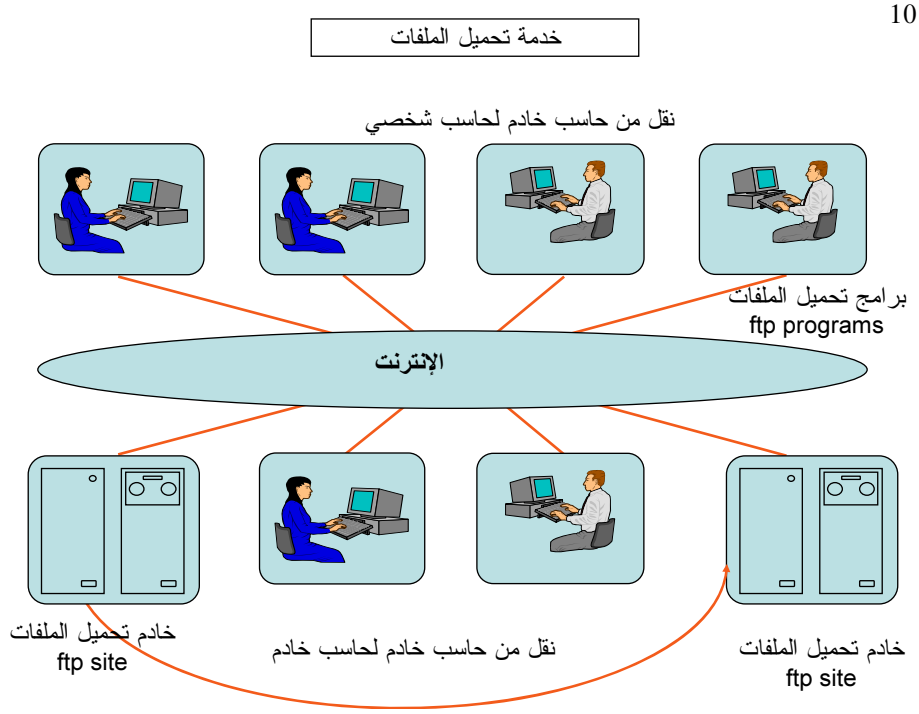
2) المجموعات الإخبارية News Groups وخدمة استخدام الشبكة Usenet

المجموعات الإخبارية هي مجموعات من الأفراد المتخصصين في تبادل الأخبار والمعلومات والنقاشات عبر الشبكة حيث يستطيع أي مستخدم جديد أن ينضم إلى إحدى هذه المجموعات حسب ميوله ويشارك معهم في الحوارات والنقاشات ويتبادل المقالات والأخبار وكافة أنواع المعلومات عبر الشبكة وعندما تزيد القوائم البريدية إلى حد معين تتكون "مجموعة إخبارية" وهي عبارة عن تجميع لعدد كبير من مشتركي الشبكة الذين يجمعهم تخصص معين من التخصصات المهنية والعلمية الدقيقة (مثل المجموعة السياسية والرياضية والإعلامية والبنكية والتجارية والصحية ... الخ) وتتبادل المجموعة المعلومات التخصصية فيما بينها بطريقة تتضمن اصطلاحات لا يفهمها المستخدم العادي. ويطلق أيضاً على هذه الخدمة "USENET" أو استخدام الشبكة والمعلومات الموجودة في هذه المجموعات متاحة لكل المتصلين بشبكة الإنترنت ويمكن للمتخصص الدخول على المجموعة الخاصة به لتبادل الآراء والمعلومات معها أو لاستقبال المعلومات الموجودة بها والاستفادة منها دون الدخول معهم في الحوار. ويوجد أكثر من 10 آلاف مجموعة إخبارية تحتوي على معلومات هامة مثل الأحداث العالمية – أخبار السلع والمنتجات – البورصة وأسعار العملات – الاكتشافات العلمية في كافة المجالات – الطقس – الخرائط العالمية – أخبار الرياضة – علاج الأمراض – وغيرها من الموضوعات والإعلام الهامة.

3) تداول البرامج والملفات والوثائق

يوجد بالشبكة عدة مواقع توفر برامج وملفات تسمى Download Sites مثل المكتبات وشركات تطوير وبيع البرمجيات يتم من خلالها وباستغلال برامج تحميل للحاسبات الشخصية (Down Load Programs) يتم تحميل البرامج والملفات – تشمل البرامج تطبيقات الأعمال – الألعاب – تشغيل الحاسب – اكتشاف الفيروسات وتلك البرامج يكون منها البرامج المجانية (Free Ware) ومنها برامج للتجربة محدودة زمن الاستخدام (shareware) ومنها برامج للبيع وتشمل الملفات الكتب والمراجع والوثائق والأغاني وما شابه. ويعتبر بروتوكول نقل الملفات (File Transfer Protocol (FTP)) هو أداة لنقل الملفات الكبيرة وتبادلها مع حاسبات أخرى موصولة على الشبكة والشكل رقم (10) يوضح كيفية تحميل الملفات من مواقع البرامج والملفات.

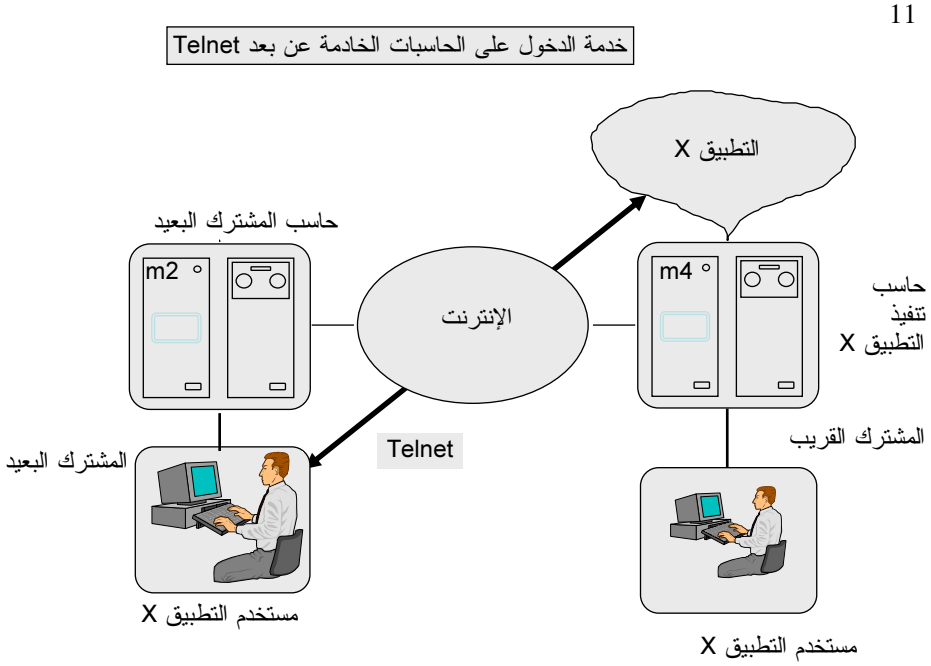
10



الشكل رقم (10): تحميل الملفات من مواقع البرامج والملفات

4) الدخول عن بعد Telnet

هي أداة تستعمل لوصول الحاسبات الشخصية إلى الحاسبات البعيدة، فتسمح الشبكة للحاسبات الشخصية بالعمل كنهاية طرفية لحاسب خادم آخر بعيد ووظيفتها هي أنها تتيح لمستخدمي الإنترنت تشغيل الحاسبات البعيدة التي تحتفظ بفهارس مصادر المعلومات التي تتزايد وتنمو باستمرار في الشبكة العالمية. فمن خلال Telnet يستطيع المستخدم الدخول إلى مختلف المكتبات المرتبطة بالإنترنت والبحث عن الكتب في هذه المكتبات أو المقالات في الصحف والمجلات الموجودة داخل المكتبات الجامعية منها أو الحكومية وكذلك مراكز المعلومات. والشكل رقم (11) يوضح كيفية الدخول عن بعد على الحاسبات الخادمة.



الشكل رقم (11): الدخول عن بعد على الحاسبات الخادمة

5) الاتصال التليفوني عبر الإنترنت/الهاتف بواسطة بروتوكول الإنترنت (Voice Over IP or IP telephony)

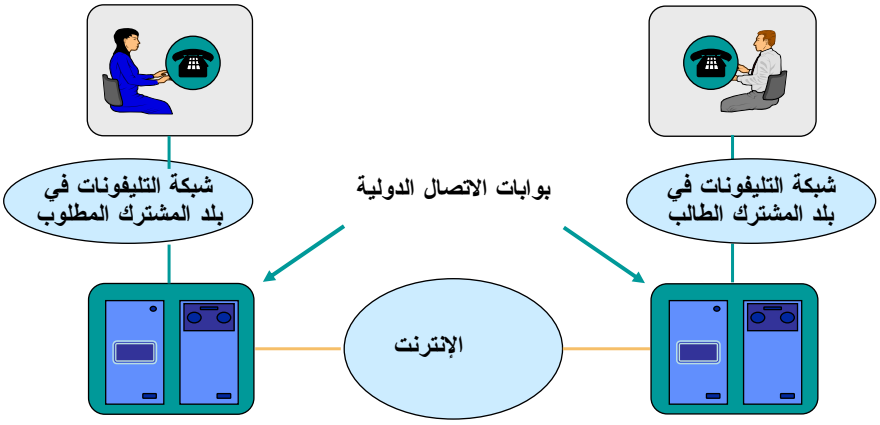
تهدف هذه الخدمة إلى استغلال الإنترنت لإجراء المكالمات بعيدة المدى (الدولية) وكأنها مكالمات محلية. كما تهدف هذه الخدمة إلى إحلال الحاسب الشخصي محل التليفون العادي وتجهيزه بسماعة وميكروفون وكاميرا تليفزيونية لتحقيق الاتصال بينه وبين آخرين بغض النظر عن أماكن تواجدهم. كما يتم استخدام الخدمة لتحقيق الاتصال الهاتفي بالتليفون الثابت والتليفون المحمول. والجدير بالذكر أنه جاري في بعض الدول ومنها مصر وضع الضوابط والقوانين التي تنظم هذه الخدمة وتحافظ على حقوق شركات الاتصالات القومية حيث إن تكلفة الاتصال الدولية بهذه الطريقة تبلغ أقل من 2,5% من التكلفة العادية.

ويوجد ثلاث أنواع من الاتصال التليفوني بالإنترنت:

- اتصال بين تليفون وتليفون (ثابت ومحمول).
- اتصال بين حاسب شخصي (مجهز بالتجهيزات الخاصة) وتليفون.
- اتصال بين الحاسبات الشخصية المجهزة بالتجهيزات الخاصة.

الشكل رقم (12) يوضح الاتصال التليفوني عبر الإنترنت.

خدمة الاتصالات الهاتفية عبر شبكة الإنترنت
Internet Telephony



الشكل رقم (12): الاتصال التليفوني عبر الإنترنت

6) تداول الرسائل القصيرة للمحمول

ظهرت بعض المواقع التي توفر خدمة إرسال الرسائل القصيرة SMS (Short Message System) من الحاسب الشخصي إلى التليفونات المحمولة في أي بلد بالعالم.

7) البنك الشخصي (INTERNET HOME BANKING)

خدمة هامة من خدمات الإنترنت بغرض تحقيق الاتصال المؤمن بين حاسب العميل (الثابت – المتنقل – أو التليفون المحمول) والحاسبات الخادمة للبنك بتكلفة بسيطة وبدون انقطاع. ويمكن للعميل تنفيذ الآتي:

- مراجعة الرصيد.
- طلب دفتر شيكات.
- كتابه الشيكات وإصدار أوامر دفع الفواتير والكمبيالات.
- طلب فتح "خطابات الضمان والائتمان".
- طلب ربط الودائع.
- تحويل مبالغ لعملاء من بنوك أخرى بشرط معرفته لرقم حساب الشخص الآخر.

لتحقيق الاتصال المؤمن بين العميل والبنك يتم تسليم العميل اسم وكلمة مرور ورقم سري مكون من 9 حروف شفرية تتغير باستمرار – كما يتم استخدام نظام شفري من النوع العلني به مفتاح سري يتكون من أكثر من 1024 نبضة ولا يمكن نظرياً كسره.

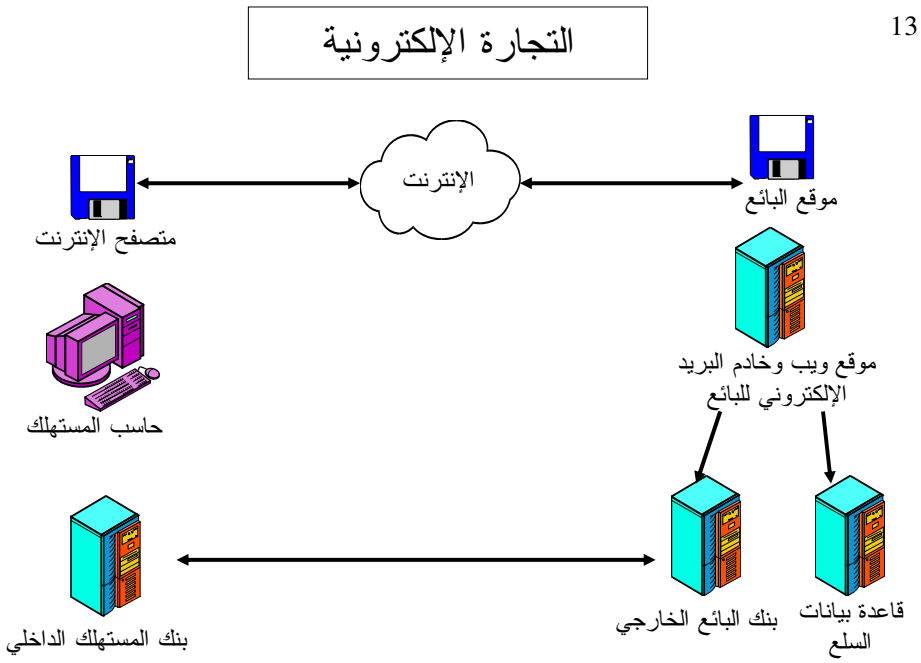
8) استخدام الإنترنت في إدارة الأعمال والتجارة الإلكترونية

إذا ذكرنا الاختراعات التي أثرت تأثيراً مباشراً على الحضارة الإنسانية اقتصادياً واجتماعياً وسياسياً لوجدنا من أهمها التليفون والتليفزيون ووسائل النقل والحاسب الآلي وأخيراً (شبكة الإنترنت) وطبقاً لآخر إحصائيات الأمم المتحدة فإن مستخدمي الإنترنت يومياً وصل عددهم عام 2007 إلى 1319 مليون. هؤلاء يمارسون أنشطتهم من خلال الشبكة حيث يتبادلون المعلومات ويمارس منهم نسبة 8% أي حوالي 105 مليون عقد الصفقات على الإنترنت. وقد وصل حجم التجارة الإلكترونية أو التسوق في أمريكا 29 مليار دولار عام 98 وارتفعت في عام 2005 إلى 990 مليار وارتفعت إلى ألف بليون دولار عام 2008 – بينما تجارة الشرق الأوسط من خلال الإنترنت عام 98 بلغت 100 ألف دولار وقد ارتفعت عام 2005 إلى 12 مليار دولار.

ولقد تم التوسع في استخدامات خدمات الإنترنت المتعددة في مجال إدارة الأعمال مثل التعليم والترجمة والهندسة والتصميم والبحث عن العمل واستخدمت حتى في الزواج – وتمثل الإنترنت العمود الفقري أو الطريق السريع للاتصالات لكافة الأعمال الإلكترونية وعلى رأسها التجارة الإلكترونية التي من المتوقع أن تنمو بسرعة رهيبة لأنها تخدم المنتجين والموزعين والمستهلكين للبضائع والمعلومات كما تخدم البنوك بصفتها الوسطاء بين المنتج والمستهلك سواء في الدفع أو دراسات الجدوى أو التأمين والسرية للمعلومات البنكية لكافة الفئات.

التجارة الإلكترونية مصطلح يطلق على عملية بيع أو شراء أو تبادل منتجات/خدمات أو معلومات عن طريق شبكات الحاسبات وشبكة الإنترنت. وحالياً استخدام الإنترنت كمصدر أساسي في التجارة الإلكترونية والمتوقع في الولايات المتحدة الأمريكية وحدها أن تستخدم شبكة الإنترنت في تداول أكثر من ألف بليون دولار سنوياً نتيجة التجارة الإلكترونية للمنتجات والمعلومات. والشكل رقم (13) يوضح عملية التجارة الإلكترونية بين مستهلك وبائع ودور بنك كل منهما في إتمام الصفقات التجارية.

13

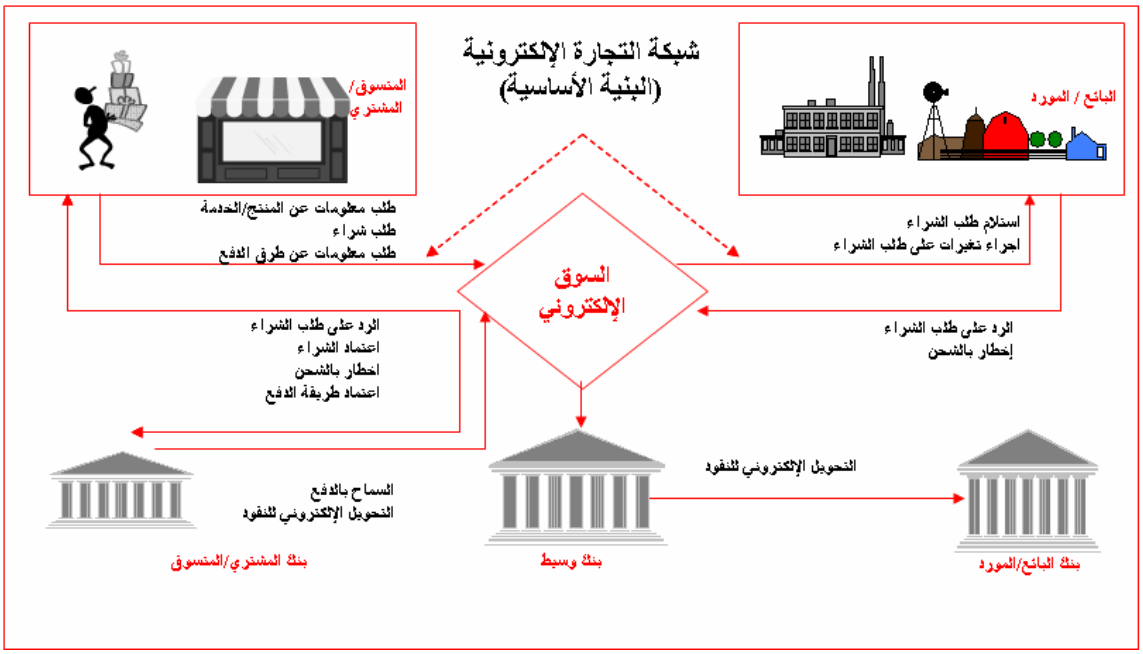


الشكل رقم (13): عملية التجارة الإلكترونية بين مستهلك وبائع

أطراف التجارة الإلكترونية هم:

- بين وحدتي أعمال أو بائعين (B2B Business-to-business)
- بين وحدة أعمال ومستهلك (B2C Business-to-consumer)
- بين مستهلك ومستهلك (C2C Consumer-to-consumer)
- بين القطاع الحكومي والمستهلك (G2C Government-to-consumer)

الشكل رقم (14) يوضح الخطوات الأساسية لتنفيذ منظومة التجارة الإلكترونية من خلال الثلاثة عناصر المكونة للمنظومة وهي: وحدة الأعمال (التاجر) – المستهلك – والبنك.



الشكل رقم (14): الخطوات الأساسية لتنفيذ منظومة التجارة الإلكترونية

9) الحكومة الإلكترونية

تعد خدمات الحكومة الإلكترونية من أهم وأحدث خدمات الإنترنت وهى تعرف بأنها استخدام تكنولوجيا الاتصالات والمعلومات وخاصة الإنترنت كوسيلة لتقديم خدمات حكومية متميزة مما يترتب عليه سياسات وخدمات أحسن ومشاركات أفضل من قبل المواطن. ويعتبر تحديث الدول وتدعيمها بأحدث ما توصلت إليه تكنولوجيا الاتصالات والمعلومات أحد الوسائل الرئيسية للاستمرار في برنامج الإصلاح الاقتصادي والاجتماعي مما ينعكس بشكل إيجابي على المواطنين والمستثمرين وشركات قطاع الأعمال التي تتعامل مع الجهات الحكومية حيث تهدف عملية التطوير بشكل رئيسي إلى تقديم الخدمات الحكومية للمواطن في زمن قياسي وبأقل جهد ممكن وبمستويات الكفاءة العالمية.

تهدف برامج الحكومة الإلكترونية إلى تحقيق الآتي:

1) خدمة المواطنين والشركات والمستثمرين.
2) توصيل الخدمة إلى طالبها.
3) تقديم الخدمات للمواطن مجمعة بصرف النظر عن الجهات الحكومية المختلفة المسؤولة عن أداء تلك الخدمات مع ضمان وصول الخدمات المستحدثة إلى المواطنين في أماكن تجمعهم وقرب محل سكنهم دون الحاجة إلى الانتقال إلى دواوين الحكومة.

4) سرعة إنجاز الأعمال.

5) تقديم خدمات متميزة للمواطنين ومؤسسات قطاع الأعمال تمنحهم طلبهم في فترة وجيزة عن طريق عدة وسائل منها تطوير الإجراءات وحذف غير الضروري منها وإزالة المعوقات وتقديم الخدمات الحيوية لساعات أطول يومياً وخلال أيام العطلات.

6) التميز ورفع كفاءة الأداء.

7) رفع مستوى الكفاءة في تقديم الخدمات وذلك عن طريق إعادة هيكلتها بشكل يتناسب مع توجهات المواطنين وذلك مع إمكانية تقديم الخدمات بأسلوب شخصي يتناسب مع طالب الخدمة.

8) توفير مناخ مشجع للمستثمرين وتذليل العقبات التي يواجهونها والتي تتمثل بشكل أساسي في بطء الإجراءات وتعقيدها، مما سينعكس بشكل إيجابي على تشجيع الاستثمار المحلي وجذب المزيد من الاستثمارات الأجنبية.

9) تحديث نظم العمل بالوزارات والهيئات.

10)تهيئة الحاسب الحكومي للاندماج في النظام العالمي.

الشكل رقم (15) يوضح جزء من خدمات بوابة الحكومة الإلكترونية المصرية كمثال لما يمكن أن تقدمة بوابة الحكومة الإلكترونية للمواطنين.

الشكل رقم (15): جزء من خدمات بوابة الحكومة الإلكترونية المصرية

10) محركات البحث

نختتم خدمات الإنترنت بتقديم محركات البحث حيث إنها الوسيلة الأهم من بين وسائل الوصول المباشر للمعلومات المطلوبة من قبل المستخدم. وهي تتباين في أدوارها ووظائفها وفعاليتها لكن ما يجمعها أنها أمست طريق المستخدمين لطلب المعلومات فهي تتيح الوصول للموضوع ذاته أو للمواقع المهتمة بالموضوع مدار البحث. وتتيح الآن الوصول للأشخاص أو الوصول لأجزاء المعلومات كما يتيح تطورها التقني استخدام أكثر من لغة في عملية البحث والبحث عن مواد بأكثر من لغة.

وتقوم محركات البحث والأدلة الإرشادية في تطور أوسع على شبكة الإنترنت بعمليات جمع وتبويب وتحليل بيانات الاستخدام على نحو واسع مستخدمة إما وسيلة الكعكة (كوكيز – cookie) أو برامج التتبع والالتقاط/الشم (Sniffing Programs) أو غيرها من حزم البيانات اللاصقة (sticky bits) التي تخزن في حاسبات الزائرين من أجل مساعدة الموقع على التعرف على الاتجاهات الخصوصية للزائر ومساعدته في تحديد اتجاهات الإعلان وتقديم المحتويات. وغالباً ما تتيح محركات البحث خدمات إضافية للمشتركين مثل البريد الإلكتروني والدردشة والاتصال الهاتفي وتحميل البرامج. ومن أشهر محركات البحث العالمية المواقع: ياهوو وجوجل وأمريكا أون لاين وفايسبوك وارشى وفيرونيكا. والعربية المواقع: مصراوي وعجيب ومحيط ونسيج واين.

الفصل الثالث

الإطار العام لتأمين شبكات المعلومات

1-3 المقدمة

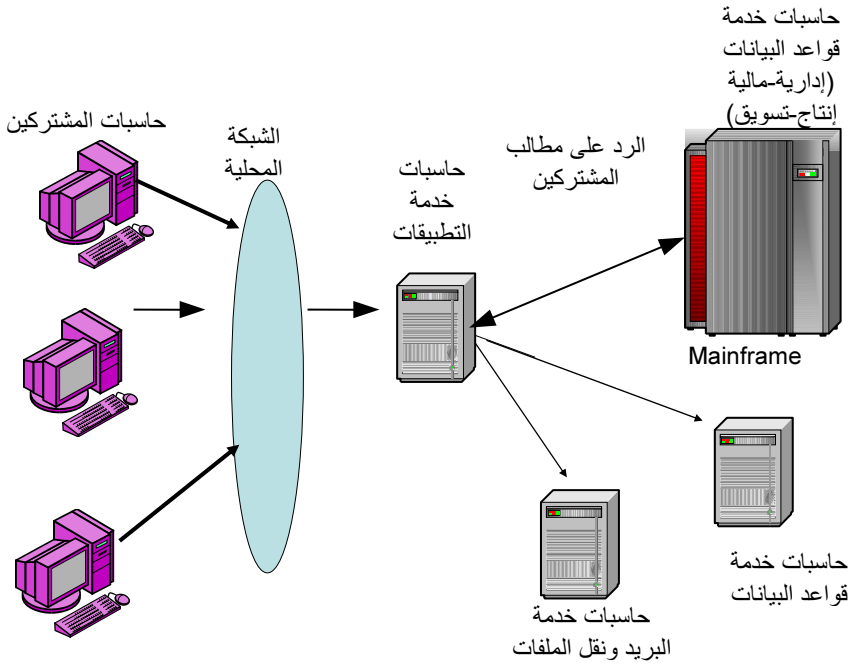
تعتبر البنية المتكاملة لتكنولوجيا الاتصالات والمعلومات ومشاريع شبكات المعلومات على مستوى الدولة ثروة قومية هامة حيث زادت تكلفتها على مدى السنوات عن مئات الملايين من الجنيهات لذلك لا بد وأن تحظى بدعم متواصل لصيانتها واستمرارية تشغيلها بأمان وهذا يعني أنه لا بد من وضع سياسة على المستوى القومي تتبعها خطة على مستوى كل مؤسسة لتأمين وحماية شبكات المعلومات من المخاطر المحتملة سواء كانت طبيعية أو غير طبيعية. وهذا يستلزم توفير المخصصات اللازمة وكذلك توفير الأجهزة الفنية اللازمة المتمكنة من الحفاظ على تلك الثروة. ومن هنا جاءت الحاجة لوضع سياسة أمن المعلومات وإدارة المخاطر.

يتناول هذا الفصل الإطار العام لتأمين شبكات المعلومات بداية بمقدمة عامة حول تكنولوجيا شبكات المعلومات ثم تقديم لخدمات شبكات المعلومات يليها كل ما يتعلق بمعايير التأمين والحماية ثم يناقش متطلبات التأمين الطبيعي ثم يتعرض لبعض الاعتبارات والأبعاد المتعلقة بأمن شبكات المعلومات. ويقدم هذا الفصل الإطار العام لتأمين شبكات المعلومات. وأخيراً يتناول الفصل طرق تنفيذ "السياسة الأمنية" لشبكات المعلومات.

2-3 بنية شبكات المعلومات

يشكل كل من الحاسب الآلي والبرمجيات والبيانات العناصر الأساسية لتقنيات نظم المعلومات في المؤسسات الحديثة. وترتبط الحواسب الخادمة للتطبيقات وقواعد البيانات بالنهايات الطرفية بواسطة أجهزة الاتصال الخاصة بالشبكة المحلية LAN التي غالباً ما تمتد على نطاق عمل المؤسسة لتشمل كافة القطاعات المالية والإدارية والإنتاجية – ويطلق على هذا النظام "الإنترانت". وتشتمل شبكات المعلومات المحلية على معدات فعالة مثل الموجهات (Routers) ووحدات التحويل (Ethernet Switches) بالإضافة إلى المعدات غير الفعالة مثل الكابلات ولوحات التوصيل – ومن الأجهزة الأخرى التي ترتبط بالشبكات المحلية الطابعات وأجهزة الاتصالات. وتتضمن برمجيات الحاسبات نظم تشغيل وبرمجيات التطبيقات التي تصمم خصيصاً لتنفيذ مهمة أو مهام معينة (نظم إدارية – مالية – إنتاج – تسويق –...) وقد تحمل البرمجيات مباشرة في الذاكرة الصلبة للحاسب الآلي أو تخزن على أقراص مدمجة (CD-ROM) – أو على أي وسائل تخزين أخرى متاحة. وتشتمل أساليب العمل على كيفية تشغيل الأجهزة والبرمجيات واستخدامها وصيانتها. كما في الشكل رقم (1).

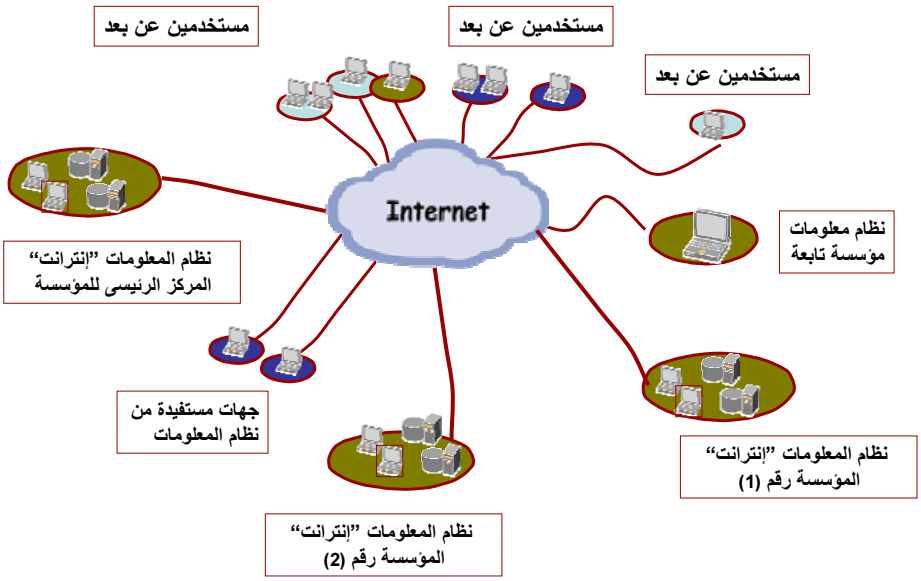
1



الشكل رقم (1): مكونات شبكات المعلومات المحلية

وغالباً ما يكون هناك أكثر من فرع للمؤسسة ويكون لكل فرع الإنترانت الخاصة به. يأتي بعد ذلك دور الشبكات الواسعة WAN "الإكسترانت" للربط بين الإنترانت سواء من خلال شبكة خاصة بالمؤسسة يتم تأجيرها من مزودي خدمة نقل البيانات القومية أو من خلال شبكة المعلومات الدولية الإنترنت أو كلاهما. كما قد تكون هناك أكثر من وسيلة اتصال للمشتركين الخارجيين المصرح لهم تتكون من الوسائل التكنولوجية السلكية واللاسلكية التي تمكن من الوصول إلى نظام معلومات المؤسسة باستخدام موديم وبروتوكول شبكات مثل بروتوكول الاتصال عن بعد (Telnet) كما في الشكل رقم (2).

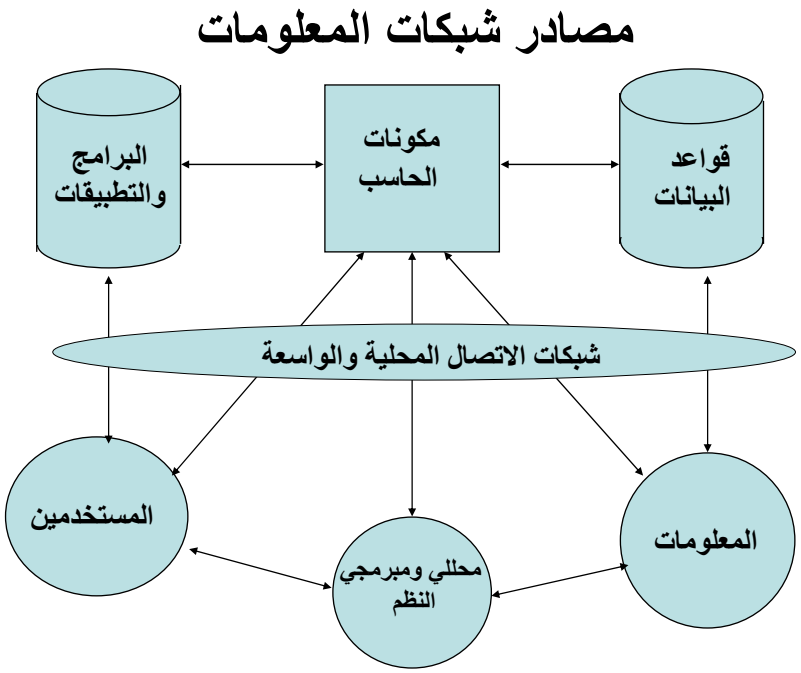
2



الشكل رقم (2): مكونات شبكات المعلومات الواسعة

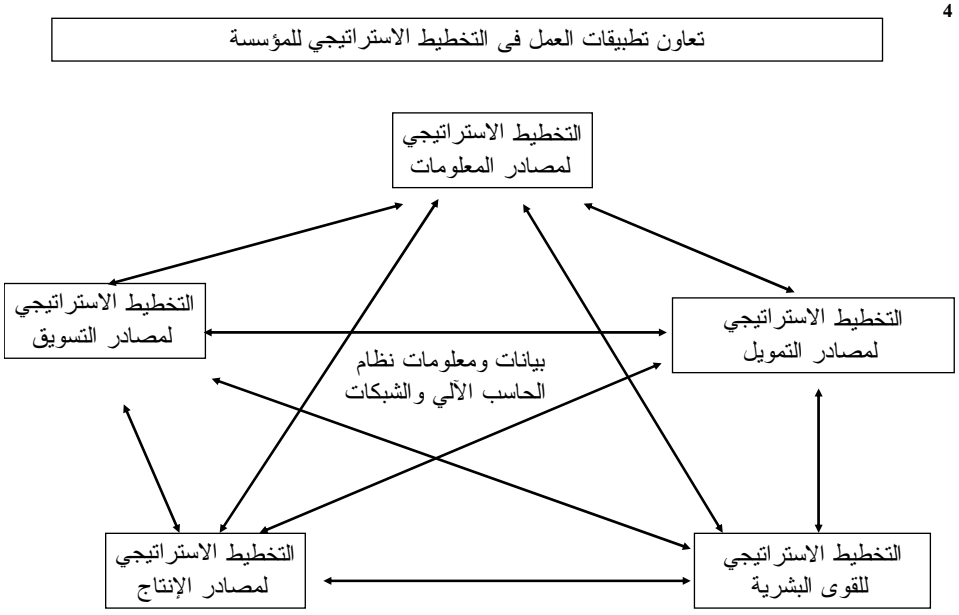
وينشأ الهيكل التنظيمي المساند لنظم وتطبيقات وشبكات المعلومات من أفراد من كافة التخصصات بهدف تخزين البيانات والمعلومات ومعالجتها واسترجاعها وإرسالها أو نقلها للمستخدمين والمستفيدين. وتجمع كل هذه العناصر المختلفة والعديدة معاً لتشكل مصادر شبكات المعلومات (الشكل رقم (3)).

3



الشكل رقم (3): مصادر شبكات المعلومات

وهكذا تدعم تكنولوجيا المعلومات والاتصالات المتقدمة وتساند تنفيذ تطبيقات العمل والتخطيط الاستراتيجي ودعم اتخاذ القرار بالمؤسسة وما قد يرتبط من قرارات تتعلق بالتقنيات الرقمية الحديثة من تطورات كالحكومة الإلكترونية والتجارة الإلكترونية والتعليم الإلكتروني والعلاج عن بعد ... الخ – الشكل رقم (4).



الشكل رقم (4): تعاون تطبيقات العمل في التخطيط الاستراتيجي ودعم اتخاذ القرار

3-3 عمليات المعلومات الرئيسية المتصلة بأمن المعلومات

تتعدد عمليات التعامل مع المعلومات في بيئة شبكات المعلومات المؤمنة ويمكن بصفه عامة تحديد العمليات الرئيسة التالية:

1) تصنيف المعلومات (Information classification):

وهي عملية أساسية لدى بناء أي نظام يتعلق بالمعلومات وتختلف التصنيفات حسب طبيعة عمل المؤسسة مدار البحث. فمثلاً قد تصنف المعلومات إلى معلومات "متاحة" و"موثقة" و"سرية" و"سرية للغاية". أو قد تكون المعلومات مصنفة لتكون "متاح الوصول إليها" وأخرى "محظور الوصول إليها" وهكذا .

2) التوثيق (Documentation):

تتطلب عمليات المعلومات أساساً اتباع نظام توثيق مكتوب ومصدق عليه من الجهة الإدارية العليا للمؤسسة لتوثيق تصميم وبناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها.

وبشكل رئيسي فإن التوثيق لازم وضروري لنظام تعريف الهوية والتصريح للمستخدمين وتصنيف المعلومات والأنظمة التطبيقية ومصادر المعلومات. وتحت إطار الأمن فان التوثيق يتطلب أن تكون "السياسة الأمنية" موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة وفعالة ويتم تحديثها باستمرار. إضافة إلى تحديد خطط التعامل مع المخاطر والحوادث والجهات المسؤولة ومسؤولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر.

3) المهام والواجبات الإدارية والشخصية (Administration and Personnel Responsibilities):

إن الخطوة الأولى في تحديد الهيكل التنظيمي المساند لأمن المعلومات تبدأ في الأساس من حسن اختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية على أن يكون كل فرد مدركاً أن التأهيل العملي يتطلب تدريباً متواصلاً ولا يقف عند حدود المعرفة والخبرة وقت التعيين. بشكل رئيسي فإن المهام الإدارية أو التنظيمية للهيكل التنظيمي المساند تتكون من خمسة عناصر أو مجموعات رئيسة هي: تحليل المخاطر بوضع "السياسة الأمنية" محل التنفيذ – وضع خطط التأمين والحماية – تصميم البناء التقني الأمني – تشغيل الأجهزة والمعدات والوسائل – وأخيراً تنفيذ الخطط والسياسات الأمنية التي تشمل عمل النسخ الاحتياطية باستمرار ووجود مركز للطوارئ.

ومن المهم إدراك أن نجاح الواجبات الإدارية أو الجماعية للمؤسسة يتوقف على إدراك كافة المعنيين في الإدارة بمهامهم التقنية والإدارية والمالية واستراتيجية وخطة وواجبات الأمن والتزام المؤسسة باعتبار مسائل الأمن واحداً من الموضوعات التي يدركها الكافة ويتمكن الكل من التعامل مع ما يخص واجباتهم من بين عناصر الأمن.

وعلى المستوى الشخصي أو مستوى المستخدمين فإن على المؤسسة أن تضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن بل المطلوب بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات استخدام التقنية وبين الإجراءات المتطلبة من الكل لدى ملاحظة أي خطأ أو تعطل أو خلل. وعلى المؤسسة أن تحدد للمستخدمين ما يتعين عليهم القيام به والأهم ما يحظر عليهم القيام به في معرض استخدامهم للوسائل التقنية المختلفة.

4) وسائل التعريف والتحقق من المستخدمين وحدود صلاحيات الاستخدام (Identification and Authorization):

يتم تقييد الدخول إلى أنظمة الحاسب وقواعد البيانات والمواقع المعلوماتية بصفة عامة من خلال استخدام العديد من وسائل التعرف على شخصية المستخدم وتحديد صلاحيات الاستخدام وهو ما يعرف بأنظمة التعريف والتخويل (Identification and Authorization systems). والتعريف بالهوية مسألة تتكون من خطوتين: الأولى وسيلة التعرف على شخصية المستخدم – والثانية قبول وسيلة التعريف أو ما يسمى التوثق من صحة الهوية المقدمة.

ووسائل التعريف تختلف تبعاً للتقنية المستخدمة وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات في قطاعات استخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية. وبشكل عام فإن هذه الوسائل تتوزع إلى ثلاثة أنواع:

أ) شيء ما "يملكه الشخص" مثل البطاقة البلاستيكية أو غير ذلك.

ب) شيء ما "يعرفه الشخص دون غيره" مثل كلمات المرور أو الرمز أو الرقم الشخصي أو غير ذلك.

ج) شيء ما "يرتبط بذات الشخص أو موجود فيه" مثل بصمة الإصبع أو بصمة العين والصوت والوجه وغيرها.

وتعد وسائل التعريف والتوثيق الأقوى تلك الوسائل التي تجمع بين هذه الوسائل جميعاً على نحو لا يؤثر على سهولة التعريف وفعاليته في ذات الوقت.

وأياً كانت وسيلة التعريف التي سيستتبعها توثق أو تحقق من قبل النظام authentication فإنها بذاتها وبما سيترتب على استخدامها تخضع لنظام أمن وإرشادات أمنية يتعين مراعاتها. فكلمات المرور على سبيل المثال وهي الأكثر شيوعاً وسهولة من غيرها من النظم تتطلب أن تخضع لسياسة مدروسة من حيث طولها ومكوناتها والابتعاد عن تلك الكلمات التي يسهل تخمينها أو تحريها وكذلك خضوع الاستخدام لقواعد عدم الاطلاع وعدم الإفشاء والحفاظ عليها.

ومتى ما استخدمت وسائل تعريف ملائمة لإتاحة الوصول للنظام ومتى ما تحققت عملية التوثق والمطابقة والتأكد من صحة التعريف (الهوية) فإن المرحلة التي تلي ذلك هي تحديد نطاق الاستخدام Authorization وهو ما يعرف بالتخويل أو التصريح باستخدام قطاع ما من المعلومات في النظام. وهذه المسألة تتصل بالتحكم بالدخول أو التحكم بالوصول إلى المعلومات أو أجزاء النظام (Access Control system).

5) سجل الأداء (Logging):

تحتوي مختلف أنواع الحاسبات على نوع من السجلات أو التقارير التي تكشف استخدامات الحاسب وبرمجياته والنفاذ إليه وهي ما يعرف بسجلات الأداء أو سجلات النفاذ إلى النظام. وتتخذ سجلات الأداء أهمية استثنائية في حال تعدد المستخدمين وتحديداً في حالة شبكات الحاسب التي يستخدم مكوناتها أكثر من شخص وفي هذه الحالة تحديداً – أي شبكات المستخدمين – فإن هناك أكثر من نوع من أنواع سجلات الأداء وتوثيق الاستخدامات كما أن سجلات الأداء تتباين من حيث نوعها وطبيعتها وغرضها. فهناك سجلات الأداء التاريخية والسجلات المؤقتة وسجلات التبادل وسجلات النظام وسجلات الأمن وسجلات قواعد البيانات والتطبيقات وسجلات الصيانة أو ما يعرف بسجلات "الأمور التقنية" وغيرها.

وبشكل عام فإن سجلات الأداء منوط بها أن تحدد شخصية المستخدم ووقت الاستخدام ومكانه وطبيعة الاستخدام (محتواه) وأية معلومات إضافية أخرى تبعاً للنشاط ذاته.

6) عمليات حفظ النسخ الاحتياطية (Back-up):

تتعلق عمليات الحفظ بعمل نسخة احتياطية من ما تحتويه الذاكرة الخارجية للحاسبات الخادمة من معلومات وتقارير وبرمجيات على أجيال من وسائط التخزين الاحتياطية سواء داخل النظام أو خارجه (جيل احتياطي "الابن" – "الأب" – "الجد"). وتخضع عمليات الحفظ لقواعد يتعين أن تكون محددة سلفاً وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية.

ويمثل (وقت الحفظ وحماية النسخ الاحتياطية ونظام الترقيم والتبويب وآلية الاسترجاع والاستخدام ومكان الحفظ وأمنه وتشفير النسخ التي تحتوي معلومات خاصة وسرية) مسائل رئيسة يتعين اتخاذ معايير واضحة ومحددة بشأنها.

7) وسائل التأمين التقنية الفنية ونظام منع الاختراق:

تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة شبكات المعلومات كما تتعدد أغراضها ونطاقات الاستخدام. وقد تناولنا فيما تقدم مسائل التعريف والتوثيق وتحديداً كلمات المرور ووسائل التعريف الأخرى. وتتخذ وسائل التأمين والحماية مثل الجدران النارية (Firewalls) وإضافة لخوارزميات التشفير (cryptography) وكذلك نظم التحكم في الدخول ونظم منع وكشف

الاختراقات الأمنية Intrusion Detection Systems (IDS) وIntrusion Prevention Systems (IPS) – وأنظمة وبرمجيات مقاومة الفيروسات أهمية متزايدة. لكنها لا تمثل جميعها وسائل الأمن المستخدمة بل هي إضافة لوسائل التعريف والتوثيق السابق الإشارة إليها التي تمثل مع التشفير أهم وسائل الأمن التقنية في الوقت الحاضر.

8) نظام التعامل مع الحوادث (Incident Handling System):

بغض النظر عن حجم وسائل الأمن التقنية المستخدمة ومعايير الأمن وإجراءاته المتبعة فإنه يلزم توفير نظام متكامل للتعامل مع المخاطر والحوادث والاعتداءات. ويعدو متطلباً رئيسياً بالنسبة لمؤسسات الأعمال كما في حالة البنوك والمؤسسات المالية.

وأول ما يتعين إدراكه في هذا الصدد أن التعامل مع الحوادث عملية وليست مجرد مشروع أو خطوة واحدة بمعنى أنها عملية متكاملة تتصل بأداء متواصل متدرج خاضع لقواعد محددة سلفاً ومتبعة بدقة وانضباط. ومتى ما تم التعامل مع الحوادث على أنها مجرد "حالة" تنشأ عند "أي حادث" كنا أمام حالة قصور تمثل بذاتها أحد عناصر الضعف في نظام الأمن.

وتختلف مكونات ومراحل وخطوات نظام التعامل مع الحوادث من مؤسسة إلى أخرى تبعاً لعوامل عديدة تتعلق بطبيعة الأخطار التي أظهرتها عملية تحليل المخاطر وما أظهرته استراتيجية الأمن الموضوعة في المؤسسة وتبعاً للنظام محل الحماية وما إذا كنا نتحدث عن شبكات معلومات مغلقة على فروع مؤسسة أم مفتوحة أو قواعد بيانات أو شبكات أو مزيج منها – وما إذا كنا نتحدث عن نظام خدمة "خاص" أم عن خدمات للعامة عبر الشبكات الخاصة أو عبر الإنترنت. وتبعاً لوظيفة التطبيق محل الحماية إذ تتباين خطوات ومحتوى وعناصر خطط التعامل مع الحوادث لدى البنوك مثلاً عنها لدى المواقع المعلوماتية.

ومع ذلك وبوجه عام فإن نظام التعامل مع الحوادث يتكون عادة من ستة مراحل (خطوة فخطوة) هي: الإعداد المسبق – التحري – الملاحظة – الاحتواء والاستئصال – التعافي والعودة للوضع الطبيعي – والمتابعة.

وفي إطار بيئة شبكات المعلومات المؤمنة يمكن تحديد العوامل الحاكمة التالية:

أ) هناك زيادة رهيبة في استخدام وفعالية قيمة شبكات المعلومات نتيجة للتطور التقني في قدرات الحاسبات الآلية وخدمات شبكات الحاسبات والاتصالات والبيانات والمعلومات التي تخزن وتعالج وتسترجع وترسل بواسطتها متضمنة البرامج والتطبيقات وأساليب العمل.

ب) الطابع العالمي لنظم وتطبيقات شبكات المعلومات وانتشارها على كافة المستويات المحلية والقومية والدولية.

ج) نتيجة لزيادة دور نظم وتطبيقات شبكات المعلومات المتزايد الأهمية والاعتماد المتنامي عليها في الاقتصاد والتجارة والإدارة والتعلم أي في كافة أوجه الحياة الاجتماعية والثقافية والسياسية – زادت المخاطر والاختراقات الأمنية وقد أدى ذلك إلى بذل جهود خاصة لضمان الثقة والمصداقية لهذه النظم والتطبيقات من حيث أمنها وشفافيتها.

وحيث إن للبيانات والمعلومات المتوافرة في نظم وتطبيقات المعلومات الإلكترونية مزايا إضافية تجعلها مختلفة ومتميزة عن النظم الورقية أو الوثائقية التقليدية فإنه يحتم ذلك ضرورة توافر ما يلي:

أ) طرق ملائمة لزيادة الوعي بالمخاطر المحيطة بنظم وتطبيقات المعلومات.

ب) وسائل تقنية فنية للتأمين والحماية من المخاطر المتوقع حدوثها توفرها كل مؤسسة بطريقتها الخاصة وفي حدود متطلبات حماية شبكات المعلومات الخاصة بها والبيانات ومصادر المعلومات التي تم تحديدها وبحدود إمكاناتها المادية (الأفراد والأماكن الطبيعية للأجهزة والشبكات) والميزانية المخصصة للحماية. فلا تكون وسائل التأمين التقنية ضعيفة لا تكفل الحماية وبالمقابل لا تكون مغالاً فيها إلى حد تكون شبكة المعلومات عبء على المؤسسة وقد تؤثر على عنصر الأداء في النظام محل الحماية.

ج) إجراءات ومعايير وأساليب مقننة "سياسة أمنية" مكتوبة ومصدق عليها لحماية أمن شبكات المعلومات ونظمها وتطبيقاتها.

د) إجراءات مناسبة تجرم المساس بسرية وخصوصية وتوافر البيانات ومصادر المعلومات لمستخدميها.

هـ) مواصفات قياسية عالمية وإجراءات تعكس المبادئ التي تخص أمن شبكات المعلومات.

وعلى هذا الأساس فإن تعزيز الثقة والتأمين في استعمال تكنولوجيا شبكات المعلومات سوف يعزز إطار الطمأنينة الذي يشمل أمن المعلومات وأمن الشبكات وحماية الخصوصية والسرية وحماية المستخدم مما يعتبر شرطاً مسبقاً لبناء الثقة في استخدام تلك التكنولوجيا تمهيداً لإنشاء مشروعات الحكومة الإلكترونية والأعمال الإلكترونية التي تنمي مجتمع المعلومات.

يتضمن هذا الإطار عدة محاور ترتبط بالتوسع في استخدامات نظم وتطبيقات وخدمات المعلومات التي تتاح على شبكات المعلومات والتي صارت تتسم بالاعتمادية وقابليتها للتعرض للضرر والخطر وحاجتها لاكتساب الثقة في التعامل معها من قبل المستخدمين.

يمثل أمن شبكات المعلومات وتطبيقاتها وخدماتها حماية البيانات وسريتها وسلامتها وتوافرها في مواجهة التهديدات الأمنية والمخاطر والاعتبارات العامة التي تشكل معالم شبكات المعلومات من أساليب العمل والأفراد والتكنولوجيا والثقافة المتاحة ومتطلبات التأمين الطبيعي والمنطقي والتقني التي تحدد عمليات التحقق من معايير التأمين المستهدفة (التعريف والاعتماد والإدارة والمراجعة).

يشمل التأمين والحماية أيضاً تفهم الاستخدام الأمن للشبكات والتطبيقات ومحاسبة إدارة التأمين وتنفيذ أدوات ومخرجات النظم المؤمنة واعتبارات وأبعاد أمن المعلومات ومعايير الأمن من حيث الغرض العام والمجال والتعاريف والأهداف والمبادئ الخاصة بها. وتنفيذ نظم أمن شبكات المعلومات مرتبط بتطوير "السياسة الأمنية" التي تشمل زيادة الوعي الأمني والتعليم والتدريب المصاحب لتطوير النظام وتبادل المعلومات الأمنية والتعاون في كافة المجالات الأمنية لشبكات المعلومات وتطبيقاتها وخدماتها.

4-3 التوسع في استخدامات تطبيقات وخدمات شبكات المعلومات

تقبل المجتمع المعاصر أهمية تكنولوجيا الحاسبات والاتصالات اقتصادياً واجتماعياً وسياسياً. وتعتبر هذه التكنولوجيات المتقدمة جوهرية وأساسية لا من أجلها فحسب ولكن أيضاً بما تمثله كبنية أساسية لكل الأنشطة والمكونات الأخرى التي ترتبط بالمنتجات والخدمات النابعة منها.

وقد شهد المجتمع المعاصر كثيراً من التطورات التي منها:

أ) انتشار الحاسبات الآلية وتشعبها وانتشارها في كل أوجه حياة المجتمع المعاصر.

ب) تلاحم وتشابك تكنولوجيات الحاسبات والمعلومات مع الاتصالات.

ج) تواصل أعظم لتكنولوجيا الحاسبات والاتصالات والتشغيل المتداخل لنظمها وتطبيقاتها.

د) زيادة في لا مركزية وظائف الحاسبات والاتصالات.

هـ) نمو استخدام الحاسبات إلى المدى الذي يعتبر كل فرد في المجتمع إما مستخدم فعلي أو مستفيد أو مستخدم محتمل لشبكات المعلومات.

وتقدم استخدامات وتطبيقات وخدمات شبكات المعلومات مدى واسع وممتد من الإمكانيات في الوصول الأعظم للموارد والخبرة والتعلم والمشاركة في الحياة المدنية والثقافية للمواطن العادي ويتجه العالم المعاصر بخطى حثيثة ومتأنية نحو مجتمع المعلومات الذي يتسم بأنه مجتمع لا حدود له غير متأثر بالمسافة أو الوقت. كما تعتبر اقتصاديات وسياسات ومجتمعات اليوم مبنية أقل على البنية الأساسية الجغرافية والطبيعية عما كانت عليه في الماضي وصارت حالياً تعتمد بزيادة مطردة على البنية الأساسية لنظم وتطبيقات المعلومات في البيئة الرقمية التي أصبحت تفيد الحكومات والمنظمات والمؤسسات والأفراد على حد سواء. وصارت هذه النظم والتطبيقات المعلوماتية تمثل جزءاً مكملاً وأساسياً لأنشطة الشؤون المالية والصناعة والإدارة والتجارة وكافة تطبيقات الأعمال على المستوى القومي والدولي كما أصبحت تستخدم بتوسع.

وعلى هذا الأساس صارت هذه النظم والتطبيقات الرقمية تستخدم في أداء كثير من الخدمات والأنشطة الحكومية من خلال الحكومات الإلكترونية (E-Government) والتعليم الإلكتروني (E-Learning) والتجارة الإلكترونية ... الخ.

وتنقسم نظم وتطبيقات وشبكات المعلومات الحديثة بالعوامل أو الخصائص الثلاثة التالية:

1) الاعتمادية (Dependency)

يتأثر كل شخص ومؤسسة مباشرة بتطبيقات وشبكات المعلومات ويصبح معتمداً على وظائفها المختلفة التي تلائم استخداماته المتنوعة. على سبيل المثال لا الحصر إن استخدام شبكات المعلومات المتزايد قد ساهم في تعميق التغييرات الأساسية التي تحدث في ميكنة الإجراءات التنظيمية الداخلية في أي مؤسسة مما أدى إلى تبديل وتغيير الطريقة التي تتفاعل بها مع جمهور المتعاملين معها. أما في حالة تعطل نظام معلومات يصبح من المستحيل على المؤسسة الاستمرار في الإجراءات الحالية بدون هذه النظم كما يصبح من الصعب العودة مرة أخرى إلى الطرق والإجراءات القديمة التقليدية. وأصبح غير كاف تواجد سجلات ورقية أو الاعتماد فقط على مهارات العاملين اليدوية أو حتى توافر عدد كبير من القوى العاملة لكي

يسمح للمؤسسة المعنية من الاستمرار في أداء وظائفها بمعدلات إنتاجية عالية وجودة أحسن بنفس المدى الذي قد تعمل به مع تواجد نظم وتطبيقات المعلومات الرقمية الحديثة حتى تتمكن من مواجهة المنافسين في عالم مفتوح يتسم بالعولمة. فعلى سبيل المثال أيضاً في الإمكان ملاحظة تأثير تعطل نظام المعلومات الإلكتروني على الأداء وفعالية الخدمات وانتظام حركة المعاملات على شركات خطوط الطيران والبنوك وغيرها من المؤسسات التي لا تستطيع الاستغناء على التطبيقات والخدمات والنظم الإلكترونية المتقدمة. مما سبق يمكن استنباط مدى نمو الاعتماد على شبكات وخدمات المعلومات الرقمية بمعدلات كبيرة غير مسبوقة. وقد صاحب هذا الاعتماد المتنامي بزوغ الحاجة الملحة لتوفير الثقة والشفافية لهذه الشبكات المستمرة في التطوير والتواجد في المستقبل.

2) قابلية تعرض الشبكات والتطبيقات للضرر (Vulnerability)

كما أن استخدام تطبيقات وخدمات وشبكات المعلومات الرقمية قد زاد بطريقة هائلة مما أدى إلى بزوغ فوائد ومزايا كبيرة عادت بالنفع على المنظمات والأفراد المستخدمين لها إلا أنها أدت إلى تواجد فجوة كبيرة بين الحاجة لحماية هذه الشبكات والتطبيقات ودرجة التأمين المتوفرة والموظفة لها بالفعل. فقد أصبح مجتمع المعلومات الحديث المتضمن الأعمال والخدمات العامة والأفراد معتمداً بصفة كبيرة على تكنولوجيات المعلومات والاتصالات الغير موثوق منها لحد كبير. وتعتبر كل استخدامات شبكات المعلومات وتطبيقاتها الرقمية المحملة على شبكات الحاسبات معرضة للهجمات الضارة أو للتعطل فيما يتصل بإفشاء سرية معلوماتها أو عدم حفظ خصوصية بيانات الهيئات والمتعاملين معها أو التأخر في توافرها في الوقت الملائم لمن يحتاج إليها بسرعة. أي توجد مخاطر جمة نتيجة الوصول غير المصرح به والاستخدام غير الملائم وغير المخصص أو تعطل النظم ذاتها بأسباب عرضية جانبية. مع العلم بأن كثير من شبكات وتطبيقات المعلومات سواء كانت عامة أو خاصة (كتلك المستخدمة في الأغراض الحربية والأمنية والبنوك والمستشفيات وغيرها) تمثل أرضية خصبة للإرهاب المعلوماتي المتنامي اليوم.

وفي إطار التطورات المتلاحقة المتمثلة في: تزايد الحاسبات الآلية وزيادة قدرة وقوة الحاسبات والتواصلية المتداخلة واللامركزية ونمو الشبكات وعدد مستخدميها المتزايد وتعزيز نفعية شبكات المعلومات مع زيادة قابليتها للتعرض للضرر والخطر – كل ذلك جعل من الصعوبة تحديد موقع المشكلات التي يتعرض لها النظام وتحديد أسبابها للعمل على تصحيحها بطريقة متوازنة مع وظائف ومتطلبات النظام الأخرى حتى يمكن منع تكرار حدوثها أو ارتدادها.

وكما تصبح شبكات المعلومات وتطبيقاتها لا مركزية وتنمو بطريقة متناهية فمن المهم مراعاة اعتماد مكوناتها وملحقاتها وتداخلها معاً الموردة والمباعة من قبل موردين وبائعين ومن مصادر مختلفة ومتعددة – إضافة لما تقدم فإن نمو تواصلية شبكات المعلومات واستخدامات الشبكات الخارجية أدى إلى مضاعفة أوجه الأعطال والقصور الممكنة.

ومن الملاحظ أيضاً أن تطور الأوجه القانونية والتشريعية لتأمين نظم المعلومات قد لا تتم دائماً بخطى متوازية مع التقدم التكنولوجي ففي بعض الأحيان يعتبر ذلك غير كافي على المستوى القومي إلى جانب من تواجد عدد من القوانين غير المطورة حتى الآن على المستوى الدولي. إن تناسق وانسجام القوانين والتشريعات المرتبطة بشبكات المعلومات يعتبر من الأهداف الهامة التي يجب مراعاتها والعمل على سنها بصفة مستمرة.

3) بناء الثقة (Building Confidence)

يجب أن يثق مستخدمي شبكات المعلومات وتطبيقاتها في البيئة الرقمية للمؤسسة المعنية في أنها تعمل وفقاً لما هو مقرر لها بدون أي أعطال أو أخطاء أو اختراقات أو مشكلات أخرى غير متوقعة. وعلى ذلك فإن الوصول لتأمين الشبكات وإعداد توجيهات ومعايير أمن حاكمة قد تنبع نتيجة لمتطلبات المستخدمين ذاتهم وإن فقد الثقة في النظام والتطبيق القائم عليه قد ينبع من سوء الاستخدام أو من عدم تلبية التوقعات أو من عدم التأكد من الذي قد يتم الوصول إليه.

وعلى ذلك تحتاج شبكات المعلومات الرقمية إلى توفير وبناء إجراءات وقواعد مقبولة لكل الأطراف المتعاملة معها حتى تقدم نتائج ملموسة تزيد من الثقة والمصداقية في هذه الشبكات.

ويمثل أمن المعلومات وشبكاتها والقدرة على تطويرها وتشغيلها واستخدامها قضية عالمية لأن شبكات المعلومات غالباً ما تتعدى الحدود القومية أو الوطنية المحدودة. فهي مشكلة تتطلب تعاوناً دولياً مكثفاً للتغلب عليها. وفي الواقع بافتراض تجاهل شبكات المعلومات للحدود الجغرافية والتشريعية فإنها تعتبر من المعاهدات والاتفاقات الأحسن قبولاً ودعماً على المستوى العالمي.

وبالرجوع إلى الخبرات المكتسبة في قطاعات مثل النقل الجوي أو البحري فالتكنولوجيات المتقدمة الجديدة التي قد تتضمن أخطاراً وأضرار معينة تجابه تحديات ثلاثة تتمثل في:

أ) تطوير التكنولوجيا وتطبيقها.

ب) تجنب ومجابهة تعطل التكنولوجيا.

ج) كسب المساندة العامة والموافقة على استخدام التكنولوجيا.

وفي هذا الإطار يمكن على سبيل المثال اعتبار أن صناعة الطيران ناجحة في تنفيذ أساليب ومتطلبات السلامة الملاحية الجوية حيث إنها تسهل الأداء السلس الآمن للنقل الجوي وتبعث على إضفاء الثقة لدى الجمهور المتعامل معها. وبصفة مشابهة للمثال السابق تستخدم هيئة تأمين الملاحة البحرية العالمية نظم اعتماد وسلامة لبناء السفن وتشغيلها بنجاح.

ومن هذا المنطلق يجب أن يكون الهدف من صناعة المعلومات والاتصالات شبيهاً للمثالين السابقين ويرتبط بتجنب أي قصور أو تعطل يرتبط بهذه الصناعة وتجنبه التهديدات الأمنية والأعطال والكوارث وتمنع التطفل والوصول غير المصرح به للبيانات ومصادر المعلومات وذلك بقدر الإمكان وبدرجة كبيرة من الفعالية والكفاءة والموثوقية.

5-3 أمن شبكات المعلومات

يمثل أمن المعلومات وشبكاتها في البيئة الرقمية حماية البيانات ومصادر المعلومات من كل خطر يتهددها فيما يتعلق بتوافرها وإضفاء الثقة فيها وتأكيد سلامتها. ويعبر توافر (Availability) المعلومات عن خاصية من خصائص شبكات المعلومات الممكن الوصول إليها واستخدامها على أساس فوري في إطار نمط محدد ومطلوب. كما يصبح في الإمكان الوصول إلى النظام عندما يطلب بطريقة معتمدة ووفقاً لمواصفات ملائمة لهذا للنظام. وتعتبر السرية (Confidentiality) خاصية ترتبط بعدم تغيير البيانات والمعلومات أو فقدها أو إهدارها وإتاحتها فقط لأشخاص وكيانات معتمدة ومصرح لها فقط باستخدامها وتتضمن السرية العمليات التي تستخدم أساليب التشفير والحجب لمحتويات البيانات والمعلومات أو السماح بها في أوقات وفي طرق معتمدة. أما التكامل والسلامة (Integrity) فهي خاصية البيانات

والمعلومات الدقيقة والكاملة التي تحفظ بدرجة كبيرة من الدقة والاكتمال. وتتنوع الأولوية والأهمية النسبية لتوافر المعلومات وسريتها وسلامتها طبقاً لنظام المعلومات المتاح.

والجزء التالي يوضح معالم أمن نظام المعلومات وإطار التأمين ومكوناته والتهديدات المختلفة التي يتعرض لها نظام المعلومات.

1-5-3 سياسة أمن شبكات المعلومات

الهدف من أي سياسة أمن تصمم لنظام المعلومات هو حماية المعلومات بتخفيض احتمالية تعرضها للمخاطر التي قد تؤثر على توافرها وسريتها وسلامتها بمستوى مقبول ومحدد. وتتضمن سياسة أمن شبكات المعلومات الجيدة توافر عنصرين رئيسيين يتمثلان في تحليل المخاطرة وإدارة المخاطرة.

في مرحلة "تحليل المخاطرة" يراعي قيمة ما تحتويه وسائل التخزين من قواعد البيانات والمعلومات لكل النظم المتوافرة في المؤسسة. ويمثل كل نظام من نظم المعلومات قيمة سرية خاصة للمؤسسة وبالدرجة التي يتم تقديرها عند تعرض شبكة معلومات المؤسسة للمخاطرة. وتتطلب كثير من الأساليب المتبعة في تحليل المخاطرة خبرة فنية عالية في مجال تكنولوجيا المعلومات وأساليب رقابة متوافقة وتوافر تكرار أحداث الخطر المحتملة التي قد تكون خارج نطاق عمليات المراجعة التقليدية المتبعة. ويتمثل الهدف من تحليل المخاطرة بناء خبرات وموارد مكتسبة بمرور الوقت.

أما "إدارة المخاطرة" فهي من جهة أخرى تتضمن أساليب الرقابة ومقاييس التأمين التي تقلل تعرض المؤسسة لمستوى مقبول ومسموح به من المخاطرة لكي يكون أمن نظام المعلومات فعالاً وكفء ويعكس الإحساس المشترك يجب أن تعمل إدارة المخاطرة مع إطار التأمين حيث تكمل مقاييس أمن المعلومات من خلال القوى العاملة المهنية في تكنولوجيا المعلومات والاتصالات والإدارة إلى جانب مقاييس التأمين الطبيعية والمعدات والبرامج وأساليب العمل والشبكات كما في الشكل رقم (5).

الشكل رقم (5): طبقات أمن المعلومات المتممة بعضها ببعض

يتضح من الشكل رقم (5) أن إدارة أمن المعلومات هي قضية إدارية في المقام الأول حيث يتم التوصل فيها إلى توازن بين قيمة المعلومات للمؤسسة من جهة وتكلفة الأفراد والوسائل التقنية والإدارية من جهة أخرى. وتضع مقاييس التأمين الحاجة في التوصل إلى أقل تكلفة من التعرض للمخاطر أو الأضرار التي قد تسبب فقد سرية المعلومات وتحد من سلامتها وتوافرها.

2-5-3 إدارة المخاطر

يمثل أمن المعلومات أحد عناصر البنية الأساسية التي يجب أن تتاح لأمن نظام المعلومات. وعلى ذلك يجب ألا يفحص من فراغ – كما يجب وجود إطار "سياسة أمنية" يختص بكل أوجه التأمين الطبيعي وأمن الأفراد وأمن المعلومات بالإضافة إلى وجود أدوار ومسؤوليات واضحة للمستخدمين وأفراد الأمن وأعضاء لجنة إدارة شبكات المعلومات.

ويشتمل برنامج أمن المعلومات على كل الأوجه الحساسة لمعلومات المؤسسة التي تضمن سريتها وسلامتها وتوافرها. كما يجب أن يحدد أيضاً برنامج أمن المعلومات برنامجاً للتوعية يوضح سبل تنفيذ الأمن ويذكر كل العاملين بالمؤسسة المعنية بالمخاطر والهجمات الممكنة ومسؤولياتهم في حفظ معلومات المؤسسة. وإلى جانب الإشارة للشكل رقم (5) السابق يمثل أمن المعلومات مجموعة من الوسائل المختلفة على كافة المستويات الطبيعية وتلك المتعلقة بالأفراد والوسائل الإدارية لمستويات نظام المعلومات المتكاملة معاً.

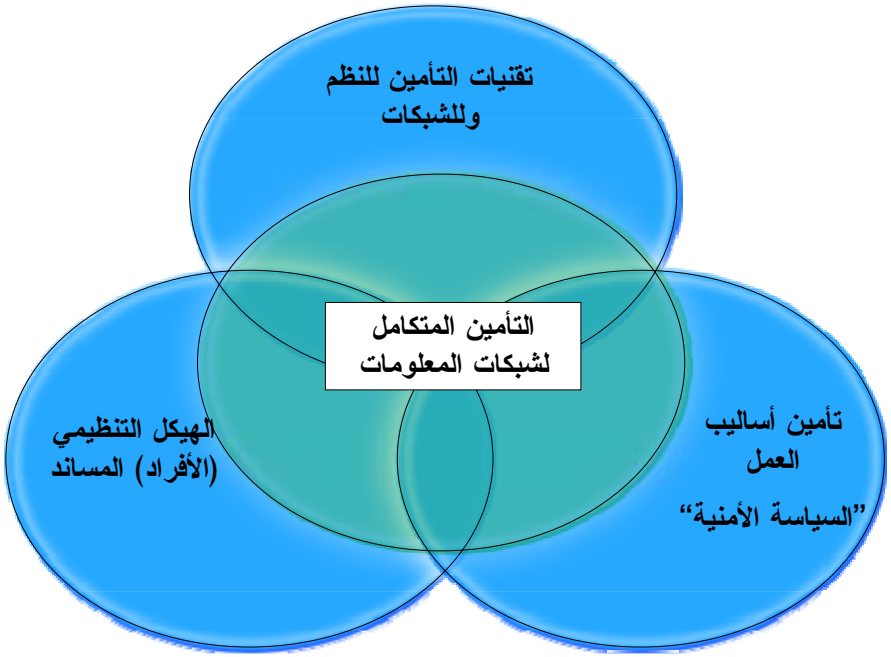
ويمثل أمن المعلومات مقاييس الرقابة الإدارية الجيدة – وعند وجود أي قصور في أحد المستويات يمكن أن يهدد كل المستويات الأخرى. على سبيل المثال إذا كانت سياسات أمن الأفراد غير متوافرة وبالتالي غير منفذة يصبح أمن المعلومات باهظ التكلفة أو على الأقل غير ممكن مساندته. ومن جهة أخرى يجب أن تؤكد الوسائل المخططة لكل المستويات حداً أدنى من حماية المعلومات على أن تكون مخاطرة التأمين محسوبة ومقبولة من قبل الإدارة المعنية.

وتوجد بعض الأوضاع المعينة التي يمكن لمقاييس التأمين في أحد مستويات نظام المعلومات أن تعوض ضعف التأمين في مستويات أخرى. على سبيل المثال تضيف عملية التشفير (Encryption) تأمين وحماية للبيانات (أثناء تداولها عبر الشبكات وأثناء تخزينها) حتى في الحالات التي تكون فيها مقاييس التأمين الطبيعية أو تلك المتعلقة بالأفراد أو الوسائل الإدارية ضعيفة – وبالتالي يصبح التشفير أحد معالم الدفاع الأولى والأخيرة للمساعدة في حماية أي أخطار تتعلق بسرية المعلومات.

وعند التخطيط لأمن المعلومات يجب أن يكون هناك توازن بين قيمة المعلومات الخاصة بالإدارة العليا للمؤسسة (المستخدمة في اتخاذ القرارات) وبين الحجم النسبي لأنواع المعلومات الأخرى في مواجهة تكاليف تقنيات التأمين العالية لمعلومات الإدارة العليا والمتوسطة لباقي المعلومات. والهدف من تحقيق التوازن هو خفض القيمة الإجمالية لتقنيات التأمين.

في كثير من المؤسسات التي يؤثر تعرض بياناتها ومصادر معلوماتها للمخاطر بالسلب على أرباحها أو سمعتها أو حتى بقاءها فإنه يجب توافر تقنيات تأمين عالية التكاليف ومتطلبات أمن صارمة لمعالجة وتخزين واسترجاع المعلومات في قواعد البيانات وتداولها بطريقة تحمي سريتها وسلامتها كما يتضح من الشكل رقم (6).

6



الشكل رقم (6): تكامل تقنيات التأمين و"السياسة الأمنية"

إدارة المخاطر بشكل عام هي عملية قياس وتقييم للمخاطر وتطوير سياسات لإدارتها – وتتضمن هذه السياسات تدني المخاطر قدر الإمكان وتقليل آثارها السلبية وقبول بعض أو كل تبعاتها.

في حالة إدارة المخاطر يتم اتباع عملية "إعطاء الأولويات" بحيث إن المخاطر التي تسبب الخسائر الكبيرة واحتمالية حدوث عالية تعالج أولاً بينما المخاطر ذات الخسائر الأقل واحتمالية حدوث أقل تعالج فيما بعد.

عملياً قد تكون هذه الخطوة صعبة جداً كما أن الموازنة ما بين المخاطر ذات الاحتمالية العالية والخسائر القليلة مقابل المخاطر ذات الاحتمالية القليلة والخسائر العالية قد يتم معالجتها بشكل سيء مما قد يؤثر بالسلب على أرباح أو سمعة أو حتى بقاء المؤسسة. ومن هنا يأتي أهمية الاستعانة بالمتخصصين عند إدارة المخاطر.

إدارة المخاطر غير الملموسة تعرف بأنها نوع جديد من المخاطر التي قد تكون احتمالية حدوثها 100% ولكن يتم تجاهلها من قبل المؤسسة وذلك بسبب الافتقار لمقدرة التعرف عليها. ومثال على ذلك "مخاطر المعرفة" والتي تحدث عند تطبيق معرفة ناقصة. و"مخاطر العلاقات" وتحدث عند وجود تعاون غير فعال بين المؤسسات. كذلك "مخاطر الأمن الاجتماعي" وتحدث عند كشف بعض الأفراد الذين ليس لديهم "الحس الأمني" لمعلومات قد تضر المؤسسة بقصد أو من باب التباهي بالمعرفة. إن هذه المخاطر جميعها تقلل بشكل مباشر إنتاجية العاملين في المعرفة وتقلل فعالية الإنفاق والربح والخدمة والنوعية والسمعة وقيمة المكاسب.

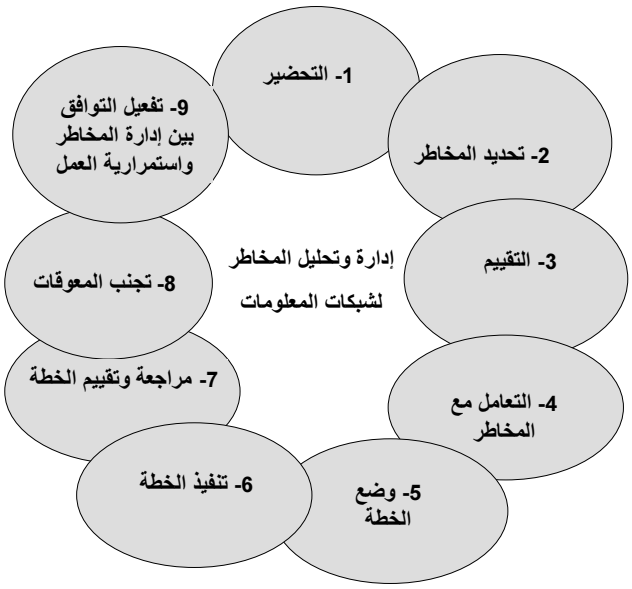
كذلك تواجه إدارة المخاطر صعوبات في تخصيص وتوزيع المصادر وهذا يوضح فكرة تكلفة الفرصة حيث إن بعض المصادر التي تنفق على إدارة المخاطر كان من الممكن أن تستغل في

نشاطات أكثر ربحاً. ومرة أخرى فإن عملية إدارة المخاطر المثالية تقلل الإنفاق في الوقت الذي تقلل فيه النتائج السلبية للمخاطر إلى أقصى حد ممكن.

1) خطوات عملية إدارة المخاطر

الشكل رقم (7) يوضح خطوات عملية إدارة المخاطر التي سيتم تناولها في هذا القسم:

[7]



الشكل رقم (7): يوضح خطوات عملية إدارة المخاطر

1) التحضير

يتضمن التخطيط للعملية رسم خريطة نطاق العمل والأساس الذي سيعتمد في تقييم المخاطر وكذلك تعريف إطار لكل عملية تشغيلية وتحضير أجندة للتحليل.

2) تحديد المخاطر

يتم في هذه المرحلة التعرف على المخاطر ذات الأهمية حيث إن المخاطر عبارة عن أحداث عند حصولها قد تؤدي إلى مشاكل – وعليه يمكن أن يبدأ التعرف على المخاطر من مصدرها أو من آثارها بحد ذاتها. عندما تحدد المصدر فإن الحوادث التي تنتج عنها قد تقود إلى المشكلة نفسها. والطرق الشائعة للتعرف على المخاطر هي:

أ) التحديد المعتمد على التأثير السلبي على الأهداف: إن لدى كل مؤسسة أهداف تساعد تكنولوجيا شبكات المعلومات على تحقيقها فأي حدث يعرض تحقيق هذه الأهداف إلى خطر سواء جزئياً أو كلياً يعتبر مخاطر.

ب) التحديد المعتمد على السيناريو: في عملية تحليل السيناريو يتم خلق سيناريوهات مختلفة قد تكون طرق بديلة لتحقيق هدف ما أو تحليل للتفاعل بين النظم الفرعية المكونة لشبكات المعلومات. لذا فإن أي حدث ينتج عنه سيناريو مختلف عن الذي تم تصوره وغير مرغوب به يعرف على أنه "خطر".

ج) التحديد المعتمد على التصنيف: وهو عبارة عن تصنيف البيانات وجميع مصادر المعلومات المحتمل تعرضها للمخاطر طبقاً لحساسيتها بالنسبة للمؤسسة.

د) مراجعة المخاطر الشائعة: في العديد من المؤسسات هناك قوائم بالمخاطر المحتملة وعلى سبيل الاسترشاد يمكن الرجوع إلى إحدى القوائم المنشورة لمخاطر تعرضت لها مؤسسات ذات نشاط قريب من نشاط المؤسسة.

3) التقييم

بعد التعرف على المخاطر المحتملة يجب أن تجرى عملية تقييم لها من حيث شدتها في إحداث الخسائر واحتمالية حدوثها. أحياناً يكون من السهل قياس هذه الكميات وأحياناً أخرى يتعذر قياسها. تكمن صعوبة تقييم المخاطر في تحديد معدل حدوثها حيث إن المعلومات الإحصائية عن الحوادث السابقة ليست دائماً متوفرة. وكذلك فإن تقييم شدة النتائج عادة ما يكون صعب في حالة الموجودات غير المادية مثل البرامج والبيانات والمعلومات.

4) التعامل مع المخاطر

بعد أن تتم عملية التعرف على المخاطر وتقييمها فإن جميع التقنيات المستخدمة للتعامل معها تقع ضمن واحدة أو أكثر من أربع مجموعات رئيسية هي:

أ) الوقاية: تعتبر أهم واعقد مراحل حياة نظام المعلومات المؤمن وأكثرها تكلفة وقد تتضمن وسائل وإجراءات معقدة مثل تحصين جميع المعدات ووجود احتياطيات كاملة من المواقع والمعدات واستخدام تقنيات الشفرة ذات درجة السرية العالية جداً في تأمين جميع البيانات والمعلومات المخزنة على أوساط التخزين والمرسلة عبر الشبكات – وقد تعني الوقاية محاولة تجنب الأنشطة التي تؤدي إلى حدوث خطر ما. ومثال على ذلك عدم شراء ملكية ما أو الدخول في عمل ما أو عدم تحقيق الاتصال بين شبكة المؤسسة والشبكات الواسعة والإنترنت لتجنب تحمل مسؤولية المخاطر إدارياً ومالياً وقانونياً. إن التجنب يبدو حلاً لجميع المخاطر ولكنه في الوقت ذاته قد يؤدي إلى الحرمان من الفوائد والأرباح التي كان من الممكن الحصول عليها من النشاط الذي تم تجنبه.

ورغم ذلك لا يمكن ضمان الوقاية التامة لنظام المعلومات ضد كافة المخاطر في ظل التطور المستمر لتكنولوجيا المعلومات والشبكات وبالتالي وسائل الاختراقات الأمنية كما أن الحاجة إلى التوسع في استخدام الشبكات لتبادل المعلومات فيما بين المؤسسات أدى إلى اعتمادية نظام تأمين معلومات المؤسسة على نظام تأمين معلومات المؤسسات المتصلة بها والمتشاركة معها.

ب) سرعة الكشف والعلاج: وتشمل طرق للتقليل من حدة الخسائر الناتجة. ومثال على ذلك شركات تطوير برمجيات التطبيقات التي تتبع منهجيات للتقليل من المخاطر وزرع البرامج الخبيثة (مثل كود برنامج حصان طروادة) وذلك عن طريق تطوير البرامج بشكل تدريجي (Structured Programming) مع اختبار كل درجة على بيانات غير حقيقية بواسطة وسائل اختبار وتفتيش محددة. وفى حالات كثيرة قد تلجأ المؤسسة إلى تطوير برامج تطبيقاتها ذاتياً وهذا يحقق أهداف كثيرة من أهمها خفض التكاليف وضمان عدم زرع اكواد برامج خبيثة مثل حصان طروادة.

ج) عودة النظام للعمل: وتعنى استخدام الوسائل التي تعود بالنظام إلى حالة التشغيل الطبيعية. وقد تعني هذه المرحلة قبول الخسائر عند حدوثها. إن هذه الطريقة تعتبر سياسة مقبولة في حالة المخاطر الصغيرة والتي تكون فيها تكلفة اقتناء وسائل التأمين التقنية ضد الخطر على مدى الزمن أكبر من إجمالي الخسائر. كل المخاطر التي لا يمكن تجنبها لارتفاع تكاليف التأمين أو لانخفاض نسبة حدوثها أو لتأثيرها المحدود يجب القبول بها.

5) وضع الخطة

تتضمن هذه الخطوة أخذ قرارات تتعلق باختيار مجموعة الطرق التي ستتعامل مع المخاطر. وكل قرار يجب أن يسجل بعد أن يتم الموافقة عليه من قبل المستوى الإداري المناسب. فعندما يتعلق الأمر بمخاطر تمس صورة المؤسسة فيجب أن يتخذ القرار من قبل الإدارة العليا أما في حالة القرارات المتعلقة بجزء من شبكة المعلومات على سبيل المثال فإن مسؤولية القرار تعود إلى مدير تكنولوجيا المعلومات. على الخطة أن تقترح وسائل تحكم أمنية تكون منطقية وقابلة للتطبيق من أجل إدارة المخاطر. وكمثال على ذلك يمكن تقليل مخاطر الفيروسات التي تتعرض لها الحاسبات من خلال استخدام برامج مضادة للفيروسات يتم تعديلها باستمرار.

6) التنفيذ

يتم في هذه الخطوة اتباع الطرق المخطط أن تستخدم في التخفيف من آثار المخاطر على مراحل بحيث يجب أولاً التغلب على المخاطر التي تؤثر على تنفيذ أهداف المؤسسة مادياً ومعنوياً – وثانياً يتم التقليل من المخاطر الأخرى طبقاً لدرجة خطورتها.

7) مراجعة وتقييم الخطة

قد تكون الخطط المبدئية لإدارة المخاطر ليست كاملة – فمن خلال الممارسة والخبرة والخسائر التي تظهر على أرض الواقع تظهر الحاجة إلى إحداث تعديلات على الخطط واستخدام المعرفة المتوفرة لاتخاذ قرارات إضافية مكملة لما تم اتخاذه من قرارات. ومن هنا يجب الاستعانة بالجهات أو الأفراد المتخصصين والموثوق فيهم في مجال تأمين شبكات المعلومات.

يجب تحديث نتائج عملية تحليل المخاطر وكذلك خطط إدارتها بشكل دوري وذلك يعود للأسباب التالية:

أ) من أجل تقييم وسائل السياسة الأمنية المستخدمة سابقاً لتحديد إذا ما زالت قابلة للتطبيق وفعالة.

ب) من أجل تقييم مستوى التغييرات المحتملة للمخاطر في بيئة العمل – فمثلاً تعتبر المخاطر المعلوماتية مثالاً جيداً على بيئة عمل سريعة التغيير.

8) تجنب المحددات (المعوقات)

إذا تم تقييم المخاطر أو ترتيبها حسب الأولوية بشكل غير مناسب فإن ذلك قد يؤدي إلى تضييع الوقت في التعامل مع المخاطر ذات الخسائر التي من غير المحتمل أن تحدث – وكذلك إضاعة الوقت الطويل في تقييم وإدارة مخاطر غير محتملة – مما قد يؤدي إلى تشتيت المصادر التي كان من الممكن أن تستغل بشكل مربح أكثر. وفي نفس الوقت فإعطاء عمليات

إدارة المخاطر أولوية عالية جداً يؤدي إلى إعاقة عمل المؤسسة في إكمال مشاريعها أو حتى الشروع فيها. لذا يفضل أن تتم إدارة المخاطر بالتوازي مع تنفيذ شبكة المعلومات وتنفيذ تطبيقات العمل. ومن المهم أيضاً الأخذ بعين الاعتبار القدرة على التمييز بين الخطورة الحقيقية والشك.

9) تفعيل التوافق بين إدارة المخاطر واستمرارية العمل

إن إدارة المخاطر ما هي إلا ممارسة لعملية اختيار سياسة أمنية ذات تكلفة فعالة من أجل التقليل من أثر تهديد معين على المؤسسة. كل المخاطر لا يمكن تجنبها أو تقليص حدتها بشكل كامل وذلك ببساطة يعود لوجود عوائق تقنية وإدارية ومالية. لذلك على المؤسسة أن تتقبل مستوى معين من الخسائر (مخاطر متبقية).

فبينما تستخدم إدارة المخاطر لتفادي الخسائر قدر الإمكان فإن التخطيط لاستمرارية العمل وجدت لتعالج نتائج ما يتبقى من مخاطر. وتكمن أهميتها في أن بعض الحوادث التي ليس من المحتمل أن تحدث قد تحدث فعلاً إن توفر الوقت الكاف لحدوثها. إن إدارة المخاطر والتخطيط لاستمرارية العمل هما عمليتين مربوطتين مع بعضهما ولا يجوز فصلهما. فعملية إدارة المخاطر توفر الكثير من المدخلات لعملية التخطيط لاستمرارية العمل مثل: (الموجودات – تقييم الأثر – التكلفة التقديرية ...الخ).

وبناءاً على ذلك فإن إدارة المخاطر تغطي مساحات واسعة مهمة لعملية التخطيط لاستمرارية العمل والتي تذهب في معالجتها للمخاطر أبعد من عملية إدارة المخاطر.

وفيما يتصل بإطار شبكات المعلومات يمكن ملاحظة تواجد مدخلاً يتضمن طبقتين لمراجعة أمن المعلومات. ويعتمد هذا المدخل على توظيف الإدراك المشترك والسليم وفي إيجاد توازن بين تكلفة التأمين المطلوبة للنظام وبين قيمة المعلومات الموجودة والمتداولة فيه.

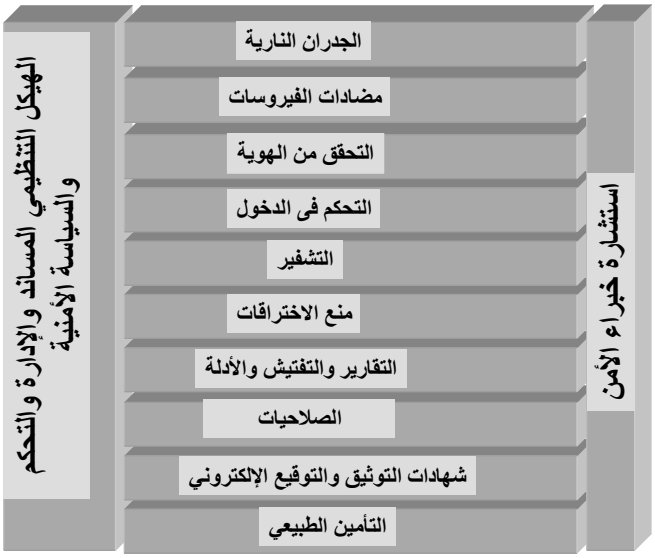
الشكل رقم (7) السابق يمثل هذا المدخل المرتبط بتحليل وإدارة المخاطرة على مستوى كل عملية تشغيلية حيث يساهم ذلك بأسلوب فعال في تنفيذ أهداف المؤسسة وتحتاج لمستوى عالي من التأمين.

3-5-3 مكونات ومحاور أمن شبكات المعلومات

تنفيذ وتشغيل نظام أمن المعلومات يمثل طريقة حياة تعتمد على أربع مكونات أساسية كل منها مهم ولا يمكن التعامل معه بصفة فردية مستقلة.

ويحدد الشكل التالي رقم (8) أهم الوسائل التقنية والسياسة الأمنية التي تحقق أمن شبكات المعلومات.

تأمين شبكات المعلومات من خلال:
الوسائل التقنية الفنية والسياسة الأمنية [8]



الشكل رقم (8): مكونات شبكة المعلومات المؤمنة بالوسائل التقنية

1) العمليات (Processes)

تعتبر العمليات لا غنى عنها لأي نظام أمن فهي جوهرية وذات طبيعة مستمرة. ويحكم أداة عمليات أمن المعلومات مجموعة من المعايير كتلك التي نصت عليها كل من الاتحاد الدولي للاتصالات (ITU) [المراجع أرقام (10 و41 و42)] والمنظمة الدولية للتوحيد القياسي (ISO) [المراجع أرقام (14 و23 و36 و37 و38)] التي تعتبر ذات قيمة كبيرة لأي نظام أمن معلومات. وتطبق العمليات بطريقة منظمة كما تراجع باستمرار في إطار الخبرة المتراكمة بغية استبعاد الأخطاء والمخاطر.

2) الأفراد (People)

يتكون الأفراد العاملين في نظام المعلومات من المستخدمين والمستفيدين والمستشارين والمتعاقدين والفنيين الذين ينجزون كل العمليات والخدمات. ويحتاج النظام إلى تواجدهم بأعداد وتخصصات ملائمة وبمهارات وخبرات مناسبة. وللأفراد دوراً رئيسياً في تأمين نظام المعلومات والشبكات بل يعتبر العنصر البشري من أهم مصادر النظام والسبب الرئيسي لنجاح أو فشل المؤسسة في تنفيذ أهدافها. فالمخاطر الأمنية مصدرها الأفراد (بقصد أو من غير قصد) ومن المهم أن يدرك الأفراد بأن المخاطر ربما تؤثر على كفاءة عملهم وعلى مستقبلهم أنفسهم.

3) التكنولوجيا (Technology)

تعتبر التكنولوجيا الخاصة بالتأمين متوافرة وجاهزة للاقتناء ويتوافر لدى الشركات منتجات ذات دورة حياة قصيرة نسبياً (حوالي 3 سنوات) قد يتم تغييرها طبقاً لما يستجد من تطورات سواء في وسائل التأمين أو في وسائل الاختراقات الأمنية.

فعلى سبيل المثال استبدلت الشركات منتجاتها من "كشف الاختراقات" (Intrusion Detection) إلى منتجات أخرى "لمنع الاختراقات" (Intrusion Prevention). كما تقوم حالياً شركة سيسكو (Cisco) باستبدال منتجاتها من الجدران النارية PIX إلى منتجات جديدة. ويعتبر سوق التكنولوجيا ذو طبيعة تنافسية حيث يتواجد فيه عدد كبير من الشركات المنتجة الكبرى والصغرى. وقد تندمج الشركات الصغرى في شركات أكبر أو قد يخسرون ويخرجون من سوق الأعمال.

4) الثقافة (Culture)

ترتبط الثقافة بتفسير بيئة الأعمال وتتعلق بأخلاقيات المؤسسة تجاه المجتمع حيث يكون لإدارة المؤسسة دوراً رئيسياً تؤديه في حفظ ثقافة المؤسسة المتوافقة مع ثقافة مجتمعها.

وتشتمل الأوجه الثقافية ذات الطبيعة الحرجة في إدارة نظام أمن المعلومات الناجح على التالي:

أ) المساندة والالتزام الكامل تجاه أمن المعلومات من قبل الإدارة العليا بالمؤسسة.

ب) الانضباط التنظيمي القوي.

ج) السياسة الموثقة والموصلة بوضوح لكل العاملين.

د) العمليات الموثقة والمساندة بواسطة المراجعات المستمرة.

هـ) توافق عمليات المراجعة المستمرة.

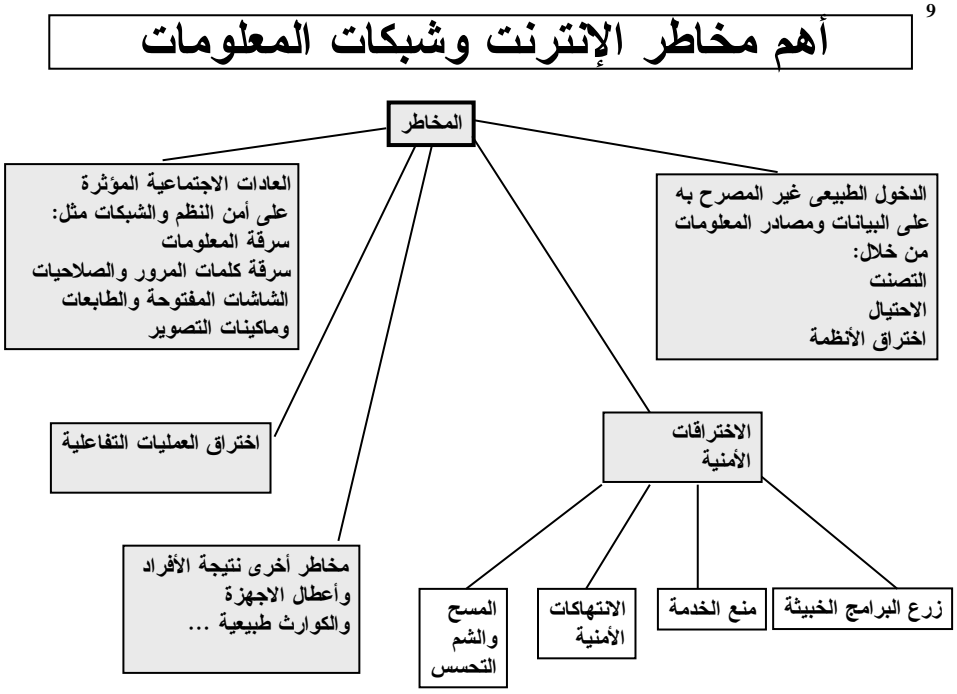
و) الاختبارات والمراجعات العادية الدورية.

6-3 تهديدات أمن شبكات المعلومات (Threats to Information Systems)

توجد كثير من التحديات تؤثر على الأداء السليم لوظائف شبكات المعلومات التي منها:

التطورات التكنولوجية المتسارعة والمشكلات الفنية المتزايدة والأحداث البيئية المتغيرة والضعف البشري وعدم ملاءمة المؤسسات الاجتماعية والسياسية والاقتصادية الراهنة للمتغيرات المتلاحقة ... الخ. والشكل رقم (9) يتضمن أهم المخاطر التي تتعرض لها شبكات المعلومات.

[9]

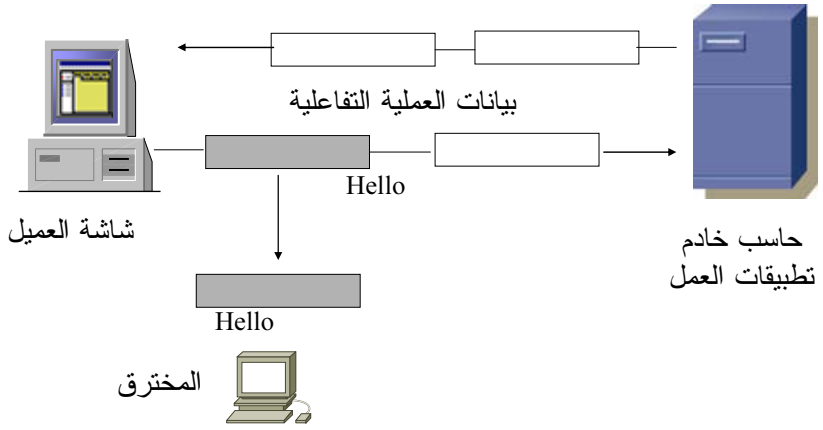


الشكل رقم (9): المخاطر التي تتعرض لها شبكات المعلومات

وعلى سبيل المثال فإن الشكل رقم (10) يوضح كيفية اختراق عملية تفاعلية (مثل دخول العميل على البنك أو المستشفى أو الضرائب – أو شراء سلعة) ويكون نتيجة الاختراق إما التصنت للاستفادة من البيانات الشخصية للعميل أو التحايل إما بتغيير بيانات العملية التفاعلية أو بإجراء عمليات على حساب العميل).

[10]

خطر اختراق العمليات التفاعلية

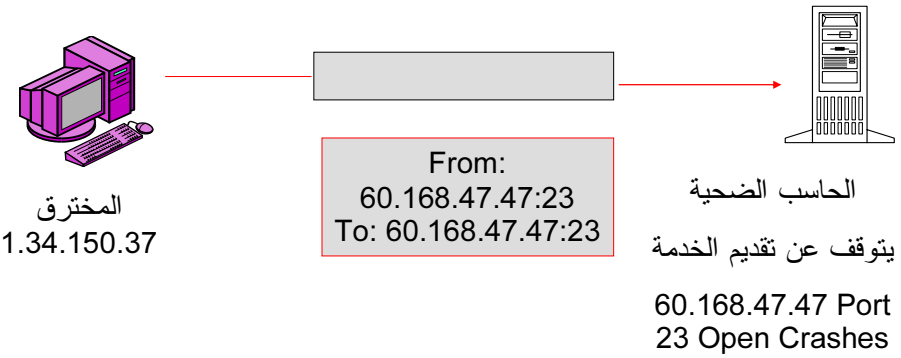


المخترق يتصنت بهدف: الاستفادة/محو/تغيير البيانات

الشكل رقم (10): اختراق العمليات التفاعلية

مثال ثان هو خطر "منع الخدمة" أو "الهجمات الإغراقية (DoS)" هو فقد خدمات النظام المتاحة للمستخدم الفعلي حيث تصبح "غير متاحة" في وقتها المحدد كما تستهدف إبطاء أو شل حركة مرور البيانات عبر الشبكة. على سبيل المثال من الممكن إرسال عدد كبير جداً من الرسائل مجهولة المصدر أو المصب عبر الشبكة تستهلك الحيز الترددي للشبكة (Network Bandwidth) وبالتالي لا يستطيع المستفيدون من النظام الدخول عليه والاستفادة منه. وفى بعض الأحيان يقوم المخترق بتشغيل معالج الحاسب الضحية بطريقة مكثفة بحيث لا يكون لديه الوقت أو المصادر لتنفيذ برامج أو تطبيقات أخرى. ويوضح الشكل رقم (11) خطر "منع الخدمة" حيث يرسل المخترق حزم بيانات غير متعارف عليها في بروتوكول الشبكات (IP) (مثل حزمة بيانات لها نفس عنوان المرسل والمرسل إليه) للحاسب الضحية يكون نتيجتها عدم مقدرته على التعامل مع الكم الهائل من حركة البيانات ودخوله في مرحلة تراكم أو تحميل زائد للحركة (Congestion) وبالتالي منع الخدمة عن المشتركين الأصليين.

11 خطر منع الخدمة



يرسل المخترق رسائل لها نفس عنوان المرسل والمرسل إليه وهما عنوان الحاسب الضحية وينتهى الأمر بتوقف الحاسب الضحية عن تقديم الخدمة للمشتركين الأصليين لكونه تائه يبحث طبقاً لبروتوكول الاتصال IP عن عنوان المرسل للرد عليه

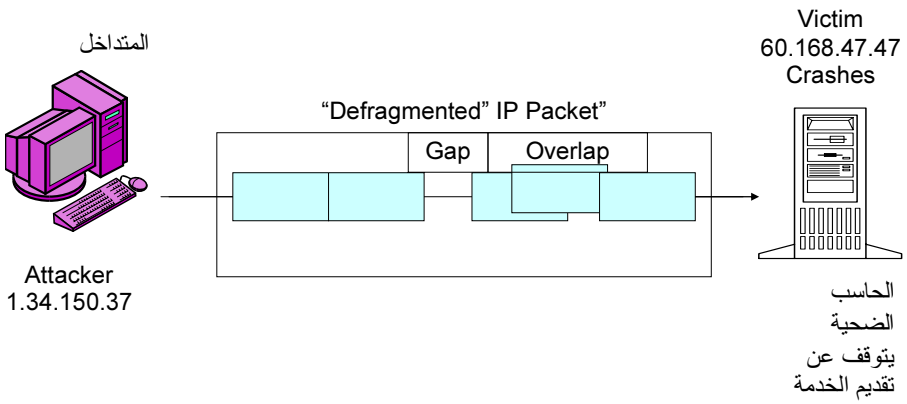
الشكل رقم (11): منع الخدمة بواسطة حزم بيانات البروتوكول IP

نفس التأثير يحدث إذا أرسل المخترق عدد كبير ومتتالي من حزم بيانات التزامن SYN Packets دون انتظار الرد. أو إرسال حزم بيانات غير قابلة لإعادة تجميعها طبقاً للشكل رقم (12) أو إرسال حزم بيانات حجمها غير قياسي أو بواسطة إرسال حزم بيانات ضمن بروتوكول التحكم في الاتصال ICMP (مثل حزم بيانات Ping-Echo, ...) بدون أن يكون الهدف منها التحكم وإنما تهدف إلى إرباك الحاسب الضحية وإرغامه على إرسال بيانات يستفيد منها المخترق (مثل عنوان IP للحاسب الضحية) ... الخ.

ويوجد بمواقع الإنترنت عدد كبير من برامج الاختراق التي يمكن بسهولة استغلالها في هذه النوعية من الاختراقات الأمنية.

خطر منع الخدمة

12

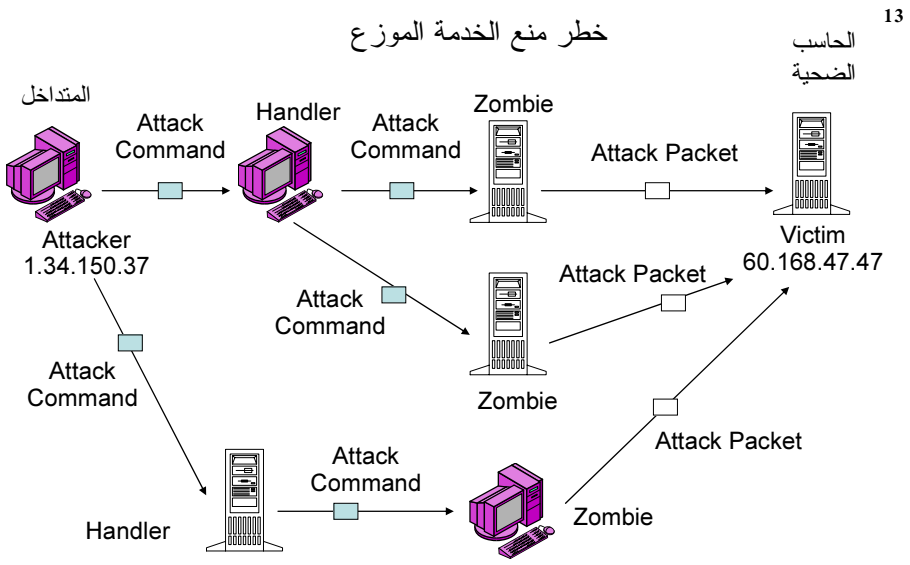


يرسل المتداخل حزم بيانات لا يمكن إعادة تجميعها مرة أخرى وينتهى الأمر بتوقف الحاسب الضحية عن تقديم الخدمة للمشتركين الأصليين

الشكل رقم (12): منع الخدمة بواسطة حزم بيانات لا يمكن إعادة تجميعها

من خلال خطر "منع الخدمة الموزع" أو "الهجمات الإغراقية الموزعة (DDoS)" يقوم المعتدي باستخدام عدد من الحاسبات التي سيطر عليها Zombie للهجوم على حاسبات ضحية قد تكون تابعة للحاسبات التي سيطر عليها. ويتم تركيب البرنامج الرئيسي للهجمات الإغراقية الموزعة (DDoS) في الحاسبات Zombie مستخدماً حساباً (اسم وكلمة مرور) مسروقاً.

ويوضح الشكل رقم (13) خطر "منع الخدمة الموزع" حيث يتم إرسال عدد ضخم من حزم البيانات لنفس الحاسب الضحية من خلال أكثر من حاسب يكون نتيجتها عدم مقدرته على التعامل مع الكم الهائل من حركة حزم البيانات وبالتالي منع الخدمة عن المشتركين الأصليين.



يستغل المتداخل عدة حاسبات "ضحية" ويوظفهم لإرسال سيل من حزم البيانات المتتالية فى وقت واحد وينتهي الأمر بتوقف الحاسب الضحية عن تقديم الخدمة للمشتركين الأصليين لكونه مشغول ومتحمل فوق طاقته

الشكل رقم (13): خطر منع الخدمة الموزعة

وتنبع التهديدات التي تواجه شبكات المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء التي قد ترد من مصادر داخلية أو خارجية. كما أنها تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم الكفاءة اليومية المتوقعة. على سبيل المثال قد تنتج الأخطار من أعطال كبيرة تؤدي إلى توقف العمل أو إبطال العمل بصفة دائمة أو تقلل من قيمة النظام وتتعطل خدماته. وفي هذه الحالة يجب مراعاة توقيتات الأعطال وأخطاء تنفيذ العمل الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية.

وقد تنبع أخطاء النظام من سوء استخدام الأجهزة والبرمجيات أو الأخطاء الكامنة (Bugs) أو التحميل الزائد أو المشكلات التشغيلية وغير ذلك. وقد تظهر الصعوبة في مكون النظام الداخلي كما في حالة أجهزة وملحقات النظام المتعلقة بوحدة الذاكرة أو وحدة تجميع نظام الشبكات الموزعة أو في برمجيات نظم التشغيل والتطبيقات مثل المحرر (Editor) والمكود (Compiler) أو من مصادر شبكة الحاسبات المحلية LAN. وقد تكون الصعوبة نابعة من مكون الشبكات الواسعة الخارجية WAN كما في حالة عدم توافر دوائر الاتصالات عن بعد أو الأقمار الصناعية أو نتيجة ضبط غير دقيق للموائمة والتكامل والترابط بين مكونات النظام المختلفة معاً.

وقد تتسبب المشكلات الفنية في فقد تكامل النظام حيث يعطي النظام بيانات غير صحيحة نتيجة للهجمات المختلفة التي يتعرض لها. فغالباً تدخل الفيروسات (Viruses) في النظام من خلال البرمجيات المصابة (Infected) أو المتطفلين (Parasites) أو أبواب الشراك (Trap Doors) أو الديدان (Worms) أو القنابل المنطقية (Logic Bombs) التي تمثل بعض الوسائل التقنية المستخدمة لتعطيل النظام وتشويهه أو إتلاف أو تحريف في بياناته ووظائفه المختلفة.

وتنشأ الصعوبة في صيانة وحماية أمن المعلومات والنظم والشبكات من تواجد بيئات تشغيل متعددة من الأطراف المرتبطة بها كالمتعهدين والموردين والبائعين ... الخ – ومن مقاييس التأمين الشائعة ضرورة توافق البرمجيات في بيئة الموردين المتعددة – وحتى يمكن التوصل لذلك يصبح من الضروري توافق توجيهات منظمات التوحيد القياسي مثل ITU وISO والشركات المنتجة والموردين والهيئات القومية ومستخدمي شبكات المعلومات على المعايير والتوجيهات الحاكمة لقياسات التأمين ذات الطابع الدولي.

وتقع التهديدات المادية لشبكات المعلومات في مجموعتين عريضتين: الأحداث البيئية الجسيمة والتجهيزات المادية غير السليمة للمعدات والبرامج. وتشتمل الأحداث البيئية الجسيمة على الحرائق والزلازل والفيضانات والعواصف الكهربائية والموجات الحرارية المرتفعة والرطوبة الزائدة وما شابه ذلك. ويضم الموقع الطبيعي معدات الحاسبات الآلية ومعدات الشبكات وخطوط الاتصال حيث قد يحدد له حجرات للحاسبات الآلية وحجرات لتخزين البيانات لها تجهيزات للطاقة الكهربائية والاتصالات تتعرض كلها للأحداث البيئية الجسيمة عند حدوثها.

أما أوضاع التجهيزات المادية غير السليمة فقد تظهر من خلال اختراق مقاييس التأمين المادية في حالات انقطاع التيار الكهربائي وسوء استخدام أجهزة التكييف وتسرب المياه أو بسبب الغبار والأتربة. وقد يتأثر نظام المعلومات من الإهمال المباشر في الأماكن المخصصة له أو غير المباشر في نقاط الربط الجوهرية خارج المؤسسة كما في إمدادات الطاقة الكهربية أو قنوات الاتصال عن بعد. كما يساهم الأفراد وما يتم إنشاؤه بواسطتهم من أنظمة مختلفة اقتصادية أو سياسية أو اجتماعية في قصور قيمتها وأدائها مما ينجم عنه مشكلات أمنية أيضاً.

وقد يؤدي التنوع الكبير لمستخدمي شبكات المعلومات والمتعاملين معها من العاملون والمستشارون والعملاء والمنافسون والجمهور العام فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن شبكات المعلومات.

إن نقص التدريب والتوعية الملائمة عن أمن المعلومات وأهميته تسهم في الجهل باستخدام شبكات المعلومات المناسبة. وبدون تنظيم دورات تدريب ملائمة قد يجهل كثير من الأفراد بأعراض الأضرار النابعة من سوء استخدام شبكات المعلومات كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها مما قد يؤدي إلى مزاولات تعود بالإساءة لأمن المعلومات.

ويعتبر اختيار كلمة المرور (Password) الذي يمثل نشاط المستخدم في كل أنحاء العالم بل يمثل النشاط الرئيسي لأي نظام معلومات مثالاً واضحاً لأمن المعلومات. فعلى الرغم من أن كلمات المرور تطبق عادة على رقابة الوصول إلى معظم شبكات المعلومات لا زال عدد قليل جداً من المستخدمين يعلم بأهمية الحاجة لأمن الاسم وكلمة المرور بالطريقة التي تتمثل في تحديد طول وتكوين الاسم وكلمة المرور ومن العواقب التي قد تنشأ من سوء استخدام هذه الوسيلة الأمنية الفعالة. على أنه بدون تدريب أو توجيه قد يختار كثير من المستخدمين كلمات مرور واضحة يسهل تذكرها واستنتاجها مثل أسماء العائلة أو الأسماء القصيرة أو الكلمات المرتبطة بالمهام ... الخ.

وبعد الدخول إلى البيانات ومصادر النظام قد يترك المستخدمون غير المدربين كلمات المرور الخاصة بهم مكتوبة بصورة مكشوفة وواضحة للدخلاء على النهايات الطرفية الفعالة المتصلة بشبكة نظام المعلومات. كما قد يفشل الأفراد في إنشاء ملفات بيانات إضافية مساندة. أو قد يشتركون في رموز التعريف وكلمات المرور. أو قد يتركون منافذ الرقابة والوصول مفتوحة في مواقع التأمين مما يعرضها للاختراق.

كل ذلك يمثل مشكلات التأمين التي تؤدي إلى الدخول غير المصرح به على ملفات الحاسب الآلي أو اختراق الحاسبات الخادمة أو النهايات الطرفية للعملاء وامتلاك كلمات المرور بواسطة الدخلاء وبالتالي سوء استخدامها وتعرض مكونات النظام للاختراقات.

وقد تحدث الأخطاء والاختراقات أثناء تجميع البيانات وإنتاج المعلومات ومعالجتها وتخزينها وإرسالها وحذفها. كما أن تعطل عمل النسخ البديلة ومساندة للملفات والبرمجيات ذات الطبيعة الحرجة يضاعف من آثار الأخطاء والاختراقات ذات الطابع السلبي. وعندما لا توجد "سياسة أمنية" للمؤسسة تتصل بإعداد وحفظ نسخ إضافية مساندة لملفات المعلومات والبرمجيات التي تمتلكها فإنها سوف تتحمل نفقات وخسائر واضحة ترتبط بالوقت والجهد والمال الذي ينفق في إعادة إنشائها من جديد.

إن سوء الاستخدام المقصود للنظام والوصول غير المصرح به بغرض التطفل والنزوع للأذى وتعمد التخريب والتدمير والاحتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلبياً على قابلية نمو حياة النظام والمؤسسة المالكة له بل تؤثر أيضاً على القابلية للبقاء والتواجد. على سبيل المثال فإن تحميل البرامج المجهولة المصدر أو غير المصرح بها أو النسخ غير المصرح بها للبرامج المرخصة – وهي أعمال منتشرة على نطاق واسع – قد تؤدي إلى خسائر كبيرة لنظم المؤسسة.

ومن المألوف أن جزءاً كبيراً من التهديدات التي تواجه شبكات المعلومات قد يأتي من المصادر الخارجية. كما أنه على النقيض من ذلك فإن الأفراد من الداخل الذين لهم حق الوصول المصرح به للنظام قد يمثلون تهديدات أعظم تواجهه شبكات المعلومات أيضاً. فعلى الرغم من أنهم قد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة فإنهم بسبب التعب أو الإرهاق أو الإهمال أو التدريب غير الملائم قد يقترفون أفعالاً غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات الهامة للمؤسسة التي يعملون بها. وفي حالة كون الأفراد غير مؤتمنين فإنهم يسيئون استخدام شبكات المعلومات أو يتعمدون من خلال الوصول المصرح به العبث والتلاعب في النظام بطرق متعمدة بغية الاستغلال أو الثراء الذاتي للإضرار بالمؤسسة التي يعملون بها.

وبرامج الحاسبات التي تمثل عنصراً مهماً من عناصر نظام المعلومات من المحتمل أن تكون مجالاً خصباً للتهديدات التي يتعرض لها النظام حيث قد تشتمل هذه البرامج على أكواد فيروسات الحاسبات المزروعة في النظام مما قد يعرض سرية البيانات وخصوصيتها وتوافرها للخطر المتزايد. بالإضافة لذلك فإن التحميل الزائد للحاسبات والشبكات قد يتسبب في محو البيانات والمعلومات أو تحويرها وتغييرها. كما أن انتهاكات اتفاقيات الترخيص الممنوحة قد تعرض أمن نظام المعلومات للخطر الإضافي. على سبيل المثال فإن تعديل البرامج المرخصة بطريقة غير مصرح بها قد يؤدي إلى قصور الأداء عند تفاعل البرامج المعدلة والأصلية مع أجزاء النظام الأخرى. كما أن إفشاء البيانات الضمنية قد يضر بالوضع التنافسي للمؤسسة مما يؤدي إلى خسارتها بل ويهدد بقائها.

من هذا المنطلق يجب أن تمتد إجراءات التأمين الملائمة لما بعد النهايات الطرفية وخطوط الاتصال إلى مجال نظام المعلومات بالكامل. فعلى سبيل المثال فإن عدم ملاءمة تداول وسائل تخزين البيانات والمعلومات (سواء كانت ورقية أو ممغنطة أو ضوئية، الخ) – بالإضافة إلى عدم ملاءمة طريقة التخلص أو محو التقارير التي تمثل مخرجات النظام – قد تؤدي إلى ثغرات أمنية مكلفة. فمثلاً قد تشتمل مخرجات الحاسبات الورقية على معلومات ضمنية أو تنافسية أو مفاتيح تخص الوصول للنظام وأصوله. كما أن كثيراً من المؤسسات لا يتوافر لها سياسات واضحة للتخلص من أصولها المعلوماتية مما يجعل يسهل اختراق أمن المعلومات.

وقد يؤدي عدم وجود سياسات واضحة لاستخدام نظام المعلومات إلى مشكلات أمن ضخمة يتعرض لها النظام. كما في حالة أعمال الصيانة والدعم الفني عند نقص الأفراد المؤهلين بالمؤسسة أو بسبب تغيير ودوران العمالة أو عند إدخال تكنولوجيات متقدمة تتطلب مهارات جديدة – مما قد يؤدي إلى إبطاء العمل أو توقفه – وهذه الحالات يجب مراعاتها من بدء التخطيط لنظم التأمين والحماية المطلوبة.

ومن الملاحظ أن كثيراً من المؤسسات القائمة حالياً وخاصة في دول العالم الثالث لم تجار حتى الآن التطور والنمو التكنولوجي المرتبط باستخدام شبكات المعلومات وتأمينها. فلا يزال يوجد قصور واضح ونقص كبير وتأخر في التقنيات والتوحيدات القياسية لعدم الأخذ بالمعايير الدولية والتشفير الخاص بالمزاولة الأحسن إلى جانب قصور الإرشاد والتوعية والحقوق والالتزامات القانونية مما يزيد في النفقات ويسبب تأخير الأعمال وعدم تكامل البيانات.

إن السماح باستمرار الوضع الراهن يحد من النمو المستقبلي ويؤخر اللحاق بعصر المعلومات والمعرفة المستهدف.

7-3 متطلبات التأمين لشبكات المعلومات

توجد أشكال متنوعة للمعلومات المطلوب تأمينها يمكن تلخيصها في الآتي:

1) المعلومات والبيانات المخزنة بقواعد البيانات.
2) المعلومات والبيانات المخزنة في ذاكرة الحاسبات الآلية.
3) البيانات المتداولة على الشبكات المحلية والشبكات الواسعة.
4) المعلومات والبيانات المخزنة المطبوعة والمكتوبة على الورق أو على السبورات البيضاء أو ما شابه.
5) المعلومات المتداولة بواسطة أجهزة الفاكس والتلكس أو أي أجهزة اتصالات مشابهة.
6) المعلومات والبيانات المخزنة في جميع أنواع الأوساط التخزينية الصلبة والمرنة والشرائط والضوئية.
7) المعلومات المخزنة على الميكروفيلم والميكروفيش.
8) المعلومات والبيانات المعروضة على اللوح وأجهزة العرض والأوساط المتعددة الأشكال.
9) المعلومات المنطوقة من خلال التليفون العادي والمحمول والفيديو وما شابه.

ويفضل أن يتم تأمين شبكات المعلومات على مستويات متتالية أو على خطوط دفاعية متتالية بحيث يكون لكل خط دفاع دور في حماية نظام المعلومات من الاختراقات الأمنية والأعطال – وبالتالي تتلخص مستويات ووسائل التأمين التقنية لشبكات المعلومات في الآتي:

1) على مستوى الربط الطبيعي:
   أ) التأمين الطبيعي لمكان نظام المعلومات والشبكات.
   ب) استخدام معدات التشفير على مستوى النبضات.

2) على مستوى الشبكات:

أ) استخدام أجهزة الجدران النارية.

ب) استخدام أجهزة اكتشاف ومنع الاختراق.

ج) استخدام الشبكات الافتراضية المؤمنة.

د) استخدام المناطق الأمنية.

ه) استخدام ترجمة العناوين ((Network Address Translation (NAT)

و) استخدام التشفير على مستوى الشبكات IPSEC وتوفير قنوات مؤمنة (Secured Tunnels) على مستوى التحكم في المحور.

ز) استخدام ماسحات الكشف عن الاختراقات الأمنية.

3) على مستوى التطبيقات:

أ) استخدام شهادات التوثيق والتوقيع الإلكتروني.

ب) التعرف على المستخدم وحق وصلاحيات الدخول.

ج) التشفير على مستوى تطبيقات التجارة الالكترونية (SSL) واستخدام وسائل مضادة لمنع زرع الفيروسات.

د) التحصين المستمر لبرامج الحاسبات الخادمة والشخصية من خلال ما تقدمة الشركات المنتجة من تحديثات Service Packs لغلق ما يتم اكتشافه من ثغرات أمنية في برامج التشغيل وبرامج التطبيقات.

1-7-3 التأمين الطبيعي لموقع الأجهزة

يعتبر التأمين الطبيعي لموقع شبكات المعلومات مطلباً أساسياً لا بد من توافره لخدمة إنشاء بيئة نظام حاسب إلى مؤمنة – ويتم زيادة كفاءة التأمين الطبيعي بوسائل حق الدخول للأفراد يتم مراقبتها وتحقق التأمين والحماية لمكونات شبكة المعلومات ضد الاختراقات الأمنية والأعطال والتوقف والكوارث الطبيعية.

ومن المفضل إنشاء نظام المعلومات في مبنى منفصل أو في جزء من مبنى المؤسسة (داخل دور أو أكثر) على أن يكون بالأدوار العليا لزيادة التأمين ضد الكوارث الطبيعية ولتوفير خطوط حماية طبيعية إضافية من خلال مداخل المبنى. ويكون الموقع بعيداً قدر الإمكان عن أماكن تخزين المواد القابلة للاشتعال. كما يجب ألا يكون للموقع إشارات أو علامات تمييز واضحة يفهم منها الغرض من الموقع.

كما من المهم توفير وسائل اكتشاف الحريق قبل وقوعه باستخدام كشافات الدخان وكشافات الحرارة وأن يتم اختيار مواد البناء من المواد التي تقاوم الحريق ويفضل أن تكون الغرف محصنة لمنع الإشعاع من الداخل إلى الخارج والعكس. وأن يساعد تصميم المبنى على تطويق الكوارث الأمنية مثل الحريق والتغلب عليها في مدة لا تزيد عن ساعة. بالنسبة للطاقة الكهربية يفضل استخدام مصدرين لتيار المدينة بالإضافة إلى ماكينات الديزل الاحتياطية إذا كان ذلك ممكناً – كما يتم استخدام أجهزة الحماية ضد قطع التيار (UPS).

تكون عدد المداخل محدودة قدر الإمكان والأبواب مزدوجة بحيث يكون لكل غرفة بابين لا يتم فتحهما معاً – مع استخدام الأقفال الميكانيكية والإلكترونية واستخدام كروت التعارف الذكية للأفراد التي تعتمد على الصفات البيولوجية للفرد مثل الصورة – بصمة اليد – بصمة العين – الصوت.

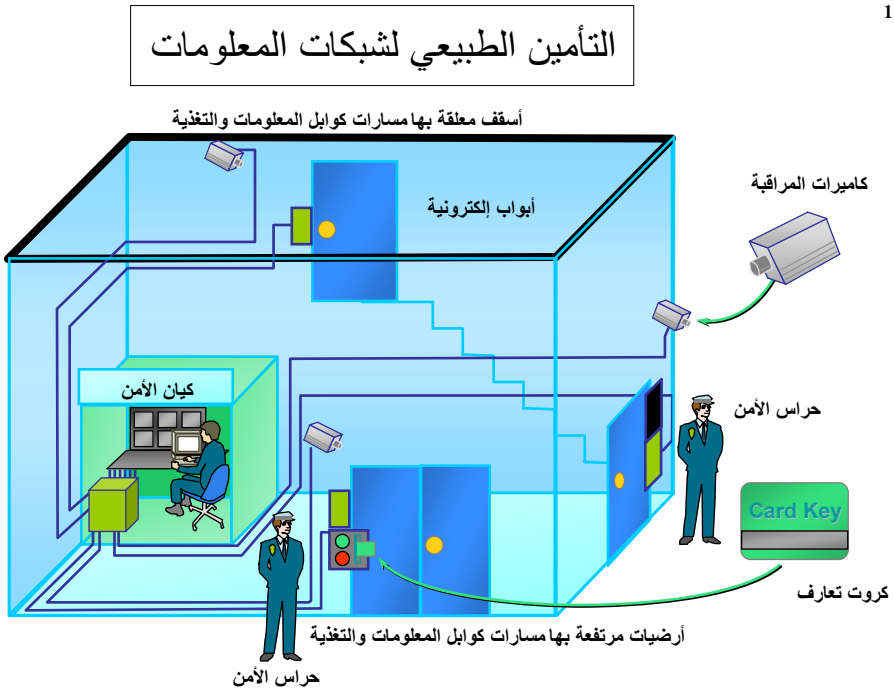
ومن المهم أيضاً تأمين مسارات كوابل التغذية والشبكات من خلال الأسطح المعلقة الافتراضية (False Ceiling) والأرضيات المرتفعة (Raised Floors). مع أحكام غلق فريمات الاتصالات. ويتم اختيار عدد المداخل بحيث تسمح بسرعة إخلاء المبنى من الموظفين في حالة حدوث كوارث طبيعية.

يفضل أيضاً أن يكون للموقع منطقة خاصة بتفريغ ونقل المعدات بحيث لا تكشف ما يحدث داخله – ويكون بالموقع وسائل التحكم في الدخول للموقع من خلال:

1) حراس الأمن ومكاتب الاستقبال.
2) الكروت الممغنطة.
3) كاميرات المراقبة.

والشكل رقم (14) يوضح مثال لموقع شبكات المعلومات متضمناً وسائل التحكم الطبيعية المذكورة عالية.

14

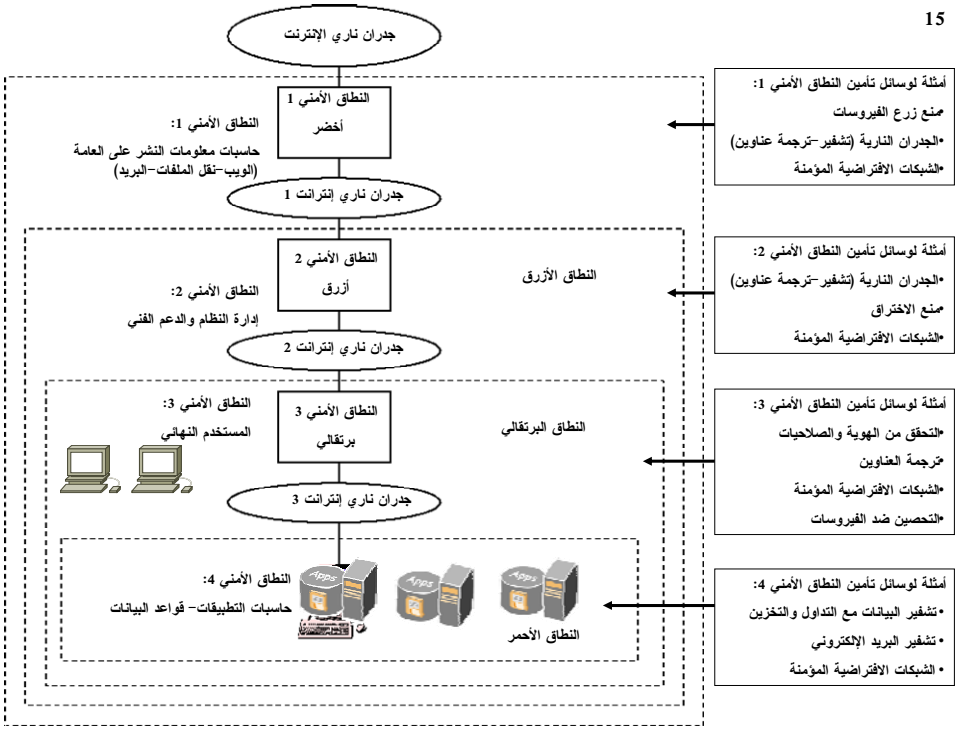


الشكل رقم (14): مثال لموقع شبكات المعلومات

من المهم استخدام نظم التحكم في الوصول لأماكن الحاسبات باعتبارها مناطق أمنية. وتسمح 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 الأمنية.

تؤسس نظم التحكم في الدخول على تقسيم المكان الطبيعي لنظام المعلومات إلى مناطق ذات درجات أمنية متدرجة طبقاً لدرجة حساسيتها بالنسبة للمؤسسة. والشكل رقم (15) يوضح مثال لاستخدام مستويات من معدات الجدران النارية (firewalls) في تقسيم شبكة المعلومات إلى نطاقات أمنية DMZ.

15



الشكل رقم (15): استخدام مستويات من معدات الجدران النارية (firewalls) في تقسيم شبكة المعلومات إلى نطاقات أمنية DMZ

تصدر تصاريح المرور بين النطاقات الأمنية باستخدام كروت تعارف بألوان مختلفة تتناسب مع درجة سرية النطاق الأمني مع تزويد التصاريح إذا أمكن بوسائل تحديد المحل لتحديد الموجودين بكل منطقة مؤمنة. كما يجب الإشراف على زوّار المناطق الأمينة حتى يتم خروجهم – مع تسجيل وقت دخولهم ووقت خروجهم ومن الضروري السماح لهم فقط بالزيارة في حالات معينة مصرح بها وفى أماكن محددة ويتم إخطارهم والحصول على موافقتهم على "تعليمات أمن المكان" وعلى "إجراءات العمل عند الطوارئ".

التحكم في الدخول للمعلومات الحساسة واستخدام وسائل إعداد المعلومات يكون مقصوراً فقط على المصرح لهم مع الاستعانة بوسائل تحديد الهوية مثل البطاقات الشخصية والكروت ذات الرقم الكودي الشخصي (Personnel Identification Number (PIN)) لتسجيل جميع حالات الدخول والخروج.

قد يطلب من كلّ العاملين بنظام المعلومات لبس زي مميز إذا أمكن ذلك مع إظهار بطاقات الهوية ومن الضروري أن يتشجّعوا لمجابهة واعتراض الزوار غير المرافقين وأي فرد من العاملين لا يرتدي الزي المميز أو لا يضع بطاقة الهوية بطريقة ظاهرة.

وتتطلب الوسائل القابلة للتطبيق لأمن شبكات المعلومات تعريف التالي:

أ) الأفراد الذين يتواجدون بمواقع نظام المعلومات كغرفة الشبكات أو مركز المعلومات سواء كانوا يعملون بها أو مترددين عليها لوحدهم أو بطريقة جماعية في بعض الوقت أو في كل الأوقات.

ب) الشروط والإجراءات المتعلقة باستبعاد أي من مكونات النظام الاحتياطية التي لا تستخدم إلا في حالات الطوارئ.

ج) الشروط المحددة لنقل وتخزين الأجهزة ووسائط التخزين الطبيعية كالأشرطة أو الأقراص الممغنطة – الأقراص المدمجة – أو أقراص الفيديو الرقمية ... الخ.

وتعتبر هذه الأمور مهمة بصفة معينة عند توافر خدمات شبكات الحاسبات الآلية أو مراكز المعلومات من مصادر خارجية تختص بظاهرة "التعهيد" (Outsourcing). وعلى أي حال فإن مراقبة أو مراجعة مقدم أو مورد الخدمة تصبح من المتطلبات والشروط الهامة التي يجب مراعاتها.

وكما سبق ذكره يجب ألا يتطلب أمن المعلومات السماح للمتطفلين أو الدخلاء من الربط الطبيعي سلكياً أو لا سلكياً مع الحاسب الآلي وملحقاته.

ويتحقق التأمين الطبيعي عندما تستخدم آليات إضافية عديدة في نمط فعال تتكامل مع الإجراءات الطبيعية بواسطة تقديم إجراءات وأدوات وبرمجيات تتمثل في التالي:

أ) معدات الرقابة على الوصول (Access Control) أو كروت التعريف والهوية.

ب) معدات تأمين نوافذ ونقاط الوصول الأخرى.

ج) وسائل تحديد كيفية الوصول للبيانات ومصادر المعلومات وبواسطة من.

د) إعداد نسخ إضافية مساندة لكل البرمجيات وملفات البيانات حتى يمكن استعادتها مرة أخرى عند حدوث الكوارث أو الفقد.

هـ)تطبيق خوارزميات تشفير ملائمة.

و) اكتشاف ثغرات وانتهاكات التأمين.

ز)اكتشاف البرمجيات الخبيثة المتعلقة بخدمات الشبكات مثل البريد الإلكتروني والتجارة الإلكترونية والوسائل الأخرى المختلفة.

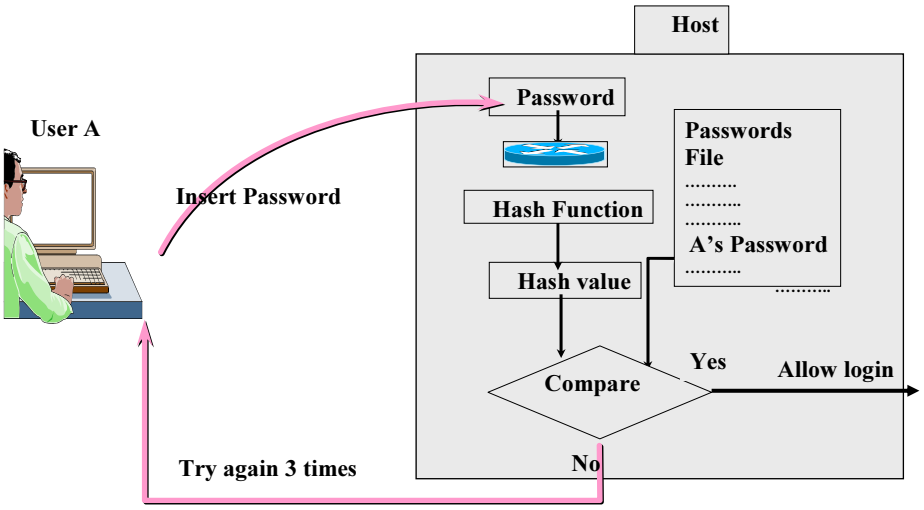
2-7-3 عمليات التحقق من التأمين المستهدف

يمكن تحديد أربع أبعاد رئيسية تستهدف تأمين شبكات المعلومات تتمثل في التالي:

1) التعريف والتحقق من الهوية (Identification and Authentication)

تعتبر هذه الوسيلة أهم وسائل التحكم في الدخول للبيانات ومصادر المعلومات حيث إنها تساعد على التغلب على معظم التهديدات. ويعتبر التعريف أول خطوة في سبيل منح حق الدخول إلى النظام بهدف التحقق من يسمح له دخول النظام. والشكل رقم (16) يوضح خريطة تدفق البيانات التي تحتوى على مقارنة الاسم وكلمة المرور مع الاسم وكلمة المرور المخزنين في ذاكرة الحاسب الرئيسي بطريقة تشفير أحادية الاتجاه ليس لها مفاتيح شفرية تسمى "الهاش" (Hash Function) (سوف يتم تناولها بالتفصيل في الفصل الخامس) وهذا التحقق عادة يتم مرة واحدة باستثناء نظم الحاسبات السوبر التي تتطلب عدة مستويات من وسائل التحقق من الهوية.

استخدام التشفير الآحادي الاتجاه "هاش" في تشفير الاسم وكلمة المرور



الشكل رقم (16): مقارنة الاسم وكلمة المرور مع الاسم وكلمة المرور المخزنين في ذاكرة الحاسب الرئيسي بطريقة التشفير أحادية الاتجاه Hash Function

يتم التحقق من شخصية المستخدم من خلال ثلاث مداخل أساسية ومميكنة هي:

أ) إخبار الحاسب الآلي عن شي معروف لكل مستخدم مثل الاسم (Username) وكلمات المرور (Password): وعلى الرغم من أن كلمات المرور سهلة التطبيق والتنفيذ إلا أنها تشتمل على بعض القصور حيث يمكن لطرف ثالث الحصول عليها. لذا يفضل أن تكون موضوعة طبقاً لقواعد معقدة ترتبط بعدد الحروف والأعداد. كما يجب أن تتغير كل فترة زمنية أو عند الحاجة. وفي هذه الحالات يلزم وجود توجه قوي من الإدارة العليا للمؤسسة نحو الأفراد في اختيار كلمات المرور التي يمكنها البقاء وعدم إفشاء محتواها وتشفيرها حتى لا تتكشف عندما يعثر عليها شخص آخر. كما يراعى ألا تزيد عدد محاولات الدخول الفاشلة على معدات النظام عن 3 مرات. وفي الحالات الفاشلة يفضل غلق حساب المشترك مدة تتراوح بين 8-12 ساعة. ومن أهم القواعد العامة لحماية كلمات المرور الآتي:

1) يجب أن تكون الأسماء وكلمات المرور مشفرة أثناء تخزينها بالحاسب.
2) عدم ظهور كلمات المرور على الشاشات أثناء كتابتها.
3) تغيير الاسم وكلمات المرور كل فترة (حوالي 40 يوم) أو عند اكتشاف خطر أمني خاص بمحاولات كسر كلمات مرور معينة.
4) يمنع استخدام اسم وكلمات مرور سابقة.
5) يتم إصدار كلمات المرور بواسطة المتخصصين أو الأفراد أنفسهم بطريقة سرية وبمعزل عن باقي الأفراد.

6) لا يقل طول كلمات المرور عن "6" – تتكون من حروف (عالي وواطي) وأرقام وعلامات ترقيم بحيث لا تبدأ بالحروف العالية ولا تنتهي بأرقام. وكمثال لكلمة مرور قوية: **triV6#ial.**

ب) تقديم شيء ما مملوك للشخص للدخول في النظام كبطاقة الهوية أو التعريف الشخصي أو رمز ما: حيث يمكن أن يزداد أمن النظام بأن يطلب النظام من الشخص تعزيز الاسم وكلمة المرور ببعض أنواع المعدات الطبيعية ككارت أو بطاقة هوية أو رمز إلكتروني معين للسماح بالدخول.

ج) إعطاء النظام شيء ما خاص بالمستخدم يرتبط بالخواص الشخصية (البيولوجية) له مثل: بصمة اليد أو الإصبع أو العين أو الوجه أو نمط ذبذبة الصوت الشخصي. وهذه يطلق عليها السمات البيولوجية Biometrics حيث يتم حالياً استخدامها في بيئة شبكات المعلومات المؤمنة. وعلى الرغم من أن التكنولوجيا المرتبطة بذلك معقدة وباهظة التكلفة إلا أن استخدامها في تزايد مستمر.

(2) الاعتماد أو وسائل التحكم في الدخول للبيانات (Authorization)

بمجرد معرفة النظام بالمستخدم المصرح له فإن السؤال التالي الطبيعي هو ما يسمح به لهذا المستخدم؟ وعلى ذلك فإن عملية الاعتماد يقصد بها حق الوصول إلى البيانات ومصادر المعلومات المصرح بها لهذا المستخدم. على سبيل المثال تحديد المعاملات أو البيانات التي يسمح له بها وتلك التي يمكن للمستخدم تعديلها أو إضافتها. وتبني مزايا الوصول المصرح به على تحديد دور المستخدم ومسؤولياته وحقوقه من قبل النظام. وفي حالة مقدمي الخدمات المعلوماتية كشركات مقدمي خدمة نقل البيانات وشركات التجارة الإلكترونية ... الخ – يتم إقرار هذه الصلاحيات بمعايير محددة تحددها العقود والاتفاقات المبرمة بين الأطراف.

تتبع سياسة عملية الدخول (Access Control) إلى البيانات ومصادر المعلومات إحدى السياسيات الآتية:

- السياسة القوية: كل شيء ممنوع إلا ما يصرح به.
- السياسة الضعيفة: كل شيء مصرح به إلا ما يتم منعه.

في الدول المتقدمة يتم تطبيق السياسة الأولى في عملية التحكم في الدخول إلى البيانات ومصادر المعلومات. ومن المفيد أن تتبع دول العالم الثالث نفس السياسة. أحد الفروق المهمة هو أن السياسة الأولى تعمل على تحديد ما هو ممنوع بينما الثانية تعمل على تحديد ما هو مسموح به. والبديهي أن يكون نسبة السري أو الممنوع أكثر بكثير من الغير سري أو المسموح.

وفي الأولى يكون هناك نسبة بسيطة جداً لما هو سري وممنوع وبالتالي يسهل تأمينه وحمايته بينما في الثانية يكون هناك نسبة عالية جداً لما هو سري وممنوع مما يصعب تأمينه وحمايته.

توفر السياسة الأولى إمكانيات فائقة لحماية وأمن المعلومات وتسمح بل تنمي عوامل التطور حيث إنها تحقق الآتي:

- تيسر انسياب المعلومات أفقياً ورأسيا.
- تسمح بالمشاركة في اتخاذ القرار.
- توفر الشفافية.

- تدعم إمكانية التوقع أو التنبؤ والاستنباط .
- تدعم الوثوقية في النظام وأبسط أشكالها معرفة من عمل ماذا للمعلومات وبصورة قاطعة للشك.
- تضمن المحافظة على تكامل وسلامة المعلومات وعدم السماح بتزويرها.

السياسة الأولى تنقسم إلى نظامين للتحكم بالدخول إلى المعلومات هما:

1) نظام التحكم بالدخول إلى المعلومات الإجباري (Mandatory Access Control).
2) نظام التحكم بالدخول إلى المعلومات المبني على الصلاحية أو السماحية أو التمييز (Discretionary Access Control).

1) نظام التحكم الإجباري في الدخول إلى المعلومات (Mandatory Access Control): ويطبق مبدأ "أقل امتياز" (Least Privilege) حيث لا يحق لأي شخص بحكم مركزه أو نفوذه الإطلاع على معلومات سرية أو حساسة – ما لم تتطلب طبيعة عمله ذلك – ويسمح له فقط بالاطلاع على ما هو ضروري لإنجاز الأعمال المطلوبة منه. ويستخدم نظام التحكم الإجباري في الدخول إلى المعلومات (Mandatory Access Control) على سبيل المثال في نظم المعلومات المؤمنة في الولايات المتحدة الأمريكية حيث تنقسم نظم التحكم في الدخول إلى نوعان من هياكل التحكم هما:

- الهيكل الهرمي.
- الهيكل اللا هرمي.

ويتكون الهيكل الهرمي من أربعة تصنيفات للمعلومات الحساسة (وبالتالي الأفراد المصرح لهم الدخول إلى تلك المعلومات) وهي:

- سري للغاية (Top Secret): وهي المعلومات التي يؤدي إفشاؤها إلى خطر كبير على المؤسسة.
- سري (Secret): وهي المعلومات التي يؤدي إفشاؤها إلى ضرر مادي أو معنوي للمؤسسة.
- خاص (Confidential): وهي المعلومات التي يؤدي إفشاؤها إلى أذى لمصالح المؤسسة.
- غير مصنف (Unclassified): وهي المعلومات المسموح بنشرها للعامة.

يتكون الهيكل اللا هرمي من التصنيفات التالية للمعلومات الحساسة:

- تقسيمات مستقلة: وهي مختصة بالموضوعات الأمنية – فبعض التقسيمات المستقلة قد تكون على سبيل المثال: ذرية ونووية – أمن اتصالات – استخبارات الاتصالات – والاستخبارات البشرية – والمعلومات السرية للغاية والمرتبطة بالتقسيمات المستقلة تسمى تقسيمات معلومات حساسة وتستدعي معاملة خاصة وأعلى درجاتها هي الخطة العملية المتكاملة أو رد فعل المؤسسة أثناء أوقات التوتر أو عند حدوث كارثة.
- التقسيمات التحذيرية: وهي مختصة بجنسية المطلع على المعلومات وملكية الموضوع. فعلى سبيل المثال بعض التقسيمات التحذيرية قد تكون "ليست للأجانب".

2) نظام التحكم بالدخول إلى المعلومات المبنى على التمييز (Discretionary Success Control): وذلك باستخدام "مصفوفة التحكم في الدخول" لكل شخص أو برنامج أو حاسب مدرج في يمين المصفوفة يتعامل مع أية مادة من المعلومات المدرج اسمها في أعلى المصفوفة – ويمكن الاستدلال مما في المصفوفة عما يستطيع هذا الشخص عمله باستخدام هذا الأمر شاملاً ذلك: القراءة – الكتابة – المحو – التعديل – التنفيذ ... الخ.

(3) الإدارة (Administration)

تمثل الإدارة عملية حفظ سمات المستخدمين بالإضافة إلى تعريف أمن مصدر معين. ويشتمل ذلك على أنشطة مثل استبعاد مزايا وصول مستخدم أو موظف ترك الخدمة أو تغيير الصلاحيات أو لتحديد قائمة النظام لما يسمح به لمستخدم معين بعد الترقية أو النقل ... الخ.

(4) المراجعة (Audit)

تمثل عملية المراجعة التأكد من أن مقاييس التأمين مقبولة في نظام عمل محدد. وفي هذا الصدد لا توجد طريقة معينة لمعرفة مدى تجاوز المستخدم الاعتماد أو الصلاحيات الممنوح له بدون تلك المراجعات – كما لا توجد طريقة أخرى أيضاً توضح أن مقاييس التأمين يجب أن تحدد وتقوى بدون معرفة أولية لنواحي القصور التي قد تتواجد فيها – وبذلك تعتبر عملية المراجعة تكملة أساسية لكل مقاييس التأمين.

في نفس الوقت لن تكون أي من الوسائل فعالة بدون توافر عدد من الخصائص ذات التوجه البشري التي تتمثل في التالي:

أ) مساندة الإدارة (الإدارة العليا بصفة خاصة) لسياسات ومقاييس وعمليات أمن المعلومات – كما يجب عليهم الالتزام الكامل بها قبل إعداد التأمين وإدارته.

ب) ضرورة إلمام كل العاملين في كل مستويات الإدارة بالمخاطر المرتبطة بأمن المعلومات وبأهميتها.

ج) أهمية توافق وترابط كل برامج التدريب والتوعية عن أمن المعلومات مع حاجات المؤسسة.

د) ضرورة مراعاة التزام الأفراد الآخرين (كأفراد الصيانة والمستشارين والمتعاقدين والعمالة المؤقتة وعمال النظافة) المتعاملين مع المؤسسة والمتاح لهم الوصول إلى أصول معلومات المؤسسة بقواعد وشروط التأمين التي تم الموافقة عليها.

ه) يراعى أن تحقق شبكة المعلومات المؤمنة أهداف المؤسسة وأن تكون جزء لا يتجزأ من نظام المعلومات وأن يكون وسائل التأمين مناسبة التكلفة ويتم تطوريها باستمرار.

8-3 تطوير سياسة أمن المعلومات

يتم تطوير سياسة أمن المعلومات استرشاداً بمعايير المنظمة الدولية للتوحيد القياسي (ISO) في إصداراتها (Information Systems Security Standards ISO 17799 and ISO 27001) الخاصة بإدارة أمن المعلومات والمعايير المشابهة التي أصدرها الاتحاد الدولي للاتصالات (ITU).

وتعتبر السياسة الموثقة لأمن المعلومات جوهرية وضرورية خاصة أنها تهدف إلى إنجاح أمن المعلومات – كما أنها تمثل الطريقة الفعالة للتعامل مع الأعذار المتمثلة في عدم المعرفة عن الأشياء أو المهام.

وتبني سياسة أمن المعلومات على حاجات العمل للمؤسسة وترتبط بالتهديدات التي تصادفها أو تتعرض لها ويتحتم عليها ضرورة فهمها والالتزام بأهمية تطبيقها. وفي هذه الحالة يجب إعادة تأكيد أن أمن المعلومات ليس أمراً فنياً فقط يمكن تصحيحه والتغلب عليه بوسائل تقنية فنية مثل الجدران النارية (Firewall). بل إن هذا يمثل أيضاً عملاً إدارياً حيث يجب على القوى العاملة بالمؤسسة والأطراف الأخرى المتعاونة معها الاعتراف باستلام وتفهم وثيقة "سياسة أمن المعلومات" والتعهد بتطبيق ما جاء بها من مبادئ ومعايير وقبول ما بها من إجراءات رادعة في حالة عدم الالتزام بذلك.

وكأي عملية توثيق موجهة قد توجد مخاطر في أن إعداد هذه السياسة وصيانتها وتوزيعها قد ينتج عنه مركزية في حد ذاتها – لذلك يصبح الحكم الجيد والصائب على الأمور المتضمنة ضروري فيما يتصل بنسب الإجراءات التي يجب تبنيها والأخذ بها إلى جانب عدم التقليل في تقدير الجهد الذي بذل في إعداد هذه السياسة وحفظها أو صيانتها.

وتتوافر كثير من المبادئ والأسس لإعداد وثيقة "سياسة أمن المعلومات" لكي تصبح مفيدة ومقنعة وقابلة للتنفيذ إلا أن قيمتها المضافة سوف تقرر كيفية النجاح الذي يتم الوصول إليه مما يعمل على تطبيقها ومتابعتها المستمرة.

إن وثيقة سياسة التأمين المبنية على أسس معينة وتحفظ أو تخزن ولا يتم تفعيلها لا تعني وجود سياسة حقيقية للأمن حيث إنها لا تلبي أي قيمة للعمل – لذا يجب تعميم الوثيقة والتدريب عليها وتطبيقها ومراجعتها باستمرار. لذلك يجب أن يساند نشر الوثيقة حملة توعية عن أهمية التأمين لإعلام أفراد المؤسسة والأطراف الأخرى المتعاملة معها بأهمية تطبيق سياسة التأمين الموثقة حيث يعتبر ذلك خطوة مهمة عند تدريب وتوعية العاملين الجدد.

والنظم الفرعية التي يجب أن تشملها وثيقة السياسة الأمنية بالحماية والتأمين هي:

(1) تأمين المؤسسة نفسها وحماية أهدافها وسمعتها.

(2) تأمين المعلومات شاملاً ذلك تصنيف المعلومات والوثائق ومصادر المعلومات.

(3) التأمين ضد مخاطر الأفراد شاملاً جميع مراحل العمل مثل:

- توظيف الأفراد.
- إضافة كيان الأمن للهيكل التنظيمي للمؤسسة مع تحديد مهامه واختصاصاته.
- التعامل مع الأطراف الثلاثة والمقاولين الخارجيين شاملاً ذلك مقدمي خدمة الاتصالات – شركات الأمن والنظافة – شركات التأمين – مهندسي الإصلاح والصيانة – موردي المعدات والبرامج – مطوري النظم والتطبيقات – المستشارين.
- تعريف المستخدم بالاسم وكلمات المرور.
- التعامل مع البرامج الجاهزة وكذلك برامج التطبيقات التي يتم تطويرها ذاتياً بالمؤسسة.
- إدارة الدخول على الشبكات الواسعة خاصة الإنترنت وتأمين تطبيقات البريد الإلكتروني والتجارة الإلكترونية.

(4) إدارة التعامل مع النهايات الطرفية الثابتة والمحمولة.

(5) التأمين الطبيعي لمكان نظام المعلومات والبيئة المحيطة شاملاً ذلك اختيار المكان الطبيعي لنظام المعلومات وتوفير وسائل الحماية الطبيعية ضد الدخول غير المصرح به أو الكوارث الطبيعية.

(6) تأمين الشبكات والإنترنت شاملاً ذلك إدارة أساليب العمل – تفعيل أحقية الدخول وصلاحيات التعامل – أسلوب الدخول على الشاشات والخروج منها – استغلال النظم الشفرية – استغلال وثائق التشغيل وتقارير اقتفاء الأثر التي تصدرها برامج التشغيل وبرامج التطبيقات – عمل النسخ الاحتياطية من البرامج والبيانات – إدارة العمل في النظم التي تعمل بالمشاركة الموزعة من خلال خدمات الشبكات – الدخول والخروج على النظام عند العمل عن بعد – استخدام وسائل التأمين مثل الجدران النارية واكتشاف التداخلات – الدخول على الأنظمة الأخرى المتعاونة من خلال الشبكات – الإبلاغ والتعامل مع حوادث الشبكات الأمنية.

(7) تأمين تطوير التطبيقات شاملاً ذلك: تضمين التأمين في مراحل دورة حياة النظم من التصميم إلى التشغيل الفعلي – تقسيم الأعمال والأنشطة لمنع خطر التواطوء – أساليب التطوير والتحديث – التعامل مع البرامج الجاهزة – الحماية ضد الأبواب الخلفية والاكواد الخبيثة.

(8) التخطيط لاستمرارية عمل شبكة المعلومات عند حدوث الاختراقات الأمنية والتهديدات والكوارث شاملاً ذلك سياسة النسخ الاحتياطية والانتقال لمواقع الطوارئ التبادلية (Disaster Recovery Sites).

9-3 المبادئ الرئيسية المتعلقة بحماية المعلومات الحساسة

بافتراض أن هناك سياسة أمنية لشبكات المعلومات قد تم تبنيها ونظاماً للتصنيف والتصريح قد أسس – فإن هناك على الأقل عشر مبادئ رئيسية يجب اتباعها توضح طرق تنفيذ هذه السياسة وتصنيفاتها لحماية المعلومات الحساسة هي:

1) مبدأ الشبكية: يتكون تصنيف عناصر المعلومات من تصنيفها الهرمي مضاف إليه كل الأجزاء التي وضعت فيها تلك العناصر. التصريح لشخص ونوع الاحقية أو المعالجة (مثل تنفيذ برنامج معين من قبل هذا الشخص) سيكون مؤلفاً من التصريح الهرمي لهذا الشخص مضافاً إليه تصريح كل العناصر التي يعالجها.

2) مبدأ الحماية البسيطة: لا يسمح لشخص برؤية معلومات يتجاوز تصنيفها تصريح ذلك الشخص (بصيغة مختصرة لا يمكنه القراءة للأعلى).

3) مبدأ النجمة (*): لا يسمح "لشخص أو معالج بيانات" الكتابة على أي موضع يكون تصنيفه أقل من أي من الموضوعات التي سبق وعالجها نفس الشخص. هذا المبدأ وجد لمنع تسريب المعلومات من تصنيف عالي إلى تصنيف أقل (بصيغة مختصرة لا يمكن للشخص الكتابة للأسفل).

4) مبدأ التكامل الأولى: لا يسمح لبرنامج حاسب أن يقبل معلومات من برنامج أقل منه في الامتيازات – وتعني الامتيازات ما يمكن عمله أكثر ضمن نظام الحاسبات (مثل اطلاع – قراءة – تعديل – مسح – إضافة) الهدف هنا هو حماية نظام التشغيل من أن يخدع من قبل مستخدم ماكر. (بصيغة مختصرة وبالنسبة لنظام التشغيل لا يمكن للشخص القراءة للأسفل).

5) مبدأ التكامل الثاني: لا يسمح لبرنامج حاسب الكتابة إلى برنامج آخر أعلى منه في الامتيازات – الهدف هنا هو تجنب تدمير أجزاء من نظام التشغيل من قبل برامج المستعملين. (بصفة مختصرة وبالنسبة لامتيازات النظام لا يمكن الكتابة للأعلى).

6) مبدأ العنونة والتصنيف: كل معلومة يجب أن تتم عنونتها أو تسميتها بوضوح ومسجل عليها التصنيف بطريقة يمكن قراءتها من قبل الأفراد والحاسبات باستخدام مثلاً "الخانة الشفرية" (Bar Code) أو "ترددات الراديو المحددة للهوية" (RFID).

7) مبدأ الثبات: لا يحق لأي "لشخص أو معالج بيانات" أن يبدل تصنيف أو معلومة أو تصريح أي شخص آخر بدون اتباع الإجراءات المنصوص عليها بوثيقة "السياسة الأمنية".

8) مبدأ عدم الدخول: لا يدخل للنظام أي شخص ما عدا المسموح لهم ضمن الإجراءات المنصوص عليها بوثيقة "السياسة الأمنية".

9) مبدأ التدقيق والتفتيش: يجب الاحتفاظ بسجل لا يمكن إلغاؤه لكل العمليات التي تتم والمتعلقة بأمن وحماية النظام.

10) مبدأ عدم الالتزام بسياسة موثوق فيها: قد لا تجد مؤسسة تطبق كل المبادئ السابقة وتظل تعمل بفعالية وكفاءة عالية. لذا وجد هذا المبدأ للسماح لبعض المؤسسات الأمنية الموثوق بها بكسر أحد أو كل القواعد السابقة دائماً أو مؤقتاً إذا تطلبت الضرورة ذلك.

الفصل الرابع

الهيكل التنظيمي المساند لتأمين المعلومات

1-4 الأهداف والسياسة العامة لتطبيق الهيكل التنظيمي المساند لتأمين شبكات المعلومات

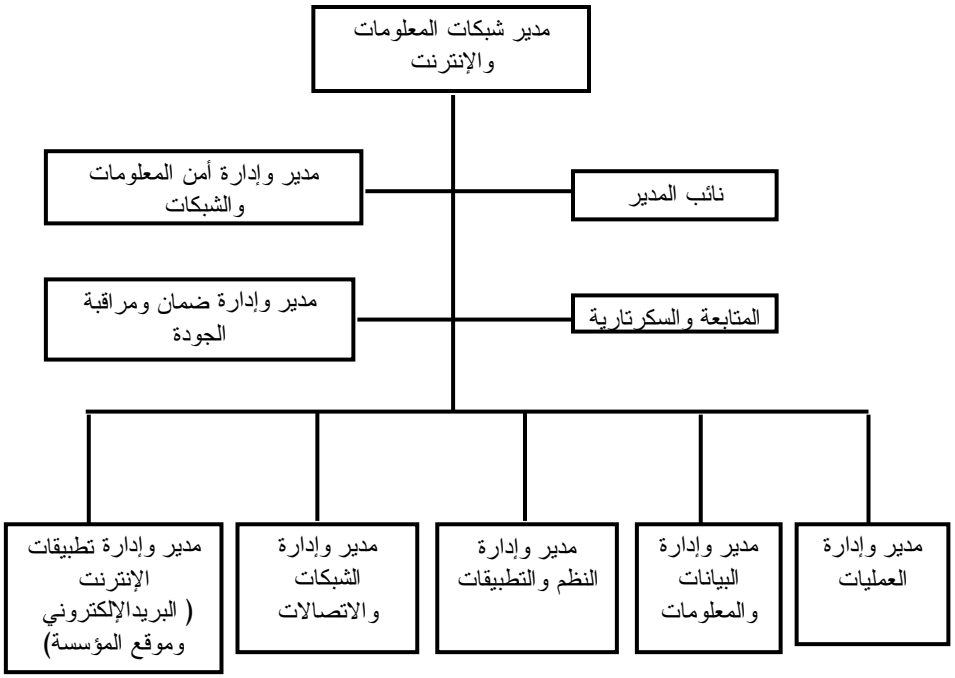
تهدف المؤسسة من خلال تطبيق الهيكل التنظيمي الخاص بها إلى تنفيذ تطبيقات العمل (Business Applications) بالإضافة إلى متابعة المستجدات والتطورات الإدارية والعملية في أنظمة الإدارة المتجددة وبمراعاة الأهداف المشتركة التالية:

- وضع الخطة البشرية والمالية اللازمة سنوياً لتنفيذ مهامها واختصاصات المؤسسة.
- التنسيق فيما بين الإدارات والأقسام المختلفة تخطيطاً وتنفيذاً من خلال تبادل التقارير والمعلومات بصورة مستمرة.
- التطبيق الدقيق لنظام المعلومات والبيانات المؤمن في المؤسسة.
- الاستخدام السليم للأجهزة والمعدات والتقنيات طبقاً للإرشادات الفنية الخاصة "بالسياسة الأمنية" بهدف المحافظة عليها.
- تطبيق مبادئ وأخلاقيات وآليات العمل المعتمدة من إدارة المؤسسة.
- تبنى العلاقات التنظيمية من حيث سلطة الإشراف والمسؤولية على أساس انسياب خطوط الإدارة وتصاعد خطوط المسؤولية في مختلف المستويات الإدارية في الهيكل التنظيمي للمؤسسة.
- تأسيس العلاقة القوية ما بين الوحدات التنظيمية وعلى أساس من التعاون والتشاور والتنسيق الدائم والمستمر.
- تأدية العمل في المؤسسة من خلال كادر مؤهل ومتخصص في كافة مجالات أنشطتها بهدف الارتقاء المستمر بمستوى أداء أعمالها.
- التزام كافة الوحدات والتقسيمات التنظيمية للمؤسسة بجمع وتحليل المعلومات والإحصائيات المتعلقة بأنشطتها كأسلوب علمي وعملي لاتخاذ القرار.
- العمل بصورة جماعية ومن خلال تأسيس فرق عمل منسجمة ومؤهلة تحقق وتخدم الأهداف الرئيسية التي رسمتها المؤسسة ضمن خطة عملها.

ويتم تسكين وإعادة تسكين وتعيين الموظفين المؤهلين والمناسبين على الوظائف الإشرافية المدرجة في الهيكل التنظيمي بقرار من الإدارة العليا وذلك بما يمكن المؤسسة من مباشرة مهامها وأعمالها على الوجه المطلوب وبما لا يتعارض مع لائحة الموارد البشرية الخاصة بالمؤسسة.

الشكل رقم (1) يقدم أحد النماذج الجيدة للهيكل التنظيمي لإدارة شبكات المعلومات والذي يتضمن مجموعة من الإدارات التخصصية من أهمها إدارات: أمن المعلومات والشبكات – مراقبة الجودة – العمليات – النظم – البيانات والمعلومات – الشبكات والاتصالات.

- ينصب اهتمام إدارة العمليات على التنفيذ اليومي لمهام تشغيل النظام ويدخل في مسؤولية القائمين على هذه الإدارة إعداد بيانات المدخلات للتشغيل وتشغيل الحاسبات الآلية والتحكم في المخرجات وتوزيعها عند إتمامها.
- تختص إدارة البيانات والمعلومات وإدارة النظم والتطبيقات بتخطيط احتياجات المؤسسة من البيانات وتحليل تلك البيانات ووضع قاموس للبيانات إضافة إلى إدارة قواعد البيانات بما يشمله ذلك من تخطيط وتصميم وتطبيق وتقويم وصيانة مستمرة. ويعمل محللو النظم والمبرمجين وأفراد العمليات عادة تحت رئاسة مدير معالجة البيانات.
- تختص إدارة الشبكات والاتصالات بتخطيط وتنفيذ وإدارة شبكات العمل بين الحاسبات الآلية في المؤسسة وبعضها البعض إضافة إلى تدبير وصيانة اتصالات حاسبات المؤسسة بالحاسبات خارجها طبقاً لاحتياجات الإدارة.



الشكل رقم (1): أحد النماذج الجيدة للهيكل التنظيمي لإدارة شبكات المعلومات

1) إدارة أمن المعلومات والشبكات تمارس المهام التالية:

- وضع معايير ومقاييس مجالات أمن المعلومات والبيانات والمعدات وشبكات الاتصالات والوثائق.
- متابعة تطبيق المعايير والمقاييس الخاصة بأمن المعلومات وفقاً للمنهجيات المتبعة في المؤسسة.

- إدارة وتوثيق نظم أمن استخدام البرامج والتطبيقات.
- تحديد أساليب وطرق تعريف أسماء الهوية وكلمات المرور لمستخدمي النظم والبرامج والتطبيقات.
- متابعة ومعالجة ثغرات الاختراقات التي قد تحدث على أمن المعلومات أولاً بأول.
- إعداد خطة مواجهة الكوارث بمشاركة الإدارات المختصة بالمؤسسة.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

2) إدارة ضمان ومراقبة الجودة (Quality Assurance)

يقصد بضمان الجودة الأفعال المخططة والمنظمة والضرورية لإعطاء ثقة مناسبة بأن المنتج النهائي والخدمة المعلوماتية التي يؤديها نظام المعلومات والشبكات بالمؤسسة يحقق متطلبات الجودة التي يتطلع إليها جمهور المستفيدين من نظام المعلومات. المسؤولية الرئيسية لهذه الإدارة هي ضمان جودة برامج وبيانات ومعلومات تطبيقات العمل وتوافقها مع المواصفات القياسية العالمية في هذا المجال.

وتمارس إدارة الجودة المهام التالية:

- تتعاون مع باقي الإدارات بهدف التأكد من تنفيذ جميع مهام نظام المعلومات والشبكات طبقا للخطة الموضوعة والمرفقة مع عقود الشركات المنفذة لشبكة المعلومات.
- وضع المعايير والسياسات التي تضمن جودة المنتج النهائي والخدمة المعلوماتية التي يؤديها قطاع المعلومات والشبكات.
- تراجع وتتأكد من المشروعات التي ينفذها قطاع المعلومات والشبكات طبقاً للخطة الموضوعة والمتفق عليها لكل مشروع.
- التأكد من تنفيذ معايير ضمان الجودة خلال مختلف مراحل تنفيذ المشروعات.
- وضع معايير قياس الجودة عند كل مرحلة.
- مراجعة وثائق النظم الحديثة في كل مرحلة للتأكد من تحقيقها لمعايير ضمان الجودة المتفق عليها.
- إبداء النصائح والاستشارات لإدارات العمليات الخاصة بتنفيذ وتطوير وتشغيل تطبيقات العمل فيما يتعلق بضمان الجودة.
- إصدار التقارير والمراجعات والاستفسارات التي تساعد في تقييم جودة المنتج ومدى رضاء المستخدم النهائي عنه.
- تحليل المشكلات وتعريف الأهداف والأغراض واقتراح الحلول والاتفاق على الحلول المناسبة.
- تقييم النتائج – فإذا لم تتحقق الأهداف يتم تحليل المشكلات وإعادة الدورة.
- تطوير خطة التصحيح وتحديد المسؤوليات.
- تنفيذ الخطط، ومراقبة التقدم في تنفيذ الأعمال وحل مشاكل التنفيذ.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

3) إدارة العمليات تمارس المهام التالية:

- تقديم المساندة الفنية لمختلف مراكز التشغيل التابعة للمؤسسة والجهات ذات الصلة وذلك فيما يتعلق بأمور التشغيل وتطبيق النظم.
- وضع وتنفيذ خطط تشغيل الأنظمة والحواسب الآلية وملحقاتها والبرمجيات المساندة لها.
- ضمان استمرارية تشغيل الأنظمة وخاصة المتواجد منها في مراكز التشغيل من خلال استخدام الاحتياطات الفنية اللازمة.
- حفظ النسخ الاحتياطية من المعلومات والبيانات وما يطرأ عليها من تعديل بصورة دورية.
- تغذية البيانات على الحاسبات الخادمة الآلية الرئيسية.
- التشغيل اليومي لأجهزة وبرامج قواعد البيانات وضمان استمرارها.
- متابعة أعمال الصيانة الدورية لتجهيزات غرف الحواسب والخوادم الرئيسية.
- مراقبة عمليات التشغيل اليومية لكافة الأنظمة والبرامج وإخطار الجهات المعنية بأي أعطال أو مشاكل طارئة تواجه عمليات التشغيل.
- تنظيم مناوبات مستمرة بما يتناسب مع حفظ العمل وضمان استمراره وتوفير إجراءات الأمن والسلامة.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

4) إدارة البيانات والمعلومات تمارس المهام التالية:

- تنفيذ وتصميم قواعد البيانات الفعلية بناءاً على التصميم المنطقي المعتمد من المؤسسة.
- إدارة وتغطية قواعد البيانات وتنفيذ التطبيقات الفنية الخاصة بتحقيق مرونة التعديل والإضافة والحذف مع مراعاة سرعة إدارة العمليات واستخراج النتائج المطلوبة بيسر وسهولة.
- المشاركة في اختبار المنهجية وتحديد الأنماط المتوائمة معها.
- تنفيذ إجراءات التأمين والحماية الخاصة بمنح تفويضات استخدام قواعد البيانات للجهات المستفيدة بالتعاون مع إدارة أمن الشبكات والمعلومات.
- توحيد رموز المفاهيم المستخدمة في النظم بقصد تبسيط إجراءات التكامل.
- دراسة المشكلات المتعلقة بتشغيل قواعد البيانات والتطبيقات والعمل على إيجاد وتنفيذ الحلول المناسبة لها.
- وضع مواصفات برمجيات نظم التطبيقات المساندة والمشاركة في تطبيقها.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

5) إدارة النظم والتطبيقات تمارس المهام التالية:

- دراسة المتطلبات من الأجهزة والحاسبات الآلية وملحقاتها بالمؤسسة.
- إعداد المواصفات الفنية الخاصة بالأجهزة والحاسبات الآلية وملحقاتها بالتنسيق مع الإدارات التنظيمية المعنية بالمؤسسة.

- وضع خطة وبرنامج صيانة وإصلاح الأجهزة والحاسبات الآلية وملحقاتها.
- المشاركة في تقييم مواصفات برمجيات نظم التطبيقات الجاهزة.
- دراسة متطلبات الإدارات المستفيدة أو التي ترغب في الاستفادة من نظم ميكنة المكاتب.
- الإشراف على إدخال الوثائق إلى نظم ميكنة المكاتب.
- تركيب الأجهزة والحواسب الآلية وملحقاتها بالتعاون مع إدارة الشبكات والاتصالات.
- المشاركة في تقييم أجهزة وبرامج الاتصالات.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

6) إدارة الشبكات والاتصالات تمارس المهام التالية:

- تركيب وصيانة نظم الاتصالات والشبكات على الحواسب الآلية.
- إدارة ومراقبة شبكات الاتصالات.
- إعداد وتحديث دليل الإجراءات والأنماط الفنية وتقديم أجهزة ووسائل التشغيل والاتصالات.
- تقييم أداء أجهزة وبرامج الاتصالات والشبكات وتقديم التوصيات اللازمة.
- وضع خطط تركيب الشبكات المحلية الداخلية لمواقع المؤسسة والإشراف على تنفيذها.
- وضع التصميمات الضرورية للشبكة الواسعة الخاصة بالمؤسسة وتنفيذها والمحافظة على استمراريتها وتطويرها.
- متابعة وحل مشاكل شبكات الاتصال وخطط نقل البيانات والتجهيزات المتوفرة لدى الشبكات المحلية للجهات المعاونة والأطراف الأخرى.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

7) إدارة تطبيقات الإنترنت تمارس المهام التالية:

- تخطيط وتنظيم وإدارة دخول موظفي المؤسسة على الإنترنت وخدمات استضافة موقع الويب وخدمات البريد الإلكتروني.
- تسجيل أسماء النطاق للمؤسسة بغرض إنشاء موقع الويب على الإنترنت.
- صيانة أنظمة التشغيل والتطبيقات التي تستخدم قواعد البيانات والتطبيقات الأخرى التي لها علاقة بالإنترنت وأخذ نسخ احتياطية للبيانات والمعلومات.
- التأكد من أن أنظمة تشغيل الحاسب الآلي والشبكة وتوصيلات الإنترنت وخدمات البريد الإلكتروني وتطبيقات العمل تعمل 24 ساعة في اليوم و7 أيام في الأسبوع.
- تشغيل مركز لاستقبال شكاوى الموظفين من داخل وخارج المؤسسة والتأكد من حل المشكلة أو تنفيذ التغيير المطلوب.
- أية مهام أخرى ذات صلة بطبيعة عمل الإدارة.

2-4 المهام التفصيلية لإدارة أمن المؤسسة

تنشأ "إدارة الأمن" ضمن الهيكل التنظيمي المساند لأمن شبكات المعلومات بالمؤسسة ليكون مسؤول عن بدء عملية التحكم وتطبيق تأمين المعلومات. تصدق الإدارة العليا للمؤسسة على الشكل الإداري المناسب لهذا الكيان بهدف متابعة تنفيذ السياسة الأمنية وتحديّد أدوار الأمن وتنسيق تطبيق الأمن عبر المؤسسة. إذا دعت الضرورة يمكن الاستعانة باستشاريون متخصصون في النواحي الأمنية لتقديم النصيحة لتأمين المعلومات ضمن المؤسسة. الشكل رقم (2) يوضح أهم مهام "كيان الأمن".

الشكل رقم (2): أهم مهام "كيان الأمن" فيما يخص تأسيس وتنفيذ السياسة الأمنية

تتضمن مسؤولية كيان التأمين الآتي:

- تحديد الأهداف الأمنية: التكامل – الإتاحة – السرية – التحقق من الهوية...
- تقييم الأداء.
- المقارنة المنتظمة للأداء.
- اتخاذ الإجراءات المناسبة لتقريب الفرق بين الأداء والأهداف.
- الإبلاغ عن حالات انتهاك النظام الأمني.
- توفير الاختبارات المتعددة للنظام التي تجعل أي اختراق للأمن يمر بخطوات واختبارات متعددة قبل أن ينجح في تحقيق ذلك.

يفضل أن يكون هناك وسائل اتصال بالمتخصصين في مجال التأمين الخارجيين بهدف تطوير الوسائل الأمنية لمجاراة الاتجاهات التقنية الحديثة ولمراقبة أحدث طرق التقييم والمعايرة الأمنية. ويلزم تزوّيد وسائل اتصال مناسبة بالمتخصصين الخارجين حتى يمكن استشارتهم عند التعامل مع حوادث الأمن.

4-2-1 اللجنة العليا لإدارة تأمين المعلومات

تأمين المعلومات مسؤولية عمل مشتركة من كلّ أعضاء فريق الإدارة ولذلك يتم تشكيل لجنة عليا لتأمين معلومات المؤسسة تتولى كل ما يتعلق بإجراءات التأمين طبقاً لوثيقة السياسة الأمنية. من الضروري أن يكون هناك مدير أو مالك واحد مسؤول عن كلّ نشاط له علاقة بالأمن. من المفضل عقد ورشة عمل أو منتدى أو مؤتمر دوري لإدارة الأمن ليضمن وجود اتجاه واضح ودعم إداري مرئي لمبادرات الأمن. يمكن أن يروج لذلك المؤتمر ضمن المؤسسة بالأسلوب الملائم بهدف إعادة تحديد المصادر التشغيلية للمؤسسة من وجهة نظر التأمين. قد تكون اللجنة العليا لتأمين المعلومات دائمة وضمن الهيكل التنظيمي للمؤسسة.

يكون للجنة العليا لإدارة تأمين المعلومات المهام التالية:

1) المراجعة والموافقة على سياسة تأمين المعلومات والمسؤوليات العامّة.
2) مراقبة المتغيرات الهامّة في تعرّض أصول المعلومات الرئيسية للتهديدات.
3) مراجعة ومراقبة حوادث أمن المعلومات.
4) تقديم مبادرات رئيسية لتحسين أمن المعلومات.

4-2-2 تنسيق جهود تأمين المعلومات

في المؤسسات الكبيرة يفضل إنشاء "كيان وظيفي عابر بين المواقع الإدارية للمؤسسة" يمثل به مختلف الإدارات ذات العلاقة داخل المؤسسة لتنسيق وتطبيق إجراءات التحكم وإدارة تأمين نظام المعلومات. يكون للكيان الوظيفي العابر المهام التالية:

1) الموافقة على الأدوار والمسؤوليات المحددة لتأمين المعلومات على مستوى المؤسسة.
2) الموافقة على وتحديد المنهجيات التي تعالج تأمين المعلومات مثل: إدارة المخاطر وأسلوب ومعايير التصنيف الأمني للمعلومات.
3) الموافقة على ودعم مبادرات تأمين المعلومات في كافة أنحاء المؤسسة مثل: برامج الوعي الأمني.
4) ضمان أنّ التأمين جزء لا يتجزأ من عملية تخطيط المعلومات.
5) تقييم الأداء وتنسيق تطبيق تأمين المعلومات خاصة على الخدمات أو التطبيقات الجديدة التي توفرها المؤسسة.
6) مراجعة حوادث أمن المعلومات على مستوى المؤسسة.
7) وضع وكذلك دعم رؤية واضحة لتأمين المعلومات في كافة أنحاء المؤسسة.

رئيس اللجنة العليا هو المسؤول الأول عن نجاح خطط إدارة تأمين نظام المعلومات.

4-2-3 تحديد مسؤوليات تأمين المعلومات

يتم توضيح المسؤوليات تجاه حماية الأصول التشغيلية بصفة فردية ولتنفيذ عمليات التأمين المحددة. وتزود سياسة تأمين المعلومات بتوجيه عام لتخصيص الأدوار ومسؤوليات التأمين في المؤسسة.

ويفضل عندما يكون ضرورياً أن يستكمل هذا بالتوجيه الأكثر تفصيلاً عن المواقع أو النظم أو الخدمات المحددة التي يشملها التأمين.

يتم تعريف المسؤوليات المحليّة والطبيعية الفردية لأصول المعلومات وعمليات التأمين بشكل واضح وبشفافية مثل تخطيط استمرارية العمل. يتحمل مدير أمن المعلومات المسؤولية الخاصة بتطوير ومراجعة وتطبيق الأمن وكذلك دعم تعريف وسائل الإدارة والتحكم. وتبقى مسؤولية إعادة تحديد المصادر وتطبيق إجراءات التأمين للمصادر الجديدة مع الإدارة العليا للمؤسسة.

من التقاليد الأمنية المعروفة أن يعيّن مالك لكلّ مصدر معلومات ثم يصبح هذا المالك مسؤولاً عن التأمين اليومي للمصدر.

قد يفوض مالكو مصادر المعلومات مسؤوليات التأمين إلى المديرين الفرديين التابعين لهم أو مقدمي خدمة المعلومات والشبكات. على الرغم من هذا يبقى مالك مصدر المعلومات في النهاية هو المسؤول عن تأمين مصدر معلومات المؤسسة الخاص به ويلزم أن يكون قادر على تحديد أيّ مسؤولية تم تفويضها لشخص آخر للتأكد من استخدامها بالشكل الصحيح.

يكون مديري شبكات المعلومات بالمناطق مسؤولين بشكل خاص عن متابعة السياسة الأمنية ويكونوا مسؤولين عن الإبلاغ عن الانتهاكات الأمنية التي قد تحدث في مناطق نفوذهم. بالتحديد من الضروري الأخذ في الاعتبار الآتي:

1) تمييز العلاقة بين الأصول المختلفة وعمليات التأمين لكلّ أصل بطريقة فردية مع ضرورة أن يتم تعريف الأصول ومطالب تأمينها بشكل واضح.
2) أن يتقبل المدير المسؤولية عن كلّ إجراءات الأمن والسرية ويتم توثيق تفاصيل هذه الإجراءات.
3) تكون مستويات تفويض استخدام أصول المعلومات معروفة بشكل واضح وتكون أيضاً موثّقة.

4-2-4 إقرار الوحدات الجديدة لإعداد البيانات

نتيجة للتطور التكنولوجي الحالي ظهرت الوحدات الجديدة الثابتة والمحمولة لإعداد البيانات مثل الحاسبات الشخصية أو المحمولة (شاملاً ذلك الأجهزة الشخصية المتطورة مثل Personnel Digital Assistance PDA, Ruggedized PC, Palm PC, Pocket PC, Tablet PC). لذا يتم تأسيس عملية الإدارة الأمنية عند استخدام تلك الوحدات الجديدة شاملاً ذلك وسائل التحكم التالية:

1) أخذ الموافقة قبل استعمال الوسائل الجديدة على أن تحدد الموافقة وقت ومكان وأسلوب الاستخدام.

2) الحصول على الموافقة من المدير المسؤول عن تأمين نظام المعلومات لضمان التوافق بين سياسات ومطالب الأمن ذات العلاقة.

3) فحص الأجهزة والبرامج المخزنة بوسائل إعداد البيانات لضمان التوافق بينهما وبين باقي مكوّنات النظام الأخرى مع ملاحظة أهمية تنفيذ إجراءات "توافق أو تطابق النوع" من خلال مؤسسات أخرى مرتبطة بالمؤسسة.

4) إعطاء تصاريح خاصة باستعمال وسائل إعداد المعلومات الجديدة مثل الحاسبات الشخصية أو المحمولة لأنها تتطلب وسائل تأمين وسيطرة إضافية. حيث إن استعمال وسائل إعداد البيانات في موقع العمل قد يسبّب نقاط ضعف جديدة ويفتح ثغرات أمنية عديدة لذا يلزم أن يكون ذلك مقيّماً ومصدّقاً عليه.

تزداد أهمية وسائل التحكم هذه خصوصاً في بيئة نظم الحاسبات الموزعة والمرتبطة من خلال شبكات المعلومات الخاصة والعامة خاصة الإنترنت.

5-2-4 استشارة خبراء تأمين المعلومات

يتم الاستعانة بالنصيحة في مجال تأمين شبكات المعلومات من الخبراء والاستشاريين من خلال الاتصال بالعديد من المؤسسات المتخصصة في المجال الأمني.

رغم أهمية الاستعانة بمستشاري تأمين المعلومات المتخصصين إلا أن بعض المؤسسات قد لا ترغب في الاستعانة بالمستشارين الخارجيين. في مثل هذه الحالات نوصي بأن يتم تعيين "خبير تأمين" متميز لتنسيق المعرفة الخاصة بتأمين المعلومات ولضمان التوافق بين مختلف وسائل التحكم الأمنية ولتقديم المساعدة في مجال اتخاذ القرارات الأمنية. رغم ذلك نوصي أيضاً بأهمية الاستعانة بالمستشارين الخارجيين المناسبين لإعطاء النصيحة المتخصصة التي قد تقع خارج نطاق تجربة خبير التأمين المعين.

يكلف مستشارو تأمين المعلومات بمهمّة تقديم النصيحة للتأمين الداخلي والخارجي للمؤسسة ومن الضروري أن تكون هناك وسائل اتصال دائمة ومناسبة بهم.

تزيد فعالية تأمين معلومات المؤسسة عند تنفيذ الآتي:

1) الاستعانة بالخبراء والمستشارين الخارجيين في مجال التأمين والسرية.

2) تحسين أسلوب التعامل السريع للخبراء والمستشارين مع التهديدات الأمنية والنصيحة التي يقدمونها لدعم وسائل التأمين والتحكم.

4) السماح للمستشارين الخارجيين بالوصول المباشر للإدارة في كافة أنحاء المؤسسة لضمان أقصى تأثير إيجابي لهم على تأمين المعلومات والشبكات.

يتم توفير مكان ووسائل اتصال مناسبة بالخبراء والمستشارين الخارجيين من خلال "مسؤول التأمين المعين" داخل المؤسسة للاستعانة برأيهم في أسرع وقت ممكن وفى المرحلة التي تتبع حدوث مشكلة أمنية فعلية أو حدوث اختراق أمني مشتبه به وذلك للاستفادة القصوى من توجيهاتهم ونصائحهم المتخصصة لمجابهه تلك الحوادث الأمنية.

طبقاً للإحصائيات فإن أخطر الحوادث الأمنية تتم من داخل المؤسسات لذلك قد يستعان بالمستشارين الخارجيين عند إجراء التحقيقات في الحوادث الأمنية التي تتم داخل نطاق سيطرة

الإدارة. قد يطلب من مستشارو تأمين المعلومات إبداء النصح والمشورة أثناء إجراء التحقيق في مثل هذه الحوادث الأمنية.

3-4 الأفراد كعنصر أمني لنظام المعلومات

للأفراد دوراً رئيسياً في تأمين نظام المعلومات والشبكات بل يعتبر العنصر البشري من أهم مصادر النظام والسبب الرئيسي لنجاح أو تعطل المؤسسة في تنفيذ أهدافها. فالمخاطر الأمنية مصدرها الأفراد (بقصد أو من غير قصد) والتي قد تؤثر على عمل ومستقبل الأفراد أنفسهم.

بدراسة الهيكل التنظيمي لإدارة شبكات المعلومات (الشكل رقم (1)) يتضح أن المديرين على كافة مستوياتهم وإدارات العمليات والمعلومات والتطوير تتضمن وظائف مثل مدير قواعد البيانات ومدير الشبكات والتطبيقات ومهندسي الصيانة تمنح لصاحبها كلمات مرور وأحقيات دخول عالية على البيانات ومصادر المعلومات. بالإضافة إلى إدارة الأمن التي بها الأفراد المتخصصون في تأمين النظام مثل فرد أو ضابط الأمن والموظفين الآخرين الذين يؤدون مهام الأمن من خلال عملهم. وقد يمثل هؤلاء الأفراد خطراً كبيراً على النظام سواء بقصد أو عن غير قصد.

وأثبتت الإحصائيات والتجارب أن الأفراد الساخطين أو غير الأمناء أو الغير مؤهلين أو المهملين يمثلون نسبة كبيرة من تهديدات النظم وهذه التهديدات يمكن تقليلها إلى درجة كبيرة عن طريق سياسة المؤسسة في إدارة الأفراد.

من الضروري توفير الرعاية الصحية والاجتماعية للأفراد لمنع خطر الإهمال في العمل وسوء استخدام النظام نتيجة الإرهاق وخطر كشف أو تدمير أو فقد المعلومات نتيجة التهديد الخارجي أو الابتزاز أو التواطوء أو التحايل.

ومن المهم أن يدرك الموظفين التهديدات الأمنية التي قد تحدث لنظام المعلومات وأنه من المهم تنفيذ إجراءات "سياسة تأمين النظام" أثناء أدائهم لعملهم اليومي. من الضروري توثيق إجراءات تأمين نظام المعلومات لتحقيق هدفين هما:

- الاستفادة بالخبرات السابقة ونقل المعرفة فيما بين أجيال العمل بالمؤسسة خاصة مع التطور الذي تشهده الآن تكنولوجيا الحاسبات والمعلومات والاتصالات.
- تدريب الأفراد على إجراءات تأمين نظام المعلومات بالاستعانة بهذه الوثائق التي تفيد في شرح سياسة المؤسسة في مجابهة الأخطاء وفى تحديد أسلوب العمل فيما بين الإدارات وشرح ما تم سابقاً من تطوير أو تعديل أو أعمال صيانة للمعدات والبرامج وأخيراً بيان لسياسة ضمان استمرارية العمل تحت ظروف المخاطر والأعطال التي قد يتعرض لها نظام المعلومات.

يشارك المراجعين ومدير قواعد البيانات وأفراد الأمن في تحقيق السياسة الأمنية من خلال إشرافهم ومراقبتهم للأفراد التابعين لهم.

1-3-4 مدير قواعد البيانات

نتيجة لتعقيد مهام إدارة قواعد البيانات فإن السيطرة عليها يجب أن تكون مسؤولية فرد واحد هو "مدير قواعد البيانات" الذي يكون مسؤولاً أمام "الإدارة العليا" عن الأمن والسرية وكفاءة التشغيل وأمن التشغيل بالتنسيق مع "كيان أمن المعلومات".

مدير قواعد البيانات رغم أهمية وجوده يمثل خطراً كبيراً نتيجة تركيز كثير من الوظائف الأمنية الحساسة في يده. تنبع الخطورة الأمنية من حيث إن مدير قواعد البيانات قادر على تعديل البيانات دون معرفة أي فرد آخر لأنه يملك التحكم في كافة الوظائف الفنية. ويجب اختيار مدير قواعد البيانات بعناية فائقة وليس نتيجة للتسلسل الوظيفي فقط. وتشمل سياسة اختيار مدير قواعد البيانات على الآتي:

- دوران الوظائف بمعنى أن الشخص المعين كمدير لقواعد البيانات يتم تغييره بانتظام وفى فترات عشوائية.
- أن يكون هناك مراقب أو مشرف على عمل مدير قواعد البيانات.
- أن يسجل النظام حالات دخول مدير قواعد البيانات إلى البيانات ليتم فحص الحالات بعد ذلك بواسطة المراجعين وبالاستعانة ببرامج التشغيل وبرامج التطبيقات لاكتشاف أي دخول غير مصرح به.

وتمثل برامج إدارة قواعد البيانات DBMS مشكلة لأمن نظام المعلومات حيث إن نفس البرامج تكون مستخدمة بواسطة مؤسسات مختلفة وهناك احتمال أن يكون قد تم اختراقها.

ومن الضروري منع أي مستخدم من خارج النظام من الدخول إليه وذلك بالوسائل الآتية:

- السماح للمستخدمين بالدخول على بياناتهم فقط من خلال وسائل التحقق من الهوية والتحكم في الدخول.
- مراجعة قواعد البيانات بانتظام بواسطة مدير قواعد البيانات والتأكد من إجراءات التأمين وتكامل الملفات.
- تصنيف الملفات والبيانات طبقاً لحساسيتها.
- دخول المستخدمين إلى قواعد البيانات يكون طبقاً لحاجة العمل فقط.

2-3-4 الفنيون والمراجعون لنظام الأمن

تشمل وسائل المراجعة الأمنية لنظام المعلومات الآتي:

- الوسائل والإجراءات الأمنية أثناء التصميم الأولى وتطوير النظم شاملاً ذلك: تأمين التصميم – وسائل التحكم في مصدر البيانات – وسط التسجيل – تصميم النماذج – القوائم الرئيسية – تطبيقات الشبكات – أحقيات الدخول...الخ.
- وسائل وإجراءات تعديل تطبيقات العمل.
- وسائل التحكم التي تهدف إلى التأكد من تحقيق الأهداف المالية والإدارية والقانونية.
- وسائل التحكم للتأكد من كفاءة النظام الأمني ومن كفاءة نظام المعلومات في إنتاج المعلومات الدقيقة الموثوق بها وفي الوقت المناسب.

3-3-4 تدريب الأفراد في مجال تأمين المعلومات

يؤدي تدريب الأفراد إلى رفع مستوى المهارات الخاصة بالوظائف وكذلك المسؤوليات تجاه إدارة أمن المؤسسة. ويراعي ألا تتعدى نسبة عدد ساعات العمل إلى عدد ساعات التدريب عن النسب القياسية المقررة مسبقاً. وتتنوع اتجاهات التدريب والوعي الأمني لتشمل:

- المهارات الأمنية للتغلب مثلاً على حالة حدوث حريق.
- احتياطيات الأمن.
- الاستجابة للمتغيرات الأمنية متضمناً كيفية الإبلاغ عن حدث أمني والتغلب على تأثير حدث أمني واسترجاع الجزء من النظام الذي تعرض للحادث الأمني إلى حالته الطبيعية.
- إجراءات التأمين والاستعمال الصحيح لوسائل إعداد البيانات خاصة الحديثة منها والتي قد تعمل عن بعد وذلك بهدف تقليل المخاطر الأمنية المتوقعة.

يجب أن يتلقى الموظفون وممثلي الجهات التابعة التدريب الملائم والمتطور والمتجدد على إجراءات "السياسة الأمنية". يشمل هذا التدريب على مطالب التأمين ووسائل السيطرة على تنفيذ العمل والمسؤوليات القانونية بالإضافة إلى التدريب الأمني على الاستعمال الصحيح لوسائل إعداد البيانات.

ومن المهم أن يتم هذا التدريب للموظفين خاصة الجدد قبل السماح لهم بالدخول إلى البيانات ومصادر المعلومات.

يهدف التدريب في مجال التعامل مع الحوادث الأمنية إلى:

- تقليل الضرر من الحوادث التي قد تعطل جزئياً أو كلياً نظام المعلومات.
- اكتساب المهارات الخاصة بالمراقبة والتعلّم واكتساب الخبرة في مواجهة هذه الحوادث.
- التدريب على الإبلاغ الفوري عن الحوادث التي تؤثّر على الأمن من خلال قنوات الإدارة الملائمة وفى أسرع وقت ممكن.
- تنبيه الموظفين وأفراد الجهات المتعاقدة إلى أهمية الإجراءات الخاصة بكتابة تقارير الأنواع المختلفة من الحوادث الطارئة (مثل اختراق أمني أو ضعف أو تهديد أو عطل) ذلك لاحتمالية أن يكون للحوادث الطارئة تأثير سلبي على تأمين أصول المؤسسة المعلوماتية.
- الإسراع بإبلاغ مدير نظام المعلومات ونقطة الاتصال الأمني المحددة بالمؤسسة (مثل كيان الأمن) عن أيّ حوادث ملاحظة أو مشتبه بها وذلك بأسرع ما يمكن.
- تنفيذ إجراءات تأديبية رسمية للتعامل مع الموظفين أو المقاولين الذين يرتكبون المخاطر والاختراقات الأمنية.
- الإبلاغ الفوري عن الحوادث الأمنية يؤدي إلى سرعة التعامل معها وتجميع الأدلة وتقليل الخسائر التي قد تحدث لنظام معلومات المؤسسة وللمؤسسة بالكامل.

كتابة تقارير نقطة ضعف أمني:

- من المهم تدوين أي ملاحظة أو تهديد أو اشتباه عن أيّ نقاط ضعف أمني قد تسبب مخاطر لنظام معلومات المؤسسة ويتم الإبلاغ عنها.
- من الضروري أن يدرك المستخدمين للخدمات المعلوماتية بأن إبلاغهم عن الحوادث الأمنية إمّا إلى إدارتهم أو مباشرة إلى كيان تأمين المؤسسة هو لحمايتهم من أي ضعف أو تهديد حيث إن نتيجة اختبارات ضعف في النظام الأمني قد تؤدي إلى وتترجم على اتهامهم بالتواطؤ أو سوء استعمال محتمل لمصادر نظام المعلومات.

مسؤولية الإدارة العليا والإدارة المتوسطة:

من أهم مسؤوليات الإدارة العليا والمتوسطة المعرفة الكاملة بالموظفين التابعين لهم بما يكفل لهم ملاحظة أي تغيير في سلوكهم. وتقع المسؤولية النهائية للأمن على عاتق الإدارة العليا والمتوسطة لذا يلزم مشاركتهم في:

- وضع السياسة الأمنية للمؤسسة ومتابعة تنفيذها.
- وضع خطط تحويل السياسة الأمنية إلى إجراءات وتعليمات واضحة يمكن فهمها بحيث تكون قابلة للتنفيذ.
- توفير التدريب المستمر للأفراد التابعين.

إن البنية المتكاملة لتكنولوجيا شبكات المعلومات والمشاريع المعلوماتية المختلفة التي أنشأت في المؤسسات على مستوى الدولة والتي زادت كلفتها عن مئات الملايين من الجنيهات تعتبر "ثورة قومية" ولا بد وأن تحظى بدعم متواصل لتأمينها وصيانتها واستمرارية تشغيلها. وهذا يعني أنه لا بد من وضع خطة لحمايتها من جميع المخاطر المحتملة سواء كانت طبيعية أو منطقية.

وهذا يتم من خلال توفير الكوادر الفنية المؤهلة التي تشغل الهيكل التنظيمي المساند للأمن طبقاً للمهام التي تمت الإشارة إليها في هذا الفصل. وكذلك توفير الأجهزة الفنية والبرامج والشبكات ووسائل التأمين والحماية اللازمة التي تتمكن من المحافظة على هذه الثروة.

الفصل الخامس

التشفير والنظم الشفرية

1-5 المطالب الأمنية التقنية لتأمين البيانات

تتكون بنية شبكات المعلومات من معدات الحاسبات الآلية وقواعد البيانات وبرامج النظام وبرامج التطبيقيات الجاهزة والبرامج التي تم تطورها بواسطة مبرمجي النظام. ويتم الربط بين كل العناصر بواسطة شبكات الاتصال. وتعتبر أنشطة التصميم والبناء والبرمجة لتطبيقات العمل حاسمة لأمن نظام المعلومات خاصة إذا تم الأخذ في الاعتبار مطالب التأمين منذ التنفيذ الأولى للمشروع وعند تطوير مكونات النظام ذات درجة التأمين العالية شاملاً ذلك تطبيقات العمل والتقارير والشبكات والبريد وموقع المؤسسة على الإنترنت. كما يلزم تحديد مطالب تضمين التأمين والتصديق عليها من قبل الإدارة العليا قبل تطوير نظام المعلومات.

وكما سبق إيضاحه في الفصول السابقة تنقسم المطالب الأمنية التقنية لتأمين البيانات إلى ثلاثة أقسام رئيسية هي:

1) التحكم في الدخول للنظام بوسائل التعرف على الهوية وصلاحيات الدخول.
2) التحكم في تدفق البيانات بتصنيف البيانات إلى مستويات تأمين طبقاً لدرجة حساسيتها لتطبيقات العمل بالمؤسسة.
3) التشفير.

ولضمان عدم إخفاق وسائل التحكم في الدخول والتحكم في تدفق البيانات فمن الضروري التوسع في استخدام نظم التشفير مع البيانات المتداولة عبر الشبكات ومع البيانات المخزنة في أوساط التخزين حيث يجعل التشفير تلك البيانات مجهولة إلا للمصرح له فقط والذي يمتلك مفتاح وخوارزم فك التشفير.

2-5 تدقيق الرسائل

تدقيق الرسائل تقنية تستعمل لكشف التعديلات غير المصرح بها على محتوى الرسائل الإلكترونية المتداولة أو لكشف أي فقد أو تلف في تلك الرسائل. يمكن تطبيق التدقيق عن طريق معدات أو برامج آلية تستخدم بروتوكولات لاكتشاف الأخطاء وتصحيحها وتساند وسائل تستخدم للتحقق الطبيعي من صحة الرسالة. كما تستخدم النظم الشفرية للتأكد من صحة الرسائل وعدم تعرضها للكشف أو التعديل أثناء انتقالها عبر الشبكات. ومن أشهر النظم الشفرية خوارزم "دليل الرسالة" Message Digest or Signature والتشفير غير المتماثل التي سيتم الإشارة إليهما بالتفصيل في البنود التالية.

يتم التحقق من صحة الرسائل التي تتصل مباشرة بتطبيقات العمل الإلكترونية (شاملاً ذلك التجارة الإلكترونية والحكومة الإلكترونية والتعليم عن بعد) حيث إن هناك مطالب تأمين لحماية نزاهة محتوى هذه الرسائل شاملاً تلك التطبيقات ذات الطبيعة الهامة مثل المدفوعات المالية الإلكترونية ووثائق المواصفات والعقود والعروض الفنية الإلكترونية (E-Tenders) وتطبيقات تداول بيانات إلكترونية أخرى مماثلة.

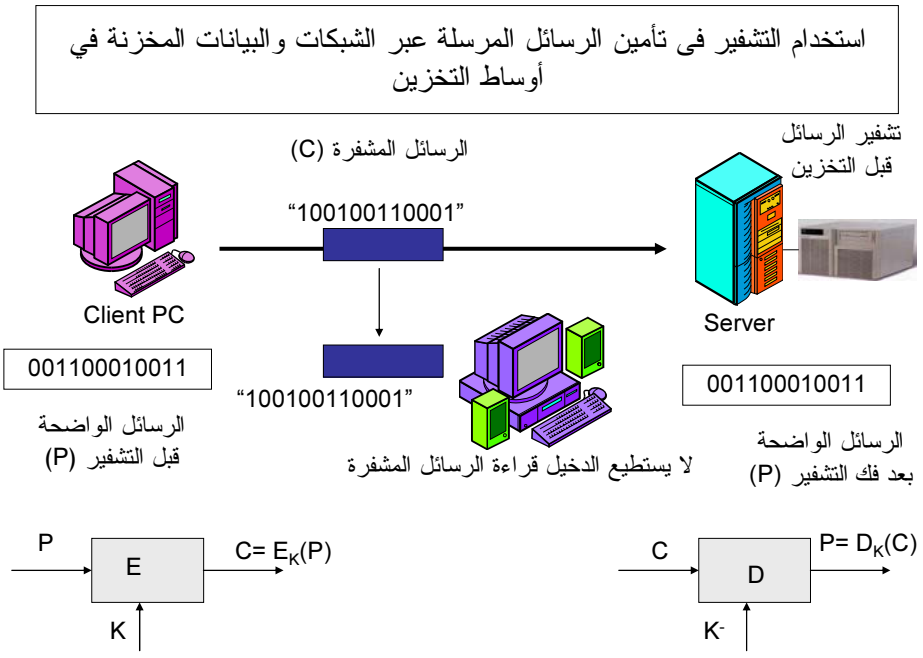
من المهم تطوير وتقييم وسائل التغلب على مخاطر تداول الرسائل باستمرار لتوضيح أهمية استخدام نظام تدقيق وتأمين الرسائل ولتحديد أنسب الوسائل لتطبيق هذا النظام.

تدقيق الرسائل بصورتها الواضحة قد يكون ضروري ولكنه غير كاف للحماية ضد خطر اختراق النظم التفاعلية أو للتأكد من أن محتويات الرسائل لم يتم كشفها أثناء تداولها عبر الشبكة لغير المصرح لهم. لذا فمن الضروري تطبيق واستخدام النظم الشفريّة كوسيلة فعالة للتأكد من صحّة الرسائل وهوية مرسليها.

3-5 التشفير

يهدف التشفير إلى حماية السرية والأصالة والنزاهة للبيانات التي قد تتعرض للمخاطر والتي لا يوجد لها وسائل حماية أخرى خلاف التشفير. ومن المعلوم وكما سبق الإشارة إليه في الفصل الثاني أن الإنترنت شبكة مدنية تجارية ولذلك هي وبالهدف من إنشائها غير مؤمنة بطبيعتها رغم أنها تشكّل في هذه الأيام الوسطَ الأضخم والأكثر انتشاراً والأقل تكلفة لنقل المعلومات. لذلك يلزم تداول المعلومات الحساسة (مثل الحركَات المالية) على الشبكات وخاصة الإنترنت بصيغة مشفَّرة إن أريدَ الحفاظ على سلامتها وتأمينها من عبث المتطفلين والمخربين واللصوص.

الشكل رقم (1) يوضح استخدام نظم التشفير مع الرسائل المتداولة عبر الشبكات ومع البيانات المخزنة في أوساط التخزين.



الشكل رقم (1): استخدام نظم التشفير مع الرسائل المتداولة عبر الشبكات ومع البيانات المخزنة في أوساط التخزين.

يعتمد التشفير في الإرسال على تحويل الرسالة الواضحة (Plain text P) إلى رسالة مشفرة (Ciphered text C) باستخدام خوارزم التشفير (E) ومفتاح التشفير (K) وبالتالي يمكن كتابة المعادلة $C=E_K (P)$ بمعنى أن الرسالة المشفرة هي ناتج تطبيق خوارزم الشفرة E على الرسالة الواضحة P باستخدام مفتاح التشفير K– وبالتالي لا يتمكن الدخيل من الحصول على الرسالة الواضحة C طالما لا يمتلك خوارزم التشفير E ولا مفتاح التشفير K.

ويعتمد التشفير في الاستقبال على تحويل الرسالة المشفرة (Ciphered text C) إلى الرسالة الواضحة (Plain text P) باستخدام خوارزم إعادة التشفير (D) ومفتاح إعادة التشفير (K^-) وبالتالي يمكن كتابة المعادلة $D=D_{K^-} (C)$.

ويلاحظ أن مفتاح التشفير (K) ومفتاح إعادة أو فك التشفير (K^-) يكونا متساويين في التشفير المتماثل ويكونا غير متساويين (ولكن بينهما علاقة رياضية) في التشفير غير المتماثل.

[المراجع أرقام (26 و27 و40 و41 و56 و57 و60 و68)].

1-3-5 سياسة التعامل مع أنظمة التشفير

اتخاذ القرار المتعلق باستخدام وانتقاء أنظمة التشفير المناسبة لتطبيقات العمل يمكن اعتباره من أهم أنواع القرارات التي تشملها سياسة "تقدير وإدارة المخاطر" في المؤسسة حيث يتم انتقاء مستوى الحماية المناسبة للبيانات ومصادر المعلومات ضمن تقدير وإدارة المخاطر.

تستخدم قرارات "تقدير وإدارة المخاطر" للإجابة على التساؤلات التالية: هل توجد جدوى من استخدام النظم الشفرية؟ وما الأنواع المناسبة من النظم الشفرية التي يمكن استخدامها؟ وما هي وسائل التحكم اللازمة عند تطبيقها؟ ولأي هدف ولأي بيانات عمليات تشغيل يتم استخدام النظم الشفرية؟ هل تستغل النظم الشفرية أثناء تداول البيانات عبر الشبكات الواسعة فقط أم يتم تشفير جميع البيانات بما فيها المرسلة عبر الشبكة المحلية أيضاً؟ وهل من الأفضل تخزين البيانات بصورة مشفرة داخل أوساط التخزين؟ وأخيراً هل يكتفي باستخدام النظم الشفرية التجارية أم من المناسب التطوير الذاتي لتلك النظم؟

من المفيد أن تطور المؤسسة "السياسة الأمنية" الخاصة بها من خلال استغلالها الأمثل لوسائل التحكم الشفريّة لحماية معلوماتها. هذه السياسة ضروريّة لتعظيم الاستفادة من نظام المعلومات في تحقيق الأهداف وتقليل التهديدات الأمنية والتغلب عليها ومنع الاستخدام غير المصرح به للبيانات ومصادر المعلومات. وبالتالي إعطاء ثقة لمتخذ القرار في النظام.

عند تطوير سياسة التعامل مع أنظمة التشفير يؤخذ في الاعتبار العوامل التالية:

1) خطة الإدارة نحو استعمال وسائل التحكم الشفريّة عبر المؤسسة بما في ذلك المبادئ العامّة التي من خلالها يتم حماية نظام المعلومات.
2) خطة استخدام وإدارة المفاتيح الشفرية بما في ذلك طرق استرجاع المعلومات المشفرة في حالة فقدها وكذلك التعامل مع المفاتيح الشفرية التي فقدت أو تم فك سريتها (خطة استعادة مفاتيح التشفير (Key Recovery)).
3) كيفية تحديد الأدوار والمسؤوليات الخاصة بالنظم الشفرية بمعنى تحديد من يكون مسؤول عن ماذا؟
4) كيفية تنفيذ السياسة الأمنية لاستخدام النظم التشفير.

5) كيفية تحديد مستوى الحماية الشفرية المناسبة للمعلومات والتقارير.

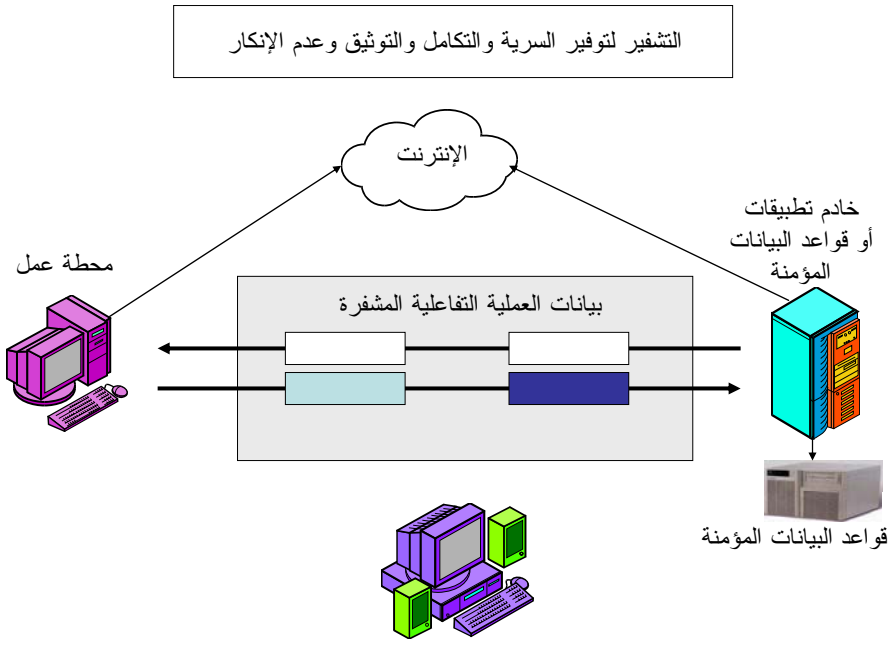
6) المعايير والمقاييس التي على أساسها يتم تنفيذ الحماية الشفرية على نطاق تأمين المعلومات خلال المؤسسة (أيّ تحديد الحل الذي تم اختياره لتشفير بيانات تطبيقات العمل).

7) كيفية الاستفادة من مشاريع الأنظمة الشفرية الحديثة مثل بنية المفتاح العام (Public Key Cryptography (PKI)) التي توفر التوقيع الإلكتروني وشهادات التوثيق من جهات التوثيق الجذرية والحكومية.

[المراجع أرقام (23 و29 و30 و31 و32 و33 و35 و40 و42 و53 و63)].

2-3-5 المصطلحات الخاصة بالتشفير

* التشفير: هو تحويل البيانات من صورة واضحة مفهومة إلى صورة غير مفهومة بطريقة محددة. الطريقة تسمى خوارزم التشفير وهي عبارة عن عملية تحويل رياضي أو منطقي معقدة ولكن قد تكون الطريقة معلنة وغير سرية ولكن تكمن السرية في المفتاح الشفري ونظام إدارة المفاتيح الشفرية. وتعتبر الوسائل الشفرية (إذا أحسن استغلالها واعتمدت على خوارزميات تشفير وطنية) أفضل وسائل تحقيق السرية والتكامل والتوثيق وعدم الإنكار للبيانات على الإطلاق وتقاوم أعمال التصنت والاحتيال والخداع كما في الشكل رقم (2).



المتداخل: غير قادر على التصنت أو الاحتيال أو الخداع أو الاختراق نتيجة تشفير البيانات

الشكل رقم (2): التشفير لتوفير السرية والتكامل والتوثيق وعدم الإنكار

وتعتمد قوة أو درجة سرية تقنية التشفير على ثلاثة عناصر هي:

1) طول المفتاح الشفري.

2) طريقة أو خوارزم التشفير.

3) أسلوب إدارة المفاتيح الشفرية.

* استخراج الشفرة: هي عملية إعادة البيانات المشفرة غير المفهومة إلى أصلها الواضح من قبل الأفراد المصرح لهم ويتم ذلك باستخدام طريقة أو خوارزم معاكس للتشفير وباستخدام مفتاح خاص (مفتاح فك الشفرة).

تحليل أو كسر الشفرة: عملية تتم بواسطة الأفراد أو الجهات غير المصرح لهم (الدخلاء) للحصول إما على البيانات الواضحة أو لمعرفة المفتاح الشفري. وقد يستخدم فيها النص المشفر للتوصل إلى النص الواضح أو قد يستخدم المفتاح الشفري بدون معرفة مسبقة بالنص الواضح أو بالمفتاح الشفري ولكن بالتقاط النص المشفر فقط، وربما بمعرفة طريقة التشفير.

ومن الممكن استخدام أحد الوسائل الآتية لفك الشفرة:

1) التحليل الرياضي.
2) الطرق الإحصائية اعتماداً على معدل تكرار الحرف الواحد ومجموعة الحروف للغة المكتوب بها الرسالة.
3) سرقة المفاتيح.
4) شراء الذمم من خلال الجواسيس والمتواطئين.

* وسائل أو خوارزميات التشفير: في الماضي انحصر استخدام التشفير في المجالات العسكرية والدبلوماسية فقط. أما حالياً فتستخدم وسائل التشفير في مجالات مختلفة ومن قبل الجهات الأمنية والجهات الحكومية والمدنية (الصناعية والتجارية والمالية والتلفزيونية وشركات مزودي خدمة الاتصالات) والأفراد. في الماضي انحصر استخدام التشفير في تأمين الرسائل فقط. أما الآن فيستخدم التشفير في تأمين جميع أنواع الإشارات شاملاً ذلك إشارات الصوت والصورة والرسائل. وفي الماضي استخدم التشفير لتحقيق السرية فقط. أما الآن فيستخدم لتحقيق السرية والأصالة (أي ضمان صحة مصدر الرسائل ومحتوياتها) وعدم الإنكار من خلال نظم التوقيع الإلكتروني وشهادات التوثيق.

وتنقسم وسائل التشفير لنوعين هما التشفير المتماثل حيث يكون مفتاح التشفير = مفتاح فك التشفير والذي ينقسم إلى نوعين هما تشفير متماثل متوالي نبضة بنبضة (Stream ciphers) وتشفير متماثل بمجموعة أو كتلة البيانات (Block Ciphers). وأشهر الخوارزميات العالمية المتماثلة بمجموعة البيانات هي DES، 3DES، IDEA، AES، ...إلخ.

والنوع الآخر من خوارزميات التشفير هو غير المتماثل حيث يكون مفتاح التشفير ≠ مفتاح فك التشفير ولكن بينهما علاقة رياضية تضمن أن لكل مفتاح تشفير مفتاح فك تشفير واحد فقط. ويوجد أشهر خوارزميات العالمية للتشفير غير المتماثل مثل:
RSA- EL GAMAL- PGP- Fiage Fiat Shamir

الأنظمة الشفرية: ويقصد بها الأنظمة التي تشفر حزم البيانات عند مستوى معين من مستويات البنية المعمارية للحاسبات والشبكات أو بروتوكول IP طبقاً للجدول التالي: (وسوف يتم تناول خصائص بعض هذه الأنواع في هذا الفصل).

[المراجع أرقام (26 و27 و40 و41 و56 و57 و60 و68)].

مستوى بروتوكول IP	الأنظمة الشفرية
التطبيقات (Application)	Kerberos, RADIUS Dial-Up Remote Access
النقل (Transport)	SSL/TLS: Secure Socket Layer/Transport Layer Security SET: Secured Electronic Transactions
الإنترنت (Internet)	IPsec: Internet Protocol Security
التحكم في المحور (Data Link)	PPTP Point to Point Tunneling Protocol , L2TP: Layer 2 Tunneling Protocol
الربط الطبيعي (Physical)	تشفير نهاية بنهاية أو تشفير حزمي

* التوقيع الرقمي (الإلكتروني): قد تحتوي الرسائل المتداولة عبر الشبكة على أوامر خاصة أو تعليمات مهمة مثل طلب صرف شيكات أو تحويل أموال من حساب شخص إلى حساب شخص آخر أو إصدار أوامر الشراء والفواتير خاصة في تطبيقات التجارة الإلكترونية. في هذه الحالة يلزم إثبات صحة الرسائل والوثوق فيها وعدم إنكارها. لذلك يستخدم التوقيع الرقمي للتحقق من صحة المعلومات (الحماية من التحريف والتزوير الخارجي). ولتأكيد أصالة المصدر (الحماية من الادعاء والانتحال) ولضمان أن المستقبل للبيانات لم يقوم بتزويرها أو تعديلها. ويتم أيضاً استخدام التشفير كدليل لدقة الرسائل وكذلك لضمان التزام المرسل والمستقبل وعدم إنكار الإرسال والاستقبال للرسائل.

* شهادات التوثيق: الشهادات هي عبارة عن ملفات مشفرة يتم تخزينها على وحدة مثل الكارت الذكي المغناطيسي (Smart Card) أو العملة الإلكترونية (Token) وتستخدم الشهادات مع الأفراد والمؤسسات والمواقع والبرامج والحاسبات الخادمة لتطبيق ما. وعادة يتم الحصول على الشهادات وتسجيلها من خلال طرف ثالث (جهات توثيق الشهادات الحكومية أو الجذرية) لضمان صحة تداول وتوقيع وتسجيل العمليات المالية والتفاعلات الإلكترونية الأخرى مثل التجارة الإلكترونية والتعليم الإلكتروني وخدمات الحكومة الإلكترونية.

على سبيل المثال يمكن تسجيل الشهادة على حاسب خادم الموقع الخاص بالمؤسسة وبعد ذلك تتصل الملفات المخزن بها شهادات توثيق الموقع بمتصفح العميل بمجرد دخوله لتؤكد له أن الموقع الذي تم الدخول عليه هو بالفعل موقع المؤسسة.

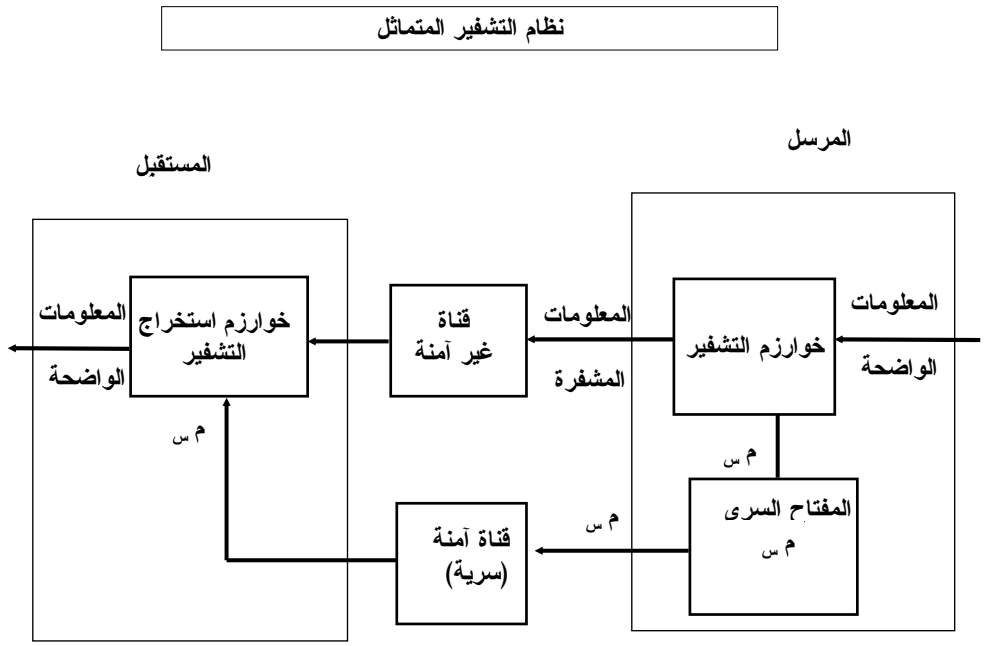
كما تستخدم الشهادات للتأكد من هوية الأفراد الذين يتصلون بالشبكات الخاصة بالمؤسسة سواء كانوا داخل أو خارج أماكن عملهم. وفى هذه الحالة قد توفر شهادة لشخص محدد سيقوم فيما بعد بتخزين الملف على حاسبه الشخصي وعندما يكون الشخص داخل نطاق عمل نظام المؤسسة ستبحث وحدة الخدمة عن الشهادة قبل السماح له بالدخول.

* أنواع التشفير: كما ذكرنا آنفاً يوجد وسيلتين رئيسيين للتشفير هما:

1) وسائل التشفير المتماثلة (ذات المفتاح السري الواحد):

- وفيها مفتاح التشفير (م ت) يساوي مفتاح فك التشفير (م ف) وكل منهما سري (م س) أي إن (م ت = م ف = م س)

والشكل رقم (3) يوضح أسلوب تنفيذ نظام التشفير المتماثل على البيانات الواضحة عند المرسل ثم إرسالها مشفرة عبر الشبكة بعد حمايتها من المتداخلين ثم إعادة استخراج البيانات الواضحة عند المستقبل.



الشكل رقم (3): نظام التشفير المتماثل

يستخدم التشفير المتماثل في ضمان سرية المعلومات (عدم التحريف) كما يستخدم في تشفير الاسم وكلمات المرور وعند تخزين المعلومات على أوساط التخزين.

من أهم مزايا التشفير المتماثل السرعة العالية في تنفيذ التشفير في الزمن الحقيقي ودرجة السرية العالية لخوارزم ومفتاح التشفير. ومن أهم عيوب التشفير المتماثل صعوبة إدارة المفاتيح الشفرية.

2) وسائل التشفير غير المتماثلة (ذات المفتاحين أو التشفير العلني العام):

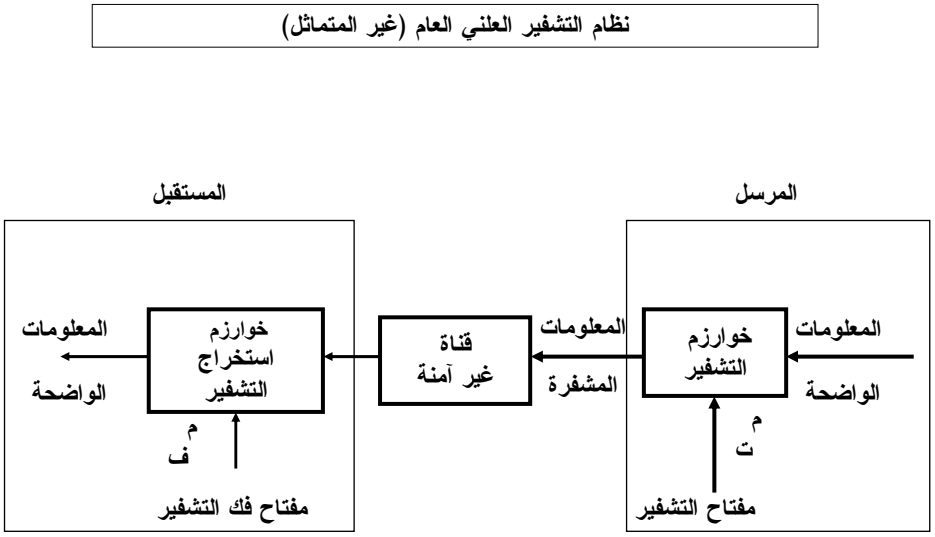
يستخدم فيها مفتاح للتشفير لا يساوي مفتاح فك الشفرة ولكن بينهما علاقة رياضية معقدة تضمن أن لكل مفتاح تشفير مفتاح فك شفرة واحد فقط. ويستخدم التشفير غير المتماثل في ضمان التوثيق والتكامل وعدم الإنكار للرسائل المرسلة والمستقبلة. والمفاتيح السرية والعلنية هي كالآتي:

- المفتاح السري (م ت = م س أو م ف = م س): ربما يستخدم كمفتاح التشفير أو كمفتاح فك الشفرة "سري".

- المفتاح العمومي أو العلني الغير سري (م ف = م ع أو م ت = م ع) ربما يستخدم أيضاً كمفتاح التشفير أو كمفتاح فك الشفرة "علني".
- بمعنى أن المفتاح الأول سري: م ت= م س أو م ف = م س

  والثاني علني: م ف = م ع أو م ت = م ع

الشكل رقم (4) يوضح أسلوب تنفيذ نظام التشفير غير المتماثل:

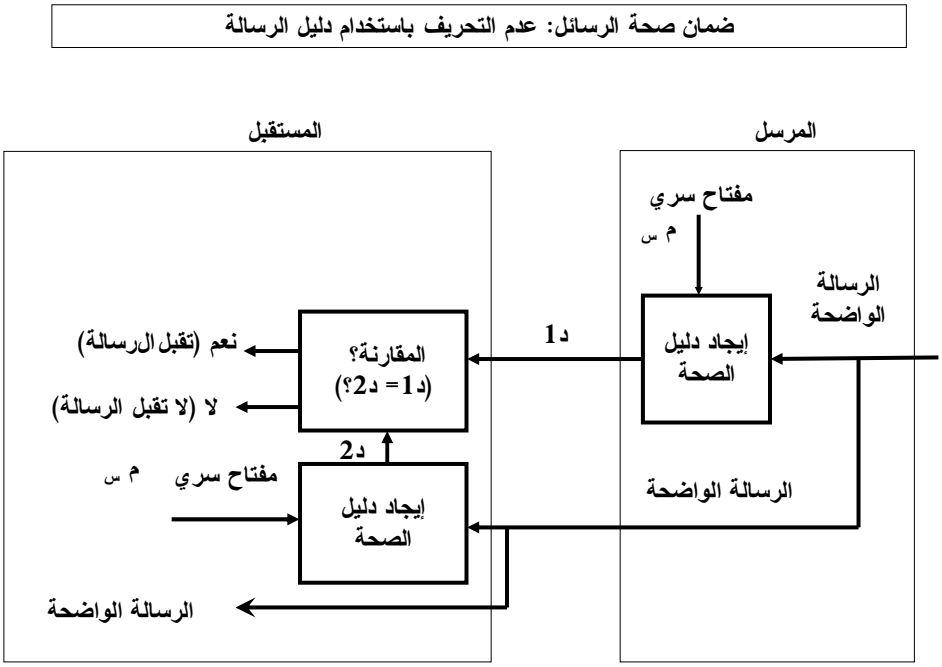


الشكل رقم (4): نظام التشفير غير المتماثل

* خوارزم التشفير أحادي الاتجاه (One way encryption) :

هو أسلوب من أساليب التشفير يهدف إلى إنتاج "دليل الرسالة Message Digest or Signature" حيث تؤخذ الرسالة المراد تدقيقها أو تشفيرها ويتم تحويرها بواسطة خوارزم التشفير (Hash function) والناتج يسمى دليل الرسالة أو المفتاح الشفري (Hash Key). وأهم ما في هذا المفتاح هو أنه لا توجد طريقة لفك التشفير والحصول على الرسالة الأصلية منه ولهذا السبب سمي هذا الأسلوب بأسلوب التشفير آحادي الاتجاه. ومن أشهر خوارزميات "الهاش" المستخدمة حالياً ((Message Digest-5 (MD5)). كما يعتبر خوارزم (Standard Hashing Algorithm 1 (SHA1)) هو خليفة MD5 وقد بدأت بعض الأنظمة الشفرية بالانتقال تدريجياً لاستخدامه. وقد نتساءل عن الحاجة لتشفير البيانات في اتجاه واحد وبدون مفتاح شفري إذا لم نكن قادرين بعد ذلك على فك تشفيره؟ لكن هذا الأسلوب من أساليب التشفير هو في الواقع أكثر الأساليب تأميناً واستخداماً. وهو يستخدم في تشفير الاسم وكلمات السر ومع الأنظمة التي تحتاج للتحقق من صحة معلومات ما دون الحاجة لمعرفة فحوى هذه المعلومات – وذلك لأن تشفير نفس الرسالة بنفس الخوارزم ينتج الدليل أو مفتاح الشفرة نفسه في كل مرة.

الشكل رقم (5) يوضح استخدام كلا من خوارزم "دليل الرسالة Message Digest or Signature" والتشفير غير المتماثل في التأكد من صحة المعلومات.

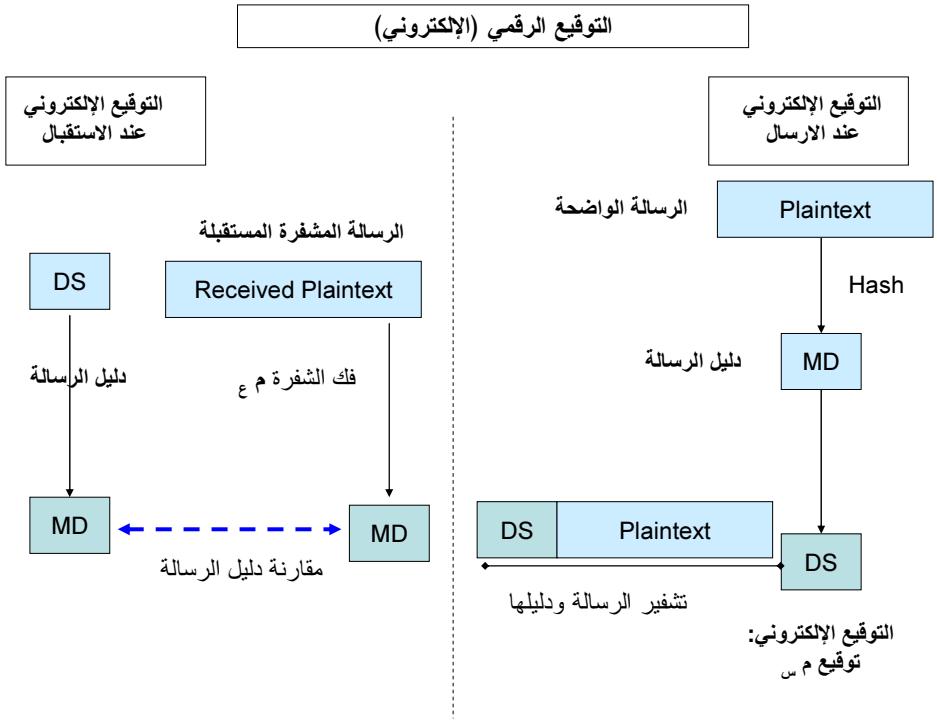


الشكل رقم (5): ضمان صحة المعلومات باستخدام دليل الرسالة والتشفير غير المتماثل

طبقاً للشكل رقم (5) فإن المرسل يشفر الرسالة باستخدام خوارزم التشفير أحادي الاتجاه "خوارزم الدليل" أو "الهاش" (Hash Function) لإنتاج دليل الرسالة (Message Digest (MD)) المرسلة "د1" وهذا الدليل له علاقة بمحتويات الرسالة بحيث إذا تغيرت المحتويات بالحذف أو التعديل ينكشف هذا بواسطة الدليل.

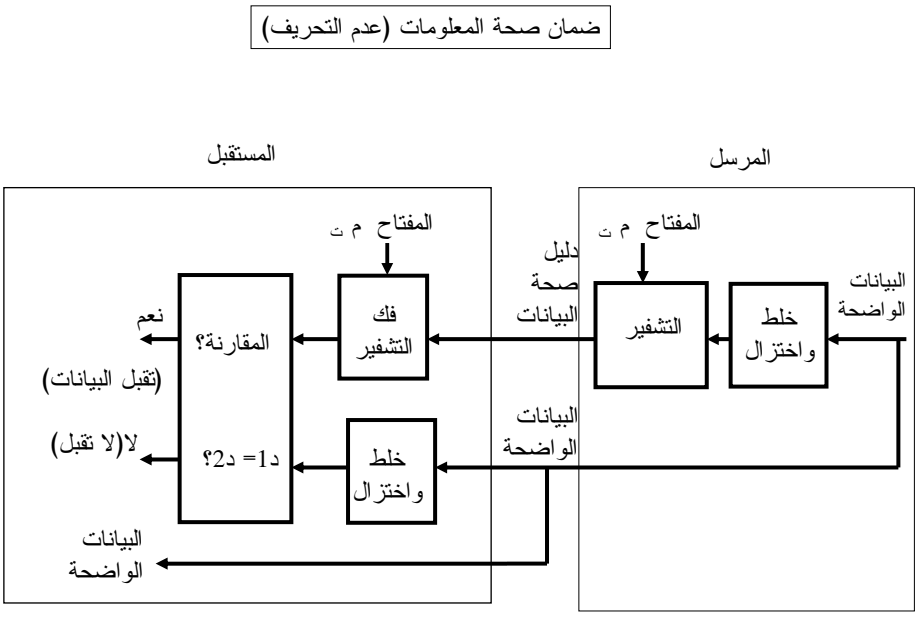
ويشفر المستقبل الرسالة (بعد عبورها شبكة الاتصال) بنفس خوارزم التشفير لإنتاج دليل الرسالة المستقبلة "د2". تكون الرسالة سليمة إذا تساوت "د1" مع "د2". وفيما عدا ذلك يتم رفض الرسالة وطلب إعادة إرسالها مرة أخرى.

يطلق على الدليل "التوقيع الإلكتروني للرسالة" (Message Authentication Code (MAC)) حيث يكون خوارزم الدليل ومفتاح وخوارزم التشفير ضمن مكونات شهادة التوثيق والتوقيع الإلكتروني ومخزنة على الكارت الذكي الذي يمتلكه المرسل ويعلم عنه المستقبل وذلك طبقاً للمواصفات القياسية X.509 التي وضعها الاتحاد الدولي للاتصالات (ITU) [المرجع رقم (42)] والتي تعتبر الأساس في استخدام بنية المفتاح العام في إنتاج شهادات التوثيق والتوقيع الإلكتروني. والشكل رقم (6) يوضح كيفية استخدام الدليل والتوقيع الإلكتروني وخوارزميات التشفير غير المتماثلة في تشفير كل من الرسالة الواضحة ودليلها أثناء تداولهم عبر الشبكة.

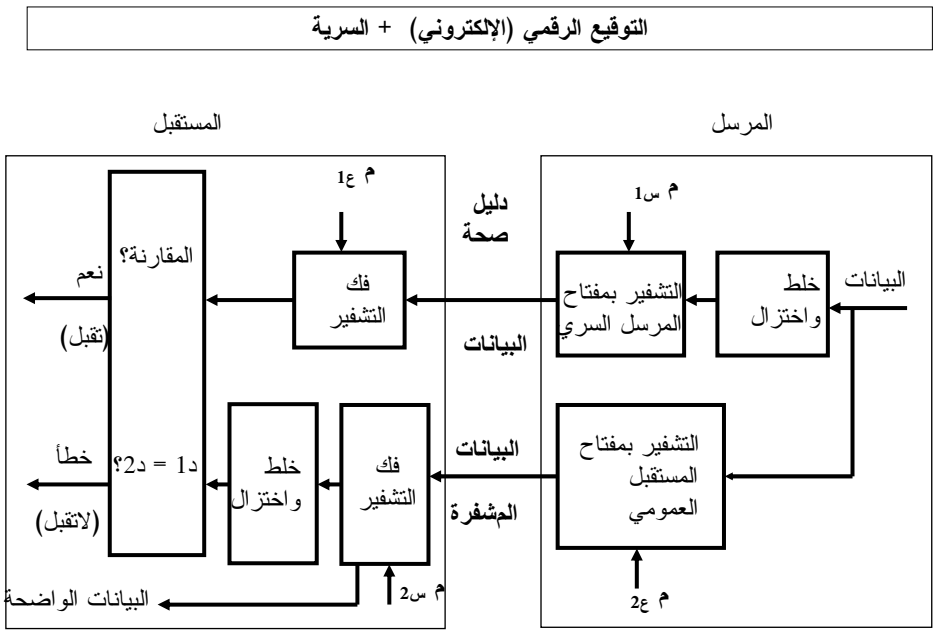


الشكل رقم (6): ضمان عدم تحريف الرسالة بدمج الدليل (Sign) مع التشفير (Encrypt)

الشكل رقم (7-1) والشكل رقم (7-2) يوضحان أسلوب تنفيذ التوقيع الإلكتروني والسرية باستغلال نظام التشفير غير المتماثل:

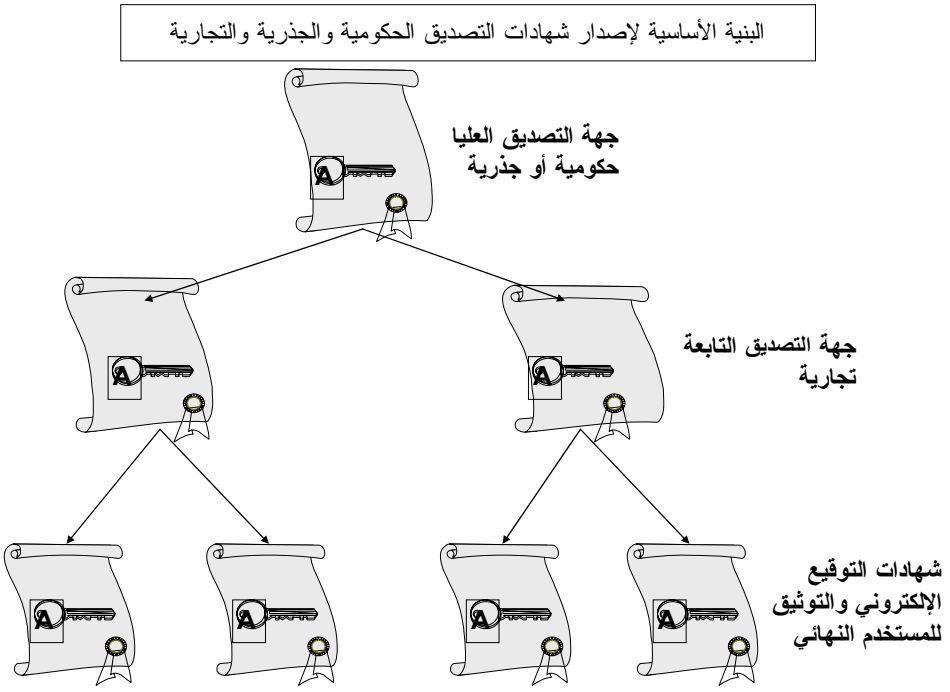


الشكل رقم (7-1): التوقيع الإلكتروني والسرية باستغلال نظام التشفير غير المتماثل



الشكل رقم (7-2): التوقيع الإلكتروني والسرية باستغلال نظام التشفير غير المتماثل

الشكل رقم (8) يوضح أسلوب تنفيذ شهادات التوثيق التي تصدرها جهات التوثيق باستغلال نظام التشفير غير المتماثل:



الشكل رقم (8): شهادات التوثيق باستغلال نظام التشفير غير المتماثل

يستخدم نظام التشفير العلني في إثبات صحة الرسالة وإثبات هوية المرسل والمستقبل ولضمان عدم الإنكار وكذلك لتوقيع وتوثيق المعاملات المالية والمدفوعات الإلكترونية (التوقيع الرقمي).

ولإضافة خاصية السرية التي يوفرها التشفير المتماثل يتم عملياً في تطبيقات التوقيع الإلكتروني وشهادات التوثيق استخدام التشفير المختلط (Hybrid Encryption) وهو تشفير مزيج من التشفير المتماثل وغير المتماثل والهاش. ويطلق على هذا النوع "بنية المفاتيح العامة" (Public Key Cryptography (PKI)) أو بروتوكول التشفير مثل (Pretty Good Privacy (PGP)).

5-3-3 السياسة الأمنية للنظم الشفرية

التشفير هو التقنية الفعالة التي توفر سرية البيانات الحسّاسة أو الحرجة لتطبيقات عمل المؤسسة وطبقاً لتصنيف البيانات. وتؤسس مستوى الحماية الشفرية المناسبة ضمن "تقدير وإدارة المخاطر" التي تأخذ في الاعتبار أيضاً نوع وكفاءة خوارزم التشفير والطول المناسب للمفتاح الشفري وأسلوب إدارة المفاتيح الشفرية وهو ما يسمى "السياسة الأمنية للنظم الشفرية". عند تطبيّق هذه السياسة يؤخذ في الاعتبار الإجراءات والقيود التي قد تفرضها الدولة والتي يلزم تطبيقها على استخدام النظم الشفرية على مستوى مؤسسات الدولة وكذلك عند التعامل مع بلدان العالم المختلفة. كما يلزم الأخذ في الاعتبار الإصدارات الخاصة بتدفق المعلومات المشفرة عبر الدول وعند استيراد أو تصدير النظم الشفرية.

تحدد نوعية الحماية الشفرية المناسبة للبيانات باستشارة الخبراء المتخصصون كما يلزم أخذ النصيحة القانونية فيما يتعلق بالقوانين واللوائح المطلوب تطبيقها على المؤسسات التي تخطط لاستخدام النظم الشفرية داخل الدولة.

5-3-4 تطبيقات التوقيع الإلكتروني

يوفر التوقيع الإلكتروني وشهادات التوثيق وسيلة فعالة لحماية الأصالة والنزاهة للمعاملات والوثائق الإلكترونية. يمكن استخدام التوقيع الإلكتروني في أعمال التجارة الإلكترونية حيث هناك ضرورة للتحقق من هوية الذي حرر وثائق "أمر الشراء" و"فاتورة البيع" و"أوامر الدفع" ولتدقيق ما إذا كان قد تم تغيير في بيانات الوثيقة الموقعة من عدمه. كما يطبق التوقيع الإلكتروني على جميع أشكال الوثائق المعالجة إلكترونيّاً شاملاً ذلك المعاملات المالية ونظم الدفع الإلكترونية ووثائق العقود والاتفاقات. والجدول الآتي يوضح أمثلة لتفاصيل الشهادة طبقاً للمرجع 42 الخاص بالمواصفة X.509 للاتحاد الدولي للاتصالات.

X.509 CERTIFICATE V3 USING RSA ALGORITHM
الرقم المسلسل للشهادة
فترة صلاحية الشهادة
اسم مالك الشهادة (فرد – مؤسسة – موقع – برنامج – اختراع – ... الخ)
اسم سلطة التوقيع الإلكتروني المانحة للشهادة
المفتاح العام لمالك الشهادة
توقيع سلطة التوقيع الإلكتروني المانحة للشهادة
معلومات عن خوارزم التشفير المتماثل المستخدم
معلومات عن خوارزم "دليل الرسالة الهاش" المستخدم
الهدف من إصدار الشهادة

من المهم العناية بحماية المفاتيح السرية حيث إن أي جهة أو شخص يكون له إطلاع أو يمتلك المفتاح السري يستطيع توقيع وثائق مالية مثل المدفوعات والعقود وبالتالي يخدع صاحب المفتاح السري الأصلي.

بالإضافة إلى ذلك يلزم الاهتمام بحماية تكامل ونزاهة المفتاح العلني. هذه الحماية تتم باستعمال شهادات التوثيق للمفتاح العلني العام (بند 5-3-5).

من المهم حسن اختيار نوع وكفاءة خوارزم التشفير المستخدم مع التوقيع الإلكتروني فيما يخص بالتحديد سرية الخوارزم وأطوال المفاتيح المستخدمة وأسلوب إدارتها. من المهم أيضاً الأخذ في الاعتبار إن مفاتيح التشفير المستخدمة في تطبيقات التوقيع الإلكتروني تكون مختلفة عن تلك المستخدمة في تشفير البيانات (بند 5-3-2).

عند تطبيق التوقيع الإلكتروني يجب أن يؤخذ في الاعتبار وجود تشريع قانوني متوافق مع هذه التقنية ويصف الشروط التي من خلالها يعتبر تطبيق التوقيع الإلكتروني قانوني وشرعي (مثل قانون التوقيع الإلكتروني المصري رقم 15 لسنة 2004 والذي اعتبر التوقيع الإلكتروني مقبول قانوناً ويجب الأخذ به عند التقاضي). فعلى سبيل المثال في التجارة الإلكترونية من المهمّ معرفة الموقف التشريعي لتطبيق التوقيع الإلكتروني. قد يكون من الضروري تأجيل تفعيل أي تطبيقات للحكومة الإلكترونية أو المعاملات المالية أو إبرام العقود الملزمة أو اتفاقيات أخرى مشابهه (مثل البورصة أو البنك الشخصي) عندما تكون التشريعات القانونية غير وافية في الوقت الراهن وحتى يتم التطبيق الفعلي للتوقيع الإلكتروني وشهادات التوثيق. بالإضافة إلى ذلك يلزم أخذ النصيحة القانونية فيما يخص القوانين واللوائح المطلوب تطبيقها على المؤسسات التي تخطط لاستخدام النظم الشفرية.

5-3-5 خدمة عدم الإنكار

تستخدم خدمة عدم الإنكار عندما تكون هناك ضرورة لحلّ المنازعات والقضايا حول حدوث أو عدم حدوث حادثة أو فعل. على سبيل المثال منازعة حول صحة التوقيع الإلكتروني على وثيقة خاصة بعقود أو مدفوعات مالية. توفر خدمة عدم الإنكار تأسيس بنية خاصة بإثبات ما إذا كان قد تمّ حادث أو عمل وبواسطة من. على سبيل المثال من الممكن إثبات من قام بالتوقيع الإلكتروني على رسالة مرسلة بالبريد الإلكتروني أو من قام بإرسال الملف الضريبي أو من استلم وثيقة شهادة ميلاد أو شهادة وفاة ... الخ.

أسّست خدمة عدم الإنكار على استعمال نظم التشفير العلني العام غير المتماثل والتوقيع الإلكتروني (بند 5-3-2 وبند 5-3-3).

6-3-5 إدارة المفاتيح الشفرية

1-6-3-5 حماية المفاتيح الشفريّة

إدارة المفاتيح الشفريّة أساسيّة للاستخدام الفعّال للنظم الشفريّة. أيّ كشف أو فقد للمفاتيح الشفريّة يؤدي إلى كشف أو حلّ أو فقد السرية والأصالة والنزاهة للمعلومات.

لذا يتم تفعيل إدارة المفاتيح الشفرية لحماية استخدام المؤسسة للنوعين من أنواع النظم الشفريّة كما سبق توضيحه وهما:

1) نظم المفتاح السري المتماثل حيث يكون هناك اثنان أو أكثر من الجهات التي قد تشترك في استخدام نفس المفتاح السري في التشفير وفي فك الشفرة. ومن المهم الاحتفاظ بسرية هذا المفتاح داخل خزنة خاصة حيث إن أيّ شخص أو جهة تطلع عليه أو تفكه أو تسرقه تكون قادرة على تشفير وإعادة تشفير معلومات المؤسسة أو يمكن بواسطته الاضطلاع غير المصرح به على المعلومات.

2) نظم المفتاح العلني العام وغير المتماثل حيث يكون لكلّ جهة أو شخص زوج من المفاتيح الشفرية: مفتاح عامّ (أيّ يستطيع أي شخص أن يكشفه أو يحصل عليه) ومفتاح سري خاصّ (الذي يلزم الإبقاء عليه بطريقة سرية).

وتستخدم نظم المفتاح السري في التشفير (بند 5-3-2) ونظم المفتاح العلني في إنتاج التوقيع الإلكتروني وفي إدارة المفاتيح الشفرية (بند 5-3-3) وتستخدم نظم التشفير أحادية الاتجاه "الهاش" في إنتاج "كود دليل الرسالة" ((Message Authentication Code (MAC).

من الضروري حماية جميع المفاتيح من التعديل والكشف غير المصرح به. وتحتاج المفاتيح السرية والخاصة وسائل حماية إضافية ضد الكشف غير المصرح به ويمكن استخدام النظم الشفريّة لهذا الغرض بمعنى أن يتم تشفير المفتاح نفسه بمفتاح شفري آخر (Key Encrypted Key). يلزم أيضاً توفير الحماية المادية للحاسب الآلي المستخدم في إدارة المفاتيح الشفرية والخاص بإنتاج واختبار وتخزين وشحن وتوزيع المفاتيح الشفرية والذي يطلق عليها اسم: "وحدة إنتاج المفاتيح ((Hardware Security Module (HSM)". وهو يستخدم بكثرة مع شبكات المدفوعات المالية البنكية العالمية "السويفت" ومع شبكات حجز تذاكر الطيران العالمية "سيتا".

5-3-6-2 معايير وإجراءات ووسائل إدارة المفاتيح الشفري

يتم تأسيس إدارة المفاتيح الشفرية على مجموعة من المعايير والإجراءات والوسائل السرية الخاصة بالآتي:

1) إنتاج المفاتيح للنظم الشفرية المختلفة وللتطبيقات المختلفة.

2) إصدار شهادات التوثيق العامة أو الحصول عليها من جهات التوثيق (بند 5-3-2).

3) توزيع المفاتيح السرية لمن يخطط في استعمالها على أن يتضمّن ذلك كيفية تفعيل المفاتيح بعد استلامها.

4) تخزين المفاتيح على أن يتضمّن ذلك كيفية وصول المصرح لهم إلى تلك المفاتيح.

4) تغييّر أو تحدّيث المفاتيح على أن يتضمن ذلك قواعد وتوقيتات تغيير المفاتيح الشفرية.

5) التعامل مع المفاتيح التي تم كشفها.

6) إبطال المفاتيح الشفرية التي فقدت أو تم كشفها متضمناً ذلك كيفية إبطال عمل وإعادة تفعيل المفاتيح. مثلاً عند حالات مثل كشف المفاتيح أو عندما يترك المستخدمين المؤسسة (في هذه الحالة يلزم أرشفة جميع المفاتيح التي أصدرتها المؤسسة).

7) استرجاع المفاتيح التي يمكن أنّ تكون قد فقدت أو أفسدت نتيجة عملية التشغيل المستمرة على سبيل المثال عند الحاجة لاستعادة المعلومات المشفرة.

8) الاحتفاظ بالمفاتيح على سبيل المثال لأرشفة المعلومات وعمل النسخ الاحتياطية.

9) محو المفاتيح.

10)الدخول والارتباط والتدوين والتدقيق لأنشطة إدارة الأمن الأساسية.

11)استرجاع البيانات المشفرة (Key Recovery or Key Escrow) عند الحاجة لذلك.

لكي تقل احتماليّة الكشف غير المصرح به للمفاتيح الشفرية فإنه يلزم تحديد توقيتات لتفعيل (تنشيط) وإعادة تفعيل وإخماد المفاتيح التي يتم استخدامها لفترة زمنية محدودة.

من المهم تحديد هذه الفترة طبقاً للظروف التي تعمل عندها وسائل التحكم الشفريّة وكذلك المخاطرة المحتملة من عدم تغيير المفاتيح على نظام معلومات المؤسسة.

قد يتم اتخاذ إجراءات لمعالجة المطالب القانونية للنفاذ إلى المفاتيح الشفريّة عند الحاجة إلى ذلك.

على سبيل المثال قد يطلب فك مفتاح الشفرة أو بعض المعلومات المشفرة عند الاحتياج لها كدليل في المحاكم (استرجاع المفاتيح الشفرية (Key Recovery or Key Escrow)) أو في حالة فقد المفتاح الشفري بعد التشفير (استرجاع البيانات المشفرة).

يلزم أيضاً الإصدار المؤمن لوثيقة "أسلوب إدارة السرية والحماية الخاصّة بالمفاتيح العلنية" حيث إن هناك تهديد من أن يقوم دخيل بعملية احتيال أو خداع للحاسب الخادم الخاص بالتوقيع الإلكتروني باستبدال مفتاحه العلني بدلاً من المفتاح العلني للمؤسسة. هذا الخداع يمثل مشكلة عند استعمال شهادات التوثيق العامّة.

من الضروري إنتاج شهادات التوثيق بالطريقة التي تضمن استقلالية وخصوصية المعلومات الخاصة بالمؤسسة المالكة للشهادات والتي تستخدم تقنية المفتاح العلني في إنتاج زوج المفاتيح العلنية والخاصة.

لذلك يلزم الاهتمام بإدارة عملية إنتاج شهادات التوثيق لكي تكون محل ثقة عالية لجميع الجهات المشتركة في نظام التوقيع الإلكتروني وشهادات التوثيق.

تتم هذه العملية عادة بكيان سلطة التصديق الحكومية أو الجذرية التي تكون مؤسسة معروفة وموثوق بها داخل الدولة ويكون لها وسائل تحكم وسيطرة خاصة لتوفير قدر الحماية المطلوبة في هذا النوع من التطبيقات والنظم.

7-3-5 تشفير البيانات أثناء حفظها بأوساط التخزين

يتم حالياً استغلال وسائل التشفير المتماثلة وغير المتماثلة (سواء المعتمدة دولياً وتجارياً أو المبتكرة محلياً) في تأمين البيانات المخزنة في أوساط التخزين العاملة والاحتياطية.

ولقد تفاوتت قوة خوارزم ومفتاح التشفير حتى وصل طول المفتاح العلني إلى 3096 بت في النظم التجارية. ولكن هذه الدرجة بالغة القوة والتعقيد بحيث لا يمكن كسر الشفرة باستخدام تقنيات الحاسبات الآلية الحالية.

والجدير بالذكر أن الحكومة الأمريكية لا تسمح إلا بتصدير معدات Hardware Encryptors تقنيات تشفير متماثل بمفاتيح طولها لا يزيد عن 128 بت والتي قد تكون كافية لحماية

التطبيقات الإلكترونية الجديدة مثل التجارة الإلكترونية بشرط الإدارة الجيدة للمفاتيح الشفرية. إذ يحتاج كسر الشفرة إلى أرقام فلكية من المحاولات تقاس بالأنديسليون (10^{36}). كما أن هناك بروتوكولات شفرية ذات درجة سرية عالية أنتجت للمساعدة على التشفير لعل من أشهرها وأقواها على الإطلاق بروتوكول PGP (Pretty Good Privacy) بالإضافة لبروتوكول ديفي هيلمان (Diffie–Hellmann). كما يجب الاهتمام بالتطوير المحلي لبروتوكولات شفرية خاصة. وبرامج بروتوكولات التشفير ((Pretty Good Privacy (PGP) وديفي هيلمان موجودة على الإنترنت على هيئة برامج المصدر (Source Code) من مواقع "برامج المصدر المفتوحة" opensource.org. ويمكن للمؤسسة اختيار الأنسب من هذه البروتوكولات وتطويره ذاتياً واستخدامه في تأمين وسرية حفظ البيانات.

4-5 أمن الملفات ونظم التطبيقات

يهدف أمن الملفات ونظم التطبيقات إلى ضمان أن التفاعلات التي تتم على بيانات تطبيقات تكنولوجيا المعلومات والخدمات المساندة لها تتم بالدخول المصدق له على النظام وتحت إجراءات التحكم والرقابة.

تقع مسؤولية ضمان نزاهة النظام على عاتق إدارة التطوير وإدارة التشغيل التابع لها الملفات وبرامج النظام وبرامج التطبيقات.

1-4-5 ضوابط تأمين برامج التطبيقات للحاسبات

من المهم توفير وسائل التحكم التالية لتقليل مخاطر أخطاء أو تعطل برامج التطبيقات:

1) تنفيذ التعديلات في مكتبة برامج التطبيقات بواسطة المسؤول المعين فقط وتحت وسائل التحكم الأمنية الخاصة بذلك.
2) عدم برمجة أكواد برامج التطبيقات على نظام تشغيل فعلي إلا بعد التأكد من اجتياز تلك البرامج لجميع الاختبارات وتمام قبول المستخدم النهائي لها. كذلك التأكد من أن برامج المصدر قد تم تعديلها وتوثيقها.
3) الاحتفاظ بسجل تقارير النظام Audit Log والتأكد من أن جميع التعديلات على برامج التطبيقات قد تضمنها سجل التقارير.
4) الإبقاء على النسخ السابقة من برامج التطبيقات للاستعانة بها في الحالات الطارئة.
5) المحافظة الجيدة على برامج النظام الجاهزة والموردة بواسطة المنتج الأصلي وطبقاً لتعليماته. تؤخذ في الاعتبار وسائل التحكم الأمنية ومستوى السرية عند اتخاذ قرارات بشأن تعديل أو تحديث نسخ برامج التطبيقات. على سبيل المثال عند تقديم خدمة تأمين وسرية جديدة كذلك عند تحديد عدد الرخص. والهدف من ذلك التعامل مع أي مشاكل تأمين وسرية قد تحدث نتيجة النسخ الحديثة.
6) تطبيق التعديلات على برامج التطبيقات بطريقة مجمعة إذا كان ذلك يساعد على التغلب على أو تقليل مستوى الضعف الأمني للبرامج الأساسية للنظام.
7) السماح للموردين بالدخول الطبيعي أو المنطقي على مصادر النظام بغرض الدعم الفني فقط وعندما يتطلب الأمر ذلك مع ضرورة الحصول على تصديق من الإدارة

العليا على ذلك. كما يلزم مراقبة نشاط ممثلي الموردين أثناء دخولهم على مصادر النظام حتى لو كان بغرض الدعم الفني.

2-4-5 الحماية ضد بيانات اختبار النظام

من الضروري التحكم في بيانات الاختبار وتأمينها. تتطلّب اختبارات قبول النظام عادة أحجام جوهريّة من البيانات الاختبارية (Test Data) تكون قريبة من أو مشابهة لبيانات النظام الحقيقية. يلزم عدم استخدام قواعد البيانات التشغيلية الحقيقية في الاختبارات لأنها تتضمن بيانات شخصية عن أفراد المؤسسة. إذا كان لا بد من استخدام جزء من قواعد البيانات التشغيلية الحقيقية فيجب أولاً إلغاء البيانات الشخصية منها قبل استخدامها.

ومن المهم تطبيق وسائل التحكم التالية لحماية البيانات التشغيلية أثناء استخدامها في اختبارات النظام:

1) تطبيق نفس إجراءات التحكم في الدخول على الملفات (التي تطبق على النظم التشغيلية) على إجراءات التحكم في الدخول على الملفات الاختبارية.
2) أن تكون هناك وسائل تحقق منفصلة كل مرة يتم فيها نسخ البيانات التشغيلية بغرض اختبارات برامج التطبيقات.
3) مسح نسخ البيانات التشغيلية بمجرد الانتهاء من اختبارات برامج التطبيقات.
4) يتم تضمين الدخول على عمليات النسخ والاستعمال للبيانات التشغيلية في تقارير "تدقيق الأثر" (Audit Trails).

3-4-5 المراجعة الفنية للتغييرات في البرامج والتطبيقات

من الضروري كلما كان ذلك ممكناً وبصفة دورية إجراء تغييرات وتعديلات في برامج التشغيل. على سبيل المثال عند الحاجة لتثبيت تحديثات جديدة أو ملفات برامج إصدارات أو دفعة ملفات "تأمين ضد الثغرات الأمنية" (Security patches) بواسطة المنتج. عندما تتم التغييرات فإنه يلزم مراجعة واختبار برامج التشغيل المعدلة لضمان عدم وجود ثغرات أمنية جديدة قد يكون لها تأثير سلبي على تشغيل نظام المعلومات. سوف تغطي هذه العملية ما يلي:

1) مراجعة برامج تطبيق التحكم وإجراءات النزاهة لضمان عدم وجود ثغرات أمنية جديدة نتيجة تغيير برامج التشغيل قد يكون لها تأثير سلبي على تشغيل النظام.
2) ضمان أنّ خطة وميزانية الدعم الفني السنوي ستغطّي مراجعات واختبارات النظام الناتج من تغيير برامج التشغيل.
3) ضمان أنّ الوثائق المتعلقة ببرامج التشغيل قد تم تعديلها في الوقت المناسب بما يسمح بإتمام المراجعات المناسبة قبل تنفيذ التعديل.
4) ضمان أن التغييرات المناسبة قد تمت على خطط استمرارية العمل.

4-4-5 اكتشاف الأبواب الخلفية والاكواد الخبيثة (مثل حصان طروادة)

تلتقط الأبواب والنوافذ الخلفية (Back-doors) المخفاة المعلومات بوسائل غير مباشرة وغير مؤمنة. قد يتم تنشيط الأبواب الخلفية من خلال تعديل قيم معطيات مزروعة بواسطة دخيل ضمن أكواد البرامج الجاهزة. وقد تكون الأبواب الخلفية متاحة للنوافذ أو بوابات النظام

السرية وغير السرية أو غير المستخدمة في تطبيقات العمل. وقد تكون ضمن برامج تطبيقات عاملة مثل الأكواد التي تكون داخل سلسلة متتالية ومتصلة من التعليمات (Series of Instructions). ولقد تم تصميم كود حصان طروادة والبرامج الخبيثة الأخرى للتأثير على النظام بطريقة غير مصرح بها وغير ملحوظة وغير مرغوب فيها. ونادراً ما تحدث الأبواب الخلفية وكود مثل حصان طروادة بالصدفة. والأرجح أنه يتم زرعها مسبقاً في البرامج. وللتغلب على مخاطر الأبواب الخلفية وكود حصان طروادة يتم مراعاة وسائل التحكم التالية:

1) اقتناء البرامج من المصدر ذو السمعة الطيبة فقط.
2) اقتناء البرامج التي لها كود المصدر ليتم اختباره.
3) استخدام المنتجات التي تم تقييمها عالمياً.
4) تفتيش واختبار جميع أكواد برامج المصدر قبل استعمالها.
5) استخدام طاقم من الأفراد ذوى الثقة للعمل في النظم التي تعتبر بمثابة مفاتيح أساسية للنظام.

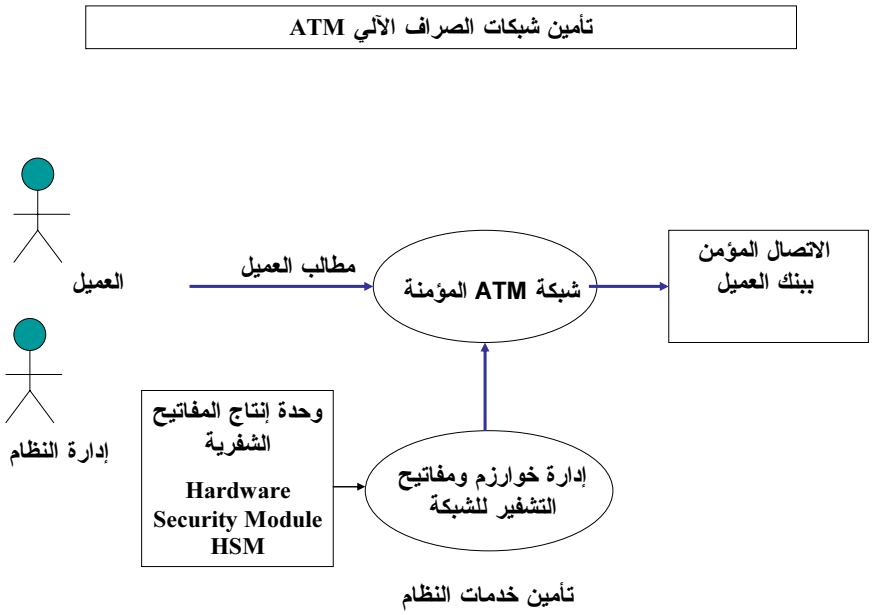
5-5 النظم الشفرية

1-5-5 خوارزميات وبروتوكولات التشفير

استخدم الإنسان النظم الشفرية منذ نحو ألفي عام قبل الميلاد لحماية رسائله السرية وكان أول من استخدم الرمز للتعبير عن جمل كاملة قدماء المصريين. وبلغ هذا الاستخدام ذروته في فترات الحروب خوفاً من وقوع الرسائل الحساسة في أيدي العدو. وقام يوليوس قيصر بتطوير خوارزميته المعيارية المعروفة باسم شفرة قيصر (Cesar Cipher) التي كانت نصّاً مشفَّراً (Cipher text) لتأمين اتصالاته ومراسلاته مع قادة جيوشه. وظهرت فيما بعد العديد من الآلات التي تقوم بعمليات التشفير ومنها آلة التلغيز الألمانية (Enigma machine).

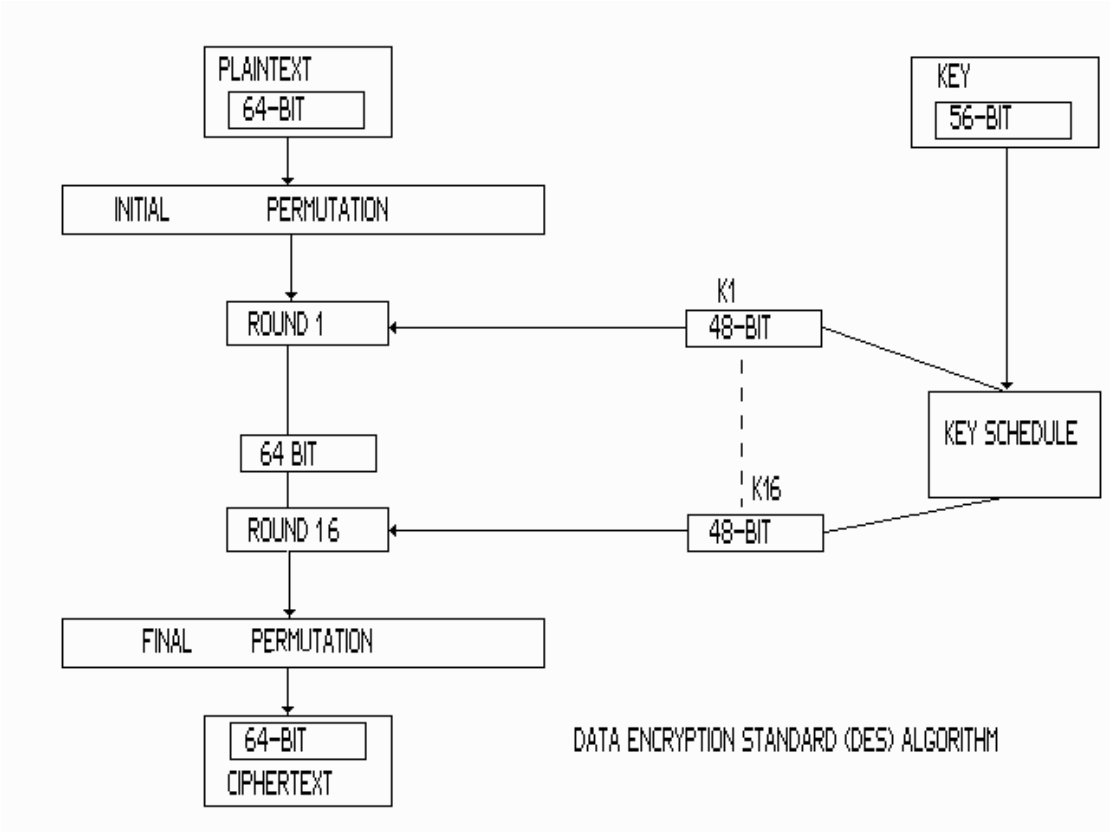
وشكَّل الكمبيوتر في بدايات ظهوره وسيلةً جديدة للاتصالات الآمنة وفك تشفير الرسائل. واحتكرت الحكومات في فترة الستينيات حق التشفير وفك التشفير. وفي أواخر الستينيات أسَّست شركة آي بي إم (IBM) مجموعةً تختص بأبحاث التشفير ونجحت هذه المجموعة في تطوير نظام تشفير أطلقت عليه اسم لوسيفَر (Le cipher) وكان درجة سرية هذا النظام مثاراً للجَدَل. ورغم تحفظات الحكومة الأمريكية عليه لاعتقادها بعدم حاجة المؤسسات المدنية والتجارية إلى التشفير إلا أنه حقق انتشاراً واسعاً في الأسواق. ومنذ ذلك الحين طورت العديدُ من الشركات المتخصصة أنظمة تشفير جديدة مما أبرز الحاجة إلى وجود معايير لاستخدام التشفير.

ومن أبرز الجهات التي ساهمت في مجال وضع معايير للتشفير المعهد الوطني للمعايير والتكنولوجيا ((National Institute of Standards and Technology (NIST) المعروف سابقاً باسم المكتب الوطني الأمريكي للمعايير (U.S. National Bureau of Standards) إذ طوَّر هذا المعهد عام 1973 معياراً أطلق عليه "تشفير البيانات القياسي" (Data Encryption Standard) (DES). ويستنِد هذا المعيار إلى خوارزم لوسيفَر (Le cipher) السابق الإشارة إليه ويستخدِم مفتاح تشفير بطول 56 نبضة. ويشترط لاستخدامه أن يكون لكل من المرسِل والمستقبِل نفس المفتاحَ الشفري. وقد استخدمت الحكومة الأمريكية "تشفير البيانات القياسي" عام 1976 واعتمدته البنوك الأمريكية في تشغيل آلات الصراف الآلي (ATM) طبقاً للشكل رقم (9).



الشكل رقم (9): استخدام النظم الشفرية القياسية مع ماكينات الصرافة الآلية.

والشكل رقم (10) يوضح العمليات الحسابية والمنطقية التي ينفذها خوارزم DES حيث يتم أولاً تحويل الرسالة الواضحة إلى مجموعات بيانات طول كل منها 64 نبضة. ويتم ثانياً استخدام 56 نبضة من المفتاح الشفري لتحويل 64 نبضة من البيانات الواضحة إلى 64 نبضة بيانات مشفرة. وتتم 16 عملية تباديل Rounds (زحزحة ودوران) على البيانات المشفرة ويختلط الناتج ببيانات واضحة جديدة لتعقيد التشفير. ويتم استخدام مفتاح شفرة جديد مع كل عملية تشفير.



الشكل رقم (10): نظام التشفير القياسي DES

وتم مؤخراً تطوير هذا النظام عن طريق تنفيذه ثلاثة مرات متتالية كل منها له مفتاح مستقل. وهذه العمليات في الإرسال هي: تشفير ثم إعادة تشفير ثم تشفير. وفى الاستقبال العكس بمعنى إعادة تشفير ثم تشفير وأخيراً إعادة تشفير. وبذلك ظهر النظام الشفري 3DES الذي له مفتاح شفري بطول 114 بت (أي ثلاثة أضعاف مفتاح النظام DES).

وبعد عام واحد من تطبيق نظم تشفير البيانات (DES) و(3DES) طوَّر ثلاثة أساتذة جامعيون نظامَ تشفير غير متماثل آخر أطلقوا عليه اسم (RSA). ويستخدم هذا النظام زوجاً من المفاتيح مفتاح عام (public key) ومفتاح خاص (private key) بدلاً من استخدام مفتاح شفري واحد فقط. ورغم أن هذا النظام كان ملائماً جداً لأجهزة الحاسبات المعقَّدة إلا إنه قد تم اختراقه فيما بعد خاصة عندما كان طول المفتاح أقل من 1024 نبضة.

ويعتمد التشفير RSA رياضياً على عملية "الأس" Modular Exponentiation بمعنى أن الرسالة المشفرة C تستنتج من الرسالة الواضحة P بواسطة مفتاح التشفير K (السري أو العلني) وباستخدام المعادلة: $C= P^{K} MOD\ N$.

ويتم فك التشفير بواسطة مفتاح فك التشفير K^{-} وباستخدام المعادلة: $P= C^{K^{-}} MOD\ N$.

وللحصول على N و K و k^{-} يتم اتباع الخطوات التالية:

1) إنتاج رقمين عشوائيين أحاديين طول كل منهما أكبر من 11 رقم عشري هما p,q

2) يتم الحصول على الرقم N = p x q

3) يتم حساب عدد المفاتيح الممكنة من الرقميين ويسمى هذا العدد $\phi(n)$ حيث: $\phi(n) = (p-1)(q-1)$

4) يتم اختيار الرقم e ليكون أقل من $\phi(n)$ وأحادي معه ويمثل كل من e و N المفتاح السري (أو المفتاح العلني) k.

5) يتم حساب العدد d من المعادلة $de = 1 + k\phi(n)$ حيث k رقم أحادي ويمثل d و N المفتاح العلني (أو السري) k^-.

وبقيت الحال على ذلك حتى قام فيل زيمرمان (Phil Zimmerman) عام 1986 بتطوير بروتوكول تشفير يُدعى "برنامج الخصوصية المتفوّقة" ((Pretty Good Privacy (PGP) وهو يعتمد على ثلاثة أنواع من النظم الشفرية وهي: نظام التشفير غير المتماثل (RSA) ونظام التشفير المتماثل (3DES or AES) ونظام التشفير أحادي الاتجاه (Message Digest MD5) ومن هنا أطلق عليه اسم "نظام أو بروتوكول التشفير" لأنه يتضمن أكثر من نظام تشفير. ويتميز PGP باستخدام مفتاح بطول 128 بت وهو من أكثر برامج التشفير انتشاراً في وقتنا الحالي ويتوافر منه نسخ تجارية مرخصة ونُسخ مجانية.

يتم التشفير بالبروتوكول PGP من خلال الخطوات التالية:

1) يتم أولاً تجهيز الرسالة المطلوب تشفيرها.

2) يتم تطبيق برنامج ضغط (Compression program) على الرسالة لتقليل حجمها ولمحو أي أجزاء من البيانات متشابهة ومتكررة قد تساعد الدخيل على كسر الشفرة.

3) يتم عمل "دليل للرسالة د1" باستخدام خوارزم الدليل Hash Function.

4) يتم إنتاج مفتاح من خوارزم التشفير المتماثل بطريقة عشوائية (سواء من خلال تحريك الفارة عشوائياً أو بالضغط العشوائي على لوحة المفاتيح) ويسمى الناتج "مفتاح الجلسة" (Session Key).

5) يتم تشفير الرسالة المضغوطة "بمفتاح الجلسة" و"خوارزم التشفير المتماثل" للحصول على الرسالة المشفرة.

6) يتم تشفير "مفتاح الجلسة" بالمفتاح العلني للمرسل إليه للحصول على "المفتاح المشفر".

7) يتم تشفير "الرسالة المشفرة" و"دليل الرسالة" و"المفتاح المشفر" باستخدام المفتاح السري للمرسل ويتم إرسال الناتج عبر الشبكة.

ويتم فك التشفير بالبروتوكول PGP من خلال الخطوات التالية:

1) يتم فك الرسالة المشفرة بواسطة المفتاح العلني للمرسل.

2) يتم فك "مفتاح الجلسة" بالمفتاح السري للمرسل إليه.

3) يتم فك شفرة الرسالة "بمفتاح الجلسة" و"خوارزم التشفير المتماثل" للحصول على الرسالة الواضحة المضغوطة.

4) يتم مطابقة دليل الرسالة الواضحة المضغوطة د2 مع الدليل المرسل مع الرسالة د1.

5) إذا تطابق الدليلين د1 و د2 يتم إعادة فك ضغط الرسالة للحصول على الرسالة الأصلية.

ويتضح مما سبق أن البروتوكول PGP قد حقق جميع المعايير الخاصة بتأمين البيانات وهي: السرية والتوثيق والتكامل وعدم الإنكار.

والجدير بالذكر أن العالم المصري اد/ طاهر الجمل قد طور الخوارزم الشفري El Gamal الذي يعتبر أقوى واعقد من الخوارزم RSA وتستخدمه حالياً الحكومة الأمريكية في تطبيقات التوقيع الإلكتروني وشهادات التوثيق.

ونظام RSA رغم أنه أفضل وأكثر أمناً من نظام DES إلا إنه أبطأ إذ إن عملية التشفير وعملية فك التشفير يجب أن تكونا متزامنتين في الوقت تقريباً. وحالياً نظام RSA ليس عصياً على الاختراق إذ إن اختراقه أمر ممكن إذا توافر ما يلزم لذلك من وسائل تقنية (حاسبات فائقة السرعة). لذلك يعتبر بروتوكول أو نظام PGP نموذجاً محسَّناً ومطوَّراً من نظام RSA خاصة إذا استخدم مفتاح شفري بطول أكثر من 128 نبضة. بالإضافة إلى استخدامه لكل من ضغط البيانات والتشفير المتماثل والتشفير غير المتماثل والدليل أو البصمة الإلكترونية للرسالة (message digest) ولا يزال هذا النظام منيعاً على الاختراق حتى يومنا هذا.

2-5-5 تطبيقات الأنظمة الشفرية القياسية

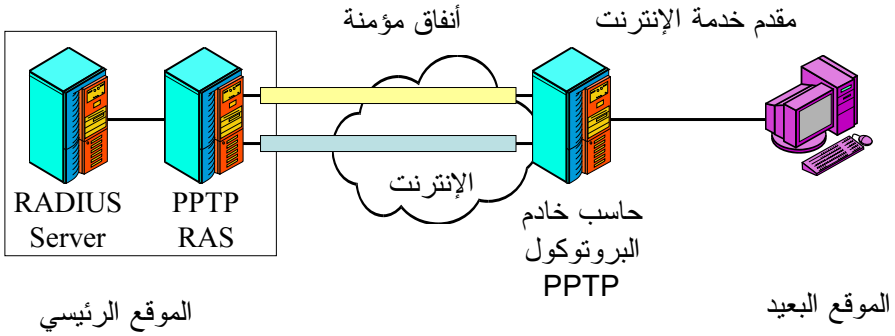
1-2-5-5 الأنظمة الشفرية التي تعمل على مستوى التحكم في المحور

يوجد نظامين شفريين على مستوى التحكم في المحور بهدف تكوين أنفاق مؤمنة (Secured Tunnels) بين الموقع الرئيسي والمشترك البعيد المتصل من خلال قنوات الدايال أو قنوات الإنترنت ADSL. حيث يتم تشفير البيانات ودمجها داخل حزم البيانات بحيث لا يتم الاطلاع عليها إلا بواسطة المستقبل المصرح له والذي يملك مفتاح وخوارزم التشفير. [المرجع رقم (26)] وهذان النظامان هما:

1) بروتوكول الأنفاق المؤمنة نقطة لنقطة (Point to point Tunneling Protocol PPTP) كما في الشكل رقم (11).

2) بروتوكول الأنفاق على الطبقة الثانية (Layer Two Tunneling Protocol L2TP) كما في الشكل رقم (12).

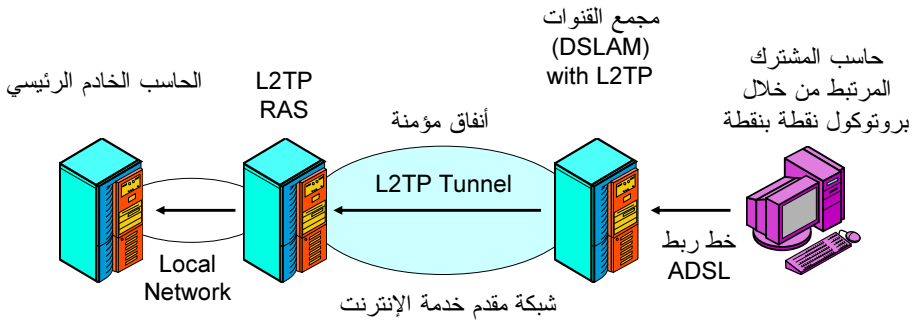
Point-to-Point Tunneling Protocol (PPTP)
بروتوكول الأنفاق المؤمنة على مستوى التحكم فى المحور



الشكل رقم (11): بروتوكول الأنفاق المؤمنة نقطة لنقطة

Layer 2 Tunneling Protocol (L2TP)

بروتوكول الأنفاق على الطبقة الثانية



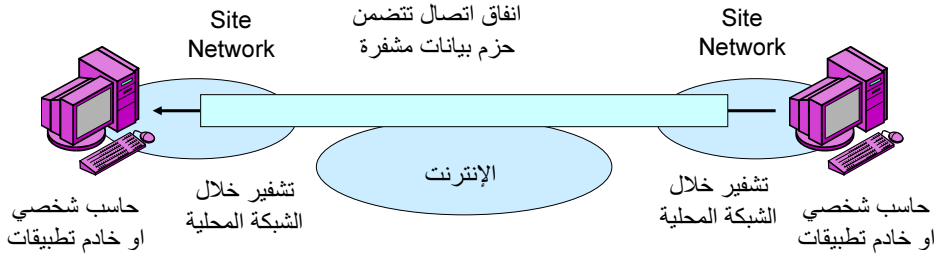
الشكل رقم (12): بروتوكول الأنفاق على مستوى الطبقة الثانية

ومن الممكن أن تعمل بروتوكولات التشفير على مستوى التحكم في المحور منفردة أو بالإضافة إلى برتوكولات المستوى الأعلى مثل IPSEC.

5-2-5-2 الأنظمة الشفرية التي تعمل على مستوى الشبكات

بروتوكول IPsec: هو مصطلح يبين سلسلة من القياسات غير النهائية التي نشرتها منظمة تطوير الإنترنت IETF وتعرف أسلوبين لحماية البيانات أثناء نقلها عبر طبقة الشبكة باستخدام المصادقة والتشفير: التشفير من البداية إلى النهاية على الشبكة الواسعة ومروراً بالشبكة المحلية إذا كانت درجة الثقة في شبكة مقدمي خدمة الاتصالات عالية. أو يشفر فقط البيانات بين طرفي الاتصال للشبكة الواسعة على أن يستخدم نظام تشفير آخر على الشبكة المحلية إذا كانت درجة الثقة محدودة في شبكة مقدم الخدمة. ومعظم بروتوكولات التأمين التي تقوم بتشفير البيانات المنقولة عبر طبقة الشبكة مصممة للاستخدام على الإنترنت إما لتشفير جميع حزم البيانات أو لتشفير أنواع معينة من حزم البيانات كما في الشكل رقم (13). [المرجع رقم (54)].

IPsec Operation: Tunnel and Transport Modes
بروتوكول التشفير على مستوى الشبكات

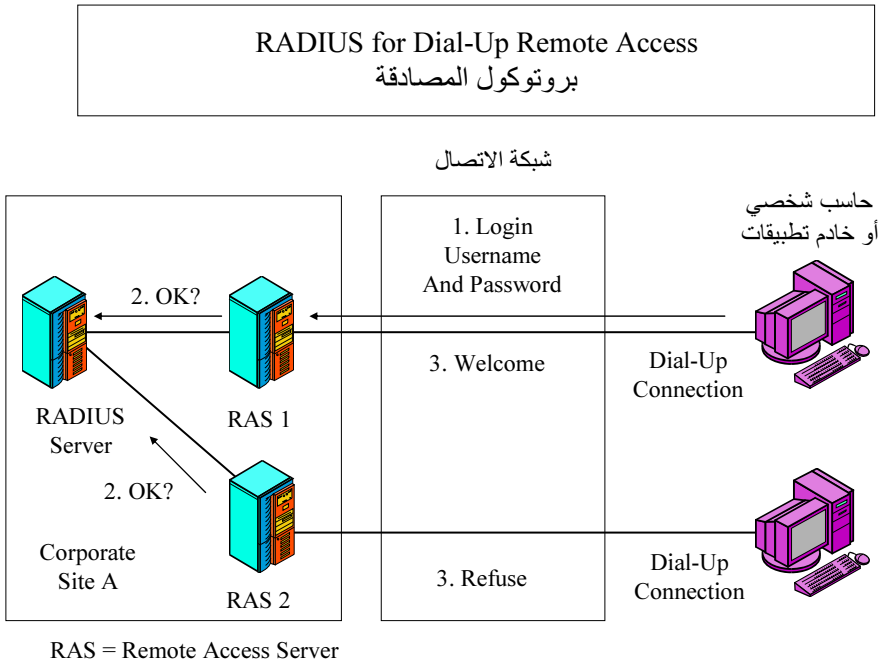


الشكل رقم (13): بروتوكول IPsec

5-2-5-3 الأنظمة الشفرية التي تعمل على مستوى التطبيقات

1) بروتوكول Kerberos: هو بروتوكول مصادقة Hand shake تستخدمه عادة خدمات الدليل المؤمن Active Directory لنظم التشغيل للحاسبات الخادمة Windows server لتوفير تعريف واحد فقط Single Sign On للمستخدمين طوال مدة دخولهم على البيانات ومصادر المعلومات. حيث يطلب من المستخدم (القريب والبعيد) اسمه وكلمة المرور ورقم شفري. ويتم التحقق من ذلك بواسطة خادم بروتوكول Kerberos وبناء عليه يسمح الخادم للمستخدم بتكملة الاتصال أو يتم منع الاتصال عنه.

2) بروتوكول RADIUS: هو بروتوكول مشابه للبروتوكول السابق ويعمل بنفس الأسلوب ولكن على خطوط الدايال ولذلك يسمى RADIUS for Dial-Up Remote Access كما في الشكل رقم (14). [المرجع رقم (56)]



الشكل رقم (14): بروتوكول RADIUS for Dial-Up Remote Access

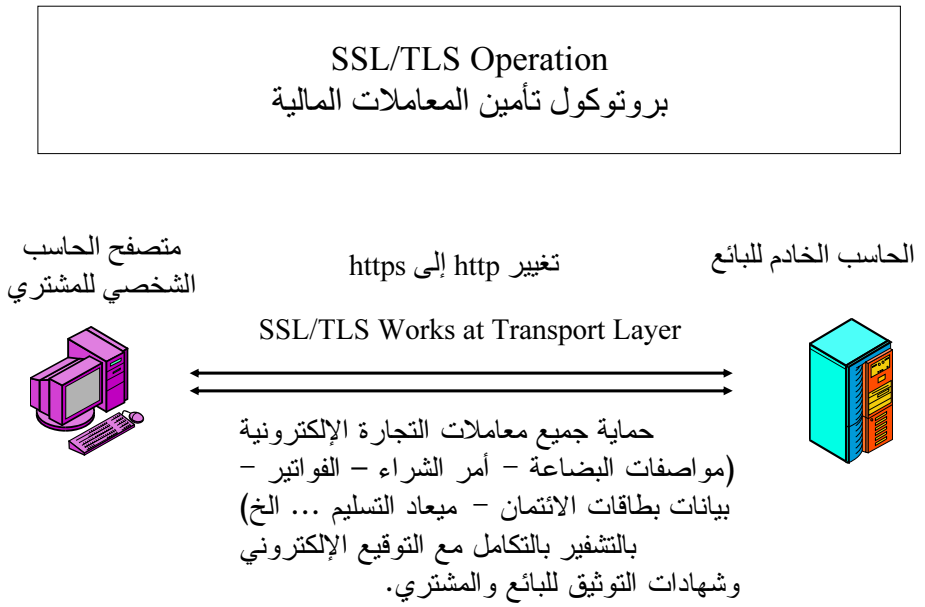
3) بروتوكول تأمين التطبيقات المالية SSL ((Secure Socket Layer (SSL):

Transport Layer Security (TLS) أو Secure Socket Layer (SSL) هي تقنية خاصة بتأمين جميع العمليات الإلكترونية الحديثة وليس فقط التجارة الإلكترونية. حيث يتم التأمين بتشفير المعلومات المرسلة عبر الإنترنت بحيث تقتصر إمكانية إعادة تجميع المعلومات وقراءتها على الحاسبات الخادمة المرسلة والمستقبلة فقط. ويستخدم التشفير مع شهادات التوثيق والتوقيع الإلكتروني التي تستخدم خدمة التسجيل من الطرف الثالث (جهات التوثيق الجذرية والحكومية والتجارية) من أجل التأكيد على سلامة ونزاهة وعدم الغش سواء من جانب المواقع الخادعة أو العميل المخرب مما يحقق قدر الإمكان الأمان لعقد الصفقات وللتجارة الإلكترونية. فمجرد تحقيق الاتصال بين حاسبات كل من الموقع والعميل يتم الاتفاق على خوارزم التشفير ومفاتيح التشفير وكيفية إدارة المفاتيح الشفرية. ويتم توفير المفاتيح بخوارزم التشفير غير المتماثل في صورة زوجين أحدهما سري والآخر علني كما سبق الإشارة إليه.

وعندما يتطلب الأمر اتصالاً آمناً يقوم الطرف البادئ باستخدام كلاً من المفتاح السري الخاص به والمفتاح العلني للطرف الآخر في تشفير وفك الرسائل الخاصة بالتجارة الإلكترونية. وقد تتضمن تلك الرسائل: أمر الشراء – الفواتير – أسلوب الدفع – زمن ومكان التوريد ... الخ.

ولقد صمم بروتوكول Secure Socket Layer (SSL) لحماية البيانات التي يتم نقلها بين حاسب خادم الويب للمنتج ومتصفح أو مستعرض العميل Explorer. وحالياً جميع متصفحات الويب تدعم بروتوكول SSL ويتم تخزين شهادات التوثيق والتوقيع الإلكتروني عليها.

فحين يتم اتصال عميل بموقع على الإنترنت ويريد أن يتأكد ما إذا كان هذا الاتصال مؤمن ومحمي وهذا الموقع موثق – فإذا ظهر في شريط العنوان للمتصفح بروتوكول https:// بدلاً من http:// فهذا يعني أنه يتم تأمين الاتصال بالموقع المؤمن والموثق وأنه لا توجد مخاطر ستتعرض لها رسائل التجارة الإلكترونية. كما يحق لأي طرف الاطلاع على شهادة التوثيق للطرف الآخر من جهة التوثيق التابع لها. والشكل رقم (15) يوضح بروتوكول تأمين التطبيقات المالية SSL. [المراجع أرقام (27 و48 و57 و69)]



الشكل رقم (15): بروتوكول تأمين التطبيقات المالية SSL

6-5 سلطات التصديق للتوقيع الإلكتروني وشهادات التوثيق الجذرية والحكومية

1-6-5 مسؤولية سلطة التصديق ألإلكتروني

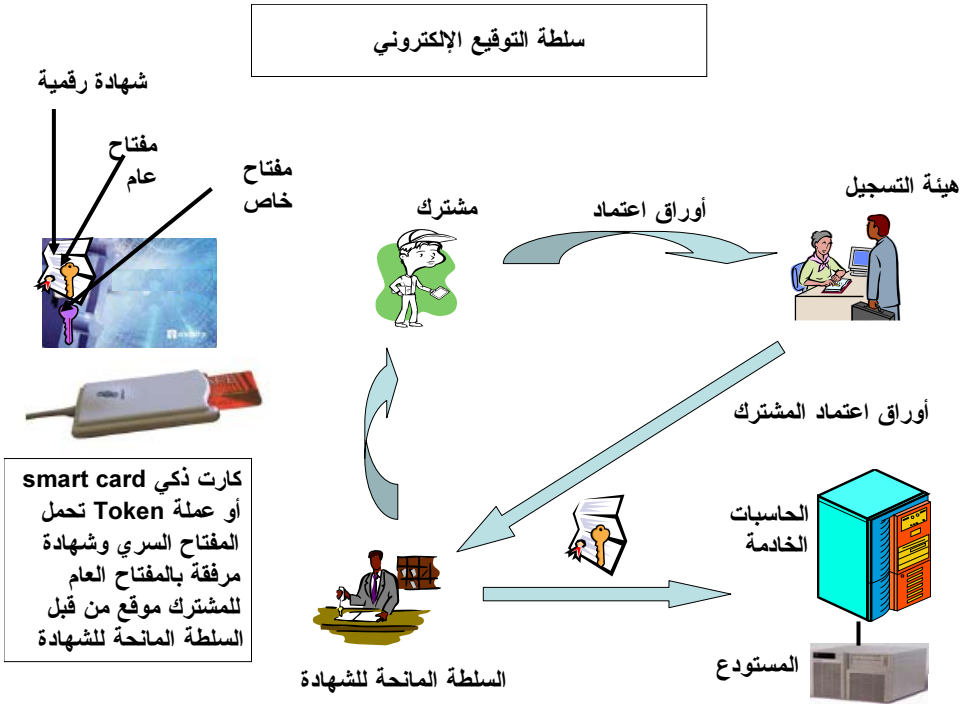
هناك حاجة ملحة للتعامل الآمن عن طريق شبكة الإنترنت لا سيما في ظل الانتشار السريع لها والتوسع في استخدامها في شتى المجالات خاصة التطبيقات الإلكترونية مثل:

- التبادل الإلكتروني للرسائل فيما بين الأفراد والمؤسسات الحكومية والمدنية والتجارية.
- التبادل التجاري للرسائل فيا بين الشركات أو بينها وبين البنوك أو الحكومة الإلكترونية.
- الربط فيما بين المؤسسات الحكومية (الوزارات والهيئات) التي تحتاج إلى مستوى عال من السرية والوثوقية لتبادل البيانات ونقل الملفات كل حسب طبيعة عمله.

لذلك سعت الدول إلى إنشاء سلطات للتوقيع الإلكتروني وشهادات التوثيق وقد تكون على عدة أنواع من أهمها سلطات التوقيع الإلكتروني الحكومية والجذرية والتجارية.

وسلطة التوقيع أو التصديق الإلكتروني (الشكل رقم 16) تكون مسؤولة عن الآتي:

- إدارة تسجيل طالبي الشهادات وإنتاج الشهادات التي تحوي التوقيع الإلكتروني والمفتاح العلني لحاملي الشهادات.
- نشر قائمة الشهادات العاملة والملغاة.
- إدارة نظام الكروت الذكية.
- تجديد الشهادات.
- إنتاج وإدارة المفاتيح الشفرية.



الشكل رقم (16): سلطة التوقيع الإلكتروني

2-6-5 تطبيقات التوقيع الإلكتروني وشهادات التوثيق

تشمل تطبيقات التوقيع الإلكتروني وشهادات التوثيق الآتي:

1) التوقيع الإلكتروني وتطبيقات الحكومة الإلكترونية:

إن أهم معوقات التحول من المكتب الورقي إلى المكتب اللا ورقي هو عدم القدرة على تضمين التوقيع في الوثائق والخطابات والنماذج وغيرها الأمر الذي يمكن تحقيقه من خلال تقنية التوقيع الإلكتروني. كما أن التوقيع الإلكتروني هو الذي سيحول تطبيقات الحكومة الإلكترونية التي تم تناولها في الفصل الثاني إلى حقيقة. فمن خلال التوفيق الإلكتروني وشهادات التوثيق ممكن أن يتأكد البنك مثلاً من أن الشخص الذي يود الدخول إلى حسابه الشخصي هو في الواقع صاحب الحساب وليس شخص آخر. وتتأكد إدارة المرور من أن من

يطلب تجديد رخصة القيادة هو بالفعل صاحب الرخصة. وتتأكد الجامعة من أن من يود الدخول إلى سجلاته الدراسية هو الطالب المعني وليس شخص آخر. ويتأكد المواطن من أن الموقع الذي سيدخله لكتابة إقراره الضريبي مثلاً هو بوابة الحكومة الإلكترونية وليس موقع تم إنشاؤه للاحتيال عليه. ويتأكد وسيط الأسهم من أن العميل لن ينكر قيامة بإدخال طلب شراء لعدد من الأسهم وبالقيمة المالية المحددة عندما يكون العميل بالفعل قد أدخل أمر الشراء. وأخيراً تتأكد الأطراف الموقعة على عقد تجاري فيما بينهم عبر الإنترنت من هويتهم ومسؤوليتهم وعدم إنكارهم لما تم من اتفاقات وتفاعلات دون الحاجة لتواجدهم معاً في نفس المكان.

2) البريد الإلكتروني الآمن:

يتيح البريد الإلكتروني الآمن للمستخدمين تشفير الرسائل الإلكترونية منعاً لقراءتها من قبل المتطفلين والعابثين وتتم العملية بقيام المرسل بتشفير الرسالة بواسطة المفتاح العام للمرسل إليه والمفتاح السري للمرسل. ويقوم المرسل إليه بعد استلام الرسالة بفتحها بإعادة التشفير بواسطة المفتاح السري الخاص به والعلني الخاص بالمرسل. ولضمان الموثقية والسرية فإن المرسل يحتاج إلى الحصول على الشهادة الرقمية الرسمية للمرسل إليه والتي من المفضل أن تكون صادرة من نفس مركز التصديق.

أما المرسل إليه فيستطيع التحقق من مصدر الرسالة (التأكد من أن المرسل هو بالفعل الشخص الظاهر اسمه في البريد الإلكتروني) بالقيام بمطابقة التوقيع الإلكتروني للمرسل كما يظهر في الرسالة وذلك بجلب الشهادة الرقمية للمرسل وإجراء عملية مطابقة.

3) إنشاء مواقع الإنترنت الآمنة:

تستخدم الشهادات في توثيق مواقع الإنترنت خصوصاً تلك المعنية بالأعمال الإلكترونية (التجارة الإلكترونية والحكومة الإلكترونية والتعليم عن بعد) في هذه الحالة تقوم الجهة المقدمة للخدمة الإلكترونية بالحصول على "شهادة موقع" لاستخدامها مع برتوكول (Secure Sockets Layer (SSL)) وتسمى هذه الشهادة SSL Server Certificate وتحتوى على اسم الجهة واسم النطاق الخاص بالموقع (Domain Name) إلى جانب المفتاح العام للموقع. تكمن الفائدة من هذه الشهادة في أنها تتيح للزائر معرفة هوية الموقع وتسمح بتشفير البيانات الصادرة عن الموقع والواردة آلية. ويجد هذا الاستخدام قبولاً كبيراً في تطبيقات الحكومة الإلكترونية وفى جعل مواقع التعليم عن بعد ومواقع الطب العلاجي أكثر أماناً وموثوق فيها.

4) استخدامات أخرى للتوقيع الإلكتروني:

هناك استخدامات أخرى كثيرة للتوقيع الإلكتروني وشهادات التوثيق ومنها ما يلى:

- التوقيع على حزم البرامج بحيث يتمكن المستخدم من معرفة الجهة التي أصدرت البرنامج منعاً لانتشار الفيروسات أو استخدام برامج مقلدة أو رديئة المستوى.
- وضع الختم الزمني (Time Stamp) للمراسلات والوثائق. وهى طريقة يتم من خلالها إضافة الوقت الفعلي الرسمي الذي تمت فيه العملية الإلكترونية ويستخدم لأغراض الإثبات القانوني لوقت حدوث عمل ما. وتتم عملية إضافة الختم الزمني من قبل جهة مستقلة مختصة بهذه المهمة.
- تصديق الخطابات التي تحتاج إلى مصادقة من جهة معينة كما هو متبع في الطرق التقليدية كالحصول على مصادقة مدير العمل أو رئيس الحي أو مأمور قسم الشرطة والتي من الممكن أن تتم بشكل إلكتروني كامل.

- تحديد الصلاحيات بواسطة التوقيع الإلكتروني للجهة المانحة للصلاحية. على سبيل المثال للدخول في مزاد إلكتروني يشترط وجود مركز رئيسي في مدينة معينة للجهة المشاركة في المزاد. يمكن في هذه الحالة قيام الجهة بالحصول على التوقيع الإلكتروني من الغرفة التجارية المعنية.
- التبادل الموثق والمؤمن للملفات والرسائل فيما بين خوادم الحاسبات من خلال إصدار شهادة رقمية لكل حاسب مع إضافة إمكانية للحاسب تهدف إلى إجراء التوقيع الإلكتروني الخاص به. [المراجع أرقام (27 و33 و40 و41 و42 و56 و57 و60 و65 و69)]

3-6-5 فئات شهادات التوثيق:

تصدر سلطات التوقيع الإلكتروني الشهادات التالية:

- شهادة تشفير: تستعمل في أغراض تشفير البيانات والمراسلات لحفظها بشكل سري وآمن أثناء التعاملات الإلكترونية.
- شهادة هوية: عبارة عن توثيق أو هوية إلكترونية صادرة من جهة التصديق على كارت ذكي (Smart Card) أو عملة ذكية (Smart Token) للتعريف بحامل الشهادة والإقرار بأنه الشخص المعني الواردة مواصفاته في الوثيقة. وبناءً على ذلك فهو مصرح له بما تمنحه الوثيقة من صلاحيات. على سبيل المثال تعتبر بطاقة الأحوال المدنية وثيقة هوية لأنها تقر بأن الشخص الوارد اسمه في البطاقة مصري الجنسية وإن اسمه الكامل ورقم بطاقته كما هو ظاهر في البطاقة. وتبعاً لذلك فهو يتمتع بالصلاحيات الممنوحة للمواطن المصري. كذلك فإن بطاقة الصراف الآلي وبطاقة التأمين الصحي للمستشفى وغيرها من البطاقات عبارة عن إقرار بأن الاسم الظاهر في البطاقة له الحق في التمتع بالصلاحيات والميزات التي تمنحها هذه البطاقة. وبما أن "شهادة التوقيع الإلكتروني" التي حصل عليها المواطن من سلطة التصديق الحكومية أو الجذرية عبارة عن "شهادة هوية" فإنها تستخدم كذلك في إجراء التوقيع الإلكتروني طبقاً للضوابط الفنية والتعاقدية التي يلتزم بها حاملي الشهادات.

وتقع شهادات التوقيع الإلكتروني تحت ثلاثة فئات رئيسية هي:

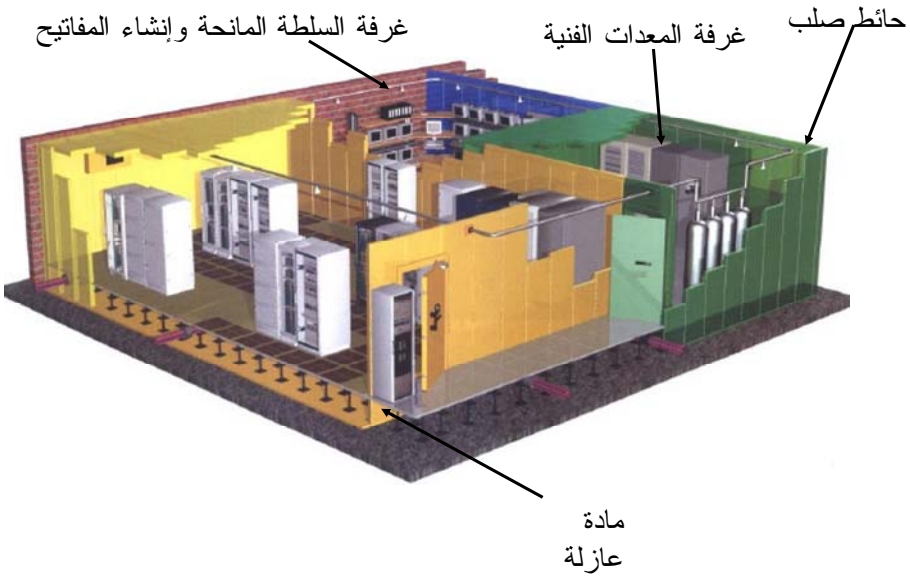
- شهادة من فئة (أ): تكون هذه الشهادة عالية الوثوقية ويتطلب إصدارها التحقق الكامل من هوية صاحبها بالحضور الشخصي لدى مركز التصديق الحكومي أو الجذري وبالتالي يتم التحري عنه. وقد يستلزم الأمر أخذ بصمة صاحب الشهادة أو أي صفة حيوية له. وتستخدم هذه الشهادة لأغراض التحقق من الهوية في بعض التطبيقات الحكومية والتجارية المهمة كإصدار جواز السفر أو تجديده.
- شهادة من فئة (ب): تكون هذه الشهادة متوسطة الوثوقية وتبعاً لذلك تقل شروط وضوابط إصدارها عن الفئة (أ). وقد تستخدم لأغراض التجارة الإلكترونية أو الحكومة الإلكترونية متوسطة الحساسية. على سبيل المثال قد تستخدم هذه الشهادة في بعض التطبيقات الحكومية التي من خلالها يستطيع المستخدم الحصول على معلومات شخصية خاصة به أو إجراء عملية معينة لا تعتبر ذات حساسية عالية.
- شهادة من فئة (ج): هذه الشهادة عبارة عن وسيلة تعريف إلكترونية قليلة الخطورة ولا يتطلب استخراجها أي نوع من التحقق من هوية صاحبها وتستخدم في التطبيقات غير الحساسة. على سبيل المثال لمنح المستخدم مساحة تخزينية صغيرة في موقع حكومي إلكتروني أو في التعاملات التجارية والمالية المحدودة.

4-6-5 متطلبات الأمن والتشغيل لسلطة التوقيع الإلكتروني

هناك عدد من المتطلبات والتجهيزات الفنية والإدارية الواجب توافرها في مركز "سلطة التوقيع الإلكتروني" التي تعتمد على بنية المفاتيح العامة لكي تتم أعمال التشغيل بشكل سليم وآمن. ومن أهم المتطلبات الآتي:

1) فمن حيث التأمين المادي للموقع فان مركز "سلطة التوقيع الإلكتروني" هو غالبا ما يكون له مثل تجهيزات نظم المعلومات العسكرية المؤمنة طبيعياً طبقاً للشكل رقم (17). ويتم الرجوع لبند 3-8-1 الخاص بالتأمين الطبيعي لموقع الأجهزة الذي يحدد تجهيزات المواقع الحصينة ومن ضمنها "مركز التصديق الإلكتروني".

مثال لتصميم موقع السلطة الرئيسية المانحة للشهادات



الشكل رقم (17): مثال لتصميم التأمين المادي للسلطة الرئيسية
المانحة لشهادات التوقيع الإلكتروني

2) من حيث التجهيزات الفنية كأجهزة الحاسبات الخادمة (servers) فغالباً يتكون المركز من عدد كبير من الأجهزة والحاسبات الخادمة لإصدار الشهادات والتوقيع عليها والتي غالباً ما تحتوي على خوارزميات التشفير عالية السرية. وكذلك توجد معدات استخراج الأرقام العشوائية Hardware Security Modules HSM التي تستخدم في إنتاج المفاتيح السرية والمفاتيح العلنية لخوارزم RSA السابق الإشارة إليه. وهناك أجهزة أخرى تختص بإدارة قواعد البيانات والتطبيقات. وأجهزة تعمل كخادم تطبيقات الويب والبريد الإلكتروني ونقل الملفات الخاصة بالسلطة. إلى جانب أنظمة الحفظ والأرشفة وأنظمة حماية الشبكة من الاختراقات وأنظمة تأمين الأجهزة والشبكات مثل الجدران النارية ومضادات الفيروسات.

ويجب أن تكون هناك آلية متكاملة لإعادة تشغيل المركز في حالة وقوع كارثة أو خلل كبير ومن الممكن أن يتم ذلك عن طريق حفظ نسخة من الأجهزة والبرمجيات في مركز الطوارئ.

3) إدارة المفاتيح والشهادات: نظراً لكون مفاتيح التشفير تقع في صلب عمل مركز التصديق فيجب أن يتولى المركز عمليات إدارة مفاتيح التشفير من الألف إلى الياء. وتشمل العمليات استخراج المفاتيح وحفظها وأرشفتها وتوزيعها على المستفيدين واستعادتها في حالة فقدانها أو إلغائها. ويقوم المركز كذلك بإدارة الشهادات الرقمية منذ وقت صدورها مروراً بنشرها واستخدامها وحفظها حتى يتم تجديدها أو إلغائها أو إتلافها.

4) وثيقة البيئة التشغيلية: هي عبارة عن وثيقة تبيّن الطرق المتبعة من قبل مركز التصديق للقيام بمهامه وتشمل إعداد الأنظمة وقواعد التشغيل وتحديثها باستمرار والإجراءات الأمنية المادية والبيئية وتلك المعنية بالأفراد إلى جانب إدارة أنظمة الدخول والخروج والحفظ والأرشفة والتطوير والصيانة وغيرها.

5) إصدارات أو وثائق مركز التصديق: يصدر مركز "سلطة التوقيع الإلكتروني" الوثائق التي تحقق إرساء الأمن والوثوقية وإضفاء المصداقية في طريقة عمل المركز والإجراءات المتبعة فيه. ويتم نشر تلك الوثائق للعامة على موقع ويب مركز "سلطة التوقيع الإلكتروني". ومن أهم الوثائق الآتي:

- وثيقة سياسة الشهادة الرقمية (Certificate Policy): وتحدد هذه الوثيقة مدى الثقة المطلوب افتراضها في الشهادات الصادرة من مركز التصديق والأوجه المشروعة لاستخدامها إلى جانب التزامات مركز التصديق تجاه الأطراف المستفيدة وحقوق المستخدمين.
- إجراءات التصديق الرقمي (Certification Practice Statement): يستطيع المستخدم معرفة الطرق الفنية والأمنية والإجرائية المتبعة لإصدار الشهادة من قبل مركز التصديق عن طريق تلك الإجراءات. وهي عبارة عن اللائحة التنفيذية لسياسة الشهادة الرقمية.

والخلاصة أن شهادات التوثيق عبارة عن ملفات مشفرة يتم تخزينها على البطاقة الذكية (Smart Card) أو وحدة العملة الذكية Token الخاصة بحامل الشهادة. يتم تسجيل بيانات الشهادة ونشرها على موقع ويب مركز "سلطة التوقيع الإلكتروني" حتى يستعان بها لمعرفة موقف كل شهادة (هل هي سارية المفعول أم ملغاة). وآلية توفير الحماية PKI هي التي تؤسس عليها الشهادات وبشكل أساسي هي الآلية الخاصة بتخزين المفاتيح السرية والعلنية التي تحدد مالك الشهادة. ويشترط ألا يمكن بأي حال معرفة المفتاح السري الخاص بكل شخص حتى من قبل سلطات التوثيق. وتقوم سلطات التوثيق بعمل قاعدة بيانات لتسجيل حاملي الشهادات سواء أفراد أو مواقع أو برامج وبالتالي يتم التأكد من هويتهم قبل التعامل معهم. كما يتم إبطال الشهادات غير الصحيحة أو الملغاة ونشر شهادات جهات التوثيق على نطاق واسع من خلال موقع الويب.

وتحقق سلطات التصديق الإلكتروني وشهادات التوثيق وآلية توفير الحماية PKI جميع المعايير والأهداف الأمنية التي تحتاج إليها التطبيقات الإلكترونية والتي من أهمها:

1) الخصوصية بالحماية ضد التصنت.
2) نزاهة المحتوى بالحماية ضد تبديل المحتوى.
3) إتاحة البيانات.
4) الحماية ضد الإنكار.
5) الحماية ضد محاكاة المواقع عن طريق توثيق المواقع الصحيحة فقط.

الفصل السادس

تأمين الإنترنت

1-6 مقدمة

لقد تم بناء بروتوكول الإنترنت TCP/IP من أربعة طبقات أو بروتوكولات أساسية كما ذكرنا في الفصل الثاني وكل طبقة مسؤولة عن مهمة ما تساعد في تداول حزم البيانات وتتفاعل كل طبقة مع الطبقات المجاورة لها إذ تقدم الطبقة خدماتها إلى الطبقة الموجودة تحتها وتطلب الخدمة من الطبقة التي أعلاها.

وحيث إنه قد تم شرح مهام الطبقات في الفصل الثاني فسنكتفي هنا بتقديم ملخص عن اختصاصات كل طبقة تمهيداً لتحديد وسائل التأمين الأمثل لكل طبقة:

- تختص طبقة الربط الطبيعي بتحديد خصائص وسط الاتصال وطبيعة الإشارات المتبادلة عليه ومعدل سريان البيانات وعملية التشفير الانتهائي (إن وجدت). كما تختص بتبادل البيانات بين المعدة النهائية (حاسب خادم أو شخصي) وبين معدات الشبكة المحلية. ويتم ذلك من خلال بروتوكول نقطة إلى نقطة ((Point to Point Protocol (PPT) أو بروتوكول الإثرنت (ETHERNET).
- تختص طبقة بروتوكول الشبكة IP بتداول حزم البيانات فيما بين المعدات الانتهائية المتصلة بعدة شبكات من خلال وجود الموجهات وبوابات الربط. ينشأ هذا البروتوكول مسارات لكل حزمة بيانات وهذه المسارات تتكون من مجموعة عناوين IP لكل معدة موجودة بالشبكات. أي أن الهدف الأساسي من البروتوكول هو تسيير حزم البيانات من خلال الشبكات المتعددة.
- تختص طبقة النقل TCP بسلامة وصول حزم البيانات إلى الوجهة النهائية وأيضاً وصولها بترتيب سليم من خلال وجود آلية مخصصة لذلك تقوم في الإرسال بتحويل الملفات إلى حزم بيانات مرقمة. وفى الاستقبال تستخدم الترقيم في إعادة ترتيب الحزم لتكوين الملف أو الرسالة مرة أخرى. كما تختص طبقة النقل TCP بإنشاء مسارات الربط (Connections) ذات القدرة العالية على البقاء (Reliable).
- تختص طبقة التطبيقات بدعم التطبيقات الخاصة بمطالب المستخدم النهائي من الحاسبات الخادمة بالشبكة من خلال تحقيق الربط والتفاعل والتزامن بين برنامجين هما الخادم والعميل بحيث يكون هناك تطبيق للخادم (ممثلاً في موقع الويب أو البريد الإلكتروني) وتطبيق مقابل له للعميل (ممثلاً في المتصفح). العميل يحدد مطالبة على هيئة استفسارات (Queries) والخادم يحققها على هيئة أجوبة (Responses).

إن حركة حزم البيانات المتبادلة على الإنترنت ضخمة جداً ويطلق عليها عدة تعبيرات مثل "نهر المعلومات المتدفق" أو "فيضان أو فورة المعلومات". وتتضمن الحزمة حقول بيانات خاصة بعنوان الحاسب المرسل والمرسل إليه وبروتوكول الإنترنت المستخدم ونوع المتصفح المستخدم ونوع الحاسب وآخر ما قام به المستخدم في زيارته الأخيرة السابقة للموقع وربما

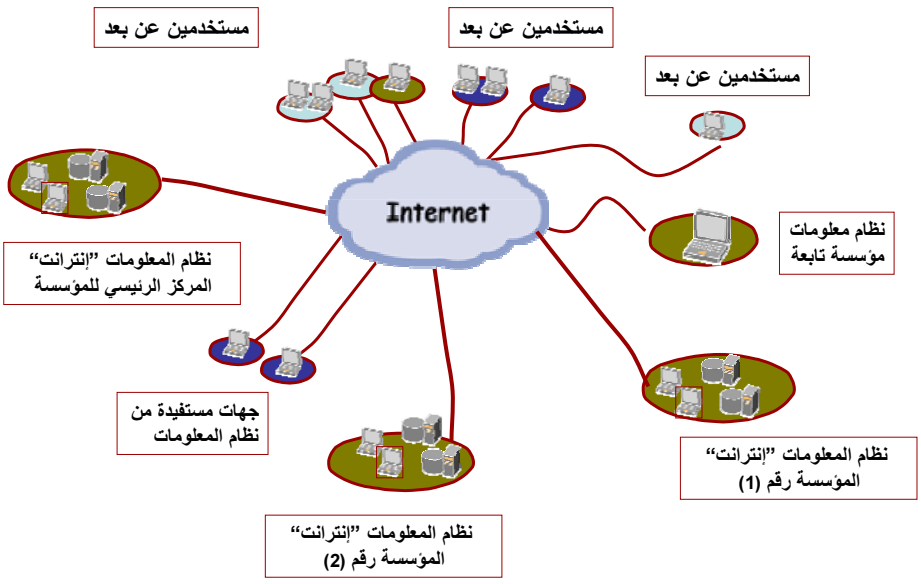
المواقع الأخرى التي زارها. بالإضافة إلى ذلك فإن الإنترنت عبر بروتوكولات الاتصال بين الحاسبات الخادمة ونظم إدارة الشبكات تصنع قدراً كبيراً من المعلومات عند كل وقفة في فضاء الشبكة. كل هذه البيانات قد يتم اصطيادها ومعرفتها وجمعها في نقاط عديدة في الرحلة عبر الشبكات وهو ما يثير مخاطر إساءة استخدام هذه البيانات مما يستلزم وجود مستويات من التأمين والحماية التقنية والإدارية والقانونية للإنترنت وهو ما سنتعرض له تفصيلاً في هذا الفصل.

ونتيجة لسرعة انتشار الإنترنت زادت طلبات المستفيدين من الشركات المنتجة بهدف تصنيع معدات وتطوير برامج تسهل التعامل مع الشبكات باستخدام برامج ذات أوامر وتعليمات تتيح لأي فرد استخدامها. والمعروف أنه كلما كان بروتوكول ولغة التعامل مع الشبكة سهلة كلما تزايد عدد الدخلاء عليها وكلما زاد بالتالي عدد القراصنة والمتطفلين (Hackers) والمتلصصين (Message Tapping/ Eavesdroppers) عليها وكلما ألقى ذلك عبء كبير على أساليب التأمين والحماية. لذلك كان من الطبيعي أن تتعرض شبكات المعلومات للعديد من التهديدات المتعلقة بسرية المعلومات التي قد تكون على هيئة اختراقات أمنية تهدف إلى تدمير وسرقة المعلومات وحرمان المؤسسة من استغلال مواردها لاستفادة الدخيل الشخصية.

وتواجه الشبكات التهديدات الأمنية من مجموعة واسعة من المصادر مثل الاحتيال أو التجسس أو التخريب أو التدمير. كما قد تواجه أخطار أعطال في المعدات أو البرامج أو في مصادر التغذية. وكذلك هناك الأخطار والكوارث الطبيعية مثل النيران والزلازل والفيضان. أصبح حالياً زرع فيروس الحاسبات والبرامج الخبيثة وأعمال القراصنة وهجمات منع الخدمة أكثر شيوعاً وأكثر طموحاً وأكثر تطوّراً.

يهدف تأمين الإنترنت إلى توفير الحماية لبيانات ومصادر معلومات المؤسسة التي تعتمد على الإنترنت كجزء هام من بنيتها المعمارية طبقاً للشكل رقم (1).

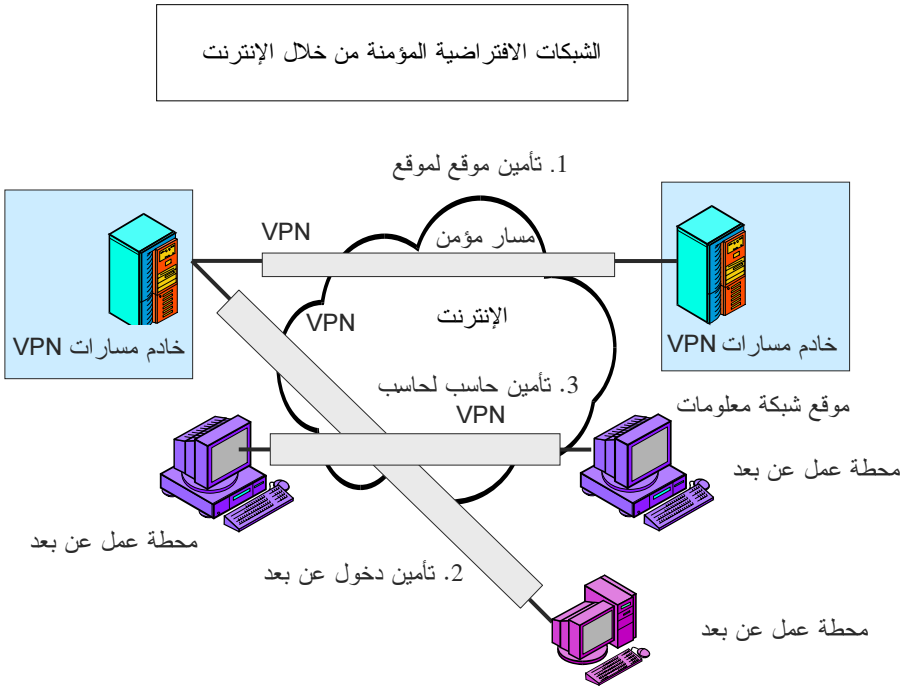
2



الشكل رقم (1): نظام المعلومات المعتمد على الإنترنت

تستغل الإنترنت في تنفيذ تطبيقات العمل الخاصة بالمؤسسة لتحقيق مزايا من أهمها التغطية الشاملة للاتصالات على المستوى القومي والدولي وخفض التكلفة مقارنة بالوسائل الأخرى. وقد تستغل الإنترنت في تنفيذ عدة تطبيقات من أهمها:

1) الربط بين المواقع المنتشرة جغرافياً بتكوين شبكات افتراضية مؤمنة (Virtual Private Networks (VPN)) بين مواقع الحاسبات الخادمة (تأمين موقع لموقع) وبين الحاسبات الخادمة ومحطات العمل الثابتة والمتنقلة (تأمين دخول عن بعد) أو بين محطات العمل (تأمين حاسب لحاسب) طبقاً للشكل رقم (2) وبند 6-5-1-2-1.
2) نقل الملفات وتداول البريد الإلكتروني والاتصالات الهاتفية ببروتوكول الإنترنت.
3) الحصول على المعلومات التي تساعد في تنفيذ تطبيقات العمل.
4) نشر المعلومات من خلال موقع الويب بغرض تسويق المنتجات أو تعريف الأفراد بأنشطة المؤسسة.
5) توفير اتصال دائم (24 ساعة يومياً لمدة 7 أيام أسبوعياً) لكافة المستفيدين من نظام المعلومات بسهولة ويسر.



الشكل رقم (2): الشبكات الافتراضية المؤمنة من خلال الإنترنت

ويتحقق تأمين الإنترنت من خلال التوافق بين الوسائل التقنية وإجراءات "السياسة الأمنية" وبالتالي تتحقق الأهداف التالية:

1) يكون للأفراد المصرح لهم فقط الحق في الدخول على البيانات ومصادر المعلومات.
2) تكون الاتصالات داخل الإنترانت (الشبكات المحلية) بعيدة عن متناول الدخلاء والمتصنتين والمتطفلين.
3) تكون البيانات المتداولة عبر الإنترنت مؤمنة ضد الاطلاع غير المشروع أو المحو أو التغيير.

4) تكون البيانات ومصادر النظام متاحة للمستفيدين منها بكفاءة وبدون اختناقات.
5) يتم تحقيق أهداف المؤسسة وتكون البيانات والمعلومات مؤمنة ومتكاملة ومتاحة وموثوق فيها وتستخدم في اتخاذ القرارات.
6) تكون البيانات ومصادر المعلومات مؤمنة طبيعياً ضد الأعطال والأخطاء الطبيعية والمنطقية.

ويتم تأمين الإنترنت على محورين هما:
1) تأمين نظام المعلومات نفسه على مستوى الإنترانت.
2) تأمين الربط بين الإنترانت والإنترنت.

2-6 تأمين الإنترانت والإنترنت

1-2-6 معايير التأمين

يهدف تأمين نظام المعلومات إلى توفير كافة وسائل وأساليب التأمين والحماية للمعلومات وللمستفيدين منها بتحقيق معايير التأمين الآتية:

1) السرية والخصوصية (Confidentiality)

تعني السرية حماية البيانات ومصادر المعلومات من الوقوع في أيدي أي فرد ليس له حق الإطلاع عليها أو استخدامها ويتم حماية البيانات ضد الاستخدام غير المشروع بتحديد صلاحيات الوصول للبيانات وتحديد مسؤولية كل من يستخدم هذه البيانات وعدم السماح لأشخاص بتنفيذ إجراء معين على البيانات لا يمتلكون الصلاحيات الكافية لتنفيذه. ويتم تنفيذ السرية من خلال تفعيل وسائل التحقق من الهوية وصلاحية الوصول (Access Control) طبقاً لدرجة التصنيف التي تعكس مدى حساسية تلك البيانات لنظام المعلومات. وبواسطة استغلال النظم التشفير أثناء تداول البيانات أو تخزينها في أوساط التخزين الذي تمت الإشارة إليه في الفصل السابق.

2) تكامل البيانات (Integrity)

يهدف التكامل إلى التأكد من أن محتوى البيانات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لم يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التفاعل الداخلي أو عن طريق تدخل خارجي غير مشروع. وتتم هذه العملية باستخدام تقنية تشفير البيانات ((Message Authentication Code (MAC) وبالتوقيع الإلكتروني (Digital Signature) الذي تمت الإشارة إليه في الفصل السابق.

3) الإتاحة (Availability)

تهدف الإتاحة إلى التأكد من استمرارية عمل كافة مكونات النظام وفعاليته في تنفيذ مهامه من جهة إتاحة البيانات ومصادر المعلومات وتقديم الخدمة لمواقع المستفيدين. كما تهدف الإتاحة إلى التأكد من أن مستخدمي نظام المعلومات لن يتعرضوا إلى منع استخدامه أو الدخول إليه.

4) المسؤولية (Accountability)

تهدف المسؤولية إلى متابعة ومراقبة وتتبع التفاعلات التي ينفذها كل مستخدم على البيانات ومصادر المعلومات وفي أي وقت حيث يكون المستخدم مسؤول عن تفاعلاته مع النظام.

5) عدم الإنكار (Repudiation Non)

يهدف عدم الإنكار إلى التأكد من المرسل والمستقبل للبيانات ومن توقيت الإرسال وعدم إنكار أي منهما لها أو عدم التملص منها ويتم ذلك بوجود طرف ثالث (سلطة إصدار شهادات التوثيق والتوقيع الإلكتروني) يمكنه إثبات قيام طرف معين بفعل إلكتروني معين في وقت وزمن معين (Time Stamp) كذلك يضمن عدم قدرة مستلم لرسالة معينة على إنكار استلامه لها.

6) كفاءة إدارة الشبكة (Network Management)

تدار الشبكة من خلال توفير برامج ومعدات إدارة الشبكة (Network Management) التي تتضمن وسائل: مراقبة إشارات الإنذار عن الأعطال والأخطاء – اكتشاف وإصلاح الأعطال – تسجيل حركة حزم البيانات – وتسجيل التفاصيل الدقيقة عن ما يتم في شبكة المعلومات شاملاً ذلك بيانات تعريف المستخدمين (كلمات المرور وأحقيات الدخول لكل فرد) والمعدات والبرامج وخدمات وموارد الشبكات المحلية والواسعة والإنترنت التي يستغلها الأفراد. كما توفر الوسائل كل المعلومات عن نتائج سجلات التدقيق (Auditing) والتشغيل والتفتيش والاختبارات وتقارير عن حالات الانتهاكات الأمنية السابقة وإجراءات معالجتها. وتعتبر هذه المعلومات الهامة بمثابة قواعد المعرفة للنظام.

يعتبر تأمين شبكات المعلومات أهم ما يشغل بال الإدارات العليا والمدير المسؤول عن نظام المعلومات. وكلما زاد اعتماد المؤسسة على بيانات أنظمة المعلومات والوسائل والخدمات الآلية كلما كانت أكثر عرضة للتهديدات الأمنية.

ومن المهم تأمين شبكات المعلومات على عدة مستويات (الربط الطبيعي – الشبكات – التطبيقات) وهناك حاجة ماسة لتعدد هذه المستويات بهدف وجود أكثر من خط حماية للبيانات ومصادر المعلومات وبالتالي تزيد درجة السرية والنزاهة والتكامل مما يكون له تأثير كبير على التفوّق التنافسي والالتزام القانوني والصورة التجارية للمؤسسة.

وتزيد نظم المعلومات الموزعة والمتعددة الفروع وعلاقات العمل صعوبة في تنفيذ التأمين خاصة من ناحية التحقق من هوية العدد الكبير من المستخدمين المحليين والخارجيين وصلاحيتهم. وبالتالي يمكن القول بأن استخدام نظم الحاسبات الموزعة أضعف فعالية وسائل تأمين الشبكات. كما أن العديد من أنظمة المعلومات لم تصمّم من البداية لتكون آمنة والمعروف أن وسائل تأمين المعلومات تكون أكثر فعّالية وقليلة التكلفة إلى حدّ كبير إذا تم اتخاذها إثناء وضع المواصفات وتحديد المطالب وفى مرحلة التصميم.

6-2-2 المكونات الرئيسية في الإنترانت المعرضة للمخاطر

تتعرض المكونات الأساسية لنظم المعلومات للمخاطر أو الاختراقات أو الأعطال أو الأخطاء أو الكوارث وهي:

1) الأفراد: الأفراد هم المستخدمون والمشتركون والمستفيدون من شبكة المعلومات ويشملوا الإدارة العليا – المديرين بالقطاعات – طاقم عمل نظام المعلومات – المتعاقدين – مقدمي الخدمة – المتعاونون والمشاركون في الأنشطة. وهؤلاء هم محور النجاح وفى نفس الوقت مصدر الخطر خاصة طاقم المشتغلين أو المستخدمين أو الفرد المناط به تنفيذ مهام تقنية معينة تتصل بالنظام.

كما أن هناك وظائف في الهيكل التنظيمي تتيح لصاحبها كلمات مرور وأحقيات دخول على بيانات ومصادر المعلومات الحساسة جداً ومن الممكن أن يمثلوا خطراً كبيراً على النظام (مثل مدير قواعد البيانات أو مدير الشبكات أو مهندسي الصيانة). وللأفراد دوراً رئيسياً في تأمين نظام المعلومات والشبكات بل يعتبر العنصر البشري من أهم مصادر النظام والسبب الرئيسي لنجاح المؤسسة في تنفيذ أهدافها وفى نفس الوقت فالمخاطر الأمنية والأعطال والمخاطر الطبيعية قد يكون مصدرها الأفراد (بقصد أو من غير قصد) وربما تؤثر على عمل ومستقبل وربما حياة الأفراد. ويتحقق تأمين الأفراد من خلال إدراك كل منهم بحدود صلاحياته وإدراكه آليات التعامل مع الخطر وتسليمه بأهمية الرقابة على أنشطته في حدود احترام حقوقه القانونية. وهي مسائل رئيسة يعنى بها نظام الأمن الشامل تحديداً في بيئة العمل الموزعة المرتكزة على نظم الحاسبات وقواعد البيانات.

2) الأصول المعلوماتية: مثل ملفات البيانات – وثائق النظام – أدلة المستعمل – برامج تدريبية – إجراءات دعم فني – خطط الاستمرارية – إجراءات الاحتياطي – أرشيف المعلومات.

3) أصول برمجيّات: مثل برامج تطبيقية وبرمجيّات ونظم وأدوات التطوير.

4) أصول مادية: مثل أجهزة الحاسبات (المعالجات – أجهزة تحويل وتوجيه – حاسبات محمولة – أجهزة اتصالات نقل بيانات مثل المودم وخلافه) وأجهزة اتصالات تليفونية (مسارات – سنترال داخلي – أجهزة فاكس) وأجهزة تخزين مغناطيسية (أشرطة وأقراص) وأجهزة تقنية أخرى (تجهيزات طاقة – تكييف) وأثاث وخلافه.

5) الشبكات والاتصالات: وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها ببعض محلياً ودولياً وعالمياً بالإنترنت. وتتيح فرصة اختراق النظم عبرها كما أنها بذاتها محل للاختراق وموطن من مواطن الخطر الحقيقي.

6) قواعد البيانات: وهى الثروة الحقيقية للأنظمة وما سيكون محلاً للجرائم. وتشمل كافة البيانات الداخلة والمعلومات المستخرجة عقب معالجتها وتمتد بمعناها الواسع لبرمجيات التطبيقات التي تستخدم للدخول على البيانات. والبيانات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات. وقد تخزن داخل النظم أو على وسائط التخزين الخارجية.

ولقد ازدادت الحاجة إلى تأمين قواعد البيانات بانتشار الشبكات خاصة الشبكات الواسعة (Wide Area Networks) والإنترنت نظراً لكون التطبيقات هي وسيلة وصول المستخدم للبيانات. وعندما تتبنى المؤسسة استخدام نظم الأعمال الإلكترونية والتطبيقات المعتمدة على شبكة الإنترنت تتعرض قواعد البيانات للانتهاكات أيضاً من خلال أخطاء البرمجة أو برامج التطبيقات التي تعتمد على الإنترنت في نقل الملفات أو البريد الإلكتروني أو الدخول عن بعد على قواعد البيانات للبحث أو التعديل.

بإمكان قواعد البيانات المؤمنة التصدي لمحاولات الاختراق الممكن حدوثها ويقوم نموذج قواعد البيانات بتطبيق التحكم في التعريف بهوية المستخدم وصلاحية الاستخدام (Identification and authentication) وذلك بتطبيق سياسات الحماية والتأمين مباشرة على البيانات بصرف النظر عن التطبيق أو الأداة المستخدمة للوصول لها. ومن هنا يكون التركيز على تأمين وحماية قواعد البيانات نفسها بدلاً من التركيز على إضافة مستويات التأمين لكل تطبيق مما يؤدي لخفض التكلفة.

تعد قواعد البيانات العنصر الأساسي لشبكات المعلومات وهو من دون شك أهم ما تملك المؤسسة وتحرص على تأمينها وحمايتها وبالتالي يجب على مدير المؤسسة وكيان الأمن بها التأكد من أن هذا الجزء من البنية المعمارية للنظام يتمتع بالنصيب الأكبر والمستوى الملائم من التأمين والحماية ضماناً للسرية والوثوقية والتكامل وبالتالي زيادة ثقة متخذي القرارات والمؤسسين والعملاء في البيانات والمعلومات التي تصل إليهم من نظام المعلومات.

يؤكد خبراء تأمين شبكات المعلومات إن كثير من الاختراقات الأمنية التي تحدث تكون من داخل المؤسسات وفى مثل هذه الحالات تكون تكنولوجيا الدفاع المتوافرة مثل الجدران النارية أو الحوائط النارية (Firewalls) ليست ذات قيمة. ووفقاً لدراسة قام بها معهد أمن وسرية المعلومات المعروف باسم (USA CSI, Computer Security Institute) ومكتب التحقيقات الفيدرالية (FBI, Federal Bureau Of Investigation) فإن العاملين من داخل المؤسسة يعتبرون مسؤولين عن 47% من الانتهاكات الأمنية. وقد تركز المؤسسة أكثر اهتمامها على الانتهاكات الأمنية الخارجية لكن مثل هذه الإحصائيات توضح أنه من الضروري الاهتمام بالتأمين الداخلي أيضاً عن طريق وسائل مثل مراقبة صلاحيات الوصول (Access Rights) الممنوحة للموظفين الداخليين واستخدام الأنظمة الشفرية بنفس قدر الاهتمام بتأمين قواعد وشبكات المعلومات من الانتهاكات الأمنية الخارجية.

وتلجأ معظم المؤسسات لاستخدام الاسم وكلمة السر (User Name and User Password) لمنح صلاحية الوصول للشبكة. لكن في أغلب الأحيان قد تمثل وسائل تعريف المستخدم هذه خطراً رئيسياً حينما يساء استخدامها ويسهل اكتشافها أو استنباطها. وتضم هذه الطائفة كلمات المرور بأنواعها والبطاقات الذكية المستخدمة للتعريف ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي ومختلف أنواع المنتجات التي توفر كلمات سر آلية أو وقتية متغيرة إلكترونياً والمفاتيح المشفرة. بل تضم هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ للنظام. وتعد صلاحية الوصول التي يتم منحها بناء على الطرق البيولوجية للتحقق من الهوية (مثل إجراء مسح لشبكية أو قرنية العين أو بصمات الأصابع أو الصوت) من أهم طرق التحكم الأمنية مستقبلاً لكنها في الوقت الحالي صعبة المنال ومكلفة بالنسبة لمعظم المؤسسات.

ولحماية شبكة المعلومات من الانتهاكات الداخلية فإن أقل شيء تستطيع المؤسسات تبنيه هو وضع "السياسة الأمنية" المشددة لتحديد الأفراد الذين يتم منحهم حق الوصول للبيانات والمعلومات داخلياً وخارجياً من الإنترنت. بالإضافة إلى تحديد أضعف أجزاء الشبكة والتي قد يسهل اختراقها والاهتمام بتأمين هذه الأجزاء عن طريق مستشعرات (Sensors) تقوم بالمسح الدائم لها لسرعة اكتشاف أي اختراقات أمنية والتغلب عليها.

تمثل سرقة بيانات الملكية الفكرية (الابتكارات والاختراعات الحديثة في المعدات والبرامج) والاحتيالات التي تتعلق بالنواحي المالية أكثر ما يسبب الخسائر المادية والمالية ويؤدي إلى مخاطر فقد السمعة. فالمؤسسة من واجبها نحو المستفيد منها وعملائها ومالكي أسهمها حماية الأصول الخاصة بها الفكرية منها والمادية. والسرقة المباشرة من خلال الشبكات العامة مثل

الإنترنت تمثل خطر دائم يهدد هذه الأصول ويهدد أيضاً استقرار تطبيقات الأعمال خاصة الحديثة مثل التجارة الإلكترونية والحكومة الإلكترونية.

وعلى سبيل المثال فالمعروف أنه من خلال التجارة الإلكترونية يتم يومياًعلى الإنترنت تداول تفاعلات وحركات مالية تقدر قيمتها ببلايين الدولارات. وتحتاج المؤسسات المالية إلى ضمان الأمان لهذه الحركات بالإضافة إلى التكاليف المباشرة التي تتمثل في تكلفة نظم المعلومات. كما أنه يصعب تقدير التأثير المالي الذي قد يؤدي إليه التهديد الأمني والذي قد ينتج عنه فقدان ثقة العميل وأصحاب الأسهم في معلومات المؤسسة إلى جانب فقدان القدرة على اكتساب عملاء جدد. ولذلك فإنه يجب على المؤسسة التعامل مع الحلول المتعلقة بالحماية والتأمين باعتبارها استثمارات على المدى الطويل تكتسب من خلالها مصداقيتها وثقة باقي المؤسسات بها والشركاء والموردين والمساهمين والعملاء.

6-2-3 تأمين الربط مع الإنترنت

لقد تركزت أغلب وسائل التأمين التقنية على حماية الربط مع الإنترنت باعتبارها الوسيلة الأكثر فاعلية وكفاءة والأقل تكلفة. ومما أشعر مديري تكنولوجيا شبكات المعلومات بالارتياح ظهور وسائل تقنية حديثة لتأمين الربط مع الإنترنت مثل الجدران النارية (Firewalls) ووسائل منع وسرعة الكشف عن التداخلات (Intrusion Prevention/Detection) وترجمة العناوين (Network Address Translation NAT) والشبكات الافتراضية المؤمنة (Virtual Private Networks VPN) ووسائل مسح الشبكات وبرامج الكشف السريع عن الفيروسات (Virus Detection) والتغلب عليها (وهذا ما سنتناوله في هذا الفصل). بالإضافة لاستخدام وسائل التشفير (Encryption) وشهادات التوثيق والتوقيع الإلكتروني (التي تم تناولها في الفصل الخامس). [المراجع أرقام (27 و48 و57 و69)]

والجدير بالذكر أن الحماية ضد الاختراقات الأمنية التي يمكن إنجازها من خلال الوسائل التقنية برغم تطورها وأهميتها محدودة التأثير حيث إنها تعتبر "ضرورية ولكنها غير كافية". ويلزم أن تكون مدعومة بالإجراءات الأمنية الملائمة (السياسة الأمنية) ولذلك تتطلب وسائل التأمين المتميزة التخطيط والانتباه الحذر لكافة التفاصيل. كما تتطلب إدارة أمن المعلومات مشاركة جميع المستفيدين من النظام. وغالباً ما يحتاج الأمر أيضاً إلى الاستعانة بالنصيحة الأمنية المتخصصة من الجهات أو الإفراد المتخصصين الموثوق بهم خاصة عند حدوث حالات اختراق أمني.

6-3 المواصفات القياسية لنظم الحاسبات والشبكات المؤمنة

6-3-1 البنية المعمارية للتأمين

تهدف البنية المعمارية للتأمين إلى توفير الحماية للإنترنت على عدة مستويات من أهمها الحماية ضد الدخول غير المصرح به على البيانات بهدف التصنت أو المحو أو التغيير أو الحجب. ومن المهم جداً أن تعرف كل مؤسسة كيف تصنف المستوى الحالي لتأمين شبكة المعلومات الخاص بها حتى يمكن اتخاذ القرارات التي ترفع من مستوى التصنيف تدريجياً إذا أرادت ذلك على مراحل طبقاً للتكلفة المالية المتاحة. علماً بأن التأمين يشتمل على اقتناء وسائل التأمين التقنية بالإضافة إلى تحرير وثيقة "السياسة الأمنية" وتطبيقها على جميع المستويات الإدارية بالمؤسسة.

ولقد صنفت وثائق تأمين نظم وشبكات المعلومات القياسية لوزارة الدفاع الأمريكية أربعة بنيات معمارية للتأمين في أعلاها البنية "أ" الذي تحقق الحد الاقصى من مستويات التأمين وفي أدناها البنية "د" الخاصة بالحد الأدنى من التأمين. [المراجع أرقام 41 و42] كما حددت الوثائق لكل بنية سبعة مستويات تأمين فرعية.

وقد صدرت عدة وثائق للمواصفات القياسية لبنية تأمين النظم نذكر منها الآتي:

1) Trusted Computer System Evaluation Criteria (TCSEC)
2) Orange Book (USA MOD 1996)
3) Red Book (USA MOD 1999)

وتعتبر وثيقة "الكتاب الأحمر" هي الأحدث وهى تتضمن المعلومات الإضافية التي تجعل ما تضمنه "الكتاب البرتقالي" ملزماً خاصاً عندما يكون نظام المعلومات متصل بالإنترنت. كما أن هذه الوثيقة صدرت لتشمل تأمين الشبكات عند العمل بنظام المعلومات وبالمواصفات (TCSEC). وبذلك يعتبر "الكتاب الأحمر" و"الكتاب البرتقالي" بمثابة وثائق تأمين للإنترنت وبدأت الشركات في تنفيذ بنود تلك الوثائق خلال مراحل إنتاجها للنظم بهدف الحصول على "شهادة إجازة" لمعداتها وبرامجها وشبكاتها حيث إن الحصول على شهادات الإجازة تزيد من انتشار وتسويق منتجاتها على المستوى العالمي.

2-3-6 تصنيف شبكات المعلومات طبقاً لمستوى التأمين بها

طبقاً لمستوى التأمين فإن "الكتاب البرتقالي" يتضمن شرح لأربعة بنيات معمارية رئيسية قياسية هي: أ وب وج ود خاصة فيما يتعلق بتأمين الدخول على البيانات ومصادر النظام. حيث إن التعرف على الهوية وأحقيات الدخول لكل فرد هو شرط أساسي في تأمين التشغيل وتوفير الهيكل المؤمن لنظام المعلومات وهذه البنيات المعمارية القياسية هي:

1) نظم شبكات المعلومات من البنية المعمارية "د1" : توفر أقل مستوى للتأمين ويعتبر النظم الذي تصنف على أنها "د1" غير موثوق ببياناتها ومعلوماتها وشبكاتها على الإطلاق لأنها فشلت في تحقيق مطالب التأمين التي ذكرناها سابقاً.
2) نظم شبكات المعلومات من البنية المعمارية "ج1" : تصنف ضمن النظم المؤمنة من حيث إنها تسمح للمستخدمين بحماية مشروعات نظم المعلومات وتوفر الحد الأدنى من حماية للبيانات ومصادر المعلومات ضد الدخول غير المصرح به بهدف التصنت أو المحو أو التغيير.
3) نظم شبكات المعلومات من البنية المعمارية "ج2": تصنف ضمن النظم المؤمنة حيث لها القدرة على التحكم في دخول الأفراد على مصادر المعلومات. ويكون لكل فرد حساب خاص به "اسم وكلمة مرور" كما يوفر هذا المستوى سجلات للتدقيق (auditing) وتقارير (journal files) عن حالات الانتهاكات الأمنية السابقة وإجراءات معالجتها.
4) نظم المعلومات والشبكات من البنية المعمارية "ب1" : توفر مستويات تأمين وحماية محددة (Labeled security protection) من خلال عدة مستويات وتسمح للمستخدمين المصرح لهم فقط بالدخول على البيانات ومصادر المعلومات طبقاً لوسائل تعرف على الهوية ولمستويات سماحية محددة وتتضمن وسائل حماية للبيانات ومصادر المعلومات ضد الدخول غير المصرح به من خلال النظم الشفرية.

5) نظم شبكات المعلومات من البنية المعمارية "ب2": توفر مستويات تأمين وحماية متعددة (Structured security protection) من خلال وسائل تعرف على هوية المستخدمين ذات درجة سرية عالية بواسطة الوسائل البيولوجية مع تحديد أحقيات الدخول لكل منهم. وتوفر هذه النظم مستوى حماية متطورة وعالية وتعتبر مقاومة هذه النظم للاختراقات الأمنية متوسطة.

6) نظم شبكات المعلومات من البنية المعمارية "ب3": توفر مستويات تأمين وحماية متعددة (Structured security protection) أعلى من المستوى "ب2" من خلال وسائل تعرف على هوية المستخدمين ذات درجة سرية عالية مع تحديد أحقيات الدخول لكل منهم. يتم استخدام النظم الشفرية أثناء تداول وتخزين البيانات وموقع المعدات مؤمن طبيعياً كما يوفر هذا المستوى سجلات للتدقيق (auditing) وتقارير (journal files) عن حالات الانتهاكات الأمنية السابقة وإجراءات معالجتها ويعتبر مستوى الحماية لهذه النظم متطور وعالي جداً كما تعتبر ذات مقاومة عالية أيضاً للاختراقات الأمنية.

7) نظم شبكات المعلومات من البنية المعمارية "أ1" : يتم تصميم هذه النظم من البداية لتوفر التأمين والسرية والحماية على كافة العناصر (الأفراد – المكان – المعدات – البرامج – الأفراد – الشبكات المحلية والواسعة – الإنترنت – أساليب العمل) لغلق الثغرات الأمنية وتصحيحها بصفة مستمرة. والمستوى "أ1" هو أعلى مستوى تصنيف تضمنه "الكتاب البرتقالي".

وتستخدم هذه النوعية من النظم في تطبيقات ذات مستوى تأمين "سري للغاية" مثل النظم العسكرية ونظم شهادات التوثيق والتوقيع الإلكتروني حيث إن التأمين والحماية متوافر للبيانات المخزنة في قواعد البيانات وعند تبادل تلك البيانات عبر الشبكات.

ويلتزم الأفراد العاملين في هذه النوعية من النظم بتنفيذ إجراءات "سياسة أمنية" محددة وصارمة والمعدات ذات درجة تحصين عالية والبرامج محصنة أيضاً ويتم نقل المعدات والبرامج بأسلوب يوفر لها التأمين والحماية العالية جداً ومكان المعدات محصن وغير قابل لصدور إشعاعات منه وجميع المعلومات مصنفة "سري للغاية".

4-6 المخاطر التي تتعرض لها الإنترنت

عندما يتم ميكنة تطبيقات المؤسسات بتكنولوجيا المعلومات والإنترنت فإن بياناتها ومعلوماتها وأساليب العمل بها سوف تعتمد اعتماداً أساسياً على التأمين والحماية والقدرة على البقاء التي توفرها تلك التكنولوجيا.

وبالتالي يصبح أمن المعلومات أهم من ما يشغل أفراد المؤسسة من المستويات الاستراتيجية العليا إلى المستويات المتوسطة وحتى المستويات التنفيذية والجدول التالي يوضح أنواع المخاطر التي تهدد الإنترنت وشبكات المعلومات.

نوع الخطر/التهديد	التأثير	التعريف بالخطر/التهديد
1- الكشف الغير مشروع للبيانات والمعلومات	• تعريض سرية المعلومات للخطر • الحجز/الإعاقة للبيانات	• إطلاع شخص غير مصرح له على البيانات. • تعمد شخص دخيل حجز أو منع وصول البيانات
2- التعديل الغير مشروع للبيانات والمعلومات	• التغيير/التداخل المتعمد • الخداع/ التمويه	• التغيير الطارئ للبيانات • التغيير المتعمد للبيانات
3- تقييد مصادر وموارد النظام	• الحذف المقصود/الغير مقصود نتيجة تعمد أو أخطاء أو إهمال "منع استغلال الأمثل لموارد النظام	• شطب البيانات والمعلومات
4- زرع الفيروسات والبرامج الأخرى الدخيلة	• التدمير/التسريب/المنع	• تغيير محتويات البرامج • تدمير البيانات والمعلومات • تسرب البيانات إلى خارج النظام • تعطل المعدات (الحاسبات) عن العمل

وتتعرض الإنترنت لعدة مخاطر بعضها نتيجة الإهمال أو سوء الاستخدام وبعضها نتيجة الاختراق أو الانتهاكات وبعضها نتيجة الأعطال أو الظروف المحيطة القهرية (مثل الحرائق وانقطاع التيار الكهربي والزلازل والبراكين والسيول وما شابه).

ومما يسهل الاختراقات والانتهاكات الأمنية على الإنترنت الحقائق التالية:

1) وجود أكثر من موقع على الإنترنت يشرح كيفية اختراق النظم وبه برامج اختراق مثل المواقع: rootshell.com و l-pht.com و 2600.com.
2) وجود عدد من أدوات ووسائل اختراق النظم مثل: tcpdump و netcat و ping sweepers و crack و NTrack و port scan و Nimda SATAN/SAINT/SARA/.
3) وجود أكثر من كتاب ووثيقة مؤلفها أصلاً مخترق للنظم (مثل كيفين ميتنيك).
4) وجود ثغرات أمنية في بروتوكول الشبكة TCP/IP.
5) وجود ثغرات أمنية في خدمات الشبكات.
6) وجود عدد ضخم جداً من البيانات المفيدة التي تشجع على الاستفادة منها بدون تصريح.
7) وجود عيوب أو مشاكل في تشغيل التطبيقات التي تعتمد على الإنترنت.
8) وجود مشاكل في تشكيل نظام العمل الأمثل (Configuration) لمعدات الاتصال خاصة الموجهات (Routers).
9) غياب التدريب والوعي لدى الأفراد.

ومخاطر الاختراق ممكن أن تكون من الداخل أو الخارج وهى تتمثل في:

1) سرقة المعلومات أو التجسس عليها.
2) اعتراض رسائل البريد الإلكتروني وقراءتها بواسطة شخص غير مصرح له.
3) اختراق معدات أنظمة الحاسبات المتصلة بالشبكات والاطلاع على البيانات والمعلومات الموجودة بها بهدف تغييرها أو تدميرها أو منع استغلال الموارد من حاسبات وبرامج.
4) تعطيل برامج التشغيل للحاسبات المتصلة بالشبكات.
5) إرسال معلومات زائفة بهدف الاستفادة أو أشغال الشبكة ومنع الاستفادة منها.
6) زرع الفيروسات والبرامج الدخيلة مثل حصان طروادة والقنابل المنطقية القنابل الموقوتة وديدان الشبكات.
7) الحصول على معلومات تفيد المتطفلين مثل: بيانات بطاقات الائتمان والتأمين الصحي وحسابات البنوك والأرقام السرية والبيانات الأخرى الخاصة بالتجارة أو الأعمال الإلكترونية.

1-4-6 أعداء الإنترنت

يمكن حصر أعداء الإنترنت في الآتي:

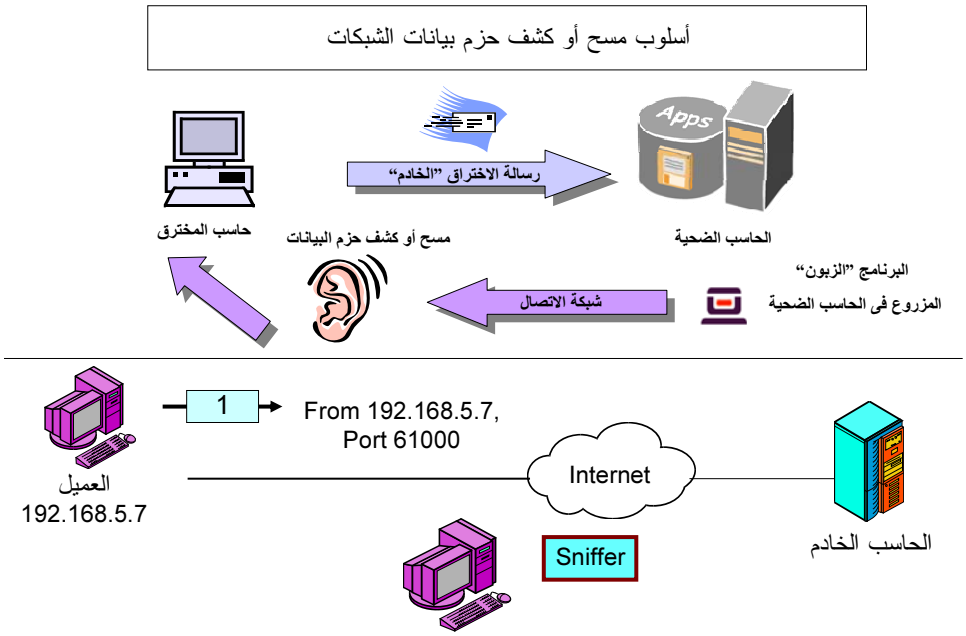
المتطفلون (Hackers): المتطفل هو الشخص الذي يشعر بالفخر لمعرفته بأساليب عمل النظام بحيث يسعى للدخول إليه بدون تصريح. وهؤلاء الأشخاص عادة يستخدمون برامج اختراق جاهزة أغلبها موجود مجاناً على الإنترنت (كبرنامج NetBus أو Net Sphere أو Back Orifice) كانت تستخدم في أغراض مفيدة أخرى مثل ومراقبة حركة البيانات والدعم الفني وتصحيح الأخطاء وإصلاح الأعطال هذا ولا يشترط أن يكون المتطفل خبير في الشبكات أو في تطوير البرامج ولكن المطلوب منه فقط دراسة وثيقة التشغيل لبرامج الاختراق. ولهؤلاء المتطفلون مواصفات عامة هي:

أ) لديهم القدرة والرغبة على التعلم واكتساب المهارات بسرعة والبحث في أدق تفاصيل لغات البرمجة والتعامل مع الجوانب الأكثر صعوبة منها والتطبيق العملي لكل ما يتعلمونه.

ب) الشعور بالسعادة والمتعة في تصميم برامج اختراق أو في استغلال برامج الاختراق الجاهزة أكثر من تصميم برامج مفيدة لهم ولمؤسساتهم تؤدي وظيفة قد تطلب منهم.

ج) لديهم معلومات فنية عن الثغرات الأمنية في بروتوكول الاتصال بالشبكة TCP/IP وعن وسائل تأمين الشبكات وعن برامج تطوير مواقع الإنترنت بغرض البحث عن طريقة لاختراقها.

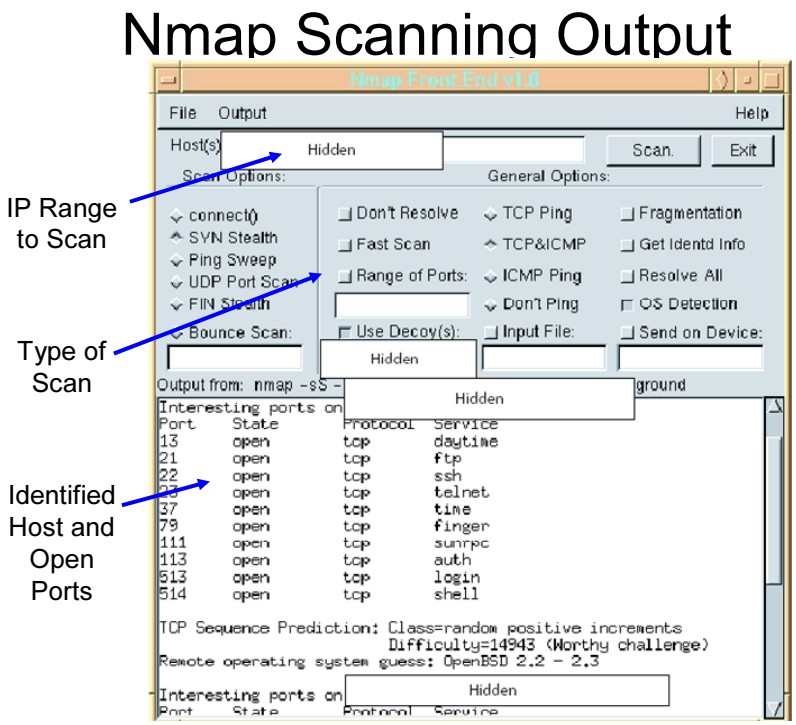
ويستخدم المتطفل حاسبه الشخصي المتصل من خلال الإنترنت بضحاياه (سواء حاسب خادم للتطبيقات أو قواعد البيانات أو موقع ويب). ويتم أولاً كشف أو مسح حزم البيانات يليها زرع برامج الاختراق (مثل برنامج "نت باص" Netbus أو Nmap). والشكل رقم (3) يوضح كيفية استخدام برامج المسح أو الكشف لحزم البيانات. [المراجع أرقام (27 و48 و57 و69)]



يضع الدخيل معدات وبرامج الشم أو الكشافات خارج الشبكة التى تقوم بالتقاط جميع حزم البيانات وبالتالي تحديد عنوان المرسل والمرسل إليه وأرقام نوافذ الاتصال المفتوحة فى الحاسب الضحية تمهيداً لاختراقه.

الشكل رقم (3): استخدام برامج المسح أو الكشف لحزم البيانات

والشكل رقم (4) يوضح القائمة الرئيسية لأحد برامج المسح (Nmap) حيث يمكن بواسطته مسح أو كشف عناوين IP الحاسبات المتصلة بالشبكة.



الشكل رقم (4): القائمة الرئيسية لأحد برامج مسح أو كشف عناوين IP الحاسبات

والمعروف أنه قد تم ويتم يومياً اختراق عدة مواقع أمريكية وعالمية وعربية وما زالت حالات الاختراق الناجحة تتوالى ولسوء الحظ عدد كبير من المواقع العربية قد تكون غير محصّنة بنظم تأمين حديثة ومنيعة مثل الجدران النارية (Firewall) أو منع الاختراق (Intrusion Prevention) مما يجعلها فريسة سهلة للمتطفلون الذين من خلال الاختراق قادرون على تنفيذ الآتي:

أ) حذف الملفات الحقيقية وإضافة ملفات أخرى إلى الحاسبات الخادمة بحيث يتم إدارة الملفات المضافة طبقاً لرغبة من أضافها.

ب) نقل ما يظهر على شاشات حاسبات النظام الضحية المخترق إلى شاشة المتطفل تمهيداً لطباعة هذه الشاشات للاستفادة من البيانات فيما بعد.

ج) التجسس على لوحة المفاتيح وحركة الماوس للحاسبات الضحية وبذلك يمكن كشف الاسم وكلمات المرور.

د) التحكم في إدخال وإخراج وحدات التخزين الخارجية للحاسبات الضحية.

هـ) سرقة بيانات الأنظمة التي تم اختراقها.

2) المخربون (Crackers): المخرب هو الشخص الذي يحاول الدخول على الأنظمة المتصلة من خلال الإنترنت دون تصريح بهدف تخريب بيانات النظام وإيقافه عن العمل وقد تم عام 1998 تخريب عدة مواقع عربية وأمريكية عالمية مثل (AOL−Yahoo- CNN, Amazon- EBay) وقد ترجاهم رئيس أمريكا في ذلك الوقت "الرئيس كلينتون" أن يبتعدوا على تلك المواقع لأنهم تسببوا في إحداث خسائر مالية قدرت بملايين الدولارات وتسببوا في إفلاس شركات عديدة وجدت أن تكاليف التأمين تفوق مكاسبها ففضلت وقف نشاطها. والمخربون على عكس المتطفلون يتسببوا في إحداث الأضرار المالية والمادية – ويستخدم المخربون أيضاً برامج جاهزة أغلبها موجودة مجاناً على الإنترنت – ولا يشترط أن يكون المخرب أيضاً خبير في الشبكات أو في تطوير البرامج إنما يستخدم معلومات تم تسريبها بطريق الإهمال عن النظام والشبكة وأساليب العمل وهذه المعلومات تستخدم كبداية للاختراق من قبل المخربون.

3) زارعي ومطوري البرامج الخبيثة مثل الفيروسات (Computer Virus): الفيروس هو برنامج خبيث يدخل شبكة المعلومات دون علم المستخدم. وهو برنامج له القدرة على تكرار نفسه داخل ذاكرة الحاسبات كما له القدرة على دمج نفسه في البرامج الأخرى. كما تعرف الفيروسات بأنها أكواد برامج مخفاة يتم زرعها في النظام سواء في برامج النظام أو في برامج التطبيقات وتظهر آثارها في التوقيت أو الموقف الذي حدده "للهجوم" المبرمج لها.

وكما أن الفيروسات الطبيعية خطيرة على الإنسان لدرجة أنها قد تقضى عليه فكذلك فيروسات الحاسبات خاصة الحديث منها قد تقضي على شبكة المعلومات بالكامل سواء باستمرار أو لفترة محدودة طبقاً للتعليمات التي دمجها مطور الفيروس داخله. وللفيروسات أشكال وأحجام كثيرة لذلك يكفى أن نذكر أن أهم أنواع البرامج الدخيلة الخبيثة هي الديدان (Worms) وحصان طروادة (Trojan Horse Programs) والقنابل المنطقية (Logic Bombs) والقنابل الموقوتة (Time Bombs).

ويمكن تصنيف الفيروسات عدة تصنيفات مختلفة من حيث آلية عمل الفيروس أو من حيث أثره على المستخدم أو من حيث الفئة المستهدفة من الفيروس أو نوع الأنظمة التي يتمكن من إصابتها.

وطبقاً لطبيعة عمل الفيروس والغرض منه تنقسم الفيروسات والبرامج الخبيثة إلى الأصناف التالية:

أ) حصان طروادة (Trojans horse): هو جزء صغير من الكود يضاف إلى برامج التطبيقات ولا يخدم الوظائف العادية التي صممت من أجلها هذه البرامج ولكنه يؤدي عملاً تخريبياً للنظام، وتكمن خطورته في أن النظام لا يشعر بوجوده حتى تحين اللحظة المحددة له ليؤدي دوره التخريبي ومن أنواعه:

- القنبلة المنطقية (Logic Bomb): وهي أحد أنواع حصان طروادة وتصمم بحيث تعمل عند حدوث ظروف معينة أو لدى تنفيذ أمر معين فقد تصمم بحيث تعمل عند بلوغ عدد المتصلين على نظام المعلومات عدداً معيناً مثلاً أو إذا كان هناك محاولة لإزالة البرنامج أو إذا تم رفع اسم المخرب (زارع القنبلة) من كشوف المرتبات. وتؤدي القنبلة في هذه الحالة إلى تخريب بعض النظم أو إلى مسح بعض البيانات أو تعطيل النظام عن العمل.
- القنابل الموقوتة (Time bomb): وهي نوع خاص من القنابل المنطقية وهي تعمل في ساعة محددة أو في يوم معين.
- باب المصيدة (Trap door): وهذا الكود يوضع عمداً بحيث يتم لدى حدوث ظرف معين تجاوز المخرب لنظم الحماية والأمن في النظام ويتم زرع هذا الكود عند تركيب النظام بحيث يعطي المخرب حرية تحديد الوقت الذي يشاء لتخريب النظام فهو يظل كامناً غير مؤذ حتى يقرر المخرب استخدامه وكمثال على ذلك زرع كود خبيث في نظام الحماية والأمن يتعرف على شخصية المخرب ويفتح له الأبواب دون إجراء الفحوص المعتادة .

ب) ديدان الشبكات (Worms): الدودة هي عبارة عن كود يسبب أذى للنظام عند استدعائه. وتتميز الدودة بقدرتها على إعادة توليد نفسها بمعنى أن أي ملف أو حاسب متصل بالشبكة تصل إليه الدودة وتلوثه وتنتقل الدودة إلى ملف آخر أو حاسب آخر في الشبكة وهكذا تنتشر وتتوالد.

ج) الفيروسات المموهة: وهي الفيروسات التي تقوم بتغير شكل شيفرتها مع كل إصابة جديدة تماماً وقد تحوي على بلايين وبلايين التحولات. ولا توجد بصمة واحدة وثابتة من عينة إلى عينة أخرى لهذا النوع من الفيروسات يمكن من خلالها اكتشافها.

د) الفيروسات المصاحبة: وتقوم باستبدال البرنامج المستهدف بعد أخذ نسخة احتياطية منه.

هـ) الفيروسات الخفية "الشبحية": تقوقع نفسها بعد تنفيذها وتقوم بإخفاء زيادة حجم الملف المصاب أو التغير في الوقت والتاريخ للأجهزة المصابة ... الخ

و) فيروسات القطاعات: تقوم بتغير عناوين الملفات في جدول توزيع الملفات ليصبح العنوان المحول عنوان الفيروس.

ز) فيروسات المناعة: تهاجم برامج الحماية ضد الفيروسات.

ويعتبر البريد الإلكتروني من أكثر التطبيقات شيوعاً لنشر البرامج الخبيثة وعادة ما تصل هذه البرامج ملحقة على رسائل شيقة مع عنوان يغري متلقي الرسائل على فتح الملفات الملحقة وقراءتها وبالتالي تشغيل البرامج الخبيثة.

كما قد تصل هذه البرامج من خلال مواقع بالإنترنت. فإذا تم الدخول على صفحة معينة ترسل هذه الصفحة البرامج الخبيثة إلى الحاسبات دون أن يشعر المستخدم وذلك عن طريق بروتوكول الخادم والعميل أو تنفيذ بعض برامج تطوير المواقع الحديثة مثل ActiveX أو جافا Java.

وتتلخص خطورة الفيروسات والبرامج الخبيثة في النقاط التالية:

أ) يمكن لهذه البرامج إلغاء الملفات بنفس السهولة التي يلغى بها مستخدم النظام الملفات.

ب) نقل الملفات التي يريد قراصنة الشبكات الحصول عليها من نظام المعلومات المصاب.

ج) تغيير محتويات الملفات.

د) تغيير وقت وزمن الحاسب الضحية.

هـ)تثبيت برامج دخيلة أخرى على النظام المصاب مع إعطائها صلاحيات مدير النظام الأصلي Admin أو Super User وبذلك يمكنها اختراق حاسبات أخرى موجودة على نفس الشبكة أو الحصول على ملفات من نظم معلومات أخرى.

و)إصابة نظام المعلومات بالشلل الجزئي ومنع الاستغلال الأمثل لمصادر النظم من قدرة وذاكرة حاسبات وطابعات وتطبيقات شبكات أو إصابة النظام بالشلل الكلي وإيقافه تماماً عن العمل.

وتزداد مخاطر زرع الفيروسات للنظم المعتمدة على الإنترنت عن طريق:

أ) تحميل البرامج من الشبكات وتشغيلها دون فحصها والتأكد منها.

ب) تشغيل البرامج من الأقراص الصلبة والضوئية دون فحصها والتأكد من سلامتها.

ج) عدم وضع خطة للنسخ الاحتياطية للبرامج والتطبيقات والبيانات.

د) عدم اقتناء برامج فعالة مضادة للفيروسات تقوم باكتشاف البرامج الدخيلة وتدميرها.

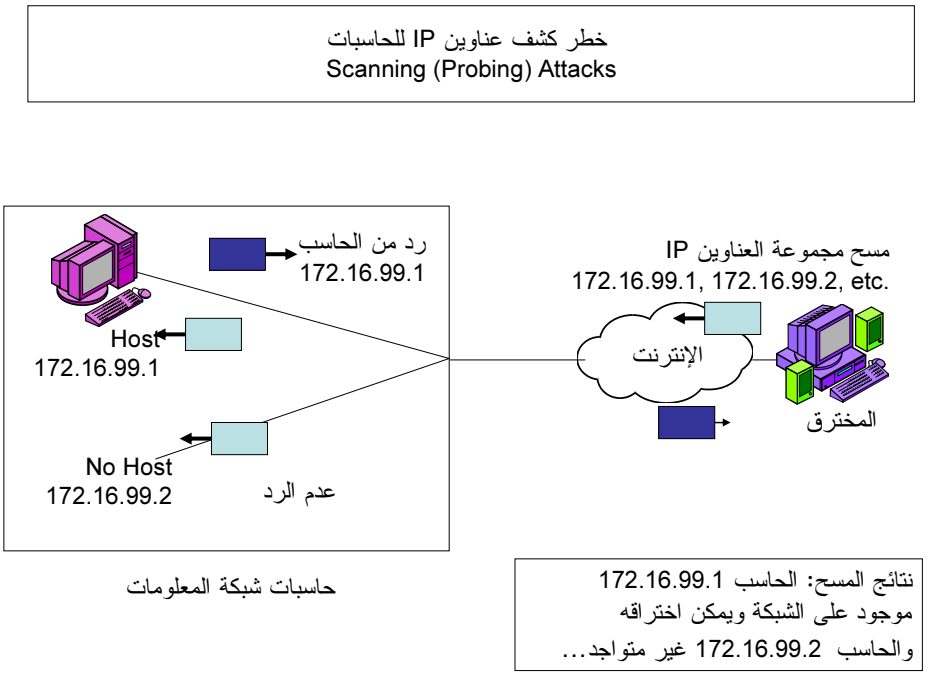
هـ)عدم التعديل المستمر للبرامج المضادة للفيروسات.

و)عدم وجود إجراءات "سياسة أمنية" للتعامل مع البرامج وتطبيقات الإنترنت مثل الويب والبريد الإلكتروني ونقل الملفات والتجارة الإلكترونية.

ز)عدم التدريب وفقدان الوعي لدى الأفراد عن مخاطر البرامج الخبيثة على بيانات ومصادر معلومات المؤسسة.

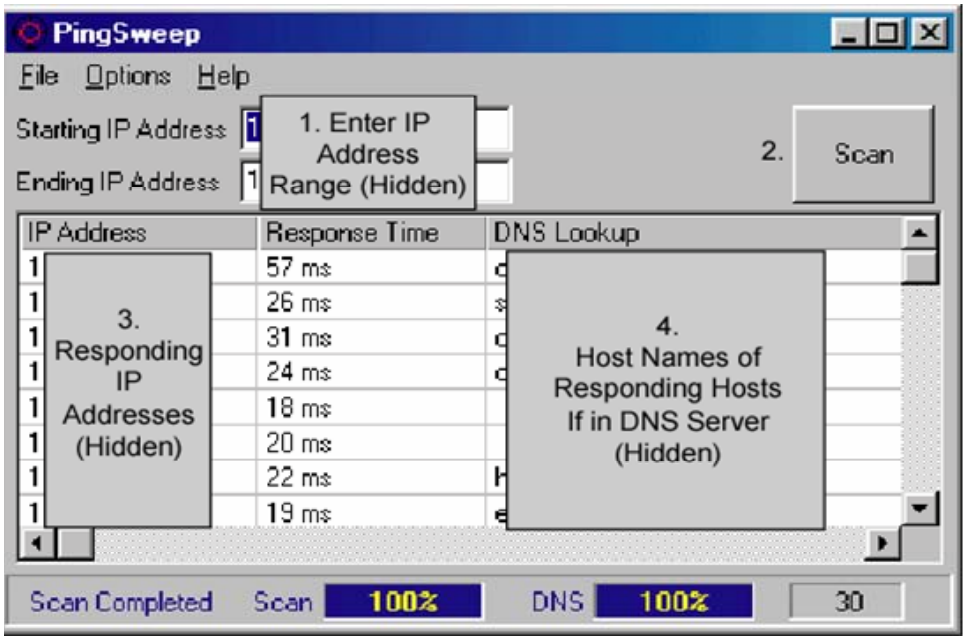
4) مخترقي عناوين الحاسبات المتصلة بالشبكة:

الخطوة الأولى في الاختراق تتمثل في تحديد عناوين IP للحاسبات الخادمة الموجودة حالياً في الشبكة. ويتم ذلك باستخدام حزم بيانات Ping لبروتوكول التحكم في الشبكة ICMP وبرنامج ماسح IP Scan طبقاً للشكل رقم (5). كما يوضح الشكل رقم (6) القائمة الرئيسية لبرنامج كشف عناوين الحاسبات Ping Sweep الموجود مجاناً على الإنترنت. [المراجع أرقام (32 و30 و33 و57 و69)]



الشكل رقم (5): كشف عناوين IP حاسبات شبكة المعلومات

القائمة الرئيسية لبرنامج مسح عناوين IP لحاسبات نظم المعلومات
Ping Scanning With Ping Sweep



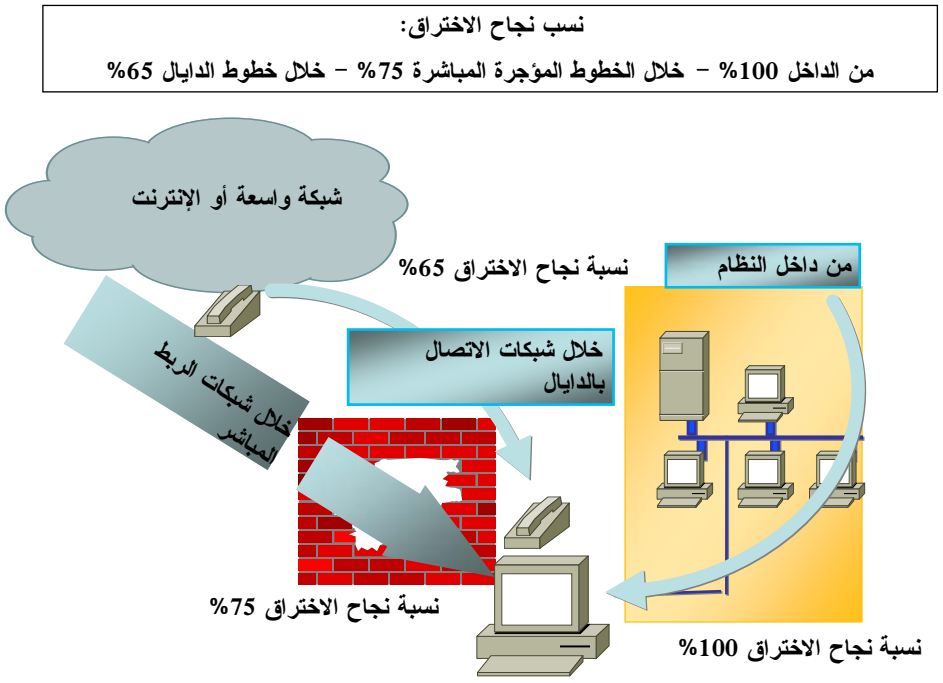
الشكل رقم (6): القائمة الرئيسية لبرنامج كشف عناوين الحاسبات

5) الأفراد الداخليين غير المصرح لهم

يصعب تحديد أخطار الدخول غير المصرح به من داخل المؤسسة فهو يميز مجموعة ضخمة من الأخطار تبدأ من الأخطار غير المدمرة وتنتهي بالأخطار المدمرة.

هناك خطر الإهمال في العمل وسوء استخدام النظام وخطر كشف أو تدمير أو فقد المعلومات وخطر "الهندسة الاجتماعية" (Social Engineering) الذي يتمثل في كشف المعلومات الحساسة للغير بغرض التباهي أو بالخداع أو بالتحايل شاملاً ذلك المعلومات وتصنيفها الأمني والاسم وكلمات المرور وأحقيات الدخول. كما أن الزائرين لمواقع الأجهزة قد يمثلوا خطورة إذا لم يكن بصحبتهم أحد. ولقد أثبتت الإحصائيات والتجارب أن الأفراد الساخطين أو غير الأمناء أو الغير مؤهلين أو المهملين يمثلون نسبة كبيرة من تهديدات النظم.

كما يوضح الشكل رقم (7) وطبقاً للإحصائيات العالمية فإنه إذا توافرت للمخترق وسائل الاختراق فإن نسبة نجاح الاختراق هي كالتالي: من داخل النظام 100%. ومن خلال خطوط الربط المباشرة المؤجرة 75%. ومن خلال المودم والدايال 65%. [المراجع أرقام (27 و48 و57 و69)]



الشكل رقم (7): نسبه نجاح الاختراق

2-4-6 الآثار السلبية من مخاطر الإنترنت

1) الاختراقات الأمنية:

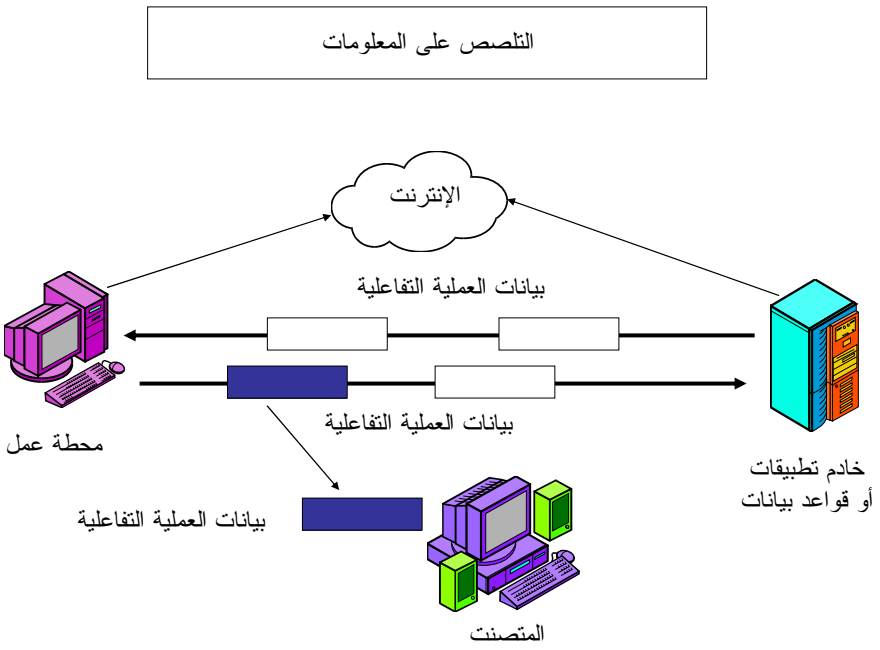
الاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن فتح طريق ثغرات في نظام الحماية الخاص بشبكة المعلومات. وحينما نتكلم عن الاختراق بشكل عام فنقصد بذلك قدرة المخترق على الدخول إلى حاسب شخص ما بغض النظر عن الأضرار التي قد يحدثها، فحينما يستطيع الدخول إلى حاسب آخر فهو مخترق (Hacker) أما عندما يقوم بحذف ملف أو تشغيل آخر أو جلب ثالث فهو مخرب (Cracker).

واختراق الأجهزة هو كأي اختراق آخر لشيءٍ ما له طرق وأسس يستطيع من خلالها المخترق التطفل على أجهزة الآخرين عن طريق معرفة الثغرات الموجودة في أجهزتهم. وغالباً ما تكون تلك الثغرات في المنافذ (Ports) الخاصة بالحاسب. والتي يمثل كل منها تطبيق من تطبيقات بروتوكول الإنترنت TCP/IP. وهذه المنافذ يمكن وصفها بأبسط شكل على أنها بوابات للحاسب على الإنترنت. فعلى سبيل المثال: المنفذ رقم "80" غالباً ما يكون مخصصاً لموفر الخدمة كي يتم دخول المستخدم على مواقع الويب بالإنترنت (http port). وفي بعض الأوقات يكون المنفذ رقمه 8080. والمنفذ رقم (25) مخصص للبريد الإلكتروني والمنافذ أرقام (21 و23) مخصصة لنقل الملفات ... وهكذا.

وهناك طرق عديدة للاختراق أبسطها والتي يمكن استخدامها هي البرامج التي تعتمد على أسلوب الزبون والخادم (client/server) حيث يكون هناك ملفين: أحدهما للخادم (Server) يتم إرساله إلى الحاسب الضحية بطريقة ما. والآخر للزبون (Client) يتم تشغيله من قبل المخترق بهدف التحكم في الحاسب الضحية. وعند تشغيل ملف Server من قبل المُختَرَق يصبح الحاسب الضحية عرضة للاختراق حيث يتم فتح أحد المنافذ (Ports) وغالباً ما تكون البوابات أرقام (12345 أو 12346). وبذلك يمكن الاختراق ببرنامج مخصص لذلك (كبرنامج NetBus أو Net Sphere أو Back Orifice). كما يستطيع مخترقون آخرون (إضافة إلى المخترق الأول الذي وضع الملف في الأجهزة) فعل نفس الشيء حينما يقومون بعمل مسح للبوابات (Port Scanning) فيجدونها مفتوحة. وطريقة الاختراق هذه هي أبسط أشكال الاختراق. وهناك طرق عديدة تمكن المخترق من اختراق الأنظمة مباشرة بدون إرسال ملفات لدرجة أن جمعية للقراصنة في أميركا ابتكرت طريقة للاختراق متطورة للغاية حيث يتم الاختراق عن طريق حزم البيانات التي تتدفق مع حركة الاتصالات الهاتفية عبر الإنترنت (VOIP or Voice Over Internet Packets) حيث يتم اعتراض هذه النوعية من حزم البيانات والتحكم من خلالها في حاسبات أطراف الاتصال التليفوني.

2) التلصص على المعلومات (Eavesdropping):

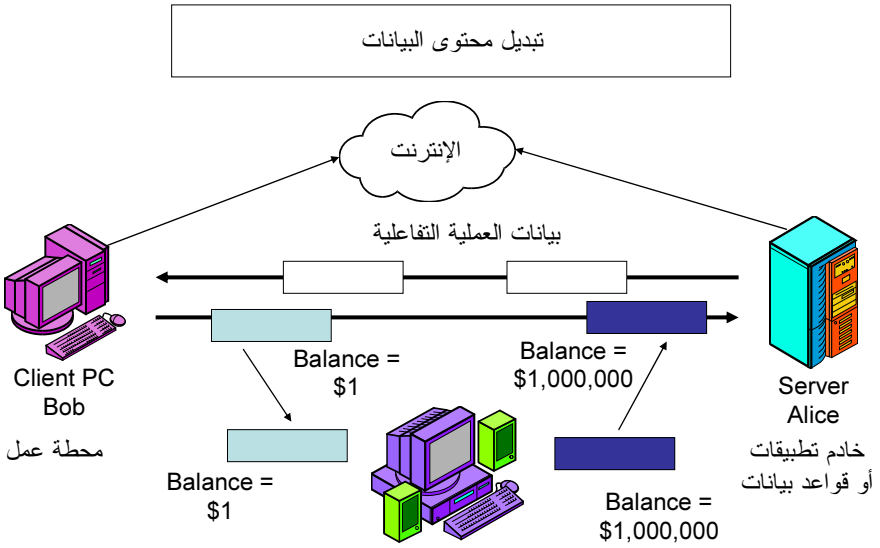
التلصص أو التصنت هو مصطلح يصف فعل قراءة معلومات غير محمية في أثناء انتقالها عبر أية شبكة. إن التلصص على مجموعات المعلومات تعد عملية سهلة نسبياً مع استخدام برامج شم أو اكتشاف (Sniffing) كانت مصممة بشكل أساسي للمساعدة في اكتشاف أخطاء الشبكة. ويتلصص محترفوا الشبكة على الرسائل الصادرة والواردة من عناوين مزودي خدمات الإنترنت وإذا وجدوا شيئاً ما يقومون ببيع ما وجدوه إلى المجرمين والمنافسين. ويوضح الشكل رقم (8) كيفية التلصص على المعلومات عبر الإنترنت.



الشكل رقم (8): التلصص على المعلومات عبر الإنترنت

3) تبديل محتوى البيانات (Data Modification):

على سبيل المثال فى العمليات المالية فإحدى طرق تحويل الأموال المدفوعة إيقاف رقم الحساب المصرفي وتغييره إلى رقم آخر وهذا ما يطلق عليه "تبديل المحتوى" ويستخدم المتلصصون نفس الاسلوب فى استبدال المحتوى الاصلي والخداع Impersonation/Spoofing عن طريق إرسال مجموعة بديلة من البيانات إلى المستلم الأصلي (شخص أو بنك). ومن البيانات التي يمكن تبديلها عنوان تسليم الشحنة أو رقم الحساب فى البنك أو المبالغ المحولة. ويوضح الشكل رقم (9) كيفية تبديل محتوى البيانات المالية عبر الإنترنت.



الشكل رقم (9): تبديل محتوى البيانات عبر الإنترنت.

4) إنكار تنفيذ الأعمال (Repudiation):

يقصد بهذا الأسلوب غير القانوني القيام بعمل تجاري مع أية مؤسسة إلكترونياً عبر الإنترنت ثم إنكار حدوث هذه الصفقة أو حتى إنكار البدء فيها. وقد يقوم الدخيل بطلب منتج على خط ائتماني ثم يشحنه إلى موقع آخر وعندما يتسلم الفاتورة ينكر المستخدم أنه على علم بهذه الشحنة والموجودة بالفعل في مخزن تابع له مؤجر أو مهجور.

5) انتحال الشخصية بالخداع والمحاكاة (Spoofing):

المحاكاة هو مصطلح يطلق على عملية انتحال شخصية للدخول الى النظام حيث تحتوي حزم البيانات فى بروتوكول الشبكة IP على حقول بيانات مفيدة مثل عناوين المرسل والمستقبل. وهذه العناوين ينظر إليها على أنها عناوين مقبولة وسارية المفعول من قبل البرامج وأجهزة الشبكة ومن خلال طريقة التعرف على مسارات المصدر (Source Routing) فإن حزم البيانات IP قد يتم إعطائها شكلاً تبدو معه وكأنها قادمة من حاسب خادم صديق قد يكون تم اختراقه أيضاً. بينما هي في الحقيقة ليست قادمة منه وعلى ذلك فإن النظام إذا وثق ببساطة بالهوية التي يحملها عنوان مصدر الحزمة فإنه يكون بذلك قد حوكي أو خُدِع. البريد الإلكتروني يمكن أيضاً أن يخدع بسهولة ولكن النظام المؤمن بشكل جيد لا يثق بهذه المصادر ولا يسمح عموماً بالحركة المسيّرة من قبل المصدر (Source routed).

6) سرقة الاسم وكلمات المرور:

يقصد بسرقة الاسم وكلمات السر هو إجراء جميع المحاولات "Brute-Force attacks" لتحديد الاسم وكلمات السر الخاصة بمستخدمي نظام المعلومات المصرح لهم.

وتوجد وسائل أخرى مثل زرع أكواد برنامج حصان طروادة التي تتجسس على الاسم وكلمات المرور أو استخدام برامج خداع حزم البيانات IP spoofing أو استخدام برامج المسح والكشف packet sniffers.

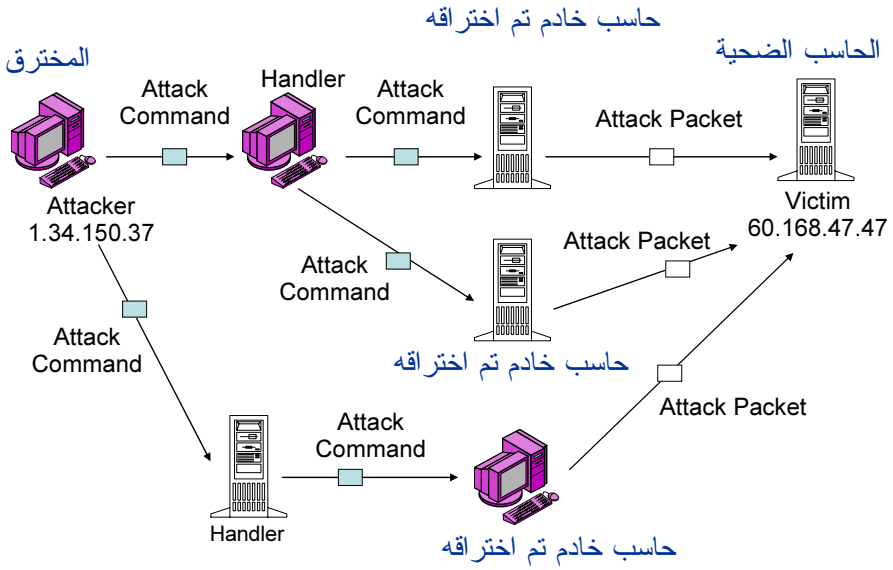
7) محاكاة المواقع (Web Sites Fraud):

هو تقليد موقع ويب حقيقي على الإنترنت (مثل موقع تجاري) بما في ذلك تخطيط الموقع والألوان والوظائف من أجل الحصول على بيانات من عملاء الموقع مثل بطاقات الاعتماد أو قد يكون لسرقة اختراع لمنتج تجاري. ويتم التقليد بتسجيل اسم نطاق URL وثيق الشبه بموقع مشهور وسليم قانوناً وربما يختلف اسم النطاق في حرف واحد للتمويه مثل تطوير موقع باسم www.amazin.com ليحاكي موقع مكتبة الأمازون الشهيرة www.amazon.com. ويقوم موقع الويب (Web Site) الغير قانوني بنسخ نص رسومات الموقع القانوني وينشئ بعض الوظائف بغرض تقليد الإحساس بالروابط المحتواة في الموقع. والخطوة التالية هي تقديم منتج أو خدمة عامة بسعر مدهش لحث الناس وتشجيعهم على إرسال بيانات الشخصية أو بيانات بطاقاتهم الائتمانية. وبالطبع ليست كل المواقع المقلدة تستخدم أسلوب اختلاف حروف الهجاء سيئة فبعضهم يحاول جذب الشركات إلى موقعهم القانوني والبعض الآخر يحاول جمع الأموال باستخدام العبارات الشهيرة.

8) منع الخدمة (Denial Of Services DOS):

الهدف من هذا الاختراق هو منع المستخدم الفعلي من استخدام مصادر النظام كمثال من الممكن إرسال عدد كبير جداً من الرسائل مجهولة المصدر أو المصب عبر الشبكة لتستهلك الحيز الترددي لها (Network Bandwidth) طبقاً للشكل رقم (10) وبالتالي لا يستطيع المستفيدون من النظام الدخول عليه والاستفادة منه. وفى بعض الأحيان يقوم مستخدمو هذه التقنية بتشغيل معالج الحاسب بطريقة مكثفة بحيث لا يكون لديه الوقت أو المصادر (الذاكرة) لتنفيذ برامج أو تطبيقات أخرى. وبعض قراصنة الإنترنت المهرة قد يستخدمون حاسب نظام في الهجوم على نظام آخر. وهذا النوع من الانتهاك أو الهجوم كان الهدف من تطوير فيروس "ميليشيا" "Melissa". وقد تم حديثاً تطوير برامج أكثر كفاءة من هذا الفيروس وأحدثت الكثير من الخسائر في نظم شبكات المعلومات فبمجرد تعرض النظام لهذا الهجوم تتوقف الحاسبات عن العمل. ومن يستخدم هذه التقنية في الدخول على نظم معلومات الآخرين يهدف إلى ترك هذه الحاسبات محطمة وغير قادرة على العمل أو توفير الخدمات للمستفيدين منها.

خطر منع الخدمة الموزع
Distributed Denial Of Services DDOS



الشكل رقم (10): خطر منع الخدمة

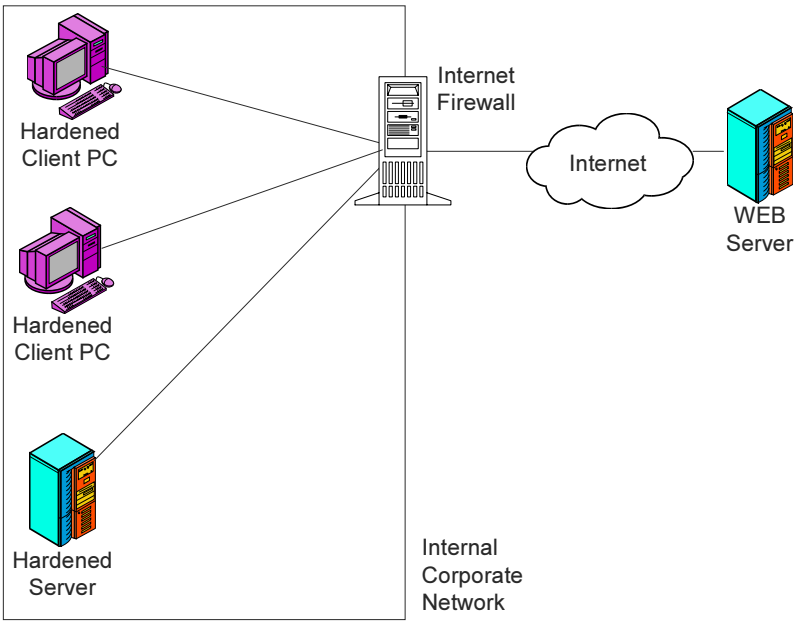
5-6 التأمين عند استخدام الإنترنت

هناك عدد من الوسائل التقنية لمكافحة المخاطر والاختراقات التي قد تتعرض لها الإنترنت ويشترط في هذه الوسائل عدة شروط من أهمها:

1) توفير التأمين والحماية دون الحد من استخدام الشبكة كوسيلة ربط وكمصدر أساسي للمعلومات.
2) توفير التأمين والحماية دون الحد من كفاءة أداء مصادر المعلومات (الحاسبات الخادمة – التطبيقات – قواعد البيانات – الشبكات – محطات العمل).
3) ألا تكون التكلفة باهظة وتتعدى تكلفة الخسائر التي تسببها الأخطار التي قد تتعرض لها نظم المعلومات.
4) توافر متدربين مؤهلين ضمن "كيان تأمين نظام المعلومات" من ذوي الخبرة في التعامل مع وسائل التأمين والحماية.
5) وجود إجراءات "سياسة أمنية" لاستخدام وسائل التأمين حتى لا يتعرض نظام المعلومات لخطر نتيجة جهل أو إهمال أو سوء الاستخدام.

الشكل رقم (11) يوضح العناصر الأساسية لربط نظم المعلومات بالإنترنت وهي:

1) الحاسبات الشخصية والحاسبات الخادمة ضمن الشبكة المحلية لنظم المعلومات.
2) وسائل التأمين والحماية.
3) شبكة الإنترنت والحاسبات الخادمة بالإنترنت.



الشكل رقم (11): العناصر الأساسية لربط نظام المعلومات مع الإنترنت

طبقاً للشكل رقم (11) فإنه يمكن تقسيم محاور التأمين عند استخدام الإنترنت إلى قسمين متكاملين هما:

1) التأمين والحماية بالوسائل التكنولوجية ويتم ذلك على أربعة مستويات هي:
   - أ) تأمين وحماية الحاسبات الشخصية والحاسبات الخادمة
   - ب) تأمين وحماية شبكة الربط بالإنترنت
   - ج) تأمين المعلومات المتداولة
   - د) الحماية من التهديدات والاختراقات
2) التأمين بوضع "السياسة الأمنية" ويتم ذلك على 10 محاور تم تناولهم بالتفصيل في الفصل الرابع وهم:
   - أ) أمن الأفراد
   - ب) التأمين الطبيعي
   - ج) تحديد الهيكل التنظيمي المساند شاملاً "كيان الأمن"
   - د) تصنيف المصادر العملياتية والبيانات والمعلومات
   - هـ) تحديد مستويات الدخول وأحقيات التعامل
   - و) تأمين عمليات التشغيل
   - ز) تأمين التطبيقات والشبكات والخدمات (البريد الإلكتروني – نقل الملفات – التجارة الإلكترونية ... الخ)
   - ح) تأمين مراحل تطوير النظم (تجميع البيانات والتحليل والتصميم والبرمجة والتشغيل والصيانة والدعم الفني)

ط) إدارة وتحليل المخاطر وتحديد خطط استمرارية العمل

ي) الالتزام بتشريع تأمين وحماية البيانات على المستوى القومي.

1-5-6 التأمين والحماية بالنظم التكنولوجية

1-1-5-6 تأمين وحماية الحاسبات الشخصية والحاسبات الخادمة

تتفاوت أجهزة الاتصال بالإنترنت في أنواعها وأحجامها وتطبيقاتها طبقاً للشكل رقم (12)

الشكل رقم (12): الأجهزة الشخصية المستخدمة حديثاً للدخول على الإنترنت

يتضح من الشكل رقم (12) أن الوسيلة الرئيسية للدخول على الإنترنت هي الأجهزة الشخصية التي تشمل الحاسب الشخصي الثابت والمحمول (Personnel Digital Assistance PDA, Rigged zed PC, Palm PC, Pocket PC, Tablet PC). تليها الحاسبات الخادمة وتشمل حاسبات التطبيقات وقواعد البيانات والبريد الإلكتروني ونقل الملفات ... الخ. وهذه الأجهزة يمكن حمايتها بالأساليب التالية:

1) الحماية المادية:

هي حماية الحاسبات بما يسمى الحماية الطبيعية (Physical Security) كأن يتم وضع الأجهزة في غرف مؤمنة بعيداً عن أيدي المتطفلين والعابثين والمتصنتين والسارقين وذلك إما بحراسة فعلية أو بإقفال إلكترونية أو بغيرها. ويكون التحكم في دخول الفرد المصرح له الغرفة بحسب مستوى الثقة فيه وطبيعة مهمته وأهمية الحاسب والمعلومات المخزنة به. ويتم تسجيل حالات دخول وخروج الفرد. ويفضل أيضاً استغلال وسائل الحماية الطبيعية المتوافرة بالأجهزة بواسطة المنتج مثل الأقفال الميكانيكية لغلق وحدة التشغيل ولغلق لوحة المفاتيح.

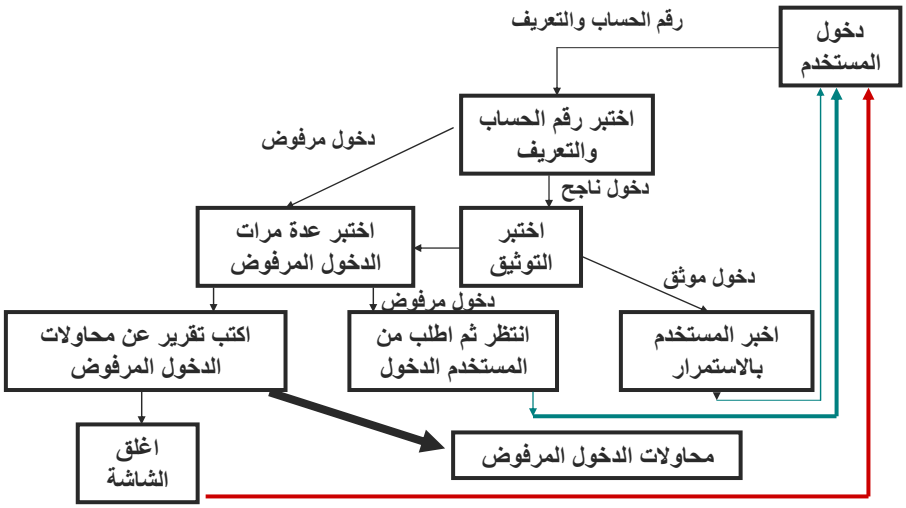
2) *الحماية بتعريف هوية المستخدم والاستخدام ومشروعية استخدامه:*

توجد أدوات تعريف معقدة جداً متوفرة للدخول على الإنترنت وللشبكات التي تتطلب درجات غير عادية من التأمين. فعلى سبيل المثال تتطلب إحدى آليات التأمين استخدام بطاقة ذكية (Smart Card) وهي أداة تشبه بطاقة الاعتماد مع شريط مغناطيسي عليها يجب تمريرها عبر قارئ بطاقات (Card Reader) متصل بالحاسب حتى يستطيع المستخدم الوصول للشبكة. وتوجد أيضاً أجهزة مسح بيولوجي يمكنها التعرف على الشخصية عن طريق مسح سمات فيزيائية فريدة مثل بصمة الإبهام أو بصمة الصوت أو صورة شبكة العين أو قرنية العين.(الشكل رقم (13))

Identification, Authentication and Authorization

الشكل رقم (13): الوسائل البيولوجية المختلفة للتعرف على الهوية

يتم التأكد من الاسم وكلمات المرور بعدة عمليات توثيق تتم داخل الحاسب طبقاً للشكل رقم (14).



الشكل رقم (14): التأكد من الاسم وكلمات المرور

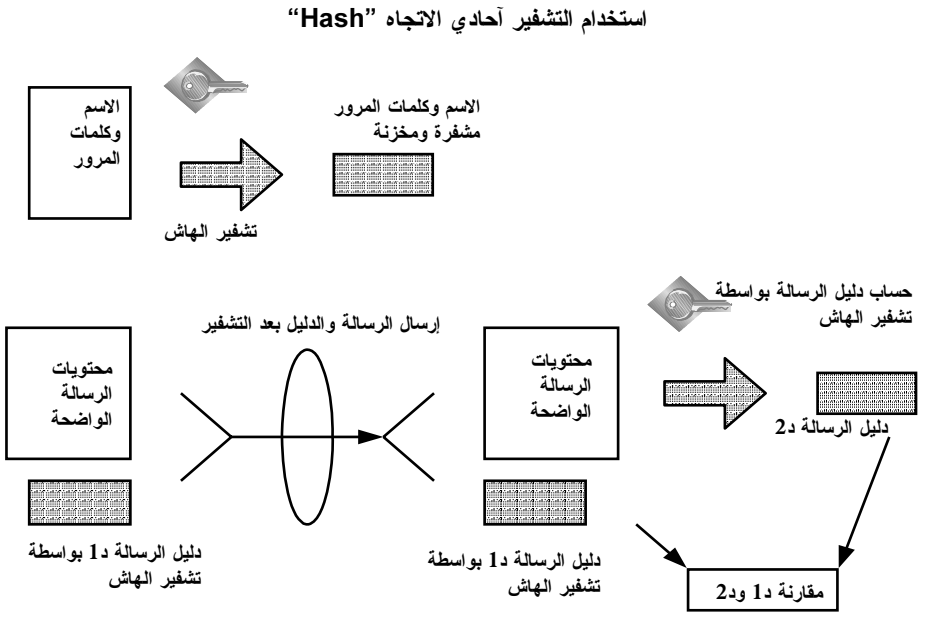
ومن الممكن أن يكون استخدام كلمات المرور طريقة ممتازة لحماية موارد الشبكة ويمكن في نواحي أخرى أن يكون استخدامها أسوأ من عدمه. فحين يعطي مسؤول النظام الحرية للمستخدمين بإنشاء كلمات المرور الخاصة بهم يختاروا كلمات مرور قصيرة يسهل تذكرها ونادراً ما يغير المستخدمون هذه الكلمات وقد يضعوا كلمات مرور بأسمائهم أو كلمات مرور تتألف من أحرف أو أرقام يسهل تخمينها مثل الأحرف الأولى من أسمائهم أو تاريخ ميلادهم أو ما شابه ذلك مما يسهل استنتاجها بواسطة الدخلاء. في حين أن البعض الآخر لا يستخدم كلمات مرور إطلاقاً. وقد يلجأ مسؤول النظام إلى إنشاء الاسم وكلمات المرور بنفسه. وقد ينشئها معقدة وطويلة نوعاً ما. وقد يجد المستخدمون صعوبة في تذكرها وبدون شك سيدونونها أو يتركونها في أماكن واضحة كوضعها على الشاشات أو كتابتها على لوحة المفاتيح أو في مكان ظاهر على المكتب.

والحل الأمثل لمشاكل كلمات المرور هو أن يقوم نظام المعلومات نفسه بإجبار المستخدمون على اختيار كلمات مرور ذات طول معين وصعوبة معينة وتغييرها بشكل دوري وهذا ما يحقق الغالبية العظمى من برامج التشغيل الحديثة. وهذه الطريقة يحددها المدير المسؤول بناء على نوع نظام التشغيل الذي يدير الشبكة عليه.

تحديد طول كلمات المرور: كلما كانت كلمة المرور طويلة كلما كان تخمينها أصعب حسب الاحتمالات الرياضية. تدعم خدمة الدليل (Active directory) المستخدمة ضمن برامج التشغيل للحاسبات Windows كلمات مرور يصل طولها حتى 14 حرفاً وبحد أدنى يعتبر 6 أحرف كافياً لمعظم الشبكات. ويمكن تعيين سياسة لكلمات المرور وأحقيات الدخول باستخدام ميزة "نهج المجموعة"(Group Policy) حيث يمكن تطبيق هذه السياسة على وحدات تنظيمية معينة (مثل الوحدات الإدارية أو المالية) بحسب الحاجة كما يمكن تحديد الحد الأدنى لطول كلمة المرور وإلزام المستخدمين باتباع ذلك.

يعتبر نظام التشغيل Windows 2003 أكثر أنظمة مايكروسوفت تأميناً ويتيح تعيين كلمات مرور وفق سياسة محددة كأن تكون كلمات المرور أكثر تعقيداً عن طريق دمج أحرف كبيرة وأخرى صغيرة واستخدام الأرقام وحروف الترقيم وهذا ممكن أن يزيد من صعوبة توقع أو استنتاج كلمات المرور.

معظم أنظمة التشغيل تخزن كلمات مرور المستخدمين بشكل مشفر باستغلال خوارزم شفري أحادي الاتجاه Hash Function (تم تناوله بالتفصيل في الفصل الخامس) وذلك حتى لا يتمكن أي متطفل محتمل من معرفتها باستخدام أحد برامج قراءة محتويات الأقراص الصلبة وتظهر كلمات المرور عند كتابتها على شكل نجوم أو نقاط مبهمة لا تدل على حقيقتها. والشكل رقم (15) يوضح كيفية تشفير الاسم وكلمات المرور.



الشكل رقم (15): استخدام الهاش في تشفير الاسم وكلمة المرور وفى دليل الرسالة

3) الحماية بالتحصين:

يتم التحصين (Hardening) المستمر للحاسبات من خلال تعديل برامج التشغيل Windows، Linux، Unix، بواسطة الشركة المنتجة التي تصدر دائماً مستحدثات Service Packs بهدف غلق الثغرات الأمنية Vulnerabilities التي يتم اكتشافها في برامج التشغيل.

4) الحماية بغلق المنافذ Ports/Applications/Sockets:

حدد بروتوكول الشبكات TCP/IP رقم منفذ لكل تطبيق وقد يصل عدد المنافذ إلى حوالي 1000 ويستغل المخربون والمخترقون النوافذ المفتوحة لاختراق النظام. فإنه لدواعي التأمين والحماية يتم بواسطة الجدران النارية غلق جميع النوافذ ما عدا ما هو ضروري لتقديم الخدمات أو التطبيقات الفعالة.

بمعنى أنه إذا تم الدخول على مواقع الويب :http يكون المنفذ رقم (80) الخاص بهذا التطبيق مفتوحاً وباقي المنافذ مغلقة. نفس الشيء إذا تم الدخول على خادم البريد يكون المنفذ رقم (25) فقط هو المفتوح وباقي المنافذ مغلقة. هذا الأسلوب يحمى من الاختراقات الأمنية من خلال المنافذ غير المستخدمة.

5) غلق الأجهزة والشاشات غير المستخدمة:

إن ترك المستخدم لحاسبة مفتوحاً عند الخروج من المكتب يشكل خطورة على هذا الحاسب بالإضافة إلى الأجهزة الأخرى المتصلة معه على نفس الشبكة. لذا يتم من خلال إجراءات "السياسة الأمنية" التنبيه على المستخدمين بغلق أجهزتهم عند خروجهم من المكاتب أو استخدام كلمة سر الشاشة التي تتيح غلق الحاسب عند مغادرة المكتب دون الحاجة إلى إعادة تشغيل الحاسب عند العودة مرة أخرى.

6-5-1-2 تأمين وحماية شبكة الربط بالإنترنت

تشكل الشبكات المحلية عنصراً مهماً في تكوين منظومة شبكات المعلومات وتختلف طرق الحماية بحسب نوع وحجم الشبكة وطرق اتصالها بالشبكات الأخرى (اتصال طبيعي مباشر بخطوط مؤجرة (leased lines) – اتصال منطقي بخطوط نقل حزم البيانات (data lines frame relay) أو MPLS من مزودي خدمة نقل البيانات Packet Switched Data Network Operators – اتصال من خلال الإنترنت – بالإضافة إلى كافة أنواع الاتصالات اللاسلكية).

وتتعاظم أهمية التأمين والحماية عندما يتم الربط مع الإنترنت التي من طبيعتها وبالهدف من إنشاؤها خالية من أي وسائل تأمين أو حماية ذاتية. اتصالات الإنترنت هي الباب الذي يمكن أن تنفذ منه المخاطر والتهديدات الأمنية لذا يتم حماية الشبكة المحلية بالطرق التالية:

6-5-1-2-1 الشبكات المحلية الافتراضية VLAN

الهدف منها تحويل الشبكة المحلية الطبيعية إلى شبكات مؤمنة منطقية قد يصل عددها حسب نوع معدة التحويل (Switch) إلى أكثر من (8000) شبكة كل منها تتكون من مجموعة من الأجهزة التي لها علاقة ببعضها. بمعنى تجميع أجهزة الشؤون الإدارية على شبكة محلية افتراضية مؤمنة وتجميع أجهزة الشؤون المالية على شبكة أخرى ... وهكذا. وهذه الشبكات تحقق لنظام المعلومات مزايا عديدة من أهمها:

أ) توفير التأمين والحماية للشبكات المحلية ذات الطبيعة الحساسة لتطبيقات عمل المؤسسة.

ب) منع اختراق شبكة محلية من خلال شبكة محلية أخرى.

ج) زيادة معدل تدفق حزم البيانات فيما بين أجهزة نفس الشبكة المحلية الافتراضية المؤمنة.

د) منع انتشار الفيروسات وديدان الشبكات.

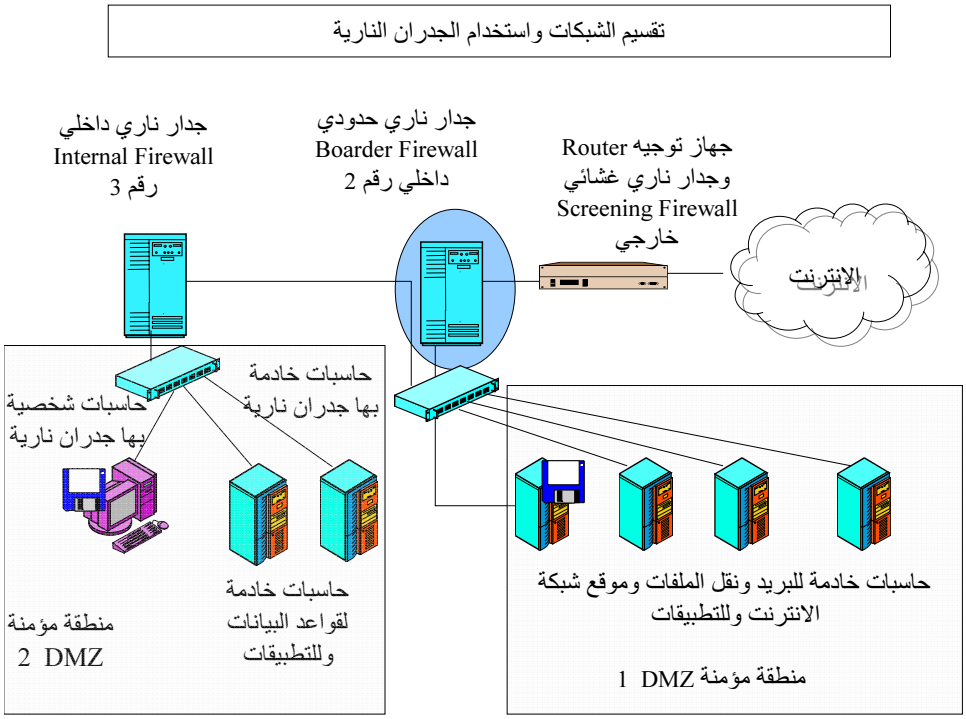
هـ)توفير المسؤولية والمحاسبة (Auditing and Accounting) فيما بين مستخدمي الشبكة الواحدة.

و) الاستغلال الأمثل لقواعد البيانات ووسائل التخزين ((Storage Area Networks (SAN).

ويشكل استخدام الشبكة المحلية الافتراضية المؤمنة وسيلة تأمين مساعدة للحماية من المتصنتين. حيث تنتقل حزم البيانات بين حاسبين في نفس الشبكة المحلية الافتراضية دون أن تتمكن باقي الأجهزة الموجودة معها في نفس شبكة الربط الطبيعي (ولكنها في شبكة افتراضية أخرى) من الاطلاع عليها.

2-2-1-5-6 الجدران النارية (Firewall)

الجدار الناري عبارة عن حاسب أو برنامج يصمم لحماية شبكة معلومات المؤسسة من الأشخاص والجهات غير المصرح لها وبالأخص عند الدخول من خلال الإنترنت. من المهم توافر أحد أشكل الجدران النارية الخارجية لحماية الشبكة من المتطفلين والمخربين وزارعي البرامج الخبيثة الموجودين على الإنترنت. والشكل رقم (16): يوضح أسلوب عمل الجداران النارية الخارجية التي توضع مابين الشبكة المحلية والإنترنت.



الشكل رقم (16): أسلوب عمل الجدران النارية بين الشبكة المحلية والإنترنت

وبدراسة الشكل رقم (16) يتضح وجود ثلاثة أنواع من معدات وبرامج الجدران النارية طبقاً للمكان الطبيعي لوجودهم ضمن البنية الأساسية لشبكة النظام وهم:

أ) الجدران النارية الغشائية (Screening Firewalls) وغالباً ما تكون برامج ضمن الموجهات Routers وتعمل "كخط دفاع أول" بين الانترانت (الشبكة المحلية) والإنترنت التي تربط نظام المعلومات بالمشتركين الخارجيين المصرح لهم بالإضافة للمستفيدين منه.

ب) الجدران النارية الحدودية (Boarder Firewalls) وتعمل "كخط دفاع ثاني" بين الحاسبات الخادمة لتطبيقات الإنترنت (Internet Applications) (مثل البريد والويب ونقل الملفات) والحاسبات الخادمة لتطبيقات العمل (Business Applications) (مثل قواعد البيانات والتطبيقات).

ج) الجدران النارية الداخلية (Internal Firewalls) وقد يوجد أكثر من جدار ناري حيث تعمل "كخط دفاع ثالث" بين محطات العمل للمشتركين الداخليين والخارجيين وبين الحاسبات الخادمة للتطبيقات والحاسبات الخادمة لقواعد البيانات.

وتعمل أجهزة وبرامج الجدران النارية كحاجز/فلتر/مرشح بين شبكتين أو أكثر طبقاً لعدد منافذ الأجهزة وتختبر كافة حزم البيانات الصادرة والواردة وتقرر طبقاً "لقواعد المرور" Access Control List ACL or Rule Base ما إذا كان يجب السماح للحزم بالمرور إلى الشبكة الأخرى أم لا. ويمكن أن تأخذ الجدران النارية عدة أشكال مختلفة فقد تكون على هيئة حاسب يتضمن برنامج خاص يراقب حركة حزم البيانات الواردة والصادرة وقد يكون برنامج فقط يعمل مع الموجهات أو وحدات التوصيل أو على الحاسبات الشخصية أو الحاسبات الخادمة. وغالباً ما يكون ضمن حزمة من برامج التأمين الأخرى تشمل التعرف على الهوية ومنع الفيروسات واكتشاف الاختراقات والتشفير والشبكات الافتراضية المؤمنة والنطاقات الأمنية وترجمة العناوين.

وتستخدم الجدران النارية الداخلية لحماية أجزاء من الشبكة المحلية عن بقية الأجزاء الأخرى حيث يتم من خلالها إنشاء نطاقات أمنية (Security Zones) أو DMZ وتستخدم الجدران النارية عند المرور من نطاق أمني إلى النطاق الآخر طبقاً لسياسة مرور محددة كما يتضح من الشكل رقم (16).

أهم أنواع الجدران النارية طبقاً لمستوى اختبار وفلترة المرور:

أ) فلترة حزم البيانات (Packet Filter) التي توجه تدفق المرور في الشبكة

ب) فلترة دوائر الربط (Circuit-Level Firewall) بين الإنترنت والشبكة الداخلية

ج) الجدران النارية لفلترة التطبيقات (Application-Level Firewall)

د) ترجمة عناوين الشبكة (NAT)

هـ) الموجه أو (Router) الوكيل

أ) فلترة حزم البيانات (Packet Filter): فلترة حزم البيانات هو النوع الأساسي بين أنواع الجدران النارية ويعمل بطريقة فحص حزم البيانات التي تصل إلى بوابات الربط Ports التي تفصل بين الشبكة الداخلية والإنترنت أو فيما بين النطاقات الأمنية للشبكة الداخلية. ويقرر ما إذا كان سيسمح للحزم بالوصول إلى الشبكة الأخرى اعتماداً على معلومات يجدها في جدول المرور Access Roles or Rule Base للبروتوكولات المستخدمة لبناء الحزم. ويمكن فلترة الحزم على أي طبقة من طبقات المواصفات القياسية للشبكات (TCP/IP).

كما يمكن أن يتسبب نظام الفلترة في إبطاء سرعة الشبكة بشكل ملحوظ. ومن المهم التطوير المستمر للجدران النارية لأن وسائل اختراقها تتطور سريعاً.

ومن أهم سمات فلترة حزم البيانات الآتي:

- فلترة العناوين الطبيعية (Permanent IP addresses): يتم فلترة الحزم طبقاً لعناوين الأجهزة الحقيقية بهدف تمكين حاسبات معينة فقط من إرسال البيانات إلى الشبكة الأخرى. ولا يستخدم هذا النوع كثيراً لحماية الشبكات من الوصول غير المصرح به

عن طريق الإنترنت. ولكن يمكن استخدام هذه التقنية في الجدران النارية الداخلية للسماح لحاسبات معينة فقط بالوصول إلى نطاق أمني معين من الشبكة.

- فلترة العناوين المنطقية الافتراضية (الديناميكية) (Dynamic IP addresses): يمكن استخدام فلترة العناوين IP للسماح فقط لحزم البيانات الموجهة إلى أو الواردة من عناوين معينة بالمرور إلى الشبكة.
- فلترة محددات البروتوكولات (Protocol Identifiers): تستطيع الجدران النارية فلترة حزم البيانات بحسب البروتوكول الذي ينتج حزم البيانات المحمولة ضمن المواصفات القياسية للشبكات (TCP/IP) شاملاً ذلك بروتوكول التحكم النقل (TCP) وبروتوكول المخططات البيانية للمستخدم (UDP) أو بروتوكول رسائل التحكم بالإنترنت (ICMP)
- فلترة أرقام المنافذ وأنواع التطبيقات (Port Numbers): تستطيع الجدران النارية فلترة الحزم بحسب رقم منافذ المصدر والوجهة المحددين في جدول المرور طبقاً لنوع النقل المتضمن في بيانات الحزمة.

دفع التنافس الحاد بين الشركات المنتجة للجدران النارية إلى المزيد من الابتكارات والتطوير في المعدات والبرامج ليس فقط في مجال سرعة الأداء وتقديم الخدمات حتى مستوى التطبيقات. بل وأيضاً في تضمينها قدرات متعددة تفوق ما كان متوفراً في تلك الأيام.

وتتمثل أهم القدرات التي أضيفت للجدران النارية الحديثة ما يلي:

1) التحقق من هوية المستخدمين: ذلك إن أول ما أضافه المطورون إلى الجدران النارية الأولى كانت القدرات القوية للتحقق من الهوية. وإذا كانت السياسيات الأمنية التي تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة المحلية البعيدة من خلال شبكة خارجية واسعة مثل الإنترنت فإنه لا بد من استخدام تقنية متعددة للتحقق من هوية المستخدمين ومنحهم الصلاحيات طبقاً لهويتهم. والتحقق من الهوية يعني ببساطة التأكد من صحة هوية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية والتي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين.

   ذلك أنه وعلى وصلة غير خاصة مثل وصلة غير مشفرة عبر الإنترنت فإن أسماء المستخدمين وكلماتهم المرورية يمكن نسخها وإعادة استخدامها (Attacks Replay). أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية (Certificates) أو برمجيات حساب الشفرات الرقمية الخاصة. وبواسطة الشهادات الرقمية يمكن تفادي هجمات إعادة الاستخدام حيث يتم نسخ اسم المستخدم وكلماته المرورية وإعادة استخدامها للدخول على الشبكة .

2) الشبكات الافتراضية المؤمنة: أما الإضافة الثانية إلى الجدران النارية للإنترنت فكانت التشفير البيني للجدران النارية (firewall - to firewall) عن طريق تكوين الشبكات الافتراضية المؤمنة. وكان أول منتج من هذا النوع هو ans interlock وهذه المنتجات هي ما ندعوها اليوم بالشبكات الافتراضية المؤمنة الخاصة (Virtual Private Network (VPN)) التي سبق الإشارة إليها في مقدمة الفصل والشكل رقم (2) وهذه الشبكات خاصة لأنها تستخدم التشفير وهي افتراضية خاصة لأنها تستخدم الإنترنت وشبكات عامة لنقل المعلومات الخاصة. ورغم أن الشبكات الافتراضية الخاصة كانت متوفرة قبل برمجيات الجدران النارية باستخدام المودمات أو الموجهات للتشفير لكنها أصبحت تستخدم فيما بعد ضمن برمجيات الجدران النارية.

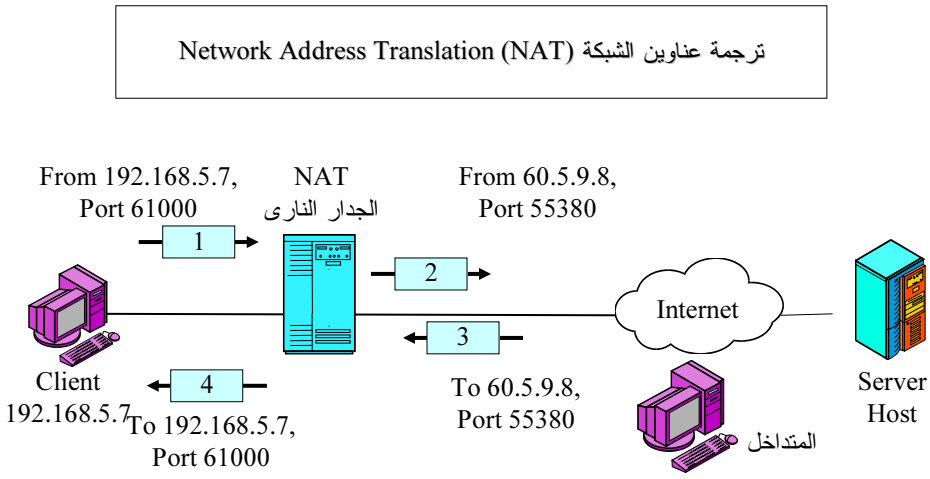
ويمكن باستخدام النظم الشبكات الافتراضية الخاصة أن تستبدل المؤسسة القنوات المؤجرة من مقدمي خدمة نقل البيانات بالقنوات المشفرة عبر الشبكات العامة مثل الإنترنت.

3) مراقبة المحتوى (Content Control, Filtration, and Screening): خلال العامين الماضيين أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة المحتوى الوارد من أو إلى الشبكة وترشيح المحتويات غير المرغوب فيها.

4) ومن بعض الإضافات التي وضعت في برامج الجدران النارية أيضاً هي العمل كمضادات للفيروسات ومراقبة عناوين الإنترنت ومنع برمجيات جافا غير المرغوب فيها مع إضافة برامج فحص ومراقبة الاسم وكلمات المرور.

3-2-1-5-6 ترجمة عناوين الشبكة (NAT):

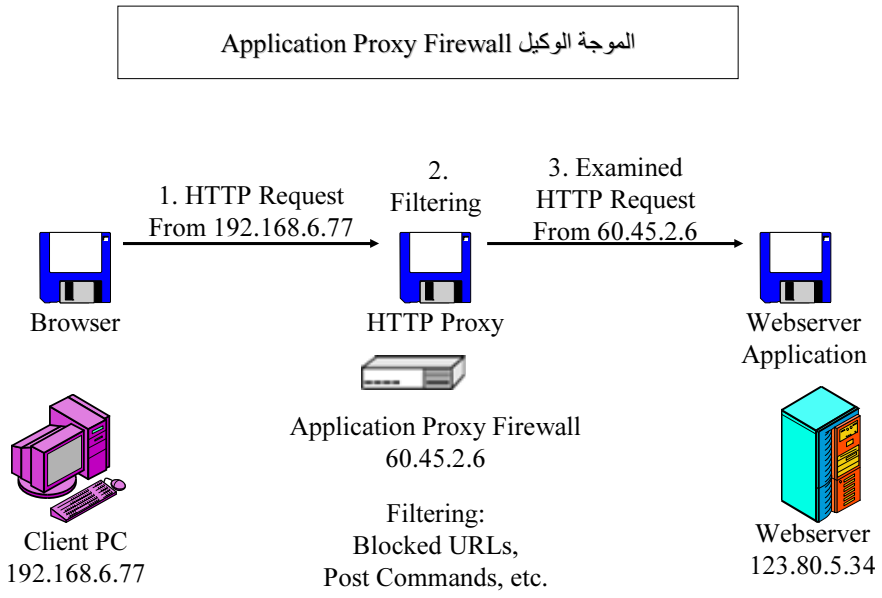
تعمل تقنية ترجمة عناوين الشبكة على مستوى طبقة النقل وتحمي حاسبات الشبكة من المتطفلين الخارجين بالإنترنت عن طريق حجب العناوين IP الخاصة بها طبقاً للشكل رقم (17) وبهذه الطريقة لا يستطيع المستخدمين الخارجيين رؤية الحاسبات عن طريق الإنترنت. لكن هذا يعني أن أي حاسبات على الشبكة لا يستطيع إلا إرسال حزم البيانات إلى الإنترنت لكنه لا يستطيع استلامها إلا من خلال الدخول عن بعد Telnet على حاسب ترجمة عناوين الشبكة NAT.



الشكل رقم (17): ترجمة العناوين NAT

6-5-1-2-4 الموجه أو المسيّر (Router) الوكيل (Proxy):

تشبه برامج الوكيل (Proxy) موجهات NAT وتعمل كوسيط بين المستخدمين بالشبكة المحلية وبين موارد الإنترنت التي يريدون الوصول إليها طبقاً للشكل رقم (18). وتستطيع الموجهات الوكيلة (Proxy Router) تخبئة المواقع والمعلومات التي تصلها من الإنترنت في ذاكرتها الضمنية الداخلية (Cache Memory) بحيث إذا طلب عميل آخر نفس المواقع أو المعلومات يستطيع الموجه (Router) الوكيل تقديمها في الحال من الذاكرة الداخلية بدلاً من طلبها ثانية من الإنترنت. وتستخدم الموجهات (Router) الوكيلة لفرض القيود كثيرة على وصول المستخدمين إلى الإنترنت كما تقوم بترشيح المواقع ومحتويات المواقع لحجب المواقع أو المواد غير المرغوب فيها.



الشكل رقم (18): الموجة الوكيل (Applications Proxy)

6-5-1-2-5 بروتوكولات التشفير لتطبيقات الإنترنت

هنالك عدد من البروتوكولات القياسية الخاصة بالتأمين تعرضنا لها بالتفصيل في الفصل الخامس تستخدمها التطبيقات وأنظمة التشغيل لحماية بياناتها أثناء الإرسال عبر الشبكة وتطبق هذه البروتوكولات بشكل عام أنواعاً معينة من نظم تشفير البيانات من أهمها الأنواع الموجودة في الجدول التالي:

مستوى بروتوكول IP	الأنظمة الشفرية
التطبيقات (Application)	Kerberos, RADIUS Dial-Up Remote Access
النقل (Transport)	SSL/TLS: Secure Socket Layer/Transport Layer Security SET: Secured Electronic Transactions
الإنترنت (Internet)	IPsec: Internet Protocol Security
التحكم في المحور (Data Link)	PPTP Point to Point Tunneling Protocol , L2TP: Layer 2 Tunneling Protocol
الربط الطبيعي (Physical)	تشفير نهاية – بنهاية أو تشفير حزمي

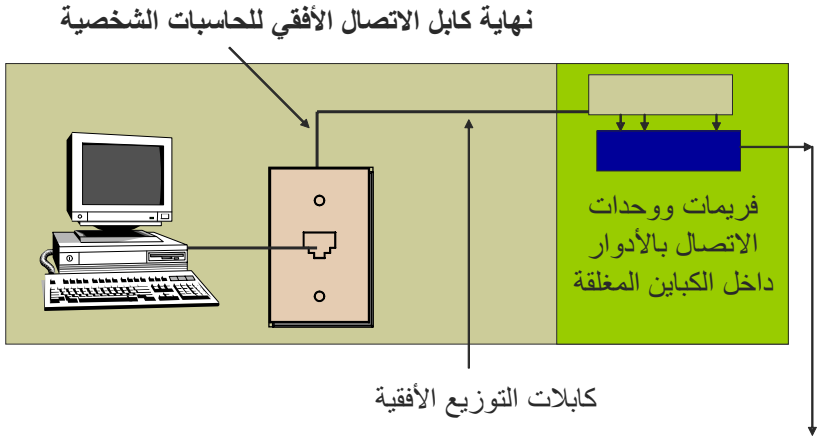
6-2-1-5-6 استخدام الاسم وكلمة المرور لمعدات الشبكة

يؤدى استخدام الاسم وكلمة المرور إلى حماية مكونات الشبكة المحلية القابلة للبرمجة مثل الموجهات (Routers) والموصلات (Core and access switches) ومعدات تأمين وإدارة الشبكة. ويفوت اختراق المتطفلين لها ومعرفتهم بمحددات البرمجة (Configuration parameters).

7-2-1-5-6 الحماية الطبيعية لمعدات الشبكة

الحماية الطبيعية لمكونات الشبكة المحلية هامة جداً (الشكل رقم (19)) حيث يتم وضع المكونات في كباين خاصة تكون مغلقة في جميع الأوقات لمنع وصول المتطفلين إليها. كما يتم إنشاء كوابل الشبكة داخل مواسير خاصة مغلقة أو من أعلى الأسقف المعلقة أو أسفل الأرضيات المرتفعة. ويفضل التوسع في استخدام كوابل الألياف الضوئية التي لا تشع أي موجات كهرومغناطيسية مما يجعلها مؤمنة طبيعياً ضد التصنت.

تأمين معدات الشبكة المحلية

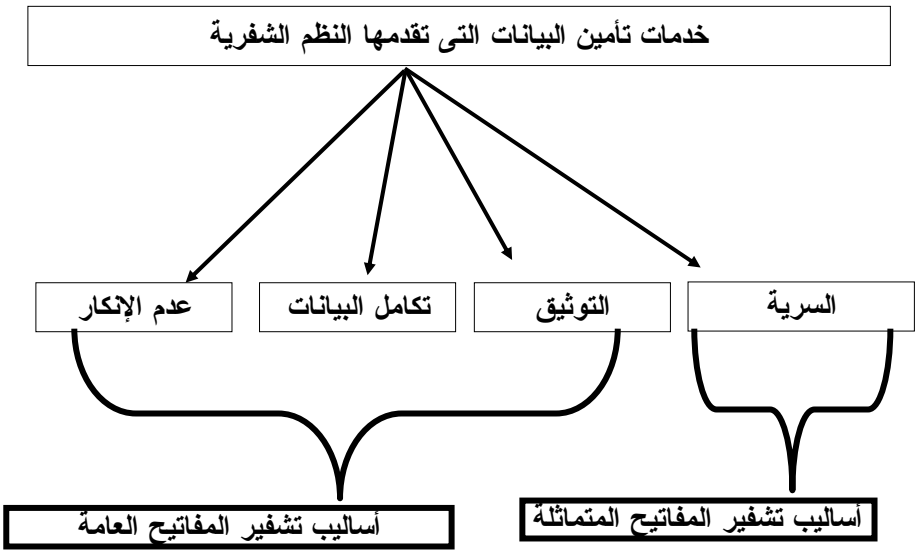


الشكل رقم (19): التأمين الطبيعي لمكونات شبكة المعلومات المحلية

3-1-5-6 تأمين المعلومات المتداولة على الإنترنت

إن من البديهيات في حماية المعلومات منع الوصول غير المصرح إليها والاهتمام بتقوية هذا الجانب وذلك من خلال ما يلي:

1) وضع كلمات سر إضافية عند الدخول للملفات الحساسة.
2) مراجعة الصلاحيات الممنوحة للمستخدمين جيداً قبل وضعها قيد التنفيذ.
3) استخدام وسائل التشفير فيها يتم تحويل البيانات الواضحة إلى بيانات مشفرة باستخدام خوارزم ومفتاح شفرة بحيث يتمكن المستقبل للبيانات فقط من إعادة تحويل البيانات المشفرة إلى بيانات واضحة مرة أخرى. وتستخدم وسائل التشفير لحماية المعلومات ذات درجة السرية العالية سواء عند تخزينها بالحاسبات أو عند تداولها عبر الشبكات. وعندما يتم تشفير البيانات فان المتطفلين لن يتمكنوا من الوصول للبيانات الواضحة مثل البيانات الشخصية أو بيانات بطاقات الاعتماد وبالتالي لن يتمكنوا من التصنت عليها أو تحريفها كما لن يستطيع المستقبل للبيانات أن ينكر استلامه لها خصوصاً مع استخدام التوقيع الإلكتروني وشهادات التوثيق كما تم شرحه في الفصل الخامس حيثما تم إيضاح أساليب التشفير المتماثلة وغير المتماثلة التي تحقق للبيانات خدمات التشفير التي من أهمها السرية والتوثيق والتكامل وعدم الإنكار طبقاً للشكل رقم (20).



الشكل رقم (20): خدمات تأمين البيانات إلى تقدمها النظم الشفرية

4-1-5-6 الحماية من المخاطر والاختراقات

يوجد عدد من الوسائل لتوفير الحماية لشبكات المعلومات أغلبها في شكل منتجات معدات وبرامج. وقد يكون للمنتج الواحد أكثر من وظيفة ومن هذه الوسائل ما يلي:

1) أدوات كشف الاختراقات الأمنية (Intrusion Prevention and Intrusion Detection):

وهى عبارة عن معدات وبرامج ومستشعرات وحواجز وعوائق يتم وضعها أمام المخترقين تعمل على منعهم أو تأخير وصولهم إلى البيانات ومصادر المعلومات مما يعطى شبكة المعلومات الفرصة والوقت لاكتشافهم وإغلاق المنافذ التي يحاولوا الدخول منها.

وتساعد أدوات كشف الاختراق على مراقبة الشبكة وأجهزة الحاسبات ذات درجة الحساسية العالية – وتنذر المدير وكيان الأمن بالنظام عند الاشتباه بحدوث محاولة للاختراق. وتعتمد بعض هذه الأدوات على التعرف على أسلوب الهجوم وبعضها يتوقع الهجوم قبل حدوثه. حيث إن كل نوع هجوم له سمة أو بصمة (Signature) فيتم التعرف على نوع الهجوم من خلال تطابق السمات الموجودة أصلاً في برنامج كشف الاختراق والسمات التي تصل مع البيانات – بينما تعتمد أنواع أخرى من أدوات كشف الاختراق على سمات التعامل مع الحاسبات حيث يسجل لكل مستخدم سمات مميزة له مثل: وقت الدخول للنظام ووقت الخروج منه وطبيعة البرامج والتطبيقات والبيانات والتقارير التي يستخدمها وسرعة استخدامه للوحة المفاتيح – ويتم الفحص لكل مستخدم أثناء تشغيل الحاسب وعند اكتشاف عدم التطابق يتم تحذير مدير النظام وكيان الأمن بإشارة إنذار عن وجود تصرف "مشكوك فيه" أو "شاذ" أو "غير مألوف".

تقوم بعض تطبيقات الحماية بمراقبة ملفات النظام والملفات الحساسة بإضافة توقيع خاص لكل ملف يعتمد على مكونات الملف Digest لسرعة اكتشاف أي تعديل غير مصرح به على الملف.

والشكل رقم (21) يوضح استخدام معدات منع الاختراقات (Intrusion Prevention System) وكشف الاختراق (Intrusion Detection System) بعد معدات الجدران النارية الغشائية (Screening Firewall Router) مباشرة لتمثل خط دفاع قوى ضد الاختراقات التي قد لا تقدر الجدران النارية على منعها. ولقد تم مؤخراً وقف إنتاج معدات كشف الاختراقات (IDS) واكتفت الشركات بإنتاج معدات منع الاختراقات (IPS) التي تتميز بالخصائص التالية:

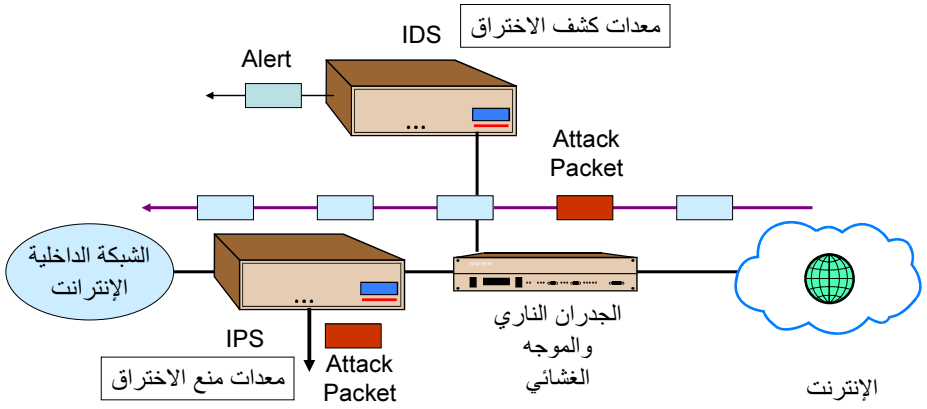
أ) السرعة الفائقة في منع الاختراقات حيث إنها مبنية على مكونات إلكترونية فائقة التجميع وتنفذ تطبيق المنع فقط ((Application Specific Integrated Circuit (ASIC) وتعمل على سرعات تصل إلى جيجاب/ث مما يؤهلها لتكون في مسار حركة البيانات (In Line) دون أن تؤثر على كفاءة الشبكات.

ب) مخزن بها جميع بصمات الاختراقات الأمنية وتعتمد عليها في المنع مع إمكانية إضافة بصمات جديدة لها. كما لها القدرة على التعلم الذاتي (self learning) وتحديث بصمات أي اختراقات جديدة.

ج) تعمل على جميع الطبقات المعمارية للأنظمة حتى مستوى التطبيقات.

د) تمد مدير الشبكات بتقارير تساعد على كشف مصادر التهديدات وأنواعها.

معدات الكشف ومنع الاختراقات الأمنية
Intrusion Detection System IDS
and Intrusion Prevention System IPS



الشكل رقم (21): معدات كشف الاختراقات (IDS) ومعدات منع الاختراقات (IPS)

2) وسائل منع زرع الفيروسات والبرامج الخبيثة وسرعة اكتشافها والتخلص منها:

تقوم وسائل "منع زرع الفيروسات والبرامج الخبيثة وسرعة اكتشافها والتخلص منها" أو ما نسميه "مضادات الفيروسات" بفحص الملفات بشكل دوري أو حسب ما يحدده المستخدم ضمن "السياسة الأمنية للتعامل مع مضادات الفيروسات" وتبحث هذه الوسائل (معدات وبرامج) في الملفات عن بصمة أو سمات الفيروسات الشهيرة وتقوم بإنذار المستخدم ثم التخلص منها سواء بمسح برنامج الفيروس أو عزله أو مسح الملف المصاب بالكامل إذا تعذر علاجه. ومن المهم تحديث مضادات الفيروسات بشكل دائم كما يوجد بعض أنواع المضادات التي تخدم المؤسسة بأكملها حيث يتم تحديث المضادات عن طريق حاسب خادم متصل من خلال الإنترنت بموقع الشركة المنتجة التي تقوم بتعديل البرنامج بإضافة إمكانية كشف بصمة الفيروسات والبرامج الخبيثة التي تكتشف حديثاً. ومن الوسائل الفعالة للحماية ضد الفيروسات الآتي:

أ) فحص أيّ ملفات يتم تحميلها من نظام البريد على أوساط التخزين قبل استعمالها ويكون الفحص عند أماكن مختلفة شاملاً خادم البريد والحاسبات الشخصية أو عند الدخول لشبكة معلومات المؤسسة.

ب) الاهتمام بتدريب الأفراد على كتابة تقرير عند اكتشاف هجمات الفيروس.

ج) التخطيط لتحقيق استمرارية عمل ملائمة للعلاج من هجمات الفيروس يشمل ذلك خطة التخزين الاحتياطي لكلّ البيانات والبرامج الضرورية.

د) عمل إجراءات التدقيق والتفتيش على النشرات التحذيرية التي تتعلّق بالبرامج الخبيثة. والتي تضمن بأنّ النشرات التحذيرية دقيقة وغنيّة بالمعلومات المفيدة في الوقاية وسرعة الكشف والعلاج من الفيروسات.

هـ) التأكد من نزاهة مصادر البرامج والمعلومات المتعلقة بالفيروسات ومثال على ذلك الدوريات والنشرات والمجلات العلمية ذات الثقة في مواقع شركات موثوق فيها على الإنترنت.

و) توفير وسائل التمييز بين مضادات الفيروسات الخادعة والحقيقية.

3) تأمين التجارة الإلكترونية:

أصبح بمقدور أي شخص في أي دولة استخدام الإنترنت للاتصال من أجل تنفيذ الأعمال التجارية وأصبح مفهوم الشركة العالمية حقيقة حيث إن كل شركة لها موقع على الإنترنت تعتبر عالمية. وزالت حدود التجارة وأمكن تكوين الشراكات بين الشركات الموجودة على مستوى العالم. وأصبح من الممكن للشركات الاتصال بمورديها في أي مكان بالعالم من أجل الحصول على أفضل الأسعار أو للبحث عن منتج معين أو لمعرفة مطالب زبائن الشركة في كل مكان وبالتالي سينتج عن ذلك زيادة عدد المنتجات وتقليل أسعارها وتطويرها باستمرار. ومن مزايا التجارة الإلكترونية بناء الشركات الضخمة والوصول إلى أسواق متنامية بخطوات حثيثة تضم ما يزيد عن مليار شخص والوصول كذلك إلى النظم الحديثة في الإنتاج والتسويق وفى ميكنة إنتاجية الشركات وفى وسائل الدفع الإلكتروني عن طريق بطاقات الائتمان والشيكات الإلكترونية وحوافظ النقود الإلكترونية وغيرها. مما يعود بالنفع على كل عناصر التجارة الإلكترونية وهم: الحكومات – الشركات – الموردين – والمستهلكين.

وتتعرض التجارة الإلكترونية عبر الإنترنت إلى مخاطر عديدة من أهمها محاولة المجرمون سرقة أو تبديل بيانات السداد والغرض هو الاستيلاء على بيانات شخصية مثل أرقام بطاقات الائتمان والاسم الموجود على البطاقة وتاريخ الاستحقاق ثم يقومون باستخدام هذه المعلومات فيما بعد لشراء سلع أخرى عبر الإنترنت للتسليم إلى عنوان مؤقت وبمرور الوقت يتم اكتشاف عملية الغش ويختفي المجرمون ومن هذه الأساليب محاكاة المواقع والتلصص على المعلومات وتبديل المحتوى والإنكار. ويتم تأمين التجارة الإلكترونية من خلال نظم تأمين نقل البيانات (Security Socket Layer (SSL)) أو (Transport Layer Security (TLS)) التي تمت الإشارة إليها في الفصل الخامس.

4) تأمين البريد الإلكتروني:

كما سبق الإشارة إليه في الفصل الثاني يستخدم البريد إلكتروني لتنفيذ تطبيقات العمل وهو يعتبر بديل حديث وفعال للإشكال التقليديّة من وسائل الاتصالات مثل تداول الرسائل والتلكس. ولكن يختلف البريد الإلكتروني عن باقي أشكال الاتصالات التقليديّة في بعض المزايا والعيوب. فمن مزايا البريد الإلكتروني السرعة والسهولة في تداول الرسائل وكذلك إمكانية التنميط القياسي للشكل ولمكونات الرسائل.

ويعيب البريد الإلكتروني عدم إمكانية تقييد تداوله وعدم مقاومته لأعمال التداخل والتعديل والتصنت غير المصدق بها. لذا يحتاج البريد الإلكتروني إلى وسائل تحكم خاصة لتقليل المخاطر من استخدامه.

تشمل المخاطر الأخرى لنظم البريد الإلكتروني الآتي:

أ) إمكانية الدخول غير المصرح به على الرسائل بهدف الإطلاع أو التعديل أو المحو.

ب) إمكانية وجود أخطاء في تداول الرسائل مثل إرسالها للعناوين الخطأ أو سوء توجيهها إلى الجهة المرسل إليها بالإضافة إلى الاعتمادية الضعيفة والقدرة على البقاء المحدودة لخدمة البريد الإلكتروني.

ج) تأثير التغيير في وسيلة ووسط الاتصال على تنفيذ تطبيقات العمل من خلال البريد الإلكتروني. على سبيل المثال قد يحدث تأخير في تداول البريد الإلكتروني نتيجة الحركة الزائدة للرسائل. كما أن هناك قيد خاص بتداول الرسائل الرسميّة من فرد إلى فرد بدلاً من تداولها من مؤسسة إلى مؤسسة أخرى.

د) الاعتبارات القانونية مثل الحاجة للتأكد من هوية جميع أطراف عملية تداول البريد الإلكتروني شاملاً ذلك المرسل (الذي يجب أن يقوم بأرشفة جميع رسائله أما داخل ذاكرة حاسبة الشخصي أو في ذاكرة خادم البريد) وخوادم البريد والمستلم والمسؤول عن الرد على الرسائل.

هـ)مخاطر ضمنية مثل إمكانية نشر قائمة بالعناوين البريدية للمديرين والأفراد الآخرين المخزنة في القوائم البريدية لخوادم البريد.

و) الحاجة لوجود نظام تحكم في دخول المشترك البعيد على "خادم بريد" المؤسسة بهدف التأكد من هويته.

5) تأمين نظام النشر على شبكة الإنترنت:

يلزم العناية بحماية نزاهة ومصداقية نشر معلومات المؤسسة إلكترونياً على موقع الويب لمنع أي تعديلات غير مصرح بها الأمر الذي قد يؤدى إلى الضرر لسمعة المؤسسة. يتم التأكد من أن المعلومات المصرح بنشرها علنياً تتطابق مع تلك الموجودة على موقع المؤسسة بشبكة الإنترنت وأنها تلتزم وتتطابق مع القوانين والإجراءات ولوائح السلطة القانونية الموجودة في بلد المؤسسة أو الإجراءات المطلوبة مثلاً لتنفيذ نظم التجارة الإلكترونية. ويلزم أن يكون هناك تصديق رسمي من الإدارة العليا على عملية النشر العلني للمعلومات.

تتطلب البرامج والبيانات والمعلومات الأخرى للنشر علنياً مستوى عالي من النزاهة والمصداقية من خلال تطبيق وسائل التأمين والحماية المناسبة مثل شهادات التوثيق والتوقيع الإلكتروني.

يلزم توفير وسائل التأمين والحماية للمعلومات المنشورة إلكترونياً خاصة تلك التي تحتاج إلى التفاعل والرد العكسي أو إدخال مباشر للبيانات على قواعد بيانات المؤسسة بطريقة إلكترونيّة. والغرض من وسائل التأمين ضمان الآتي:

أ) التأكد من أن المعلومات متطابقة مع تشريع حماية البيانات الشخصية على المستوى القومي.

ب) التأكد من أن المعلومات الداخلة إلى والمعالجة بواسطة نظام النشر العلني قد تمت معالجتها بدقة وفي الوقت المناسب.

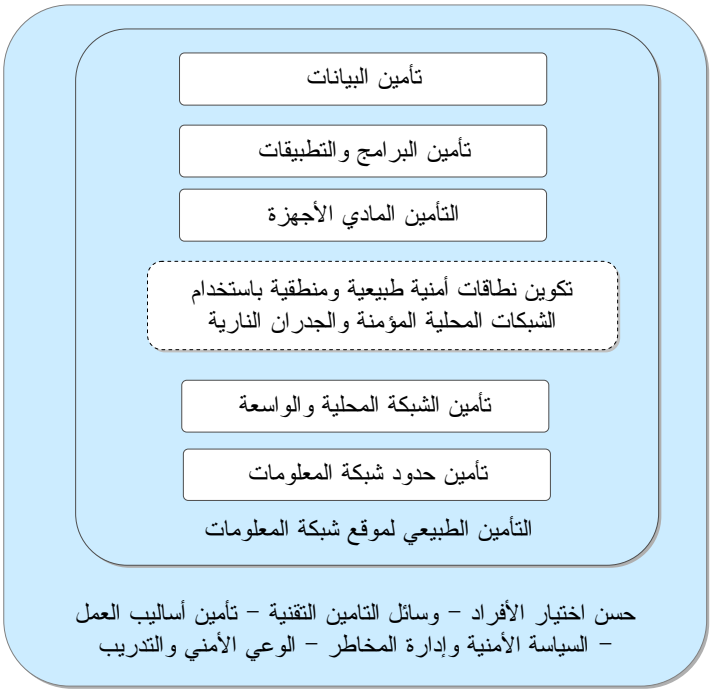
ج) حماية المعلومات الحسّاسة أثناء عملية التجميع وعند التخزين.

د) للحماية ضد الدخلاء. لا يتم السماح للدخول إلى نظم معلومات المؤسسة من خلال الدخول إلى المعلومات المنشورة علناً بواسطة شبكات الاتصال وهذا دور الجدران النارية الحدودية (Boarder Firewalls) المشار إليها في بند 6-5 والشكل رقم (2).

2-5-6 التأمين المتكامل

تم في هذا الكتاب تقديم عدة وسائل لحماية النظم التي تعتمد على الإنترنت من التهديدات. وتعتبر هذه الوسائل "ضرورية ولكنها غير كافية" ويجب زيادة كفاءتها طبقاً للشكل رقم (22) بوسائل تتكامل معها من أهمها إجراءات "السياسة الأمنية" التي يجب أن تتوافق مع: الهيكل التنظيمي المساند لنظام المعلومات واتجاهات تطبيقات العمل للمؤسسة والتطور التقني المستمر في مجال نظم الشبكات والمعلومات.

تحدد "السياسة الأمنية" إجراءات ووسائل الإدارة والتحكم في سرية المعلومات وإجراءات حماية التشغيل والاتصالات ومن المهم تطوير السياسة الأمنية بالاستعانة للخطوط العريضة التي تتضمنها المواصفات والمعايير القياسية العالمية في أمن وسرية المعلومات ومن أهمها وثيقة ISO/IEC 27001 /17799:



الشكل رقم (22): التأمين المتكامل لشبكات المعلومات

ومن أهم الأهداف عند تطوير السياسة الأمنية الفعالة لشبكات المعلومات الآتي:

1) أول وأهم الأهداف حماية الأشخاص من مخاطر استخدام الشبكة عندما تكون غير مؤمنة خاصة ضد أخطار الإهمال والتخريب والظروف المحيطة الطارئة.
2) توفير وسائل أمنية كافية للشبكات دون الحد من استغلالها في تطبيقات العمل.
3) إعطاء ثقة المستفيدين في إمكانية استخدام الشبكات دون خوف من تأثير الاختراقات الأمنية.
4) تعظيم استغلال الشبكات خاصة الشبكات الواسعة وعلى رأسها الإنترنت في تنفيذ تطبيقات العمل والنظم الإلكترونية الحديثة مثل التجارة الإلكترونية والبريد الإلكتروني.

من المهم وضع النقاط الآتية في الاعتبار عند وضع "السياسة الأمنية" لشبكات المعلومات:

أ) الهدف الأساسي هو تطوير سياسة متكاملة للتأمين والحماية لجميع عناصر شبكة المعلومات.

ب) التأمين والحماية من أهم الخدمات التي يوفرها النظام.

ج) سياسة التأمين والحماية يجب أن تكون ديناميكية وتتغير مع ظهور أساليب جديدة للاختراقات.

د) يكون اتصال الأشخاص عن بعد بالنظام من خلال الجدران النارية ومعدات منع الاختراقات وليس مباشرة.

هـ) تكون خدمات شبكة المعلومات بسيطة جداً ليسهل تتبع التفاعلات على البيانات (بالاستعلام أو التعديل) وبالتالي سرعة اكتشاف الاختراقات الأمنية.

و) يكون النظام بالكامل قابل للاختبارات وتحدد المسؤوليات طبقاً لأحقيات الدخول الممنوحة للأفراد من داخل وخارج النظام.

ز) يكون الاتصال من خلال خطوط الدايال في أضيق الحدود حيث إنه أكثر عرضة للاختراقات الأمنية مع التوسع في استخدام التشفير والتأكد من الهوية في جميع أنواع الاتصالات.

ح) تشفير أسماء المستخدمين وكلمات المرور والبيانات والمعلومات.

ط) التوسع في وسائل التحقق من الهوية والكروت الذكية عند استخدام البريد الإلكتروني.

ي) الاهتمام بالتدريب والتوعية على وسائل التأمين والحماية.

ك) إنشاء كيان الأمن ضمن الهيكل التنظيمي بحيث يكون مسؤول عن التأمين والحماية لنظم وشبكات المعلومات.

تشارك جميع أنواع التأمين والحماية المذكورة في هذا الفصل في إعاقة المتطفلين والمخترقين للإنترنت وكلما زادت الحماية كلما تأخر دخول هؤلاء على البيانات ومصادر المعلومات لفترة أطول مما يجعل فرصة كشفهم أكبر. وتكون لدى المؤسسة "السياسة الأمنية" التي تحدد وسائل التأمين والحماية المتبعة مع المخاطر والتهديدات وأساليب التعامل معها ومع كافة مكونات تأمين شبكة المعلومات والإنترنت. فعلى سبيل المثال هناك سياسة التعامل مع الجدران النارية وسياسة التعامل مع البريد الإلكتروني وسياسة التعامل مع خوارزميات التشفير وسياسة الدخول للحاسبات الشخصية والحاسبات الخادمة وسياسة التغلب على الفيروسات ... الخ.

المراجع

1. أ.د.احمد الشربيني وأ.م.د. وفائي بغدادي محمد:" إدارة تأمين نظم وشبكات المعلومات" المعهد القومي للاتصالات–2007.

* **أهم المنظمات والهيئات القياسية العالمية في مجال تأمين الإنترنت وشبكات المعلومات:**

2. CERT: Computer Emergency Response Team, www.cert.org
3. CIS: The Center for Internet Security, www.cisecurity.org
4. DISA: Defense Information Systems Agency, www.disa.mil
5. GAISPC: Generally Accepted Information Security Principles Committee, www.issa.org/gaisp.html
6. IANA: Internet Assigned Numbers Authority, www.iana.org
7. ICANN: The Internet Corporation for Assigned Names and Numbers, www.icann.org
8. IEFT: The Internet Engineering Task Force, www.ieft.org
9. IESG: The Internet Engineering Treering Group, www.iesg.org
10. ITU: International Telecommunication Union, www.itu.int
11. ISA: Internet Security Alliance, www.isalliance.org
12. ISACA: The Information Systems Audit and Control Association, www.isaca.org
13. ISF: Information Security Forum, www.securityforum.org
14. ISO: International Organization for Standardization, www.iso.org
15. ISSA: Information Systems Security Association, www.issa.org
16. NTIA: National Telecommunication and Information Administration, www.ntia.doc.gov
17. NCSA: National Cyber Security Alliance, www.staysafeonline.info
18. NIST: National Institute for Standards and Technology, www.nist.gov
19. NSA: National Security Agency, www.nsa.gov
20. NSI: Network Solution Inc, www.nsi.com
21. SANS: Systems Administration, Audit, and Network Security Institute, www.sans.org
22. U.S.A. CSI : Computer Security Institute و
www.gcsi.com

* أهم الكتب والبحوث والتقارير:

23. BS 7799: Parts 1&2 Code Practice for Information Security Management London, 2005 (British Standards Institute), www.bsi.org.uk

24. DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. London, 2005. (Became BS 17799), www.dti.gov.uk

25. Corporate Information Security Evaluation for CEO's (TechNet), www.technet.org/cybersecurity

26. Cisco Systems: "Security technologies [WWW document]. URL http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/security.htm, 2004

27. Cisco Systems: "Security Overview", http://www.cisco .com/univercd/cc/ td/doc/product/software/ios 11 3ed/ 11 3ed_cr/secur_c/scoverv.htm, 2004

28. D.L. Whealer: the Internet in the Arab world, digital divides and cultural connections, Rifs, 16 June 2004, www.rifs.org

29. D.E.Porter: ITSG, Information Technology Standards Guidance, USA Department of the Navy, 7 April 1999, www.doncio.navy.mil/itsgpublic

30. Electronic Security: Risk Mitigation in Financial IT Transactions, The World Bank, (Thomas Glaessner, Tom Kellermann, and Valerie McNevin), June 2002, http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf

31. GASP: Generally Accepted Information Security Principles Currently available, Generally Accepted Systems Security Principles (GASSP) consisting of Pervasive Principles (PP), Broad Functional Principle (BFP), And June, 1999.

32. H.F.Tipton, M.Mraise: " Information security management handbook". 5th edition, CRC PRESS LLC 2004

33. ICC Handbook on Information Security Policy for Small to Medium Enterprises, International Chamber of Commerce, April 11, 2003, www.iccwbo.org

34. IDC: International Data Center, http://www.internetworldstats.com/stats.htm

35. IFAC: International Guidelines on Information Technology Management, Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999, www.ifac.org

36. ISO 21827 System Security Engineering Capability Maturity Model, http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail

37. ISO 17799: Information Technology Code of Practice for Information Security Management, www.iso.org/iso/en/CatalogueDetailPage.

38. ISO TR 13335: "Guidelines for the Management of Information Security", Parts 1-5, ww.iso.org/iso/en/StandardsQueryFormHandler

39. ITCG: Information Technology: Control Guidelines 1998, www.cica.ca

40. ITU: Recommendations for Security in telecommunication systems architecture: Security architecture and frame works (X.800- X.816), Telecommunication Security (E.408, E.409, X.805, X.1051, X.1081, X.1121, X.1122).

41. ITU: Recommendations for Security techniques: (X.841- X.843)

42. ITU: Recommendations for Directory services and authentications (H.350, X.500, X.509, X.519).

43. J.H.Yu, M.K.Le: Internet and network security, Journal of Industral Technology, Vol. 17, No.1, Jan2001.

44. L.Gong: Mozilla: open source, and the future of the Internet, Mozilla online ltd, November 2007, www.spreadfirefox.com

45. Marianne Swanson & Barbara Guttmann: GAPP, Generally Accepted Principles and Practices, NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998

46. M. Stalney: Internet Trends, Morgan Stanley Research Estimates, 18 March 2008, www.morganstanly.com

47. NIST: DOC 800-14: Generally Accepted Principles and Practices for Securing IT Systems, 1996 , http://csrc.nist.gov/publications/nistpubs/index.html

48. NIST 800-12: The Computer Security Handbook, 1995, http://csrc.nist.gov/publications/nistpubs/index.html

49. NIST 800-37: Guide for The Security Certification and Accreditation of Federal Information Systems, http://csrc.nist.gov/publications/nistpubs/index.html

50. NIST 800-53: Recommended Security Controls for Federal Info Systems, http://csrc.nist.gov/publications/nistpubs/index.html

51. NIST 800-55: Security Metrics Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/index.html

52. NIST 800-26: Security Self-Assessment Guide for Information Technology Systems, http://csrc.nist.gov/publications/nistpubs/index.html

53. NIST 800-50: Building an Information Technology Security Awareness and Training Program, http://csrc.nist.gov/publications/nistpubs/index.html

54. OECD: Guidelines for the Security of Information Systems and Networks, December 2002.

55. Personal Information Protection and Electronic Documents, Act (PIPEDA), Canadian, www.pipeda.org

56. Raymond R. Panko: Corporate Computer and Network Security, University of Hawaii`, Prentice Hall, 2004, ISBN 0130384712, Ray@Panko.com

57. RSA: Data Security, http://www.rsa.com/rsalabs/faq/html/glossary.html. 2006

58. Shelly, G. S., Cushman, T. J., Vermaat, M. E., & Walker, T. J.: Concepts for a Connected World, Cambridge, MA, Course Technology, 2005

59. Sound Practices for Mgmt & Supervision of Operational Risk, http://www.bis.org/publ/bcbs96.pdf

60. SSH Communications Security: Introduction to Cryptography, http:// www.ssh.fi/tech/crypto/intro.html,2006

61. Stallings, W., Van Slyke, R: Business Data Communications, 5th Ed., Upper Saddle River, NJ, Prentice Hall, 2005

62. Standard of Good Practice for Information Security (Information Security Forum), www.isfsecuritystandard.com/index_ie.htm

63. Sun Microsystems: How to Develop a Network Security Policy, http:// www.sun.com/security/sec.policy.wp.html, 2000

64. Sun Microsystems: Mastering Security on the Internet for Competitive Advantage, Network Security Technologies, http:// www.sun.com/security/wpmastering, Sec/intro.html, 2005

65. T.L.Laquery: Directory of computer networks, digital press, 1990.

66. United States Department of Defense: Orange Book Parts I and II: The Criteria and Rationale and guidelines, A guideline on configuring mandatory access, http://libs/security/orange-Linux/refs/orange/orange-II-9.html, 1996

67. United States General Accounting Office: Information Security, Computer Attacks at Department of Defense Pose Increasing Risks, Report GAO/AIMD-96-84, Washington, D.C., Author, 1996

68. Usage and population statistics for the Internet world, www.internetworldstats.com

69. W. Stalling: Cryptography and network security, 4th edition, Prentice Hall, 2005.