الفصل 14

السياسات والإجراءات

تستخدم معظم المنظمات السياسات والإجراءات الأمنية للشبكات والنظم لغرض ضمان أمن المعلومات ويمكن التحقق من ذلك من خلال تحديد ما يهدد أمـن المعلومات، ومن المهم، تحديد كيفية المحافظة على المعلومات،وبالإضافة إلى ذلك ان تكون سياسات وإجراءات تحديد مستويات أمن المعلومات مقبولة. وقبل القيـام بذلك يجب عليك أولا وضع العملية التي تمكنـك مـن تحديـد المسـتوى الكـافي مـن الأمن لأية منظمة معينة.

يجب أن نتذكر ما تم نقاشه في الفصل 1 بأن عناصر أمن المعلومات تشمل السرية والنزاهة والوفرة، والتوثيق، ومراقبة الـدخول،ولابـد مـن معالجتهـا بخمسـة عناصر من سياسات وإجراءات يتم تنفيذها لمعالجة أمـن المعلومـات بصـفة عامـة، والسياسات الأمنية هي مجموعة من القواعـد والإجـراءات الـتي تنظـم كيفيـة ادارة المنظمة، والاستخدام، والحماية، وتوزيع كافة المعلومات التي تنتمي بشكل مباشــر أو غير مباشر لتلك المنظمة.

السياسات قبل الإجراءات:

ينبغي دائماً وضع السياسات قبل الإجراءات. وضع الإجراءات ينبغي أن تتدفق من السياسات. وينبغي أن تكون السياسات المعنية مع الأصول لحماية ما يحتــاجون إليه من الحماية. وهي واسعة عموما في نطاقها، ومصممة لضبط الصوت والاتجـاه. بشكل عام، فإنها يمكن أن تكون من حيث الفكر الوثـائقي تـبين اهميـة المعلومـات الأمنية للمنظمة،والإجراءات من ناحية أخرى يجب أن تكون أكثر دقة وتفصيلا بكثير. كما ينبغي أن تكون الإجراءات مهتمة بوضع التدابير المحددة اللازمة لحمايـة أصـول المؤسسة. فإنها يمكن أن تكون من حيث الفكر الوثائقي التي تنتهجه للحفاظ علــى أمن المعلومات داخل المنظمة.

أهداف سياسة أمن المعلومات:

هناك عدة أسباب للمنظمة لتطوير سياسات وإجراءات الشبكة وأمن النظام. بعضها واضح، في حين أن البعض الآخر ليست واضحة جدا. بعض الأسـباب تتعلـق بالفائـدة المباشرة حيث تحقق المنظمة مكاسب من وجود السياسات والإجراءات، مثل منـع أواكتشاف الغش أو ردع المتسللين. اما الفوائد الأخرى الغير مباشرة مثل سياسات حماية المنظمة من المسؤولية المحتملة أو حفظها من الإحراج. ولقد أدرجت بعــض الأهداف المرتبطة عادة مع سياسات أمن الشبكات:

• مخاطر العضو المنتدب: إن الهدف الرئيسي من أي سياسة تتعلق بـأمن الشـبكة والنظام لإدارة المخاطر, تكاد تكون من المستحيل التأمين التام لأصول المعلومـات في المؤسسة. ونتيجة لـذلك، تحتـاج المنظمـة إلـى تحديـد المخـاطر الـتي تواجههـا ووضع تدابير للحد من تأثير تلك المخاطر.

• ضمان اسـتمرارية العمـل: يجـب أن تكـون العمليـة الجاريـة فـي المنظمـة هـدف أساسي من السياسات التي وضعت من قبل أي منظمـة. ومـن المـثير للاهتمـام أن نلاحظ ميل سياسات المنظمات على توضيح ما لا يمكـن القيـام بـه بقـدر كـبير مـن التفصيل ولكن القيـام بأعمـال خاطئـة للغايـة مـن اجـل معالجـة مـايجب القيـام بـه لضمان التشغيل للمنظمة. ينبغي للسياسات والإجراءات التنظيمية ضمان اسـتئناف الأعمـال الـتي تحـدد الإجـراءات المناسـبة الضـرورية فـي وقـت وقـوع الحـادث أو الكارثة.

• تحديد المسؤوليات، والتوقعات، والسلوكيات المقبولة: للحصـول علـى أي سياسـة أو إجراء فعّال، يجب على الأفـراد الـذين يقومـون بالسياسـة أو الإجـراء فهـم م ـاهو مطلوب منهم للامتثال. لايمكن أن يتحقق الامتثال لسياسة دون التوصل إلى فهم ما يشكل الامتثال. وبالإضافة إلى ذلك نجـد المـوظفين بحاجـة إلـى فهـم مسـؤولياتهم وكيف قد تختلف مسؤولياتهم تبعا للظروف.

• تفريغ واجب الأمانة والامتثـال للمتطلبـات التنظيميـة: معظـم المنظمـات تخضـع لقواعد أو لوائح تنظم مسؤولية موظفي الشركات وتنظم عمـل المؤسسـة. اذا تـم تداول الواجب الائتماني لموظفي الشركات لضمان السلامة الماليـة للمنظمـة. وإذا فشلوا في ذلك يجب عليهم أن يكونوا مسؤولين شخصيا عن الخسائر التي تكبـدتها. مطلوب من معظم المنظمات الالتزام بمعايير معينة عندما يتعلـق الأمـر بالسـجلات المحاسبية ومسك الدفاتر. العديد من المنظمات تخضـع لدولـة اتحاديـة، أوالقـوانين المحلية التي تتطلب اتخاذ تدابير معينـة لحمايـة أصـول المنظمـة أيضـا. العديـد م ـن المنظم ـات تخضـع للقواعـد والأنظمـة المتعلقـة بحمايـة والإفصـاح عـن المعلومـات المتعلقة بالموظفين والعملاء. وهذا صحيح بالتأكيد في القطاعـات الماليـة والصـحة. هذا بالنسبة للعديد من المنظمات، ويـودي غيـاب السياسـات والإجـراءات المناسـبة لعدم الالتزام التلقائي.

• حماية المنظمة من المسؤولية: غالبا ما يطلـب مـن السياسـات والإجـراءات الـتي وضـعتها منظمــة لحمـايته مــن المســؤولية. فــي بعــض الحــالات، وجــود سياســات وإجراءات ضرورية لإثبات أن المنظمة لم يوافق من الإجراءات المسـتخدم النهـائي أو أن الموظف أو لم يتصرف بإذن من المنظمة.

• ضمان سلامة المعلومات وسريتها: مكـون رئيسـي لأمـن المعلومـات هـو حمايـة أصول المعلومات في المؤسسة. ضمان سلامة وسرية المعلومـات فـي المؤسسـة أمر أساسي لتحقيق هذا الهدف. لا يمكن أن تجعل القرارات التجارية السـليمة دون سلامة المعلومات، وهي منظمـة. دون سـرية المعلومـات، والمنظمـة تفقـد قـدرتها التنافسية من خلال فقدان المعلومات السرية المتعلقة بالمنتجـات، والعملاء، وحـتى الشركاء والموردين.

تطوير سياسات الأمن:

لسياسات وإجراءات أمن المعلومـات فـي المؤسسـة لتحقيـق الأهـداف المـذكورة، فمن الضروري أن يتم تضمين بعض العناصر في السياسات والإجراءات.

ويمكن اعتبار هذه العناصر من تدابير رئيسية من أجل نجاح السياسـات والإجـراءات المنظمة. العناصر هي الحجارة التي يخطى بها في عملية التنمية. يتم سـردها علـى النحو التالي:

• تحديد أصول المنظمة.

• تحديد المخاطر.

• تحديد كيف هي أصول المعلومات إلى أن تدار.

• تحديـد كيفيـة يمكـن الوصـول أصـول المعلومـات ومـا هـي العمليـة الـتي سـيتم استخدامها من أجل المصادقة.

• تحديد بوضوح وبالتفصيل ما يفعل والتي لا تشكل الاسـتخدام المناسـب للشـركة المملوكة الإعلام والخدمات الإلكترونية.

• تحديـد مـن الواضـح أي نـوع مـن المعلومـات يمكـن الوصـول إليهـا وتوزيعهـا .. وماذايعني.

• تحديد ماهي ضوابط توضع في مكان.

• إخطار مستخدمي إجراءات الرصد والتدقيق والإفصاح عن المعلومات، وعـواقب لعدم الامتثال.

• تحديد المسؤولين عن إنفاذ الأمن وكيف سيتم فرض السياسات والإجراءات.

• خطوات التطوير الواجب اتخاذها في حـال عـدم الامتثـال للسياسـة، وهـو خـرق أمني، أوكارثة.

الخطـوة الأولـى هـي تحديـد المسـؤولية عـن وضـع سياسـات أمـن المعلومات.

في كثير من الأحيان تكون وحدة تكنولوجيا المعلومات هي المسؤولة. ومع ذلك، إذا كانت السياسات والإجراءات شاملة، سوف تتطلب المشاركة الفعالة لجميع وحدات الأعمال. يجب أن يكون وضع سياسات أمن المعلومات جهد تعاوني بين وحدة تكنولوجيا المعلومات ووحدات الأعمال الأخرى داخل المنظمة. أي أن تنفيذ سياسة وإجراء دون مشاركة نشطة من وحدات الأعمال الأخرى ستواجه معركة شاقة.

العامل الأكثر أهمية في نجاح أو فشل أي سياسة لأمن المعلومات هو الدعم من الإدارة العليا. حيث يجب تمكين تطوير السياسة من قبل الإدارة العليا مع السلطة لتنفيذ التدابيراللازمة لحماية أصول المعلومات للمنظمة. حقيقة لا نستطيع تأكيد هذه المعلومة بقوة كافية من دون دعم الإدارة العليا للسياسات والإجراءات.

هنالك فرق تحاول تنفيذ الإجراءات فقط لرؤية جهودهم متراجعة عن فشل الإدارة العليا لعدم دعمه المقاومة المواجهة. كان وضع فشل الفريق بتوجيه تهمة إليهم بالعمل على تطوير وتنفيذ الإجراءات الأمنية ولكن لا سلطة مع السلطة اللازمة لتحقيق النجاح. ونتيجة لذلك، فإنها اعتبرت في نهاية المطاف كما انهم اشرار مستهدفين من قبل الجميع. في الأساس، قد حكموا عليهم بالفشل. إذا لم يكن لدى المجموعة وضع لسياسات الدعم النشط من الإدارة العليا فمن الأفضل عدم محاولة مزاولة المهمة.

الإدارة العليا يجب أن تفعل أكثر من مجرد دعم لتطوير وتنفيذ السياسات والإجراءات. تحتاج الإدارة العليا لدعم ثقافة أمن المعلومات داخل المنظمة. يجب أن يكون هناك اعتراف بالحاجة إلى أمن المعلومات داخل كل منظمة. للأسف، في معظم الشركات غالبا ماينظرون إلى أمن المعلومات على أنها شيء يمكن أن يتم تناولها في أي وقت آخر. لم يعترف بها على أنها الكفاءة الأساسية المطلوبة للشركة. هذه المغالطات العقلية يمكن تعرض وضع المنظمة للخطر.

يمكن النظر في المثال التالي: طالب في احدى الصفوف روى قصة تدل على القيمة التي تجعل معظم الشركات تهتم في أمن المعلومات. عمل الطالب لشركة برمجيات كبيرة بتسويق قاعدة بياناتها المعروفة. ومن خلال الهبوط الدوري في مجال الأعمال التجارية، ذهبت الشركة من خلال جولة لمكان ما يسمى مجازا "rightsizing". في حين شهدت معظم وحدات الأعمال تخفيضات معتدلة في الموظفين، ودمر أمن المعلومات ومجموعات التخطيط استئناف العمل. وفي الأساس، تم حل كل من الوحدات، وكانت قد وضعت جميع العاملين بالخروج. من

الواضح، ان الشركة لاترى أمن المعلومات واستئناف العمل كنشاط للأعمال الهامة.

وكمثال آخر، في شركة حيث كنت في مرة واحدة عملت فيها ، قدمت إلى الإدارة العليا توصية بأن الشركة تحتاج تطويرسياسة المعالجة "ذرع الدعوة". ذرع الدعوة هو ممارسة واسعة الانتشار تستخدم من قبل وسطاء المعلومات للحصول على المعلومات عن الأفراد من الشركات المستقرة. عموما، وسيطا لمعلومات يشكل كشخصأ وكجهة ترتبط مع الفرد ومع من يفعل الشركة المستهدفة الأعمال. الشركة المستهدفة يمكن أن تكون مستشفى، مؤسسة مالية، شركة التأمين، أو حتى وكالة المدرسة أوالحكومة.

وسيط المعلومات عادة مايحصل على القليل من المعلومات من كل جهة اتصال. المعلومات التي تم جمعها هي تراكمية.

كالاتصال مع وسيط المعلومات يحصل على مزيد من المعلومات، والتي بدورها يمكن استخدامها للحصول على أكثر من ذلك. ويجري ضرب العديد من الشركات من خلال ذريعة الدعوة. على الرغم من أن وسيط المعلومات يكمن ويشوه نفسه أو نفسها للشركة المستهدفة ،هذه الممارسة ليست غير قانونية. الشركات تعطي دون قصد من المعلومات عن موظفيها، والعملاء. انها ليست فقط سيئة للعميل، لكنه أمر سيء للأعمال التجارية.

وبالإضافة إلى ذلك، يمكن للشركة أن تجد نفسها مسؤولة عن كيفية استخدام هذه المعلومات. انها بالتأكيد لن تغرس الثقة للعملاء لمعرفة أن الشركة كانت تعطي من معلومات للعميل لأي شخص مدعي. لهذا السبب، نوصي السياسات والإجراءات وضعها لتصدي ذريعة الدعوة.

على وجه التحديد، كانت توصيتي على ان الشركة ينبغي أن تضع سياسة خصوصية المعلومات العامة. سيكون جزء امن تنفيذ تلك السياسة لتشمل برنامجا تدريبيا لتثقيف موظفيها على كيفية التعرف على ذريعة المكالمات. وذكرت أن ذلك من شأن شركتنا أن توفر ميزة تنافسية في أننا يمكن أن نعلن لعملائنا أن معلوماتهم كانت أكثر أمنا معنا من منافسينا. وبالإضافة إلذلك، فإنه حماية الشركة من المسؤولية المحتملة. وأخيرا، فإنه يوفر للشركة مع استجابة للعملاء الذين اتصلوا بنا مع طلبات للحصول على معلومات حول كيفية التعامل مع حدوث مثل هذاالنوع.

اعتقدت الإدارة العليا أنها فكرة جيدة ولكنها ليست ذات أولوية عالية، وهكذا انتهت.

لا أحد يريد استثمار الوقت لتطوير هـذه السياسـة. دون الـدعم النشـط مـن الإدارة العليا، كـان يمكـن أن يكـون مـن المسـتحيل وضـع سياسـة ومحاولـة فرضـها علـى وحدات الأعمال الأخرى.

شائع آخر هو للمنظمات وضع سياسـات دون سـبب سـوى أن نقـول إن السياسـات الموجودة. السياسات هي حقـا للعـرض فقـط مـرة واحـدة فـي العـام، عنـد وجـود المنظمين أو المدققين في الموقع، يمكن للشركة أن تشير إلى أدلـة سياسـة جمـع الغبار في الزاوية وتعلن بفخر أن لديهم كل السياسات المطلوبة المغطية. وبطبيعـة الحال، فإن حقيقة أن لا أحد يعرف سياسات أوما إذاكـان أو لـم تكـن الشـركة فـي الامتثال للسياسات لا يعتبر.

جزء أساسي من وضع السياسات الأمنية هوعمليـة تقييـم المخـاطر. مـن المهـم أن تذهب من خلال عملية تقييم المخاطر لتحديد ما تريـد حمـايته، لمـاذا تريـد حمـايته، وعنما كنت بحاجة إلى حمايته. كما هوموضح فـي الفصـل 1، والخطـوات المرتبطـة بتقييم المخاطر تشمل ما يلي:

1. تحديد وترتيب أولويات الأصول؛

2. تحديد نقاط الضعف.

3. تحديد التهديدات والاحتمالات بها؛

4. تحديد المضادات؛

5. تطوير تحليل التكاليف والمنافع.

6. تطويرالسياسات الأمنية.

الخطوة الأولى هي تحديد وترتيب أولويات الأصـول والنظـم ومـن ثـم تحديـد نقـاط الضعف المرتبطة بتلك الأصول. عند تقييم نقاط الضـعف والمخـاطر المرتبطـة بهـا، من المهم التخلص من تهديدات محتملة من تلك المحتملة،وينبغـي أن تكـون عمليـة واحدة لتحديد ماهي الأرجح للتهديدات ووضع السياسات التي تعالـج تلـك التهديـدات والقضايا.من المهم جدا أن السياسات والإجراءات المنفذة داخل أي منظمـة ينبغـي أن تكون القائمة على العالم الحقيقي. وبعبارة أخرى، ينبغي للسياسات والإجراءات القائمة لغرض تعزيزعملية موجودة من قبل أو وظيفة. علـى هـذا النحـو، ينبغـي أن يأخذوا في الاعتبار القيود من العالم الحقيقي وليس محاولة لتحقيق قمة الأمن.على سبيل المثال، قد تكون مبالغة تتطلب كافة رسائل البريدالإلكتروني لتكون مشـفرة. يجب أن لا تتطلب كلمات المرور إلى تغيير كـل أسـبوع أو تتطلـب منهـم أن تتكـون

من 15 حرف أبجدي رقمي في الطول. في حين أنه قد يكـون آمـن جـدا، فـإنه لـن يكون من المنطقي لتنفيذ ماسح ضوئي يدل تحديد البيومترية في بيئـة مثـل "غرفـة نظيفة"، حيث ارتداء الفنييـن للـدعاوى الخاصـة، بمـا فـي ذلـك القفـازات،وكقاعـدة عامة، فان السياسات والإجراءات الأمنية التي تتداخل مع عملية منظمـة ذات قيمـة تذكر. هذه الأنواع من التدابير عادة مايتم تجاهلها أو القفز فوقها مـن قبـل مـوظفي الشركة، لذلك فإنهم يميلون إلـى خلـق الثغـرات الأمنيـة بـدلا مـن سـدها.إذا قمـت بإجراء عملية شاقة جدا أو مزعجه، فـان النـاس سـوف تتجاهلهـا. إذا قمـت بـإجراء عملية الوصول إلى غرفـة صـعبة جـدا،والنـاس سـوف تـدعم فتـح البـاب. إذا قمـت بـإجراء كلمـات السـر مـن الصـعب جـدا أن تعـرف،والنـاس سـوف تكتبهـا. جميـع التدابيرالأمنية (وليس فقـط السياسـات الأمنيـة)،كلمـا أمكـن ذلـك،ينبغ ي أن تكمـل الاحتياجات التشغيلية والتجارية للمنظمة.

الخطوات المتبعة في تنفيذ سياسة أمن المعلومات لتكون واضحة إلى حد ما:

1. وضع السياسات والإجراءات الأمنية بدليل مكتوب.

2. تطوير وعي المستخدم النهائي وبرنامج التعليم؛

3. تطوير عملية لإنفاذ السياسات وتنفيذها الداخلي؛

4. تطوير العملية للاستعراض الدوري وتحديث السياسات والإجراءات.

كتيبات السياسات والإجراءات:

السياسة الأمنية لتكون عمليه، لابد من توثيقها.

ويجب أيضا أن تكون الخطة متاحه كمرجع لجميع الخاضعين لهذه السياسة.

تحتـاج أدلـة السياسـات والإجـراءات إلـى أن تبقـى الحاليـة وتحـديثها مـع تغييـرات ضرورية.

يجب أن تنعكس التعديلات على الأنظمة والأفراد وأولويات العمل، والعوامل البيئيــة الأخرى في الخطة.

وهذا يعني استعراضات منتظمة ومتكررة لهذه السياسة.

تنسيق السياسات:

هناك العديد من الطرق المختلفة التي يمكن للمرء تنسيق بها السياسات. نوع الشكل غيرمهم نسبيا طالما أن السياسة هي مفهومة وتحقق النتائج المرجوة.الشيء الأكثر أهمية هو أن السياسات رسمية وموثقة في بعض الطرق،وينبغي أن تتضمن السياسة،كحد أدنى،على العناصرالتالية:

• بيان السياسة العامة: وينبغي لهذا القسم نص السياسة العامة،على ماتنص عليه السياسة،وماتنطوي عليه. هذاالقسم يمكن أن يكون قصير بقدر جملة واحدة أو طويلة مثل صفحة. إذا كان يتجاوز صفحة،وربما تحاول تغطيته في قضايا السياسة الوحيدة التي يجب أن تشملها أكثر من سياسة واحده.

• الغرض: وينبغي لهذا القسم ذكرالسبب لحاجة القسم إلى السياسة. ومن أمثلة هذا الغرض للسياسة تشمل مامعناه أن السياسة هي حماية الشركة أو موظفيها،وضمان استمرار عمل المنظمة،أوحماية الصحة المالية للشركة.

• النطاق: ينبغي أن يغطي هذا القسم مدى تمدد هذه السياسة. يجب على النطاق توضيح الظروف التي تنطبق عليها هذه السياسة. كما يمكن أن تشمل الإطار الزمني، الأجهزة أوبرامج معينة ، و / أوالأحداث التي بموجبها تصبح هذه السياسة فعالة.

• التوافق مع السياسة: يجب أن يتضمن هذا القسم شرح مفصل لما يتم فعله والتي لا تتماشى مع السياسة. ويمكن أن تشمل القسم الأمثلة، ولكن كن حذرا في كلمة في مثل هذه الطريقة. لتشمل الحالات التي قد لاتكون مدرجة في الأمثلة الخاصة بك. وينبغي أن يشمل القسم صياغة التأثيروتشمل الأمثلة، ولكن لا تقتصر على أن تكون محددة جدا في التفاصيل مما قديجعل التعريف ضيق جدا.

• العقوبات / العواقب: هذا القسم يجب أن يوضح عواقب عدما لامتثال لهذه السياسة. يجب أن يتم سرد العقوبات المحددة المرتبطة بعدم الامتثال. إذا كانت عواقب لعدم الامتثال يمكن أن تشمل الإنهاء ، ثم أنه يجب أن تحدد بصورة واضحة في هذا القسم هذه السياسة. يخدم هذا القسم بمثابة تحذير للموظفين ويمكن أن تحمي المنظمة في حال أنها تجد نفسها في المساءلة نتيجة لإنهاء الموظف لعدم الامتثال لهذه السياسة.

حقيقة أن المنظمة قد حذرت بوضوح جميع الموظفين من عواقب يمكن أن تقل لأي حجة التي قد تقع على الموظف للإنهاء دون سبب.

التوعية السياسية والتعليم:

السياسة لا قيمة اذا لم يكن احد يعرف ما ينص عليها.

يجب على المستخدمين النهائيين والأفـراد علـى فهـم توقعـات الإدارة ومسـؤولياتها فيمـا يتعلـق بالامتثـال لسياسـات المنظمـة. يجـب علـى المسـتخدمين النهـائيين والموظفين أيضا فهم عواقب لعدم الامتثال.

وهذا الجانب مهم جدا لحماية المنظمة إذا كانت النتائج تقضي من عدم الالتزام.

قد تكون هنا كحاجة إلى وجود سياسـة لاتخـاذ إجـراءات عقـوبيه ضـد المسـتخدمين النهائيين أو الموظفين الذين تصرفوا بطريقة غير مقبولة.

المنظمات التي ليس لديها سياسة واضحة تحدد السلوك غير المقبـول. يمكـن أيضـا قد لا يكون اللجوء لوجود سياسة في المكان الذي يحظر أنواع معينـة مـن السـلوك من حفظ المنظمة من المسؤولية عن تصرفات المستخدمين النهائيين أو موظفيهـا. غياب سياسة رسمية وعملية الوعي قد تجعل من الصعب عقد الموظـف للمسـاءلة في حال تم اكتشاف بعـض السـلوك غيـر اللائـق مـن جـانب الموظـف. عنـد وجـود سياسـة مكتوبـة يمكـن للمنظمـة تثبـت أن أي إجـراءات مهينـة اتخـذتها المسـتخدم النهائي أو الموظف لم تكن في الامتثال مع السلوك المقبول، وبالتالي فالمنظمـة لا تتغاضى عنه.

ينبغي للمنظمات أن تنظر في الحصول على إقرار خطي من المستخدمين النهائيين والمـوظفين مشـيرا إلـى أن لـديهم قـراءة وفهـم لسياسـة أمـن المعلومـات فـي المنظمة. ويمكن القيام بذلك كجزء مـن التـوجه العـام للعـاملين المعينيـن حـديثا أو كجزء من تسجيل المستخدمين النهائيين الجديد.

تنفيذ السياسة:

الامتثال للسياسات يحتاج إلى القسري. الطريقة الوحيدة لضمان الامتثـال هـي مـن خلال الرصد والتدقيق. لإنفاذ المسؤولين لسياسات أمن تكنولوجيا المعلومات يجـب أن يكـون الـدعم مـن الإدارة العليـا. ولتصـبح سياسـة أمـن تقنيـة المعلومـات فـي المؤسسة ناجحة، فإنه تحتـاج أيضـا إلـى الـدعم مـن جميـع وحـدات الأعمـال داخـل المنظمة.

اقتراحات سياسة الأمن:

تذكر أن التركيز الرئيسي لجميع السياسات والإجـراءات هـو منـع "الأشـياءالخاطئة" من الحدوث. لايهـم مـا إذا كـان الشـيء السـيء خطـأ، كـوارث، أو إثـم.السياسـات والإجراءات مصممة تصميما جيد او مرنة بما فيها لكفاية لمعالجة معظـم التهديـدات المحتملة". هذا هو السبب في تحليل المخاطر هو مثل جزءا استيراد هذه العملية".

أيضا ينبغي للسياسات والاجراءات بافتراض أن التدابير الوقائيـة سـوف تفشـل فـي بعـض الأحيـان. ونتيجـة لـذلك، ينبغـي أن تشـمل خطـوات للكشـف عـن "الأشـياء الخاطئة". ومن المهم بصفة خاصة أن الإجراءات توضح بالتفصيل مـاهي الخطـوات التي يجب اتخاذها في حـال أن جميـع التـدابير الأخـرى قـد فشـلت فـي منـع بعـض "الخطأ" من الحدوث. وبعبارة أخرى، فإنه ينبغـي بالتفصـيل معرفـة كيفيـة اسـتجابة المنظمة للحادث.

عندما وضعت إجراءات تحتاج إلى معالجة العناصر الأساسية لأمن الشبكات الانظمة المشمولة في الفصل 2. وهي مدرجة على النحوالتالي:

• تحديد.

• مصادقة.

• التحكم في الوصول (إذن)؛

• توافر.

• السرية (السرية)؛

• النزاهة (الدقة)؛

• المساءلة.

في نفس الوقت، تحتاج إلى دمج كل العناصر المختلفة من الأمن في جميـع جـوانب العمليـة بالمنظمـة والتصـدي لجميـع الاحتمـالات،ويشـمل ذلـك إجـراءات لمعالجـة الكوارث الطبيعية للأمن والمادية وكذلك الأجهزة والبرامج الأمنيـة.تحتـاج أيضـا إلـى معالجة الضوابط لوسائل الاعلام والأمن والاتصالات.

الأهم من ذلك، تحتاج إلى معالجة المتغير البشري في الإجراءات الخاصـة بـك، فـي محاولة للحد من الإغراء والغباء وضمان الامتثال.

الإطار اللازم لمعالجة احتياجات تنظيم معين بشكل كاف يعتمد إلـى حـد كـبير علـى نوع من التنظيم. الشركات الكبيرة تتطلب سياسات واسعة النطاق التي تغطي كـل الاحتمالات، في حين أن معظم المنظمات الصغيرة، الـتي قـد تسـتخدم التكنولوجيـا لأكثر محدودية المدى أو على الأقل من ذلك، سوف تتطلـب مجموعـة أقـل اتسـاعا بكثير من السياسات.لا تستخدم رطل عنـدما تكـون اوقيـة (الاونصـة) كافيـة للقيـام بهذه المهمة.السياسات المعقدة بشكل مفرط أو مفصلة تميل إلى خلـق المشـاكل وغالبا ما يتم تجاهلها.

ينبغي أن تكون السياسات بسيطة لفهما وتذكرها. فإن مستوى التفاصيل لكل منظمة تختلف، ولكن توفر الأقسام التالية بعض الاقتراحات الأساسية.

استخدام وخدمات وسائل الإعلام المملوكة للشركة الإلكترونية:

مع ظهور تكنولوجيات جديدة، ومنظمات يجدون أنفسهم يعتمدون بشكل متزايد على وسائل الاتصال الإلكترونية وتخزين المعلومات. نجد معظم الموظفين في المنظمة من الوصول إلى واحد أو أكثر من أشكال وسائل الإعلام الإلكترونية أوالخدمة. وهي تشمل ولكن لا تقتصر على ما يلي:

- الكمبيوتر (الحاسوب الشخصي ومحطات العمل، متوسطة، وكبيرة)؛
- البريدالإلكتروني.
- الهواتف والبريد الصوتي،
- أجهزة الفاكس.
- الشبكات المحلية، الشبكات الداخلية، وشبكة الانترنت.

ينبغي أن يكون لكل منظمة تستخدم وسائل الإعلام والخدمات الإلكترونية سياسة تحدد بوضوح الاستخدام المقبول من هذه الوسائط والخدمات وممتلكات الشركة. وجود سياسات ليس فقط لحماية المؤسسة ولكن أيضا لحماية العاملين في المنظمة.

السياسة ينبغي أن تحدد الاستخدام الشخصي مقبول الملكية للشركة مرفق خدمات تكنولوجيا المعلومات.

السياسة ينبغي أن تشمل أيضا عندما يكون من الضروري الحصول على إذنا لإدارة وعملية للقيام بذلك.

هذه السياسة يجب أن تغطي كل التقنيات التي يمكن استغلالها لتلقي وتوزيع المعلومات. أنظمة الشركة والشبكات لا ينبغي أن تستخدم لتوليد أو توزيع مواد غير قانونية أو غير أخلاقية أو تخالف مبادئ الشركة. هذه السياسة تضمن أن يتم سن التدابير المناسبة لحماية أصول الشركة وتثقيف الموظفين بمسؤولياتهم.

في كثير من الأحيان، تشعر المنظمة بوضع سياسة لاستخدام البريد الإلكتروني كشيء مطلوب. لتكون السياسة فعالة حقا، يجب أن تشمل أكثر من مجرد بريد إلكتروني.

عندما يتعلق الأمر بتطوير مثـل هـذه السياسـة، يمكـن للمنظمـات تشـغيل سلسـلة كاملة من ليبرالية في نهجها وتعريفها بشكل عام إلى تعريفات ضيقة جدا من مــاهو الاسـتخدام المقبـول مـن ممتلكـات الشـركة مـع قيـود شـديدة علـى الاسـتخدام الشخصي.كل منظمة مختلفة النهج، والفلسفة يتـم إحضـارها لمهمـة وضـع سياسـة سوف تختلف اختلافا كبيرا من شركة إلى أخرى.

ما هو الغطاء السياسي ؟

من المهم جدا أن الموظفين أو المسـتخدمين النهـائيين فهـم مـا التقنيـات أو أنـواع تكنولوجيات الأغطية السياسـة. وفقـا لـذلك، تحتـاج المنظمـات لشـرح مـا لوسـائل الإعلام والخدمات الإلكترونية للشركة هي وما يترتب عليها.هو لمصـلحتهم ومصـلحة موظفيها أنهم يفهمون أن السياسة تغطي أكثر من مجرد بريد إلكتروني.

ما هي الملكية؟

ينبغـي أن تكـون سياسـة الدولـة بعبـارات واضـحة أن وسـائل الإعلام والخـدمات الالكترونية هـي ممتلكـات الشـركة، وليـس الممتلكـات الشخصـية للموظـف. علـى سبيل المثـال، المـوظفين فـي كـثير مـن الأحيـان يصـبح لـديهم غيـور حـول أجهـزة الكمبيوتر الخاصة بهم. انهم يشعرون كمـا لـو أن أجهـزة الكمـبيوتر هـي ممتلكـاتهم الشخصية، وأنه لا أحد لديه الحق في الوصـول إلـى أجهـزة الكمـبيوتر الخاصـة بهـم دون الحصـول أولا علـى إذن (المـوظفين). ينبغـي أن يكـون واضـحا فـي أي وقـت لحصول العاملين على أذن في مراجعة الملفات على أجهزة الكمبيوتر الـتي تملكهـا شركة، والبريد الإلكتروني، أوالبريد الصوتي.

هذا ليس تجسـس. الشـركات فـي بعـض الأحيـان ملزمـة لأداء هـذه الاستعراضـات لتحديد من بين أمور أخرى، ما إذا كان هناك خرق للأمن، وانتهاك سياسـة الشـركة، أو إساءة استخدام لأي وسائل الإعلام المملوكة للشركة أوالخـدمات.يجـب أن يق ال للموظفين أن الشركة تحتفظ بحقل أداء تلك التعليقات من دون إخطار مسـبق مـن الموظفين. نوضح للموظفين انه اذا كانوا لا يريدون الشركة لمعرفة شيء ما، فإنهـا لا ينبغي تخزينها على شركة مملوكة الممتلكات.

ماهو الاستخدام المقبول؟

تحـدد المنظمـة لنفسـها مـا إذا كـان سـيتم السـماح لوسـائل الإعلام والخـدمات الإلكترونية لاستخدامها لأغراض غير ذات الصلة بالشـركة. النهـج الأكـثر معقـول هـو السماح المحدود، استخدام في بعض الأحيان للأغراض الشخصية الغير تجاريـة (كمـا هوالحال مع المكالمات الهاتفية الشخصية). ومن المهم أيضا وجود سياسات متسقة مع بعضها البعض.فإنه لا معنـى للسياسـة لمنـع اسـتخدام شـركة البريـد الإلكـتروني

لأسباب شخصية ، بينما تتجاهل تماما المكالمات الشخصية الهاتف، والبريدالصـوتي، والفاكس.

كلما تقرر المنظمة، يحتاج قرار يتم لترحيل للموظفين بعبارات واضحة أن يوضح ما هي عواقب انتهاك هذه السياسة.يجب علـى المنظمـة أيضـا تحمـي نفسـها بـالقول خطيا أنه يحظر استخدام أي مـن خـدمات الشـركة الإلكترونيـة لأيـة أغـراض تنتهـك قوانين الدولة الاتحادية،ويشمل هذا بتطلب الامتثال لجميع قوانين حقوق النشـر. إذا كانت الشركة تقوم بتطـوير البرمجيـات، والسياسـة يجـب أن تشـمل أيضـا بـراءات الاختراع والعلامـات التجاريـة والملكيـة الفكريـة،وبالإضـافة إلـى ذلـك، يجـب وجـود سياسة تحظر استخدام الخـدمات المملوكـة للشـركة الإلكترونيـة لنقـل أو تلقـي أو تخزين معلومات أو بيانات من مضايقة أوطبيعة تمييزية أو التي هـي تحـط علـى أي مجموعة أوفرد.كما يجب على السياسـة بحظـر أي موظـف مـن اسـتخدام خـدمات الشـركة الإلكترونيـة لنقـل أو تلقـي أو تخزيـن المعلومـات أو البيانـات الفاحشـة أو الإباحية أو التي هي تشهيرا أو تهدد في الطبيعة.هذا لا يحمـي فقـط المنظمـة؛ لكـن هي حميت الموظفين كذلك.

القرصنة:

كما يجب علـى السياسـة بحظـر المحـاولات مـن قبـل المـوظفين أو المسـتخدمين النهائيين من "الاختراق" الى النظم الأخرى،ويجب توضيح ان محـاولات الاخـتراق أو الوصول إلى المعلومات دون إذن لن يتم التسامح فيه من قبل المنظمة، ويجـب أن تكون هنا كعواقب وخيمة على القيام بذلك.

ينبغـي أن تنطبـق هـذه السياسـة ليـس فقـط لمحـاولات القرصـنة علـى الأنظمـة المملوكة للشركة. يجب أن تنطبق أيضا على القرصنة للأنظمة الخارجيـة باسـتخدام الأنظمة المملوكة للشركة أوالخدمات.

بالإضـافة إلـى ذلـك، ينبغـي للسياسـة تحديـد مسـؤولية المـوظفين للتأكـد مـن أن معلومات تسجيل الـدخول الخاصـة وكلم ات السـر طـي الكتمـان والخطـوات الـتي كـانت مطلوبـة لاتخـاذ إذاكـانوا يشـتبهون فـي أن كلمـات المـرور الخاصـة بهـم قـد تعرضت لما يثير الشبهة.

يجب أن يكون واضحا أن هذه الخطوات ليست اختيارية أومقترحـة ولكـن هـي جـزء من المطلوب لوظيفة وظائفهم وأن عـدم الامتثـال للسياسـة يمكـن أن يـؤدي إلـى عواقب وخيمة.

البرامج غير المصرح به:

العديد من المنظمات تستخدم نهجا قطع الكعكة لنشر أنظمة سطح المكتب. كل شخص يحصل على نفس الصورة من مجموعة محددة من البرمجيات المعتمدة لديهم.

في حين أن هذا يمكن أن يكون مشددا بالنسبة للمستخدمين النهائيين، بلهو ممارسة الإدارة السليمة. على أقل تقدير، وهذا النهج يقلل من التكاليف المرتبطة بتركيب أنظمة سطح المكتب.هذا صحيح بشكل خاص عند استخدام حزمة مثل (SMS)، نظام إدارة خادم مايكروسوفت والذي يدفع في الأساس صورة على سطح المكتب من الخادم.يمكن لهذا النهج أيضا تقليل تكاليف الدعم للمؤسسة عن طريق الحد من عدد من التطبيقات التي تدعم مكتب المساعدة.

بشكل عام، هو ممارسة أمنية جيدة لديها سياسة تحظر المستخدمين النهائيين من تثبيت البرنامج على أنظمة سطح المكتب من دون إذن من مجموعة تكنولوجيا المعلومات.

بهذا يمكن منع البرامج الضارة على من يجري إدخالها إلى الشبكة.

عندما يتعلق الأمر إلى تثبيت البرنامج على الخادم، يجب أن لايكون هناك سوى سياسة في المكان الذي يحظر نشاط من هذا القبيل، ولكن ينبغي أن تكون آليات مراقبة الدخول في المكان لمنع مثل هذا النشاط.

في العديد من البيئات، قد يكون من الحكمة لتنفيذ التدابير التي تمنع المستخدمين النهائيين من تثبيت البرنامج على أنظمتها أو بأي طريقة تغيير لتكوين سطح المكتب لديها NTالخاص بهم. على سبيل المثال، يمكن تثبيت أنظمة سطح المكتب ويندوز قدرة تعطيل التكوين المحلي. ،يمكن تثبيت بعض البرامج المصممة لتأمين سطح Windowsالمكتب، مثل درع كامل، حصن 101، وإثبات كذبة مع نظام التشغيل 3.X،95و 98.توفر هذه النظم مستوى معين من الحماية، ولكن يمكن القفز فوقها، وفي بعض الحالات، في الواقع قد تشكل مخاطر.

البريد الإلكتروني:

ينبغي بذل بينة للموظفين على حقيقة أن البريد الإلكتروني ليس من وسائل الإعلام الآمن.

ليس هناك ما يضمن أن البريد الإلكتروني سيبقى خاص. وينبغي أيضا أن يتم على بينة من حقيقة أن البريد الإلكتروني المنقولة عبر الانترنت هو عرضة للاعتراض والكشف.

على هـذا النحـو، لا ينبغـي أن تنتقـل المعلومـات ذات الطبيعـة الحساسـة للغايـة أو سرية على شبكة الإنترنت ما لم يتم تشفير الرسالة.

يجب على كل منظمة لديها الحق في مراجعة والكشف عـن البريـد الإلكـتروني لأي موظــف لتلقــى أونقلــه أو مــن وســائل الإعلام الإلكترونيــة المملوكــة للشــركة أوالخدمات.

يجب أن يكون واضحا أن كل موظف يمكن أن يتم الاسـتعراض والإفصـاح مـن دون الحصول على موافقة مسبقة من الموظف. هذه ليست "الاخ الاكبر"، فمـن الحـس السليم.

والشركة لديها الحق في حماية نفسـها. كـان هنـاك عـدد مـن الحـالات فـي وسـائل الإعلام حيث هبوط الأنشطة غير لائق في المساءلة للموظـف مـن صـاحب العمـل. والعثورعلى أنشطة غير لائقة لاحقا بالتفصيل في البريد الإلكتروني للشركة. ونتيجة لذلك، فإنه يمكن للشركة ان عثورها على التشهيرلأنشطة الموظف.

وذكرت نتائج مسح الحواسيب فيما يتعلق برصد البريد الإلكتروني نشـرت فـي عـدد المجلة في اكتوبر تشرين الاول عام 1999 أن 31٪ من المشاركين في الاسـتطلاع قد ركبوا البرنامج التي تسمح لرصد نشاط مـن البريـد الإلكـتروني وأن 21٪ أخـرى كانوا يخططون حول تثبيت البرامج مع تلك القـدرة مـن المنتجـات مثـل جدارالبريـد التراسـل مـن MAمن تقنيات المحتـوى، ومـدير 2 MIMEمن أو من رباعية كاسحة إعادة لينة, توفر للمسؤولين مع القدرة على تفحص البريد الإلكتروني للمسـتخدمين النهائيين "عن الكلمات الرئيسية".يمكن لهذه البرامج تفحص كل من موضوع البريـد الإلكـتروني والجسـم للمحتـوى المشـكوك فيـه، الفـاحش، المسـيء، أوبصـورة غيرمشروعة.

تحديد:

ينبغي لأي سياسة اسـتخدام المقبـول لتغطـي المملوكـة وسـائل الإعلام والخـدمات الإلكترونيـة للشـركة أيضـا التعامـل مـع قضـايا توثيـق الهويـة والانتحـال.يجـب حـذر الموظفين من الاعتماد على الهوية المعلنـة للمرسـل مـن البريـد الإلكـتروني أو أي نوع آخر من الانتقال العدوى. يمكن بسهولة تزوير رسائل البريد الإلكـتروني بشـكل خاص،وينبغي لأي سياسة أيضـا منـع المـوظفين مـن أي محاولـة لإخفـاء هـويتهم أو تزوير تمثيل أنفسهم أو محاولة لتمثيل أنفسهم على أنهم اشخاص آخرين عنـد نقـل أو استلام أو تخزين البريد الإلكتروني أو الرسائل الإلكترونية الأخرى.

آثار التواصل:

أخيراً، ينبغي على المنظمة تحدد بوضوح العواقب على أي موظف يخالف علم السياسة أو يسمح لموظف آخر لانتهاك هذه السياسة، حتى لا يكون هناك أي إمكانية لسوء الفهم.لتطوير هذا النوع من السياسة للمنظمة، والإدارة العليا، تقنية المعلومات، تحتاج إلى موارد بشرية للعمل معا، ووضع سياسة شاملة تنظم استخدام وسائل الإعلام المملوكة للشركة والخدمات الإلكترونية التي يمكن أن تحمي المنظمة وتحفظها من المشاكل القانونية أسفل الطريق. لأن السياسة لتكون فعالة، يجب أن تشمل أكثر من مجرد بريد إلكتروني. والمنظمة لتجعل السياسة واسعة بما فيها الكفاية لدمج جميع التقنيات التي تستخدم في الوقت الحاضر،وفي الوقت نفسه، العناصرالفردية للسياسة يجب أن تكون محددة بدقة بما يكفي لجعلها ذات معنى ومفهومة.

وبالإضافة إلى ذلك، تحتاج السياسة إلى إعادة النظر دوريا للتأكد من أنه يتضمن تقنيات يتم تنفيذها حديثا.

معلومات الخصوصية:

من المهم أن الخطوات الفعالة يتعين اتخاذها لجميع الموظفين لضمان خصوصية المعلومات لدى البنك. ينبغي إعادة النظر في المعلومات المؤسسية المتعلقة بالعملاء، والموظفين، ومشاريع الشركة والمنتجات لتحديد مستواهم في الحساسية.هذا أمر مهم سواء من رجال الأعمال ومن المنظور التنظيمي. الكشف عن المعلومات الحساسة يمكن أن تساعد المنافسين لتخيف الزبائن.

وبالإضافة إلى ذلك، قد تكون الشركة أيضا تخضع لمتطلبات تنظيمية التي تحكم الكشف عن المعلومات بالمواقع على شبكة الإنترنت التي تلبي للأطفال وتخضع للأطفال عبر الإنترنت بقانون حماية الخصوصية، والتي يتم فرضها من قبل لجنة التجارة الاتحادية (FTC). اليابان ومعظم الدول الأوروبية لديها لوائح أكثر صرامة بكثير من الولايات المتحدة التي تنظم الإفصاح وتبادل المعلومات للموظفين من قبل الشركات. ونتيجة لذلك، يوصى بالسياسة العامة.السياسة ينبغي أن تحدد المتطلبات والمعلومات التي تحكم الإجراءات المنظمة للخصوصية.

وأخيراً، فإن سياسة المنظمات التي لديهم موظفين موجودين في كثير من الأحيان في مؤتمرات أو الذين عرضت عليهم محاضرات ينبغي أن تشمل ما يمكن وما لا يمكن الكشف عنها من قبل الموظف في عرضه أولها. السياسة يمكن أن تذهب أبعد من ذلك لتشمل بعض الانواع من عملية المراجعة من قبل إدارة المواد التي يجري تقديمها. هذا هو ضمان أن يتم الإفصاح عن أي معلومات الملكية أو العملاء الحساسة عن غير قصد.

المعلومات وإدارة البيانات:

اعتمادا على البيئة التي كنت تعمـل بهـا،قـد ترغـب فـي النظرفـي تصـنيف وترتيـب أولويات المعلومات من خلال مستوى من الأهمية أوالحساسـية. فـي المقابـل، ف إن طبيعة البيانات تملي التدابيراللازمة لحمايتها. وينبغي أيضاأن تملي تحديـد مسـتويات وصول حساسيةالمعلومات أوالبيانات.أيضا ينبغي لأي سياسة تحديـد حيـث يجـب أن تتواجد المعلومات وكيـف يجـب ان تكـون لنقلـه،نقـل،أونقلـه. ينبغـي أن تؤخـذ فـي مســتوى أهميــة وحساســية الاعتبارعنــد وضــع هــذه التعــاريف. علــى ســبيل المثال،المنظمة قد ترغب في قدرمن المعلومات ذات أهمية حاسمة من يتم نسخها إلى الوسائط القابلة للإزالة مثلا لأقراص المرنة أو الأشرطة.

المعلومات والبيانات هي أصول للشركات ذات قيمة ويجب حمايتها. ويمكن تعريف البيانات والمعلومات الخام،أويمكن تعريف المعلومات عن بيانات ذات مغزى تم تنظيمها بطريقة متماسكة تسمح لاسترجاع موثوق بها من عناصرالبيانات.واحـدة من المكونات الرئيسية لحماية المعلومات غير لتعيين الملكية.سياسة الملكية ينبغي أن تحدد مسؤوليات المعلومات والعلاقة مع خادم البيانات. أيضا السياسـات اللازمـة لمعالجـة إدارة اسـتباقية المعلومـات والبيانـات.يجـب أن تعالـج السياسـات تـوافر البيانات وضمان أن الضوابط المناسبة في مكانهـا الصـحيح والاسـتفادة منهـا. وضـع هذه السياسات يجب أن تتضمن تحليل المخاطر وإنشاء تصـنيف وترخيـص المعـايير المناسـبة للبيانـات. سـلامة المعلومـات والبيانـات ليسـت معنيـة فقـط مـع حمايـة المحتوى من المعلومات. يجب أيضا معالجة سلامة دقـة عناصـرالبيانات. وينبغـي أن تكون السياسة بشـأن سـلامة البيانـات وتحديـد المتطلبـات لتـأمين تخزيـن البيانـات والآليات للنسخ الاحتياطي للبيانات،ومتطلبات الإجراءات للحفاظ عليها واختبـار دقـة البيانات. فـي بيئـة مناسـبة،ويتضـمن سـلامة البيانـات أيضـا معـايير إدخـال البيانـات لضمان اتمام إدخال هذه المعلومات في شكل ثابت وموحد.لضمان سلامة البيانات، ينبغي سن سياسة تحكـم الإجـراءات المناسـبة للحمايـة مـن التهديـد المحتمـل مـن فيروسات الكمبيوتر.

ينبغي على السياسة أن تغطي متطلبات الفيروس بمسح ونسخ الملفات من مصادر خارجية للأنظمة المملوكـة للشـركة.ينبغـي للسياسـات إدارة المعلومـات والبيانـات أيضا وتذكير بأن جميع الملفات الموجودة على الأجهزة المملوكة للشركة أو وسـائل الإعلام، مثـل أجهـزة الكمـبيوتر، والأقـراص القابلـة للإزالـة، والأشـرطة، هـي ملـك للشركة. على هذا النحـو، ينبغـي للسياسـة بحظـر المـوظفين مـن إزالـة معلومـات الشركة من المباني دون ترخيص هذه السياسة، في حين مـن الصـعب فرضـها، قـد تكون شرعية مفيدة أن تكون في المكان.

وبالإضافة إلى ذلك، كإجراء وقائي، يجب على الشركة التي لديها الحق في فحص والنفاذ واستخدام والكشف عن أيأ وكل المعلومات أو البيانات أونقلها أو توريد، أوتخزينها على أي وسائل الإعلام الإلكترونية، الجهاز، أوالخدمة التي تملكها أو دفع ثمنها من قبل الشركة.

إدارة أنظمة:

واحدة من أكبر التحديات في وضع الإجراءات الأمنية المناسبة هو تحديد كيفية التعامل مع مراقبة ورصد مديري النظم المختلفة للمنظمة. على سبيل المثال، تعمل العديد من المنظمات في بيئة حيث تمنع الفرد أوالأفراد منا لوصول إلى المسؤولية عن جميعأ وجوانب إدارة النظام.قد يكون تنظيم وحدة تكنولوجيا المعلومات الصغيرة حيث استخدام ترسيم المسؤولية والفصل بين المهام كإجراء للسيطرة ليس عمليا. حيث كيف يمكنك فصل الواجبات عندما يكون هناك شخص واحد فقط في الدائرة؟

ومع ذلك،كلما كان ذلك ممكنا،ينبغي تنفيذ الفصل بين الواجبات. لاينبغي أن يكون الشخص أوالأشخاص المسؤولين عن إدارة يوما بعد يوم أيضا الفرد أوالأفراد المسؤولين عن إنشاء حسابات جديدة. وبالإضافة إلى ذلك، ينبغي للفرد أو الأفراد الذين ينشئون حسابات جديدة لن يكونوا مسؤولين عن تحديد مستوى الوصول نظرا لتلك الحسابات.ينبغي مراجعة جميع الحسابات الجديدة من قبل الفرد المسؤول عن إنشاء الحسابات. إذا كان ذلك ممكنا، ينبغي التمييز بين إدارة النظام وإدارة الأمن. يجب تدقيق وظائف إدارة النظام على الأقل سنويا.

ينبغي تسجيل جميع التغييرات في النظام والوظائف اليومية التي يقوم بها المدراء والمشغلين في السجل أوالجدول الزمني وينبغي مراجعتها يوميا. يجب تسجيل كل نظام نسخ احتياطي وتسجيل ومراجعة السجلات والاحتفاظ بها. وينبغي أيضا أن يتم اختبار النسخ الاحتياطي بشكل دوري، على الأقل أسبوعيا. يجب توثيق جميع تغييرات وصول الأمن، استعراض، والقدوم. وهناك أيضا سياسة تنص على الجدول الزمني للاحتفاظ بالسجلات وتدمير السجلات، والجداول الزمنية، وغيرها من الوثائق.

وبالإضافة إلى ذلك، يجب أن تصنف النظم وفقا لسريتها والحرجية لتشغيل المنظمة لتحديد التدابيرالأمنية المناسبة. مطلوب أيضا تصنيف النظام للتخطيط الواقي من الكوارث. ينبغي أن يعالج التدقيق النظام والتحقق من الصحة بطريقة ما من خلال السياسات. يمكن أن تكون إما دمجها في السياسات القائمة أوتكون في سياسة منفصلة. الفصل 15 يناقش التدقيق بمزيد من التفاصيل.

الوصول إلى الشبكة عن بعد:

العديد من المنظمات تطلب للوصول إلى الشبكة عن بعد. مجال مبيعات الموظفين والمهندسين، وحتى تسليم الموظفين والسائقين غالبا ما تتطلب الوصول إلى شبكة المؤسسة.

وبالإضافة إلى ذلك، مع نمو في بعد، والعديد من الموظفين يعملون الآن من المنزل، بدلا من أن تدخل المكاتب. ونتيجة لذلك، المزيد من الموظفين يتطلب عملهم الوصول إلى أنظمة الشركة من خارج شبكة الشركة. أي الوصول عن بعد إلى شبكة الشركة توجب السيطرة بإحكام والاخضاع للإجراءات الأمنية المشددة. سياسة الوصول البعيد ينبغي أن تتناول القضايا المرتبطة المصادقة والتحكم في الوصول.

كحدأدنى، يجب تتطلب السياسة أي اتصال للاستفادة من بعض الانواع من إجراء الآمن. لمزيد من التفاصيل يمكن الرجوع إلى المناقشة في الفصل 7 ID عناوين بشأن أجهزة المودم.هناك اعتبار آخر هو وصول الطرف الثالث إلى شبكة الشركة. لدى العديد من المنظمات البائعين والشركاء والعملاء، أوالمشاريع المشتركة التي تتطلب الوصول إلى شبكة الشركة. تحتاج السياسات الواجب تطويره الضمان تنفيذ الضوابط المناسبة وصيانتها ومراقبتها لجميع وصول طرف ثالث لشبكة المنظمة.

أمن الاتصالات:

يتعلق الوصول عن بعد بالقضايا المرتبطة بالاتصالات الآمنة. أنماط مختلفة من الاتصالات تخضع لإمكانيات مختلفة للإفصاح. أن السياسة بالتفصيل ماينبغي لها اتخاذ تدابيرعند استخدام كل من وسائط مختلفة من الاتصالات الإلكترونية، استنادا إلى حساسية المعلومات. الرجوع إلى الفصل 9 لمناقشة أكثر تفصيلا للقضايا المرتبطة بالأنماط المختلفة من الاتصالات.

الأمن المادي:

ينبغي أن يقتصرالوصول الفعلي إلى مرفقات تكنولوجيا المعلومات لهؤلاء الموظفين المخولين فقط الذين يحتاجون إلى الوصول إلى أداء مهام عملهم. ينبغي تحديد سياسة منهم الأفراد المناسبين وما العمليات والضمانات التي ينبغي سنها، ينبغي للسياسة أن تشمل أيضا عند الاقتضاء أصول الشركة من تكنلوجيا المعلومات التي هي في حوزة الموظفين.ينبغي أن تشمل غرفة الحاسوب أو مركز شبكة نظم إخماد الحريق والضوابط البيئية أنواع القضايا التي تناولها. على سبيل المثال، إذا لم يتم مراقبة غرفة الحاسوب باستمرار،وهناك النظام الآلي في المكان الذي فيه

صفحات شخص في حالة أن نظام إخماد الحرائـق يتـم تشـغيلهأ و بفشـل الضـوابط البيئية؟

استخدام المعايير:

ينبغي وضع السياسات التي تملي منصة معيارية أو بيئة التشغيل المشتركة التي يتم نشرها في جميع أنحاءالمنظمة. وينبغي أن يكون التمسك بالمنصة إلزامي. بالإضافة إلى تخفيض تكاليف ومتطلبات الإدارة للمنظمة، ويمكـن أيضـا وضـع معـايير حمايـة البيانات والبنية التحتية. تسـاعد المعـايير أيضـا فـي قابليـة التشـغيل الـبيني وقابليـة التطبيقـات فـي بيئـة الحوسـبة الموزعـة.يجـب حـتى اعتبـار معـايير لمظهـر سـطح المكتب. ليس هناك ماهو أكثر ازعاج لشخص من مجموعة تكنلوجيا المعلومات مـن أن يجلس في النظام وتجد أن كافة الرموز تم تغييرهـا إلـى صـور غيـر قياسـيه مثلا لزهـور والنحـل، والوجـوه المبتسـمة.الرمـوز غيـر القياسـيه تعرقـل عمليـة الـدعم. وبالإضافة إلى ذلك، تثبيت هذه الرموزغيرالقياسيه هو الخطرالأمني لأنه هـو مقدمـة للملفات الغير معروفه في الشبكة. وينبغي إيلاء الاعتبار لتقييـد الإدارة المحليـة مـن جميع أجهزة الكمبيوترالمكتبية لضمان أن تتم المحافظة على المعايير.

الإبلاغ عن عدم الالتزام:

في كثيرمن الأحيان، تقـوم المنظمـات بتثقيـف المـوظفين والمسـتخدمين النهـائيين على مسؤوليتهم بإبلاغهم عن عدم الالتزام ولكنها لم توضع في مكـان وآليـة لتـوفير تلك القدرة.هناك أوقات عندما يكون الموظف قد لايشعر بالراحة للإبلاغ عـن حادثـة عدم الامتثال. إذا كان عدم الالـتزام ينطـوي علـى المشـرف، مـديرنظم، أوالنشـاط الإجرامي الحقيقي للفرد قد يكون مخوف للإبلاغ عن حدوث خوفا من الانتقام.

في هذا النوع من الظروف نحتاج إلى أن نكون قادرون علـى تـوفير وسـيلة لتقريـر قضايا عدم الامتثال مجهولة. النظـر فـي إنشـاء خـط سـاخن للإبلاغ عـن مثـل هـذه الأمور. لضمان عدم الكشف عن هوية المتصل، النظر في اسـتخدام خدمـة خارجيـة أوطرف ثالث لهذها لوظيفة.

اتصال السياسات بالموظفين:

مقدمة:

هناك العديد من السياسات المتعلقة بالموظفين التي ينبغـي تنفيـذ الإجـراءات الـتي تؤثر في مجالات توظيف الموظف، إنهاءالخدمة، والحضور.

فحص ما قبل التوظيف:

قبل تعيين شـخص لمجموعـة تكنولوجياالمعلومـات، والتحقـق مـن جميـع المراجـع. لاتفترض أبدا ببساطة أنه بسبب شخص أعطى إشارات أن الإشـارة سـتكون جيـدة. التحدث إلى المراجع وسؤالهم عن المرشح.

نعتبرأيضا التحقـق مـن الائتمـان. سـوءالائتمان أوتاريـخ الإفلاس علـى الاطلاق علـى موظف محتمل قد تشيرإلى شخص غير مسئول، أوالـذي يعـانى مـن ضـائقة ماليـة. هذا هو إشارة إلى أن الشخص يمكن أن يكون خطرا محتملا، وخاصة إذا كان هــو أو هي سوف تشارك مع أنظمة معالجة المعاملات المالية. المؤسسـات الماليـة، علـى وجه الخصـوص، نـود أن لـديهم مـوظفين الـذين يتحملـون المسـؤولية مـن الناحيـة المالية. إذا كان ذلك ممكنا، والنظرفـي فحـص المخـدرات.يـرى العديـد مـن النـاس فحص المخدرات لتكون غزو للخصوصية، ولكن عند تعيين مـوظفين جـدد يمكـن أن تكون أداة مفيدة للتخلص من تطبيقات مشكوك فيها لدينا. ويمكـن أيضـا أن يطلـب من اختبار الدواء إذا كنت ترغب في الحصول على حدود الموظف.

سياسة العطلة الإجبارية:

ينبغي أن يطلب من كل موظف في وحدة تكنولوجيا المعلومات لاتخاذ اجازة خمسة أيام عمل على الأقل متتالية من كل عام. أيضا ضع في الاعتبار تدوير مهام ومسؤوليات الوظيفة،ومن المؤسف، في معظم الأحيان الموظف الذي اختلس من شركة أو قام بواقعة ارتكاب بعض الغش يعتبر دائما قريبا ليكون الموظف النموذجي حتى يتم اكتشاف الجريمة.غالبا ما يعتبر هؤلاء الموظفين أن يكونواعمال الصلب، لأنها تقريبا لم تأخذ أي وقت الخروج. والسبب أنه لم يأخذ إجازة لأن اذا كان شخص ما في شغل لهم في حين أنهم كانوا بالخارج، سيتم اكتشاف المخالفات. ونتيجة لذلك، وأنه يأتي في العمل كل يوم، والمرضى أوالصحة،دون أن يغيب.لهذا السبب، أوصي بأن المنظمات تعتمد سياسة على كل موظف اخذ اجازة خمسة أيام عمل متتالية، حتى يمكن لشخصا آخر أن يؤدي وظيفته.

سياسة حساب جديد:

عند إنشاء حساب لمسـتخدم جديـد أوالموظـف المسـؤول عـن النظـام يجـب أن لا يكون واحد لتحديد ماهو مستوى التفويض والوصـول إلـى تعييـن الحسـاب. ان هـذه السياسة تغطي عملية إخطار مسـؤول النظـام مـن حسـابات المسـتخدمين جديـدة ومسـتوى الوصـول المطلوبـة. وينبغـي أيضـا أن تكـون هنـا كعمليـة اسـتعراض المتابعة.يجب أن يتم تنفيذ اسـتعراض المتابعـة مـن قبـل شـخص آخـر غيرمسـؤول النظام للتأكد من أن مستوى الوصول المسندة إلى الحساب الجديد كـان المسـتوى المأذون.

الأمن وصول طلب التغيير:

عند طلب تغيير مستوى الوصول لحساب موجود،يجب توثيـق هـذه التغييـرات وأذن مــن قبــل شــخص آخــر غيرأطــراف الطــالب. عنــدما يتــم تنفيــذ تغييرمســتوى الوصول،ينبغي إعادة النظر من قبل شـخص آخـر غيرمسـؤول النظـام الـذي أجـرى التغيير.

إنهاء المرجعية لموظف:

في حالة إنهاء عقد الموظف،إمـا طوعـا أو كرهـا،يجـب حـذف جميـع الوصـول إلـى النظم، وجميع مفاتيح، وشارات، ينبغي استعادت الملفات،أوالمعدات. إذاكان المنهى عقده موظف مسؤول عن النظام يجب تغيير جميع كلمات السر إذا أمكن.

إذا لم يكن من الممكن تغيير جميـع كلمـات السـر،يجـب علـى الأقـل تغييـر كلمـات المرور للحسابات المميزة. إذا كان الموظـف طلـب فـي الوصـول،والنظـر فيتغييـر أرقام الهاتف. يجب لشخص آخر غير مسؤول النظام بمراجعة والتاكـد مـن امكانيـة الموظف للوصول لجميع الأنظمة قد تمت إزالتها.تحتاج الإجراءات أيضا إلـى تطـوير للتعامـل مـع المناسـبات الحرجـة، عنـدما يأخـذ دوران مكـان المـوظفين بتكنلوجيـا المعلومات. مواصفات لابد من وضعها لمعالجة الأجهزة والبرامج التدريبيـة للجـدران النارية وعمليات الشبكة. ينبغي على السياسة أن تسعى إلى تجنب السماح لتطـوير الوضع حيث وجود شخص واحد لديه كل المعرفة، وليـس هنـاك خطـة الخلافـة فـي المكان.

فريق حماية المعلومات:

ينبغـي أن تتضـمن أي سياسـة لأمـن المعلومـات للشـركات تشـكيل فريـق حمايـة المعلومات. يجب أن يكون الفريق مسؤولا عن المراجعة والرصد،وتعزيـز سياسـات ومعايير لتنظيم فيما يخص أمن المعلومات.

وينبغـي أن يتضـمن ميثـاق الفريـق بمراجعـة الآثارالأمنيـة المترتبـة علـى أي نظـام رئيسي جديـد قبـل تنفيـذه. يجـب تقنينهـا لفريـق حمايـة المعلومـات وسـلطتها ف ي السياسات والإجراءات للمنظمة.

تخطيط إدارة الأزمات:

ينبغي أن يشمل التخطيط والإجراءات المنظمة كل نوع من التخطيط لإدارة الأزمة. فإن معظم المنظمات تحتاج اثنين على الأقل من المقاطع لإدارة الأزمات:

مقطع واحد يجب أن يتعامل مـع التخطيـط للوقايـة مـن الكـوارث، والمقطـع الآخـر ينبغي أن يشمل تخطيط أمن الكمـبيوتر للاسـتجابة للحـوادث. وينـاقش الفصـل 16 إدارة الأزمات بمزيد من التفصيل.

الفصل 15
المراجعة والرصد وكشف التسلل

نظرة عامة:

بديهيا أقول إنه في هذا اليوم وهذا العصر وفي الزمن القادم مستقبلاً، ستعتمد المنظمات بشكل كبير على أجهزة الكمبيوتر والشبكات للحفاظ على بقائها. ونتيجة لذلك، نجد دقة تلك الأنظمة والأشخاص الذين يستخدمونها يعملون على المحافظة عليها للحفاظ على بقاء المنظمة. وعلاوة على ذلك، لأن الناس يخطئون ولأن بعض الناس يمكن أن يكونوا غير شريفين أو أنفسهم خبيثة، تحتاج المنظمات لمراجعة منتظمة ومراقبة أجهزة الكمبيوتر الخاصة بهم والشبكات.مع إدخال أجهزة الكمبيوتر والشبكات، قد اتسع مفهوم التدقيق ولها معان متعددة. تاريخيا، كان التدقيق يؤثر من تقليل الاعتماد على الضوابط الإدارية والإجرائية. وبعبارة أخرى لم تكن مبنية الضوابط في المعالجة ولكن كانت مبنية على التحقق التي جرت بعد ذلك. هذا لا يعني أن التدقيق يبطل الحاجة إلى الإجراءات والضوابط، ولكن سيكون فقط قبض أي انحرافات من تلك الإجراءات والضوابط بعد وقوعها. اعتبرت المخاطر المتبقية مقبولة للعملية المنظمة، بحيث كان من الضروري ايجاد التدقيق فقط بشكل دوري.هذا التوجه نحو المخاطر المتبقية ربما كان مقبولا في الماضي، ولكن هذا أمر خطير جدا في بيئة اليوم. ونتيجة لذلك، في بعض السياقات "المراجعة" أصبح مرادفا لل "المراقبة".يشمل هذا الفصل ثلاثة جوانب منفصلة من التدقيق التي معظم (EDP) "التدقيق". الأول هو البيانات الإلكترونية التقليدية تجهيز أقسام تكنولوجيا المعلومات تخضع لها والذي عادة ما يكون بمساعدة شركة يمكن التدقيق بمراجعة قضايا مثل EDP خارجية أو من قبل دائرة التدقيق الداخلي ضوابط لتطوير التطبيقات، ويسجل الاحتفاظ بها، متطلبات حقوق التأليف والنشر، والمسائل التشغيلية العامة، ولكن يركز هذا الفصل على أمن عمليات مراجعة الحسابات. الجانب الثاني من التدقيق تناولها هذا الفصل هو التدقيق وأدوات النظام التي تتوفر للتحقق بشكل دوري على السلامة إما بالنظام الفردي أو بنظام الشبكة العامة. والثالث هو كشف التسلل، وهي عملية التدقيق المستمر أو رصد أمن وسلامة أنظمة المؤسسة والشبكات.

ما هو التدقيق؟

تقليديا، التدقيق هي مراجعة مستقلة لموضوع معين. والغرض منه هو أن يقدم تقريرا عن المطابقة للمعايير المطلوبة. واحدة من المهام التي تخدم عملية تدقيق هو التحقق والامتثال لسياسات الشركة والتأكد من أن الإجراءات EDP والممارسات الأمنية المطلوبة يجري اتباعها. وبالإضافة إلى ذلك، التدقيق تنطوي عادة بعملية رصد وأنظمة تحليل، والشبكات، والنشاط للمستخدم النهائي.

وبالإضافة إلى استعراض الامتثال للسياسات والإجراءات، والتدقيق هي المعنية مع بتقييم المخاطر ومرتبطة بالأنظمة والشبكات EDP تقييم المخاطر. يتضمن التدقيق

لتحديد ما إذا كانت الضـوابط الموجـودة كافيـة لحمايـة أصـول المؤسسـة. وتشـمل المناطق التي يتم تدقيق الأمن وسيتم اعادة النظر في ما يلي:

• التأكد من أن أدلة المكتب والإجراءات المحدثة.

• ضمان الفصل السليم للواجبات مع المشاركات المناسبة من العمل؛

• التأكد من أن الضوابط المادية كافية في المكان.

• التأكد من أن ضوابط مصادقة المستخدم كافية؛

• التأكد من أن التدقيق يتم على مسارات المحافظة.

• التأكد من أن خطط التعافي من الكوارث هي في مكان استئناف واختبار الأعمال بانتظام.

• ضمان الضوابط المناسبة لتطوير التطبيقات وتنفيذها؛

• ضمان أن تتم مراقبة سلامة البيانات والحفاظ عليها.

• ضمان أن يتم اتباع السياسات والإجراءات العامة.

يتضمن التدقيق يمكن أن يكون هنالك فرصة للتحقق مـن صـحة السياسـات الأمنيـة للمنظمة ويمكن أن توفر تكنلوجيا المعلومات تقنية المعلومات مع وجود فرصـة أن يكون هناك طرف خارجي لاختبار الإجراءات الأمنية التي كانت تنفذ. ليـس مـن غيـر المألوف لتوظيف "فريق النمر" أو "قراصنة قبعة بيضاء،" لأنها تسمى أحيانا لاختبـار الاجراءات الامنية. هـؤلاء هـم خـبراء أمـن الشـبكات الـذين يـوفرون اختبـار النظـام ودفاعات الشبكة لمنع محاولة "الاختراق" فيهـا. وتتـم القرصـنة دون علـم وموافقـة من المؤسسة التي تملك شبكة أو الأنظمة التي يتم فيها محاولة الاختراق.إذا كـانت المنظمـة تتعامـل مـن خلال شـريك أو طـرف ثـالث، قـد تحتـاج وحـدة تكنلوجيـا المعلومات تقنية المعلومات لتدقيق الإجراءات الأمنية للطرف الشريك أو الطــرف الثالث. وهذا صحيح بشكل خاص.

لتوفير تمكيـن الإنـترنت أو وصـفت ASP وإذا استخدمت المنظمة بوابة، مملوك، أو خدمات الإنترنت للعملاء. وسيكون ذلك في غايـة الخطـورة للمنظمـة للـدخول فـي للعمليـة، بمـا فـي ذلـك ASP دون تثبيت أو كـل جـوانب الكمـبيوتر ASP اتفاق مع ويمكـن لشـركة تجـد نفسـها ASP، الجوانب الأمنية. عند استخدام مملوك أو خدمة ضحية غير مباشرة للهجوم مما يؤدي للحرمان مـن الخدمـة الموجهـة نحـو مشـترك آخر من الخدمة.كمـا ذكـر أعلاه، هنـاك العديـد مـن المجـالات تـم استعراضـها خلال عملية التـدقيق. ونتيجـة لـذلك، مـن الضـروري تصـنيف الوظـائف وتـدقيقها بشـكل منفصل للمنشآت الكبيرة. على سبيل المثال، وظائف يمكن تصنيفها تحت العنــاوين التالية:

• التدقيق التشغيلي؛

• تدقيق النظام.

• تدقيق الاستخدام.

التدقيقات الأمنية التشغيلية تسعى إلى ضمان الضوابط المناسبة لتحديد الانحرافات عن المعايير والسياسات المعمول بها. تم تصميم هـذا النـوع مـن التـدقيق لتخفيـف نقاط الضعف التي أدخلتها سوء الإدارة.

هناك عدة أهداف لتدقيق أمن النظام. الأول هو للتحقق من صحة النظام.التدقيقات الأمنية للنظام تسـعى أيضـا لتحليـل تكـوين النظـام ولتخفيـف نقـاط الضـعف الـتي أدخلت ونفذت خطأ للنظام، والشبكة، أو التطبيق.

أنواع التطبيقات بمراجعة النظام ، من بين أمور أخرى:

• حسابات دون كلمات السر: وهو يحدث في كثير من الأحيان.

• الالتزام وإنفاذ سياسات كلمة المرور: كم هو سهل للقضاء على كلمات السر؟

• الحسابات المشتركة: هل هناك حسابات لأكثر من شخص واحد لديه نفس كلمـة السر؟

• الحسابات الساكنة: وغالبا ما تستخدم هذه الحسـابات مـن قبـل قراصـنة ويجـب حذفها.

• الملفات بدون مالك: هذه الملفات مفتوحة ، لأن أي شخص يمكن أن يستخدمها.

• الملفات مع حقوق الوصول الغير محـدودة: هـذه الملفـات مفتوحـة أيضـا لسـوء الاستخدام. فمن المهم أن ملفات النظام الهامة لديها حقوق الوصول المحدودة.

• الفصل بين الواجبات: هل هناك عملية من الضوابط والتوازنات في مكـان سـليم للاستعراض، لواحد أو اثنين من الأفراد يكون لديهم جميع الضوابط؟

حتى نظام الآمن الذي تم تكوينه بشكل صحيح هو عرضـة للهجـوم، ويـوفر التـدقيق وسيلة ممتازة لتحديد ما إذا كان وكيف لمثل هذه الهجمات قـد تحـدث.هنـاك سـبب آخر لإجراء مراجعة أمن النظام لمراقبة محاولـة الهجمـات، والحـوادث الغيـر عاديـة الأخرى. يمكن مراجعة نظام المساعدة أيضـا فـي تحديـد خطـوط الأسـاس للنظـام المستخدم، والتي تستخدم لتحديد النشاط الغير طبيعي.مراقبة النظام يعتمد بشكل كبير على سجلات التدقيق للنظام أو سجلات الأحداث. ملفات سـجل النظـام العـام تقوم بتسجيل أحداث معينة بما في ذلك ما يلي:

• محدودة أو محاولة تسجيل الدخول.

• تسجيل الخروج Logouts.

• الوصول إلى النظام عن بعد.

• فتح الملف، اغلاقه، إعادة التسمية، والحذف.

• التغييرات في الخصائص أو سمات الأمن.

• التغييرات في مستويات التحكم في الوصول.

عادة لا يتم الاحتفاظ بهذه الملفات على محركات الأقراص المحلية للملقم أو النظام لأنه بهذه الطريقة سيكون عرضة للتغيير. ومن الاسلم به عموما نقل ملفات السجل لملقم آخر على أساس يومي أو ببساطة بطباعة إدخالات سجل ذات الصلة لضمان السجل الورقي الذي لا يمكن تغييره.هناك العديد من أدوات البرمجيات المتاحة للمساعدة في عملية مراجعة النظام. اثنين منها برامج مجانية الاشهر والتي تمت مناقشتها في الفصل 7. وهناك أيضا عدد ، COPS مفتوحة المصدر هي ،(ISS) من المنتجات التجارية المتاحة من البائعين مثل نظم أمن الإنترنت والشبكات الآمنة، وسيسكو، و الاجهزة الكشفية، فقط على سبيل المثال لا الحصر.مفتاح التطبيق واستخدام التدقيق بإنشاء مقاييس أساسية للمساعدة في تحديد المشاكل الأمنية المحتملة. تدقيق تطبيق النظام يسعى إلى تحليل الانحرافات عن الأنماط العادية للاستخدام وغيرها من الأنشطة غير العادية. وينبغي أن تكون المقاييس الأساسية أنشئت للمساعدة في تحديد المشاكل الأمنية المحتملة. والغرض من ذلك هو تحديد الاستخدام غير الطبيعي وتحديد هجمات محتملة قادمه. عند تجاوز هذه المقاييس يجب تحريك أجهزة الإنذار في النظام لتسبب إجراءات تبدأ من قبل استعراض أي تقارير أو سجلات. على سبيل المثال، مقياس خط الأساس قد تكشف على وجه الخصوص موظف يصل إلى البيانات 20 مرة أكثر من أي موظف آخر ؟ لماذا؟ ما الذي يسبب لتحيد عن نمط السلوك العادي؟

مقاييس أساسية أيضا عنصرا أساسيا من أنواع معينة من فاعلية النظام، والتي سيتم مناقشتها أكثر بالتفصيل لاحقا في هذا الفصل. ومع ذلك، هذا النوع من فعالية. ويهدف التدقيق من هذا النوع نحو IDS التدقيق لا يحتاج إلى أن يكون مستوى التطبيق، ومعظم فاعلية النظام عموما موجهة نحو مستوى نظام التشغيل. وهي عادة ما تكون ليس من الصعب أن تولد استفسارات بسيطة لتحديد الحالات الشاذة في النشاط لفترة معينة. أحيانا كل ما يتطلبه الأمر هو مراجعة يوميه للتقارير القياسية. تحديد الحالات الشاذة للنشاط العام للنظام على أساس يومي من السهل نسبيا. ومن أكثر صعوبة لتحديد السلوك الشاذ للمعين المشغل على مدى فترة ممتدة. الموظف الذي يصل إلى الملفات 20 مرة سيكون أكثر من أي موظف آخر يكون من السهل على الفور اكتشافه، ولكن تحديد السلوك الشاذ لموظف معين على مدى فترة من الزمن هو أكثر صعوبة لأنه يتطلب مقارنات للبيانات القديمة. على سبيل المثال، حساب المستخدم الذي يسجل في ساعة غير عادية لفترة معينة قد تستدعي التحقيق. ومع ذلك، فإن المرء لا يعرف ما اذا

الساعة التي وقع فيها تسجيل الدخول الغير عـادي إلا إذا كـان هنـاك بيانـات قديمـة أشـارت إلـى أن سـلوك تسـجيل الـدخول غيـر طـبيعي.قـد بنيـت فـي العديـد مـن التطبيقات قدرات تسجيل التي يمكن استخدامها للاستعراضات روتينية.

وبصفة عامة، فإنه من المستحسن تسجيل المعاملات، والمراجعـة الـتي تتطلـب أي نوع من تجاوز المعلمات للنظام. على سبيل المثال، فـي الصـناعة الماليـة أنـه مـن الطبيعي الضوابط توضع في مكان لكل موظـف أن يحـدد الحـد العلـوي للمعـاملات المالية. هذه الضوابط أو معايير النظام قد يتطلب تجاوز المشرف إذا كـان الصـفقة على المبلغ المحدد. معظم أنظمة من هذا النوع تولد تقرير تجاوز المشرف اليـومي بمراجعة من قبل طرف ثالث لضمان شرعية المعاملات وأن تكون بمثابـة احـترازي ضد التواطؤ.هذه الأنواع من التقارير وعادة ما تكون واحدة من أول الأشياء التي تـم فحصها المدققين الخارجيين.المدققين الخارجيين فحصـوها للتأكـد مـن أن التقـارير هي في الواقع استعرض بشكل يومي أساسي لعينة من المعاملات للتأكـد مـن أنهـا مشروعة.قد يعيد المدققين النظر أيضا عما إذا كانت آلية التنفيذ المعلنة كافية لهذه الوظيفة.

وظيفة التدقيق هي في كثير من الأحيـان سـمة معياريـة مـن العديـد مـن تطبيقـات النظام وتتبع لتغيير البيانات. و القدرة على تحديد المشغل السابق لإجراء تغيير على عناصر البيانات. وتشـمل الحـد الأدنـى مـن الخصـائص الـتي يجـب أن يتـم تسـجيل التالي:

- تحديد مشغل إجراء التغيير.
- نوع التغيير؛
- ملف عنصر البيانات ؛
- تاريخ ووقت التغيير،
- ما إذا كان التغيير كانت ناجحة.
- ما هي عناصر قبل وبعد التغيير.

هذه القدرة يمكن أن تكون حاسمه بشكل خاص عند التحقيق للنشاط الاحتيالي التي تنطوي المطلعين، مثل الموظفين.

أخطاء التدقيق:

من الناحية المثالية، ينبغي أن ينظر إلى التدقيق كفرصة لتحسـين العمليـات. لسـوء الحظ، الحقيقة هي في بعض الأحيان بكون واحد من أوجه الاتهام وتبادل الاتهامات. وبناء على تجربة شخصية، يتم وصف بعض الأخطاء الأكـثر شـيوعا الـتي تسـهم فـي صعبة كما في التالي EDP مراجعة:

اذا لم يؤخذ في اعتبار تكنولوجيا المعلومات في جدولة أو تخطيط عملية فلن يتم الضمان.

مثل جدولة واحدة خلال فترة تتولى شعبة تكنولوجيا EDP صعوبة التدقيق المعلومات امتدت إلى حد العمل على المشاريع. وهذا يؤدي إلى الشعور بأن تكنولوجيا المعلومات مفروضة عليهم والاستياء من التدخل في شؤونها المفاجئة.تقسيم الموارد لتكنولوجيا المعلومات بالفعل قد تمتد إلى نقطة الانهيار عندما تبدأ في الحصول على طلبات لتوفير جميع أنواع المعلومات والتقارير للمراجعين.

من ناحية أخرى، فإن المراجعين يشعرون بعدم التعاون، ذلك لعدم الاستجابة في الوقت المناسب لطلبات الحصول على المعلومات. وهذا يجعل العلاقات متوترة ويضمن تقريبا أن كل عملية تنبغي أن تكون واحدة من الاتصالات المفتوحة المؤلمة والصعبة.

• لقد شاركت EDP: مراجعي الحسابات غير مدربين بشكل صحيح لإجراء تدقيق في EDP

التدقيق حيث لم يكن لدى المراجعين الخلفية التقنية اللازمة لأداء كافة المراجعة. في هذه الحالات كانت مختلطة النتائج. في بعض الحالات، ببساطة المدققين يتقبلون كل شيء من قبل مجموعة تكنولوجيا المعلومات لتكون واقعية ودقيقة. لم يكن هناك عملية التحقق المستقل. في حين أن هذا قد جعل العملية أسهل على مجموعة تكنولوجيا المعلومات، فإنه ليس هناك مراجعة حقيقية لا تخدم احتياجات المنظمة ككل. وفي حالات أخرى رأينا عدم وجود التقنية المعرفة من جانب المراجعين وغير آمنة حول المعلومات التي تقدم فيها. وبما أن المراجعين لهم الحق بشكل مستقل التحقق بأي وسيلة للمعلومات ، وأنهم يشكون في كل شيء.

• ترك الأمر لتكنولوجيا المعلومات لفرض تغييرات من جانب واحد داخل المنظمة: ليس من غير العادي ومن أوجه القصور أن يكون لوحدة تكنولوجيا المعلومات ليس لها السيطرة في إجراءات الكشف عن الهوية، على سبيل المثال، يمكن أن تدار مستويات الوصول داخل التطبيقات من قبل تكنولوجيا المعلومات تقنية المعلومات، ولكن أولئك الذين يحددون المستوى الفعلي للوصول قد تكون موجودة داخل وحدة الأعمال التجارية. وكمثال على ذلك، فإن السلطة النهائية على النحو هو مدير الموارد HRMS الذي لديه حق الوصول إلى إدارة الموارد البشرية البشرية. وتدعم مجموعة تقنية المعلومات حزمة نظام إدارة الموارد البشرية، ولكن من الموارد البشرية هنالك من يملك ذلك، وأنهم هم الذين يحددون الذين سيكون لهم حق الوصول إلى أية معلومات. في أكثر من مناسبة واحدة، لقد رأينا نتائج التدقيق في التقرير النهائي بشأن القضايا التي كان على تكنولوجيا المعلومات أي سيطرة أو القول في هذه العملية. ومع ذلك، كان لا تزال البنود المذكورة كما

في أوجه القصور في عملية المراجعة. يتم ترك مجموعة تكنولوجيا المعلومات لتصحيح النقص، على الرغم من اعتراضات مجموعة من رجال الاعمال الأخرى.

• فشل مراجعي الحسابات في بعض الأحيان أدى إلى الاعتراف واحدة من القواعد الأساسية لأمن الشبكات، وهو أن الإجراءات الأمنية والإجراءات التي تتداخل مع عملية منظمة ذات قيمة تذكر. هذه الأنواع من التدابير وعادة ما يتم تجاهلها أو الالتفاف من قبل موظفي الشركة، لذلك فإنهم يميلون إلى خلق الثغرات الأمنية بدلا من سدها. وكلما كان ذلك ممكنا، يجب أن تكمل الإجراءات الأمنية للاحتياجات التشغيلية والتجارية للمنظمة. بعض المراجعين لديهم ميل الايقاع أي انحراف عن الممارسات القياسية الموصي بها، حتى لو كان الانحراف عمليا يجعل الشعور للمنظمة. الأمن هو موازنة عملية تحقيق التوازن بين الاحتياجات الأمنية مع احتياجات العمل وممكن من المحتمل. في كثير من الأحيان المدققين يركزون على ما هو ممكن وليس احتمالا.

• تقرير المراجعة يقوم بالإجحاف على تكنولوجيا المعلومات: ليس من غير المألوف لتقرير المراجعة النهائية لتكون قاسية دون داع على وحدة تكنولوجيا المعلومات. هذا غالبا ما يكون نتيجة لأخطاء مدرجة أعلاه. سوء الفهم، وانعدام التواصل، وعدم الثقة العامة غالبا ما تؤدي إلى النتائج القاسية. وهذا أمر مؤسف جدا، لأن التدقيق الأمني هو في الواقع فرصة لاختبار، وتعلم، وتحسين الوضع الأمني للمؤسسة. على هذا النحو، ينبغي أن يكون رحب، ولكن في كثير من الأحيان اجتمع مع الرهبة.

وحدة تكنولوجيا المعلومات ومجموعة التدقيق في حاجة إلى العمل معا في إعداد التقرير النهائي، بحيث يكون شاملا وعمليا. فإنه يحتاج إلى أن يكون شاملا في أن يتم التغاضي عن أي منطقة من جديد. فإنه يجب أن يكون عملي في أن لا توجد في توصيات المراجعة انقباض أو تتداخل مع تشغيل المنظمة.

• عدم وجود دعم الإدارة لتنفيذ توصيات المراجعة : أضمن طريقة للتأكد من أن عملية المراجعة هي مراجعة الفشل في الإدارة لدعم تنفيذ توصيات المراجعة. دعم الإدارة أمر بالغ الأهمية عندما يتم تنفيذ التغييرات في السياسة، وخاصة عندما تجتمع هذه التغييرات مع المقاومة.في بعض الحالات قد يكون مجرد مسألة إدارة لا تخصيص الموارد اللازمة لتنفيذ التوصيات. معظم المنظمات لديها مشاريع مع المواعيد والالتزامات التي كانت موجودة قبل عملية المراجعة. تنفيذ تدقيق التوصيات هي دائما شيء تعطى أولوية منخفضة. في نهاية المطاف، لتنفذ أبدا بالتوصيات، وعادة ما تشار نفس النتائج في المراجعة المقبلة.

أوجه القصور في تقنيات المراجعة التقليدية:

والحقيقة المؤسفة هي أنه ليس من الممكن بناء نظام أو شبكة آمنة تماما. يتم تجاهل الإجراءات في بعض الأحيان. كلمات السر هي الضعيفة تؤدي الى تفشل

التقنيات أو تخريبها. حتى في بيئة كل شيء يعمل فيها وفقا للخطة، والأنظمة لا تزال عرضة لسوء المعاملة من قبل المطلعين المتميزين، مثل مسؤولي النظام.

الهدف النهائي للخطة أمن الشبكة هو منع الهجمات الناجحة على الشبكة.

تقليديا، كانت الأداة الرئيسية لضمان أمن الشبكة هو جدار الحماية. ومع ذلك، الجدران النارية هي عديمة الفائدة تقريبا لرصد النشاط على شبكة الاتصال الداخلية. المنظمات بدأت تدرك الحاجة لمراجعة أو مراقبة الشبكات الداخلية وذلك ببساطة لأن أغلبية جميع الهجمات والخسائر تشمل المطلعين.في اغلب التدقيقات الأمنية التقليدية قد تحدد ضعف في الإجراءات الأمنية أو حتى تعريض الخروقات الأمنية، فإنه عادة ما يكون بعد وقوعها. أدوات التدقيق مثل COPS ، لن يؤدي إلى تحديد نقاط الضعف في التكوين أو تنفيذ النظم أو الشبكات.

لا توجد واحدة من هذه الطرق تحدد بأنها تحدث المشاكل؛ بدلا من ذلك، فهي المعنية بالمخاطر المتبقية.

تقليديا، اعتبرت المخاطر المتبقية مقبولة لتشغيل المنظمة، بحيث كان المطلوب فقط التدقيق بشكل دوري يومياً للإنترنت الموصول بالبيئة هذا نموذج من المخاطر المتبقية ولم تعد صالحه. ونتيجة لذلك، أكثر النشاطات المطلوبة لطرق المراجعة أو مراقبة الشبكات والنظم. اليوم هناك أدوات جديدة متاحة التي توفر للمسؤولين القدرة على رصد أمن الشبكات ونظام على الخط في الوقت الحقيقي.

كشف التسلل:

مسؤولي النظام المختصين دائما يقومون بمراقبة الانظمه لعدم الاقتحام. تتم العملية عادة على أساس يومي بمراجعة ترتب السجلات. وكانت التدخلات نادرة بما فيها الكفاية كما أن بعد حقيقة الاستعراضات عادة كانت كافية لمعالجة أي مشاكل محتملة. للأسف الزمن قد تغير بشكل جذري. بعد حقيقة الاستعراضات لم تعد كافية. في الوقت الحقيقي أو الردود في الوقت الحقيقي بالقرب من التدخلات ضرورية. وبالإضافة إلى ذلك، فإن حجم النشاط على شبكات اليوم أقصر ما كان العرف السائد منذ 10-15 سنة. ونتيجة لذلك، فإنه ليس من الممكن منطقياً إعادة النظر في كمية المعلومات في ملفات السجل اليومية بدون بعض العمليات الآلية.

دون اتمام عملية المراجعة والرصد، يمكن أن تمر أسابيع دون أن يعرف مسؤول النظام عن وجود تسرب للنظام.بصورة عامة ب "التسلل" يمكن تعريفها بأنها محاولة غير مصرح بها أو تحقيق لوصول، يغير، أو تدمير المعلومات على النظام أو النظام نفسه.في الأساس، تدخل غير الشخص المسئول لمحاولة اقتحام أو إساءة استخدام هذا النظام. بعض المراقبين يفرقون بين سوء الاستخدام والتسلل. وعادة ما يستخدم اقتحام المدى في إشارة إلى الهجمات التي تأتي من خارج المنظمة. وعادة ما يستخدم لوصف سوء استخدام الهجوم الذي ينشأ من شبكة الاتصال الداخلية. ومع ذلك، ليس كل من يجعل هذا التمايز, كشف التسلل هو فن اكتشاف

نشاط غير مصرح به، غير مناسب، أو الشاذ.قد مورست فن كشف التسلل من قبل النظام وشبكة الإداريين لسنوات. ومع ذلك، فقد تلقت كشف التسلل في الآونة الأخيرة مزيدا من الاهتمام في وسائل الإعلام إلى حد كبير يرجع ذلك إلى حقيقة أن الكثير من الشركات تسوق الآن فاعلية النظام. ويفترض ان فاعلية النظام الجديد هذه يمكنها تحديد الهجمات التي في التقدم، وتوليد تنبيهات في الوقت الحقيقي، وحتى إطلاق المضادة أو إعادة تكوين أجهزة التوجيه أو جدران الحماية لمواجهة الهجوم.

أنظمة كشف التسلل (فاعلية النظام):

فاعلية النظام يتصرف مثل الكثير من حراس الأمن أو الحراس. أنها تفحص باستمرار حركة مرور الشبكة أو المضيف لسجلات التدقيق. في حين أن الدفعة الحالية من المنتجات IDS توفر أدوات مفيدة لزيادة أمن الشبكات المنظمة، فمن الضروري لتجاوز هذه الضجة التسويق لتقييم فعالية النظام. في الوقت الحاضر، لا يوفر نظام واحد حقا نهاية إلى نهاية فعالة للقدرة على كشف التسلل. وبالإضافة إلى ذلك، فان فاعلية النظام ليست مفهوما جديدا. في الفصل 7، ونحن ناقشنا التي كانت موجودة منذ UNIX مجانية المستندة إلى IDS وهو، TCP Wrapper سنوات عديدة.عموما، يسقط فاعلية النظام في واحدة من فئتين:

- فاعلية النظام القائم على الشبكة؛
- فاعلية النظام القائم على المضيف.

في حين أن هناك مزايا لكلا النهجين إلا ان الطريقة في حد ذاتها تكفي لرصد جميع التهديدات. ونتيجة لذلك، فإن الاتجاه الحالي في الصناعة هو الجمع بين النهجين.

أنظمة كشف التسلل القائم على المضيف:

المنتجات المستندة إلى المضيف والموجودة على المضيف هي قادرة على الرصد التلقائي والخدمات نافيا إذا تم الكشف عن نشاط مشبوه. إنها ترصد نشاط على الفرد.

استضافة المعارضين لمراقبة النشاط على الشبكة. استضافة المستندة إلى فاعلية النظام لا تزال تعتمد على نظام سجلات التدقيق، الى حد كبير مع نفس مسؤولي النظام مع طريقة القيام بها، ولكن فاعلية النظام لإتمام عملية عادة ما يكون نظام القائم على المضيف، الحدث، وسجلات الأمان على نظام التشغيل IDS مراقبي القائم على المضيف ويستخدم ملفات IDSو .UNIXو ملف ال Windows NT سجل النظام والتدقيق للنظام الخاص لوكلاء مراقبة النظام.هناك زوجين من نهج البرمجيات يمكن توظيفها لكشف التسلل القائم على المضيف:

هذا النهج يلتف حوله مختلف .TCP Wrapper واحد منها لتوظيف المجمع، مثل الشبكات المضيفة والخدمات في طبقة إضافية تفسر طلبات حزمة شبكة الاتصال

إلى مختلف الخدمات. أما النهج الآخر يعمل لوكلاء العمليات المنفصلة كما في رصد طلبات الاستضافة. كلا النهجين فعالة في الكشف عن النشاط الشاذ أو إساءة استخدام أنظمة المضيف.توكيل ميزة واحدة إلى المضيف هو أنها يمكن رصد التغيرات في ملفات النظام الهامة والتغيرات في امتيازات المستخدم. الرئيسية يقوم بمقارنة خصائص الملفات مع توقيعات الهجوم IDSالملف التغييرات النظام، و المعروفة لمعرفة ما إذا كان هناك تطابق. وواحدة من الطرق الشعبية للكشف عن الاختراقات ينطوي على التحقق من ملفات النظام الرئيسية والتنفيذية عبر اختبارية في فترات منتظمة لتغييرات غير متوقعة. على سبيل المثال، الفصل 7 يناقش الذي يوفر أيضا ،IDS لرصد التغيرات في ملفات النظام والشرارة MD5 باستخدام هذه الوظيفة.

المرة الأولى التي يتم تشغيل أحد هذه الأنظمة، فإنه يولد لقطة من سمات الملف، بما في ذلك أحجام الملفات وحقوق الوصول. يتم تخزين هذه المعلومات في قاعدة يقارن سمات الملفات الموجودة على القرص IDSابيانات. كل تشغيل لاحقة منها و للسمات المخزنة في قاعدة بياناته.إذا تغيرت السمات يبدأ الإنذار.بعض رصد فاعلية القائم على المضيف وإخطار مسؤولي النظام عندما يتم TCP النظام النشطة منفذ الوصول إلى منافذ معينة أو فحصها. ويمكن أيضا رصد وتسجيل المنافذ عند الوصول إليها. هذا يمكن أن يكون مفيدا إذا كان المنفذ لديه مودم متصل به.

TCP Wrapper فاعلية النظام ربما العائق الاكبر للقيام على المضيف، مثل والشرارة، هو أن عملية كشف التسلل ليست في الوقت الحقيقي. برامج كشف التسلل القائم على المضيف، بغض النظر عما إذا كان استخدام بعض الإزار أو الوكيل، وتحديد عموما محاولات الاقتحام بعد أن تكون قد حاولت أو نجحت. الفارق بين التسلل واكتشافه يمكن أن يكون كبيرا. بحلول ذلك الوقت يمكن أن يكون متأخرا جدا. وهذا هو الضعف مع فاعلية النظام القائم على المضيف. آخر ضعف والشرارة، هو ان TCP Wrapper عام مع فاعلية النظام القائم على المضيف، مثل لم يكن لديهم أي قدرة على التفاعل بشكل استباقي إلى التسلل. كما أنها لا تسمح لمسؤول النظام لتكون سباقة.عيب آخر للنهج القائم على المضيف هو أن لتأمين على كل كمبيوتر. ومع ذلك، هذا IDS الشبكة بالكامل، فمن الضروري تحميل الجانب من فاعلية النظام القائم على المضيف يمكن تكون ذات فائدة. إذا كنت ترغب فقط لمراقبة نظام واحد، فإن تكلفة المضيف المستندة إلى فاعلية النظام هو أقل في كثير من الأحيان من تلك التي لنظرائهم القائم على شبكتهم. كما ناقشنا ذلك بالفعل، هناك إصدارات مجانية من فاعلية النظام القائم على المضيف فان فاعلية النظام host based، المتاحة على شبكة الإنترنت. وبالإضافة إلى ذلك عادة لا تحتاج إلى أجهزة إضافية، لأنها تعمل على النظام نفسه.فاعلية النظام القائم على الشبكة في كثير من الأحيان تحتاج إلى نظام مخصص أو جهاز ليعمل. القائم على المضيف هو أنه يراقب IDSهذا أيضا يزيد من التكلفة.ميزة أخرى ل أنظمة محددة، ويمكن تحديد الهجمات على غير الشبكة. يمكن لفاعلية النظام

القائمة على المضيف مراقبة سلامة نظام الملفات، ملف الأذونات، والمعلمات القائم على الشبكة التي لا ترصد. بالإضافة إلى ذلك، IDSونظام الملفات الأخرى ل يمكن فاعلية النظام القائم على المضيف مراقبة الاتصالات الطرفية التي تجاوز الشبكة، ويمكن أيضا رصد أنشطة محددة من شخص يريد التسجيل في ملفات القائم على المضيف مراقبة IDSالمضيف والوصول. بالإضافة إلى ذلك، يمكن لل القائم على الشبكة IDSأنشطة التطبيقات والعمليات التي تعمل على المضيف. و يمكن مراقبة الشبكة فقط، وليس ما يحدث على مضيف معين.

القائمة على شبكة أنظمة كشف التسلل:

تمكنت الشبكة التي تديرها على أنماط شبكة والنشاط IDS المنتجات التي مصدرها القائم على شبكة عادة ما توظف IDSارصد وتحليل والإبلاغ عن أي نشاط مشبوه. و شبكة مخصصة الخادم أو الجهاز مع محول شبكة تكوينه لوضع مختلط لرصد IDSوتحليل كل حركة المرور في الوقت الحقيقي أثناء انتقالها عبر الشبكة. و القائم على الشبكة تراقب الحزم على السلك للشبكة ومحاولات لتبين حركة المرور الشرعي من الخبيثة. بعض البائعين ينص على أن الخادم المخصص ليس القائم على شبكتهم. ومع ذلك، في واقع الأمر لن يكون من IDS ضروري لعمل على IDS للأغراض العامة لخادم التطبيق. هل تريد IDS المستحسن لتشغيل الخادم الشبكة الخاصة بك لتعمل الرواتب للشركة؟

بالمقارنة مع استضافة المستندة إلى فاعلية النظام، فان فاعلية النظام القائم على شبكة لها مزايا وعيوب.

القائم على شبكة أقل تكلفة لتنفيذها. يرجع ذلك إلى IDS وتبعا للنظام، قد يكون القائم على شبكة تعمل مستقلة عن النظام وليس مطلوب ليتم IDS حقيقة أن تحميلها على جميع المضيفين على الشبكة لتكون فعالة.

وبالإضافة إلى ذلك، فاعلية النظام القائم على المضيف، يغيب العديد من الهجمات على الشبكة. فاعلية النظام القائم على الاستضافة لا عل ى فح ص رؤوس الحزم، لذلك لا يمكن الكشف عن الحرمان من الخدمة والهجمات.القائم على شبكة فاعلية IDS النظام هي أيضا أكثر التخفي بكثير من فاعلية النظام القائم على المضيف. مع القائم على المضيف، إذا كان النظام خطر القرصنة يمكن أن نرى بسهولة إذا هناك أساس شبكة على IDS الحاضر. وسيكون من الصعب جدا تحديد ما إذا كان IDS شبكة ببساطة عن طريق فحص الأسلاك. الشيء الوحيد للقرصنة يمكن تحديد هو القائم على IDSأن هناك جهاز على الشبكة التي تعمل في وضع مختلط. ويمكن ل الشبكة أيضا توفر الضوابط متفوقة على سجلات الأحداث.

مع العديد من فاعلية النظام القائم على المضيف، وسجلات التدقيق الموجودة على النظام محليا. ونتيجة لذلك، إذا تم اختراق النظام، يمكن للهاكر التلاعب في ملفات السجل لإخفائها له أو للمسارات.نقطة ضعف أخرى من فاعلية النظام القائم

الشبكة هو حقيقة أنها تصبح أقل فعالية كما ان زيادة حركة مرور الشبكة. أنها تعمل بشكل جيد جدا على شبكة فارغة، ولكن حيث أن عدد زيادة الحزم، يقلل من فعاليتها لدرجة أنهم لا يستطيعون تحديد الاقتحام. هذا هو نقطة الضعف الرئيسية النظر في حجم المعاملات عالية اليوم ونمو إيثرنت بسرعة وتحولت إيثرنت.

أنظمة كشف التسلل القائم على المعرفة:

هناك نهجين عامة مستخدمة لتحديد التدخلات المعادية. واحد منها هو المعرفة القائمة ، والآخر هو أساس إحصائي. النهجين مختلفة جدا وتوظف التقنيات المختلفة.نشر أكثر من فاعلية للنظام يعتمد على المعرفة. فاعلية النظام القائم على المعرفة يشار إليها أحيانا باسم أنظمة الكشف عن سوء الاستخدام، النظم فاعلية النظام.فاعلية النظام القائم signature based أو model- الخبيرة، أو القائم-A .على المعرفة تعتمد على القدرة على التعرف على الهجمات المعروفة IDSتعترف سيناريوهات التدخل المعروفة وأنماط الهجوم، و IDS على المعرفة القائم على المعرفة يعتمد على قاعدة بيانات من هجوم "التوقيعات" أو "أنماط" قائم على المعرفة IDS ،التي يمكن تغييرها لمختلف الأنظمة. على سبيل المثال لديها قاعدة IDSالقائم على المضيف مراقبة ضربات المفاتيح لهجوم الأنماط. و بيانات أنماط المفاتيح المعروفة التي هي معروفة لتكون تهديدا.فاعلية النظام القائم على المعرفة توظف العديد من التقنيات المختلفة لتحديد أنماط الاقتحام أو القائم على المعرفة القائم على المضيف عملية تنطوي المراقبة IDSالتوقيعات. ل على ضربات المفاتيح، ومراجعة الملفات لإجراء تغييرات ومراقبة المنافذ. استعراض الملفات يمكن أن تعمل بنفس الطريقة كما الفيروسات على جهاز الكمبيوتر.عمليات البحث هو مسح لأنماط معروفة أو للتغييرات التي تم إجراؤها على الملفات الهامة منذ آخر مسح ضوئي. توقيع سلسلة تبدو للنص السلاسل التي تشير إلى هجوم محتمل. مثال على سلسلة من شأنها رفع راية حمراء لان نظام يكون شخص يدرس محتويات الملف ملف كلمة السر أو المضيفين UNIX باستخدام "القط / بأسود" أو "القط / تستضيف". يجب أن تكون دائما مشبوه من شخص يريد لفحص ملف كلمة السر أو مراجعة ما المضيفين الآخرين على الشبكة. القائم على المعرفة القائم على المضيف IDS عند المراقبة للموانئ، يمكن لل مقارنة سجلات التدقيق للتوقيعات والتقنيات الشائعة. وكمثال على ذلك، فإن عددا فشل في الاشتهار وقد يكون الموانئ مؤشرا على أن TCP كبيرا من الاتصالات هو SYN-ACK شخص ما هو مسح الموانئ، أو عدد كبير من غير المعترف بها حزم هجوم الفيضانات SYN على الارجح مؤشرا على أن النظام هو تحت.

القائم على المعرفة القائم على شبكة الحزم على الشبكة. الحزم A، IDS ويدرس تعتبر المشتبه به إذا كان التطابق معروف التوقيع، سلسلة، أو نمط. وتستند الى القائم على المعرفة فحص مكدس البروتوكول المبطل IDS الشبكة، يمكن ICMP مع الحزم في .IP / TCP المشبوه أو مجزأة الحزم التي تنتهك بروتوكول

القائم على المعرفة IDS، A المتضخم سيكون مثالا للتوقيع المعروف. يمكن القائمة على الشبكة أيضا فحص رؤوس الحزم لمجموعات خطرة أو غير منطقية FINو SYN مع كل من TCP في رؤوس الحزم. آخر توقيع لرأس المعرفة هي حزمة لأعلام المجموعة، مما يدل على أن المنشئ يرغب في بدء وإيقاف اتصال في نفس الوقت. يمكن أن يكون هذا إشارة إلى أن النظام يناقش حاليا متسلل.النظم القائمة على المعرفة التي تستخدم نمط المطابقة ببساطة تترجم التدخلات المعروفة إلى الأنماط التي تتم بعد ذلك مقابل ضد نشاط النظام أو الشبكة. IDS يوافق هذا النشاط إلى أنماط تمثل سيناريوهات التسلل. تراقب IDS محاولات النشاط، وتراكم المزيد والمزيد من الأدلة لمحاولة الاقتحام حتى عبر العتبة. النهج الأساسي وراء نمط المطابقة هو أنه إذا كان يبدو وكأنه بطة، يمشي مثل بطة، والدجالون مثل البطة، ثم يجب أن تكون بطة. ومع ذلك، لنمط مطابقة العمل أن يكون أنماط التعرف عليها بسهولة، ويجب أن يكون مميزا. في الآخر، وأنهم لا يجب أن تبدو مثل أي نشاط طبيعي أو شرعي آخر.مزايا فاعلية النظام القائم على المعرفة هو أنها عادة ما تكون منخفضة مدى الإنذارات الخاطئة. ويرجع ذلك عادة إلى أن التوقيعات الحقيقة محددة للغاية، والسلاسل، والأنماط. هذا وبالإضافة إلى ذلك، مشاهدة أحداث معينة والقدرة على تقديم تقرير مع بعض التفاصيل واليقين على التهديد الذي تواجهه، مما يجعل من الاسهل تحديد مسار العمل المناسب.القصور الرئيسي لفاعلية النظام القائم على المعرفة هو أن النظام يكون فعال فقط ضد التهديدات التي هم بالفعل على دراية بها. ونتيجة لذلك، فهي غير مجدية ضد التقنيات الجديدة الموجودة لديهم لأي توقيع أو نمط في قاعدة المعرفة. وبالإضافة إلى ذلك، فإنه ليست مسألة بسيطة لإنشاء توقيع أو نمط للهجوم. ليس من السهل أن تترجم سيناريوهات هجوم معروف في الأنماط التي يمكن استخدامها ليصل إلى وقت IDS القائمة على المعرفة. فهو يتطلب الحفاظ على IDS من قبل مع نقاط الضعف والبيئات الجديدة. وعلاوة على ذلك، فإنه يتطلب تحليل يستغرق ونتيجة لذلك، لا يتم .IDS وقتا طويلا من كل ثغرة جديدة لتحديث قاعدة المعارف تحديث قواعد البيانات الخاصة بهم في كثير من الأحيان كما يجب.

آخر ضعف مشترك من فاعلية النظام القائم على المعرفة هو أنه غير فعال ضد الهجمات السلبية، مثل شبكة السحب والتنصت على المكالمات الهاتفية. بل هي DNS، أو التسلسل بالتحايل عدد الهجمات المستندة إلى IP أيضا فعالة ضد القائم على المعرفة لا IDS اختطاف الجلسة، والتحويلات. وبالإضافة إلى ذلك، فإن يكشف عن نشاط احتيالي أو سيئ من الداخل إذا كان النشاط متميز لا يتطابق مع نمط معروف أو التوقيع. هذا صحيح بصفة خاصة إذا يتم تنفيذ النشاط من خلال التطبيق. على سبيل المثال، نقل عن طريق الاحتيال أموال من حساب إلى آخر لن المنتجات IDS يتم وضع علامة، لأنه سيكون من ضمن المعايير العادية للنظام. بعض وسيسكو، وأنظمة الأمن وحماية AXENT، القائمة على الشبكة المعروفة من الإنترنت (ISS).

الإحصائية المستندة إلى أنظمة كشف التسلل:

استنادا الى الإحصائيات فان فاعلية النظام تحدد التدخلات من خلال تطوير قياسات خط الأساس للأنشطة "الطبيعية" وعلى افتراض أن كل ما ينحرف كثيرا عن القاعدة هو التسلل.بعبارة أخرى، يتم التعرف على الاقتحام من قبل تحديد الانحرافات عن السلوك العادي أو المتوقع للنظام أو المستخدمين. ويشار إلى أيضا أنماط السلوك القائمة أو IDS فاعلية النظام القائم على الإحصائيات باسم ببساطة مجرد شذوذ أنظمة الكشف. و أضافة هذه الفلسفة التي تقوم على مفهوم أن أي شيء جديد، مختلف، أو غير معروف يجب أن تمثل تهديدا لأمن النظام أو تطور النموذج لأنماط "طبيعية" (SIDS) المستندة على الإحصائية IDS.الشبكة النشاط والسلوك من خلال جمع المعلومات من مصادر مختلفة. والدول الجزرية الصغيرة النامية تتعلم ما هو طبيعي من خلال معرفة ما ان كانت الأنماط التاريخية. فهو يتطلب كميات كبيرة من المعلومات والبيانات لتطوير نموذج دقيق ومفيد. بأكثر دقة للنموذج. ويمكن تطوير IDS، لمزيد من المعلومات يمكن الحصول على هذه النماذج في النظام المستخدمة ومستوى التطبيق. ويمكن تطوير النموذج لأي نوع من النشاط الذي يحتاج إلى رصد. النماذج التي تقوم على المعلومات التاريخية، تستخدم للمقارنة والتحقق من صحة هذا النشاط المستمر للنظام أو المستخدم أو التطبيق. عندما يلاحظ الانحراف ذات دلالة إحصائية، يتم إنشاء التنبيه. وبعبارة أخرى، يعتبر أي شيء لا يتوافق مع نمط التعليمات السابقة أو السلوك مقابل النظام القائم على المعرفة هو أن SIDSتكون مشبوهة،والميزة الرئيسية ل الدول الجزرية الصغيرة النامية لا تعتمد على مجموعة محددة مسبقا من أنماط الهجوم المعروفة أو التوقيعات. ونتيجة لذلك، يمكن للدول الجزرية الصغيرة النامية الكشف عن محاولات لاستغلال نقاط ضعف جديدة. على الأقل من الناحية النظرية يمكن ذلك. الدول النامية الجزرية الصغيرة هي أيضا أقل اعتمادا على تشغيل الآليات الخاصة بالنظام.ميزة أخرى إلى الدول الجزرية الصغيرة النامية هو أنه يمكن الكشف عن نشاط متميز احتيالي أو سيئ من الداخل. على سبيل المثال، يمكن نقل احتيالي للأموال من حساب إلى آخر ستطلق أجهزة الإنذار إذا كان المستخدم لم يدخل عادة لهذا الحساب، أو إذا كان المبلغ بالدولار ليس من العادة بالنسبة للفرد، أو إذا كان ذلك تم في وقت غير عادي . وبعبارة أخرى، فإن التنبيه يطلق إذا كان طريقة النقل الإحصائية يختلف كثيرا عن النشاط العادي المستخدم أو السلوك.لايوجد في كثير من الدول النامية الجزرية الصغيرة في السوق اليوم، على الأقل ليس هنالك نظام كمبيوتر للشركات القياسية أو الشبكة. ويرجع ذلك إلى عدد من العوامل. أولا، أنها تميل إلى أن تكون عددا كبيرا من الانذارات الخاطئة. ويرجع ذلك إلى حقيقة نظر الدول النامية الجزرية الصغيرة لأي نشاط جديد أو مختلف على انه تهديد. عدد قليل جدا من الشبكات الثابتة. وبالإضافة إلى ذلك، وضع تعريف المستخدمين قد يكون من الصعب، وخاصة في بيئة للمستخدمين العمل جداول غير منتظمة أو أن هناك ارتفاع معدل دوران. ونتيجة لذلك، سيكون

من الصعب جدا التنفيذ بالدول الجزرية الصغيرة النامية في بيئة حيث التغييرات للمستخدمين، طوبولوجيا للشبكة والخوادم، أو التطبيقات هي القاعدة. يجب أيضا أن تكون الدول النامية الجزرية الصغيرة مرنة بما فيه الكفاية لتعديل نموذجهم كما يغير المستخدم أو أنماط النشاط للشبكة. ومع ذلك، يمكن في الواقع أن تستغل هذه المرونة إلى الاستفادة من الدخيل على الشيكة.إذا كانت التغييرات تدريجية طفيفة وأجريت في فترة طويلة، متسللة يمكن "اعلام" الدول الجزرية الصغيرة النامية لقبول النشاط الاحتيالي أو السيئة بأنها "طبيعية".نقطة ضعف أخرى للنهج مع مرور الوقت أن نشاط SIDS هو أنه بغض النظر عن ما إذا كان يدرس SID التدخل أمر طبيعي أم هو مجرد سهو من جانب النظام، والدول الجزرية الصغيرة النامية لن تعترف لأي نوع من الهجمات التي تتوافق مع السلوك التي كان عليها سوف SIDS الاعلام على انها طبيعية. وبعبارة أخرى، إذا لم يكن غير طبيعي، فان نفترض أنه ليس تدخلا. هذا المنطق في كثير من الأحيان مغالطاً.

قلق آخر مع الدول النامية الجزرية الصغيرة هو كيفية تحديد ما هي مكونات المراقبة لخلق النماذج. الاحتمالات لا حصر لها وتشمل الوصول إلى الملفات، وقت الوصول، وشبكة الاتصالات، وحجم الحزم، واستخدام وحدة المعالجة المركزية. وبالإضافة إلى ذلك، تحديد متى تنحرف عن القاعدة بصورة ملحوظة إحصائيا يمكن أن يكون صعبا. مثل معظم الأشياء في أمن الشبكات، بل هو عملية موازنة.العديد من الدول النامية الجزرية الصغيرة مستخدمة اليوم للاستفادة من الشبكات العصبية. الشبكة العصبية هو نوع من الذكاء الاصطناعي التي يمكن تدريبها على الاعلام. وعادة ما ينطوي تغذية الشبكة العصبية بكميات كبيرة من البيانات وبرمجة مجموعة معقدة من القواعد حول علاقات البيانات. في شكل مجموعة مرة واحدة في مكان، وقواعد يمكن تعديلها من قبل الشبكة العصبية على أساس مدخلات إضافية. الشبكات العصبية "اعلام" من الأمثلة والمدخلات الإضافية. الشبكة العصبية قادرة على الاعلام وهي من الأمثلة لإيجاد أنماط في البيانات من عينة بيانات تمثيلية. لمزيد من الأمثلة أو إدخال شبكة تتلقى أكثر اعلام. الشبكات العصبية قادرة على التنبؤ بالأحداث المستقبلية استنادا إلى الأداء السابق.

تتضمن الشبكة العصبية عادة أنظمة المعالجة المتوازية الكبيرة وتقوم بتوظيف مفهوم المنطق الضبابي. وتوصف الشبكات العصبية في بعض الأحيان من حيث طبقات المعرفة، مع شبكات أكثر تعقيدا وجود أكثر من طبقات. هذه الأنظمة تفحص البيانات المدخلة تتخذ قرارات بناء على مجموعة معقدة من القواعد والأمثلة الماضية.يجري توظيف الشبكات العصبية لتحليل مخاطر الائتمان، وتوقع اتجاهات السوق، والتنبؤ بالطقس، والكشف عن الغش. على سبيل المثال، فيزا وماستركارد تستخدم الشبكات العصبية لتحديد النشاط الاحتيالي. الشبكات العصبية تمشط الملايين من المعاملات اليومية لتحديد الحالات الشاذة في النشاط استنادا إلى أنماط لكل حامل البطاقة "فردي" في الماضي. هذا إنجاز مثير للإعجاب،

بالنظر إلى حجـم المعـاملات وعـدد حـاملي بطاقـات كـل شـركة لـديها فـي قاعـدة عملائها.

المنهج –الدفاع المعمق:

واحدة أداة أكثر فقط فـي نهـج الـدفاع IDS مثل جدار الحماية، ينبغي أن ينظر إلى المعمق.

وفاعلية النظام يمكن ،ierتقنية المعلومات mult وينبغي أن تكون الإجراءات الأمنية أن تكون بمثابة طبقة أخرى من الأمن.

يتم التأكد من وزن الايجابيات والسـلبيات والتأكـد مـن أن ، IDS ومع ذلك قبل نشر البائع الذي تختاره لديه نظام يناسب احتياجاتك. وفيما يلي بعض من الايجابيات مــن فاعلية النظام على النحو التالي:

- يمكن الكشف عن بعض التجاوزات والاختراقات.
- هل تعرف أين هي الهجمات التي تحدث.
- هل يمكن أن تكون مفيدة لجمع الأدلة؛
- يمكن أن نلفت الإداريين أن شخصا ما يحقق.
- يمكن اتخاذ إجراءات تصحيحية ضد أنواع معينة من الانتهاكات أو الاقتحامات.

على النحو التالي IDS وفيما يلي بعض سلبيات:

- ملكات العديد من أنواع التجاوزات والاختراقات.
- لا تعمل بشكل جيد او عدم السرعة الفائقة أو حجم الشبكات الثقيلة ؛
- توليد الانذارات الخاطئة.

يمكن أن تضيف عمقا للأمن الخـاص بشـكل عـام، ممـا يسـاعد علـى تحديـد IDSو في حـد ذاتـه لا يضـمن الأمـن. فاعليـة IDS الاختراقات والتجاوزات الممكنة، ولكن النظام أمامه طريق طويل ليقطعه قبل أن تكون فعالة كما ان الكثير يقوم بتصـديق ضجيج التسويق القائم على شبكة عجز فاعلية النظام "على العمـل بفعاليـة وعاليـة السرعة، الشبكات كبيرة الحجم هي مجرد مثال من احدى القيـود الـتي لهـا فاعليـة النظام للتغلب عليها قبل أن تصبح فعالة حقا.حتى عندما كانت تعمل بشكل صـحيح، جميـع فاعليـة النظـام لا تـزال يغيـب عنهـا العديـد مـن أنـواع محـددة وضـارة مـن الهجمـات. النهـج الأكـثر فعاليـة لكشـف التسـلل هـو اسـتخدام مزيـج مـن الكشـف المستندة إلى المضيف القائم على الشبكة.

الاتجاهات المستقبلية:

الاقتحام أو الانتهاكات عادة لا تقتصر على نظام واحد أو على وحدة الشـبكة. ونحـن نعمل الآن في بيئة حيث يتـم توزيـع المعلومـات عـبر الشـبكات الكـبيرة الـتي تـدار مركزيا. ونتيجة لذلك، قد يكون من المفيد الحصول على أدوات كشف التسلل الـتي مقر الشبكة ، IDS القائم على مضيف الاتصالات مع IDS تستخدم نهجا وزعت فيها فريق عمل IETF وكلاهما تخطر الإدارة المركزية من أي شذوذ.لهذه الغاية، شكلت لدراسة كشف التسلل. وفقا لميثاق الفريق العامـل، والغـرض مـن كشـف التسـلل لفريق العمل هو: "... لتعريف تنسيقات البيانـات وإجـراءات الصـرف لتبـادل IETF المعلومات التي تهـم الكشـف والاسـتجابة لأنظمـة التسـلل ونظـم الإدارة الـتي قـد والـتي تـؤدي إلـى دمـج IETF تحتاج للتفاعل معها ".يمكن للمرء التأمل فـي جهـود نهاية إلى نهاية فاعلية النظام التي هي قادرة علـى الرصـد والـرد علـى الاختراقـات والتجاوزات للمشروع بأكمله.

الفصل 16

إدارة الأزمات

يصف هذا الفصل عملية التخطيط أن كل مؤسسة من خلال التحضير يجب أن تذهب لهذا الحدث الذي يهدد العملية أو جدوى المنظمة.يمكن اعتبار الوقاية من الكوارث و التخطيط الحادث لاستجابة أمن الكمبيوتر هما وجهين لعملة واحدة. الموضوعين يرتبطان ارتباطا وثيقا ويشتركان في بعض المنهجيات والأهداف المشتركة.نشعر بالقلق على حد سواء مع ضمان توافر وسلامة الشبكات المنظمة والنظم.تخطيط الوقاية من الكوارث من وقت لآخر، يواجه العديد م ن الشركات حدثا كارثيا يمكن أن يهدد بقاء المنظمة. وفقا لذلك، يجب على كل منظمة صياغة مجموعة من الإجراءات لتفاصيل الإجراءات الواجب اتخاذها تحسبا لحدوث كارثة. وينبغي تصميم الإجراءات وكأن الحدث الكارثي أمر لا مفر منه وسوف تحدث مستقبلاً. ويشار إلى هذا النوع من الخطة على أنها خطة الوقاية من الكوارث. في بعض المنظمات، يسمى تخطيط الوقاية من الكوارث التخطيط للطوارئ أو التخطيط لاستئناف العمل.يعتقد بعض المنظمات أن وجود خدمات استعادة الموقع الساخن هو نفس وجود خطة الوقاية من الكوارث. الموقع الساخن هو منشأة تم تصميمها ليتم تفعيلها في حال أن أجهزة الكمبيوتر في المؤسسة أو مرافق الكمبيوتر غير قابلة للتشغيل. وتكوينها موقع ساخن مع السلطة، والضوابط البيئية، والاتصالات، وأجهزة الكمبيوتر اللازمة للمنظمة لاستئناف عمليات الكمبيوتر م ع تعطيل الحد الأدنى من الخدمة.

وردا على أسئلة حول خطط الوقاية من الكوارث، لقد قال لي الزملاء أن التعاقد على خدمات الموقع الساخنة أو الحفاظ على النظم الزائدة عن الحاجة في منشأة أخرى، وكأن كل ما يحتاجونه أن نهتم والتأكد من أن الأنظمة مغطاة. في اغلب الحالات، كان التركيز على الأجهزة والبرامج وليس على رجال الأعمال والناس. خطة الوقاية من الكوارث هو استئناف العمليات التجارية، وليس مجرد تواصل عمليات الكمبيوتر.متطلبات خطة الوقاية من الكوارث تختلف عن كل منظمة. ومع ذلك، بالنسبة لمعظم المنظمات، الحد الأدنى من أهداف خطة الوقاية من الكوارث هي توفير المعلومات والإجراءات اللازمة للقيام بما يلي:

1- الاستجابة لحدوث الكوارث؛

2- إخطار العاملين اللازمين.

3- تجميع فرق الوقاية من الكوارث.

4- استرداد البيانات التي قد تكون قد فقدت نتيجة للأحداث.

5- معالجة الاستئناف في أسرع وقت ممكن لضمان الحد الأدنى من تعطل عمليات المؤسسة.

6- الالتزام بأي متطلبات تنظيمية التي تملي على وجود خطة الوقاية من الكـوارث للمنظمة.

واحدة من العوامل الرئيسية في نجاح خطة استئناف العمـل هـو التخطيـط السـليم لمجموعة تكنولوجيا المعلومات. معظم المنظمـات اليـوم تعتمـد بشـكل كـبير علـى أجهزة الكمبيوتر والشبكات والاتصالات وتكنولوجيا المعلومات بشـكل عـام. ونتيجـة لذلك، وأنه يلعب دورا رئيسيا في التخطيط للوقاية من الكوارث لمعظم المنظمات. عـادة، وحـدة تقنيـة المعلومـات تطـور خطتهـا الخاصـة منفصـلة عـن الوقايـة مـن الكوارث، ادى تفاصيل الإجراءات اللازمة للحد مـن تعطـل النظـام، وبالتـالي تقليـل تعطل العملية للمنظمة. تـم دمـج خطـة تقنيـة المعلومـات مـع خطـة الوقايـة مـن الكوارث الشاملة للمؤسسة.موضوع تخطيط الوقاية من الكوارث تقنية المعلومات هو موسوعة تكفي بسهولة لملء كتاب. في الواقع قد كتب العديد من الكتـب حـول هذا الموضوع. ويهدف هذا الفصل لمناقشة تقنية المعلومات وتخطيط الوقايـة مـن الكوارث من منظور تجاري وإظهار كيف يربـط في أمن الشـبكات. مـن المهـم أن نتذكر أن واحدا من العناصر الأساسية لأمن المعلومات هو "إتاحة". وهذا يشير إلـى توافر المعلومات التي تقع على أنظمـة وشـبكات للمنظمـة. التخطيـط السـليم هـو ضروري لضمان توافر نظم ذات المهام الحرجـة. ومـن الأهميـة بمكـان فـي عمليـة التخطيط لتحديد ما هو المسـتوى الكـافي مـن الإعـداد ومـا هـو نظـام ذات المهـام الحرجة.

ما هو مستوى التحضير؟

إلى أي مدى تكون المنظمة مستعدة لاسـتثمار المـوارد فـي تكنولوجيـا المعلومـات والتخطيط للوقاية من الكوارث يجب أن تكون ذات صلة مباشرة لأعمال المنظمــة. المنظمـات المختلفـة لهـا احتياجـات الإنعـاش المختلفـة، وفيمـا يتعلـق تكنولوجيـا المعلومات. ونتيجة لـذلك، ينبغـي للخطـط الـتي وضـعتها منظمـات مختلفـة تعكـس احتياجاتهم. على سبيل المثال، يمكن لمنظمة غير ربحية تعتمد على جمع التبرعــات للدخل وربما البقاء على قيد الحياة عدة أيام إن لم يكن أسابيع، مـن وقـت التوقـف عن العمل. مصرف، من ناحية أخرى، يمكن أن تجـد نفسـها مـن الأعمـال إذا كـانت أنظمتها أسفل لتلك الفترة. يمكن أن معظم البنوك تتحمل بضع ساعات لمـدة يـوم أو يومين من التوقف نتيجـة لحـدوث كارثـة، فـي حيـن أن شـركة سمسـرة الأوراق المالية التي يتم تداولها في بورصة نيويورك أو بورصة ناسداك يمكن أن تجد نفسـها في الخراب المالي إذا كانت أنظمتهـا أسـفل لبضـع سـاعات و أنهـا لـم تتمكـن مـن التجارة. وكمية الموارد التي تدخل في تكنولوجيا المعلومـات اسـتعدادا للوقايـة مـن الكـوارث الـتي كتبهـا الاحتياجـات التشـغيلية للمنظمـة، وقـدرة المؤسسـة، أو عـدم وجودها، من أجل البقاء التوقف.في حين أنه سيكون من الرائع إذا كان كل مؤسسة موارد غير محدودة للتحضير لاستئناف فوري للعمل بعد وقوع كارثة، مثل كل شـيء آخر في مجال الأعمال التجارية، ويجب تـبرير الإنفـاق علـى التخطيـط للوقايـة مـن

الكوارث من خلال تحليل التكاليف. في حالة منظمة غير ربحية، هناك خسارة مالية ضئيلة مرتبطة تعطل نفسها.

وبعبارة أخرى، فإن عدم القدرة على القيام بأعمال تجارية لمدة يوم أو اثنين لديها الأثر المالي البسيط نسبيا على المنظمة. في مثل هذه الظروف، سيكون من الصعب تبرير تكاليف إعداد الوقاية من الكوارث واسعة النطاق التي تشمل أشياء مثل أنظمة الاتصالات السلكية واللاسلكية زائدة والمواقع الساخنة. في المقابل، يمكن لشركة الوساطة بالأرجح تثبت أن عدم القدرة على العمل، حتى لفترة قصيرة من الزمن، من المحتمل أن تكلف الشركة مبلغ كبير من المال. ونتيجة لذلك، يمكن للشركة وساطة تبرر النفقات الكبيرة لا المتعلقة بإعداد الوقاية من الكوارث والتخطيط تقنية المعلومات.قرارات التخطيط للوقاية من الكوارث يجب أن تتم مثل معظم كل قرار في المسائل الأخرى.تكلفة الوقاية يجب أن تكون وزنها ضد الخسائر التي كبدتها نتيجة التوقف التي قد تحدث. عند تقدير تكلفة الوقت الضائع، من المهم أن تشمل التكاليف الناعمة فضلا عن التكاليف الثابتة. والتكاليف الثابتة، مثل العائدات المفقودة ترتبط مباشرة إلى التوقف، من السهل قياسها كميا. التكاليف الناعمة هي البنود التي يصعب قياسها كميا مثل إرادة العملاء الجيدة، ومستوى الخدمة، ورضا أو ثقة المستهلك. يستغرق معرفة وافية من الأعمال المؤسسة لتكون قادرة على تقدير التكاليف الناعمة.

ونتيجة لذلك، قد يكون من الصعب على وحدة تكنولوجيا المعلومات لتقدير هذه التكاليف وحدها. ولذلك، مشاركة من وحدات الأعمال الأخرى داخل المنظمة هو أمر حيوي لعملية تحديد التكاليف المرتبطة وقت التوقف عن العمل.

ما الاستعادة الأولى؟

فقط المنظمات المختلفة والتي لها احتياجات الإنعاش المختلفة، وظائف مختلفة داخل المؤسسة لديها مستويات متفاوتة من أولوية لتحقيق الانتعاش. وينبغي لأي خطة وقاية من الكوارث و تقنية المعلومات تعيين مستويات الأهمية إلى كل نظام للتأكد من الأنظمة التي ستعطى الأولوية عند استعادة الخدمات. الوظائف ذات المهام الحرجة بحاجة إلى الكشف عن الهوية قبل وقوع كارثة، حتى أنه عندما يحدث كارثة، فإنه لا نضيع الوقت لاستعادة النظم الزائدة بدلا من تلك التي مطلوبة حقا. ومرة أخرى، وهذا يستغرق معرفة وافية من المنظمة للأعمال والمدخلات من خارج وحدة تكنولوجيا المعلومات. نهج واحد هو جمع هذه المعلومات من خلال فريق تقييم برئاسة تقنية المعلومات ولكن بمشاركة الإدارة والموظفين على دراية في عمل المنظمة ومألوفة مع مختلف النظم والتطبيقات. وينبغي أن تتضمن هذه العملية التحقق من الصحة رسميا وفهم الفرق من أعمال المنظمة.

ان نهج آخر يتمثل في تحديد أو تعيين ملكية لكل طلب والحصول على مدخلات أصحابها. من خلال طريقة العمل حتى التسلسل الهرمي من التطبيقات والنظم، ويجب أن تكون قادرة على إعطاء أولوية لبعضها. ينبغي أن تشمل هذه العملية أيضا

الحصول على منظور الإدارة على مدى أهمية كل تطبيق لتصريف الأعمال. يجب أن يكون كميا عملية أنظمة تحديد الأولويات، عن طريق إجراء تحليل مفصل لكل تطبيق، لتحديد ما هي التكلفة للمنظمة لتفقد الوصول إلى وظيفة معينة.استعراض واختبار من منظور تحليل التكاليف، الناجح إعداد الوقاية من الكوارث هو متناسب مع الخسائر المحتملة. من الناحية التشغيلية، خطة الوقاية من الكوارث الناجحة هي التي تستجيب لاحتياجات الأعمال التجارية للمنظمة.

من منظور الإدارة العامة، يجب أن تبقى خطة الوقاية من الكوارث الحالية وتحديثها مع أية تغييرات ضرورية. يجب أن تنعكس التعديلات على الأنظمة والأفراد وأولويات العمل، والعوامل البيئية الأخرى في الخطة. وهذا يعني استعراضات منتظمة ومتكررة من خطة الوقاية من الكوارث. بالنسبة لمعظم المنظمات، والعمر الافتراضي للخطة الوقاية من الكوارث حوالي ثلاثة إلى أربعة أشهر. وبعبارة أخرى، وهذا هو كم من الوقت سيستغرق لخطة لتصبح خارج التاريخ وتحتاج إلى تنقيح. خلال الفترة 3-4 الشهر، وسوف تتحول أفراد أكثر، وسيتم عرض تقنيات و / أو تقاعد، سيتم الافراج عن منتجات جديدة، وسوف تتغير أولويات العمل. ونتيجة لذلك، سوف تحتاج خطة للمراجعة لتعكس هذه التغييرات.

يجب أن يكون هناك أيضا اختبارات منتظمة وشاملة خطة الوقاية من الكوارث، ويجب أن تدمج نتائج أي اختبارات في الخطة. وعلاوة على ذلك، يجب على الموظفين الرئيسيين فهم أدوارهم ومسؤولياتهم في الخطة. إذا لم يفعلوا ذلك، الخطة الأفضل في العالم سوف تكون ذات قيمة تذكر للمنظمة عند وقوع الكارثة.الوقاية من الكوارث دراسة حالة التخطيط وكمثال على السبب من المهم لتحديث تلك الخطط والمؤسسة المالية علاقة تجارية مراجعة شاملة لاستعدادات الوقاية من الكوارث الحالية. في ذلك الوقت، كانت الخطة استئناف عمل حول ثماني سنوات من العمر.منذ ذلك الوقت تم تطوير الخطة في الأصل، تم تحديث المقاطع الفردية من الخطة لتعكس التغيرات في أشياء مثل الموظفين والتكنولوجيا، ولكن لم يتم استعراض الخطة في مجملها إلى تحديد ما إذا كان لا يزال كافيا لأعمال المؤسسة المالية.

وكان الغرض من هذا الاستعراض لضمان أن الشركة مستعدة بشكل صحيح للتعامل مع الكوارث إما محدودة في نطاقها أو كبيرة في الحجم، والتي توقفت العمليات التجارية العادية.للاستعراض، تم تجميع فريق لتقييم ومراجعة خطة الوقاية من الكوارث القائمة. وضم الفريق شريحة من وحدات الأعمال داخل المنظمة. وكان معظم المشاركين للفريق الأعضاء الرئيسيين أيضا في فريق استئناف العمل. وكانت الفكرة للفريق لمراجعة وتنقيح الخطة اللازمة لتلبية احتياجات المنظمة.كما هو الحال مع أي خطة الوقاية من الكوارث، وكان الهدف من الخطة الحالية لاستئناف سريع لعمليات التنظيم في حال وقوع كارثة.

كانت المهمة الأولى لمراجعة خطة موجودة من البداية الى النهاية. استعراض الخطة الحالية تأكيد فقط بان اكثر الفريق يعرف بالفعل. وكان هذا نموذج عمل المنظمة قد تغيرت بشكل كبير منذ ولدت الخطة لأول مرة ، ولكن انعكست أيا من هذه التغييرات على الخطة. بعد استعراض شامل للخطة الحالية، ووصول فريق إلى استنتاج مفاده أن مجرد مراجعة الخطة لن تكفي لتلبية احتياجات المنظمة. وكانت الخطة التي مر عليها الزمن ، وكانت هناك العديد من أوجه القصور من ذلك أن الخطة تحتاج إلى إعادة كتابة تماما. بعض أوجه القصور الرئيسية لخطة الوقاية من الكوارث المنظمة هي مفصلة على النحو التالي:

• أنظمة التسليم البعيدة: عندما وضعت خطة الوقاية من الكوارث المؤسسة المالية الأولى قبل سنوات، تم تنفيذ أكثر من 50٪ من جميع الأعمال التجارية مع العملاء في الفروع من قبل فرز الأصوات. عندما وضعت الخطة في الأصل، كانت مؤسسة مالية اقل من أنظمة توصيل الإلكترونية التي كانت في المكان في وقت الاستعراض. تلك التي كانت قد نشرت في وقت سابق من سنوات لم تستخدم على نطاق واسع من قبل قاعدة عملاء المؤسسة المالية عن تلك التي كانت في المكان خلال فترة الاستعراض. ونتيجة لذلك، فإن التركيز الرئيسي للخطة الوقاية من الكوارث للمنظمة، كما كان موجودا، وكان استئناف عمليات الفروع. كشف استعراض لكيفية تعمل المؤسسة المالية أن أكثر من 85٪ من جميع المعاملات التي أجريت من خلال أحد أنظمة تسليم الإلكترونية. ونتيجة لذلك، خطة الوقاية من الكوارث المؤسسة المالية اللازمة لتعديلها لتعكس التركيز في المقام الأول على استعادة النظم التي تم لها توفير الخدمات للعملاء. وقال إن الخطة الأصلية لم تعالج بشكل كاف لاستعادة عمليات مركز الاتصال للمنظمة، الخدمات المصرفية عبر الإنترنت، أو الخدمات المصرفية عن طريق هاتف الأنظمة. ونتيجة لذلك، كان من الضروري إعادة الكتابة بشكل كبير من الخطة الحالية لضمان استئناف سريع لهذه الخدمات لتسليم الالكترونية في حال وقوع كارثة.

• النطاق الجغرافي: وثمة مشكلة أخرى مع الخطة أنه عندما تم تطويرها لأول مرة قبل سنوات، الأغلبية الساحقة من قاعدة العملاء وجميع من مكاتب المؤسسات المالية تقع في منطقة خليج سان فرانسيسكو. كان واحدا من الافتراضات الأساسية للخطة أن أي حدث كبير يكفي لتعطيل عمل المؤسسات المالية، مثل الزلازل، من شأنها أن تؤثر أيضا على العملاء. وقد استخدم هذا الافتراض لتحديد أولويات النظم. على سبيل المثال، تأثير الهواتف لدينا، كان الافتراض أن هواتف العملاء ستتأثر. في هذه الحالة، واستعادة للنظام مثل النظام المصرفي عن طريق الهاتف لن تعطى أولوية قصوى. وبالإضافة إلى ذلك، كان من المفترض أن عملائنا الذين سيتعرضون للكوارث، من شأنهم أن يفهموا انه كان يتطلب وقتا لاستعادة الخدمة العادية. في الوقت الذي تصور الخطة، ان الشركة تفكر مثل، مؤسسة مالية صغيرة ، وينعكس الخطة على العقلية. لم يكن بالضرورة خطأ عقلي، لأن في ذلك الوقت وقد صممت هذه الخطة، كانت المنظمة مؤسسة مالية صغيرة. ومع

ذلك، في السنوات الفاصلة، نمت المؤسسة المالية وتوسعت خارج منطقة خليج سان فرانسيسكو. في وقت المراجعة، كان لديها مكاتب في جميع أنحاء ولاية كاليفورنيا، تكساس، ولاية أوريغون، نيو جيرسي، وأريزونا. في الواقع، يعيش أكثر من 40٪ من قاعدة عملائها وتعمل خارج منطقة خليج سان فرانسيسكو. ونتيجة لذلك، لم يعد من الممكن افتراض أن العملاء سوف يخضعون لنفس الكارثة التي ضربت المؤسسة المالية. وبالإضافة إلى ذلك، لا يمكن، وينبغي ألا يفترض أن العملاء سوف يفهمون ان كانت هناك كارثة كبرى في منطقة خليج سان فرانسيسكو. سيكون عملاء الخارج منطقة الخليج لا يهتمون ان كان هناك زلزال في سان فرانسيسكو. فإنها لا تزال تريد الوصول إلى الخدمات التي يتوقع أن مؤسسة مالية تقدمها. ونتيجة لذلك، فان المؤسسة المالية اللازمة لوضع خطة الوقاية من الكوارث التي كفلت الاستئناف السريع للعمليات لجميع الأحداث، حتى لو كان هناك كارثة كبرى في منطقة خليج سان فرانسيسكو.

- خدمات الوقاية من الكوارث: استعراض التغييرات التي يتعين إدراجها في خطة الوقاية من الكوارث لدى المؤسسة المالية، تقرر أن المؤسسة المالية قد تجاوزت الشركة التي كانت قد تعاقدت ل "الموقع الساخن" لخدمات الوقاية من الكوارث. وكان هناك عدد من الأسباب لاختيار المراجعة بدائل لمزود الخدمة الحالي:

- المواقع الساخنة المتعددة (المحلية مقابل البعيدة): على مقدم الخدمة على المؤسسة المالية التي كانت تستخدم في ذلك الوقت يمكن أن توفر موقع ساخن واحد، التي كانت تقع خارج الدولة فقط. في حال اضطرت المؤسسة المالية لتفعيل خطة الوقاية من الكوارث لها، فإنه سيتعين عليها لنقل الأفراد ووسائل الإعلام، والإمدادات إلى الموقع خارج الدولة. وهذا من شأنه إضافة 24-48 ساعة على الوقت الذي سيستغرقه لاستئناف عمليات الكمبيوتر. في حين أن هذا السيناريو قد يكون مقبولا في حال وقوع كارثة كبرى، مثل وقوع زلزال، فإنه لن يكون مقبولا إذا شهدت المؤسسة المالية حدثا محليا مثل النار في غرفة الحاسوب أو مجرد فشل نظام كبير.

تحت سيناريو كارثة محدودة، فإن المؤسسة المالية تريد خيار تفعيل الموقع الساخن التي من شأنها أن تكون في المتناول محليا. منذ وقت السفر سيكون ضئيلا، فإن الموقع الساخن المحلي يقلل بشكل كبير من كمية الوقت الذي ستستغرقه الشركة للحصول على الأنظمة مرة أخرى من على الإنترنت. من الناحية المثالية، يمكن أن يكون مزود الخدمة أفضل بعرض المواقع الساخنة المتعددة، مع اختيار المواقع المحلية والبعيدة.

خلاف محتمل للخدمة: وثمة قضية أخرى حقيقة أن الشركة المؤسسة المالية المستخدمة لخدمات الوقاية من الكوارث متعاقدة مع العديد من العملاء في منطقة خليج سان فرانسيسكو لتقديم خدمات الوقاية من الكوارث. وفي حال وقوع كارثة

كبرى، مثل الزلازل، فإن المؤسسة المالية تتنـافس مـع غيرهـا مـن العملاء منطقـة خليج سان فرانسيسكو في الوقت والموارد في مركز الوقاية من الكوارث.

قدرة مركز الوقاية من الكوارث: بعد الاطلاع على التسـهيلات المتاحـة فـي مركـز الوقاية من الكوارث، تقرر أن مزود الخدمة لم يكـن لـديهم مـا يكفـي مـن المـوارد للتعامل مع جميع عملائها في منطقة خليج سان فرانسيسكو.

للتواصـل مـع مركـز ISDN وبالإضافة إلى ذلك، المؤسسة المالية استغلت الـدوائر الوقاية من الكوارث مزود الخدمة. ونتيجة لذلك، فإنه يتطلب أن يكون هنـاك علاقـة مزود الخدمة في مركـز ISDN واحد الى واحد بين المكاتب الفرعية لدينا والموانئ الوقاية من الكوارث. في الوقت الذي تم توقيع العقد فـي الأصـل لخـدمات الوقايـة من الكوارث، وكانت المؤسسة المالية لديها عدد محدود من المواقـع الـتي تتطلـب الاتصال إلى مركز الوقاية من الكوارث في حال وقوع كارثة. في السنوات الفاصلة، المؤسسة المالية نمت ومستمرة في النمو. وبالتالي استنتج أن في ذلك الوقت لـم يكن في مركز الوقاية من الكوارث الحالية ليس لديها القدرة الكافية علـى التعامـل مع جميع مكاتب فرع المؤسسة المالية في وقت واحد. ان الوضع أصبح أسوأ فقط، منذ تم فتح مكاتب جديدة بمعدل اثنين أو ثلاثة في السنة.

بعد مراجعة قائمة كارثة استرداد الاستعدادات، تقرر أن المؤسسـة الماليـة تسـتلزم مزود خدمة الوقاية من الكوارث مع قدرة وفيرة والقدرة على توفير مواقـع سـاخنة متعددة. من الناحيـة المثاليـة، فإن أي مـزود خدمـة تكـون قـادرة علـى تقـديم كـل المواقع المحلية الساخنة، والتي يمكن تفعيلها لحدث محدود، والمواقع الساخنة عـن بعد في حال تأثر منطقة خليـج سـان فرانسيسـكو بكارثـة كـبرى.اسـتنتاج آخـر مـن استعراض الخطـة الحاليـة أن تكـوين الاتصـالات الحاليـة تصـمم لاسـتئناف عمليـات الفروع، وعلى هذا النحو، لم تكن كافية لأنظمة تسـليم الإلكترونيـة. وبالإضـافة إلـى ذلك، لم يكن مرنا بما فيه الكفاية لمعالجة جميع الحـالات الطارئـة. ولكـان التكـوين بوصفها سهلة التنفيذ كما يجب أن تكون في حالة وقوع كارثة. في حال وقوع كارثة، كانت الرغبة في تقليل كمية التدخل المطلوبة لتنفيذ الاتصالات السلكية واللاسـلكية والنسخ الاحتياطي.المؤسسة المالية اللازمة لنشـر تكـوين الاتصـالات الـتي تشـملها النظم تسليم الإلكترونية، والتي كانت مرنة بما فيه الكفاية لمعالجـة جميـع الحـالات الطارئة، والتي كان من السهل نسبيا للتنفيذ. أن تحقيق هـذا الهـدف يتطلـب إنفـاق الأموال لشراء معدات وخدمات جديدة. والاستعانة بمصـادر خارجيـة لخطـة التنميـة وصيانة العديد من المنظمات ليس لديها الوقت والمـوارد والخـبرات اللازمـة لوضـع خطة شاملة للوقاية من الكوارث. وفي ظل هذه الظروف، ينبغي أن تنظر المنظمة الاستعانة بمصادر خارجية فـي عمليـة تطـوير وصـيانة خطـة الوقايـة مـن الكـوارث، وحتى الخطة. عموما،- مصادر الخروج في وضع خطة استئناف الأعمال يتضـمن مـا يلي:

- تخطيط المشروع والتوجه.

- مراجعة استراتيجيات الإنعاش؛
- تحديد خطط الإنعاش والوثائق الداعمة؛
- تطوير برامج الاختبار؛
- وضع وتنفيذ إجراءات الصيانة الخطة.

أي استئجار مستشار لوضع خطة يجب توفير تعليم الوقاية من الكوارث لموظفي الشركة المختارة لتعزيز قدرتهم على فهم والاستجابة لحالات الطوارئ وانقطاع التيار لإعدادهم للمشاركة في تطوير قدرة الانتعاش العامة للمنظمة.تفعيل خطط الإنعاش التي وضعها مستشار ينبغي أن تحدد الإجراءات التفصيلية التي يجب أن تأخذ الشركة للإعلان عن الكوارث، إخطار الموظفين المناسبين من وقوع الكارثة، وخطط الإنعاش، وتنفيذ ترميم والانتعاش في الوقت المناسب. وينبغي أن تتضمن الخطة أيضا برامج الاختبار التي تحدد الأهداف الأساسية والثانوية من الاختبار وتواتر الاختبار. وبعبارة أخرى، يمكن لكل اختبار لديهم هدف مختلف. يمكن للمرء اختبار الاتصالات في حين اختبارات الإجراءات التنفيذية الأخرى.

ينبغي أن تتضمن أي خطة للوقاية من الكوارث برنامج الصيانة لضمان أن خطة الإنعاش تبقى ما يصل إلى التاريخ. وينبغي أن تشمل إجراءات الصيانة استعراضات دورية لمنصات التكنولوجيا.

عادة، يتم وضع خطة من خلال جمع المعلومات من خلال المقابلات وورش العمل والمؤتمرات، والاستبيانات، ما يراه مناسبا من قبل الاستشاري. ينبغي أن عملية وضع الخطة أيضا الاستفادة من الوثائق الموجودة حيثما ينطبق ذلك.يتم استخدام المعلومات التي تم جمعها لتقييم قدرة خطة الوقاية من الكوارث للشركة لتلبية متطلبات العمل في المنظمة. وعند الانتهاء من وثائق خطة الوقاية من الكوارث، ينبغي للشركة تصحيح محتوياته عن طريق إجراء مفصل ودقيق يمر عبرها.خطة الاستجابة لحوادث أمن الحاسب الآلي وثمة جانب آخر من تخطيط إدارة الأزمات هو الحاسوب وشبكة تخطيط الاستجابة للحوادث الأمنية. وينبغي أن تتضمن كل وتحدد .(CSIRP) خطة إدارة الأزمات خطة الاستجابة لحوادث أمن الحاسب الآلي هذه الخطة الإجراءات التي يجب أن تتخذ الشركة عندما يكون هناك تزوير أو إساءة استخدام المملوكة للشركة إعلاميا أو الخدمات الإلكترونية، وسرقة أو تدمير المعلومات عن الشركة، أو اختراق، أو الهجوم على الأنظمة المملوكة للشركة والشبكات. يجب أن الخطة تعالج أمور مثل ما يشكل حادث أمني، وتحديد الموظفين الرئيسيين، وهي عملية الاتصال والإعلام، فضلا عن عملية التصعيد. وغني منذ .CSIRP عن القول، ينبغي أن يكون فريق حماية المعلومات عنصرا أساسيا حدوث حوادث أمنية مع تردد أكثر من الكوارث والمنظمات وتجد أن التخطيط استجابة للحوادث الأمنية في بعض النواحي هو أكثر أهمية من التخطيط للوقاية من الكوارث. بشكل عام، تجربة المنظمات القليلة كوارث حقيقية ولكن التعامل مع

العديد من الحـوادث الأمنيـة. الحرمـان مـن الخدمـة والهجمـات وتفشـي الفيـروس أصبحت شـائعة. معظـم الشـركات علـى اسـتعداد لقبـول الحرمـان مـن الخدمـة أو حوادث الفيروس، ولكن قلة منهم على استعداد للكشف عن شبكات أو حتى عنـدما تتعرض أنظمتها لخطر حقا.

CSIRP توصيات عامة كما هو الحال مع التخطيط للوقاية من الكوارث، ليـس هنـاك عالمي يمكن تطـبيقه علـى CSIRP الذي يناسب جميع المنظمات.ليس هناك قالب أي منظمة. المتطلبات الأمنية لكل منظمة والاحتياجات هي فريدة مـن نوعهـا. ومـع ذلك، فإن الأقسام التالية توضح بعض التوصيات العامة لCSIRP.

المستشار القانوني

الخطوة الأولى هي تحديد فريق الاستجابة لحوادث أمن الحاسوب (CSIRT). يمكن ولكن يجب أن يكـون ، (IPT) لهذا الفريق يكون مختلفا عن فريق حماية المعلومات الممثل في هذه المجموعة. وبالإضافة إلى ذلك، لأنه قد يكـون مـن الضـروري IPT اتخاذ إجراءات قانونية ضد الأطـراف المسـؤولة عـن الحـادث، هـو فكـرة جيـدة لان أو على الأقل يكون ذلك في متناول الجميع. CSIRT يكون المستشار القانوني على قد يكون المستشار القانوني اللازم لتحديد ما إذا كان من الممكن إنهـاء أو مقاضـاة الشخص أو الأشخاص المسؤولين عن الحادث.

مسئولية

قد تكـون هنـاك حاجـة أيضـا للمستشـار القـانوني للمسـاعدة فـي تقييـم مسـؤولية المؤسسة عن أي حادث أمنـي للكمـبيوتر. المسـؤولية يمكـن أن تـأتي فـي أشـكال كثيرة. قد تكون المنظمة مسؤولة عن الخسارة المباشـرة الناتجـة عـن الاحتيـال أو تـدمير أصـول الشـركة. قـد تجـد المنظمـة نفسـها مسـؤولة ماليـا للإفصـاح عـن المعلومات المتعلقة للعملاء والموظفين، أو الشركاء. يجـوز للمنظمـة أيضـا الحاجـة إلـى تقييـم مسـؤوليتها نتيجـة العملاء، الموظـف، الشـريك، أو القراصـنة باسـتخدام أنظمة المنظمة علـى شـن هجـوم علـى نظـام شـركة أخـرى.لقـد قـرأت حسـابات مسؤولي النظام وتتبعت أنشطة القراصنة على أنظمتها لجمع مزيد من المعلومـات عن القراصـنة. بـدلا مـن اغلاق القراصـنة تمامـا، المسـؤول يحـد الأضـرار وتراقـب النشاط لجمع الأدلة على الجريمة والتعرف على الجاني. حساب كليفورد ستول في كتابه البيض الوقواق هو مثال.

هذا النوع من العمـل أو الـتراخي يمكـن أن يكـون المخـاطر، وليـس أقلهـا سـتكون مسؤولية المؤسسة بضرر القراصنة، والسرقة، أو إسـاءة اسـتخدام أنظمـة منظمـة أخرى أو المعلومات. إذا كانت أضرار القراصنة على أنظمة شركة أخـرى، قـد ينشـأ السؤال، لماذا لم تقم الشركة الأولى بوقف القراصنة عنـدما سـنحت لهـا الفرصـة؟ ونتيجة لذلك، فإنني أوصي ضد هذا النوع من النهج ويشـير إلـى أنـه إذا تـم الكشـف عن القراصنة، واغلاقها على الفور. ومع ذلك، لجمع أكبر قدر من الأدلـة فـي عمليـة

ممكن: حفظ سجلات التدقيق ونظام للتعرف على أصول ووقت الهجوم. طباعة جميع السجلات لتجنب وجود تغييرات أو الكتابة فوقها. تدوين الملاحظات التفصيلية حول ما حدث، عندما وقعت، وأي إجراءات اتخذت نتيجة لذلك. وبالإضافة إلى ذلك، تجنب استخدام النظام للخطر أو شبكة للاتصالات بشأن الحادث. ومن الممكن أن القراصنة أو المتسللين يمكن اعتراض الرسائل.

انتقام

أي تدابير للانتقام. ويمكن أن يكون مغريا للانتقام من CSIRP يجب أن لا يتضمن مرسلي البريد المزعج أو لتعقب القراصنة إلى نظام المنشأ له أو لها. هذا النوع من التنظيمات غير قانوني ويمكن أن يؤدي إلى مسؤولية إضافية. حتى سمعت بعض الروايات حيث تتبع مسؤولي النظام أسفل المتسللين، جسديا ذهب إلى أماكن للهاكر، وهددوهم بالأذى الجسدي. في حين أن هذا النهج قد يوفر قدرا معينا من الارتياح، وإنني أوصي بشدة ضدها.هناك سبب آخر لتجنب الانتقام هو أن المتسللين غالبا ما يستخدمون أنظمة الضحايا الأبرياء الأخرى لشن هجمات. هذه الأقنعة يجعل من الصعب تتبع الهجوم إلى المصدر الحقيقي لها. في هذه الحالة، سوف يخلقون فقط ضحية أخرى. في كثير من الحالات، وهذا هو في الواقع النية الحقيقية للهاكر. ويأمل القراصنة للانتقام ليكون موجها ضد النظام أو الشبكة التي كان هو أو هي شن الهجوم. إذاً المنظمة هي التي تفعل الانتقام يمكن أن تجد نفسها اصبحت ضحية، ولكن الجاني مسؤولا عن أفعاله.

نخب

عملية الفرز للتعامل مع جميع المعلومات المتعلقة CSIRP وينبغي أن تشمل الحوادث. وينبغي أن توفر هذه العملية الفرز والتقييم والتحليل الأولي وتحديد ما إذا كان أي تصعيد هو ضروري. الفرز يجب أن تكون بمثابة مركز التنسيق لجميع المعلومات وبضخ هذه المعلومات إلى المجموعات المناسبة.

وكما ذكر سابقا، أنه ليس من العملي لاستخدام CSIRP مصادر للمعلومات على ومع ذلك، هناك العديد من مصادر المعلومات .CSIRP نهج قطع الكعكة لتطوير المتاحة التي يمكن أن توفر بعض الإرشادات العامة للمساعدة في وضع خطة.

لديه "دليل لفرق الاستجابة لحوادث أمن الحاسوب CERT موقع ويب التنسيق URL والتي يمكن تحميلها مجانا على ،"(CSIRTs) وثيقة أخرى مفيدة هي "توقعات .http://www.cert.org/nav/reports.html URL في IETF الاستجابة لحوادث أمن الحاسب الآلي"، والذي يتوفر من لديه معهد SANS .http://www.ietf.org/rfc/rfc2350.txt؟number=2350 أيضا المنشورات مع توصيات مفصلة للتعامل مع مختلف مراحل حوادث أمن الكمبيوتر. ومع ذلك، هناك التكاليف المرتبطة المنشورة، وأنها ليست رخيصة. متاحة في SANS معلومات بشأن المطبوعات

http://www.sans.org/newlook/publications/incident_handling.htm
URL. هذه وغيرها من المصادر المتاحة للخوض في مزيد من التفاصيل المستطاعة
في هذه المساحة المحدودة.

الأهم من ذلك، تحتاج المنظمات لقضاء بعض الوقت في التخطيط مـا يجـب القيـام به في حالة وقوع هجوم، اختراق أمني، أو الاحتيال قبل وقوعها. الوقت لبدء التفكير في ما يجب القيام به ليس أثناء الأزمة، ولكن قبل وقوع الازمة.

الفصل 17

الكوكيز ، ذاكرة التخزين المؤقت، والإكمال التلقائي

اليوم، الملايين من الناس يستخدمون الانترنت كل يوم للتسوق، والأعمال المصرفية، والتعليم، والأعمال التجارية،والترفيه. والعنصرالأساسي في هذه العمليات هو برنامج متصفح الويب.

المتصفحات مثل المستكشف نتسكيب و مايكروسوفت إنترنت إكسبلورر واجهة المستخدم النهائي إلى الويب. عادة عندما يفكر متصفحي الويب أمن المتصفح، إذا الناس عادة ما تكون .SSL كانوا يعتقدون من ذلك على الإطلاق، بل هو اشارة الى أكثر قلقا بشأن اعتراض المعلومات مثل أرقام بطاقات الائتمان، كما يخترق الشبكة. ومع ذلك، هناك التعرض المرتبطة بالملفات الموجودة على محرك سيرفر ويب. يتم إنشاء هذه الملفات، والوصول إليها، PCالأقراص المحلي لل والتلاعب بها من قبل متصفح ويب ومختلف خوادم الويب في كل مرة خادم الويب يستخدم برنامج متصفح الويب الخاص له أو لها. عدد قليل جدا من الناس على بينة من المخاطر المحتملة المرتبطة بهذه الملفات. على أقل تقدير أنها تثير قضايا الخصوصية. وفي أسوأ الأحوال أنها تعرض خادم الويب للاحتيال من مواقع الويب الخبيثة أو من حقيقة أن الملفات يمكن الوصول إليها بعد فترة طويلة من احدهم عند اغلاق المتصفح وتسجل الخروج من الويب. وهذا الفصل يناقش بعض القضايا الأمنية الأساسية المرتبطة مع برنامج متصفح الويب. على وجه التحديد، وسوف نناقش الوظائف الداخلية من المستكشف وإنترنت إكسبلورر. ونحن سوف ننظر في كيفية عملها، ما الذي تبحث عنه، وطرق لحمايتك عند تصفح الويب.

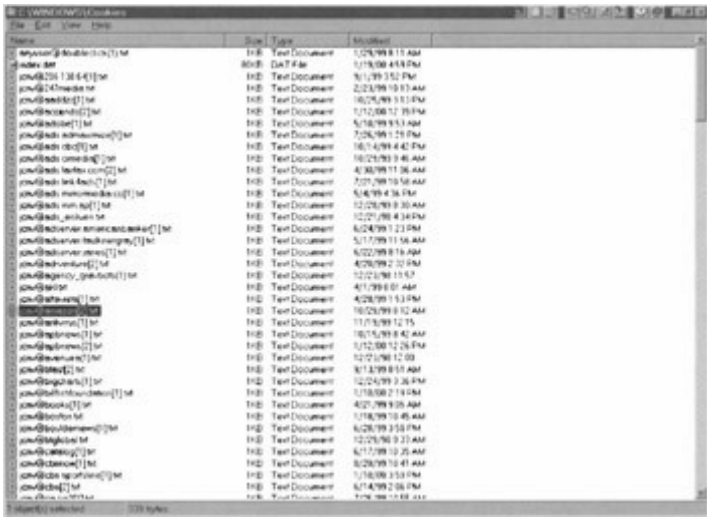
الكوكيز:

لقد كتب الكثير حول ملفات تعريف الارتباط والاستخدامات الممكنة، والانتهاكات. أساسا الكوكيز هي عبارة عن ملفات نصية يتم تخزينها على محرك في واجهة الويب من خلال برنامج متصفح الويب، مثل PCالأقراص المحلي لل Netscape Navigator المستكشف وإنترنت إكسبلورر. الكوكيز هي اختراع من ولكن تم نسخها من قبل مايكروسوفت إنترنت إكسبلورر. البرنامجين الاثنين توظف مقاربات مختلفة قليلا عند تخزين ملفات تعريف الارتباط. يخزن برنامج الملاح كل Internet Explorer برنامج .COOKIE.TXT ملفات الارتباط في ملف واحد يسمى هو في WINDOWS \COOKIES بإنشاء ملف لكل كويكي، ويقوم بتخزينها فيدليل الواقع تكوين الكوكي من قبل خادم الويب وتمريرها إلى المتصفح. والكوكيز تحتوي PCعلى معلومات تتعلق بموقع ويب تم زيارته ثم تخزينها على القرص الصلب لل

عن طريق تخزين المعلومات على قرص واجهة الويب، ومواقـع الـويب .txt. كملف تتجنب الاطرار إلى تخزين المعلومات على أجهزتهم.

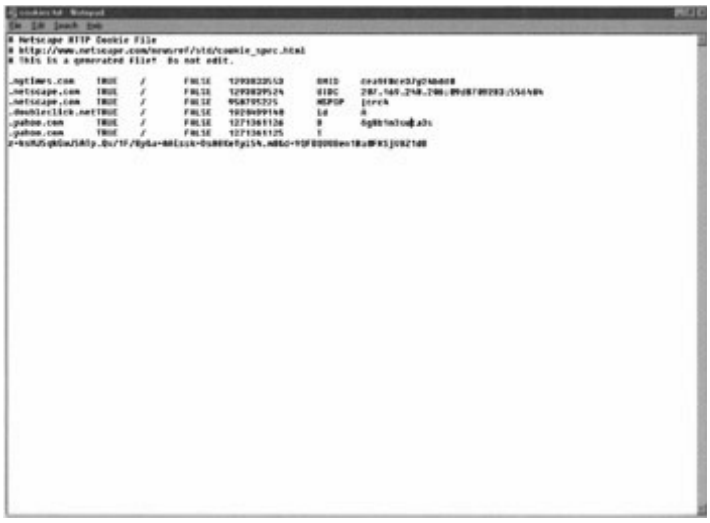
في الأساس تستخدم الكوكيز لتعقب المواقع الـتي قمـت بزيارتهـا. الكـوكي يمكـن استخدامها لتعقب عدد المرات الـتي قمـت بهـا لزيـارة الموقـع، وذلـك عنـد تخزيـن تفضيل شخصي وضع لموقع معين، أو لعقد المصادقة الخاصة بك لموقع معين. على سبيل المثال، إذا كان ملف تعريف الارتباط هـو تتبـع عـدد المـرات الـتي قمـت بها لزيارة موقع معين، سيتم فتح ملفات تعريف الارتبـاط فـي كـل مـرة تتصـفح يـزداد العداد المخزن في ملف تعريف الارتباط بالعدد 1. هذا النوع من المعلومـات يمكـن أن تكون مفيدة للمتسوقين وأصحاب المواقع لتحديد عدد الزائرين العائدين للموقع.

عندما تخصيص المواقع المفضـلة مثـل يـاهو، سـيتم إنشـاء ملـف تعريـف الارتبـاط الخاص بك. وسوف تسـتخدم معلومـات ملـف PCوتخزينها على القرص الصلب لل تعريف الارتباط لتخصيص لمعلومات الشعار التي تناولت مناطق معينة مـن الفائـدة أو لتحديد ما إذا كان استخدام الإطارات أو لا. في كل مرة تقوم بزيارة موقع ويــب، فإن خادم الـويب يفتـح ملـف تعريـف الارتبـاط وتعـديلالمعلومات المعروضـة وفقـا للتفضيلات المخزنة في ملف تعريف الارتباط. وعندما يستخدم سـيرفر الـويب وهـو الموقـع الـذي يتطلـب عمليـة التسـجيل، مثـل نيويـورك تـايمز أو مواقـع ويـب يتـم كتابـة معلومـات الصـلاحيات علـى الكويـك وتخزينهـا علـى Amazon.com، المسـتخدم.مـع بعـض ملفـات تعريـف الارتبـاط هـذا يمكـن أن تشـمل أسـماء PC المسـتخدمين وكلمـات السـر. تتـم قـراءة المعلومـات المخزنـة فـي ملـف تعريـف الارتباط من قبل خادم الويب فيكل مرة سيرفر الويب يزور الموقـع. والغـرض مـن ذلك هو حفظ للمستخدم النهائي عناء الحاجة إلى إدخال المعلومـات فـي كـل مـرة انه أو انها تزور موقع الويب. نظريا، موقـع الـويب فقـط الـتي خلقتمعلومـات ملـف تعريف الارتباط يمكن قراءة أو تعديل تلك المعلومات. وبالإضـافة إلـى ذلـك،وليـس كل موقع ويب يستخدم ملفات تعريف الارتباط، حتى أنك لـن تحصـل علـى الكويـك بالدليل PCتلقائيا عند زيارة الموقع . يبين مختلف الكوكيز المخزنة على القرص ال في دليل الكوكيز. في هذه الحالة تم تخزين الملفات عن طريق WINDOWS تحت وأصـول كـثير منهـم مـن السـهل تخمينهـا بأسـمائها. وهنـاك آخـرون أكـثر .IE5 غموضـــا. لقـــد ســـلط الضـــوء علـــى الكويـــك التييصـــدرها موقـــع الـــويب Amazon.com هذه الكويك يستخدم لمصادقة هويتي إلـى خـادم .Amazon.com خلال كل زيارة إلى موقعها على شبكة الانترنت.



الشكل 17.1: IE5 cookie files

وقـد اسـتخدمت ملفـات تعريـف Amazon.com على سبيل المثال، في الماضـي الارتباط لتحديد عودة الزوار إلى موقعه على الانترنت. أساسا، كان الغرض من هذه االكويك لتحديد زبون دون الحاجة إلى إدخال المعلومات. لـو كنـت زائـرا لأول مـرة فـإن صـفحة عـرض "مرحبـا! مـن جديـد ل Amazon.com، إلـى موقـع ويـب Amazon.comولكن إذا كنت أحد العملاءالعائدين إلى موقـع أمـازون يمكـن أن؟" تحــدد لــك. علــى ســبيل المثــال، لــو ان زبــون، ود أن يكتــب ببســاطة URL قائلا "مرحبا، جـون Amazon.com تفتح الصفحة الرئيسية www.amazon.com كانافان". وكان الموقع قادرا على التعرف علي منالمعلومات المخزنة في ملـف E. تعريـف الارتبـاط علـى محـرك الأقراصـلدي فـي ذلـك الـوقت الـذي دخلـت الـى إذا كان لي أن حذف ملفات تعريف الارتباط، فإن موقع ويب .Amazon.comموقع يعاملنيكزائر لأول مرة. تمنيت لتقديم أمثلـة مـن صـفحات الـويب Amazon.com لا تسمح لي أن استخدام صور Amazon.com في العمل، ولكن Amazon.com من صفحات الويب الخاصة بهـم. الشـكل 17.2 يـدل علـى محتـوى الملـف الملـف لدي. هذا هو الملف الـذي يتـم PC التي تتواجد على محرك القرص Cookies.txt إنشاؤه بواسطة المستكشفنتسكيب. مخازن برامج الملاحـة لجميـع ملفـات تعريـف الارتباط تكون في ملف واحد. وعند النظرإلى الشـكل 17.2 يمكنـك رؤيـة المواقـع التي زرتها باستخدام المستكشف تشمل نيويورك تايمز، انقر نقـرا مزدوجـا، ويـاهو، ونتسكيب. فإن المعلومات الأخرى المخزنة في ملفات تعريف الارتباط تختلـف مـن موقع إلى آخر.



الشكل 17.2: ملف cookie.txt المستكشف

فائدة ملفات الكوكيز لمتصفحي الويب هي مشكوك فيها في أحسن الأحوال. وقد وضعت ملفات تعريف الارتباط لأغراض التسويق وتتبع. حتى لهذا الغرض قيمتها مشكوك فيها لأنه يمكن للمستخدمين النهائيين الوصول، وتغير أو حذف أو حجب معلومات ملف تعريف الارتباط. ومع ذلك، فإن متوسط سيرفر الويب ليست على علم بوجود ملفات تعريف الارتباط ولا من القدرة على التلاعبها. المخاطر المرتبطة ملفات تعريف الارتباط واضحة. ملفات تعريف الارتباط يمكن أن تكون غزو لخصوصيةالمرء. أنها في الأساس ترك الناس يعرفون أين كنت على الويب. إذا كان شخص غير قادرا على الوصول إلى جهاز الكمبيوتر الخاص بك يمكن من عرض ملفات تعريف الارتباط. إذا كنت قد زرت موقع ويب بلاي بوي واذا كان يصدر ثم سوف تظهر بشكل playboy.com ،(!الكوكيز (أنا حقا لا أعرف. بكل صدق واضح في ملفات تعريف الارتباط الخاصة بك. أعتقد أنك يمكن أن نقول دائما أن قمت بزيارة الموقع لقراءة المقالات. حقيقة أن ملفات تعريف الارتباط تكشف هذا النوع من المعلومات يمكن أن ينظر إليه باعتباره أمرا جيدا أو سيئا. يمكن للوالدين استخدام الكوكيز لضمان أن الأطفال لا يمكنهم الوصول إلى مواقع غير مناسبة،ويمكن للشركات استخدامها للتحقق من انتهاكات السياسة. ومع ذلك، في كلتا الحالتين سيكون أكثر فعالية بكثير لوضع تدابير وقائية في مكان بدلا من تحقق بعد وقوعها. بالإضافة إلى المخاطر المرتبطة مع شخص وجود إمكانية الوصول المباشر إلى جهاز الكمبيوتر الخاص بك هناك مخاطر من مواقع الويب الخبيثة.

ذكرت في وقت سابق أن موقع ويب "نظريا" فقط التي أنشات أو إصدرت الكويك أن يكون قادر على الوصول إليه. ومع ذلك، فإن الواقع هو أن من وقت لآخر، تم العثور على نقاط الضعف في المستكشف وإنترنت إكسبلورر تسمح لمواقع ويب الخبيثة لقراءة، أو تغيير، وحذف ملفات تعريف الارتباط الصادرة عن مواقع ويب أخرى. ونتيجة لذلك، فإنه أمر خطير جدا لمواقع الويب لتخزين المعلومات الحساسة في ملفات تعريف الارتباط. تخيل المخاطر المرتبطة مع خادم الويب

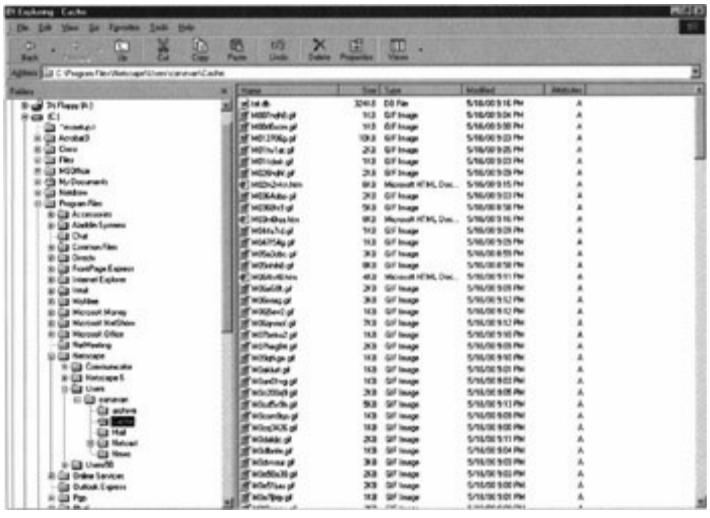
يستخدم الكوكيز لتخزين معلومات بطاقة الائتمان للمعاملات على الخط الفوري. عدة خدمات بريد الإلكتروني على شبكة الإنترنت المجانية تستخدم الكوكيز لمنح الصلاحيات. ونتيجة لذلك، المشغل من موقع ويب ضار لديه القدرة على الوصول إلى الكوكي، وتحديد مزود خدمة البريد الإلكتروني، وسرقة كلمة السر، والوصول إلى حساب البريد الإلكتروني. على أقل تقدير، يستطيع شخص ما قادرا على تحديد صاحب الكويك عن طريق زيارة موقع الويب إصداره. بالعودة إلى مثال إذا كان موقع للقراصنة الوصول إلى الكوكي صدر لي عن طريق Amazon.com، الأمازون، وأنها يمكن أن تذهب إلى الموقع أخذ اسمي.

وهناك أيضا المخاطر المرتبطة باستخدام موقع يسمح ببساطة خيار استخدام ملفات تعريف الارتباط للمصادقة. أنا أعرف واحد على الأقل خدمة تداول الأسهم عبر الإنترنت الذي يتيح للعملاء خيار استخدام الكوكيز كجزء من التوثيق. لقد رأيت بنفسي مثل ذلك حيث ذهب المستخدم النهائي إلى موقع تجاري لظهرأسم شخص آخر ومعلومات الحساب. فمن الممكن تماما أن الشخص الذي تم عرض معلوماته خطأ فعل الشيء الصحيح ولم يتمكين من خيار ملفات تعريف الارتباط، ولكن موقع ويب تجاري قرأ بعض المعلومات في ملفات تعريف الارتباط للمستخدم النهائي التي تسببت في التحديد الغير صحيح. يمكن للمرء أن نعتقد أنه أو أنها محمية من خلال عدم استخدام الكوكيز فقط للعثور على سوء التصميم من تطبيق خادم الويب والتحايل على جميع الاحتياطات. في هذه الحالة، فإن أفضل حماية ليست لمواقع الويب المتكررة التي تستخدم الكوكيز للمصادقة. هناك العديد من الخيارات المتاحة للمستخدمين النهائيين للسيطرة على ملفات تعريف الارتباط.

أولا، يمكن للمستخدمين النهائيين تكوين المتصفح الخاص بهم ليطالبك قبل تحميل ملف تعريف الارتباط. وهذا يعطي المستخدمين النهائيين الفرصة لقبول أو رفض ملفات تعريف الارتباط اعتمادا علىالموقع. ويمكن أيضا تعطيل الكوكيز تماما، بحيث متصفحك ينفي كل ملفات تعريفالارتباط. ويمكن القيام بذلك مع المستكشف تحت يمكن العثور عليها ضمن أدوات / خيارات IE5اتحرير / تفضيلات والمتقدم. ل الإنترنت ثم النقر على علامة التبويب أمان لمستوى مخصص. تعطيل الكوكيز يمكن أن يسبب مشاكل تماما، لأن بعض المواقع تتطلب الكوكيز لتمكين الوصول إلى الموقع. وللأسف، فإن المستخدمين النهائيين يستلمون رسالة خطأ لا تقول لهم تحديدا أنها تحتاج إلى تمكين ملفات تعريف الارتباط. وهي عادة ما تكون بعض الرسائل لاتوصف حول المتصفح لا يتم دعمها. وثم خيار آخر للنظر في حماية نفسك ضد هذا النوع من التهديد هو تعطيل أو المطالبة جافا، جافا سكريبت، و مرة أخرى، هذا على الأقل تعطيك خيار قبول أو رفض على أساس ActiveX. مستوى من الراحة مع الموقع الذي تقوم بزيارته. نضعفي اعتبارنا، بيد أنه إذا قمت بتكوين متصفحك ليطالبك قبل قبول ملفات تعريف الارتباط، جافا، جافا سكريبت، و سيتم مطالبتك باستمرار. وهناك أيضا عدد من المرافق التي ActiveX، يمكناستخدامها لرصد ومراقبة الكوكيز. برامج مثل كوكي بال، كوكي جرة، كوكي الشرطي، الإنترنت الحرس الكلب مكافي، ونورتون إنترنت سيكيوريتي يمكن لجميع العاملين للتحكم في ملفات تعريف الارتباط.

ملفات ذاكرة التخزين المؤقت:

ملفات تعريف الارتباط ليست هي فقط الملفات التي تم إنشاؤها على محرك الأقراص من جهاز الكمبيوتر سيرفر ويب عند زيارة موقع ويب. كلا من المستكشف نتسكيب ومايكروسوفت إنترنت إكسبلوررأيضا يعتمدعلى ملفات "مخبأ" أو مخزنه و التي تم مؤخرا الوصول إليها فيمواقع الويب. ويشار إلى ذلك بالتخزين المؤقت، ويشار إلى الملفات المخزنة على القرص جهاز كمبيوتر كملفات ذاكرة التخزين المؤقت. ميزة التخزين المؤقت من تأتي عند إعادة تحميلصفحات ويب التي تم مؤخرا عرضها. المتصفح قادر على تحميل صفحة من ملفات التخزين المؤقت على محرك الأقراص المحلي بدلا من الاضطرار إلى إعادة تحميله من الخادم. تحميل الملفات من محرك الأقراص المحلي هو أسرع بكثير من تحميلها عبر الشبكة من والرسم أو ملفات HTML الخادم. ويمكن أن تشمل الملفات المخزنة مؤقتا ملفات وملفات نصية. المخاطر المرتبطة بالملفات ،JPGSالصور مثل صور متحركة و المخزنة مؤقتا مماثلة لتلك التي ترتبط مع ملفات تعريف الارتباط. في الأساس، فإنها تخبر أحدا اين انت. ومع ذلك، عرض ملفات ذاكرة التخزين المؤقت تستطيع أن تخبر الشخص اين هو عند التصفح، وكذلك يمكن أن تسمح في الواقع لهم إلى جانب الرسم HTML لعرض الملفات التي تم تصفحها، حيث يتم مؤقتا ملفات أو الصورة الملفات المرتبطة بهاعلى القرص الصلب الخاص بك عند تصفح معظم صفحات ويب. الشكل 17.3 مثال على الملفات المخزنة مؤقتا على القرصلدي من قبل المستكشف نتسكيب. يتم التخزين المؤقت للملفات في دليل فرعي يسمى على مسمى ذاكرة التخزين المؤقتولها أسماء ولا توصف، ولكن ملحقات تحديد أنواع الملفات، Internet. وينظر الى الملفات بسهولة بمجرد النقر عليها يخزن ملفات ذاكرة التخزين IE أيضا تخزين مؤقتللملفات، ولكن. Explorer المؤقت تحت دليل ملفات إنترنت مؤقتة ، وهو دليل فرعي من دليل Windows.

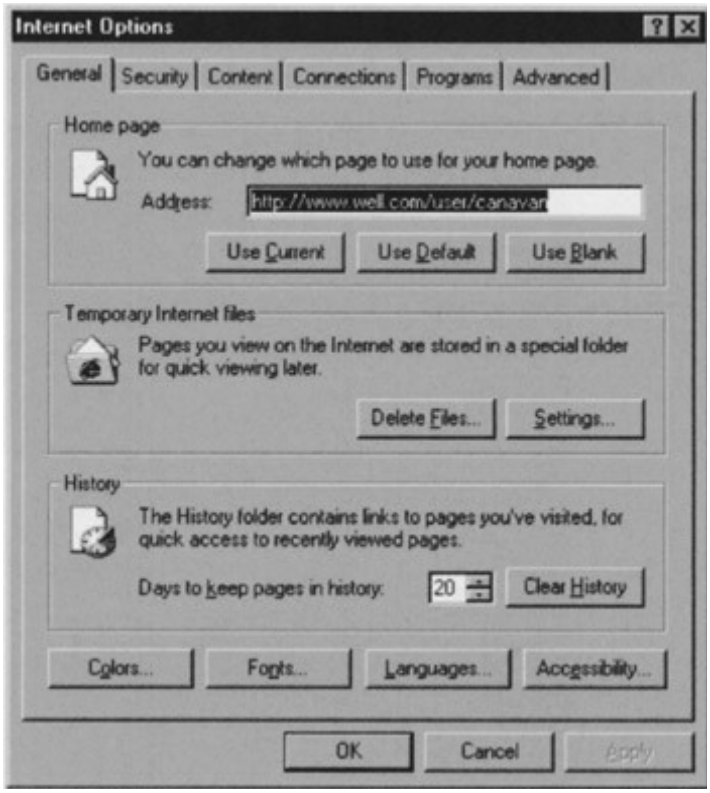


الشكل 17.3: ملفات ذاكرة التخزين المؤقت IE5.

حقيقة أن المتصفحات تخبأ صفحات عرضها على الإنترنت يجب أن نتذكر عند استخدامالإنترنت للوصول إلى البنك و حسابات الوساطة للمعاملات المالية. على سبيل المثال، كل الصفحات ينظر عند استخدام نظام الخدمات المصرفية عبر الإنترنت يتم تخزينها في الملفات المخزنة مؤقتا في الكمبيوتر الشخصي.

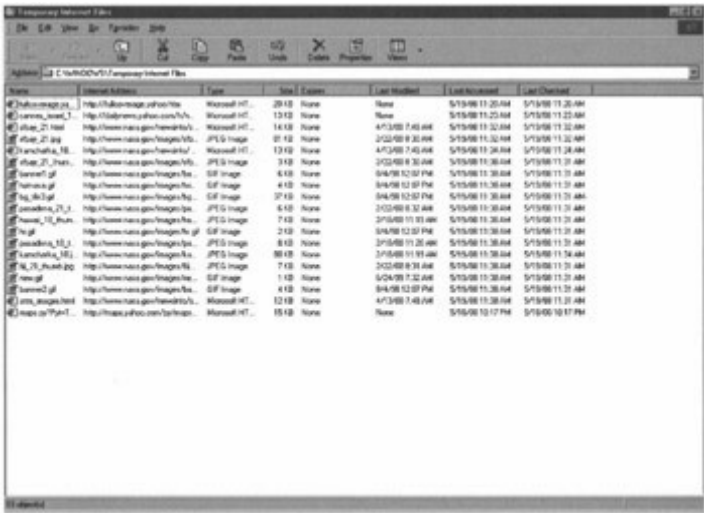
ويمكن أن تشمل تلك الملفات المخبأه أرقام الحسابات والارصده. إذا كنت تستخدم نظام الخدمات المصرفية عبر الإنترنت الخاص بك على جهاز الكمبيوتر التي يتم مشاركتها من قبل الآخرين، يكون من مكان عمله، ثم أي شخص لديه الوصول الفعلي إلى أن جهاز الكمبيوتر يمكن أن يحتمل عرض معلومات بشأن للوصول إلى الدليلحيث توجد الملفات Windows حساباتك.باستخدام مستكشف التي يمكن استرداد الملفات ذاكرة التخزين المؤقت. وبالإضافة إلى ذلك،يوفر إنترنت إكسبلورر القدرة على عرض الملفات المخزنة مؤقتا. ضمن أدوات / خيارات إنترنت ضمن علامة التبويب عامسوف تجد ملفات إنترنت المؤقتة. هناك نوعان من الأزرار: واحد هو حذف الملفات والآخر هو الإعدادات.

ويصور هذا في الشكل 17.4. إذا نقرت على إعدادات، هناك خيار لعرض الملفات.



الشكل 17.4: IE5 خيارات الإنترنت

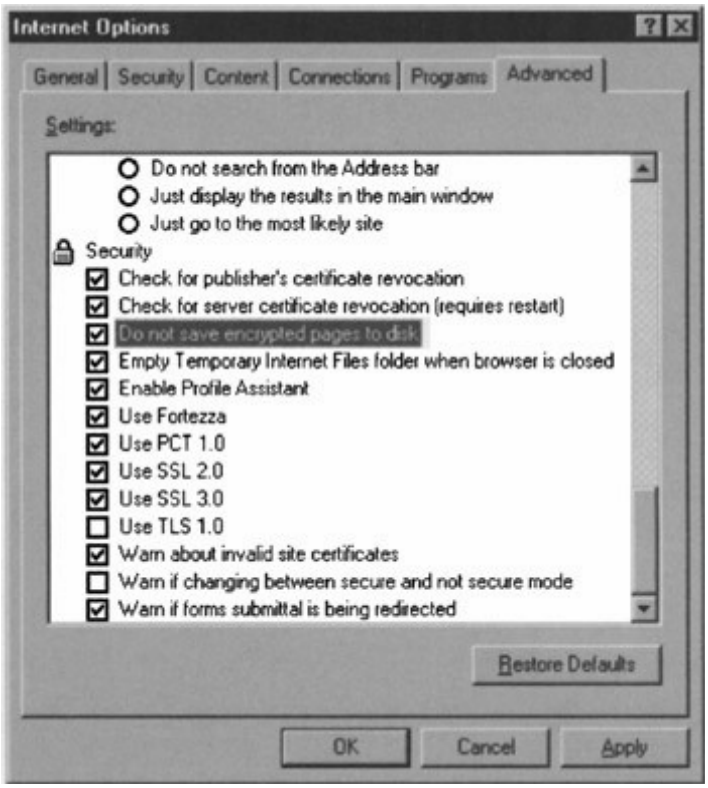
الشكل 17.5 يدل علي ملفات ذاكرة التخزين المؤقت إنترنت إكسبلورر الموجــودة لدي. فإنه يـدل علـى أنـواع الملفـات وموقـع مـن الـتي PCعلى محرك الأقراص لل والملفات من ياهو وكالة ناسا JPG، GIF، نشأت الشكل 17.5يظهر أتش تي أم أل الويب



الشكل 17.5: ملفات التخزين المؤقت.

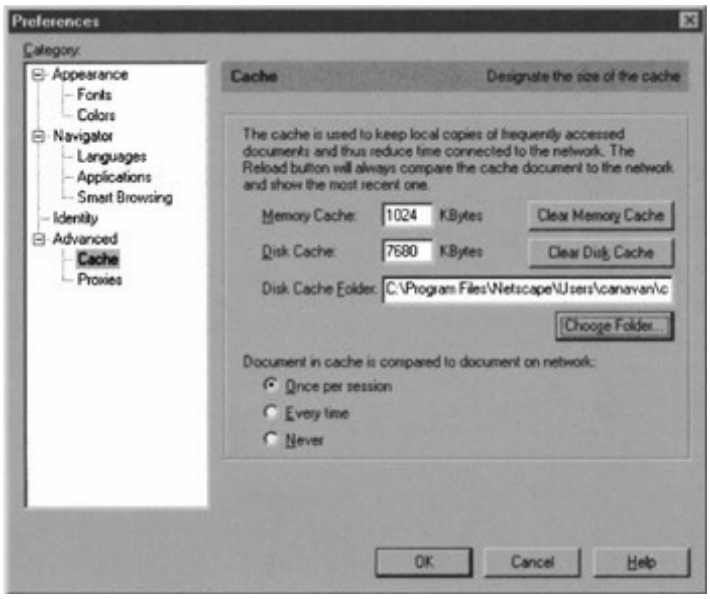
وبالإضافة إلى خطر من الأفراد مع الوصول الفعلي إلى جهاز الكمبيوتر الخـاص بـك أن تكون قادرة على استرداد المعلومات من ملفات ذاكرة التخزين المؤقت الخاصة بك، وهناك أيضا من خطـر شخصـتفعل الشـيء نفسـه عبرالشـبكة. طريقـة واحـدة يمكن تحقيق ذلك هو إذا كنت تشارك محرك الأقراص.والآخريكـون مـن خلال نقـاط الضعف الـتي لـديها مـن وقـت لآخـر تـم تحديـدها مـع كـل مـن برنـامجي المتصـفح والمستكشف. ويشمل هذه ضعف ذاكرة التخزين المؤقت-البقرة، والتي أثـرت فـي والمستكشـف الـذي IE نتسكيب 4.05، والضعف المكتشفة في الآونة الأخيرة لكلا ينطوي على استخدام الكوكيز لتشغيل جافا سـكريبت الـتي يمكـن انـتزاع الملفـات هذه الأنواع مـن نقـاط الضـعف قـد .HTML ذاكرة التخزين المؤقت وحتى العلامات يسمح موقع ويـب ضـار لانـتزاع أو عـرض المعلومـات فـي ملفـات ذاكـرة التخزيـن المؤقت الموجودة على محرك الأقراص جهاز الكمبيوتر الخاص بـك. عنـد اسـتخدام يمكنك التخفيف من خطر تعريـض المعلومـات السـرية فـي Internet Explorer ملفات ذاكرة التخزين المـؤقت عـن طريـق تكـوين متصـفحلا إلـى ذاكـرة التخزيـن ثم HTTPS مع SSL المؤقت صفحات آمنة. وبعبارة أخرى، إذا كان يستخدم صفحة المتصفح لنذاكرة التخزين المـؤقت الملفـات إلـى محـرك الأقـراص فـي الكمـبيوتر الشخصي. ويتم إنجاز ذلك عن طريق الذهاب إلى أدوات / خيارات الإنـترنت والنقـر على التبويب خيارات متقدمة. ثم الانتقال لأسفل حتى تجد "عـدم حفـظ الصـفحات مـن SSL المشفرة إلى القرص" وانقر على مربع بجوار الخيار. وهذا يمنع صفحات

يتم التخزين المؤقت على القرص الصلب الخاص بـك. الشـكل 17.6 يظهـر شاشـة الخيارات الإنترنت باستخدام الخيار المناسب تسليط الضوء.



الشكل 17.6: IE5 خيارات الإنترنت.

Navigator وثمة خيار آخر هو ببساطة حذف الملفات المخزنة مؤقتا قبل أن تخرج أو الإنترنتالمتصـفح. الإنـترنت إكسـبلورر يمكـن القيـام بـذلك فـي إطـار الخيـار الإنترنت. مع الإشارة إلـالرقم 17.4 يمكنـك أن تـرى أن هنـاك زر حـذف الملفـات تحت القسم ملفات إنترنت المؤقتة. بمجرد النقر على هذا الزر حذف كافة الملفات المخزنة مؤقتا. مع نتسكيب يتم حذف ملفات ذاكـرة التخزيـن المـؤقت عـن طريـق الـذهاب إلـى تحريـر / تفضـيلات والنقـر علـى زر التخزيـن المـؤقت علـى القـرص واضح. وصفت هذه الشاشة في الشكل 17.7.



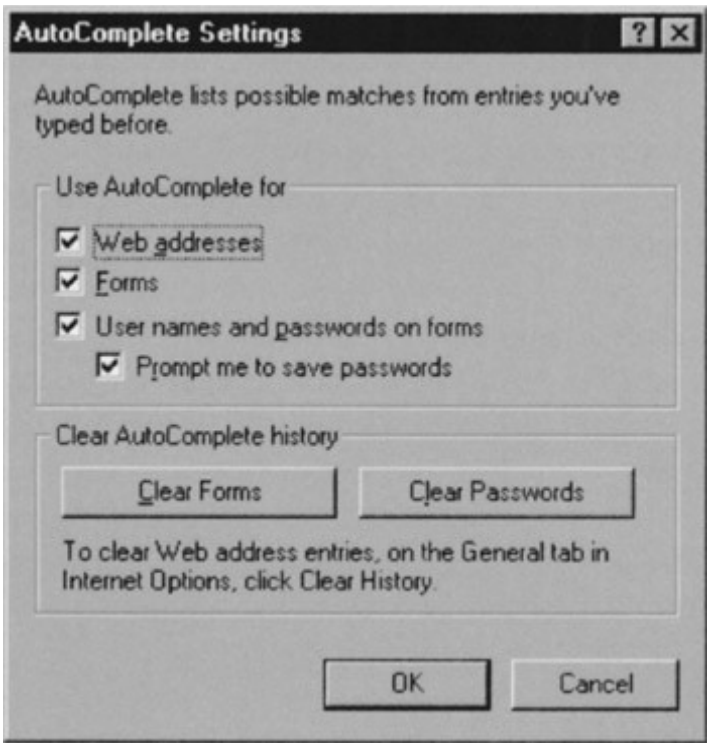
الشكل 17.7: تفضيلات IE5.

مع إنترنت إكسبلورر، لديك أيضا خيار تكوين المتصفح لحذف مخبأملف تلقائيا عند الخروج من البرنامج. مشيرا إلى الشكل 17.6، خيار مباشرة تحت عنوان "عدم حفظ الصفحات المشفرة إلى القرص" هو خيار "حذف مجلد ملفاتإنترنت المؤقتة سيتم حذف ملفات التخزين IE عند إغلاق المتصفح." عن طريق فحص هذا الخيار المؤقت على القرص الصلب أثناء جلسة عمل المتصفح في وقت انتهاء الجلسة.معظم الضعف المرتبطة بالاستيلاء أو عرض المعلومات المخزنة مؤقتا عبر الشبكة ينطوي جافا سكريبت، يجب عليك أن تنظر تعطيل وظيفة. ومع ذلك، العديد من مواقع ويب ذات السمعة الطيبة تستخدم جافا سكريبت لأغراض مشروعة، حتى لا يكون هناك علاقة تبادلية مع هذا الخيار.

الإكمال التلقائي:

في بيئة حيث قد يكون جهاز Internet Explorer 5.0 قلق آخر مع استخدام كمبيوتر تقاسمها مع أو استخدامها من قبل الآخرين هو خيار الإكمال التلقائي. خيار الإكمال التلقائي يمكن العثور تحت أدوات / خيارات الإنترنت من خلال النقر على علامة التبويب المحتوى.

الشكل 17.8 يوضح مربع إعدادات الإكمال التلقائي. القلق هنا هو الخيار "أسماء المستخدمين وكلمات المرور في النماذج." إذا تم اختيار هذا المربع، سوف IE5 تخزين توقيع على معلومات الحساب لتلك المواقع التي تتطلب مصادقة، الوساطة المالية. المخاطر المرتبطة مع هذا واضح.



الإكمال التلقائي IE5 الشكل 17.8: إعدادات

الشكل 17.9 يوضح كيفوظائف الإكمال التلقائي. على سبيل المثال تستخدم مرة وهمية. ف Any bank أخرى في نظام الخدمات المصرفية عبر الإنترنت من شركة إلى الإكمال التلقائي أسماء المستخدمين وكلمات IE5 ي الشكل 17.9، تم تكوين السر. وبالإضافة إلى ذلك، وأنا قد قمت بتسجيل بالفعل في النظام المصرفي على IE5 الانترنت باستخدام اثنين من أرقام الحسابات المختلفة، و إيقاف وإعادة فتح لإثبات آثار الإكمال التلقائي. عندما كنت مسجلا في أي نظام الخدمات المصرفية معلومات الحساب. خلال محاولات لاحقة لتسجيل IE5 عبر الإنترنت البنك، سجل الدخول إلى نظام الخدمات المصرفية عبر الإنترنت أحتاج أدخل الرقم الأول من عرض رقم الحساب بأكمله لجميع الحسابات بدءا IE5 الحساب فقط، وسوف يقوم من الرقم المدخل.

الشكل 17.9: مثال الإكمال التلقائي.

في الشكل 17.9عند إدخال رقم 5 في حقل رقم الحساب تظهر قائمة منسدلة بعرض اثنين من أرقام الحسابات 55000037390، 59001260504. وهذه هي أرقام الحسابات اللذين سبق لي أن استخدمتها للدخول إلى نظام الخدمات المصرفية عبر انترنت البنك.ال IE5 تخزن فيها أرقام الحسابات وكلمات المرور بهذه الطريقة، يحتاج IE5 لأنترنت أي بنك. عندما يتم تكوين URL وضمها إلى المستخدم النهائي تسليط الضوء فقط على رقم الحساب، ويتم إدخال كلمة المرور تلقائيا. من الواضح، يجب أن لا يتم تمكين الإكمال التلقائي لأسماء المستخدمين وكلمات السر. هذا ينطبق بشكل خاص عند العمل في بيئة حيث قد تكون مشتركة أجهزة الكمبيوتر. وأوصى أيضا ضد استخدام وظيفة الإكمال التلقائي على جهاز كمبيوتر محمول. إذا فقد أو سرق الكمبيوتر المحمول، يمكن استخدامها للوصول إلى حسابات على الخط الفوري. إذا الإكمال التلقائي لأسماء المستخدمين وكلمات المرور يتم التمكين ثم الوصول إلى حسابات يمكن الحصول عليها بسهولة. عندما أولا وجدنا أن الإكمال التلقائي تم تمكينه افتراضيا. وأعتقد أن الذي تغير IE5 صدر منذ ذلك الحين.

النص الاصلي

SL