الفصل التاسع:
أمن المنظومة الشبكية
Network Systems Security

الكلمات المفتاحية:

مجموعات المستخدمين، ولوج، عنصر فاعل، غرض غير فاعل، مرجع، لائحة التحكم بعمليات الولوج إلى الغرض، سجلات تسجيل دورية، محللات سجلات التسجيل، نسخ احتياطي ساخن.

ملخص الفصل:

يتعرف الطالب في هذه الفصل على المبادئ الرئيسية للتخطيط لأمن المنظومة الشبكية، وأهم أنواع جدران النار المستخدمة لحماية الشبكات المتصلة بالإنترنت.

الأهداف التعليمية:

يتعرف الطالب في هذا الفصل على:

- الاستراتيجيات الرئيسية لبناء منظومة معلوماتية آمنة
- عناصر الخطة الأمنية الضرورية لتأمين المنظومة الشبكية
- جدران النار

مخطط الفصل:

1. استراتيجيات بناء منظومات آمنة Strategies of Building Secure Systems
   - 1.1. التأمين الفيزيائي للشبكة Network Physical Security
   - 2.1. تصنيف المعلومات Information Classification
   - 3.1. تحديد مهمة كلّ حاسب وتوثيق الهدف من استعماله Identifying& Documenting each Computer Tasks
   - 4.1. تحديد الخدمات الشبكية التي يقدمها كل حاسب Identifying Network Services Computer for every
   - 5.1. تأمين حسابات المستخدمين Securing Users Account
   - 6.1. إدارة أمن المستخدم Managing User Security
   - 7.1. تطوير آليات مساعدة على تحسس الاختراق الأمني Developing Helping Techniques for Identifying Security Breaches
   - 8.1. استخدام النسخ المُحدَّثة من الأنظمة البرمجية Using Software Updates
   - 9.1. تأمين مستخدمي الشبكة Securing Network Users
   - 10.1. استمرار الخدمة عند الأعطال Service Continuation on Faults
   - 11.1. معالجة الأجهزة المنسقة Processing Obsolete Components
2. جدران النار Firewalls
   - 1.2. مفلترة الرزم Packet Filtering
   - 2.2. فحص الرزم ذو الحالة SPI Stateful Packet Inspection
   - 3.2. بوابات مستوى الدارة Circuit-Level Gateway
   - 4.2. بوابة التطبيقات Application Gateway

1. استراتيجيات بناء منظومات آمنة (Strategies of Building Secure Systems):

أصبح واضحاً في أيامنا هذه أن بناء منظومة آمنة هو أحد أهم أسباب النجاح على المدى البعيد لأي منظومة شبكية. هناك عدة عوائق يمكن لها أن تعترض تطبيق آليات الأمان للمنظومات، منها أن الأمن غير مريح للموظفين الذين يعملون في الشركة لكونها تتطلب إجراءات إضافية تزداد حدتها بزيادة إجراءات الأمان المطلوبة، من التخويل عبر كلمات السر، إلى تشفير المعلومات الموجودة على أقراص التخزين وحتى المحلية منها. وينظر الكثيرين على أن هذه الإجراءات تخفّض من إنتاجية المؤسسة، ولكن يمكن أن يعوض هذا التخفيض بزيادة مستويات الأمان فيها.

وقد كان يعتبر أمن الحاسب موضوعاً سهلاً قبل انتشار الشبكات الحاسوبية، جل ما يتطلبه هو قفل الأبواب جيداً بعد انتهاء العمل. ولكن غيرت الشبكة هذا المفهوم بشكل كبير، فيمكن الآن لأي من يملك نفاذاً إلى أي حاسب على الشبكة، أن يصل إلى جميع الملفات والمعطيات المتواجدة في المنظومة الشبكية. لذلك تم تصميم أنظمة التشغيل الشبكية على أن تتضمن خدمات تؤمن سرية الشبكة. وإذا ما كانت الشبكة متصلة بالإنترنت فعلى مدير النظام تأمينها ضد التطفل عبر الإنترنت أيضاً.

عادة ما يتم إتباع المقاربات التالية عند التخطيط لتطبيق الأمن على الشبكة:

- استراتيجية الباب المفتوح: والتي تؤمن للجميع النفاذ إلى كل شيء مبدئياً، ومن ثم يتم تطبيق القيود على الموارد التي تتطلب نفاذاً محدوداً. وعادة ما تكون الأسهل للتطبيق، ويكون فيها حجماً صغيراً من معطيات الشبكة يحتاج فعلاً إلى أمان، مثل سجلات الموظفين، ومالية الشركة. ويمكن وضع المعطيات الأخرى بأن تكون متاحة للجميع.
- استراتيجية الباب المغلق: والتي تبدأ بمنع النفاذ لكل شيء في المنظومة، ومن ثم تبدأ بمنح سماحية نفاذ لمستخدمين معيين إلى موارد محددة بحسب حاجتهم. تنتج هذه السياسة أمناً وثيقاً ولكنها تشعر مستخدمي الشبكة بعدم الراحة بسبب الإجراءات المتعددة المطلوبة وعدم تمكنهم من الوصول في أكثر الأحيان إلى المعلومات التي يطلبونها.

لذلك من المهم أن يقوم القيمين على المنظومة الشبكية باتخاذ التدابير اللازمة لتأمين أمن المنظومة الشبكية ووضع الخطة الأمنية المناسبة. تتضمن هذه الخطة اعتبار أمن عدد من العناصر الأساسية في الشبكة مثل العتاديات ومكونات الشبكة، المعطيات ومعلومات المخزنة والمتناقلة عير الشبكة وبرمجياتها، وتحدد عناصر الخطة الأمنية بالمحددات التالية:

1. التأمين الفيزيائي للشبكة.
2. تصنيف المعلومات.
3. تحديد مهمة كلّ حاسب في المنظومة الشبكية وتوثيق الهدف من استعماله.
4. تحديد الخدمات الشبكية التي يقدمها كل حاسب.
5. تأمين حسابات المستخدمين.
6. إدارة أمن المستخدم.
7. تخطيط الوصول إلى مصادر المعلومات و موارد المنظومة.
8. تطوير آليات مساعدة على تحسس الاختراق الأمني.
9. استخدام النسخ المُحدَّثة من الأنظمة البرمجية.
10. تحديد الأساليب التي تكفل استمرار خدمات المنظومة في العمل عند الأعطال، وكيفية استعادة هذه الخدمات.
11. تأمين مستخدمي الشبكة.
12. تحديد العمليات اللازمة لحماية المعلومات المحتواة في الأجهزة المنسقة.

1.1. التأمين الفيزيائي للشبكة (Network Physical Security):

وهو مستوى الأمان الأول في الشركات حيث يتم تأمين حماية المخدمات فيزيائياً عبر:

- قفل غرفة الحواسيب
- إعطاء المفاتيح لمن هم موثوقون فقط
- تتبع وتعقب من يحصل على نسخ من المفاتيح
- رفع المخدمات على خزن أو على رفوف تحتوي على أقفال
- إلغاء سواقة الأقراص المرنة من على المخدمات

كذلك يمكن تأمين محطات العمل فيزيائياً عبر:

- تعليم المستخدمين بعدم ترك الحواسب قيد العمل من غير مراقبة
- يجب تأمين الحاسب عبر قفل لوحة المفاتيح في المناطق العمل عالية الازدحام (مثل مكاتب الاستقبال)
- وكذلك على المستخدمين قفل أبوابهم عند الخروج من المكاتب

2.1. تصنيف المعلومات (Classification of Information):

تطبق الكثير من المؤسسات الكبيرة الحجم سياسة تصنيف لمعلوماتها. تساعد هذه السياسة على تقسيم المعلومات التي تتعامل بها المؤسسة إلى كتل تتصف كلٍ منها بمستوى سرية محدد. تؤدي هذه السياسة إلى زيادة صعوبة الوصول إلى المعلومات بشكل عام، وتساعد على فرض استراتيجية محددة لوصول المستخدمين المحددين إلى مصادر المعلومات وإلى موارد المنظومة. مما يقلل من الأخطار التي تنتج عن حصول الفرد على معلومات زائدة لا حاجة له بها. تندرج عملية التصنيف ضمن القاعدة الأساسية (need to know)، حيث يحصل المستخدِم على المعلومات اللازمة لعمله فقط لا غير.

3.1. تحديد مهمة كلّ حاسب وتوثيق الهدف من استعماله (Identifying and Documenting each Computer Tasks):

يتم ذلك باعتبار النقاط التالية:

- تحديد أصناف المعلومات التي ستخزن على الحاسب.
- تحديد أصناف المعلومات التي ستجري معالجتها على الحاسب (دون أن يتم، بالضرورة، تخزينها على الحاسب الذي يعالجها).
- تحديد متطلبات الأمن الخاصة بالمعلومات المخزنة وبالمعلومات المُعالَجة. وتحديد سماحيات القراءة، التعديل، والكتابة لهذه المعلومات من قبل مستخدمي المنظومة الشبكية.
- تحديد الخدمات الشبكية التي سيقدمها الحاسب.
- تحديد متطلبات الأمن الخاصة بالخدمات الشبكية. من يستطيع الاستفادة منها؟ من يستطيع تشغيلها وإيقافها؟

4.1. تحديد الخدمات الشبكية التي يقدمها كل حاسب (Identifying Network Services of every Computer):

تتضمن الخدمات الشبكية خدمة البريد إلكتروني، أو خدمة الويب، أو خدمة حلّ أسماء النطاقات، أو خدمة نقل الملفات، أو برامج التعامل مع قواعد بيانات المؤسسة. ولتأمين طريقة التعامل مع هذه الخدمات يجب، ومن أجل كل خدمة يتم تثبتها على الشبكة، تحديد وتوثيق نمط العمل في الحاسب، فيما إذا كان سيعمل كزبون، أو مخدم أو بنمط كل من زبون ومخدم في آن معاً.

بشكل عام، يتم إعداد محطات العمل لتعمل كزبائن لمعظم الخدمات الشبكية. لذا علينا تحديد نمط استخدام الخاص لهذه المحطات وجعله ينعكس على مستخدميها وتحديد مستويات الوصول المطلوبة إلى كل خدمة. ويمكن أن يتم ذلك عبر تحديد:

- استخدام دون صلاحية الإدارة
- إدارة عن بعد اعتباراً من محطات محددة
- إدارة محلية اعتباراً من المحطة نفسها فقط

أما المخدمات، فيتم تكريس كلٍ منها، بشكل عام، ليعمل كمخدِّم لخدمة واحدة. يبسّط هذا الأسلوب عادةً، عمليات إعداد المخدِّم ويخفّض من إمكانية الوقوع في الأخطاء عند إعداد الخدمة. كما يساعد على إزالة التداخلات غير المتوقّعة وغير الآمنة بين مختلف الخدمات، إذ توفر هذه التداخلات أرضاً خصبةً للدخلاء والمتطفلين.

من جهة أخرى، قد يكون من الملائم في بعض الحالات تثبيت أكثر من خدمة واحدة على مخدم رئيسي واحد. فعلى سبيل المثال، يقوم العديد من الموزعين بدمج خدمة نقل الملفات مع خدمة النقل الخاصة بالويب، ضمن رزمة واحدة. لذا قد يكون من المناسب لبعض المؤسسات، توفير عمليات الوصول إلى معلوماتها العامّة عن طريق كلا الخدمتين رغم عدم توافق هذا الأسلوب مع المعايير الأمنية الدقيقة.

5.1. تأمين حسابات المستخدمين (Securing Users Accounts):

يمكن لحسابات المستخدمين المهيأة بطريقة صحيحة أن تمنع المستخدمين غير المخولين من النفاذ إلى الشبكة، حتى إذا تمكنوا من الوصول الفيزيائي إليها.

هناك عدد من المهمات الواجب إتباعها لتأمين حسابات المستخدمين:

1. استخدام أسماء غير اعتيادية أو سهلة التخمين:

مثلاً عبر:

- إضافة أرقام عشوائية إلى نهاية الاسم
- إضافة رقمين بين محارف الاسم
- والتأكد من أن أسماء حسابات المستخدمين هي مختلفة عن أسماء البريد الالكتروني

2. استخدام كلمات المرور:

إن اسم حساب المستخدم هو عملياً غير سري، ولكن كلمة المرور هي سرية. وهناك بعض الطرق لزيادة تأمينها منها:

- عدم استخدام كلمات السر الواضحة أو سهلة التخمين.
- عدم انتقاء كلمات السر تبعاً لهوايتك المفضلة.
- تخزين كلمات المرور عبر حفظها، وليس بكتابتها على الورق ووضعها في أماكن واضحة.
- تمكن معظم أنظمة التشغيل الشبكية من وضع مدة صلاحية لكلمات المرور وبهذا تجبر المستخدمين على تغييرها دورياً.
- كذلك يمكن تهيئة حسابات المستخدمين بطريقة تمنع المستخدمين من اختيار متكرر لكلمات مرور تم استخدامها مؤخراً.
- تهيئة سياسة الأمان بطريقة تجبر أن تكون كلمات المرور المختارة من المستخدمين هي معقدة، مثل استخدام مزيج من المحارف الكبيرة والصغيرة والأرقام والمحارف الخاصة.

3. تأمين حساب مدير النظام:

عادة يكون لمدير النظام كامل السماحيات والصلاحيات لاستخدام الشبكة دون أي قيود، كون هذا المدير مسؤولاً عن تثبيت نظام امن الشبكة. تنشئ معظم الشبكات حساب مدير النظام عند تثبيت برمجيات الشبكة، وينشر اسم هذا الحساب وكلمة مروره ضمن وثائق الشبكة وتكون متطابقة لكافة النسخ المباعة. لذلك من المهم جداً تغيير اسم حساب مدير النظام وكلمة مروره عند البدء باستعمال الشبكة. على مدير النظام الاحتفاظ بمكان آمن بهذه المعلومات لأن نسيان كلمة سر مدير النظام يضع الشبكة في مأزق.

6.1. إدارة أمن المستخدم (Managing User Security):

وتتضمن عدداً من المهمات منها:

- **حسابات المستخدمين:**

تعتبر حسابات المستخدمين العمود الفقري لإدارة امن الشبكة. يمكن لمدير الشبكة تحديد هوية من يمكن له النفاذ إلى هذه الشبكة، وكذلك إلى مواردها، وأي موارد يمكن لمستخدم النفاذ إليها. يمكن كذلك وضع قيود على الموارد المستخدمة من حيث نوعية العمل على هذه الموارد والوقت المسموح فيه النفاذ إليها.

وتتضمن حسابات المستخدمين معلومات مرتبطة معها من أهمها:

- كلمة مرور المستخدم: وتتضمن سياسة كلمة المرور مثل كيفية انتقاء كلمة المرور، ودورية تغييرها، ... الخ.
- معلومات الاتصال بالمستخدم: وتتضمن كامل الاسم، ورقم الهاتف والمعلومات الأخرى المتعلقة.
- قيود الحساب: وتتضمن القيود المفروضة على المستخدم للنفاذ إلى الشبكة ضمن فترات زمنية محددة من النهار، وتسمح هذه الخاصية بمنع المستخدمين من النفاذ إلى الشبكة خارج أوقات العمل الرسمي إذا لم يكونوا بحاجة لذلك.
- حالة الحساب: يمكن تعطيل حساب مستخدم مؤقتاً فلا يمكن للمستخدم الولوج إلى الشبكة.

- **الحسابات المضمنة (Built-in):**

تأتي معظم أنظمة تشغيل الشبكية مع حسابين مضمنين هي مدير النظام والضيف. كذلك تنشأ بعض خدمات المخدمات مثل مخدمات الويب وقواعد البيانات حسابات المستخدمين الخاصة بها للعمل. هذه الحسابات لها المواصفات التالية:

- حساب مدير النظام: بما أن هذا الحساب لا يحتوي على أية قيود ويمكنه عمل ما يريد على الشبكة، لذلك يفضل عادة تجنب استخدامه للمهمات الاعتيادية في الشبكة. كذلك يجب تأمين هذا الحساب في اللحظة التي يتم فيها الانتهاء من تثبيت المخدم. وعندما يطلب برنامج تثبيت نظام التشغيل الشبكي كلمة المرور لحساب مدير النظام على من يديرهذه العملية اختيار كلمة مرور تتبع القواعد المعروضة مسبقاً مباشرة من انتقاء مزيج معقد لها.
- حساب الضيف: ويتم إنشاء هذا الحساب بكلمة مرور فارغة وكذلك دون سماحيات نفاذ أو بسماحيات محدودة جداً من قبل النظام. هذا الحساب مصمم للسماح لأي شخص بالنفاذ إلى حاسب ما ولكن دون سماحيات أخرى.
- حسابات الخدمة: بعض مستخدمي الشبكة هم ليسوا أشخاصاً بل يمكن لإجراءات برمجية أن تتطلب نفاذاً إلى الشبكة أو لبعض الموارد فيها، ولذلك تتطلب إنشاء بعض حسابات مستخدمين. وعادة ما يتم إنشاء هذه الحسابات أوتوماتيكياً عند تثبيت البرامج أو تهيئة برامج المخدمات. من الأمثلة على هذه الحسابات الحساب (IUSR) المنشأ عند تثبيت مخدم الويب من ميكروسوفت (IIS). ويستخدم مخدم الويب هذا الحساب للسماح لمستخدمي إنترنت غير معروفين بالنفاذ إلى الملفات على صفحة الويب الخاصة بالنظام.

- **حقوق المستخدمين:**

يمكن إعطاء بعض الحقوق لكافة مستخدمي الشبكة بناءاً على نظام التشغيل الشبكي المستخدم. تعطي مخدمات الويندوز حقوقاً للمستخدمين من بعضها: الولوج المحلي إلى الشبكة، وتغيير زمن النظام، إنهاء أو إيقاف النظام، نسخ الملفات أو المكتبات احتياطياً، استعادة الملفات أو المكتبات المنسوخة احتياطياً.

- **السماحيات:**

تحدد حقوق المستخدمين ما يمكن لمستخدم فعله على مستوى الشبكة. أما السماحيات فتمكّن من التحكم بالنفاذ إلى موارد الشبكة المحددة مثل الملفات أو الطابعات ولكل من المستخدمين الفرديين أو مجموعات المستخدمين. كذلك تمكن السماحيات المستخدم من قراءة بعض الملفات ولكن دون الكتابة عليها أو تعديلها. يدير كل نظام تشغيل شبكي السماحيات بطريقة مختلفة. ولكن بغض النظر عن التفاصيل فإن التأثير هو إمكانية إعطاء السماحيات لكل مستخدم للنفاذ إلى الملفات، المجلدات، أو السواقات بطريقة معينة. إن أي سماحية توضع على مجلد هي نافذة على كل المجلدات الجزئية الموجودة ضمن المجلد الرئيسي، إلا إذا تم تحديد سماحيات مختلفة على مستوى المجلدات الفرعية. يمكن في أنظمة الويندوز استخدام السماحيات فقط للملفات أو المجلدات التي تم إنشاؤها على سواقات مهيأة كـ (NTFS) أو (ReFS). ولا يمكن حماية الملفات أو المجلدات في السواقات التي تستخدم التهيئة بنظام (FAT) أو (FAT32) وهذا من أهم أسباب استخدام (NTFS) لمخدمات الويندوز.

- **مجموعات المستخدمين:**

يمكن بسهولة تحديد مستخدمي محطة عمل أو مخدِّم. لكننا في أغلب الأحيان، نحتاج لتحديد المجموعات التي يحق لها استخدام المحطة أو المخدِّم، حيث تعتبر المجموعات الأداة الرئيسية في إدارة الشبكة، فهو يسهل وينظم عمل مدير النظام ويختصر زمن الإدارة. ويمكن لمستخدم الانتماء إلى أكثر من مجموعة واحدة في نفس الوقت. ويهدف تعريف مجموعات المستخدمين إلى:

  - حصر صلاحية استخدام الحاسوب بالمجموعات المُعرَّفة.
  - تحديد صلاحيات كل مجموعة من المجموعات التي يحق لها استخدام الحاسوب.
  - عدم السماح لمستخدم عادي ليس له صلاحية مدير نظام تشغيل أو مدير شبكة، بالعمل على مخدِّم.

يتم إعطاء سماحيات النفاذ على مستوى المجموعة بدلاً من المستخدمين فرادى. ويُحدد مدير المنظومة المجموعات العاملة لديه إما بطريقة مركزية وعلى مخدِّم مركزي يحوي قاعدة بيانات مستخدمي المنظومة المعلوماتية، أو أن يكون التعريف لا مركزياً على كل حاسوب على حدا.

لا يؤثر وجود سماحيات متناقضة على أداء النظام، إذ تفترض القاعدة العامة المُطبقة في معظم نظم التشغيل على أن الغرض يتعامل مع العنصر بالسماحيات الأقل. فعلى سبيل المثال، يستطيع أعضاء المجموعة (Accounting) قراءة وتعديل المجلد A، إلا أن العضو x1 من(Accounting) لا يحق له النفاذ إلى A. وبالتالي حسب السماحية الأقل لا يسمح للعنصر x1 بالوصول إلى A.

تقنياً، يجري تعريف المستثمرين وصلاحياتهم اعتماداً على خدمات قياسية مثل خدمة الدليل، والتي يُعتبر البروتوكول (Lightweight Directory Access Protocol–LDAP) أحد أكثر عناصرها شهرةً، مما يساعد في بناء قاعدة بيانات مركزية لتعريف مستثمري المنظومة المعلوماتية وفي التحقق من هوياتهم مركزياً.

- **تأمين الولوج عبر المخدمات:**

باستخدام تسجيل الدخول النصي (Logon Scripts) الذي هو عبارة عن ملف دفعي ينُفذ أوتوماتيكياً كلما يلج المستخدم إلى الشبكة. يقوم هذا الملف بعدد من المهمات الأساسية مثل إسقاط سواقات الشبكة، بدء التطبيقات، مزامنة حواسيب الزبائن مع الساعة المحلية، ... الخ. تكون هذه الملفات متوضعة على المخدم ويمكن تحديد لكل حساب مستخدم إذا ما كان يستخدم تسجيل دخول نصي أم لا، وأي نص يستخدم. يبين الشكل التالي تسجيل دخول نصي بسيط يقوم بإسقاط عدد من سواقات الشبكة ويزامن الزمن.

```
net use m: \\MYSERVER\Acct
net use n: \\MYSERVER\Admin
net use o: \\MYSERVER\Dev
net time \\MYSERVER /set /yes
```

الشكل (1): نموذج بعض أوامر ملف التسجيل الدخول النصي

7.1. تطوير آليات مساعدة على تحسس الاختراق الأمني (Developing Helping Techniques for Identifying Security Breaches):

يمكن لجميع نشاطات الشركة أن تكون مُراقبة بطريقة مستمرة بوساطة حلولٍ لوجستية متخصصة. ولكن يكون تدفق المعلومات المتولدة عن هذه الوسائل كبير جداً، مما يتطلب ترشيح المعلومات المجمّعة من هذه الحلول للإبقاء على الهامة منها فقط. كما يمكن تسجيل هذه المعلومات وتحليلها مع الزمن، كما هو الحال عندما نحتاج تسجيل نشاط كل موظف خلال فترة زمنية محددة. تعتمد العديد من طرق تعقّب المتطفلين على وجود سجلات تسجيل لمختلف البرمجيات والأنظمة العاملة، وعلى توفر الأدوات اللازمة لمراجعة هذه السجلات وتحليلها. لذا يجب أن نحدد في خطة نشر المنظومة المعلوماتية، ماهية المعلومات التي نريد تسجيلها عند تشغيل البرامج والأنظمة المختلفة، وأماكن التسجيل.

تكون أنظمة التسجيل عادةً، مرافقة لنظم التشغيل أو مرافقة للبرمجيات، وذلك تبعاً لتعقيد هذه البرمجيات. فعلى سبيل المثال، تمتلك أنظمة البريد الإلكتروني برامج تسجيل خاصة بها، يكون إعدادها جزءاً من إعداد نظام البريد. في حين لا تمتلك برامج مكتبية عادية مثل معالجات النصوص مثل هذه الأدوات. عندها يمكننا، على سبيل المثال، تسجيل عمليات الوصول وعمليات استخدام مثل هذه البرامج، اعتماداً على نظام التسجيل الخاص بنظام التشغيل الذي يعمل به الحاسب.

8.1. استخدام النسخ المُحدَّثة من الأنظمة البرمجية (Using Software Update):

يصعِّب تعقيد الأنظمة البرمجية من عملية اختبارها. فعند اكتشاف ثغرات ضمن أنظمة برمجية قيد التوزيع والاستثمار، يعمل مطوروها على تطوير نسخ مُحدَّثة أو برامج تصحيح تساعد على إصلاح هذه الثغرات والأخطاء.

ويحاول المطورون توزيع النسخ المُحدَّثة أو برامج التصحيح على نحوٍ واسع يضمن حلّ المشاكل على أوسع نطاق. لذا يجب أن يكون المسؤولون عن بناء المنظومة المعلوماتية، على اطلاع على آخر التحديثات التي جرت على الأنظمة والبرمجيات التي يحتاجونها، لتثبيت المُحدَّث منها. فعلى سبيل المثال، تضمن شركة (Microsoft) لزبائنها، الحصول على برامج خاصة تساعد على تصحيح أخطاء أنظمة التشغيل التي تسوقها وعلى تصحيح أخطاء أنظمتها البرمجية المختلفة (مجموعة Office، أو أداة تصفح المواقع مثل Internet Explorer، ... أو غيرها)، بشكل مجاني اعتباراً من موقعها على شبكة الإنترنت، كما تقدم آخر النصائح في مجال تحصين الأنظمة والبرامج التي تطورها وتوزعها الشركة.

9.1. تأمين مستخدمي الشبكة (Securing Network Users):

إن كافة القواعد الأمنية المحددة في الفقرات السابقة تعتبر سهلة بالمقارنة مع تأمين سلوكيات مستخدمي الشبكة، أو ما يدعى بالقواعد السلوكية الأساسية. تعتبر القواعد السلوكية لموظفي المؤسسة إحدى الضمانات الرئيسية لنجاح مخطط الأمن المعلوماتي. إذ تحدد المؤسسات عدة قواعد لتنظيم سلوك موظفيها. ويفضل عادة كتابة هذه القواعد وتسليمها لكافة مستخدمي الشبكة والتأكد من مراعاتها من قبلهم. من أهم هذه القواعد:

- عدم كتابة كلمات المرور في الأماكن الواضحة والعامة (لصقها على شاشة الحاسب مثالاً)
- عدم مشاركة الحسابات
- عدم إعطاء معلومات الحساب لزملاء عاملين في الشركة
- عدم تثبيت أي برمجيات أو عتاديات على الحاسب دون الحصول على الإذن اللازم لذلك
- عدم تمكين مشاركة الملفات والطابعات على محطات العمل دون الحصول على الإذن
- عدم محاولة إبطال أو تجاوز ميزات أمن الشبكة
- عدم فتح رسائل البريد الإلكتروني/المرفقات الواصلة من أشخاص غير معروفين
- عدم استخدام وسائط التخزين الخارجية (مثل Flash Memory) قبل فحصها باستخدام برامج مكافحة الفيروسات

في ذات السياق، تفرض المؤسسات مبدأ "المكتب الخالي" الذي يحتِّم على الموظف أن يترك مكتبه خالٍ من أي ملف عندما يترك عمله. كما تفرض على الموظفين أصحاب الحواسب النقالة أن يضعوا عدة مستويات من الحماية وكلمات السر على الحاسب النقال (عند تشغيل الجهاز، عند شاشة التوقف، ... وغيرها).

تُعتبر جميع القواعد السلوكية السابقة أساسية لحماية الأنظمة المعلوماتية. وعلى الرغم من كونها بديهية، إلا أنها تكون مهملة في أغلب الأحيان. لقد أظهرت الإحصاءات أن أكثر من 70% من الاختراقات سببها إهمال هذه القواعد السلوكية وخصوصاً القواعد المتعلقة بكلمات السر، وأن أكثر من 50% من الاختراقات الناتجة عن اكتشاف كلمة السر لم تنتج عن عدم وضع كلمة سر ولكن عن نشرها عن غير قصد في أماكن عامة.

10.1. استمرار الخدمة عند الأعطال (Service Continuation on Faults):

لضمان توفر الخدمات في منظومتك، تحتاج إلى مستويات مختلفة من النسخ الاحتياطي لهذه الخدمات وللمعطيات التي تتعامل بها، تبعاً لتأثيرها على عمل المؤسسة:

1. **تحديد الخدمات التي تتمتع بنسخ احتياطي ساخن (Hot Backup):**

مما يعني قدرة المنظومة على العمل آنياً مع الخدمة الاحتياطية، لأن هذه الخدمة تعمل بالأساس على التوازي مع الخدمة الأصلية. كمثال على ذلك هي خدمة حلّ نطاقات الأسماء (DNS) لدى مزودي الخدمة، والتي تتمتع عادةً بنسخ احتياطي ساخن يحتم وجود مخدم رئيسي ومخدم احتياطي يعملان بآنٍ واحد. كما يحتم إعداد الحواسيب التي تستعمل هذه الخدمة على نحو يسمح لها بالاعتماد على كلا المخدمين على نحو متناظر.

2. **تحديد الخدمات التي تتمتع بنسخ احتياطي عادي (Worm Backup):**

مما يعني قدرة المنظومة على العمل مع الخدمة الاحتياطية بعد فترة وجيزة وبعد القيام بإعدادات بسيطة. يمكن تطبيق هذا النوع من النسخ الاحتياطي على مخدِّمات الويب أو البريد الإلكتروني في حال كان العمل في الشركة يحتمل توقف التعامل معهما لفترة بسيطة لا تتجاوز الساعات، وإلا وجب اعتماد النسخ الاحتياطي الساخن لهذه الخدمات.

3. **تحديد الخدمات التي تتمتع بنسخ احتياطي بارد (Cold Backup):**

تتضمن خدمات تحتاج لإعداد ولإقلاع المخدمات ولعمليات نقل معطيات إليها. كمثال على هذه الحالة، هو النسخ الاحتياطي الذي نطبقه على بيانات المؤسسة وعلى البرامج التي تتعامل مع هذه البيانات، والتي يمكن في حال تعطل المخدم الذي تعمل عليه، أن نثبتها على مخدِّم آخر وأن نقوم بإعداده ليعمل كمخدِّم جديد لهذه البيانات.

بشكل عام، تشكل أساليب التكرار والنسخ الاحتياطي، الدعامة الرئيسية لمخطط الاستمرار في العمل الذي يمنع، في حال حصول اختراق، أو حصول خطأ بشري، أو حصول عطل طارئ أو كارثة طبيعية، من حدوث شلل في أعمال المؤسسة.

11.1. معالجة الأجهزة المنسقة (Processing Obsolete Components):

يجب تحديد الخطوات الواجب اتخاذها لضمان إزالة المعلومات من الأجهزة التي يتم تجديدها أو استبدالها، أو التخلص منها.

فعلى سبيل المثال، عند استبدال الأجهزة أو الأدوات يجب حذف أو إعادة تهيئة أقراصها الصلبة، ومسح الأشرطة المغناطيسية المستخدمة في عمليات النسخ الاحتياطي، ومسح كلمات المرور الموجودة على الأجهزة.

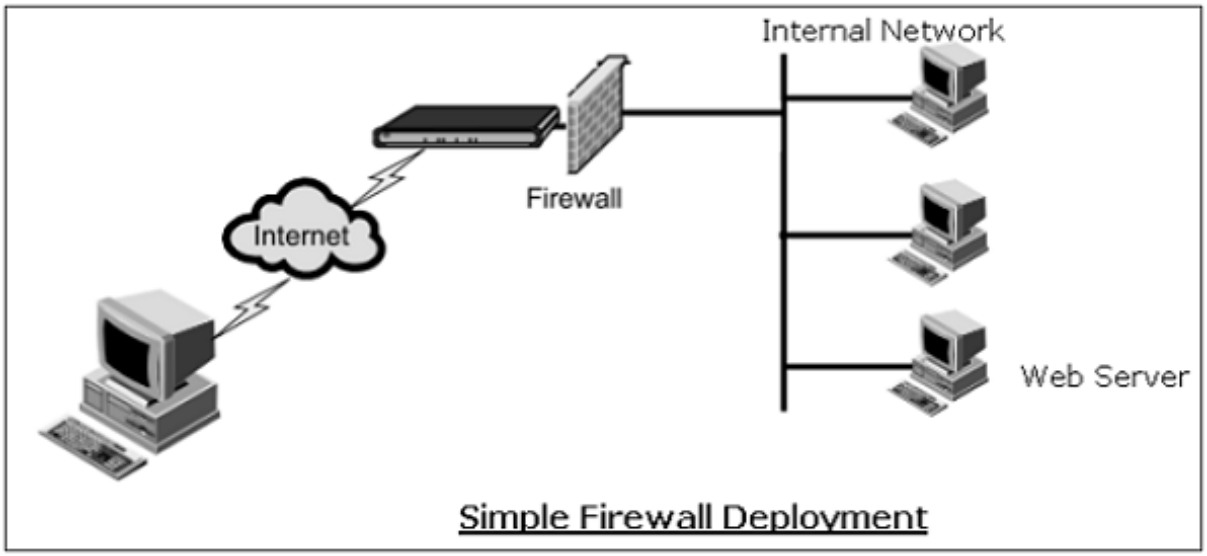
تعتمد جدية العمل المطلوب على حسّاسية المعلومات. فقد نحتاج، في بعض الأحيان، إلى الإتلاف الفيزيائي للأجهزة التي تحتوي على معلومات حسّاسة جداً، وذلك لضمان عدم استعمال تلك الأجهزة في مكان آخر وعدم التمكن من استعادة المعلومات التي كانت عليها.

2. جدران النار (Firewalls):

في حال وصل الشبكة المحلية إلى الإنترنت ستظهر مجموعة جديدة أخرى من مسائل الأمن، وعلى مدير الشبكة تأمين سلامة الشبكة المحلية من المتطفلين أو القراصنة الذين يحاولون العبث بالشبكة المحلية عبر الاتصال المفتوح مع الإنترنت. تستخدم جدران النار كوسيلة حماية أساسية للشبكات المحلية أو الشخصية المتصلة بشبكة الإنترنت.

جدار النار هو عبارة عن موجه يستطيع التعامل مع مسائل أمن الشبكة، وعادة ما يتموضع بين الإنترنت وبين الشبكة المحلية. تمر جميع التدفقات الشبكية من وإلى الشبكة المحلية عبر جدار النار، والذي يمنع النفاذات غير المخولة إلى الشبكة المحلية.

يمكن تركيب جدار النار بطريقتين أساسيتين، أولاً عبر شراء جهاز جدار نار والذي هو عبارة عن جهاز يحتوي موجه مع ميزات جدار النار مضمنة فيه. تتضمن معظم أجهزة جدران النار واجهات ويب تمكن من الوصول إلى جدار النار من أي حاسب على الشبكة باستخدام المتصفح. ثانياً يمكن تجهيز مخدم حاسوبي ليعمل كجدار نار. يمكن لهذا المخدم أن يعمل على أي نظام تشغيل شبكي، وأن كانت معظم أنظمة جدران النار المخصصة تعمل على لينوكس.



وبغض النظر عن نوع جدار النار عليه دائماً أن يتوضع بين الشبكة المحلية والإنترنت، بحيث توصل أحد نهايات جدار النار إلى مبدل الشبكة الموصول من جهة أخرى مع أجهزة الشبكة المحلية، وتوصل النهاية الأخرى لجدار النار إلى الإنترنت.

ولجدران النار الأنواع الرئيسية التالية:

1.2. مفلترة الرزم (Packet Filtering):

تقوم جدران النار في هذا النوع بفحص كل رزمة تمر من الجدار وتختبرها بناءاً على مجموعة من القواعد التي يحددها مدير النظام. يسمح للرزمة بالمرور إذا استطاعت النجاح بالاختبار، أما إذا فشلت بالاختبار فترفض وتمنع من المرور.

تعتبر جدران النار مفلترة الرزمة من أرخص أنواع جدران النار، ولذلك فهي شائعة الاستخدام. من جهة أخرى، تحوي عدداً من نقاط الضعف الذي يمكن لقراصنة محترفين استغلالها. لذلك فهي بحد ذاتها لا تشكّل جدار نار فعال.

تعمل مفلترات الحزمة على فحص حقول مصدر وهدف عنوان الإنترنت (IP)، وعناوين المنافذ المحتواة في كل من رزم (TCP/IP). منافذ (TCP/IP) هي أرقام تعيّن لخدمات محددة تساعد بتعريف كل خدمة تكون الرزمة موجهة ومخصصة لها. مثلاً منفذ بروتوكول (HTTP) هو 80، وبالتالي ستحدد الرزم المستلمة والموجهة لمخدم (HTTP) البوابة 80 كالبوابة الهدف. تحدد القواعد في مفتلر الرزم السماح بمرور الرزم أو رفضها بناءاً على عناوين (IP) محددة أو منافذ محددة. فيمكن مثلاً تحديد قاعدة تمنع كل الرزم المتوجهة إلى بوابات المستخدمة من قبل (NetBIOS)، وبالتالي تمنع قراصنة الإنترنت من الوصول إلى موارد مخدم (NetBIOS) مثل الملفات والطابعات.

أحد أهم نقاط الضعف لمفترات الرزم أنها تثق بما تحتويه الرزم على أنه حقيقة، يمكن لقراصنة الإنترنت استغلال هذه النقطة عبر تقنية خداع عنوان الإنترنت (IP Spoofing)، والتي يتم فيها إدخال عنوان إنترنت مزيف في الرزم المرسلة إلى الشبكة المحلية. من نقاط الضعف الأخرى أن مفلترات الرزم تفحص كل رزمة بمعزل عن البقية، دون الأخذ بعين الاعتبار إذا ما كانت الرزمة قد مرت مسبقاً في جدار النار وماهية الرزم التالية في الوصول. أي أن جدران النار مفلترة الرزم هي دون حالة (Stateless).

وعلى الرغم من نقاط الضعف السابقة، لدى مفلترات الرزم عدداً من المميزات من أهمها:

- عالية الكفاءة: وهي قادرة على أن تختبر الرزم بطريقة سريعة بعد استخلاص عناوين الإنترنت والمنافذ وتطبيق القواعد المحددة عليها، بالمقابل تقانات جدران النار الأخرى لديها عبئاً أعلى من ناحية الأداء.
- شفافة بالنسبة للمستخدم: ينتبه المستخدم على فلترة الرزم في حالة وحيدة وهي عندما يتم رفض الرزم. تقانات جدران النار الأخرى تتطلب أن يكون الزبائن و/أو المخدمات تم تهيئتهم بطريقة خاصة للعمل مع جدران النار.
- رخيصة الثمن: معظم الموجهات الحالية تمتلك خاصية الفلترة مضمنة في عمل الموجه.

2.2. فحص الرزم ذو الحالة (Stateful Packet Inspection – SPI):

هذا النوع هو خطوة باتجاه جدران نار أكثر ذكاءً من مفلترات الرزم. في هذا النوع ينظر جدار النار إلى الرزم كمجموعات بدلاً من فحصها فرادى. ويتعقب الرزم التي مرت مسبقاً في جدار النار، ويمكنه بالتالي اكتشاف نماذج التي تشير إلى نفاذ غير مخول. يمكن لهذا النوع في بعض الحالات الاحتفاظ بالرزم حتى يتم تجميع معلومات وافية لاتخاذ قرار ما إذا كان يجب لهذه الرزم أن تخول بالنفاذ أم يجب أن ترفض. كان هذا النوع من جدران النار يوجد فقط في موجهات مؤسساتية المستوى عالية الثمن. لكن حالياً أصبح هذا النوع من جدران النار مقبول الكلفة للشبكات الصغيرة إلى متوسطة الحجم.

3.2. بوابات مستوى الدارة (Circuit–Level Gateway):

يدير هذا النوع الاتصالات بين الزبائن والمخدمات بناءاً على عناوين (TCP/IP) وأرقام المنافذ. بعد أن يتم إنشاء الاتصال، لا تتدخل البوابة بالرزم المتدفقة بين الأنظمة. فيمكن مثلاً استخدام بوابة مستوى الدارة من النوع (Telnet) للسماح لاتصالات (Telnet) (على المنفذ 23) لمخدم معين، ومنع أنواع أخرى من الاتصالات إلى المخدم. وبعد أن يتم تأسيس الاتصال تسمح البوابة للرزم بالتدفق بحرية عبر الاتصال. ولا يمكن كنتيجة لذلك لبوابة مستوى الدارة أن يمنع مستخدماً بعيداً من تنفيذ برامج محددة أو استخدام أوامر بحد ذاتها.

4.2. بوابة التطبيقات (Application Gateway):

هو نظام جدار نار أكثر ذكاءً من الأنواع السابقة الأخرى. تتعرف بوابة التطبيقات على كل تفاصيل التطبيقات التي ولّدت الرزم المارة عبر جدار النار. فمثلاً تعرف بوابة تطبيق ويب كافة تفاصيل رزم (HTTP). وبالتالي يمكن لجدار النار أن يفحص تفاصيل أكثر من مجرد عنوان المرسل والمستقبل وعناوين المنافذ لاتخاذ قرار تمرير الرزم أو رفضها. كذلك يمكن لبوابة التطبيقات أن تعمل كمخدمات وسيطة (Proxy). هذه المخدمات هي التي تتوضع بين الحاسب الزبون وبين مخدمات الإنترنت الحقيقية. يعترض المخدم الوسيط الطلبات ويفحص إذا ما كان لديه نسخة مسبقة من الصفحة المطلوبة في ذاكرته الخابية. إذا وجدت الصفحة تعاد إلى الزبون، أما في حال عدم وجودها يرسل الطلبات إلى المخدمات الحقيقية.

تعرف بوابات التطبيقات تفاصيل كيفية معالجة مخدمات (TCP/IP) المختلفة لتتابع رزم (TCP/IP)، مما يمكنها من اتخاذ قرارات ذكية إذا ما كانت الرزم شرعية أو جزءاً من محاولة هجوم على الشبكة. تعتبر بوابات التطبيقات أكثر كلفة من الأنواع الأخرى من حيث ثمن الشراء ومن حيث التهيئة والتثبيت والصيانة. كذلك تبطئ بوابات التطبيقات الشبكة وتؤثر على الأداء العام لأنها تقوم بفحص تفصيلي على الرزم.

3. الأنشطة المرافقة:

أسئلة خيارات متعددة Multiple Choices

1. التأمين الفيزيائي للشبكة:
   - A. يقصد به حماية المكونات الفيزيائية في الشبكة.
   - B. يتضمن سياسات ولوج الأشخاص إلى المخدمات وغرف الحاسب ومدير النظام.
   - C. كذلك يتضمن التامين المادي لمحطات العمل كاستخدام أقفال لوحات المفاتيح.
   - D. كل ما سبق.
   - E. كل من (A) و(C) فقط.

2. تحديد مهمة كل حاسب في المنظومة الشبكية:
   - A. تحديد أصناف المعلومات التي ستخزن على الحاسب.
   - B. تقسيم معلومات المؤسسة إلى كتل تتصف كلٍ منها بمستوى سرية محدد.
   - C. تحديد الخدمات الشبكية التي سيقدمها الحاسب.
   - D. كل ما سبق.
   - E. كل من (A) و(C) فقط.

3. تأمين حسابات المستخدمين عبر عدد من المهمات منها:
   - A. تهيئة هذه الحسابات بطريقة تمنع النفاذ إليها حتى لو جرى الوصول فيزيائياً لها.
   - B. تحديد حقوق المستخدمين.
   - C. استخدام كلمات المرور.
   - D. كل من (A) و(B) فقط.
   - E. كل من (A) و(C) فقط.

4. تتضمن إدارة أمن المستخدم عدد من المهمات منها:

A. إدارة الحسابات المضمنة مثل حساب الضيف.

B. تأمين حساب مدير النظام وتغيير كلمة مروره الافتراضية.

C. تحديد سماحيات المستخدم للنفاذ إلى موارد الشبكة.

D. كل من (A) و(B) فقط.

E. كل من (A) و(C) فقط.

5. مجموعات المستخدمين:

A. يحق لكل مستخدم الانتماء إلى مجموعة مستخدمين واحدة محددة في النظام.

B. تسهل وتنظم عمل مدير النظام وتختصر زمن الإدارة.

C. تهدف إلى حصر صلاحية استخدام الحاسوب بالمجموعات المُعرَّفة.

D. كل ما سبق.

E. كل من (B) و(C) فقط.

6. تتضمن حقوق المستخدمين:

A. الولوج المحلي إلى الشبكة.

B. نسخ الملفات أو المكتبات احتياطياً.

C. التحكم بالنفاذ إلى موارد الشبكة المحددة مثل الملفات.

D. كل من (A) و(B) فقط.

E. كل من (A) و(C) فقط.

7. تأمين مستخدمي الشبكة:

A. من أهم القواعد الأمنية في المؤسسات وأقلها استخداماً ومراعاة.

B. تتضمن حماية المستخدمين من التهديدات عبر الشبكة.

C. تتضمن القواعد السلوكية للمستخدمين.

D. كل من (A) و(C) فقط.

E. كل من (A) و(B) فقط.

8. مبدأ المكتب الخالي:

A. يعتمد على منع أي من الأشخاص التواجد في المكتب خارج ساعات العمل.

B. عدم إعطاء معلومات الحساب لزملاء عاملين في الشركة.

C. يحتِّم على الموظف أن يترك مكتبه خالٍ من أي ملف عندما يترك عمله.

D. كل ما سبق.

E. ولا أي إجابة مما سبق.

9. النسخ الاحتياطي العادي:

A. يعني قدرة المنظومة على العمل آنياً مع الخدمة الاحتياطية.

B. عمل خدمة النسخ الاحتياطي بأن واحد مع الخدمة الأصلية.

C. يعني قدرة المنظومة على العمل مع الخدمة الاحتياطية بعد فترة وجيزة وبعد القيام بإعدادات بسيطة.

D. كل ما سبق.

E. كل من (A) و(C) فقط.

10. معالجة التجهيزات المنسقة ضمن الخطة الأمنية:

A. يجب حذف أو إعادة تهيئة أقراصها الصلبة.

B. مسح الأشرطة الممغنطة المستخدمة في عمليات النسخ الاحتياطي.

C. الإتلاف الفيزيائي للأجهزة التي تحتوي على معلومات حسّاسة جداً.

D. كل ما سبق.

E. كل من (A) و(B) فقط.

11. جدران النار:

A. تهدف إلى تقطيع الشبكة المحلية لتسهيل حمايتها.

B. هي تجهيزات عتادية تضاف إلى الشبكة لحمايتها من الخارج.

C. هي تجهيزات برمجية يمكن أن تضاف إلى المخدمات المستخدمة مسبقاً في الشبكة.

D. كل من (B) و(C) فقط.

E. كل من (A) و(C) فقط.

12. جدران النار مفلترة الرزم:

A. تفحص مجموعات من الرزم المصنفة على قواعد معينة وتختبرها لتحدد إمكانية تخويلها للمرور.

B. تفحص كل رزمة مارة عبرها وتختبرها لتحدد إمكانية تخويلها للمرور.

C. من أغلى أنواع جدران النار عادة.

D. كل ما سبق.

E. كل من (B) و(C) فقط.

13. تقنية عمل جدران النار مفلترة الرزم:

A. تعتمد على فحص مصدر وهدف عنوان الإنترنت.

B. تعتمد على فحص عناوين المنافذ المحتواة في كل من رزم (TCP/IP).

C. تثق بما تحتويه الرزم على أنه حقيقة.

D. كل ما سبق.

E. كل من (A) و(B) فقط.

14. بوابات مستوى الدارة:

A. هي من النوع دون حالة.

B. تفحص كل رزمة تمر بها اعتماداً على عناوين (TCP/IP) وأرقام المنافذ.

C. تمنع المستخدمين البعيدين من تنفيذ برامج محددة على النظام.

D. كل ما سبق.

E. ولا أي إجابة مما سبق.

15. بوابة التطبيقات:

A. تعتمد على إنشاء اتصال بناء على عناوين (TCP/IP) وأرقام المنافذ.

B. تعرف بوابات التطبيقات تفاصيل كيفية معالجة مخدمات (TCP/IP) المختلفة لتتابع رزم (TCP/IP).

C. لا تتدخل بعد إنشاء الاتصال الخاص بتفاصيل الرزم.

D. كل ما سبق.

E. ولا أي إجابة مما سبق.

رقم السؤال	الإجابة الصحيحة	توجيه في حال الخطأ
1	D	إعادة الفقرة: التامين الفيزيائي للشبكة
2	E	إعادة الفقرة: تحديد مهمة كلّ حاسب وتوثيق الهدف من استعماله
3	E	إعادة الفقرة: تأمين حسابات المستخدمين
4	D	إعادة الفقرة: إدارة أمن المستخدم
5	E	إعادة الفقرة: إدارة أمن المستخدم
6	D	إعادة الفقرة: إدارة أمن المستخدم
7	D	إعادة الفقرة: تأمين مستخدمي الشبكة
8	C	إعادة الفقرة: تأمين مستخدمي الشبكة
9	C	إعادة الفقرة: استمرار الخدمة عند الأعطال
10	D	إعادة الفقرة: معالجة الأجهزة المنسق
11	D	إعادة الفقرة: جدران النار
12	B	إعادة الفقرة: مفلترة الرزم
13	D	إعادة الفقرة: مفلترة الرزم
14	E	إعادة الفقرة: بوابات مستوى الدارة
15	B	إعادة الفقرة: بوابة التطبيقات