الفصل الحادي عشر :
الحماية في القطاعات والمؤسسات

حماية الأجهزة الشخصية هي مهمة سهلة مقارنة بحماية الأجهزة الموجودة في القطاعات والمؤسسات المختلفة. ويتعرض هذا الفصل لبعض النواحي المتعلقة بالحماية من الجريمة في القطاعات والمؤسسات.

يخطئ بعض المستخدمين عندما يعتقدون بأن الحماية تبدأ بعد حدوث الجريمة أو الاختراق، وأنه لا يجب عمل أي شيء قبل حدوث ذلك. والصحيح أن الحماية من الجريمة هي مشوار طويل يبدأ قبل حدوث الجريمة وفي أثناء حدوثها، و يستمر أيضا حتى بعد حدوثها والتخلص من أثرها.

في هذا الفصل سنتطرق لجميع هذه المراحل، وهي:

١. الحماية قبل وقوع الجريمة

٢. الحماية في أثناء وقوع الجريمة

٣. الحماية بعد وقوع الجريمة

وقبل ذلك، يَحْسُن ذكر عدد من الإحصاءات التي توضح مقدار الضرر الحاصل جراء التهاون أو الفشل في تحقيق سياسة أمنية فعالة في الشركات والمؤسسات الاقتصادية، فقد أوضحت إحصائية للحكومة البريطانية أن ٣٣ ٪ من الجهات الحكومية في الحكومة قد تعرضت لمحاولات اختراق. وأن أكثر من ٣٤ ٪ من الجهات المرتبطة بالإنترنت غير واثقة في مقدرتها بالكشف عن الاختراقات حال حدوثها. وأن أكثر من ٣٣٪ من الجهات غير قادرة على البحث والتحري في الحوادث الأمنية التي قد تتعرض لها. وأظهرت إحصائية أخرى أن أكثر من ٦٠ ٪ من المنظمات الحكومية الأمريكية سبق وأن تعرضت لهجمات من قبل الفيروسات. و ٢٠٪ منها تعرضت لعملية اختراق، و٣٨ ٪ منها أبلغت عن سرقة أجهزة كمبيوتر محمولة (laptop).

وبينت دراسات (FBI) مع معهد أمن الحاسبات بأن متوسط الخسائر الناتجة عن الاختراق

تقدر بمبلغ ٦,٦ مليون دولار لكل محاولة اختراق. وأشارت إلى أن نصف محاولات الاختراق للشركات ناتجة من داخل الشركة أو من قبل موظفين مفصولين من الشركة.

فيما أوضحت أن فيما ذكرت جريدة لوس أنجلوس تايمز أن خسائر شركة نوكيا جراء اختراق الهاكر كيفن ميتنك لها بلغت (١٣٥) مليون دولار.

وأما شركة كمبيوتر إيكونوميكس للأبحاث (Computer Economics) فقدرت الخسائر الناتجة عن فيروس (Code Red) بـ ١,٢ مليار دولار، مابين خسائر في الإنتاجية أو خسائر لإصلاح الأجهزة.

١١-١ الحماية قبل وقوع الجريمة

الحماية قبل وقوع الجريمة هي خطوة مهمة، حيث إن التعامل مع الهجمة في حال وقوعها يعتمد بشكل كبير على جودة الاستعداد في هذه الخطوة. والحماية قبل وقوع الجريمة يتلخص باختصار بالاستعداد لها قبل وقوعها، وذلك على ثلاثة مستويات:

- مستوى الأجهزة المستقلة
- مستوى الشبكة
- مستوى الأشخاص والمستخدمين

١١-١-١ تحديد ما تريد حمايته

قبل أن يبدأ الشخص المشرف على الشبكة بالتخطيط وتفعيل معايير الحماية، يجب عليه

أولاً أن يحدد النطاق الذي يرغب بحمايته. فمثلاً، تكتفي بعض القطاعات بحماية الأجهزة المرتبطة بالإنترنت فحسب، دون حماية الأجهزة الموجودة في الشبكة الداخلية. بينما قطاعات أخرى ترغب في حماية جميع الأجهزة الموجودة في شبكتها، سواءً كانت مرتبطة بالإنترنت أو لم تكن كذلك. وهناك قطاعات أخرى قد ترغب في حماية الأجهزة الموجودة في الإدارات الحساسة، مثل الإدارة المالية وإدارة شؤون الموظفين، بينما لا تهتم بحماية الأجهزة في الإدارات الأخرى. و يجب أيضاً تحديد مستوى الحماية المطلوب، فالجهاز المحتوى على مزود الويب الخاص بموقع الشركة يجب أن يكون محمياً بشكل أكبر مقارنة بجهاز أحد المستخدمين في الشبكة.

وبناء على هذا التحديد يقوم المشرف بتحديد خطة مبدئية لتفعيل الحماية في شبكته، ومن ثم ينتقل لتطبيق معايير الحماية التي يريدها.

١١-١-٢ تحديد سياسة أمن الشبكة (Information Security Policy) وسياسة الاستعمال المقبول (Acceptable Usage Policy)

هذه السياسات هي قواعد يقوم المشرف على الشبكة بتحديدها بناء على:

- مستوى الحماية المطلوب توفيره للشبكة.
- الصلاحيات التي ترغب الشركة منحها لموظفيها لاستخدام الإنترنت.

فمثلا، في ناحية السياسة الأمنية للشبكة، فبعض الشركات لا تمانع من استخدام برامج نقل الملفات في شبكتها، بينما شركات أخرى قد تعد ذلك من المخاطر الأمنية لانتشار الفيروسات وتقوم بمنع ذلك. ومثال آخر هو إمكانية الاتصال الشبكي الهاتفي (Dial-up Connection) فبعض الشركات لا تسمح بذلك، بينما شركات أخرى قد تسمح به.

أما من ناحية سياسة الاستخدام المقبول، فهو يتعلق باستخدام الموظفين للشبكة. فبعض الشركات تسمح للمستخدمين بتصفح المواقع أثناء وقت الدوام الرسمي، بينما شركات أخرى لا تسمح بذلك. وكذلك أيضا باستقبال نوعية معينة من الملحقات Attachments في

البريد الإلكتروني، فبعض الشركات تمنع استقبال بعض النوعيات من الملحقات عن طريق البريد الإلكتروني الرسمي للشركة.

بالطبع فهناك العديد من النقاط والقواعد التي يجب ذكرها في تلك السياسات، التي يجب أن يطلع عليها الموظف الجديد عند التحاقه بالشركة، ليكون على معرفة بما هو مسموح وما هو غير مسموح له بعمله.

١١-١-٣ الاستعداد على مستوى الأجهزة

ويعني بذلك أن المشرف على الشبكة سيقوم بتطبيق معايير الحماية المطلوبة في كل جهاز على حدة. وهذا ضروري جداً على الرغم من أنه متعب عند وجود الكثير من الأجهزة، وهذا ما يزيد من أهمية خطوة (تحديد ما تريد حمايته) المذكورة سابقاً. ونقوم بحصر المعايير الأمنية التي يجب تطبيقها على مستوى الأجهزة بالآتي:

١١-١-٣-١ عمل نسخ احتياطية

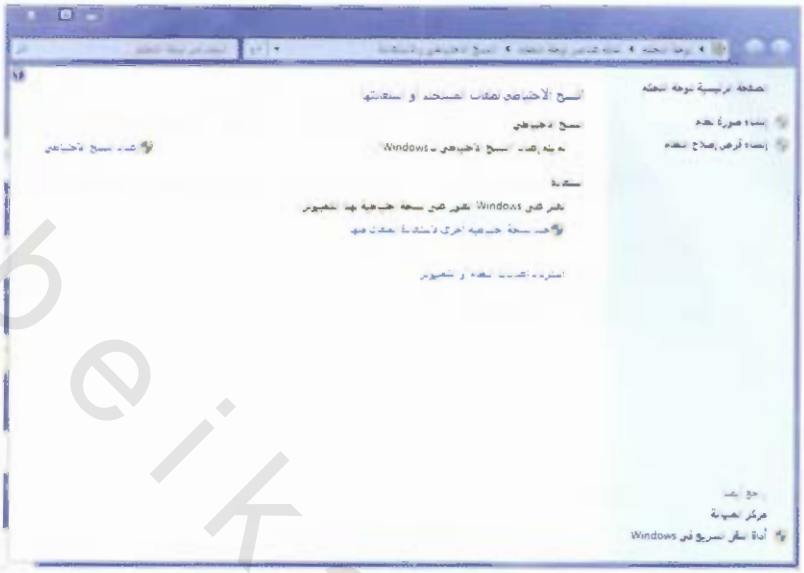
الهجمات التي تقوم بسرقة المعلومات قد لا تقوم بتدمير البيانات، ولكن هناك أنواع أخرى من الهجمات يقوم المخترق فيها بمسح البيانات. ولهذا يجب القيام بعمل نسخة احتياطية من البيانات المهمة، والتي تختلف من جهاز إلى آخر، والقيام بتحديث هذه النسخة بشكل دوري. ويتم تحديد الفترة التي يجب فيها عمل النسخة الاحتياطية في السياسة الأمنية للشركة التي سيتم الحديث عنها لاحقاً.

ومعروف أن النسخة الاحتياطية ليس الغرض منها هو استرجاع البيانات في حالة الاختراق فحسب. بل إن البيانات قد تضيع لأي سبب آخر، مثل تلف القرص الصلب أو انقطاع الكهرباء بشكل مفاجئ أو غيرها من الأسباب. كما أنها أيضاً قد تستخدم للحفظ

والتوثيق وتتبع تطور البيانات على مر الزمن، حيث تمكن أصحاب القطاع أو الشركة من رؤية حالة البيانات في الماضي ومقارنتها بالحاضر. ولكن هذا خارج عن السياق الذي نريده وهو الحماية الأمنية.

يجب التنبيه بأن النسخ الاحتياطي لا يعني وجود حماية كاملة للبيانات، فعلى الرغم من أن النسخة الاحتياطية تحتوي على البيانات المطلوبة، إلا أنه في حالة حدوث اختراق فقد يتطلب الأمر وقتاً طويلاً قبل الحصول على جهاز يمكن نسخ البيانات إليه. ويجب أيضاً ملاحظة أن البيانات المنسوخة قد تكون معرضة للعبث والتغيير قبل عمل نسخة احتياطية منها، ومن ثم فإن هذا يعني أن النسخة الاحتياطية عديمة الفائدة. لذلك لابد من وجود خطة واضحة لكيفية النسخ الاحتياطي والاسترجاع، وتجريب هذه العملية بشكل دوري.

ويوجد العديد من البرامج التي تساعد على القيام بنسخة احتياطية، وهي موجودة على مختلف أنظمة التشغيل. وتوجد أيضاً وسائل عديدة لتخزين البيانات المنسوخة بدءاً من الشريط (Tape) وانتهاءً بأقراص (DVD) القابلة للكتابة. وتحديد البرنامج ونوعية الوسيط الذي يتم النسخ عليه هو خارج نطاق الحديث في هذا الكتاب.

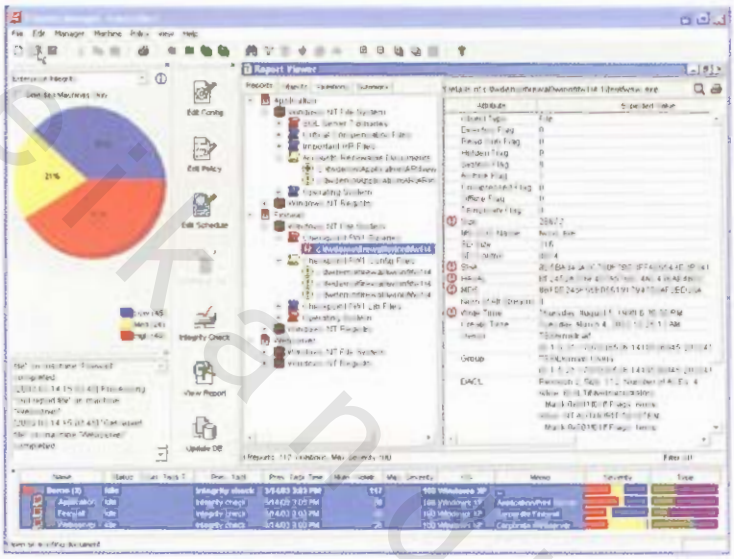


شكل ١١-١: برنامج عمل النسخ الاحتياطية في ويندوز٧

١١-١-٣-٢التأكد من سلامة الملفات من التغيير

كما ذُكر آنفاً، فإن عمل النسخ الاحتياطية غير كافٍ بشكل كامل، فعند تعرض النسخة الأصلية للتلف فإن برنامج النسخ سيقوم بعمل نسخة احتياطية من البيانات المعطوبة. ومن هنا تظهر الحاجة لوسيلة تسمح للمشرف على الشبكة أو الجهاز بالتأكد من سلامة البيانات من العبث والتغيير. وهذه هي وظيفة برامج ملخص الرسالة، وهي برامج تستقبل البيانات كمدخل، وتقوم بإخراج رمز صغير يقاس بعشرات البايتات، ويقوم بتمييز هذه البيانات. وميزة هذه الرمز هو أنه مميز للبيانات، بحيث إنه في حالة تغير البيانات، ولو بشكل بسيط، فإن الرمز الناتج سيتغير. وطريقة استخدام هذه البرامج هو أن يقوم المشرف على الشبكة، باستخراج الرموز الخاصة بالملفات التي تحتوي على البيانات المهمة، وتخزين هذا الرموز في مكان آمن.

ويقوم دورياً باستخراج الرموز لنفس البيانات. وفي حالة تغير الرموز فهذا يعني أن البيانات قد تم تغييرها بشكل غير مرغوب، ومن هنا يعلم المشرف أن البيانات قد تعرضت للاختراق. ومن أشهر البرامج من هذه النوعية هو برنامج (TripWire) الذي كانت بدايته على نظام يونكس، ومن ثُمَّ تَمَّ إصداره على نظام ويندوز. انظر الشكل ١١-٢.



شكل ١١-٢: لقطة لبرنامج TripWire

١١-١-٣-٣ تشغيل التسجيل

وهذا من أهم الاحتياطات التي تساعد على اكتشاف وجود عملية اختراق، ومن ثم تتبع المخترق. ومن دونها لا يستطيع المشرف على النظام معرفه ما يحصل في النظام. ويمكن تقسيم ملفات التسجيل إلى قسمين، الأول هو ملفات التسجيل المتعلقة بنظام التشغيل وخدماته والقسم الآخر هو المتعلق بالتطبيقات المختلفة. وفي الآونة الأخيرة ومع انتباه مصنعي برامج الحاسب إلى أهمية الناحية الأمنية، فإن معظم البرامج تأتي مع خاصية تشغيل التسجيل (Logging) فيها مفعلة تلقائياً. ولكن هذا لا يمنع من أن يقوم المشرف بالتأكد من ذلك، والقيام باختيار المعلومات

التي يريد تسجيلها. ولعل معظم البرامج والأنظمة تقوم بتسجيل عدد كبير من المعلومات، أهمها رقم (IP) للجهاز الخارجي، ونوع العملية المطلوبة وتاريخها، ورد النظام على ذلك الطلب.

١١-١-٣-٤ تحصين الأجهزة وتحديثها

توجد مقولة لدى خبراء حماية الشبكات، وهي أن مستوى الحماية في الشبكة يقاس بمستوى حماية أضعف جهاز موجود فيها. أي أنه لا يجب إعطاء مجموعة من الأجهزة قدراً كبيراً من الحماية وإهمال مجموعة أخرى، بل يجب المساواة بينها في مستوى الحماية.

ويمكن تحصين مستوى الحماية في الأجهزة بالشكل الآتي:

- إيقاف الخدمات العاملة التي لا يتم استخدامها. فبعض أنظمة التشغيل تقوم بتشغيل عدد كبير من الخدمات التي لا يتم استخدامها على الإطلاق، وتكون مصدراً للخطر على الجهاز. فجهاز خادم الملفات لا يحتاج لوجود مزود ويب، أو مزود بريد، ولذا يجب إيقافها.
- تركيب برامج اكتشاف الاختراق الخاصة بالأجهزة.
- (Host-based Intrusion Detection Systems) التي تحتوي على قدر من الذكاء يسمح لها بالتعرف على وجود محاولة اختراق وإنذار المشرف على الشبكة لحظيا.
- الحرص على تركيب آخر التحديثات سواء لنظام التشغيل أو للبرامج المختلفة الموجودة في النظام. والكثير من البرامج في الوقت الحالي مصممة بطريقة تسمح لها بالتأكد من وجود تحديثات وإخبار المستخدم بذلك.

شكل ١١-٣: شاشة البرنامج المدمج في ويندوز٧ الذي يعمل على تحديث ويندوز بشكل تلقائي

١١-١-٣-٥ المعدات البيولوجية

هي معدات يكون الغرض الرئيس منها هو التحكم في الدخول للجهاز، وهي تعتمد على الخصائص البيولوجية التي تميز الأشخاص مثل بصمة الإصبع أو قزحية العين. حيث يوجد بعض العتاد الذي يربط بالجهاز ويقوم بالتغلغل في نظام التشغيل، بحيث لا يسمح للشخص بالدخول للنظام ما لم يكن هو الشخص صاحب النظام. وتقوم الكثير من الشركات بتوفير قارئات البصمة وقارئ قزحية العين. كما أن بعض شركات الأجهزة المحمولة بدأت تصنع أجهزة محمولة بحيث يوجد قارئ البصمة مدمجاً فيها.

وكما ذكر سابقاً، فإن هذه الخاصية تعد مرغوبة ممن يتطلب عملهم قدراً أكبر من الحماية، مثل مديري الشركات الكبرى التي تحتوي أجهزتهم على أسرار شركاتهم وتعاملاتها المختلفة. فهؤلاء

يعدّون هذه النوعية من الحماية من باب الحاجة الماسة وليست من باب الرفاهية. ولكني بالنسبة للمستخدم العادي فلا أنصحه باستخدام هذه النوعية من الحماية، فهي مبالغ فيها بشكل كبير.

شكل ١١-٥: قارئ بصمة اليد في الحاسب المحمول

١١-١-٤ الاستعداد على مستوى الشبكة

تركز هذه المرحلة على الناحية الأمنية المتعلقة بالبنية التحتية للشبكة. ويوجد العديد من الاحتياطات الأمنية التي يجب أن تفعل على مستوى الشبكة، فبعضها يكون بتركيب البرامج، وبعضها الآخر يكون متعلقاً بتصميم الشبكة. وسيتم تناول هذه الاحتياطات فيما يأتي.

١١-١-٤-١ تصميم الشبكة بشكل سليم

ويقصد بذلك تصميم الشبكة بشكل سليم لتقليل الخطر الناتج عن الاختراق. حيث إن بعض المشرفين على الشبكات يظن أن الغرض الوحيد من الشبكة هو إيجاد قناة اتصال بين

الأجهزة الموجودة فيها. وهذا اعتقاد خاطئ كلياً. حيث إنه يجب وضع الحماية الأمنية في البال عند تصميم الشبكة. بالطبع فهناك طرق وتقنيات عديدة لتصميم الشبكات، ولكنها خارج نطاق الحديث في هذا الكتاب، وتوجد كتب مخصصة لهذا المجال يجب على من يريد الإشراف على الشبكة أن يقوم بالاطلاع عليها.

١١-١-٤-٢ تركيب جدر الحماية(Firewalls) و برامج اكتشاف الاختراق (IDS/IPS)

جدر الحماية هي برامج يتم تركيبها على أجهزة تفصل بين شبكتين مختلفتين، بحيث لا تمر أيه بيانات من شبكة إلى أخرى دون المرور بجدر الحماية. ووظيفتها هي إيقاف جميع البيانات المارة خلالها ومقارنتها بالقواعد والصلاحيات التي وضعها من قام بإعداد جدار الحماية، ومن ثم إصدار القرار إما بالسماح لتلك البيانات بالمرور أو منعها من ذلك. أما برامج اكتشاف الاختراق، فهي برامج يتم ربطها بالشبكة، بحيث تقوم بمراقبة جميع البيانات المارة خلال الشبكة، وبناء على معايير ذكاء صناعي فيها تقوم بتحديد ما إذا كانت هذه البيانات تمثل بيانات لعملية اختراق تجري حالياً، ومن ثم تقوم بإنذار المشرف على الشبكة.

بالطبع تركيب هذه البرامج بحد ذاته لا يكفي لحماية الشبكة، ولكن الكلمة السحرية هنا هي (الإعداد السليم). حيث إن التركيب عملية سهلة لا يلزم فيها سوا نقرة زر حتى ينتهي تركيب البرنامج. ولكن إيجاد الإعدادات السليمة لهذه البرامج هو الأمر الصعب الذي يتطلب خبرة بعلم الشبكات. وبديهي أن الإعداد يختلف من شبكة لأخرى، ويعتمد بشكل كبير على تصميم الشبكة والاحتياطات الأمنية التي يريد المشرف على الشبكة تفعيلها، وعلى السياسة الأمنية للقطاع. وغني عن الذكر أن طرق إعداد مثل هذه النوعية من البرامج لا يمكن تفصيلها في هذا الكتاب بل يجب على من يريد تعلم ذلك أخذ العديد من الدورات في هذا المجال وقراءة الكتب المختلفة حتى يتمكن من ذلك.

١١-١-٤-٣ تحصين المحولات

وظيفة المحولات هي تمرير البيانات بين شبكتين مختلفتين، وهي عموماً تقوم بعمل ذلك على مستوى الشبكة بعكس جدر الحماية الحديثة نسبياً التي تعمل غالباً على مستوى التطبيقات، فبعض المحولات الحديثة تحتوي على بعض الوظائف الموجودة في جدر الحماية، ولكنها في الغالب لا تحتوي على كافة المميزات، والعكس كذلك صحيح، فبعض جدر الحماية لديها القابلية للوصول لمستوى الشبكة. ولكن الغرض والوظيفة الخاصة بكل منهما مختلفة تماماً لذا يجب عدم الخلط بين الاثنين.

يمكن تفعيل الحماية في المحولات وجعلها مساعدة لجدر الحماية. وذلك بتفعيل وظيفة قوائم التحكم بالدخول التي يحدد فيها المشرف على الشبكة نوعية البيانات التي يسمح بدخولها والشبكات التي يجب أن تأتي منها هذه البيانات. وهذه القوائم تساعد بشكل كبير على التخلص من أضرار هجمات منع الخدمة (DoS)، حيث يمكن التخلص من معظم الطلبات الزائفة قبل أن تصل لجهاز المزود وتشغله عن خدمة الطلبات الحقيقية.

يجب التنبيه إلى أنه من المستحسن جداً أن يفعّل المشرف خاصية التسجيل في المحول، وذلك لكي يتمكن من معرفة نوعية البيانات الداخلة والخارجة من شبكته، وكذلك معرفة محاولات الهجوم التي تحدث على شبكته في الوقت الحالي.

١١-١-٥ الاستعداد على مستوى الموظفين

يغفل بعض المستخدمين عن أهمية العنصر البشري في حماية الشبكات، ويعتقدون بأن حماية الشبكات تتم عن طريق تفعيل المعايير الأمنية في الأجهزة الموجودة في الشبكة فقط، وهذا اعتقاد خاطئ كلياً. حيث إن العنصر البشري يؤدي دوراً كبيراً جداً في حماية الشبكات. وأبسط مثال على ذلك مشكلة كبيرة كانت السبب في معظم حوادث الاختراق على الشبكات، وهي أن المشرف على الشبكة يقوم بتحصين الشبكة من الخارج ووضع جميع المعايير الأمنية لحمايتها، ومن ثم يقوم أحد الموظفين في الشركة بوضع جهاز مودم في جهازه بحيث يتمكن من

الاتصال بشبكة الشركة من الخارج. فيفتح هذا العمل باباً خلفياً يسمح للمخترق بالدخول للشبكة من دون الحاجة لتخطي معايير الحماية الأمنية التي قام المشرف على الشبكة بتركيبها. وقد انتشرت في السابق برامج تسمى (War Dialer)، وهي برامج تقوم بالاتصال على رقم شركة معينة، ومن ثم تجربة التحويلات المختلفة واحدة تلو الأخرى بحثا عن جهاز مودم. وغالبا ما يقوم المخترقون بهذه التجربة في الفترة الليلة عندما لا يوجد أحد في المكاتب.

هذا مثال واحد فحسب للخطر الذي قد يتسبب به العنصر البشري على حماية الشبكة وأمنها. ويتطرق هذا القسم لبعض المعايير الأمنية المتعلقة بالعنصر البشري في الشبكة.

١١-١-٥-١ جدر الحماية البشرية

هذا المصطلح هو أحد المصطلحات التي ظهرت حديثا بعد الانتباه لأهمية العنصر البشري في حماية الشبكات. حيث لوحظ أن المستخدمين يمكن تشبيههم ببرامج جدر الحماية

التي تساعد على حماية الشبكة. وكما أن برامج جدر الحماية تساعد على ذلك بالإعداد السليم، فإن المستخدمين يساعدون على حماية الشبكة، وذلك بتثقيفهم وتعليمهم بمخاطر الشبكة وكيفية مساهمتهم في حمايتها.

تقع المسؤولية على عاتق المشرف على الشبكة في التأكد من نوعية المستخدمين بمخاطر الشبكة وكيف يمكنهم تجنبها. ويمكنه عمل ذلك بطرق عديدة، أسهلها إرسال رسائل بريد إلكترونية للمستخدمين، أو القيام بعمل ندوة للموظفين بين الحين والآخر. ولكن من أهم المعايير في ذلك هو السياسة الأمنية (Security Policy) وسياسة الاستخدام المقبول (Acceptable Usage Policy) التي سيتم الحديث عنها لاحقاً.

١١-١-٥- ٢ الهندسة الاجتماعية

الهندسة الاجتماعية تعدّ من أخطر الطرق لاختراق العنصر البشري في مجال حماية الشبكات. ويذكر الهاكر الشهير كيفن ميتنك في كتابه (Art of Deception) أنه لولا وجود هذه الطريقة لما تمكن من القيام بالعديد من عمليات الاختراق التي قام بها في السابق.

والفكرة هنا هو أن يقوم المخترق باستخدام قدرته في الإقناع للحصول على المعلومات التي يريدها ممن يتحدث إليه. وتنجح هذه الوسيلة في الغالب بسبب سذاجة المستخدمين العاديين وتصديقهم لمن يتحدث إليهم بمجرد استخدامه لبعض المصطلحات التقنية. فكم من مخترق تمكن من الحصول على كلمة السر الخاصة بالمستخدم من المستخدم نفسه عن طريق الهاتف طواعية وبتعاون من المستخدم الضحية.

١١-٢ الحماية في أثناء الجريمة

يفترض هذا القسم أن الجريمة قد حدثت أو أنها جارية الحدوث، فما هي الإجراءات التي يجب على المشرف على الشبكة اتخاذها خلال تلك الفترة؟

من المعروف أن كل جريمة لها ظروفها وملازماتها الخاصة بها التي تجعل منها فريدة في نوعها، مما يجعل من الصعب تحديد قواعد ثابتة يجب القيام بها، ويمكن تطبيقها في جميع الجرائم التي تحصل على الشبكات. ولكن يمكن مناقشة بعض التوجيهات العامة التي قد تكون متوفرة في أي جريمة، من باب توفير بعض الإرشادات التي تساعد المشرف على الشبكة على اتخاذ القرارات التي تتناسب مع ما يواجهه في شبكته.

فعلى الرغم من أن كل جريمة تتميز عن غيرها، وأن كل جريمة قد تتطلب طرق تعامل مختلفة من قبل المشرف على الشبكة. إلا أن هناك بعض الأهداف المشتركة التي يحاول كل مشرفي الشبكات الوصول لها عند تعرض شبكاتهم للاختراق، وهي كالآتي:

- التقليل من الضرر الناتج عن الجريمة
- إزالة الجريمة والعودة إلى نظام العمل الطبيعي
- عدم مسح الأدلة التي قد تساعد للوصول إلى المجرم

١١-٢-١ قبل اتخاذ القرار

حدوث جريمة على الشبكة يجعل المشرف عليها يتعرض لضغط نفسي كبير قد يتسبب في تسرعه واتخاذه لقرارات خاطئة. لذا فإن أول نصيحة يجب العمل بها هو التروّي وعدم التهور ومحاولة جمع أكبر قدر من المعلومات التي تساعد على تقييم الجريمة، وتساعد على اتخاذ القرار المناسب في التعامل معها. ولكن في الوقت نفسه يجب على المشرف أيضا ألا يتأخر في اتخاذ

القرار، لأن ذلك قد يزيد من الضرر الناتج عن الجريمة.

ويجب على المشرف على الشبكة جمع المعلومات المتعلقة بالاختراق والتي ينبغي أن تحتوي الآتي:

- **الأسئلة الخمسة المشهورة التي يسألها الصحفيون غالباً**: من ؟ متى ؟ أين ؟ ماذا ؟ ولماذا ؟ ومن الطبيعي جداً ألا تتوفر الإجابة الكاملة عن جميع هذه الأسئلة في البداية، ولكن يجب على الأقل إبقاء هذه الأسئلة في البال، ومحاولة الحصول على الإجابة لأكبر عدد منها قبل التعامل مع الجريمة.
- **إحصاء الأجهزة المتضررة من الجريمة**: حيث يجب معرفة أثر الجريمة على الشبكة، وما هي الأجهزة المتضررة من تلك الجريمة. فالجريمة التي يتعرض فيها مزود الويب للاختراق، يختلف التعامل معها عن الجريمة التي يكون تأثيرها متعلقاً بعدد أكبر من الأجهزة. ويجب على المشرف بعد تحديد هذه الأجهزة أن يجمع أكبر قدر من المعلومات عن تلك الأجهزة، مثل:
  - نظام التشغيل
  - الخدمات العاملة على ذلك الجهاز
  - المعلومات المخزنة على ذلك الجهاز
  - موقع الجهاز في الشبكة الخاصة بالمنظمة
  - العتاد الموجود في الجهاز

في حالة التصميم والإشراف السليم على الشبكة، فإن معظم هذه المعلومات يجب أن تكون متوفرة قبل حدوث الهجمة. لأنها ستفيد بشكل كبير في التعامل معها.

- **تحديد نوعية الجريمة**: يعتمد التعامل مع الجريمة على نوعيتها. وذلك ينطبق كذلك على الجريمة في الحياة الواقعية. فالشرطي عندما يقوم بالتعامل مع جريمة سرقة لمنزل معين، فإنه يستطيع أخذ وقته ومحاولة جمع أكبر قد من المعلومات، ولكن في حالة وجود جريمة استخدم فيها السلاح، ويوجد مصابين فمن الضروري التعامل معها بشكل سريع وطلب الإسعاف، لنقل المصابين للمستشفى، ومن ثم القيام بجمع المعلومات المطلوبة. وكذلك هو الحال في

جرائم الشبكات. فيجب على المشرف على الشبكة تحديد نوعية الجريمة أولاً، ومن ثم يقوم بتحديد طريقة التعامل معها، فجريمة هجمات منع الخدمة مثلاً، يختلف التعامل معها عن هجمات اختراق الموقع وتغيير محتوياته.

١١-٢-٢ اتخاذ القرار

تعد هذه هي الخطوة الفعلية تجاه التخلص من آثار الهجمة، وهي من أصعب الخطوات التي يترتب عليها الكثير من العواقب والتبعات. وهناك الكثير من الخيارات التي تتوفر للمشرف على الشبكة عندما يريد البدء في التخلص من الآثار المترتبة على الهجوم، وهذه الخيارات لا يمكن حصرها بشكل كامل في هذا الكتاب، ولكن يمكن تقديم بعض الأمثلة على تلك الخيارات وكيفية الوصول للاختيار الصحيح:

١١-٢-٢-١ إعادة التركيب

لعل من أسهل الخيارات للمشرف على الشبكة في حالة اختراق جهاز معين، هو إعادة تركيب نظام التشغيل بشكل كامل. أو في حالة الهجمة التي تقوم بتغيير الموقع فإن المشرف قد يقوم باسترجاع الصفحات الرئيسة وإعادة الموقع للشكل السليم.

هذا الإجراء سيقوم بالتخلص من أثر الجريمة بشكل سريع، ولكنه لن يكون بالتأكيد بشكل دائم. فمثلا، يمكن أن يتعرض جهاز معين للاختراق من دون أن يحتوي على ثغرات أبداً، ولكنه تعرض للاختراق كنتيجة لاختراق أجهزة أخرى، ووجود علاقة ثقة بينه وبين تلك الأجهزة. ففي هذه الحالة يمكن إعادة تركيب النظام في ذلك الجهاز، والتأكد من التخلص من الجريمة في تلك الأجهزة بطريقة أخرى. ولكن إذا كان الاختراق ناتجًا عن عدم تحديث الجهاز، ووجود ثغرة في نظام التشغيل، فإن إعادة تركيب الجهاز سيزيل أثر الجريمة بشكل مؤقت ولكنه ليس دائمًا، حيث إن المخترق يستطيع استخدام نفس الثغرة مرة أخرى لاختراق الجهاز.

بالإضافة إلى ذلك فإن إعادة تركيب النظام قد يعني إزالة بعض الأدلة التي قد يستفاد منها في الوصول للمجرم. لذا يجب على المشرف على الشبكة التأكد من أن إعادة تركيب النظام هو الخيار السليم للتخلص من الجريمة.

١١-٢-٢-٢ إبقاء الجهاز مرتبطا بالشبكة أو عزله

وهذه هي أحد الخيارات التي تواجه المشرف على الشبكة عن حدوث جريمة معينة على أحد الأجهزة في شبكته. حيث يمكنه أن يقوم بالتعامل مع الجريمة والجهاز مرتبط بالشبكة، أو مفصول عنها. في بعض الأحيان، فإن هذا الخيار لا يكون موجوداً أصلاً، مثل أن يكون الجهاز المخترق هو جهاز يستقبل تعاملات مالية من شركات أخرى، ولا يوجد منه نسخة احتياطية، وفي نفس الوقت فإن الاختراق الحاصل لا يؤثر على صحة البيانات المالية، ولكنه يتعلق بناحية أخرى من الخدمات الموجودة في الجهاز. ففي هذه الحالة فإنه من الضروري إبقاء الجهاز عاملاً، وإلا فإن الشركة ستخسر الكثير من التعاملات المالية. وفي أحيان أخرى وفي حالة جهاز آخر مشابه لذلك الجهاز في الوظيفة وفي الإعدادات، فإنه من السهل جداً عزل الجهاز المصاب وتبديله بالجهاز الاحتياطي حتى يتم إصلاح الجهاز الأصلي والتخلص من أثر الجريمة بشكل كامل.

ولكن هناك حالات أخرى تكون المعطيات فيها أعقد بكثير مما هو أعلاه، وفي تلك الحالة فإن القرار يرجع للمشرف على الشبكة، ويجب عليه اتخاذ القرار الذي يترتب عليه الضرر الأقل.

١١-٢-٣ عدم مسح آثار الجريمة

يوجد قسم مهم من علوم أمن المعلومات يختص بكيفية فحص الجهاز المصاب، والحصول على الأدلة الكافية لتحديد المجرم وهو علم التحقيق في جرائم الحاسب. وهذه من الإجراءات التي غالباً ما تتم بعد إيقاف فاعلية الجريمة، ورغبة المشرف على الشبكة في ملاحقة المجرم ووضعه تحت يد العدالة. وهذا القرار يعتمد بشكل كبير على سياسة الشركة تجاه الاختراقات، فبعض الشركات لا ترغب في الخوض في النواحي القانونية وملاحقة المجرمين وصرف المبالغ الطائلة في محاولة وضعهم في السجون. ولكن هناك شركات أخرى قد ترغب في ذلك.

إذا كانت سياسة الشركة أو المنظمة تتطلب ملاحقة المجرم، فإنه يلزم المشرف على الشبكة أن يقوم بكل ما يلزم لكي لا يفقد الأدلة المتعلقة بالجريمة. وهذا ما يجعل التعامل مع الجريمة يختلف عنه في الحالة الأخرى. ولن نخوض في تفاصيل هذه العملية فهي معقدة وخارجة عن نطاق الكتاب، ويوجد الكثير من الكتب التي تتحدث عنها بشكل مفصل وكافٍ.

١١-٣ الحماية بعد وقوع الجريمة

تمثل هذه الخطوة تكراراً ومراجعة للخطوة الأولى (الحماية قبل وقوع الجريمة). حيث إن الاستعداد واتخاذ الحذر من الجريمة لا يعني استحالة حدوثها، وحدوث الجريمة الحالية أكبر دليل على ذلك. لذا فمن الضروري على المشرف على الشبكة أن يقوم بمراجعة ما عمله في الخطوة الأولى، ومعرفة مصدر الخلل سواء كان في السياسة الأمنية أو الإعدادات أو خلافه. ومن ثم يجب عليه أن يقوم باتخاذ ما يلزم لضمان عدم حصول ذلك مرة أخرى. وكثيراً ما يكون الخلل في السياسة الأمنية أو في تطبيقها، وهذا يتطلب من المشرف على الشبكة أن يقوم بتحديث السياسة الأمنية والتأكد من تطبيقها بشكل سليم.