سياسات الأمن Security Policies

مقدمــة

المعلومات من أهم الموجودات النفيسة في أي مشروع . لذا فإن هناك حاجة لحمايتها و التأكد من خصوصيتها confidentiality و تكاملها integrity و توفرها availability . أهم عوامل الحفاظ على أمن المعلومات هو وضع السياسات و الإجراءات لكيفية حماية المعلومات[1].

الغرض من أمن المعلومات هو التأكد من استمرارية العمل و تقليل الأذى والضرر الذي قد يلحق بالنظام , و ذلك بمنع أو تقليل أثر الحوادث التي يتعرض لها النظام . إدارة أمن المعلومات توفر مشاركة المعلومات و التأكد من حمايتها و الموجودات الحاسوبية الأخرى[2].

تواجه المنظمات مخاطر أمنية من مصادر كثيرة معدة للهجوم مثل فيروسات الحاسبviruses , الاختراق hacking و هجوم رفض(تعطيل) الخدمة Denial of service . أمن المعلومات بالمعنى التقني ليس كافياً ويحتاج إلى أن يدعّم بالسياسات و الإجراءات.

سياسات الأمن هي الأساس لأمن المعلومات في أي منظمة. فالسياسة المكتوبة و المنفذة بشكل جيد تحتوي معلومات كافية لما يجب عمله لحماية المعلومات و العاملين في المنظمة. سياسات الأمن كذلك تؤسس قواعد استخدام الحاسب للموظفين فيما يتعلق بمهامهم الفعلية.

يجب أن يقر مدير النظام و صاحب(مالك) المنشأة بحقيقة وجود المخاطر الأمنية و كيفية تجنبها . فتنفيذ السيطرة و المراقبة تتطلب خطة محكمة بالإضافة إلى تفاعل جميع موظفي المنظمة, و الذي بدوره سيؤدي إلى نجاح إدارة أمن المعلومات. إن الهدف من صياغة سياسات الأمن و تنفيذها هو تحسين توافر المعلومات availability و تكاملها integrity و خصوصيتها confidentiality كذلك , من داخل و خارج المنظمة[1].

ما هي سياســة الأمن ؟

هي مجموعة قوانين أمنية تسيطر على نظام المعلومات و تزوده بمستوى حماية موثوق به. و هذه السياسات يجب أن تُوجه الإدارة و سبل الحماية والمصادر المرتبطة بالمعلومات و بنظام المعلومات. إن مستوى قسوة تلك السياسات عادة مرتبط بمستوى المخاطر المراد تجنبها[3].

على وجه العموم, سياسة الأمن هي الخطة التي تعرّف الاستخدام المقبول أو المرضي لجميع الوسائط الالكترونية في المنظمة. هناك عناصر أساسية يجب أخذها بالاعتبار عند تنظيم و تطوير سياسات الأمن, ما هي البيانات التي تحتاج للحماية؟ و لماذا؟ , ما هي الآثار السلبية المترتبة على فقد أو تلف شيء من الممتلكات في حالة خرق النظام ؟ , وهذا يشمل التحليل النهائي لنسبة حدوث هذه الحوادث سنوياً . استناداً لهذا التحليل,سيتبين هل هذه السياسة ضرورية و مبررة اقتصادياً أم لا؟. و عند تبرير هذه السياسات, هل من الواضح من المسئول عن ماذا؟. عند التنفيذ , هل تثبت فاعليتها؟ . وهكذا, لكل سياسة يراد لها النجاح خلال فترة من الزمن يجب أن يتم اختيار أشخاص متمرسين و عرضة للمحاسبة بالإضافة إلى استخدام نفوذ سلطة المنظمة لتطبيق هذه السياسة[4].

لماذا نحتاج السياسة الأمنية ؟

نحتاج سياسة الأمن لاطلاع المستخدمين على مسئولياتهم لحماية تقنية المنظمة و المعلومات الحساسة.

السياسات الموثقة و المدروسة بشكل جيد ضرورية لتنظيم أعمال منظمة تقنية المعلومات الناجحة. بدون تعيين السياسات ,و المعايير و الإجراءات الناتجة عنها, فإنه سيكون من الصعب جداً إدارة و توجيه منظمة تقنية المعلومات. هذه السياسات كذلك يجب أن تستند إلى تحليل كامل للمخاطر. من الواجب حماية الأنظمة الحساسة, إلا أن هذا لا يعني أن ندفع 100$ دولار لحماية أصلٍ قيمته 5$ دولارات. تحليل المخاطر سيؤدي إلى السياسات, و المعايير, والإجراءات المناسبة[5].

سياسة الأمن تخدم وظائف متعددة, فهي عبارة عن مستند مركزي يصف بالتفصيل النشاط المقبول للشبكة و عقوبات إساءة الاستخدام . كذلك سياسة الأمن توفر تعريف و توضيح أهداف الأمن للمنظمة ككل. سياسة الأمن الناجحة توضح لكل موظف مسئوليته للحفاظ على البيئة الآمنة[6].

تكمن أهمية سياسة الأمن في أنها الأساس لبرامج الأمن. بدون هذه السياسات, برنامج أمن المنظمة سيكون عمره قصير. سياسات الأمن تخبر الموظفين بالقواعد المهمة لحماية ممتلكات و معلومات الشركة . السياسات المكتوبة بشكل جيد توفر قواعد الاستخدام المرضي و الغير مرضي , و الذي تلقائياً يقلل المخاطر إذا التزم الموظفون هذه السياسات. تخدم سياسات الأمن كذلك كأساس جيد لحساب سلوك الشبكة و مصادرها[4].

أحد الطرق لإعداد سياسات و إجراءات الأمن تتبع الخطوات التالية[1]:

- تحديد جميع الممتلكات المطلوب حمايتها.
- تحديد جميع الثغرات و المخاطر .

- تقرير أي المعايير التي يمكنها حماية الممتلكات .
- نقل النتائج و الاكتشافات إلى الأقسام المعنية.
- مراقبة و مراجعة العملية باستمرار من أجل التطوير.

قبل البدء بسياسات الأمن Security Policies pre-Work

لتطوير مشروع واسع لسياسات الأمن , نحتاج لفهم شامل للمنظمة. يجب مراعاة أهداف و توجهات المنظمة. السياسة التي نريد تطويرها يجب أن تتكيف و تتطابق مع السياسات و القواعد و الأنظمة و القوانين الموجودة التي تتبعها المنظمة.

كبداية, نحتاج إلى شخص ذو منزلة معتبرة لتبني و تنفيذ السياسات بتحديد مسئول عن أمن المعلومات على مدار الساعة مع من ينوبه في هذه المهمة. فالحصول على أشخاص مناسبين من البداية أمر هام لنجاح المشروع و قبول السياسات لدى الجميع, و هو عبارة عن جهد مشترك بين التقنيين و مالك المنشأة و متخذي القرار الذين لديهم السلطة لتطبيق السياسات. مستوى السلطة الصحيح في تقرير السياسات يتطلب التأكد من جودة صياغتها و دعمها حتى يمتد تأثيرها ليشمل جميع موظفي المنشأة[1].

بنية السياسات Policies Structure

جميع سياسات تقنية المعلومات يجب أن تبنى حول بنية معينة. هذه البنية هرمية, تتدرج من هدف عالي المستوى نزولاً إلى إجراءات محددة جداً. بالرغم من عدم وجود إجماع كامل على المصطلحات في مجال أمن المعلومات, فإن أحد البنى الهرمية الشائعة المقبولة هي:

معاهدة Charter

سياسةPolicy

معاييرStandards

إجراءاتProcedures

السياسة تعرّف فلسفة(مفاهيم و معتقدات) عالية المستوى لأمن معلومات المنظمة على المستوى المحلي. السياسات هي موجز تقني يعتمد على الوثائق. مع ذلك , فإن السياسات توفر السلطة الضرورية لتأسيس و تطبيق التقنية و المعايير. عموماً, تبقى السياسات مناسبة و قابلة للتطبيق لفترة من الوقت, ثم تحتاج إلى إعادة النظر و التنقيح إذا تغيرت أسس و قواعد عمل المنظمة أو البيئة و الأهداف العملية[5] .

السياسات يفترض أن[7]:

- تحدد و تُعرف مجالات و جهات الخطورة .
- ترسم خطة لمواجهة الخطر.
- توفر الأساس للتأكد من امتثال هذه السياسات.
- تكون قابلة للتطبيق و نافذة المفعول .
- تكون موجزة و سهلة الفهم .
- تحقق التوازن بين الحماية و الإنتاجية.

تجميع المعلومات Information Gathering[1]

نبدأ تحديد جميع الممتلكات التي نسعى لحمايتها, و المخاطر المحتملة, و جوانب الضعف والثغرات لدينا.

1- تحديد الممتلكات Identify Assets: تبدأ بتحديد جميع العمليات الحساسة في المنظمة, ثم إنشاء قائمة بالممتلكات المستخدمة في هذه العمليات الحساسة.هذه القائمة تشمل الممتلكات الحسية كذلك مثل الخوادم Servers, الموجهات Routers, و معلومات خدمات الشبكة ...الخ. بعد ذلك ,يتم تقييم أهمية هذه الممتلكات بوضع قيمة لكل منها للمساعدة في ترتيبها حسب الأهمية. المثال التالي يوضح مجموعة من الممتلكات و قيمة كلٍ منها :

Web server	$10,000
Database	$100,000
Mail server	$10,000

2- تحديد الثغرات و المخاطر Identify Vulnerabilities and Threats: تحليل جميع العمليات بدقة لتحديد الثغرات و المخاطر, مع الأخذ بالاعتبار احتمال أن يكون أي من الثغرات قد تم

استغلالها. هناك العديد من الأدوات و الوسائل التي تساعد في تحليل النظام و إيجاد الثغرات الممكن استغلالها في النظام. بجانب المخاطر الإلكترونية, هناك مخاطر مادية مثل سرقة وسائط التخزين. القائمة التالية توضح بعض المخاطر المحتملة مع نسبة احتمال حدوثها:

Unauthorized user modifying the database تعديل قاعدة البيانات من قبل مستخدم غير مصرح له	30%
Denial-of-service on the Web server رفض الخدمة في خادم الشبكة	80%
فيروسات Virus	90%

3- تقييم المعايير و آليات التحكم Evaluation of Measures and Controls : يتم ذلك بالنظر إلى المخاطر و التشاور حول سبل الوقاية و آليات التحكم بالإضافة إلى تكلفة كل منها . كذلك تدوين نسبة انخفاض الخطر بعد تطبيق الإجراء الوقائي و آليات التحكم . الجدول التالي يوضح بعض الأمثلة :

الخطر Threat	آليات التحكم الممكنة Possible Controls	التكلفة Cost	نسبة انخفاض الخطر Risk Reduction
مستخدم غير مصرح له يقوم بتعديل قاعدة البيانات Unauthorized user modifying the database	آليات قوية و قاسية للدخول Strong access controls	$25000	%80
رفض الخدمة في الخادم Denial-of-service on the Web server	الجدر النارية Firewalls	$10000	%60
فيروسات Viruses	E-mail anti-virus	$5000	%70
	Client anti-virus	$10000	%80
	Strong policies on E-mail attachment	$500	%60

بعد ذلك , نحلل قائمة خيارات التحكم لكل خطر مع الأخذ بالاعتبار التكلفة و نسبة انخفاض الخطر و احتمالية حدوث الخطر وقيمة الممتلكات. ثم نقرر أي من آليات التحكم هو الأفضل للتطبيق بالنسبة لكل خطر , أو ربما لا يكون هناك أي خيار على الإطلاق (إذا كانت تكلفة تطبيق هذه الآلية كبيرة جداً مقارنة باحتمال حدوث الخطر).

أخيراً , وثّق عملية التقدير و النتائج , مع مراعاة أن يكون التوثيق جيداً لأن ذلك سيجعل الرجوع إليها سهلاً في المستقبل[1].

تحديد الأدوار والمسئوليات Define Roles and Responsibilities

من المفترض تحديد الأدوار في المنظمة ليتم تجميع الموظفين بناءً على أعمالهم الوظيفية. هذه الأدوار تشمل الموارد البشرية و الحسابات و التسويق و التطوير و مراقبة الجودة و دعم النظام والمتعهدون (المقاولون) ...الخ. كل مجموعة تحتاج مستوى صلاحيات دخول مختلفة للدخول للموارد لإنجاز مهامها الوظيفية . لا بد من تحديد من يستطيع الدخول و لأي شيء يدخل و ما الصلاحيات التي يحتاجها , مع الانتباه دائماً إلى الموازنة بين مستوى الحماية و الإنتاجية[1].

توصيل المرئيات Communicate Findings

يتم توصيل النتائج إلى الأقسام المعنية مع التركيز على المخاطر و الثغرات. المرئيات و التوصيات يجب أن يتم توصيلها إلى الإدارة أو مالك المشروع للتأكد من أن سياسة الأمن التي تم إنشاؤها ستطبق المعايير لحماية المنظمة بأقصى طرق الحماية الفعالة .

السياسة و الإجراءات المحسنة يجب أن تُعتمد من قبل صانعي القرار و ممثلي جميع المساهمين, مثل اتحاد الموظفين و القانون , للتأكد من أن السياسة الجديدة تطابق النظام والقانون[1].

كتابة السياسات Policies Writing[8]

سياسة الأمن ليست سوى صياغة جيدة للإستراتيجية التي تحمي و تحافظ على بقاء الشبكة و مواردها . بالحصول على سياسة ذات صياغة جيدة تغطي العناصر التالية, سيكون هناك قدرة على الاستجابة و الاستعادة من كثير من المواقف بأقصر وقت:

- تقدير المخاطر Risk Assessment
- سياسات كلمة المرور Password Policies
- المسئوليات الإدارية Administrative Responsibilities
- مسئوليات المستخدمين User Responsibilities
- سياسات البريد الالكتروني E-mail Policies
- سياسات الإنترنت Internet Policies
- الاستعادة بعد الكارثة Disaster Recovery (Backup and Restore)
- اكتشاف التطفل Intrusion Detection

بغض النظر عن كون العمل على شبكة Local Area Network (LAN) مربوطة بالإنترنت أم لا, فإن سياسة الأمن أمر ضروري . لذا فإنني سأقدم فيما يلي توضيحاً لأهمية هذه السياسة من خلال نظرة عامة للنقاط التي ذكرتها آنفاً .

1- تقدير المخاطر Risk Assessment: من المفترض أن يتم عمله قبل وضع التصميم موضع التطبيق. تقدير المخاطر سيعطي خريطة لحماية البنية التحتية للشبكة. بعمل التقديرات يمكن الإجابة على كثير من التساؤلات التي تحسّن الأمن في الشبكة. هذه التقديرات تشمل ما الذي يجب حمايته , ما المخاطر التي تواجهها الممتلكات وما مقدار التكلفة لترقية النظم و ما الذي تحتاج إضافته لمواجهة احتياجات العمل. بمعنى آخر ما مقدار التكلفة لهذه العملية.

عند عمل التقديرات يجب التذكر إلى أن المخاطر لا تأتي فقط من المخترقين Hackers و المتبجحين Crackers , بل إن هناك موظفين يقومون بأعمال تخريبية من غير قصد لا لشيء إلا لأنهم لم يتلقوا التدريب اللازم . يمكن تصنيف أنواع المخاطر بالشكل التالي :

كوارث طبيعية	من يتعمد الأذى	من لا يقصد الأذى	مكونات الحاسب
حريق / فيضان	المخترقين Hackers	موظفين غير مدربين	انقطاع التيار الكهربائي
أعاصير	المتبجحين Crackers	أشخاص غير مقتنعين بالسياسات	تلف أحد المكونات المادية
زلازل	موظفون مستائون		

من الواضح أن تقدير المخاطر تعتبر خطوة مهمة جداً لأمن الشبكة لأنها تمثل البداية لتحديد الممتلكات و ما يجب اتخاذه لضمان الحصول على الهدف من وجودها. بعد اكتمال التقديرات , لا بد من مقابلة جميع الأشخاص الذين سيتأثرون بهذه السياسة الأمنية ,وهذا لا يعني مقابلة كل شخص على حده, وإنما رؤساء الأقسام ,مثل الأبحاث و التطوير , و المالية , و هكذا. الهدف من المقابلة هو أن هؤلاء الأشخاص هم من سوف يستخدم و يشرف على الموظفين الذين يستخدمون المعلومات على الشبكة, وسيكون بمقدورهم تزويدنا بمعلومات قيمة تساعد في وضع اللبنة الأولى للسياسات . لكل قسم خصائص معينة لا بد أن تؤخذ بالاعتبار, هذا سيجعل رؤساء الأقسام يتفاعلون أكثر مع العمل خصوصاً إذا تم توضيح كل خطر و كيفية مواجهته و اعتبارهم جزء من هذا العمل المشترك[8].

2- سياسات كلمة المرور Password Policies : و تمثل جانباً مهماً جداً من جوانب سياسة الأمن . قد تمثل أضعف حاجز عند الاتصال بالشركة . من الضروري جداً أن يعي جميع مستخدمي الشبكة أهمية الاحتفاظ بسرية كلمات المرور الخاصة بهم . بعض المستخدمين يكتب كلمة المرور الخاصة به على الطاولة أو يضعها تحت لوحة المفاتيح أو يلصقها في أي مكان على شاشة الحاسب, لماذا؟ , لأنه لا توجد سياسات تحْكم استخدام كلمات المرور بحيث يكون كل مستخدم حذر تجاهها و مدرك لها. من الواضح معرفة ما سيحدث فيما لو استطاع شخص ما غير مصرح له بالدخول للشبكة , بهذا نكون قمنا بتسهيل عمل المخترق Hacker بإعطائه كلمة المرور. إذا كان لا بد من تسجيل كلمة المرور, تأكد أن السياسات تشمل طريقة للتعامل مع مثل هذه الحالة , كأن تغلف بمظروف محكم الإغلاق و تحفظ في مكان آمن . لا بد أن يتم تغطية مسئوليات المدراء و مسئوليات المستخدمين فيما يخص كلمة المرور عند وضع السياسات. أما كلمة المرور نفسها فيجب أن لا تكون واحداً مما يلي [8]:

- كلمة من القاموس (أي قاموس سواءً تقنياً أو غيره).
- اسم شخص أو اسم شيء .
- اسم مكان .
- اسم علم .
- رقم هاتف .
- كلمة مرور بنفس الأحرف (مثل aaaaaa).
- نمط سهل من الأحرف على لوحة المفاتيح (مثل qwer أو zxcv) .
- أي مما سبق مع إضافة أرقام قبلها أو بعدها .

يمكن الاستزادة فيما يخص هذا الموضوع من الموقع التالي :
http://www.mhpcc.edu/accounts/password_policy.html

3- مسئوليات المدير Administrator Responsibilities : لدى المدير الكثير من المسئوليات , و لذا فإننا سنركز على تلك التي تخص موضوعنا هذا. مما يُغفل عنه أن الكثير من نظم التشغيل Operating Systems و الموجهات Routers و المحولات Switches تأتي بحسابات مستخدمين account و كلمات مرور افتراضية , لذا يجب أن يؤخذ الحذر فور استعمالها. كإجراء أولي مناسب في هذا الصدد هو تغيير أسماء حسابات المدراء, و تعطيل أي حساب موجود مسبقاً وعدم استخدامه لاحقاً مهما كان عدد هذه الحسابات . ترك هذه الحسابات و كلمات المرور كما هي يجعل من السهل على المخترقين Hackers معرفتها و من ثم التسلل إلى الشبكة.

أحد مسئوليات المدير الأخرى و التي تحتاج إلى سياسة و خطة جيدة هي تخصيص و صيانة و حفظ كلمات المرور للمستخدمين , وهذا يختلف من منظمة لأخرى. البعض يرى أنه من الواجب معرفة كلمات المرور بل و أحياناً تخصيصها للمستخدمين, و البعض الآخر لا يريدون معرفتها و لكن يحتفظون بحق تغييرها في حالة انكشافها أو نسيانها من قبل المستخدم نفسه. هذا الأمر يجب توضيحه في سياسات الأمن, و كيف أن المدير يُعرّف المستخدم بإمكانية تغيير كلمة المرور أو فتح الحساب . تزداد صعوبة الموقف إذا كان المستخدم في مكان بعيد و لا يمكنه المجيء لإثبات الهوية, و هذا أمر يجب أخذه بالاعتبار عند وضع سياسات الأمن[8].

4- مسئوليات المستخدم User Responsibilities: أول مسئوليات المستخدم هي معرفته و فهمه لسياسات الأمن في موقعه. هذا يعني أنه لا بد أن يكون هناك برنامج تدريبي جيد في مكان العمل لتعريف الموظفين الجدد والقدامى بالسياسات المراد تطبيقها. اعتماداً على حجم العمل , هناك طرق متعددة لاستخدامها في هذا الجانب,مثلاً بعض الشركات تستخدم النشرات الدورية و البعض يكتفي باستخدام البريد الالكتروني. هناك بعض النقاط المطلوب تغطيتها عند وضع السياسات, مثل أهمية الحفاظ على آمان كلمة المرور والقواعد التي تحكم استخدام وسائط التخزين القابلة للإزالة (Diskettes, CD's,etc…) و استخدام الحاسب (personnel use,email,Internet) . الهدف هو التأكد من كفاءة التدريب للمستخدمين وبقائهم على علم بآخر التفاصيل[8].

5- سياسات البريد الالكتروني E-mail Policies : هناك بعض المخاطر التي سببت للكثير من الشركات و المشروعات و حتى الوكالات الحكومية والعسكرية الكثير من التعب و ضياع الوقت و المال. و هذا بحد ذاته مبرراً لوضع سياسات أمن للبريد الالكتروني[8].

من المستحسن استخدام أساليب مناسبة عند كتابة سياسات استخدام البريد الالكتروني. يميل المستخدمون إلى رفض هذه السياسات باعتبارها تنتهك خصوصيتهم , و لذا لابد أن تُشرك الإدارة مندوبين من جميع الأقسام المعنية حتى يشعر موظفيها بأنهم معنيون بهذا الأمر. يجب تدريبهم على الاستخدام المقبول و الغير مقبول للبريد الالكتروني , فقد يتسبب البعض في جعل المنظمة هدفاً للرسائل التطفلية و الغير أخلاقية , كذلك تحذيرهم من استخدام لغة تعسفية تجاه زملائهم أو عملاء المنظمة , أو استخدام البريد في معاملات تجارية خاصة بهم . من الجيد استخدام برامج SPAM filters لتصفية الرسائل من و إلى المنظمة. يمكن كذلك منع أنواع معينة من الملفات يحتمل أن تحمل فيروسات أو أشباهها, مثل ملفات exe. و vbs. , من الوصول[4].

6- سياسات الإنترنت Internet Policies: الانترنت , ذلك التجمع الهائل للمعلومات الذي يقع على بعد نقرة واحدة . الكثير من تلك المعلومات لا يمكن الاستغناء عنها, لذا فإننا بالتأكيد بحاجة لسياسات تحكم استخدام الإنترنت. إذا كان لديك خادم Server و جدر نارية Firewalls خاصة ستكون سهولة

السياسات بقدر تصفية عناوين URLs معينة . أو ستكون قائمة مفصلة مما يجب و ما لا يجب فعله على الإنترنت. يجب مناقشة أي نوع من المواقع يُعتبر محظوراً و فيما إذا كان استخدام الإنترنت سيكون مقصوراً للأغراض التجارية فقط أم يسمح باستخدامها للأغراض الشخصية. بغض النظر عن ملائمة قراراتك بالنسبة لاحتياجاتك , إلا أنه يجب التأكد أن جميع المستخدمين على مستوى مناسب من الوعي و الفهم[8].

7- الاستعادة بعد الكارثة (Disaster Recovery(backup and recovery : عند تقدير المخاطر سيكون من الأفضل تحديد المعلومات الحساسة و التي تحتاج إلى أن تنسخ احتياطياً . ليس هناك حاجة لإنفاق المزيد من المال و الوقت على شيء لا يمثل أي قدر من الأهمية. النسخ الاحتياطي مهم إلى درجة كبيرة لأسباب كثيرة منها:

- فشل و انهيار النظام و فقد جميع البيانات.
- تلقي فيروسات مدمرة.
- سرقة جهاز الحاسب نفسه.
- تشويه أو تحطيم البيانات على يد المخترقين Hackers.
- المستخدم يحذف ملفاته بدون قصد.
- كوارث طبيعية – حريق, فيضان,إعصار.

و نظراً لأهمية النسخ الاحتياطي فإن السياسات يجب أن تخصص خططاً لـ :

- جدول النسخ الاحتياطي – متى و كل كم من الوقت يُعاد النسخ .
- ما نوع النسخ الاحتياطي – كامل full أم تفاوتي differential أم تزايدي incremental أم تجميعي combination.
- ما نوع الأدوات المستخدمة في عملية النسخ – شريط ممغنط tape أم قرص ضوئي CD أم قرص صلب hard drive .
- أين سيتم تخزين النسخ الاحتياطية- في نفس الموقع في مكان آمن أم خارج الموقع أم كلاهما .

يمكننا القول أنه ليس هناك طريقة أفضل من النسخ الاحتياطي للمساعدة في الأزمات غير المتوقعة[8].

8- اكتشاف التطفل Intrusion Detection : يوجد الكثير من البرامج التجارية لكشف التطفل,لذا يمكن الاستفادة منها في الحفاظ على أمن الشبكة. تأكد أن البرنامج الذي وقع عليه الاختيار سيساهم في تلبية احتياجات العمل لديك. هذا الجزء من السياسات يجب أن يشمل: ما نوع كشف تطفل الشبكة(و هو جهاز يتم تثبيته في الشبكة لمراقبة حركة المرور ذهاباً و إياباً), كشف التطفل المبني على المضيف (يثبت في النظام لتتم مراقبته), تحديد أي الحوادث يمكن أن يعتبر تطفلاً في عُرف الشركة, كما أن السياسات لا بد أن توضح هل من المسموح إجراء فحص لاكتشاف الثغرات , و إذا كان كذلك فمن المسئول عن أداء هذه المهمة و متى؟ , و في حالة وقوع حادث ما كيف سيتم التعامل معه , هل سيسمح للمناوبين في تلك الفترة بالتعامل مع الحادث أم لا بد من الاتصال بالمشرف لأخذ الإذن بذلك. بغض النظر عن قراراتك بهذا الخصوص, فإنه يجب أن يكون هناك موجز واضح و موثق لمعرفة من المسئول و عن أي شيء مسئول؟, وهذا يؤدي إلى معرفة ما السلطة و الصلاحيات التي يمتلكها كل شخص[8].

للاستزادة حول كتابة سياسات الأمن , يوفر موقع SANS Institute الالكتروني نماذج لسياسات و إجراءات الأمن قابلة للتحميل, يمكن استخدامها كنقطة بداية لوضع سياساتك الأمنية و تعتبر مصدر جيد لتطبيق أوجه متعددة من إجراءات الأمن. و ذلك من خلال العنوان التالي[10]:

http://www.sans.org/newlook/resources/policies/policies.htm

التنفيذ Implementation

يجب أن تكون النسخة النهائية من سياسات الأمن متوفرة بسهولة لجميع الموظفين. كما يجب إيصالها للجميع بطريقة يدوية و من ثم الإشعار بأنه تم استلامها و قراءتها و فهمها و الموافقة على اتباعها و ذلك بالتوقيع عليها من قبل المستخدمين. الثقافة هي السبب الأساس في قبول المستخدمين للسياسات و اتباعها. تثقيف المستخدمين مهم لتحقيق الأمن و إشراكهم في عملية تطوير السياسات. الندوات و الحملات التثقيفية و التوعوية تساعد في تثقيف المستخدمين بأهمية الأمن, خصوصاً عملية اختيار كلمة المرور و إقفال الشاشة و الأمن المادي physical security[1].

سياسات الأمن يجب أن تدمج مع دليل الموظفين . أو من الممكن نشرها على الشبكة الداخلية للشركة لتكون متاحة للجميع ,أو يمكن طباعة تلميحات لها على ملصقات, أو إرسالها بالبريد الالكتروني, أو وضعها كحافظات شاشة screensavers, أو طباعتها على وسادة الفأرة mouse pad , لتذكير الموظف بأهميتها.
كما أنه تقع على الإدارة العليا مسئولية تدريب الموظفين على كيفية إتباع تلك السياسات[1].

المراقبة و المراجعة Monitoring and Review

من المهم مراقبة و مراجعة العملية السابقة(السياسات) باستمرار لتطويرها لمواجهة المخاطر الجديدة المكتشفة,و هذا يشمل التغييرات في المنظمة الناتجة عن المخاطر الجديدة. يمكن تغيير القوانين حسب الحاجة لمواجهة أي خطر جديد قادم.
بمرور الوقت, سيكون من اللازم تغيير السياسات القائمة , قد تُضاف سياسات جديدة عند الضرورة أو قد تُحذف سياسات لم تعد مجدية[1].

لماذا تفشل السياسات الأمنية Why Security Policies Fail

هناك الكثير من الأسباب التي تُفشل السياسات الأمنية , سألخص هنا بعضاً منها :

- السياسات تعيق التطور : حتى في الحالات العادية تكون السياسات سبب في تقليل الإنتاجية.
- السياسات سلوك مكتسب : إذا لم يدرك المستخدم قيمة سياسة معينة , فإنه سيعتبرها غير مهمة و بالتالي لن يتبعها.
- توقع المفاجئات : لا أحد يستطيع استباق جميع المخاطر, و لذا للإبقاء على فاعلية السياسات, لا بد من الاستمرار في حالة التأهب و التخطيط و التدريب.
- ليس هناك سياسات تامة : تطوير سياسات الأمن ليس حلاً منتهياً, و إنما عملية مستمرة .

جدير بالذكر هنا أنه لا توجد أي سياسات توفر الأمن للمنظمة بنسبة 100%. قد لا يكون بمقدورك توظيف سياسات و موارد أكثر مما فعلت و لكنك تحتاج إلى تكاتف و تعاون جميع من في المنظمة لتفعيل ما هو متوفر حالياً. قد يُطرح سؤال, ما المكاسب التي يتم الحصول عليها إذا كانت المنظمة أكثر أماناً؟. قد لا تكون هناك مكاسب نقدية , و لكن على الأقل تم منع خسائر كثيرة قد تحدث لو لم تكن المنظمة في أمان. ولكن مع كل الجهود التي بُذلت لا تتعجب من وقوع حوادث تذهب بجهودك أدراج الرياح[9].

الخاتمة

الأهداف الأساسية من الأمن هي توفر availability و خصوصية confidentiality و تكاملية integrity المعلومات. يجب أن نحدد ما الذي يجب حمايته , و من أي مخاطر نحميه, و كيف نحميه؟. في عملية تقدير المخاطر , تأكد من ترتيب المخاطر حسب شدة خطورتها و أولويتها. هذا سيساعد في اتخاذ القرار و تقليل الإنفاق لحماية أشياء لا تستحق. بمجرد وجود السياسات الأمنية , حاول أن تتبعها , و قم بمراجعتها بشكل دوري للتأكد من ملائمتها للتغيرات و الشروط المتغيرة.
أسند مسئولية السياسات لشخص ذو نفوذ و سلطة كافيتين حتى يستطيع فرضها على الجميع , لا تسند هذه المسئولية الهامة لأحد أعضاء فريق تقنية المعلومات حديثي العهد بالعمل.
هذا الموضوع واسع و مهم لدرجة أنه يمكن الكتابة و التحدث فيه لفترات أطول, و لكن المؤمل أنني أعطيت فهماً جيداً لسياسات الأمن و مدى أهميتها . ما يمكن قوله في نهاية هذا الموضوع هو أنه إذا لم يكن جميع المستخدمين بلا استثناء يطبقون سياسات الأمن و يعون أهميتها و يسعون لتحسين مستوى هذا المفهوم لديهم فليس من سبيل للحفاظ على الأمن في المنظمة و إن تعددت الوسائل على ما أعتقد.

المراجع

1) Chaiw Kok Kee , "Security Policy Roadmap – Process for Creating Security Policies", Version 1, SANS Institute 2001 , pp 1-7 .

2) Chris Wan , "Developing a Security Policy - Overcoming Those Hurdles", GSEC Practical Assignment , Version 1.4b , 24 April 2003, SANS Institute 2003 , pp 2-3 .

3) Kevin M. Dulany , "Security, It's Not Just Technical " , GSEC Practical Assignment , v1.3 , 15 January 2002 , SANS Institute 2002 , p 4 .

4) David Jarmon , "A Preparation Guide to Information Security Policies" , SANS Security Essentials GSEC Practical Assignment , Version 1.3 , SANS Institute 2002 , pp 1-3 , 11-14 .

5) Scott Woodison , "Information Technology Policies" , Working Paper- Draft, Version 1.0 , 1 October 2002 , pp 2-4 . URL: http://radio.weblogs.com/0113212/gems/InformationTechnologyPolicyworkingpaper.pdf

6) Security Complete, San Francisco: Cybex, 2001, pp. 17–40.

7) "Enterprise Information Security Policies" , Georgia Technology Authority , September 10, 2002 , pp 10-11. URL: http://gta.georgia.gov/vgn/images/portal/cit_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf

8) Joel S. Bowden , Security Policy What it is and Why - The Basics, February 18, 2003 , SANS Institute 2001, pp 1-6 .

9) Rosemary Sumajit , "Developing Security Policies: Charting an Obstacle Course" , GSEC Version 1.3 , April 4, 2002 , SANS Institute 2002, pp 8-9 .

10) Nancy J. Carpenter , "SANS Security Essentials" , Practical Assignment , Version 1.2f , September 24, 2001 , SANS Institute 2001 , p 5.

ملحوظة:
المراجع 1 ,2 ,3 ,4 ,8 ,9 ,10 مأخوذة من :
The Information Security Reading Room - SANS Institute
URL: http://www.sans.org/rr/whitepapers/policyissues