Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 30، ديسمبر 2012

---

# أمن شبكات المعلومات الإلكترونية : المخاطر والحلول

**رجب عبد الحميد حسنين**
جامعة الحصن، أبو ظبي
الإمارات العربية المتحدة
ragabhassnen@yahoo.com

**الاستشهاد المرجعي**
**حسنين، رجب عبد الحميد**. أمن شبكات المعلومات الإلكترونية: المخاطر والحلول .- Cybrarians Journal .- ع 30 (ديسمبر 2012) .- تاريخ الاطلاع <سجل هنا تاريخ اطلاعك على البحث> .- متاح في: <أنسخ هنا رابط الصفحة الحالية>

## تمهيد

لقد أضحت الشبكات الإلكترونية من الضروريات الحاصلة في عصرنا الحديث، بحيث أصبح لا غنى عنها في المؤسسات والشركات والحكومات بل وحتى في البيوت، فحيثما أنت تجد من حولك أنواع عديدة من شبكات الحواسيب التي تنقل كماً هائلاً من المعلومات والبيانات بين الأشخاص والمؤسسات على مستوى العالم، وتتنوع هذه المعلومات والبيانات في أهميتها ودرجة سريتها من المعلومات العامة والعلمية العادية إلى المعلومات والإحصائيات الحكومية وميزانيات الدول والمعلومات الاستختباراتية بالغة الخطورة والسرية، وكل هذه الأنواع من المعلومات والبيانات إنما يتم تناقلها وحفظها في غالب الأحيان عبر شبكات الحاسوب على اختلاف أنواعها وأماكنها.

ومن هنا تأتي أهمية هذه الشبكات في العالم المعاصر والتعاملات اليومية بين البشر بشكل عام، ومن هذه الأهمية تنبع خطورة ما يمثله أمن هذه الشبكات وأمن المعلومات التي يتم تداولها عبر خطوطها

، ونحن هنا نحاول إيضاح أهمية أمن شبكات المعلومات وما هي المخاطر التي تتهددها؟ وكيفية مناهضة هذه المخاطر والحماية منها.

## نظرة عامة

"**البريد**" يعد من أول وسائل نقل المعلومات بين البشر، ويمكن القول أن فكرة إرسال واستقبال البريد هي نواة أو أقدم فكرة لشبكات المعلومات، ويعود تاريخ أول وثيقة جاء فيها ذكر "البريد" إلى حوالي عام 2000 ق.م.[1] عند قدماء المصريين، وبعدها بالطبع تطورت الفكرة عبر الزمن إلى أن جاءت الطفرة باختراع الهاتف العالم ألكسندر بيل عام 1922م، وتطورت الاتصالات وأصبح منها الاتصالات السلكية واللاسلكية، وأصبح بالإمكان التخاطب بين البشر عبر شبكات الاتصال في كافة أرجاء المعمورة، ووصلنا أخيراً إلى المقولة "أن العالم أصبح قريةً صغيرة" بفضل وسائل الاتصالات الحديثة وتكنولوجيا المعلومات.

## تعريف الشبكات

يقصد بالشبكات Networks نظام معين لربط جهازين حاسوب أو أكثر باستخدام إحدي تقنيات الاتصالات، وذلك بهدف تبادل المعلومات والبيانات المتاحة بين أكثر من طرف، وكذلك بهدف تشارك الموارد المتاحة مثل الطابعات Printers والبرامج التطبيقية Software، كما أن هذه الشبكات تسمح أيضاً بالتواصل المباشر بين أفراد مجتمع الشبكة[2].

كما يمكن القول أن شبكات المعلومات هي عبارة عن نوع من تقنية الاتصالات التي تستخدم في عمليات الربط بين مجموعة من مراكز المعلومات بهدف مشاركة وتبادل المعلومات فيما بينهم عن طريق أجهزة الحواسيب.

---

[1] البريد. متوفر على الرابط:
http://ar.wikipedia.org/wiki/%D8%A8%D8%B1%D9%8A%D8%AF_%D8%B9%D8%A7%D8%AF%D9%8A . تم زيارته 2011/12/19.

[2] شبكات الحاسوب. متوفر على الرابط.
http://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9_%D8%AD%D8%A7%D8%B3%D9%88%D8%A8 . تمت زيارته في 2011/12/18.

**الحاجة إلى الشبكات**

"**الحاجة هي أم الاختراع**" فما هي الحاجة التي أدت إلى ظهور الشبكات في عالمنا المعاصر، هناك العديد من العوامل التي أدت إلى ظهور شبكات المعلومات وفي أن تصبح عاملاً مهماً من عوامل تقدم ورقي الأمم في العصر الحديث، ذلك أن كل شئ تقريباً في عصرنا الحديث والحضارة الحديثة يعتمد بشكل أو بآخر على ما تقدمه هذه الشبكات من خدمات في عمليات توفير المعلومات والبيانات على مدار الساعة وفي كل أنحاء المعمورة، وليس هناك دليل أوضح من "شبكة الإنترنت Internet" للتدليل على ذلك، فمن الصعب الآن أن تجد من يسأل ما هي جدوى وجود الشبكة العالمية "الإنترنت" في حياتنا؟ وسوف نبرز فيما يلي أهم العوامل التي يمكن أن يُعزى إليها السبب في ظهور الحاجة إلى الشبكات :-

- **تبادل المعلومات**. الهدف الرئيسي من شبكات المعلومات هو عمليات تبادل المعلومات والبيانات بين أطراف مجتمع الشبكة في سهولة ويسر وفي أسرع وقت ممكن، وهذا ما تعمل عليه الشبكات القائمة مثلاً بين أجزاء المؤسسات فهي تعمل على تحقيق السيولة والسهولة في الحصول على المعلومات وتبادلها بين العاملين في هذه الشركة[3].
- **المشاركة في البرامج التطبيقية Sharing Software**. حيث تعمل الشبكات على تحقيق إمكانية المشاركة في البرامج المتاحة في مجتمع شبكة المعلومات بين جميع أفراد الشبكة، وذلك يعمل على توفير النفقات المالية في شراء نسخ متعددة من تلك البرامج.
- **المشاركة في موراد الشبكات Sharing Hardware**. من مميزات الشبكات أنها تعمل على التوفير أيضاً في الأجهزة والمعدات المستخدمة وذلك من خلال استغلال خاصية مشاركة موارد الشبكات مثل الطابعات وأجهزة التصوير وأجهزة الفاكس وغيرها كثير.
- **البريد الإلكتروني E-Mail**. إحدى ميزات شبكات المعلومات هي توفير إمكانية استخدام البريد الإلكتروني للعاملين وأفراد مجتمع الشبكة، مما يتيح إرسال واستقبال الرسائل والوثائق وأوامر العمل فيما بينهم.

[3] سليمان بن صالح العقلا. إنشاء الشبكات : المبادئ الأساسية لإختصاصي المكتبات والمعلومات /سليمان بن صالح العقلا، فؤاد أحمد إسماعيل. – الرياض : مكتبة الملك فهد الوطنية، 2000.

- **إنشاء مجموعات العمل Work Groups**. تتيح الشبكات فرصة تكوين مجموعات العمل لتنفيذ مهمة معينة، وتكون بتخصيص جزء من مساحة التخزين على الشبكة لأفراد هذه المجموعة فقط بعيداً عن باقي أفراد الشبكة.
- **الإدارة المركزية Central Management**. يحقق وجود معظم الموارد على الشبكة في عمليات الإدارة المركزية لهذه الموارد والاستفادة منها بالشكل الأمثل، كما تحقق سهولة تنفيذ عمليات النسخ الإحتياطي Backup.
- **التأمين Security**. حيث يمكن لمدير النظام **Administrator** التحكم في عمليات الولوج Enter والإتاحة Access.
- **القدرة على ربط أنظمة التشغيل المختلفة Access to other Operating Systems**. يمكن عن طريق تكنولوجيا شبكات المعلومات ربط أنظمة تشغيل مختلفة والعمل عليها.
- **تحسين الإنتاجية Improve Productivity**. حيث تعمل شبكات المعلومات على تحسين التعاون بين أفراد مجتمعها مما يؤدي إلى تحسين الإنتاجية بين الأفراد.

### أمن شبكات المعلومات Information Networks Security

لقد أوضحنا فيما سبق الأهمية الكبيرة لشبكات المعلومات وما تقدمه من خدمات كبيرة على كافة المستويات، ومن تلك الأهمية تنبع أهمية أن يكون هناك مستوى معين من الأمان في هذه الشبكات حماية للمستخدمين والمعلومات التي تحتويها، فقد انتشرت في السنوات الأخيرة العديد من المشاكل والجرائم التي تتعلق بأمن المعلومات واختراق العديد من شبكات المعلومات على مستوى العالم، بل وصل الأمر إلى اختراق أعلى الشبكات سرية في العالم مثل شبكة المخابرات الأمريكية CIA وغيرها من الشبكات، ولنا أن نتصور ما يمكن أن يمثله ذلك من تهديد للدول في عصر أصبحت فيها الحرب هي حرب المعلومات وليس حرب الأسلحة كما كان سابقاً.

ويمكننا تعريف "**أمن شبكات المعلومات**" على أنه مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تتهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

**أو** هي مجموعة من المعايير التي تحول دون وصول المعلومات المخزنة في الشبكات إلى الأشخاص غير المخول لهم الحصول عليها.

وأمن المعلومات ليس بالاختراع الجديد ولكن دائماً ما كان يحرص الإنسان على الاستقادة مما لديه من معلومات وألا يبوح بها إلا لمن يثق به أو يمكن أن يستفيد من هذه المعلومات، ولكن مع تطور تكنولوجيا المعلومات والزيادة الهائلة والمضطردة في كميات المعلومات والبيانات المتاحة في العالم وظهور شبكات المعلومات وقواعد البيانات التي يتم تخزين المعلومات فيها، أصبح من الضروري تنظيم عمليات الوصول إلى هذه المعلومات بتحديد الأشخاص المخول لهم الوصول إلي هذه المعلومات وكيفية ومستوى الوصول إليها.

**لماذا أمن شبكات المعلومات؟**

يشكل أمن المعلومات في العصر الحديث حجر الزاوية في علميات نهضة تكنولوجيا المعلومات والاتصالات، حيث أن المساهمة المتاحة للخصوصية تتناسب عكسياً مع التقدم التكنولوجي المعلوماتية والاتصالات، لقد أنهينا في الفقرات السابقة إيضاح أهمية شبكات المعلومات للجميع، وبالتالي فإنه من البديهي أن يكون لهذه الأهمية درجة من الحماية تتدرج في الأهمية بتدرج أهمية المعلومات المخزنة في هذه الشبكات، للإجابة على هذا السؤال لابد لنا أن نعرض بعض النماذج التي تم فيها اختراق بعض الشبكات لنبين أهمية أمن الشبكات والمخاطر التي يمكن ان تحدث في حالة عدم توفره.

**الحالة الأولى**: في عام 2002 اكتشفت شركة Daewoo Securities أن ما قيمته 21.7 مليون دولاراً من الأسهم التي تديرها قد بيعت بشكل غير قانوني، وذلك نتيجة مباشرة لاختراق شبكة الحاسوب الخاصة بها.[4]

**الحالة الثانية**: في عام 2003 قام موظف بإحدى الشركات الروسية باختراق شبكة المعلومات الخاصة بالشركة، وقام بتعديل راتبه الشهري ومجموعة من زملائه بزيادة الرواتب بنسبة معينة مما أدى بخسائر مالية للشركة لعدة شهور لعدم اكتشاف هذا الاختراق[5].

[4] محمد عبد الله القحطاني. أمن المعلومات بلغة ميسرة / محمد عبد الله القحطاني، خالد سليمان الغثبر.-الرياض : مكتبة الملك فهد الوطنية، 2008.
[5] محمد عبد الله القحطاني. مصدر سابق.

وهناك العديد من الحالات الأخري مثل اختراق شبكة معلومات وزارة الدفاع الأمريكي الذي حدث مرات عديدة في السنوات الأخيرة، ويمكن أن نرى مدى الخسائر التي تمثلها مثل هذه الاختراقات الأمنية لشبكات المعلومات، سواء كانت هذه الخسائر مالية كما في حالة الشركات أو خسائر معلوماتية واستخباراتية لا تقدر بمال ويمكن أن تمس باستقلال بلدان كبيرة مثل أمريكا، ومن هنا يتضح الأهمية القصوى لعمليات تأمين شبكات المعلومات، ويمكن أن نجمل بعض الأسباب التي أدت إلى الاهتمام بموضوع "أمن شبكات المعلومات" مؤخراً في النقاط التالية : -

1- **التقدم التكنولوجي**. فكما أدت التطورات الهائلة في مجال تكنولوجيا المعلومات والاتصالات إلى طفرة كبيرة في وسائل الاتصال وتكنولوجيا شبكات المعلومات وتخزينها، فإنه في نفس الوقت أدى إلى وجود عقول تعمل على إيجاد الثغرات الأمنية في هذه الشبكات واستغلالها الاستغلال السيئ فيما يسمى بـ"الوجه القبيح للتكنولوجيا".
2- **الطفولية والإندفاع**. حيث يتملك بعض الشخصيات دوافع طفولية وإندفاعية للحصول على المعلومات بطرق غير مشروعة لمجرد الإحساس بنشوة الإنتصار وكسر حواجز السرية والأمان المفروضة على شبكات المعلومات.
3- **إنتشار جرائم المعلومات**. فقد سادت في الفترة الأخيرة هوس الجرائم الإلكترونية وجرائم المعلومات والتي تبدأ من الأشخاص والمنظمات والشركات المتنافسة وتنتهي بالدول، وذلك فيما يعرف بـ"حرب المعلومات".

**وهنا يمكن** أن نقول أن أنظمة أمن شبكات المعلومات تتطلب حماية أصول وموارد نظم المعلومات بطرق مشروعة، وكذلك تنظيم العلاقات والاتصالات داخل شبكات المعلومات من دون تأثير على كفاءة النظام ولا على قدرة المستخدمين في الأداء.[6]

**ولكن** .. هل كل شبكات المعلومات تحتاج إلى تأمين؟ بالتأكيد يعتمد ذلك على ما تحتويه هذه الشبكات من معلومات وبيانات وطبيعة المستخدمين فيها، وكذلك رغبة الجهة المسئولة عن هذه الشبكات في حماية موارد وممتلكات هذه الشبكات من عدمه، ولكن بصفةٍ عامة يجب أن يكون هناك نوع من الحماية ولو على الأقل الحماية البسيطة لهذه الشبكات على سبيل الاحتياط ومنع دخول غير المرغوب

[6] يسري زكي. تبسيط أمن المعلومات والاتصالات.- (د.م. : د.ن.). متاح على الرابط.
http://yomgedid.kenanaonline.com/tags/77115/posts#http://yomgedid.kenanaonline.com/posts/113226 . تمت زيارته في 2011/12/18.

فيهم من الأوساط الخارجية، وعلى الجانب الآخر فإن هناك أنواع من شبكات المعلومات لابد من وجود نظام أمان وحماية لها ولا يمكن أن تترك بلا أمان، وذلك نظراً لما تمثله من أهمية كبيرة سواء على مستوى ما تحمله من بيانات ومعلومات أو على مستوى المستخدمين لهذه الشبكات، ومن أمثلة هذه الشبكات ما يلي: -

- **الشبكات الداخلية LAN**. مثل شبكات الشركات الصغيرة أو المدارس أو المستشفيات.
- **الشبكات الواسعة WAN**. مثل الشبكات الدولية التي تربط بين أجزاء من الدول.
- **الشبكات الخاصة Intranet**.

**جرائم المعلومات**.

"**للحقيقة وجوه أخرى**" يمكن أن تكون هذه العبارة معبرة بشكل كبير عما يمكن الحديث عنه في موضوع جرائم المعلومات وعلاقتها بتطور تكنولوجيا المعلومات والاتصالات والطفرة الهائلة في صناعة المعلومات ومعالجتها على المستوى العالمي، فكما جلبت هذه التكنولوجيا لنا العديد من المنافع والخدمات والتسهيلات التي لا يمكن لعاقل أن يشكك في مدى جدواها للأفراد والأمم على السواء، فقد جلبت لنا نفس التكنولوجيا أيضاً العديد من الأبعاد الجديدة للجرائم والمسميات التي لم يكن يألفها من عاشوا قبلنا، بل لم يكن يتخيل أحد أن تصل الحرفية والقدرة على ارتكاب الجرائم إلى هذا الحد من استخدام التكنولوجيا التي يتغنى بها العالم على أنها أهم منجزاته وأنها ما جُعلت إلا لراحته وتحقيق أعلى معدلات الأمن والأمان له ولاستثماراته ورفاهيته.

فقد أصبح من الممكن، ولن نبالغ إن قلنا من السهل، إرتكاب جرائم مثل الإختلاس والسرقة أو جرائم التزوير عن بعد باستخدام التكنولوجيا، وأصحبت وسائل الأمان والحماية المحسوسة وصناديق الحفظ وأماكن التخزين لا تكفي وحدها لتحقيق الأمان المنشود لحماية المعلومات من لصوصها، وقد ظهر حديثاً مصطلحات مثل (Cybercrime) والذي يعني النوع الجديد من الجرائم التي يتم ارتكابها بواسطة الحواسيب وشبكات المعلومات، بل لقد وصل الأمر إلى إطلاق الحكومة الأمريكية في فبراير 2003 مبادرة خاصة تهتم بحماية المجال المعلوماتي والتي أطلقت عليها (Cyberspace)، وقد بدأت العديد من الدول المقدمة في السير في نفس الاتجاه في سبيل إيجاد الحلول التي تعمل على الحد من ظاهرة الجرائم الإلكترونية Cybercrimes.

**ومن هنا يمكن القول** أن جرائم المعلومات هي "تعبير شامل يشير إلى جريمة تتعلق باستخدام إحدي وسائل تكنولوجيا المعلومات والاتصالات بغرض خداع الآخرين أوتضليلهم، أومن أجل تحقيق هدف معين أوتربح".

**تصنيف جرائم المعلومات**

يمكننا تصنيف الجرائم التي تتم عن طريق استخدام تكنولوجيا المعلومات إلى عدة أقسام وكل قسم يختص بنوع معين من الجرائم التي يمكن ارتكابها وهي كالتالي:-

1. **جرائم تهدف لنشر معلومات**. في مثل هذا النوع يتم نشر معلومات سرية تم الحصول عليها بطرق غير مشروعة عن طريق الاختراقات لشبكات المعلومات ونشر هذه المعلومات على الملأ، ومن أمثلة ذلك نشر معلومات بطاقات الإئتمان البنكية، وأرقام الحسابات المصرفية، وأيضاً نشر المعلومات الاستخباراتية المتعلقة بدول أو أشخاص كما حدث في اختراق وكالة المخابرات الأمريكية CIA.
2. **جرائم تهدف لترويج الإشاعات**. وهنا يتم نشر معلومات مغلوطة وغير صحيحة تتعلق بالأشخاص أو المعتقدات أو الدول بهدف تكدير السلم العام في البلدان، وكذلك نشر الإشاعات عن بعض الأشياء وإحداث البلبلة في المجتمعات.
3. **جرائم التزوير الإلكترونية**. وهنا يتم استخدام وسائل التكنولوجيا في عمليات التزوير بغرض تحقيق هدف معين، مثل تزوير البطاقات الإئتمانية وجوازات السفر وغيرها من الأوراق الرسمية والثبوتية التي يمكن تزويرها باستخدام وسائل تكنولوجية متقدمة، وكذلك يندرج تحتها عمليات التحويل المصرفي الوهمية من حسابات إلى أخرى عن طريق اختراق شبكات المصارف.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 30، ديسمبر 2012

4. **جرائم تقنية المعلومات**. وأهم مثال لها هو عمليات القرصنة التي تحدث للبرامج الحاسوبية الأصلية والتي يتم عمل نسخ منها لتباع في الأسواق بدلاً من النسخ الأصلية، مثل برامج التشغيل أو البرامج التطبيقية غالية الثمن، والتي يتم تقليدها عن طريق قراصنة محترفين في هذا المجال.



**شكل رقم (1) صور لموقع وكالة الاستخبارات الأمريكية قبل وبعد الاختراق**

**مكونات أمن شبكات المعلومات.**

عندما نتحدث عن موضوع "أمن المعلومات" وشبكات المعلومات فإن أول ما يتبادر إلى الذهن هو كيفية الحفاظ على سرية المعلومات، وعند ذكر جرائم المعلومات نعني بها أنه قد تم تسريب لهذه المعلومات بما يعني أنه قد حدث انتهاك لهذه السرية، فما هي يا ترى مكونات هذا النظام الذي نطلق عليه أمن المعلومات أو أمن شبكات المعلومات.

يرى المختصون أن أمن المعلومات هو عملية ليست بالبسيطة وإنما هي عملية معقدة تتألف من مكونات ثلاثة كلهم على نفس الدرجة من الأهمية والخطورة وهذه المكونات هي:-

**أولاً: سرية المعلومات** Data Confidentiality

وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها: المعلومات الشخصية للأفراد، الميزانية المالية للشركات قبل إعلانها، المعلومات والبيانات العسكرية الخاصة بالجيوش والمواقع العسكرية في البلاد.

**ثانياً: سلامة المعلومات** Data Integrity

في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من 100 إلى 1000000 وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال.

**ثالثاً: ضمان الوصول إلى المعلومات** Availability

لعله من المنطقي أن نعرف ان كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات

العدد 30، ديسمبر 2012

---

**دوافع الهجوم على شبكات المعلومات**

يمكن أن يتبادر إلى الذهن سؤال وهو لماذا يقوم المخربون أو المخترقون بعمليات مثل اختراق شبكات المعلومات وتهديد أمن المعلومات؟ وما هي الدوافع التي يمكن أن تكون لديهم لكي يقوموا بمثل هذه الأعمال؟ فلابد لكل شخص من دوافع للقيام بعمل ما، وهنا سنتعرف على بعض الدوافع التي رصدها المختصون بمراقبة عمليات الاختراق وجرائم المعلومات لدى القائمون بهذه الهجمات.

**أولاً: وجود الدافع**

إن القاتل حين يقتل القتيل يكون لديه دافع معين سواء كان الإنتقام أو السرقة أو حتى دافع مرضي، وبالتالي فالقائمون بعمل الهجمات والاختراقات لشبكات المعلومات لابد لهم من دافع حتى يقوموا بهذه العمليات، وخاصة أنها تكلفهم جهداً ذهنياً وفكرياً وحتى مالياً كبيراً في بعض الأحيان، وقد يكون هذا الدافع الحصول على الأموال أو التخريب المتعمد أو حتى مجرد إثبات قدرات المخترق وأن يثبت قدرته على اختراق موقع معين كنوع من التحدي التقني.

وفي بعض الحالات يكون الوضع له دوافع سياسية كما حدث مع موقع قناة الجزيرة في عام 2003 إبان الغزو الأمريكي للعراق[7]، حيث ظن المهاجمين أن القناة تقف في صف العراق ضد الأمريكان فقام مخربون بالهجوم على الموقع الإنجليزي للقناة واختراقه وكان المشاهد يرى على الصفحة علم أمريكا فقط وتحته بعض العبارات التي تؤيد الغزو الأمريكي للعراق كما في الشكل رقم (5) ومن هنا يتضح التباين في دوافع من يقوم بمثل هذه الهجمات على شبكات المعلومات، حيث تتعدد ما بين الشخصية والمالية والنفسية وحتى السياسية بين الدول وبعضها البعض والإنتماءات الفكرية والعقائدية والسياسية للأفراد والدول.

[7] محمد عبد الله القحطاني. مصدر سابق.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 30، ديسمبر 2012

---


**شكل رقم (2) لموقع قناة الجزيرة الإخبارية أثناء تعرضه للاختراق من قبل بعض المخربين**

**ثانياً: وجود الخطة Plan**

ونعني هنا بالخطة أي وجود خطة لتنفيذ علمية الهجوم واختراق الموقع المراد تدميره، فالمهاجم لن يتمكن من تنفيذ أهدافه بدون وجود خطة محكمة تتيح له شن هجماته على الموقع واختراقه وتنفيذ ما يريد.

**ثالثاً: وجود الثغرات Vulnerabilities**

ونقصد هنا بالثغرات أي نقاط الضعف الموجودة في نظام المعلومات ككل أو في شبكة المعلومات أو الأجهزة التي تعمل ضمن الشبكة أو حتى البرمجيات التي يتم إتاحتها على شبكة المعلومات، ويمكن أن تكون هذه الثغرات في تصميم شبكة المعلومات Network Design أو في تهيئة الشبكة Network Configuration أو البرمجيات Software أو قواعد البيانات Data Bases التي تحتويها الشبكة، ومن خلال هذه الثغرات أونقاط الضعف يمكن للمهاجمين أن يخترقوا شبكات المعلومات ويحدثوا فيها الأضرار أو حتى الاستيلاء على ما يريدوا منها، وعلى مدير النظام ومديروا الشبكة أن يقوموا بعمليات فحص باستمرار لشبكة المعلومات لكي يقفوا على أي نقاط ضعف أو ثغرات يمكن أن تحدث ويعملوا على الفور على معالجها وسد هذه الثغرات تجنباً لاكتشافها من قبل بعض العابثين.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 30، ديسمبر 2012

---

**مصادر الخطر على شبكات المعلومات**

بعد كل ما سبق الحديث عنه من الأخطار التي تواجه شبكات المعلومات وانظمة الحماية بها، نود هنا أن نورد المصادر التي يمكن من خلالها تشكيل تهديد أو اختراقات لشبكات المعلومات.

**أولاً: الخطر الداخلي Internal**

يقصد بالخطر الداخلي المهاجمون من داخل نطاق عمل شبكة المعلومات، وهم الأفراد أو العاملون الذين ينتمون لنفس الجهة المستهدفة، ولعل هذا النوع من الخطر هو أشد فتكاً وخطورة من خطر الأعداء الخارجيون، ويمثل ذلك التهديد الأكبر للمؤسسات سواء كانت شركات أو هيئات حكومية أو حتى الحكومات نفسها، فخطر انتهاك الخصوصية من الداخل سهل الحدوث وصعب الكشف عنه في حالات كثيرة، وخصوصاً إذا الشخص المهاجم يمتلك صلاحية الولوج إلى نظام شبكات المعلومات فلا يواجه أي صعوبة في عمليات الأمان والسرية الموجودة على الشبكة بل ويمكنه طمس معالم الهجوم ويمحو آثار أي دخول بسهولة، ويمكن إيجاز أهم جوانب الأخطار الداخلية فيما يلي:-

أ. اختراق الشبكات الداخلية للمؤسسات.

ب. اختراق نظم المعلومات بالسرقة أوالتبديل أوالتغيير أو الحذف.

ت. إيجاد وتهيئة ثغرات في النظام الأمني للشبكات.

ث. تغيير تهيئة نظام شبكات المعلومات.

وقد أظهر تقرير صدر في الولايات المتحدة الأمريكية عام 2003 أن 36% من الجهات تعتبر أن المستخدمين الداخليين هم أشد خطراً على أنظمة المعلومات المتاحة داخل هذه المؤسسات من الخطر الخارجي[8].

ولكن ولأسباب إعلامية والحفاظ على هيبة الشركات والمؤسسات فإن معظمها تركز سياساتها على عمليات تأمين شبكات المعلومات فيها من الأخطار الخارجية دون الداخلية، وهنا يمكننا طرح تساؤل مشروع حول الدوافع التي يمكن أن تدفع أحد العاملين في مؤسسة أو حكومة ما إلى انتهاك سرية

[8] جمال محمد غيطاس. أمن المعلومات والأمن القومي. الجيزة : نهضة مصر، 2007.

المعلومات المتاحة وشن هجوم يمكن أن يضر بهذه الجهة التي يعمل بها؟ ونجد الإجابة على ذلك في النقاط التالية:-

1- **حالات عدم الرضا**. فكثيراً ما توضح تحقيقات حالات الاختراق الأمني الداخلي لشبكات المعلومات عن أن السبب كان هو وجود حالة من عدم الرضا عند من قام بالعمل تجاه الجهة التي يعمل بها، سواء كانت هذه الحالة عدم الرضا المادي أو الوظيفي أو الإنتقام من مدير أو ما إلى ذلك من أسباب شخصية.

2- **إثبات الذات**. أحياناً ما ينتاب العاملون في حقول المعلومات بعض لحظات الأنانية التي يشعر فيها الفرد بحاجته لإثبات قدرته على اختراق الحواجز وإنتهاك خصوصية الشبكة، أو الوصول إلى قواعد بيانات محمية بجدران سرية، وما إلى ذلك لمجرد أن يرضي غروره أنه قادر على التحدي، أو الشهرة كما يحدث في حالات كثيرة من اختراق الهاكرز للمواقع الحكومية في كافة أنحاء العالم، وقد ساعد انتشار برامج كسر الحماية والاختراق الكثير على محاولة تنفيذ هجمات لخرق الشبكات.

3- **الاستفادة المادية**. قد يكون الإختراق في حالات مدفوع الأجر من جهات منافسة بغرض الضرر أو إلحاق الهزيمة أو سرقة معلومات أو ما إلى ذلك، فتقوم بعض الشركات والمؤسسات برشوة بعض الأشخاص بغرض تسريب المعلومات واختراق شبكات المعلومات نظير مبالغ مالية.

**ثانياً**: **الخطر الخارجي** External

يقصد بالخطر الخارجي بالطبع هم الأشخاص الذين يقومون بمحاولات الاختراق لأمن الشكبات من خارج المؤسسات، سواء كانوا على صلة بهذه المؤسسات أو لا، وبالطبع نسمع كل يوم عن اختراق العديد من شبكات المعلومات من قبل بعض قراصنة الإنترنت، بل وفي بعض الأحيان تصل الأمور إلى حد اختراق المواقع الحكومية والمالية كالبنوك وغيرها من المؤسسات التي بها شبكات معلومات على درجة عالية من السرية والأمان.

ولكن في الخطر القادم من الخارج تكون درجة خطورته أقل وذلك لعدة أسباب منها أنه من المتوقع أصلاً أن تكون هناك هجمات خارجية وبالتالي فإن أي شبكة لابد وأن تكون مزودة بنظم

وبروتوكولات الحماية التي تعمل على صد المهاجمين ومحاولات الاختراق الأمني لها من قبل العابثين، كما أن بناء الشبكات الآن أصبح على درجة عالية من الحرفية والدقة بحيث أصبح القائمون على بناء وتركيب الشبكات على دراية بكافة أنواع الهجمات والاختراقات التي يتبعها المخترقون بل ويقومون بدراستها بدقة لعمل الحلول السريعة لها والحيلولة دون وقوعها.

**ثالثاً: خطر التشويش**

ويقصد بذلك العوامل التي تؤثر على إرسال واستقبال البيانات والمعلومات عن طريق شبكات المعلومات، فقد تتعرض المعلومات إلى نوع من التشويش في الإرسال والإستقبال عن طريق بعض المعدات أو البرامج التي تعمل على ذلك، وفي بعض الأحوال يكون هذا التشويش غير مقصود أي أنه يكون ناتجاً عن بعض العوامل والظروف الطبيعية كظروف الطقس والمناخ التي تؤثر على أبراج الإرسال والاستقبال وخاصة في الشبكات التي تعتمد على الألياف الضوئية ونظم الاتصالات اللاسلكية، وفي أحيانٍ أخرى يكون "التشويش" ناتج عن عمل متعمد ومقصود من جهات معينة، فقد يكون هناك من يترصد المعلومات عبر الشبكات ومن يقوم بعمليات التشويش عليها بواسطة إشارات تماثل نفس نطاقات التردد المستخدمة في عمليات الإرسال عن طريق الشبكة الأم.[9]

**رابعاً: خطر سوء التصميم**

في بعض الأحيان يكون هناك بعض الأخطاء الفنية في تصميم الشبكات أو الأنظمة التي تعمل عليها هذه الشبكات، ومع أن مثل هذه الأخطاء قليلة وأيضاًغير مقصودة إلا أنها تعد خطراً يهدد أمن وسلامة شبكة المعلومات لأنها لا تؤثر على بنيتها ووأدئها الوظيفي فحسب، ولكنها أيضاً يمكن أن تكون منفذاً سهلاً لعمليات الاختراق الأمني من قبل مخربي الشبكات، وتكون هذه الأخطاء غير المقصودة هي نقطة الضعف في شبكة المعلومات والتي يمكن من خلالها تهديد أمن وسلامة المعلومات.

[9] محمد محمد أمان. تكنولوجيا المعلومات في المكتبات ومراكز المعلومات /محمد محمد أمان، ياسر يوسف عبد المعطي. – الكويت : مكتبة الفلاح، 2004.

**خامساً: خطر سوء الاستخدام**

العامل البشري هام جداً حتى في الشبكات، وكلما كان العنصر البشري مدرباً ومؤهلاً بالشكل العلمي والقدر الكافي كان ذلك أحد أسباب حماية شبكات المعلومات، فهناك بعض الأخطاء التي تنتج عن سوء استخدام الأفراد لشبكات المعلومات تلحق بالضرر البالغ على أمن وسلامة البيانات داخل الشبكة، وسواء كان هذا الإهمال وسوء الاستخدام متعمداً أو غير متعمد فإنه في النهاية يؤدي إلى النتيجة نفسها، بحيث يمكن أن يكون نافذة إلى إحداث ثقوب في جدر الحماية الخاصة بالشبكات[10].

**سادساً: خطر الكوارث الطبيعية**

شبكات المعلومات هي جزء العالم الذي نعيش فيه تتأثر بما تتأثر به الأشياء الأخرى ومن ضمن ما يمكن أن يكون خطراً على الشبكات وبنيتها هي الكوارث الطبيعية التي يمكن أن تقع دون سابق إنذار ودون أي تدخل بشري، مثل الزلازل والبراكين والإنفجارات والحرائق وغيرها، ولذا يجب الاحتياط وعمل النسخ الاحتياطية Backup بشكل منتظم لمحتويات الشبكة وتكون هذه النسخ الاحتياطية في أماكن بعيدة عن المكان الرئيسي للشبكة الأم حتى يمكن حماية المعلومات واسترجاعها في حالة حدوث أي نوع من هذه الكوارث للشبكة نفسها.

**سابعاً: الدخلاء Hackers**

الهاكر هو الشخص الذي يقوم بإنشاء وتعديل البرمجيات والعتاد الحاسوبي، وقد أصبح هذا المصطلح ذا مغزى سلبي حيث صار يطلق على الشخص الذي يقوم باستغلال النظام من خلال الحصول على دخول غير مصرح به للأنظمة والقيام بعمليات غير مرغوب فيها وغير مشروعة، غير أن هذا المصطلح (هاكر) يمكن أن يطلق على الشخص الذي يستخدم مهاراته لتطوير برمجيات الكمبيوتر وإدارة

[10] مشبب القحطاني. أمن شبكات المعلومات / مشبب القحطاني، صالح العنزي. متوفر على الرابط:
http://www.alasmari.com/files/communicationtopics/Proj428.pdf تمت زيارته في 2011/12/18.

أنظمة الحاسوب وما يتعلق بأمن نظم المعلومات، واطلقت كلمة هاكر أساساً على مجموعة من المبرمجين الأذكياء الذين كانوا يتحدوا الأنظمة المختلفة ويحاولوا اقتحامها، وليس بالضرورة أن تكون في نيتهم ارتكاب جريمة أو حتى جنحة، ولكن نجاحهم في الاختراق يعتبر نجاحاً لقدراتهم ومهارتهم. إلا أن القانون اعتبرهم دخلاء تمكنوا من دخول مكان افتراضي لا يجب أن يكونوا فيه[11].

**ثامناً: الفيروسات Viruses**

فيروس الحاسوب هو برنامج خارجي صُنع عمداً بغرض تغيير خصائص الملفات التي يصيبها لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات. أي أن فيروسات الكومبيوتر هي برامج تتم كتابتها بواسطة مبرمجين محترفين بغرض إلحاق الضرر بكومبيوتر آخر، أو السيطرة عليه أو سرقة بيانات مهمة، وتتم كتابتها بطريقة معينة[12].

وتعد فيروسات الحاسوب من المشاكل الأكثر شيوعاً في أمن المعلومات والشبكات، والفيروس هو أحد البرامج الخبيثة أو المتطفلة، والبرامج المتطفلة الأخرى تسمى الديدان أو أحصنة طروادة أو برامج الدعاية أو برامج التجسس، يمكن للبرامج الخبيثة أن تكون فقط للإزعاج من خلال التأثير على استخدامات الكمبيوتر وتبطئيه وتتسبب في حدوث انقطاعات وأعطال في أوقات منتظمة وتؤثر على البرامج والوثائق المختلفة التي قد يرغب المستخدم في الدخول إليها، أما البرامج الخبيثة الأكثر خطورة فيمكن أن تصبح مشكلة أمنية من خلال الحصول على معلوماتك الشخصية من رسائلك الإلكترونية والبيانات الأخرى المخزنة في جهازك عبر شبكة المعلومات.

[11] هاكر. ويكيبيديا. متاح على الرابط: http://ar.wikipedia.org/wiki/%D9%87%D8%A7%D9%83%D8%B1 . تمت زيارته في 2011/12/20.

[12] فيروس. ويكيبيديا. متاح على الرابط. http://ar.wikipedia.org/wiki/%D9%81%D9%8A%D8%B1%D9%88%D8%B3_%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D9%88%D8%A8 . تمت زيارته في 2011/12/20.

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة متخصصة في مجال المكتبات والمعلومات
العدد 30، ديسمبر 2012

---

**حماية شبكات المعلومات Network Protection**

"**الوقاية خير من العلاج**" .. فيما سبق تم استعراض أهم المخاطر التي تواجه شبكات المعلومات وتحول دون حماية المعلومات في داخلها، ورأينا أنها تنقسم إلى عدة أقسام منها ما يمكن التحكم فيه ومنها ما يحدث دون تدخل من الإنسان، والسؤال الآن الذي يمكن طرحه هو هل يمكن تفادي هذه المخاطر والأضرار؟ وما هي الوسائل التي يمكن عن طريقها تجنب حدوث مثل هذه المشاكل والاختراقات في شبكات المعلومات التي تخصنا؟ وهذا ما سنناقشه في الفقرات التالية.

**أولاً: كلمات المرور Pass Words**

لكل بيت مفتاح .. هكذا هي فكرة عمل كلمة المرور، فبدونها لا يمكن لأي شخص غير مخول بالدخول على شبكة المعلومات، وهي جواز مرور المستخدم إلى الشبكة، فكلمة المرور تثبت للشبكة بأنك أنت الشخص المخول للدخول إليها، وهي أبسط أنواع حماية المعلومات على شبكة المعلومات فهي تعمل على حماية معلوماتك الشخصية ومعلومات العمل الخاصة بك وسجلاتك الشخصية، وغيرها من البيانات، كما أنها في بعض الأحيان تكون حماية للأفعال مثل كلمة السر في المشتريات والحسابات البنكية وغيرها.
ومن أهمية كلمة المرور يجب علينا أن نحرص عليها وعند اختيارها يجب مراعاة ثلاثة أمور هي:-

- اختيار كلمة مرور صعبة ولا يسهل تخمينها.
- عدم إطلاع الغير عليها.
- تغييرها بشكل دوري.
- لا تجعل كلمة المرور كلمة واحدة مثل ragab.
- لا تضمن كلمة المرور بيانات شخصية عنك مثل تاريخ الميلاد.
- لا ينبغي أن تقل كلمة المرور عن عشرة خانات.
- اجعل كلمة المرور خليط بين الحروف والأرقام.

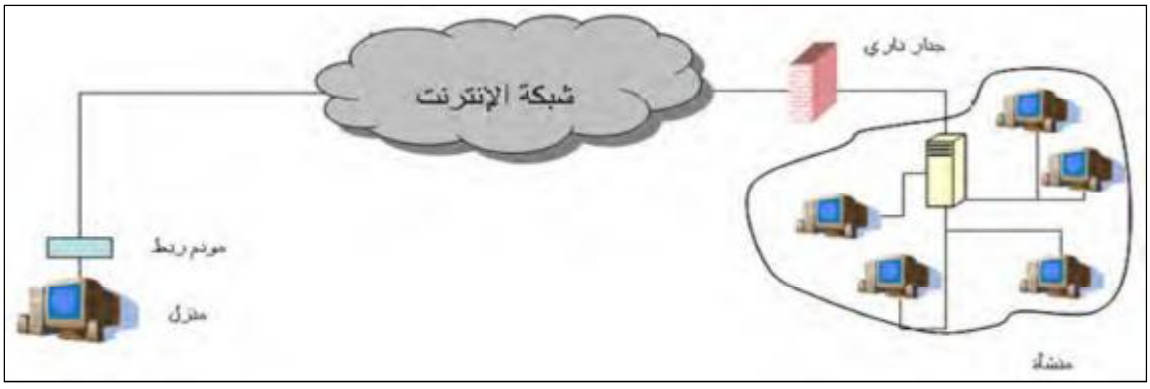

**شكل رقم (3) يوضح اسم المستخدم وكلمة المرور**

**ثانياً: جدران الحماية** Firewalls

يكون جدار الحماية الناري إما برنامجاً أو جهازاً يستخدم لحماية الشبكة والخادم من المتسللين، وتختلف جدران الحماية حسب احتياجات المستخدم، فإذا استدعت الحاجة إلى وضع جدار الحماية على عقدة منفردة عاملة على شبكة واحدة فإن جدار الحماية الشخصي هو الخيار المناسب، وفي حالة وجود حركة مرور داخلة وخارجة من عدد من الشبكات، فيتم استخدام مصافي لجدار الحماية في الشبكة لتصفية جميع الحركة المرورية، علماً بأن الكثير من الشبكات والخوادم تأتي مع نظام جدار حماية افتراضي، ولكن ينبغي التأكد فيما إذا كان يقوم بعمل تصفية فعالة لجميع الأشياء التي تحتاج إليها، فإن لم يكن قادراً على ذلك، فينبغي شراء جدار حماية ناري أقوى منه.

وفي بعض الأحيان تقوم بعض شبكات المعلومات بوضع جدران حماية لعزل شبكتها الداخلية عن شبكة الإنترنت، ولا يكون هذا العزل كلياً بالطبع حتى يمكن للمستخدمين الاستفادة من بعض خدمات الإنترنت وفي نفس الوقت منع المخربين من الدخول إلى الشبكة الداخلية أو اختراق أمن وسرية المعلومات على الشبكة.

---




**شكل رقم (4) يوضح وضع جدار الحماية Firewall**

وتعمل جدران الحماية بطرق متعددة معتمدة على نوع جدار الحماية والشبكة التي تعمل على حمايتها تبعاً لسياسة المؤسسة، ومن أهم هذه الطرق ما يلي:-

- § أسلوب غربلة مظاريف البيانات المرسلة Packet Faltering.
- § غربلة المظاريف مع تغيير عناووين المظاريف القادمة من الشبكة الداخلية.
- § أسلوب مراقبة السياق Stateful Inspection.

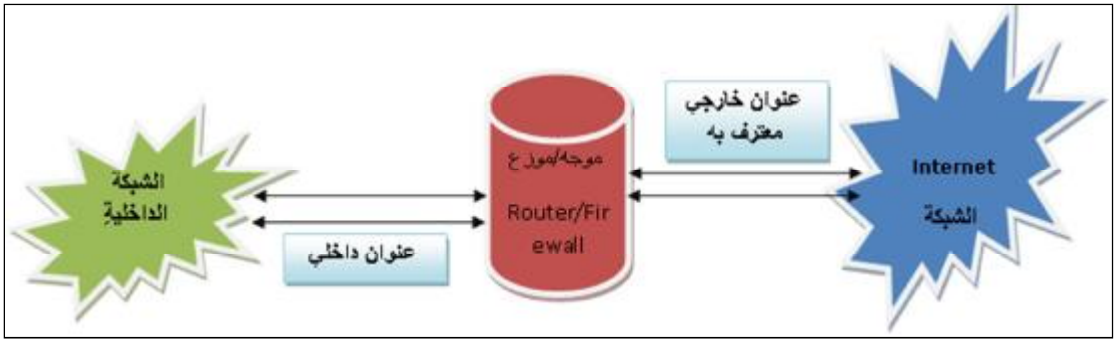
وبالطبع فإن هناك العديد من أنواع جدران الحماية التي تلائم كافة أنواع شبكات المعلومات وفقاً لحجم الشبكة والمؤسسة التي تعمل عليها، فهناك جدران الحماية التي تكون للمؤسسات الحكومية والشركات الكبيرة ذات سرعات وقدرات عالية جداً، مثل ما توفره شركة Sisco، كما أن هناك جدران حماية للمنشآت الصغيرة والشركات المحدودة، وهناك أيضاً برامج جدران الحماية التي يتم تحميلها على الحواسيب الشخصية لحماية الجهاز فقط.

**ثالثاً: تحويل العناووين الرقمية** Network Address Translation[13]

تقنية NAT تعتمد على إعطاء كل حاسوب متصل بالشبكة رقم مميز يختلف عن باقي الأجهزة، وتقوم منظمة (Internet Assigned Numbers Authority IANA) بإعطاء هذه الأرقام ولا يكون معترفاً بها إلا عن طريقها، ونظراً لقلة هذه الأرقام فإنه يعطى رقم واحد للشبكة ثم تقوم هذه الشبكة

[13] Network Address Translation. Wikipedia. Available on http://en.wikipedia.org/wiki/Network_address_translation . Visited on 20/12/2011.

بإعطاء أرقام داخلية للحواسيب المتربطة بها بحيث لا يتكرر أي رقم، وعندما يرغب جهاز حاسوب من الشبكة الداخلية في الاتصال بشبكة خارجية يأتي هنا دور تقنية NAT حيث نقوم بتنصيب جهاز حاسوب يلعب دور الوسيط بين الشبكة الداخلية والشبكة الخارجية ويحمل الرقم المعترف به المُعطى من قبل IANA للشبكة الأم، ويكون مهمته تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي معترف به من قبل IANA ومن ثم يقوم بإرسال المعلومات من الشبكة الداخلية إلى الشبكة الخارجية، وكذلك في استقبال المعلومات من الخارج يقوم بعكس الوظيفة وإرسال المعلومات إلى رقم الجهاز في الشبكة الداخلية، وغالباً ما يكون هذا الجهاز الوسيط الذي يقوم بتطبيق تقنية NAT إما جدار حماية ناري Firewall أو موزع Router.



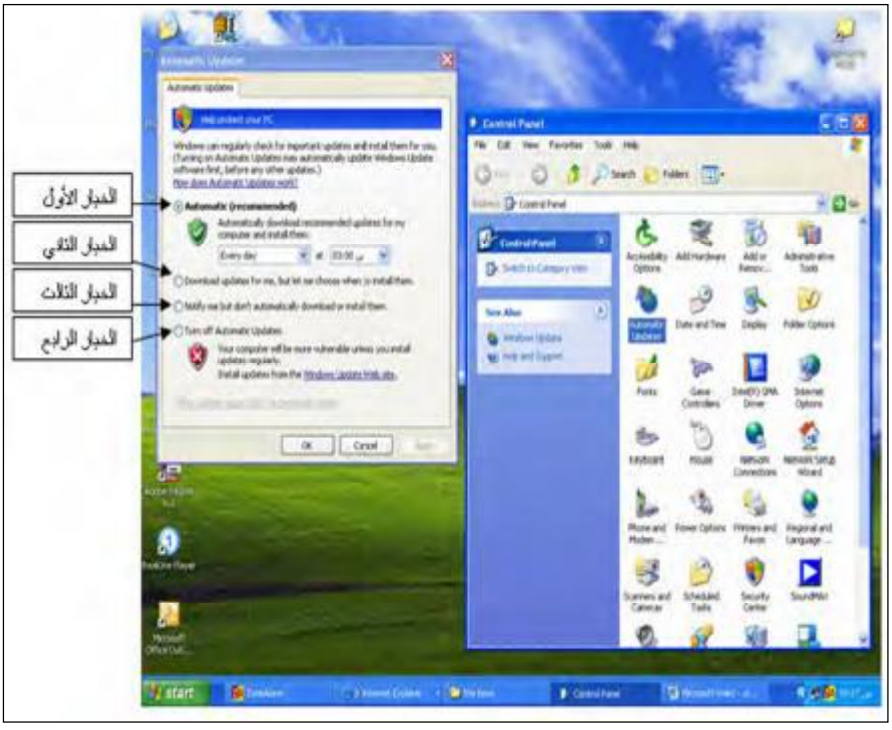

**شكل رقم (5) يوضح تقنية عمل NAT**

وفي هذه الحالة يقوم الجهاز الذي يعمل بتقنية NAT على أنه جدار حماية ناري بين أجهزة الشبكة الداخلية وأجهزة الشبكات الخارجية الأخرى، فلا يستطيع مستخدمو أجهزة الشبكات الخارجية معرفة العناوين الرقمية لأجهزة الحاسوب في الشبكة الداخلية مما يحد من عمليات الاختراق التي تعتمد على معرفة رقم IP للأجهزة.

### رابعاً: التحديث التلقائي Automatic Update

يعد التحديث الدائم والتلقائي للبرامج وأنظمة التشغيل من أهم نقاط حماية أمن شبكات المعلومات، ذلك أن عملية بناء هذه النظم هي غاية في التعقيد ولا تخلو من بعض الأخطاء التي تحدث في فترات البناء وتعمل الشركات عادة على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البرامج والأنظمة، وهذه التحسينات تتاح دائماً فيما يعرف بالتحديثات، ومن تاتي أهمية أن يقوم الشخص بعمليات التحديث

الدائم للبرامج والأنظمة التي يتبناها في جهازه الشخصي على المستوى الفردي وعلى مستوى البرامج والأجهزة المستخدمة في شبكات المعلومات، ونظراً لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فإن معظم الشركات المصنعة لهذه البرامج قامت بإضافة خاصية التحديث الآلي والتلقائي لهذه البرامج، ولكي تعمل هذه الخاصية يقوم البرنامج المثبت في الشبكة بالاتصال تلقائياً وعلى فترات معينة بالشركة المنتجة له والقيام بالبحث عن آية تحديثات جديدة وتنزيلها تلقائياً.




**شكل رقم (6) يوضح خيارات التحديث التلقائي**

**خامساً: التشفير** Encryption

التشفير هو ترميز البيانات كي يتعذر قراءتها من أي شخص ليس لديه كلمة مرور لفك شفرة تلك البيانات. ويقوم التشفير بمعالجة البيانات باستخدام عمليات رياضية غير قابلة للعكس. ويجعل التشفير المعلومات في جهازك غير قابلة للقراءة من قبل أي شخص يستطيع أن يتسلل خلسة إلى جهازك دون إذن.

عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة، أو تحويلها إلى رموز غير ذات معنى؛ حيث عندما تصل إلى أشخاص آخرين لا يستطيعون فهمها أو الإستفادة منها، لذا فهي عبارة عن تشفير وتحويل للنصوص العادية الواضحة إلى نصوص مشفرة وغير مفهومة، وتبنى على أساس أن كل معلومة تحتاج لفكها وإعادتها إلى الوضع الأصلي شفرة.[14]

ويستخدم مفاتيح تشفير Encryption النصوص المرسلة وفك الشفرة من قبل صاحبها والمسموح له بتسلمها، وتستند هذه المفاتيح إلى صيغ رياضية معقدة في شكل خوارزميات وتعتمد قوة وفعالية التشفير على نوعية الخوارزميات، ومازالت تلك العملية تتم بواسطة مفتاح سري يعتمد لتشفير النصوص وفي نفس الوقت لفك تشفيرها وترجمتها إلى وضعها الأصلي باستخدام نفس المفتاح السري، وهو ما يعرف بالتشفير المتناظر Symmetric، ثم جاء ما يعرف بالتشفير اللامتناظر Asymmetric حلا لمشكلة التوزيع الغير أمن للمفاتيح في عملية التشفير المتناظر معوضاً عن استخدام مفتاح واحد باستخدام مفتاحين اثنين مرتبطين بعلاقة رياضية عند بنائهما، وهما مفتاحان الأول: المفتاح العام؛ والثاني: المفتاح الخاص[15]


**شكل رقم (7) يوضح عملية التشفير**

14 أحمد عبد الله مصطفى. حقوق الملكية الفكرية والتأليف في بيئة الإنترنت. - Cybrarian Journal .- ع 21، ديسمبر 2009 .- متوفرة على الرابط. http://journal.cybrarians.info/index.php?option=com_content&view=article&id=487:2011-08-13-20-29-19&catid=144:2009-05-20-09-53-29&Itemid=62 . تمت زيارته في 2011/12/20.

(15) جنان صادق عبدالرازق. استخدام التكنولوجيا في الحفاظ على أمن المعلومات.- العربية 3000.- س 8، ع 33 (2008).

**سادساً: التخزين الاحتياطي** Backup

النسخ الاحتياطي Backup هو عمل نسخ احتياطية من محتويات الحواسيب أو شبكات المعلومات وحفظ هذه النسخ الاحتياطية في مكان آمن بعيد، بحيث يمكن الرجوع إليها في حالة حدوث أعطال أو حوادث وكوراث للشبكة وتدميرها لأي سبب كان، وعادةً ما يتم أخذ هذه النسخ بشكل دوري وفق النظام المتبع على الشبكة أسبوعياً أو شهرياً أو حتى يومياً، كما أنه في أغلب الأحوال يتم أخذ هذه النسخ بطريقة آلية من النظام نفسه في وقت محدد.

وتعد هذه الطريقة من أهم وأسهل الطرق التي يمكن من خلالها الحفاظ على سلامة المعلومات الخاصة بشبكات المعلومات وخاصة في حالة التدمير الكامل للشبكة أو اختراقها بهدف محو وتدمير البيانات والمعلومات المتاحة عليها، وتكون في هذه الحالة النسخ الإحتياطية هي الملاذ الآمن لمحتويات الشبكات، وأخذ النسخ الاحتياطية من محتويات شبكات المعلومات تعد من أبجديات الأمن والسلامة للمعلومات والشبكات أي أنها من بديهيات العمل في مجال حفظ شبكات المعلومات. ويقدم المختصون بشبكات المعلومات والنظم عدة نصائح يجب على الفرد اتباعها عند القيام بعمل نسخ احتياطية من محتوى شبكات المعلومات وهي:-

1- حفظ النسخ الاحتياطية Backup في مكان بعيد وآمن وسري، ويفضل أن يكون المكان بعيد عن مقر الشبكة الأم أو المؤسسة المالكة للشبكة تفادياً لضياع هذه النسخ في حالة قيام الكوارث الطبيعية في نفس المكان، فيكون قد ضاعت المعلومات الأصلية والنسخ الاحتياطية أيضاً معها.
2- اختيار وسائط تخزين ذات جودة عالية تقاوم عوامل الزمن ولا تتقادم تكنولوجياً بسرعة.
3- القيام بعمليات النسخ الاحتياطي بشكل دوري وفقاً للسياسة المتبعة والإجراءات الخاصة بالمؤسسة المالكة لشبكة المعلومات، وفي كل الأحوال ينبغي ألا تزيد المدة عن شهر.

**متطلبات أمن شبكات المعلومات**

بهذا نكون قد أتينا على المخاطر التي تحيط بشبكات المعلومات والوسائل والإجراءات التي يمكن من خلالها مكافحة ومواجهة هذه المخاطر ، وقبل أن ننهي حديثنا عن أمن شبكات المعلومات والمخاطر التي تتهددها نورد بعض النصائح العامة التي يمكن وضعها في الاعتبار كوسائل احترازية يمكن تطبيقها والتي يمكن التعبير عنها بأنها من متطلبات أمن الشبكة بصفة عامة وهي كالتالي:-

1- **تحديد سياسات العمل في شبكات المعلومات،** بأن يكون واضحاً تمام الوضوح ما هو المسموح به والممنوع فيما يتعلق بأمن المعلومات على الشبكة.
2- **توفير آليات تنفيذ سياسات العمل.** بأن يكون معروفاً كيفية تنفيذ هذه السياسات وما هي العقوبات التي ستوقع في حالة المخالفة.
3- **العنصر البشري.** بأن يتولى إدارة وتشغيل شبكات المعلومات عناصر بشرية مدربة ومؤهلة للتعامل مع هذه التكنولوجيا وألا يترك المجال للهواة للعبث بمثل هذه المقدرات الثمينة وخاصة في الأماكن الحكومية والحيوية على مستوى الدول.
4- **تغيير الأوضاع الأصلية لمعدات الشبكات.** وذلك بأن يتم كل فترة تغيير الأوضاع الأصلية للمعدات Hardware والبرامج Software الخاصة بشبكات المعلومات كإجراء احترازي كل فترة لمنع الاختراقات الخارجية.
5- **المراقبة.** يجب أن يكون هناك نوع من المراقبة والمتابعة لأنشطة المعلومات على الشبكة بشكل دقيق ودائم وذلك بهدف اكتشاف أي أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة وتفادي تفاقم الأوضاع.
6- **حسن اختيار مواقع نقاط الشبكة.** فيجب أن يتم التدقيق جيداً عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية.
7- **بروتوكولات التحقق والتشفير.** يجب أن يتم تشغيل بروتوكولات التحقق من الهوية وأنظمة تشفير البيانات لتأمين المعلومات على الشبكة، وأن يتم اختيار البرامج ذات السمعة العالمية في هذا الإطار.

**الخلاصة**

تعد قضية أمن المعلومات وتبادلها عبر الشبكات من القضايا التي تشغل بال ليس فقط الباحثين والمختصين، بل المنظمات الدولية والعالم المرتبط بها أيضًا، وذلك نظرًا للأهمية الفائقة لتقنيات المعلومات في شتى مجالات الحياة في هذا العصر، ولاشك أن تزايد الاعتماد على المعلومات وشبكاتها يزيد أيضًا من تأثير الأخطار التي يمكن أن تواجهه، ولذا فلابد من تواصل عمليات السعي إلى مواجهة هذه الأخطار والاهتمام بتطوير الأساليب والوسائل التقنية اللازمة للمواجهة هذه الأخطار، إضافة إلى إيجاد أفضل القواعد الإدارية التي تساهم في دعم هذه المواجهة من أجل الحد من الأخطار المحتملة بل والسعي إلى التخلص منها إن أمكن.

**المصادر**

**أولاً المراجع العربية:**

1- أحمد عبد الله مصطفى. حقوق الملكية الفكرية والتأليف في بيئة الإنترنت. - Cybrarian Journal .- ع 21، ديسمبر 2009 .- متوفرة على الرابط التالي: http://journal.cybrarians.info/index.php?option=com_content&view=article&id=487:2011-08-13-20-29-19&catid=144:2009-05-20-09-53-29&Itemid=62 . تاريخ الزيارة 2011/12/18.

2- البريد. ويكيبيديا. متوفر على الرابط التالي: http://ar.wikipedia.org/wiki/%D8%A8%D8%B1%D9%8A%D8%AF_%D8%B9%D8%A7%D8%AF%D9%8A . تاريخ الزيارة 2011/12/19.

3- جنان صادق عبدالرازق. استخدام التكنولوجيا في الحفاظ على أمن المعلومات.- العربية 3000.- س 8، ع 33 (2008).

4- خالد بن محمد الغثير. الاصطياد الإلكتروني : الأساليب والإجراءات المضادة. – الرياض : مكتبة الملك فهد الوطنية، 2008.

5- سليمان بن صالح العقلا. إنشاء الشبكات : المبادئ الأساسية لإختصاصي المكتبات والمعلومات /سليمان بن صالح العقلا، فؤاد أحمد إسماعيل. – الرياض : مكتبة الملك فهد الوطنية، 2000.

6- شبكات الحاسوب. [د.م : د.ن.]. متوفر على الرابط التالي:
http://ar.wikipedia.org/wiki/%D8%B4%D8%A8%D9%83%D8%A9_%D8%AD%D8%A7%D8%B3%D9%88%D8%A8. تاريخ الزيارة 2011/12/20.

7- فيروس. ويكيبيديا. متاحة على الرابط التالي:
http://ar.wikipedia.org/wiki/%D9%81%D9%8A%D8%B1%D9%88%D8%B3_%D8%A7%D9%84%D8%AD%D8%A7%D8%B3%D9%88%D8%A8.
تمت زيارته في 2011/12/20.

8- محمد محمد أمان. تكنولوجيا المعلومات في المكتبات ومراكز المعلومات /محمد محمد أمان، ياسر يوسف عبد المعطي. – الكويت : مكتبة الفلاح، 2004.

9- مشبب القحطاني. أمن شبكات المعلومات / مشبب القحطاني، صالح العنزي. متوفر على الرابط: http://www.alasmari.com/files/communicationtopics/Proj428.pdf تمت زيارته في 2011/12/18. تمت زيارته في 2011/12/19.

10- نها محمود. مذكرة الشبكات. – [د.م.، د.ن].

11- هاكر. ويكيبيديا. متاح على الرابط:
http://ar.wikipedia.org/wiki/%D9%87%D8%A7%D9%83%D8%B1 . تمت زيارته في 2011/12/20.

12- يسري زكي. تبسيط أمن المعلومات والاتصالات.- (د.م. : د.ن.). متاح على الرابط.
http://yomgedid.kenanaonline.com/tags/77115/posts#http://yomgedid.kenanaonline.com/posts/113226 . تمت زيارته في 2011/12/18.

**ثانياً: المراجع الأجنبية:**

1- Ciampa, Mark. Security + guide to network security fundamentals. – Boston : Thomson Course Technology, 2005.
2- Schwarzwalder, R. (1999). Intranet Security. Database Magazine, 22(2), 58.
3- Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. Information Technology & Management, 11(1), 7-23.
**4-** Network Address Translation. Wikipedia. Available on http://en.wikipedia.org/wiki/Network_address_translation . Visited on 20/12/2011