الباب الثامن
أمان الشبكات

الفصل الثالث والعشرون : تأمين الشبكة

الفصل الرابع والعشرون : حماية البيانات على الشبكة

الفصل الخامس والعشرون : جدران النار ***Fair Walls***

الفصل الثالث والعشرون
تأمين الشبكة

تمثل الشبكة خطراً أمنياً هائلاً علي بياناتك، يتمثل في قدرة أي شخص علي اختراقها إذا نجح في الوصول إلي أي جهاز علي الشبكة. لذلك فإن تأمين الشبكة أمر غاية في الأهمية. إذ بدونه لا وجود لشبكة . بانتهاء هذا الفصل ستتعرف علي :

- لماذا نحتاج لتأمين الشبكة
- نظام حسابات المستخدمين
- حماية كلمة المرور
- حماية الشبكة من الفيروسات
- حماية الشبكة من الهجمات الخارجية

في الماضي كان تأمين الشبكات يقتصر علي تأمين كلمات المرور الخاصة بمستخدمي الشبكة وتحديد صلاحيات للمستخدم في الوصول إلي الموارد المشتركة . أما بعد انتشار الانترنت فقد أصبحت معظم المخاوف الأمنية مصدرها الأساسي مرتبطاً بالهجمات الخارجية

من أشهر أنواع الهجمات الخارجية اختراق الهاكرز للشبكة الداخلية (توجد وسائل كثيرة لاختراق الهاكرز للشبكة أشهرها اكتشاف الهاكرز عنوان IP لنظام داخل النظام التأميني) أو إرسال رسائل الكترونية مرفق بها نوع من الفيروسات القصد منها تدمير البيانات الموجودة علي الشبكة .

ولذلك أصبح تأمين الشبكة من كل من المستخدمين الداخليين للشبكة والهجمات الخارجية للشبكة أمراً يشغل بال مدير الشبكة لأنه قد يؤدي إلي السطو علي البيانات أو تدميرها .

وفيما يلي نتناول هذه الأمور بشئ من التفصيل

تأمين الشبكة

نقصد بتأمين الشبكة أن يقوم مدير الشبكة بواحد من اثنين . إما أن يقوم بمنح صلاحيات وصول لجميع المستخدمين لكل موارد الشبكة ثم يضع قيودا على الموارد التي لايرغب في الوصول إليها أو يضع نظاما يمنع الوصول إلي جميع الموارد ثم يعطي صلاحيات لمستخدمين بعينهم للوصول إلي الموارد التي يحتاجون إليها .

من المهم جداً تعيين اسم مستخدم وكلمة مرور لتسجيل الدخول إلي الشبكة . ويتحكم مدير الشبكة في تعيين أسماء المستخدمين وكلمات المرور لكل منهم . وهنا لابد أن يجتهد مدير الشبكة لوضع مجموعة من القواعد عند تعيين أسماء المستخدمين وكلمات المرور حتي لا يمكن تخمينها من قبل أي شخص يريد السطو علي حساب مستخدم ما للوصول إلي الشبكة .

وفي النظام الأول تكون البيانات المطلوب تأمينها محددة (مثلاً ملف قاعدة بيانات الموظفين) بينما تكون باقي البيانات متاحة لمستخدمي الشبكة. وفي النظام الثاني يتم تحديد مستوي وصول لكل مستخدم علي الشبكة. فمثلاً قد يحتاج بعض المستخدمين إلي القدرة علي

قراءة ملف الموظفين علي الشبكة . في هذه الحالة يتم منح هؤلاء المستخدمين فقط إذناً أو حق قراءة هذا الملف .

نظام حسابات المستخدمين Users ID

المقصود بحسابات المستخدمين هنا حقوق دخولهم إلي الشبكة . تعمل حقوق دخول المستخدمين أو الحسابات المخصصة لهم علي قصر الدخول إلي الشبكة علي المستخدمين المصرح لهم فقط بذلك، بدون وجود حق الدخول هذا ، لا يمكن للمستخدم تسجيل الدخول إلي الشبكة .

لا يتم تسجيل دخول المستخدم إلي الشبكة إلا بإدخال **ID** والمقصود بـــــ **ID** أسماء المستخدمين ويتم تعيين أسماء المستخدمين من قبل مدير الشبكة ويجب أن يختار أسماء يسهل تذكرها (مثلاً اختيار الأحرف الأولي والأخيرة من اسم المستخدم) كما يجب مراعاة اصطلاحات التسمية التي يحددها نظام التشغيل المعمول به علي الشبكة . حيث يختلف عدد الأحرف التي يمكن استخدامها لإنشاء اسم مستخدم من نظام تشغيل إلي آخر ولذلك يجب أن يكون مدير الشبكة علي دراية باصطلاحات التسمية قبل أن يقوم بإنشاء حسابات المستخدمين

لا يقتصر دور مدير الشبكة علي تعيين أو تعريف مستخدمي الشبكة بل يمكنه التحكم في حسابات المستخدمين أو حقوق الدخول كما يلي

- يستطيع أن يمنح صلاحيات لمستخدمين معينين بالدخول إلي الشبكة في أوقات معينة . وبذلك يستطيع أن يقصر دخول الموظفين علي الشبكة خلال ساعات الدوام الرسمي فقط .
- يستطيع إنشاء حقوق دخول المجموعة . وفي هذه الحالة يكون لجميع المستخدمين التابعيين لنفس المجموعة جميع حقوق الوصول الممنوحة للمجموعة .
- يتم من خلال حقوق الدخول لمجموعة التحكم في حقوق دخول المستخدمين . مثلاً يمكن إنشاء حق دخول لمجموعة تسمي الحسابات وحق دخول لمجموعة قسم المبيعات ويخصص لكل مجموعة الملفات التي تخصها فقط بحيث لا تتداخل ملفات القسمين معاً.

- في حالة وجود مستخدم يتطلب عمله الوصول إلي معلومات قسمين (مثلا قسم الحسابات وقسم الإدارة) يمكن أن يجعل مدير الشبكة هذا المستخدم عضواً في المجموعتين . وبالتالي يكتسب الحقوق الممنوحة لكل مجموعة ينتمي إليها .

كلمات المرور Passwords

يعد استخدام كلمات المرور أهم عامل فى تأمين الشبكة . لان أسماء المستخدمين (IDs) لا تتوفر لها السرية الكاملة حيث يتطلب العمل فى كثير من الأحيان أن يعرف كل مستخدم أسماء المستخدمين الخاصة بغيره . فعلى سبيل المثال عندما ترغب فى إرسال رسالة الكترونية إلي احد المستخدمين لابد أن تكون تعرف الاسم (ID) المخصص له .

ولهذا تعتبر كلمات المرور الوسيلة الوحيدة لمنع أي محاولة تسلل إلي الشبكة باستخدام الاسم المخصص لأحد المستخدمين ولهذا يجب استخدام كلمات مرور قوية. وكلمة المرور القوية هى كلمة المرور التى ليس من السهل أن يخمنها أي شخص ليتمكن من السطو على حساب المستخدم ويحاول الوصول إلي الشبكة .

وفيما يلى مجموعة من القواعد التى تساعد مدير الشبكة فى إنشاء كلمة مرور قوية

- لا تختار كلمة مرور يمكن تخمينها بسهولة كاسمك أو اسم طفلك أو اسم شركتك.
- اختر كلمة مرور تحتوى على مزيج من الحروف الأبجدية والأرقام .
- استفد مما تنتجه اغلب نظم التشغيل من وضع تاريخ انتهاء العمل بكلمة المرور . إذا قمت بتحديد مدة انتهاء العمل بكلمة مرور بعد أسبوعين ، يجب على المستخدم تغيير كلمة المرور بعد انقضاء هذه المدة . رغم أن هذه العملية تسبب نوعا من الإزعاج لكنها تحميك من شخص ربما تلصص عليك اثناء كتابة كلمة المرور الخاصة بك .
- احذر من تجاهل عمليات التأمين الأساسية المتعلقة بكلمة المرور حتى وأن كانت الشبكة صغيرة .

حماية الشبكة من الفيروسات

لاشك أن الفيروسات من أهم الأعمال التخريبية التي تصيب أجهزة الكمبيوتر وتؤدي إلي تدمير البرامج والبيانات . ومن سوء الحظ أن عدد الفيروسات في تزايد مستمر وكلما أنتجت الشركات مضادات للفيروسات ابتكر المخربون نوعاً جديداً من الفيروسات .

تأخذ فيروسات الكمبيوتر أشكالا عديدة . منها ما ينشط عند بداية تحميل الجهاز ويؤدي إلي تخريب الأقراص ومنها ما يصيب ملفات البرامج القابلة للتنفيذ (ملفات **EXE** أو **Com**) بمجرد تشغيل الملف المصاب يتم تحميل الفيروس في الذاكرة ويؤدي إلي تدمير الملفات القابلة للتنفيذ .

من الفيروسات الخبيثة تلك التي تصيب المستندات وملفات جداول البيانات وليس فقط الملفات القابلة للتنفيذ . من الفيروسات ما يصيب برامج تشغيل الأجهزة (منها علي سبيل المثال برنامج تشغيل مشغل البطاقات) . ولهذا فان حماية الشبكة من الفيروسات امر فى غاية الأهمية وهو لا يقل عن حمايتها بالوسائل التقليدية مثل كلمات المرور وصلاحيات الاستخدام ومراقبة عمليات تسجيل المستخدمين التى شرحناها من قبل .

والطريقة الوحيدة لحماية الشبكة من الفيروسات هى استخدام برامج مضادات الفيروسات. توجد برامج كثيرة من مضادات الفيروسات تستخدم لفحص الملفات فى بداية العمل . ننصح بان تقوم بتثبيت برامج مضادات الفيروسات ليتم تشغيلها تلقائيا لتضمن القضاء على الفيروسات قبل أن يبدأ خطرها . ورغم أن هذا يبطئ العمل بعض الشيء ، إلا أن الوقت الذي ينفق فى تنظيف النظم المصابة بالفيروسات يعد وقتاً ثميناً جدا.

توفر شركة **Symantec** العديد من برامج مضادات الفيروسات و تعتبر من أشهر الشركات العاملة فى هذا المجال . المال الذي تنفقه فى شراء هذه البرامج لا يعد نوعاً من الإسراف. تابع الجديد دائما فى مجال برامج مضادات الفيروسات واحرص على اقتنائها وتثبيتها على أجهزتك .

أذونات الموارد

يعد تأمين الشبكة باستخدام استراتيجيات مرتبطة بحسابات المستخدمين وكلمات المرور طريقة واحدة فقط لتأمين الشبكة الداخلية. ترتبط طريقة أخرى لتأمين البيانات والموارد المهمة على الشبكة بحقوق المستخدمين أو الأذونات لهذه الموارد. بعد أن يسجل مستخدم ما الدخول إلى الشبكة، سوف يحتاج عادةً إلى الوصول إلى الموارد على وحدة خدمة الملفات أو الطباعة. يرجع أمر تحديد مستوى الوصول الذي سوف يتوفر لكل مستخدم إلى اشتراك ما أو وحدة التخزين على وحدة خدمة الملفات إلى مدير الشبكة. يوفر كل نظام تشغيل طريقة لتعيين إذن (أو حقوق) للمجلدات أو الأدلة على خادمات الشبكة.

على الرغم من أنه من المناسب منح كل المستخدمين نفس الوصول إلى أي مورد، فإنك سوف تحتاج إلى الوضع في الاعتبار حقيقة أن كل مستخدم سوف يتطلب مستوى وصول مختلف إلى مورد معين، لا يحتاج كل شخص على الشبكة إلى حقوق أو أذونات الكتابة والتعديل . على سبيل المثال: سوف يحتاج المحاسب إلى القدرة على تحرير جداول البيانات على وحدة الخدمة، بينما يحتاج المساعد الإداري إلى القدرة على عرض البيانات المضمنة في الملف أو قراءتها . على الرغم من ذلك، يعد الحفاظ على تعيين أذونات مستقلة لكل مستخدم للوصول إلى كل مورد عملية منظمة، أمراً مستهلكاً للوقت ومرهقاً.

إن ما يميز نظم تشغيل الشبكات أنك يمكنك إنشاء مجموعات ثم تعيين أذونات أو حقوق وصول للمجموعة. بعد ذلك، سوف تحدد عضوية المجموعة مستوى الوصول الذي يحصل عليه المستخدم لموارد معينة.

على الرغم من أن حقوق الوصول لا تبعد "الهاكرز" عن الشبكة الداخلية بالضرورة، فإنها تسمح لك بتقليل التلف الذي يمكن أن يحدثه مستخدم مهمل على ملفات البيانات المهمة، أو مستوى الوصول الذي سوف يحصل عليه الهاكر إلى مورد معين عندما يستولي على حساب مستخدم معين.

حماية الشبكة من الهجمات الخارجية

تأتى الهجمات الخارجية عادة للأجهزة المتصلة بالانترنت . بعد أن أصبح الاتصال بالانترنت ضرورة . أصبح بروتوكول TCP/IP هو البروتوكول القياسي للشبكة . ولكن للأسف لم يتم وضع التأمين فى الاعتبار عند تصميم هذا البروتوكول . تمثل بروتوكولات TCP/IP والشبكة ونظم تشغيل الجهاز التابع تغيرات ممكن أن يستغلها الهاكرز الذين يراقبون اتصال الشبكة غير المؤمن عبر الانترنت . لذلك وجد الهاكرز مجموعة من الأساليب الفنية للتحايل على استراتيجيات تأمين الشبكة.

ولكن كيف يتم حماية بيانات الشبكة من قبل الهاكرز لا المخربين ؟

هناك طريقتان لحماية الشبكة .

الاولى : استخدام النظم التأمينية　　الثانية : استخدام تأمينIP

أولا : النظم التأمينية

هناك نظم تأمينية لبرامج ونظم تأمينية للأجهزة . يفحص النظام التأميني البيانات التي تدخل إلي الشبكة أو التي تخرج منها . ويمكنه تصفية البيانات التى تنتقل بين الاتجاهين . حيث أن البيانات الداخلة إذا لم تلب قواعد معينة تم توصيفها على النظام التأميني . لن يتم السماح للبيانات بدخول الشبكة الداخلية أو مغادرتها .

*ثانيا : استخدام تأمين*IP

إذا كانت الشبكة الداخلية تستخدم بروتوكول TCP/IP يكون لكل جهاز عنوان مميز . يمكن أن تقدم عناوين IP الداخلية للمخرب الماهر فرصة الوصول إلي مناطق غير مصرح بها على الشبكة . هناك تفاصيل فنية لعملية اختراق الهاكرز للشبكة باستخدام عناوين IP وهى باختصار شديد أن كل حزمة بيانات IP تحتوى على قدر كبير من المعلومات . وبعد أن يلتقط الهاكرز حزمة البيانات ، فإنه يمكنه قراءة عناوين IP التى توفر عناوين المصدر والوجهة .

ولمواجهة هذا الوضع تم تطوير نظام يسمى IP Security أو IP Sec . يقوم هذا النظام بتزويد شبكات IP/TCP بآلية تأمين تحتفظ بالبيانات آمنة أثناء النقل .بمعنى أن أي شخص يعترض طريق البيانات سواء على الشبكة الداخلية أو عبر اتصالات الانترنت ، لا يمكن قراءتها أو تعديلها أو إعادة تشغيلها .

ملخص الفصل

في هذا الفصل ناقشنا أموراً هامة لتأمين الشبكة باعتبارها أمراً يشغل بال مدير الشبكة. من المهم جداً أن يقوم مدير الشبكة بتعيين اسم مستخدم وكلمة مرور لتسجيل الدخول إلي الشبكة. يجب علي مدير الشبكة البحث عن أحدث برامج مضادات الفيروسات لحماية الشبكة من الفيروسات باعتبارها من أهم الأعمال التخريبية التي تصيب أجهزة الكمبيوتر وتؤدي إلي تدمير البرامج والبيانات. وناقشنا أيضاً حماية الشبكة من الهجمات الخارجية التي تأتي من الاتصال بالانترنت وذلك عن طريق اختيار نظم تأمينية للبرامج والأجهزة أو استخدام نظام IP Security .

تدريبات

١. يعتبر نظام حسابات المستخدمين وكلمات المرور واحدة من وسائل تأمين الشبكات. اشرح ذلك باختصار.

٢. أذكر ثلاثة من الأمور التي تساعد في إبطال الهجمات الخارجية.

الفصل الرابع والعشرون
حماية البيانات على الشبكة

في هذا الفصل ستتعرف علي مفاهيم أخري تساعد في حماية البيانات علي الشبكة. تشمل هذه المفاهيم :

- *صلاحيات الاستخدام*
- *احتياطات الأمان*
- *تأمين الاتصال بالانترنت*
- *تأمين الشبكات اللاسلكية*

صلاحيات الاستخدام

نقصد بصلاحيات الاستخدام الصلاحيات أو الحقوق التى تخص كل من المستخدمين ونظام الملفات ومدير الشبكة نفسه.

يعد تأمين الشبكة باستخدام أسماء المستخدمين (IDs)وكلمات المرور التى شرحناها من قبل طريقة واحدة فقط لتأمين الشبكة . رغم أهميتها البالغة في تأمين الشبكة حيث تعتبر خط الدفاع الأول في خطة تأمين الشبكة .

تأتي الصلاحيات الممنوحة للعاملين علي الشبكة أو حقوق الاستخدام في المرتبة الثانية بعد استخدام الاسم وكلمة المرور لكل منهم .

فيما يلي نوضح الحقوق أو الصلاحيات التي تخص كل من المستخدم والمدير ونظام الملفات الموجود علي وحدة الخدمة للشبكة.

بالنسبة لحقوق دخول مدير الشبكة لا ينبغي أن تفرض عليه قيود أمنية من أي نوع، لأنه هو المسئول عن نظام تأمين الشبكة بأكمله . بل تعتبر مسئولية تأمين الشبكة واحدة من أهم واجباته.

حقوق دخول المستخدم

تتفاوت الحقوق التي تمنح للمستخدمين . تعتمد حقوق المستخدم علي السياسة التي تضعها الشركة والحدود التي يراها مدير الشركة للمستخدمين وفيها علي سبيل المثال تغيير الوقت والتاريخ المسجلين بواسطة وحدة الخدمة أو الدخول مباشرة من خلال لوحة مفاتيح وحدة الخدمة. أو نسخ الملفات والأدلة من علي جهاز وحدة الخدمة واسترجاعها .

حقوق نظام الملفات

تحدد حقوق الملفات العمليات المسموح القيام بها من قبل المستخدمين علي الملفات حيث أنه من غير المقبول أن تصبح البيانات المتاحة لجميع العاملين علي الشبكة . فمثلاً في غالب الأحيان لا يسمح لموظفي المبيعات بمعرفة أسعار الشراء الموجودة بملف المشتريات، كما يمكن إعداد حقوق نظام الملفات للسماح لمستخدمين بعينهم بقراءة ملفات معينة بدون

صلاحيات التعديل أو الحذف .

رغم أن طريقة إدارة حقوق نظام الملفات تختلف من نظام تشغيل لآخر . إلا أن الفكرة واحدة وهي تحديد الصلاحيات الممنوحة لكل مستخدم بالوصول إلي الملفات أو المجلدات أو الأقراص والقيام بعمليات معينة عليها .

هناك ٦ صلاحيات أساسية في نظام **Windows** يمكن تحديد أي مجموعة من هذه الصلاحيات لمستخدم أو مجموعة مستخدمين بالنسبة لملف أو مجلد معين .

يوضح الجدول التالي الصلاحيات الرئيسية في نظام **Windows**

الصلاحية	الاختصار	العمليات المسموح بها
قراءة **Read**	**R**	فتح وقراءة الملفات
كتابة **Write**	**W**	فتح الملف وتعديله
تنفيذ **Execute**	**X**	تشغيل الملف
حذف **Delete**	**D**	حذف الملف
تغيير **Change**	**P**	تغيير صلاحيات الملف
ملكية **Take Ownership**	**O**	ملكية الملف

صلاحيات الملكية Take Ownership

راجع الجدول تجد في آخر عمود الصلاحية " صلاحيات الملكية **Ownership** " في نظام **Windows** لكل ملف أو مجلد مالك . وهو المستخدم الذي قام بإنشائه ويمكن نقل الملكية من مستخدم لآخر .

الهدف من صلاحية **Take Ownership** هو منع أي شخص من إنشاء ملف أو مجلد ثم نقل ملكيته إليك بدون تصريح منك .

لا يسمح **Windows** بنقل ملكية ملف لمستخدم آخر ولكنه يسمح بمنع مستخدم آخر حق اكتساب ملكية الملف .

وجدير بالذكر أن هذه الصلاحيات لا تطبق إلا علي الملفات أو المجلدات التي يتم إنشاؤها بواسطة نظام **NTFS**. إذا كنت تستخدم نظام **Fat** أو **Fat 32** فلن تستفيد من صلاحية

الملكية في تأمين الملفات أو المجلدات .

مراقبة تسجيل دخول المستخدمين

لا يكفي استخدام كلمة مرور قوية علي الشبكة. بل لابد من استخدام نظام لمراقبة عمليات تسجيل دخول المستخدمين علي الشبكة وعادة يسمح نظام تسجيل عمليات الدخول بتسجيل عمليات الدخول التي تتم بنجاح وتلك التي لا يقدر لها النجاح . وهذا يوفر نوع من المراقبة تتيح التعرف علي محاولات الدخول غير الناجحة، التي قد تتم من قبل شخص غير مسموح له بالولوج إلي الشبكة . وبالتالي تنبه صاحب الحساب أن حسابه تعرض للسطو . وعادة توفر نظم تشغيل الشبكة نوع من أنواع مراقبة تسجيل دخول المستخدمين علي الشبكة . فمثلاً يوجد في نظام التشغيل **Windows Server 2003** سجل يسمي **Security** يستخدم لهذا الغرض .

في نظام تشغيل الشبكة **Windows Server 2003** يتم تعقب الأحداث الفعلية باستخدام سجل **Windows Security** .

احتياطات الأمان

لاشك أن التخريب المتعمد والكوارث البيئية من أخطر عوامل تدمير البيانات . ولذلك فإن وضع خطة لتأمين البيانات الموجودة على الشبكة أمر بالغ الأهمية .

ناقشنا فى الفصل السابق جوانب كثيرة من هذه الخطة شملت استخدام كلمات مرور قوية على حسابات المستخدمين. ومراقبة عمليات دخول المستخدمين والتحكم فى الأوقات التى يمكن للمستخدمين فيها الدخول إلي الشبكة. شرحنا كذلك تأمين المجلدات المشتركة والأقراص المغناطيسية باستخدام صلاحيات الاستخدام.

وفيما يلى بعض الأفكار الإضافية التى تفيدك فى تأمين الشبكة

- افرض نظاماً صارماً على كلمات المرور وتأكد من أنها تستخدم بسرية تامة .
- راقب جيدا عمليات تسجيل دخول المستخدمين على الشبكة. استفسر عن الإدخالات فى سجل دخول المستخدمين كما تستفسر عن المكالمات الهاتفية الخارجية

التى تتم بالشركة.

- تأكد تماما من أن برامج مضادات الفيروسات كافية. لايكفى وضع برنامج واحد على الجهاز الخادم. استخدم برنامج آخر على محطات العمل وآخر للنظام التأمينى. إن التكلفة التى تدفعها فى هذه البرامج أقل بكثير من تكلفة تدمير البيانات التى قد تتعرض لها.
- يجب على جميع العاملين بالشركة من مستخدمين ومديرين عدم إعطاء بيانات عن المستخدمين وكلمات المرور عبر الهاتف إلا بعد التأكد من هوية المتصل لأن الهاتف وسلية غير آمنة فى الاتصالات.
- احتفظ بوسائط النسخ الاحتياطي فى مكان آمن بعيداً عن أجهزة الشبكة أو حتى بعيداً عن مقر الشركة فإن الكوارث الطبيعة مثل الزلزال أو الحريق يمكن لن تأخذ منها النسخ الاحتياطية.
- ضع فى حساباتك أنك تواجه دائما مخاطر الهجوم الخارجي الذي يمكن أن يأتى من الرسائل الالكترونية أو هجمات مباشرة من الهاكرز.

تأمين الاتصال بالانترنت

لن أعيد عليك فكرة الانترنت وفائدها وربط الشبكة الداخلية بها. هذا ليس مكان مناقشة هذه الأفكار. سأفترض أنك تعرف هذه الأمور وأن شبكتك متصلة بشبكة الانترنت وسأقصر كلامي على كيفية تأمين الشبكة فى حالة اتصالها بشبكة الانترنت.

بعد اتصال الشبكة الداخلية بالانترنت، يصبح تطبيق إجراءات وضع خطة أمنية على الشبكة بأكملها امراً حتميا. من أهم المخاطر الأمنية للاتصال بالانترنت إمكانية تسلل شخص خارجي إلي شبكتك والقيام بإعمال تخريبية.

فيما يلى بعض الاحتياطات التى تقلل المخاطر التى تتعرض لها فى حالة اتصال شبكتك بالانترنت :

- قبل تنزيل البرامج والملفات من الانترنت،تأكد من وجود برنامج للكشف عن الفيروسات على الجهاز الذى تستخدمه.

- لا تفتح ملفات أو بريد مجهول المصدر أو يحتوى على عنوان مريب. فربما يشتمل هذا البريد على فيروس. احذر من مرفقات البريد الالكتروني لأنها من أكثر وسائل انتشار الفيروسات.
- لا ترسل المعلومات السرية والهامة مثل كلمات المرور و أرقام بطاقة الائتمان عبر الانترنت لاحتمال تعرضها للسرقة. إذا كان ولابد يمكن تشفير هذه المعلومات قبل إرسالها.
- لاتسمح لأى جهاز متصل بالانترنت بتنشيط مشاركة الملفات لاتصالات **TCP/IP**. (لمزيد من المعلومات تابع قراءة البند التالي).

إلغاء تنشيط خاصية المشاركة لاتصالات TCP/IP

يشكل الاتصال بالانترنت من خلال جهاز مودم مخاطر أمنية شديدة . وعادة يسمح نظام **Windows** فى حالة وجود اتصال قائم بين جهاز كمبيوتر وشبكة الانترنت من خلال مودم بتنشيط إمكانية مشاركة الملفات والطابعة لاتصالات **TCP/IP** عبر جهاز مودم.

استخدام تأمين IP

شرحنا فى الفصل السابق الكثير عن إجراءات الحماية من الهجمات الخارجية وتطرقنا إلي موضوع حماية الشبكة فى حالة اتصالها بالانترنت من المخربين أو الهاكرز.

لذلك سنركز هنا استخدام تأمين **IP** هناك طريقة أخرى لحماية البيانات من الهاكرز الذين يحاولون الدخول إلي الشبكة باستخدام أدوات تحليل البروتوكولات، وهى استخدام تأمين **IP** والتشفير. يستطيع الهاكرز الحصول على قدر كبير من المعلومات باستخدام أدوات تحليل البروتوكولات لالتقاط اتصالات الشبكة غير المؤمنة.

بعد أن يلتقط الهاكرز خدمة البيانات، يمكنه قراءة رءوس عنوان **IP** التى تشتمل بدورها على عناوين المصدر والوجهة.

يستخدم بروتوكول **TCP/IP** عناوين مخصوصة تعرف باسم عناوين **IP** لتعريف أجهزة الكمبيوتر المختلفة المتصلة بالانترنت.عنوان**IP** عبارة عن رقم مكون من ٣٢ بت (أي أربعة أرقام عشرية) تنفصل عن بعضها بنقاط. تخصص لشبكتك

الأرقام الثلاثة أو الأربعة الأولى من العنوان (تبعا لحجمها) بينما يعرف بقية العنوان جهاز الكمبيوتر المتصل بالشبكة. فى حالة اتصال شبكتك بالانترنت، لا يستطيع أى جهاز على الشبكة الوصول إليها إلا من خلال عنوان IP الخاص به. يتم تخصيص هذه العناوين تلقائيا من خلال وحدة خدمة خاصة تعرف باسم DHCP. (راجع الفصل السابع عشر)

تم تطوير نظام يطلق عليه IP Security أو IP Sec ومعناها تأمين IP. لتزويد الشبكات التى تستخدم بروتوكول TCP/IP بآلية تأمين تحفظ البيانات آمنة أثناء النقل .

فإذا حاول شخص اعتراض طريق البيانات على الشبكة الداخلية أو عبر اتصالات الشبكة الخارجية فإنه لن يستطيع قراءتها أو تعديلها أو إعادة تشغيلها.

من أساليب الحماية التى يوفرها IPSec ضد هجمات الهاكرز أنه يقوم بتشفير البيانات على جهاز الكمبيوتر المرسل ، وهذا الأمر لا يتيح للمخرب قراءة البيانات التى يحاول اعتراضها أثناء نقلها. يقوم IPSec كذلك بتشفير البيانات على جهاز الكمبيوتر المستلم. وبهذا يغلق الطريق أمام الهاكرز الذي يحاول خرقها.

يدعم Windows Server 2003 نظام IPSec .

تأمين الشبكات اللاسلكية

صحيح اننا لم نتعرض بعد لشرح الشبكات اللاسلكية.سيتم شرحها بإذن الله من هذا الكتاب إلا أننى فضلت مادمنا فى معرض الحديث عن تأمين الشبكات فى هذا الفصل، فضلت مناقشة بعض المفاهيم المرتبطة بتأمين الشبكات اللاسلكية.

كيف يتم اختراق الشبكة اللاسلكية

لا يلزم فى حالة الشبكات اللاسلكية أن ينجح المخرب في الدخول إلي جهاز الكمبيوتر فى شركتك حتى يخترق الشبكة ، حيث يمكن التسلل إلي الشبكات من خلال وسيلة تعرف بـــــ"التوجيه اللاسلكي". وفكرة التوجيه اللاسلكي تتلخص فى استخدام جهاز كمبيوتر محمول لاسلكي للبحث عن شبكات لاسلكية غير مؤمنة والاتصال بها .

يجهز الهاكرز أجهزتهم بهوائيات لاسلكية خارجية لتسهل لهم الحصول علي النقاط الفعالة

اللاسلكية ويلجأون في الغالب إلي استخدام جهاز يدوي يسمي **Global Positioning System** أو **GPS** وتعني (نظام تحديد مواضع عامة) لمساعدتهم في تعيين الحدود الفعلية للنقط الفعالة .

بمجرد إيجاد نقطة فعالة لاسلكية غير مؤمنة ، يستطيع الهاكرز الوصول مجاناً إلي الانترنت . بل إنهم يقومون أكثر من ذلك بإرسال معلومات عن النقاط الفعالة إلي غيرهم من المخربين الذي يستخدمون التوجيه اللاسلكي من خلال بعض المواقع علي الويب .

بل أن الأمر يصل بالبعض منهم إلي التجوال بسيارتهم في المدينة ومعهم أجهزتهم المحمولة بحثاً عن أي اتصال مفتوح بشبكة لاسلكية . وقام بعضهم بنشر خريطة طريق علي الانترنت للشبكات اللاسلكية غير المؤمنة.

يستخدم الهاكرز مصطلح **War driving** للإشارة إلي أدوات اختراق الشبكات اللاسلكية . إذا بحثت عن كلمة **War Driving** باستخدام أحد محركات البحث، ستجد الكثير من المواقع تحتوي علي عدد كبير من الأدوات للتسلل إلي الاتصالات اللاسلكية .

كيف نحمي الشبكة اللاسلكية

فيما يلي بعض الإرشادات التي قد تعينك علي حماية الشبكة اللاسلكية. تستخدم الشبكات اللاسلكية جهاز يسمي **Wireless Access Point** وتختصر هكذا **WAP** لوصل أجهزة الكمبيوتر اللاسلكية بالشبكة السلكية الموجودة بالفعل . لذلك يجب عليك تنشيط سمة **Wired Equivalent Privacy** وتختصر **WEP** لجميع الأجهزة اللاسلكية في شبكتك . تعمل سمة **WEP** علي تأمين البيانات المنقولة في الشبكات اللاسلكية . ورغم أن هذه السمة لا توفر حماية تامة للبيانات إلا إنها تمنع محاولات التسلل المعتاد إلي الشبكة .

تستخدم الشبكات اللاسلكية ما يعرف بـــ **Service Set Identifier** وتختصر هكذا **SSID** ومعناها (معرف محدد الخدمة) لتعريف الشبكة اللاسلكية . بعبارة أخري يستخدم كاسم للشبكة اللاسلكية . يتم الاتصال بنقاط الوصول للشبكة اللاسلكية عن طريق **SSID** بواسطة أجهزة وكمبيوتر محمولة .

يوصف كل مورد نقطة وصول نقاط الوصول الخاصة به باستخدام **SSID** افتراضي

ويعرف الهاكرز ماهية معرفات **SSID** الافتراضية لمعظم نقاط الوصول للشبكة . لحماية شبكتك قم بتغيير القيم الافتراضية **SSID** . ولكننا ننصحك ألا تعول كثيراً علي تغيير **SSID** لان التغيير لن يحمي الشبكة كثيرا.

- احذر من تثبيت أجهزة **Wireless Access Point** بخلاف تلك التي قمت بنفسك بتثبيتها على الشبكة. نظرا لانخفاض أسعار **WAP** وسهولة تثبيتها فقد يقوم احد المستخدمين بتثبيت أحدها على الشبكة بدون إذن من مديرها. قد تعرض هذه الأجهزة الشبكة بالكامل للخطر .
- قم بتغيير جميع كلمات المرور الافتراضية، خاصية كلمات مرور **WAP** وحقوق دخول مدير الشبكة، وذلك لجميع أجهزة وحدة الخدمة. ترجع معظم حالات فشل الخطط التأمينية لأجهزة الكمبيوتر إلي استخدام كلمات مرور غير قوية.

ملخص الفصل

في هذا الفصل ناقشنا كيف يمكن حماية البيانات علي الشبكة. تعتبر الحقوق التي تمنح للمستخدمين لأداء بعض الأعمال والامتناع عن البعض الآخر وسيلة فعالة لحماية بيانات الشبكة. وكذلك يجب وضع قيود علي العمليات المسموح القيام بها من قبل المستخدمين علي الملفات.

استخدام أساليب التأمين المعروفة كتأمين الاتصال بالانترنت أمر هام أيضا لحماية البيانات. ناقشنا أيضا بعض الأفكار لحماية الشبكة اللاسلكية باعتبارها أسهل الشبكات اختراقاً.

تدريبات

١. كيف يمكن تأمين شبكتك في حالة الاتصال بالانترنت ؟

٢. أذكر ثلاثة من الأمور التي نفيدك في تأمين شبكتك ؟

الفصل الخامس والعشرون

جدران النار

Fire Wall

في الواقع ، الويب عبارة عن مجموعة من الموجهات ووحدات الخدمة التي تؤلف أكبر شبكة منطقية واسعة (WAN) في التاريخ المدون. إن مجموعة معدات التشبيك هذه كلها متصلة بالانترنت ويستطيع أن يصل إليها كل شخص متصل أيضاً.

وإذا كان كامل المعرفة البشرية مخزنة علي وسائط مغناطيسية. فإننا قلقون بشأن أمان هذه الشبكة، تمثل جدران النار واحدة من التدابير الوقائية المستخدمة لحماية هذه الكمية الهائلة من المعلومات. بالانتهاء من هذا الفصل ستتعرف علي :

- *جدار النار.*
- *ضرورة جدار النار.*
- *جدران النار كأسلوب أمان.*
- *كيف يعمل جدار النار.*
- *جدران النار أثناء عملها.*
- *أنواع جدار النار.*

هل هناك مؤسسة ما تحافظ علي النظام في الانترنت بنفس الطريقة التي تحافظ بها الشرطة علي النظام علي الطرقات العامة؟ أو هل هناك وكالة حكومية تتطفل علينا وتفحص جيداً كل جهاز موصول بالانترنت؟ الجواب علي هذه الأسئلة هو لا؛ ليست هناك مؤسسة موحدة مسئولة عن حماية الانترنت. إن وظيفة حماية والمحافظة علي مداخل قاعات المعرفة علي الانترنت متروكة للشخص (أو الأشخاص) المسئول عن نشر تلك المعلومات في المقام الأول. كل موقع ويب يتصدره اتصال شركة بالانترنت أو مزود خدمة الانترنت (**ISP**، أو المزود)، وتكون وظيفته هي التأكد أن القراصنة (الأشرار) لا يسببون فوضى في معلومات موقع الويب المخزن والمصنفة بعناية. ولكن كيف نحمي موقع ويب أو وحدة خدمة بريد أو وحدة خدمة **FTP** أو بقية مصادر المعلومات التي يمكن الوصول إليها من الويب؟ الجواب بسيط جدا: جدار نار **(firewall)** .

جدار النار

هو جهاز أمان يجلس على حافة اتصالك بالانترنت ويعمل كضابط أمن على حدود الانترنت. إنه ينظر إلى كل حركة المرور التي تدخل إلى اتصالك وتخرج منه، منتظراً حركة مرور يمكنه أن يصدها أو يرفضها وفقاً لقاعدة معتمدة. جدار النار هو القانون في ويب عالمية خالية من القوانين . إنه يقظ دائماً في مهمته لحماية الموارد الداخيلة للشبكة الموصولة به.

لقد جعلت الانترنت كمية هائلة من المعلومات متوفرة للمستخدمين سواء للأفراد أو للشركات. لكن جعل معلوماتك متوفرة على الانترنت يمكن أن يعرض البيانات المهمة أو السرية لهجمات من أى مكان فى العالم _ الانترنت هي شبكة عالمية بكل ما للكلمة من معنى. وهذا يعني أنني عندما أتصل بالانترنت في جنوب أفريقيا يمكن أن أتعرض لهجوم من أوروبا أو آسيا، الخ. بإمكان جدران النار أن تحمي كمبيوترات الأفراد وشبكات الشركات من الاقتحام العدائي عبر الانترنت، لكن يجب أن تفهم جدار نارك لكي تستعمله بشكل صحيح.

هذا " الشرطي الالكتروني" الذي يعمل على مدار الساعة وفي كافة أيام السنة لديه وظيفة

مهمة جداً: إبقاء الأشرار خارجاً وتمكين الأخيار من الوصول إلي الموارد التى يحتاجون إليها ليقوموا بأعمالهم .يبدو هذا الكلام بسيطاً جداً على الورق، لكن ضبط تكوين جدار نار" بشكل صحيح" في الواقع هو أمراً ليس سهلاً .

قبل أن نشرح عمل جدار النار نورد فيما يلى بعض الأسئلة المشروعة التي توضح واجبات جدار النار لفهم ما الذي يجعله يعمل وكيف يؤدي عمله.

من يحتاج إلي جدار نار؟

إنه ربما أكثر أسئلة الأمان تداولاً.إذا كنت تنوى الاتصال بالانترنت، تحتاج إلى جدار نار. لا يهم إذا كنت تتصل من المنزل أو من شركتك. إن الانتشار المتزايد لخدمات الانترنت العريضة النطاق في المنازل وميزتها بأنك ستكون متصلاً بالانترنت دائماً يجعل أمان المنزل أهم بكثير من ذي قبل.

لماذا أحتاج إلى جدار نار ؟

مثلما كان القراصنة في قديم الزمان يتجولون في البحار، يتجول القراصنة في ساحات الانترنت وهم يسعون إلى النيل منا. في أغلب الأحيان لا تريدهم أن يدخلوا شبكتك ويتجولوا بين الكمبيوترات الموصلة بها.

أنت تعرف أنه يجب أن تحمي شبكتك من أولئك المهاجمين، وإحدى الطرق الأكثر فعالية لحماية شبكتك هي تثبيت جدار نار. بشكل افتراضي، أي جدار نار جيد يمنع تبادل أى حركة مرور غير مرغوب فيها بين الانترنت وبين شبكتك الداخلية. وفي سياق ذلك، يزود جدار النار قواعد فحص الرزم المبين للحالة (SPI) لكل رزمة واردة.

البديل لاستخدام جدار نار هو السماح لكل اتصال بدخول شبكتك _ يعنى لن يكون هناك أي نوع من أنواع فحص الرزم لتحديد ما إذا كان هناك هجوم يختبيء ضمن إحدى الرزم الواردة أم لا. إن عدم استعمال جدار نار سيجعل مؤسستك متاحة أمام جميع المتواجدين على الانترنت .

هل لدي أي شيء يستحق الحماية؟

ربما تسأل مثل هذا السؤال :" أنا أفهم أنه لو كان لدي شيء يستحق الحماية، لكنت سأحتاج إلي جدار نار بالتأكيد. لكنني لا أملك أي شيء سيرغب به المهاجمون، لذا لماذا يجب أن أكترث لوجود جدار نار أو لعدم وجوده؟"

الشبكات ومواردها مهمة للطريقة التي ننجز بها أعمالنا الشخصية والتجارية . هذا يعني أن هناك قيمة لشبكتك ولتمكينها من أن تعمل بفاعلية. هذا الدور المتزايد للشبكات يعني أنك بالتأكيد تملك شيئاً يستحق الحماية إلى درجة ما، ويتضح ذلك مما يلي :

- *البيانات المفقودة* : ماذا لو لم تستخدم جدار نار وقام مهاجم بحذف بياناتك لأنه يستطيع ذلك؟ ماذا سيحصل للشركة؟ هل ستتكلف أموالاً لإعادة إنشاء كل شيء؟ هل ستعاني من فقدان المبيعات؟ لا شك أنك سمعت بقصص الشركات التي فقدت كل بياناتها المهنية في هجمات الفيروسات الشهيرة ، والعديد منها لم يتمكن من استعادتها.
- *تهديد البيانات السرية*: لكل مؤسسة بيانات تعتبرها سرية وفقدانها قد يسبب مشاكل مالية أو قانونية أو إحراجاً شديداً . قد تنتج تلك الأشياء عن فقدان معلومات الزبائن كأرقام بطاقات الائتمان أو وقوع الخطط السرية في أيدي المنافسين.اللائحة لا تنتهي وعندما تتعرض للقرصنة، يجب أن تفترض أسوأ الاحتمالات. لهذا السبب على الأرجح لا يتم تبليغ الشرطة عن معظم الجرائم الإلكترونية .
- *توقف عمل الشبكة*: هل ذهبت يوماً إلي الصراف الآلي أو متجر بقاله للحصول على نقود ودفعت بواسطة البطاقة في قارئة البطاقات؟ الشبكات هي التي تسمح لتلك الأجهزة بأن تعمل بشكل جيد عادة ، لكن إذا لم تكن محمية، قد يتسبب مهاجم بتعطيلها. يمكن لخسارة الإيرادات من تلك الشبكات أن ترتفع بسرعة إذا أصبحت غير متوفرة للمستهلكين. توقف العمل هو كالخراب لأى شبكة، ويتم دائماً احتساب كلفة مقترنة بهذه الأنواع من الأحداث.

في نهاية المطاف، لدى الجميع شيء يستحق الحماية، ولا ينصح بعدم فعل ذلك؛ إنها مجرد مسألة وقت قبل أن يحصل شيء. السؤال التالي هو "ما الذي يفعله جدار النار لحماية شبكتي؟"

ما الذي يفعله لي جدار النار؟

- يفحص جدار النار مرور البيانات عند دخولها إحدى واجهاته ويطبق قواعد على حركة المرور، فيسمح أو يمنع حركة المرور بناءً على تلك القواعد ، يصفي جدار النار حركة المرور الواردة والصادرة على حد سواء.
- تستطيع جدران النار أن تصفي حركة مرور بناءً على عناوين IP المصدر / الوجهة والبروتوكول وحالة الاتصال. بمعنى آخر، قد لا تسمح عادة بدخول FTP إلى شبكتك (من خلال جدار النار)، لكن إذا بدأ مستخدم جلسة FTP من داخل شبكتك، سيسمح للجلسة لأنها بدأت من داخل الشبكة. بشكل افتراضي، تثق جدران النار بكل الاتصالات بالانترنت من الشبكة الداخلية الموثوق بها .
- بإمكان جدار النار أيضاً أن يسجل محاولات الاتصال مع بعض القواعد التي قد تصدر أيضاً إنذاراً إذا حدثت.
- أخيراً تتيح لك جدران النار تنفيذ ترجمة عناوين الشبكة (NAT) من العناوين IP الخصوصية الداخلية إلى عناوين IP عمومية.

جدران النار هي " أسلوب الأمان"

إن وجود شبكة تتصل بالانترنت من خلال جدار نار هي فقط الخطوة الأولى نحو الأمان ؛ يجب أن تعرف الآن أن أساليب الأمان تشكل الأساس لكيفية استخدام تلك القواعد.

كيف يمكن لجدار نار أن يكون أسلوب الأمان ؟ المسألة بسيطة _ فجدار النار يقوم بما يفترض أن يقوم به عن طريق إتباعه " القواعد" التي ضبطها مهندس الشبكة أو رئيس أمان المعلومات (Security Officer Information) . يجب أن تتماشى تلك القواعد بشكل مثالي مع سرد مكتوب موجود في مستند أسلوب الأمان الذي تضعه على الرف،. يجب أن يحتوى مستند أسلوب الأمان على معلومات ولائحة بقواعد الشبكة. الشيء المثير

للاهتمام هو أن كل القواعد الواردة في مستند " أسلوب الأمان " يجب ضبطها في جدار النار أيضاً .

في محاولة لتوسيع تشبيه جدار النار بـــ "أسلوب الأمان" افحص بعض النقاط الإضافية عن أسلوب الأمان وكيف يتماشى معها جدار النار:

- يبين أسلوب الأمان ما هو الإجراء الذي سيتخذ رداً على الظروف التي تنشأ .
- إن مستند أسلوب الأمان يتطور ويتغير باستمرار ليستوفي الاحتياجات الأمنية الجديدة.
- يفض أسلوب الأمان معايير الاستخدام المقبولة وغير المقبولة.

خلاصة القول أن تقتنع أن جدار النار ليس بديل لمستند أسلوب الأمان، ولكن لجعلك تفكر بالأمان كفلسفة شاملة من خطط وأساليب وأجهزة أمان. يجب أن تبذل جهداً كبيراً في التفكير بحل متكامل _ لا أن تتكل على ناحية واحدة فقط لحماية شبكتك. عندما تصبح جاهزاً لتخطيط تكوين جدار نارك وتطور القواعد التي تسمح أو تمنع حركة المرور، يجب أن تستعمل أسلوب أمانك كنقطة الانطلاق. جدران النار هي التجسيدات المادية والمنطقية لأساليب أمانك .

كيف تعمل جدران النار

معظم جدران النار (معظمها وليس كلها) يتكل علي فحص الرزم المبين للحالة **(SPI)** لتعقب أثر كل الرزم الصادرة والأجوبة التي قد تولدها تلك الرزم. تعقب أثر المضيفات على الشبكة المحمية التي تولد الرزم الصادرة يمنع رزم الشبكة **WAN** الشريرة أو التوسلية من دخول واجهة خارجية.

بمعنى آخر، جدار النار الذي يستعمل **SPI**، يراقب كل حركة المرور التي تبدأ من مضيف داخلي، ويتعقب المحادثة من ذلك المضيف إلي الوجهة الداخلية،ويضمن أن الجواب الوارد على ذلك الطلب يصل إلي المضيف الذي بدأ العملية برمتها أصلاً .

الهدف المزدوج لفحص الرزم وتصفية الرزم هو إحدى المسؤوليات الرئيسية لجدار النار. نوضح فيما يلي القواعد والميزات الأكثر شيوعاً لجدران النار:

- *صد حركة المرور الواردة إلي الشبكة بناءً على المصدر أو الوجهة* _ صد حركة المرور الواردة غير المرغوب بها هو الميزة الأكثر شيوعاً لجدار النار وهو السبب الرئيسي لاستخدام جدار نار ضد الدخول. تأتي حركة المرور غير المرغوب بها هذه من المهاجمين عادة،لذا نحتاج إلى إبقائها خارجاً .
- *صد حركة المرور الصادرة من الشبكة بناءً على المصدر أو الوجهة* _ بإمكان جدران نار عديدة أن تغربل أيضاً حركة المرور الصادرة من شبكتك الداخلية إلى الانترنت.مثلاً، تريد منع الموظفين من الوصول إلى مواقع الويب الهدامة أو الإباحية .
- *صد حركة المرور في الشبكة بناءً على المحتوى* _ بإمكان جدران النار المتقدمة أكثر أن تغربل حركة المرور في الشبكة بحثاً عن محتويً غير مقبول. مثلاً،بإمكان جدار النار المندمج مع مضاد الفيروسات أن يمنع الملفات التي تحتوي على فيروسات من أن تدخل شبكتك. وتندمج بقية جدران النار مع خدمات البريد الإلكتروني لاستبعاد البريد الإلكتروني غير المقبول .
- *جعل الموارد الداخلية متوفرة* _ رغم أن الهدف الرئيسي لجدار النار هو منع حركة المرور غير المرغوب بها من عبور الشبكة، يمكنك أيضاً ضبط تكوين العديد من جدران النار للسماح بوصول انتقائي إلى الموارد الداخلية، كخادم ويب عمومي، مع استمرار منع محاولات الوصول الأخرى من الانترنت إلى شبكتك الداخلية.
- *السماح بالاتصالات إلي الشبكة الداخلية* _ هناك طريقة شائعة لكي يتصل الموظفون بشبكة وهي استعمال الشبكات الخصوصية الوهمية (الشبكات **VPN**). تتيح الشبكات **VPN** إنشاء اتصالات آمنة من الانترنت إلي شبكة شركة. مثلاً، بإمكان المتصلين عن بعد ومندوبي المبيعات المسافرين أن يستعملوا شبكة **VPN** ليتصلوا بشبكة الشركة. بإمكان الشبكات **VPN** أيضاً أن تربط مكاتب الفروع

ببعضها البعض. يتضمن بعض جدران النار وظائف الشبكة **VPN** ويسهل إنشاء الاتصالات .

VPN اختصاراً للعبارة **Virtual Private Network** "شبكة ظاهرية خاصة" وهي شبكة يتم تأسيسها عبر خطوط هاتف رقمية، ويتم تخصيصها فقط للاتصال بمواقع وحدات تابعة محددة متعددة. يتم استخدام هذه الشبكة لتنفيذ شبكات **WANs** باستخدام الانترنت لإنشاء شبكة شبه خاصة.

- *التبليغ عن حركة المرور في الشبكة وسجلات النار* _ عند غربلة حركة المرور في الشبكة إلى ومن الانترنت، من المهم أيضاً أن تعرف ما الذي يفعله جدار نارك، ومن حاول اقتحام شبكتك، ومن حاول الوصول إلى مواد غير ملائمة على الانترنت، يتضمن معظم جدران النار آلية تبليغ من نوع أو من آخر . بإمكان جدار النار الجيد أيضاً أن يسجل النشاطات في **Syslog** (سجل نظام) أو نوع آخر من وعاء التخزين الأرشيفي. دراسة سجلات جدار النار بعد حصول هجوم هي واحدة من الأدوات الجنائية العديدة التي تتوفر بين يديك.

جدران النار أثناء عملها

من المهم الإشارة إلى أن عدة جدران نار تحتوى واجهتين ماديتين، و99 بالمئة منها ترتكز على الإيثرنت. تلك الواجهات تسمى الداخل (المحمية) والخارج (غير المحمية) ويتم نشرها بالنسبة لشبكتك. لذا عملياً، تتصل الواجهة الخارجية بالانترنت وتتصل الوجهة الداخلية بشبكتك الداخلية:

١) يفتح المضيف أ، مستعرض ويب ويرغب بمعاينة صفحة ويب. يرسل المضيف أ الطلب عبر جدار النار.

٢) يرى جدار النار الطلب الذي بدأ من المضيف أ والذي يتوجه إلى موقع الويب أ. يلاحظ جدار النار الطلب الصادر ويتوقع أن الرد سيأتي فقط من خادم

الويب.

ب. توضع علامة جلسة في جدول حالة الجلسات التابع لجدار النار الذي سيتعقب عملية الاتصال من بدايتها إلى نهايتها .

ج. توضع أيضاً قياسات مترية للاتصال في العلامة التي يحافظ عليها جدار النار لهذه المحادثة.

٣) الرد على طلب المضيف أ لرؤية صفحة الويب يُرسل من خادم الويب إلي المضيف أ عبر جدار النار .

٤) يفحص جدار النار جدول حالة جلساته ليرى إن كانت القياسات المترية التي يحتفظ بها لهذه الجلسة تطابق الاتصال الصادر أم لا. إذا كانت كل تفاصيل الاتصال المخزنة تطابق تماماً، يسمح جدار النار بحركة المرور الواردة.

فكر بمسألة واحدة أخيرة تتعلق بجدران النار المبينة للحالة بشكل عام. إذا كان جدار النار يحافظ على سياق حالة الاتصال المتعلقة بالاتصالات الواردة والصادرة، سيصبح من الصعب أن يتمكن قرصان من "تزوير" رزمة بقصد اختراق شبكتك. عندما يحاول المهاجمون إرسال رزم لعبور جدار نار فإن وجود معلومات غير صحيحة عن حالة الاتصال أو عدم وجودها على الإطلاق يعني أن الجلسة ستغلق وعلى الأرجح أنها ستدون لمراجعتها لاحقاً .

أنواع جدران النار

تأتي الكمية الهائلة من جدران النار المتوفرة هذه الأيام في أشكال وأحجام وأصناف عديدة. نوع جدار النار الذي تثبته يعتمد على متطلباتك الدقيقة للحماية والإدارة، وكذلك على حجم شبكتك أو ما الذي سيحميه جدار النار. تقع جدران النار عادة في إحدى الفئات التالية:

جدار النار الشخصي ــ جدار النار الشخصي هو عادة برنامج يثبت في كمبيوتر واحد لحماية ذلك الكمبيوتر فقط. هذه الأنواع من جدران النار توضع عادة في الكمبيوترات المنزلية مع الاتصالات العريضة النطاق أو الموظفين البعيدين. بالطبع، كلما أراد شخص نشر جدار نار، يعتبر هذا جيداً.

لقد استجاب صانعو أنظمة التشغيل كشركة أبل ومايكروسوفت لهذه الحاجة وقاموا بدمج جدران نار شخصية فيها. تأتي نظم التشغيل الحديثة مثل **Windows XP/Vista** ومعها جدار نار.

جدار النار المتكامل : هذه الأنواع من جدران النار يستعملها بشكل واسع المشتركون بالاتصال العريض النطاق (الكبل أو **DSL**) الذين يستفيدون من وجود جهاز واحد يقدم الميزات والوظائفية التالية: موجه،بدالة إيثرنت، نقطة وصول لاسلكي، وجدار نار. إذا كان هذا النوع من جدران النار يعجبك، الرجاء التأكد من تحديد قدرات جدار النار بعناية، وكن شكاكاً بالأمان الذي يمكنك اكتسابه من تلك الأجهزة بغض النظر عمن يصنعها .

جدران نار المكاتب الصغيرة إلي المتوسطة : جدران النار هذه، مصممة لتزويد أمان وحماية للمكاتب الصغيرة.

جدران نار الشركات : جدران النار هذه، كسيسكو **PIX 515**، مصممة للمؤسسات الكبيرة التي تضم آلاف المستخدمين، تتضمن ميزات وسعة إضافية، كذاكرة أكثر وواجهات إضافية.

ستشغّل كل جدران نار سيسكو نفس إصدار نظام التشغيل الذي يتضمن نفس قدرات التبليغ والإدارة بغض النظر عن الطراز . ستكون الطُرز الأكبر مطلوبة عندما تكون هناك طلبات لكميات أكبر من الاتصالات والسعة.

عادة يتم تثبيت جدار النار حيث تتصل شبكتك الداخلية بالانترنت. رغم أن المؤسسات الكبيرة تضع أيضاً جدران نار بين مختلف أجزاء شبكتها الداخلية التي تتطلب مستويات مختلفة من الأمان، إلا أن معظم جدران النار تغربل حركة المرور التي تمر عبرها بين الشبكة الداخلية والانترنت. مثلاً، إذا كانت مؤسسة كبيرة تتيح لشركائها المهنيين الاتصال بشبكتها مباشرة، ستجد عادة جدار نار يتحكم بما هو مسموح في شبكة المؤسسة من شركائها. إن وضع جدار نار داخلي بهذه الطريقة يعتبر بالتأكيد شيئاً جيداً .

ملخص الفصل

ناقشنا في هذا الفصل واحدة من أهم وأشهر الوسائل لحماية الشبكة وتأمينها. شرحنا ما الذي يجب أن يفعله جدار النار ومن يحتاج إليه ولماذا تحتاج إليه. ناقشنا كذلك كيف يمكن لجدار النار أن يكون أسلوب أمان وكيف يعمل .

أخيراً ناقشنا كيفية تطبيق جدار النار وأنواع جدران النار.

تدريبات

١. هل نحتاج إلي جدار النار ؟

٢. من يحتاج جدار النار؟

٣. لماذا نحتاج إلي جدار النار؟

٤. كيف يكون جدار النار ملحقاً لأسلوب الأمان ؟