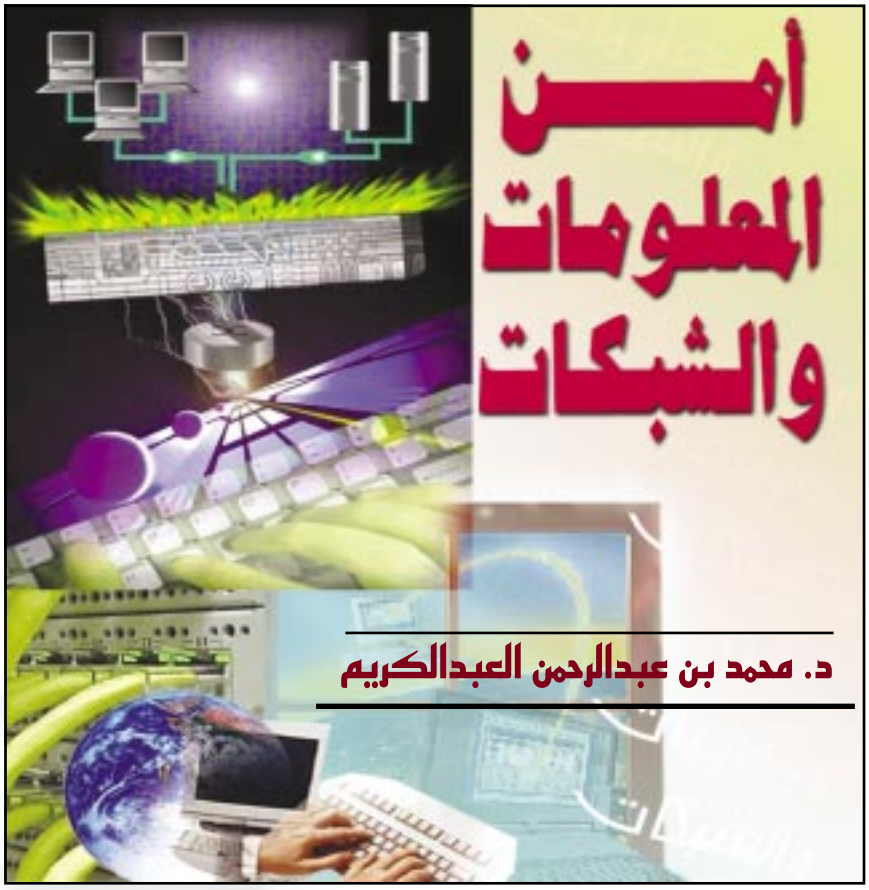


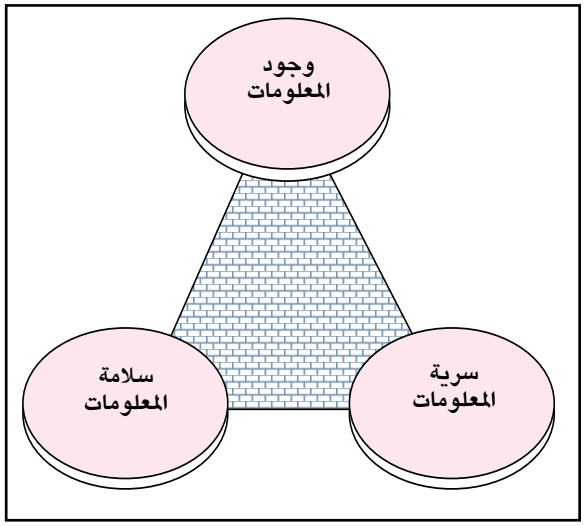
أدى تسارع التقدم التقني في مجال المعلوماتية إلى زيادة الاعتماد على هذه التقنية كوسيلة لمعالجة وحفظ البيانات والمعلومات، وبالتالي ازدادت أهمية المحافظة عليها. ومع دخولنا عصر الإنترنت - إن جاز التعبير - زادت المشاكل وحوادث السطو والسرقات المعلوماتية، حيث يتم نقل هذه البيانات عبر وسائط مختلفة قد لا نعلم عن الكثير منها. ولذا يشكِّل أمن المعلومات والشبكات هاجسا لكل من يتعامل مع الحاسب الآلي أو يخطط لاستخدامه في المستقبل.

يتفاوت الاهتمام بأمن المعلومات بحسب طبيعتها ونوعها، حيث تتدرج من معلومات عامة لا يضير نشرها إلى معلومات شديدة السرية لا يسمح بالاطلاع عليها. فعلى سبيل المثال تعد معلومات حسابات المودعين في البنوك سرية ولا يسمح بنشرها. كذلك تعد المعلومات الصحية للمريض معلومات سرية لا يسمح بالاطلاع عليها إلا للطبيب المعالج.

عناصر حفظ المعلومات

أدى التوسع المستمر في استخدام شبكة الإنترنت لنقل البيانات بين جهات عديدة وتزايد تطبيقاتها إلى طرح تساؤلات عديدة من قبل المستخدمين، مثل: هل المعلومات 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 عن طريق الإنترنت؟

وللإجابة على هذه التساؤلات وغيرها سنتناول العناصر التي يجب المحافظة عليها لكي تبقى المعلومات في أمان، والتي يوضحها الشكل (١)، وهي:



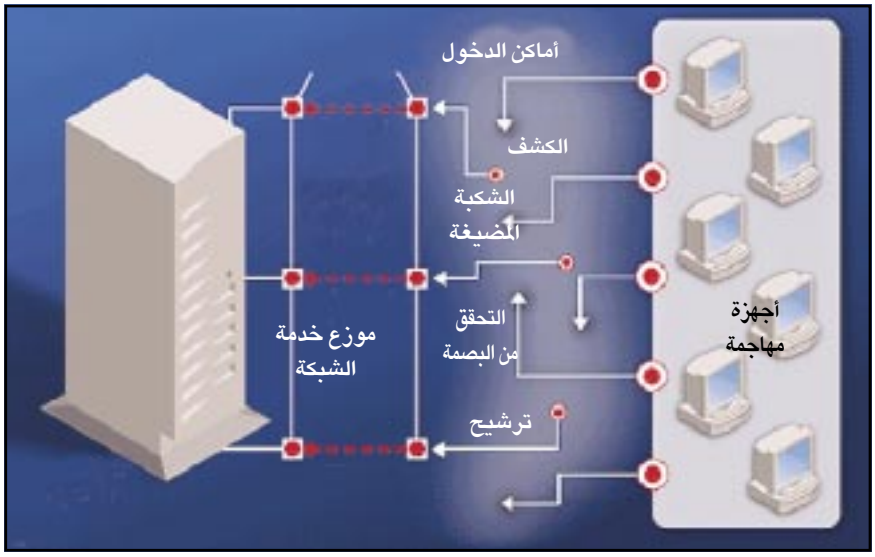
● (شكل ١) عناصر المحافظة على أمن المعلومات.

● وجود المعلومات

يقصد بوجود المعلومات (Availability) الحماية من إعاقة المصرح لهم من الوصول إلى المعلومات أو الخدمات سواء على جهاز الحاسب أو عبر الشبكة. ويمثل هذا النوع من الإعاقة ما يسمى بالإعاقة الموزعة (Distributed Denial of Service -DDoS)، شكل(٢)، حيث يعمد المهاجم أو المهاجمون إلى إغراق الضحية، سواءً كانت أفراداً أو شبكة، بالطلبات والأوامر من جهات مختلفة وموزعة مما يعيق خدمة الآخرين.

● سرية المعلومات

يقصد بسرية المعلومات (Confidentiality) المحافظة على سريتها من التطفل بأنواعه، وذلك بمنع غير المصرح لهم بالإطلاع عليها. ويشمل ذلك البيانات والمعلومات المخزنة



● شكل (٢) حماية المعلومات بواسطة الإعاقة الموزعة.

على الحاسب أو المنقولة عبر الشبكة. وفي كثير من الأحيان يمكن استراق المعلومات المنقولة عبر الإنترنت، حيث تسلك البيانات عدداً من الأجهزة الوسيطة عند انتقالها بين نقطتين.

● سلامة المعلومات

يقصد بسلامة المعلومات (Integrity) حفظها من التغيير بدون تصريح، وذلك بمنع إحداث تغييرات عليها أو مسحها من قِبل أشخاص غير مخولين. وتشمل هذه البيانات والمعلومات المخزنة على الحاسب أو المنقولة عبر الشبكة. وقد يتم التغيير أو المسح للمعلومة وهي في طور الانتقال عبر الشبكة، أو وهي مخزنة على جهاز الحاسب.

تقنيات حماية المعلومات

تفتقت أذهان الباحثين في أمن المعلومات عن عدد من التقنيات التي تساهم في تطوير وتفعيل وسائل حفظ المعلومات، وذلك بعدد من أنواع وطرق الحماية، تتمثل فيما يلي:

● جهاز الحاسب الآلي

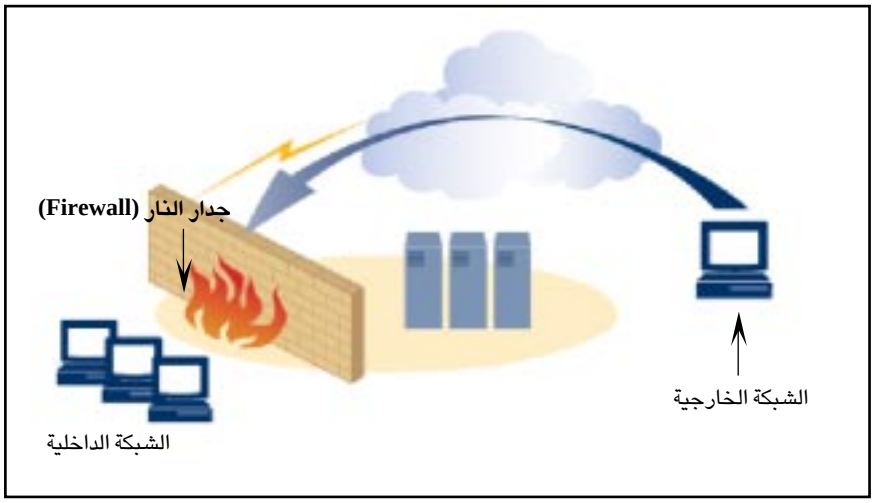
تتفاوت أجهزة الحاسب في أنواعها وأحجامها، فمنها الحاسب الشخصي، ومنها الخادم الذي يتصل به عدد من المستفيدين. ولذلك فإنه يمكن حمايتها بالأساليب التالية:

* **الحماية التقليدية:** وهي حماية أجهزة الحاسب من المتطفلين بما يسمى الحماية المحسوسة (Physical Protection)، حيث يحفظ جهاز الحاسب في مأمن من أيدي المتطفلين في غرفة مخصوصة، ويكون التحكم في دخول هذه الغرفة بحسب أهمية الجهاز والمعلومات المخزنة فيه، وذلك إما بحراسة فعلية أو بأقفال إلكترونية وغيرها. ويناسب هذا النوع من الحماية الأجهزة الخادمة، حيث يمنع الوصول إليها حسياً.

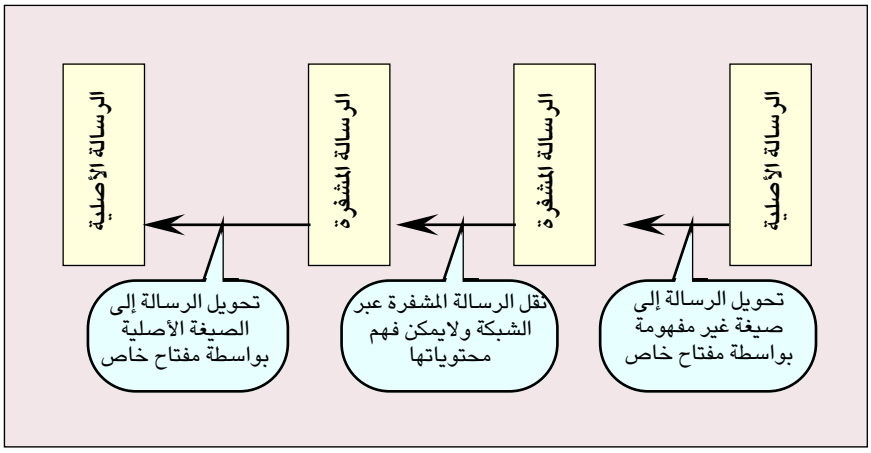
* **الحماية بكلمة سر:** وفي هذا الأسلوب من الحماية لا يمكن تشغيل الجهاز إلا بمعرفة كلمة السر، وذلك في نظم التشغيل التي توفر خاصية الدخول بكلمة السر مثل (Windows 2000) و (Linux)، أما في حالة استخدام نظم التشغيل التي لا توفر الحماية بكلمة السر فإنه يمكن استخدام كلمة تشغيل خاصة بالجهاز، وقد يستدعي الأمر حماية الجهاز بالإثنين معا.

* **غلق المنافذ:** وذلك في حالة استخدام الخوادم، حيث يستلزم وجود شبكة، لذلك فلابد من غلق جميع المنافذ (Ports) ماعدا ما هو ضروري لتقديم الخدمات. لأن ترك هذه المنافذ مفتوحة يسهل عمل المخترقين.

* **غلق الجهاز:** وهنا تبقى مشكلة جهل المستخدم، حيث أن ترك بعض المستخدمين جهازه مفتوحا عند خروجه من مكتبه لا يشكل خطرا على جهازه فقط، بل على الأجهزة الأخرى الموصولة على نفس الشبكة. ولذا يجب على المستخدم عدم ترك الجهاز مفتوحا عند مغادرة المكتب ولو لدقائق، حيث أن تحميل برنامج يحوي فيروسا على الجهاز ـ باستخدام قرص مرن ـ قد لا يستغرق أكثر من دقيقتين. ويمكن للمستخدم التقليل من عملية إيقاف التشغيل و إعادته بوضع كلمة سر لشاشة



● شكل (٣) صد الاتصالات من الشبكة الخارجية بالجدار الناري.



● شكل (٤) طريقة حماية المعلومات عن طريق التشفير.

الحفظ، ويتم غلق الجهاز عند مغادرة المكتب دون الحاجة إلى إعادة تشغيل الجهاز عند العودة إلى المكتب.

حمـــايـة الشبكـــة

تشكـــل الشبكـــات المحليـــة (Local Area Network -LAN) عنصراً مهماً في تكوين منظومة الحاسب. وتختلف طرق الحماية بحسب نوع وحجم الشبكة واتصالها بالشبكات الأخرى. وتزداد أهمية حماية الشبكة عندما تكون الشبكة المحلية موصولة بالشبكة النسيجية العالمية (الإنترنت). ويمكن حماية الشبكة المحلية باستخدام إحدى الطرق التالية:

* **جـــدار ناري (Firewall):** وهو برنامج يقوم بتصفية البيانات الداخلة للشبكة، ويحد من وصول المتطفلين. ويعمل على منع الدخول إلى الشبكة المحلية إلا عبر منافذ محددة من قبل مدير النظام (الشخص المعني بتشغيل جهاز الحاسب وإعطاء الصلاحيات للمستخدمين، وهو المسؤول عن حماية الجهاز والبرامج الموجودة عليه). كما يعمل الجدار الناري على الحد من خروج المعلومات إلا عبر المنافذ المحددة، شكل(٣)، وقد يخصص لذلك جهاز مستقل. ويمكن تشبيه هذه العملية بنقطة التفتيش عند بوابة المبنى، فهي لا تمنع دخول السيارات، ولكن تسمح بدخول المصرح لهم فقط، كما أنها قد تمنع خروج بعض السيارات التي يفترض أن لا تخرج من المبنى.

* **الشبكة التحويلية (Switched Network):** ويشكل استخدامها وسيلة مساعدة للحماية من المتنصتين، حيث تنتقل المعلومة بين جهازين دون أن يتمكن باقي الأجهزة من الإطلاع عليها.

* **كلمة السر:** ويؤدي استخدامها إلى حماية مكونات الشبكة القابلة للبرمجة، ويفوت على المتطفلين فرصة الاختراق.

* **الحماية المحسوسة:** وهي هامة لأجهزة الشبكات، حيث توضع في خزانات أوغرف خاصة لهذا الغرض تكون مغلقة في جميع الأوقات لمنع وصول المتطفلين إليها.

حمـاية المعلـومـات

إن من البدهيات في حماية المعلومات منع الوصول إليها لغير المصرح لهم، والاهتمام بتقوية هذا الجانب، وذلك من خلال ما يلي:

- وضع كلمات سر إضافية للدخول على الملفات الحساسة.
- مراجعة الصلاحيات الممنوحة للمستخدمين جيدا قبل وضعها قيد التنفيذ.
- استخدام أساليب التعمية (Encryption)، وفيها تتم عملية تعمية البيانات بتحويلها بواسطة عمليات حسابية إلى صيغة غير مفهومة، يمكن إعادتها إلى الصيغة الأصلية باستخدام رموز سرية (مفتاح) وعمليات حسابية،وتستخدم هذه الوسيلة لحماية المعلومات ذات الأهمية القصوى المخزنة على جهاز الحاسب، أوالمنقولة من خلال الشبكة. وعندما يتم تعمية البيانات بهذه الطريقة فإن المتطفلين لن يتمكنوا من الإطلاع على المعلومات، حتى وإن تمكنوا من الوصول إليها، حيث يحتاج المتطفل إلى معرفة المفتاح الذي استخدم لتعمية هذه المعلومات، شكل (٤). كما يُفضل تعمية البيانات المنقولة – وإن كانت أقل أهمية – لأن مخاطر السرقة تزداد مع عملية الانتقال عبر الشبكة. وهذا ما يتم عادة عند إرسال بعض المعلومات الشخصية عبر الشبكة مثل رقم بطاقة الإئتمان وغيرها.

وســائل الحمـايــة

يوجد عدد من الوسائل لتوفير الحماية للمعلومات أغلبها في شكل منتجات تجارية، و قد يكون للمنتج الواحد أكثر من وظيفة، و من هذه الوسائل ما يلي:-

● أدوات كشف الاختراقات

أدوات كشف الاختراقات (Intrusion Detection) عبارة عن حواجز وعوائق أمام المخترقين تعمل على منعهم أو تأخير وصولهم إلى أهدافهم، مما يعطي مدير النظام فرصة لاكتشافهم وإغلاق المنافذ التي دخلوا منها.

تساعد أدوات كشف الاختراق على مراقبة الشبكة والأجهزة الحساسة، وتنذر مدير النظام عند الاشتباه بحدوث محاولة للاختراق. و تعتمد بعض هذه الأدوات على التعرف على طراز الهجوم، لأن كل نوع

منها له سمات مميزة (Signatures)، فيتم التعرف على نوع الهجوم من خلال تطابق السمات الموجودة أصلا في برنامج كشف الاختراق والسمات التي تصل مع البيانات. بينما تعتمد أنواع أخرى من أدوات كشف الاختراق على سمات التعامل مع الحاسب، حيث يسجل لكل مستخدم سمات مميزة له، مثل: وقت الدخول للنظام والخروج منه، وطبيعة البرامج المستخدمة، وسرعة استخدامه للوحة المفاتيح. ويتم الفحص لكل مستخدم أثناء تشغيل الجهاز، وعند اكتشاف عدم التطابق يتم تحذير مدير النظام إلى وجود تصرف شاذ. وتقوم بعض تطبيقات الحماية بمراقبة ملفات النظام والملفات الحساسة بإضافة توقيع خاص لكل ملف يعتمد على مكونات الملف، بحيث يتم اكتشاف أي تعديل غير نظامي يتم بدون السماح له من مدير النظام.

● مضادات الفيروسات

تقوم مضادات الفيروسات بفحص الملفات بشكل دوري أو حسب ما يحدده المستخدم. و تبحث هذه البرامج في الملفات عن سمات الفيروسات، وتقوم بتخليص الملف منها، أو مسح الملف بحسب الحاجة. ومن المهم تحديث مضادات الفيروسات بشكل دائم. كما يوجد بعض أنواع المضادات التي تخدم المنشأة بأكملها، حيث يتم تحديث المضادات عن طريق خادم مرتبط بشبكة الإنترنت.

● جدران الحماية

يطلق عليها أيضا اسم الجدران النارية، ومنها ما هو على مستوى الشبكة كما ذكر سابقا، ومنها أنواع شخصية تمكن المستخدم من حماية جهازه بمنع تبادل المعلومات إلا ما يسمح به المستخدم.

● السياسات الأمنية

تتعاون جميع هذه الأنواع من الحماية على إعاقة المتطفلين والمخترقين، وكلما زادت الحماية كلما تأخر المخترقون لفترة أطول مما يجعل فرصة كشفهم أكبر. وتكون لدى المنشأة –عادة – سياسات أمنية تحدد أنواع الحماية المتبعة وأساليب التعامل مع الحاسب بما يحفظ أمن المعلومات. وتبقى المشكلة الكبرى في العنصر البشري، فهو المطبق لهذه السياسات وعلى عاتقه تقع الكثير من المسؤوليات من تحديث للنظم، وسد الثغرات، ومراقبة الأنظمة. وسنركز فيما يلي على العنصر البشري ودوره في أمن المعلومات.

* **العنصر البشري(الموظفون) :** ويعد العنصر الأهم في هذا الموضوع، ولذلك يجب عليهم يمختلف مستوياتهم توخي الحذر والحيطة لأن الإهمال أو ارتكاب بعض الأخطاء. ـ مهما كانت بسيطة ـ يعرض المنشأة للاختراق، ومن تلك الأخطاء مايلي:

ـ إهمال المستخدمين وتهاونهم في حفظ كلمات السر، مثل كتابتها على ورقة وتعليقها بجانب الجهاز، أو إخفائها تحت لوحة المفاتيح مما يعرضها للسرقة، وبالتالي دخول أشخاص غير مرغوبين إلى النظام.

ـ اختيار كلمات سر يسهل تخمينها، مما يؤدي في كثير من الأحيان إلى فتح ثغرة أمام المتطفلين.

ـ وضع جهاز للاتصال بالحاسب عن بعد (Modem)، مما يهدد الشبكة المحلية بالاختراق، حتى مع استخدام جدار النار للحماية من الاختراقات المحتملة عبر الشبكة. وهذا مثل المنزل ذو النوافذ الكثيرة، فلو أهمل أحد الساكنين في هذا المنزل إغلاق النافذة الخاصة به لهدد جميع من في المنزل بالخطر ولم يقتصر إهماله على نفسه فقط.

ـ إهمال مدير النظام تحديث نظم التشغيل الموجودة لديه و عدم متابعة سد الثغرات (Vulnerabilities) التي قد تكتشف بين حين وآخر، فإنه يعرض المنشأة لخطر الاختراق.

ـ تحميل البرامج و حافظات الشاشات (Screen Savers) من الإنترنت دون التأكد من محتوياتها ومصدرها، فقد تكون هذه البرامج محملة بالفيروسات أو البرامج الخفية التي تفتح ثغرات لدخول المتطفلين دون أن يشعر المستخدم.

وقد دلت الدراسات على أن الكثير من الاختراقات حدثت على أيدي أناس يعملون لدى المنشأة، وقد قاموا بها لأسباب مادية أو انتقامية. وهناك قسم من المستخدمين يروق له استكشاف هذه الثغرات وإن لم يكن لديهم نوايا سيئة.

أمثلة على الاختراقات

لا شك أن قصة **ادريان لامو** ـ حدثت الصيف الماضي ـ مع محطة **إن بي سي** تحكي كيف يمكن الحصول على المعلومات الشخصية باختراق الأجهزة المرتبطة بالإنترنت. حيث سُجلت مشاهد كانت تصور هذا المخترق وهو يشرح للمشاهدين طريقته في الدخول إلى الشبكات بدون تصريح، إلا أن محامو الشركة التي تمتلك المحطة منعوا عرض هذه المشاهد لأن المثال الذي استخدم كان اختراق لشبكة المحطة نفسها حيث نجح لامو في الدخول إلى الشبكة بسبب ضعف في كلمات السر. وقد نجح في اختراق شبكات أخرى من قبل

وعرض على أصحابهاالقيام بسد الثغرات التي اكتشفها.

ولا شك أن **لامو** ليس الوحيد الذي يقوم بهذا العمل بل قد يوجد من يقوم به بهدف سرقة المعلومات ويبقي هذا قيد الكتمان إما خوفاً من الملاحقة القانونية أو لغرض يخفيه في نفسه.

وتعد الفيروسات أشهر من تذكر قصصها، لكن آخرها الذي انتشر في شهر أكتوبر ٢٠٠٢م هو **(BugBear)** وقد اشتهر باسمه بالعربية "**باغبير**" حتى ظن الكثيرين أن مصدره عربي، إلا أن الاسم الإنجليزي ينفي هذا. وهو من أنواع الفيروسات التي تسمى بالدودة (Worm)، وعبارة عن برنامج ينقل نفسه عبر البريد من جهاز إلى آخر، وقد يسبب إعاقة للشبكة إذا لم يعالج، حيث يغرق الشبكة بالرسائل البريدية. وقد وصل هذا الفيروس إلى شبكة البرلمان الأسترالي مرتين خلال شهر أكتوبر وذلك بسبب الاتصال بشبكة البرلمان عن بعد.

ولعل من أكبر المصائب أن تصاب البرامج التي تستخدم في الكشف عن الاختراقات ومراقبة الشبكة بفيروسات حيث يتم استبدال البرامج الأصلية ببرامج أخرى تشبه البرنامج الأصلي، إلا أنه تم تعديله ليسمح للمخترقين بالدخول للجهاز المستخدم. وهذا ما حدث في شهر نوفمبر حيث اكتشفت نسخ من برنامجي (Libpcap) و (Tspdump) تم تعديل محتوياتها لتتصل بجهاز خارجي وتستقبل منه أوامر تمكن من اختراق الجهاز.

ومثل هذه القصص تدفعنا للحرص ومتابعة ما يستجد دوما في هذا المجال لحماية الأجهزة والشبكات. كما أن غير المتخصصين يجب عليهم اتباع التعليمات الخاصة بحماية أجهزتهم والتي تعطى غالبا لهم من مسؤول الشبكات بالمنشأة.

نصائح هامة للمستخدمين

يعد المستخدمون هم العنصر المهم في الحفاظ على محتويات ملفاتهم وسلامة أجهزتهم، ولذلك عليهم إتباع النصائح التالية:

* **الحفاظ على كلمة السر**، ويُنصح بما يلي:

- يفضل استخدام ستة حروف على الأقل.
- يجب خلط وتشكيل مظهر الحروف مثل (MOhaMmEd).
- يفضل أن تكون كلمة السر مكونة من أرقام وحروف مثل (K2aL4d)
- يجب أن تكون كلمة السر سهلة التذكر تفادياً للنسيان وحتى لا تكتب على ورقة.
- يفضل تغيير كلمة السر كل ستة أشهر وذلك بصورة مستمرة.
- عدم استخدام كلمة سر مستندة إلى معلومات شخصية، وبالتالي يسهل تخمينها مثل: أسماء الأولاد وتواريخ الميلاد، ونوع السيارة وغيرها.
- تجنب الكلمات والمفردات التي توجد في القاموس لأنه يسهل كشفها عن طريق بعض البرامج.
- تجنب استخدام الأسماء الدارجة المعتادة مثل : (PASS, SYSTEM, MYPASS).
- تجنب كتابة الرقم السري في ورقة خارجية أو على ملصق بجانب الجهاز.
- عدم إطلاع أحد على كلمة السر ولو لفترة وجيزة، وإذا لزم الأمر إعطاءها لمدير النظام مثلا فغير كلمة السر مباشرة.
- إذا أحسست بطلب النظام لكلمة السر أكثر من مرة بخلاف المعتاد، فغير كلمة السر فقد يكون جهازك مصابا بفيروس.

يفضل اختيار كلمة السر بحيث تشكل أوائل كلمات في جملة مثل:

This is a gift for students at KSU" "

من الجملة: " Tiag4saK"

ومن أمثلة كلمات السرالجيدة:

HoG66r, Dpd5q, KhAliD22b, aDf2FdA

أما كلمات السر غير المقبولة:

KHALID, July1992, Mom, MyPassword, Keep, man

* **استخدام الإنترنت**، ويجب على المستخدمين الحرص على ما يلي:

- استخدم برامج الحماية من الفيروسات وخاصة تلك التي تحمي من الفيروسات القادمة عبر الإنترنت.
- تحديث برنامج الحماية من الفيروسات بصورة دورية.
- الحرص على تحديث برامج التشغيل بصفة دورية.
- عدم فتح البريد الإلكتروني إذا كان من مجهول.
- تجنب تحميل البرامج من الإنترنت إلا من المصادر والمواقع الموثوقة.
- فحص الملفات المجهولة للتأكد من خلوها من الفيروسات قبل فتحها.
- التأكد من إغلاق المنافذ غير المستخدمة عند الاتصال بالإنترنت، حيث يدخل المتطفلون عبر هذه المنافذ. وقد تفيد بعض البرامج مثل (Lock Down) و (Zone Alarm).

المراجع :

http://www.sans.org

http://www.securityfocus.m

http://www.cert.org

Computer Security, Dieter Gollmann, John Wiley & Sons

Maximum Security, Anonymous, Sams