المحاضرة السادسة عشر

العناصر الاساسية لأمن المعلومات - سياسات امن المعلومات

العناصر الأساسية لأمن المعلومات :

٣. السرية (Confidentiality)

يطلق على هذا العنصر أيضا الخصوصية (Privacy) وتعني الحفاظ على المعلومات من أن يطلع عليها (يقرأها و يفهمها) غير الأشخاص المصرح لهم فقط، أو بعبارة أخرى منع الكشف الغير مصرح به. عندما يتم إرسال رسالة "سرية"، فإن ذلك يتطلب أن لا يراها إلا المرسل والمرسل إليه فقط.

هناك العديد من الطرق لتوفير السرية تتراوح بين حجب المعلومة يدويا وعدم تسليمها إلا للأشخاص المصرح لهم فقط إلى طرق التشفير الحديثة التي تعتمد على خوارزميات رياضية معقدة يصعب فكها إن لم يكن مستحيلا .

قد يتبادر إلى ذهن البعض بأنه عندما يتوفر عنصر "السرية" للمعلومة، فإنها بذلك تصبح معلومة آمنة. أو بعبارة أخرى أن التشفير (وهو وسيلة لتحقيق عنصر السرية) يضمن أمن المعلومة بشكل كامل، وهذا مفهوم خاطئ. والصحيح أن السرية ما هي إلا عنصر واحد من عدة عناصر رئيسية يجب توافرها جميعا لتصبح المعلومة آمنة.

ومن الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر "السرية":

- هي امكانية الاطلاع على معلومات هامة وحساسة من قبل أي أحد إذا تم وضع هذه المعلومات على وسط تخزين خارجي (ذاكرة قلمية مثلا) وهي غير مشفرة.
- ومثال آخر هو إرسال مرفق لبريد إلكتروني عبر البريد الإلكتروني العام (Google أو Hotmail مثلا) وهو غير مشفر وبه معلومات هامة جداً. في هذه الحالة، فإن البريد الالكتروني والمرفقات التي معه عرضة للاطلاع عليها من قبل الغير بمن فيهم الشركة المقدمة لخدمة البريد العام.

٤. سلامة وتكامل المعلومات (Data Integrity)

وتعني الخدمة التي من خلالها يمكن الحفاظ على سلامة المعلومة من التعديل أو الحذف أو الإضافة أو إعادة التركيب أو إعادة التوجيه، وهذا أمر مهم جداً لضمان الثقة في المعلومة وأنها هفي المعلومة الأصلية دون زيادة أو نقصان.

ومن الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر "سلامة وتكامل المعلومة" :

- هي إمكانية تعديل الأرقام في المعاملات المالية بسهولة دون أي تغيير في معنى الإجراء أو الرسالة. فمثلاً يمكن تكبير المبلغ بمجرد وضع صفر على يمينه (أو تصغيره بإزالة ذلك الصفر) وفي هذه الحالة لا يمكن كشف هذا التغيير إذا لم يتوفر عنصر تكامل وسلامة المعلومة.

٥. عدم الإنكار

وهي الخدمة التي من خلالها يمكن منع (وكشف) أي شخص أو جهة من إنكار أي عملية قام بها

على سبيل المثال في حالة إرسال رسالة بين طرفين، فإن عدم الإنكار يثبت قيام المرسل بإرسالها ويثبت قيام المستقبل باستلامها بحيث لا يمكن لأي منهما إنكار ذلك. وتزداد أهمية هذا الإثبات بازدياد أهمية الرسالة نفسها.

ومن الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر "عدم الإنكار" :

- هي إمكانية التنصّل من مسئولية وثيقة معينة تم توقيعها (تصديقها) إلكترونيا من قبل أحد الأشخاص. فإذا لم يتوفر عنصر عدم الإنكار فلا يمكن إثبات أن هذا الشخص هو من قام بتوقيع هذه الوثيقة

٦. توفر المعلومة (Availability)

ويقصد بتوفر المعلومة أن تكون قابل للوصول إليها واستخدامها حين الطلب من قبل أي شخص أو أي جهة معروفة ومحددة وفي أي وقت (مصرح به).

ويمكن القول بأن خدمة التوفر هي الخدمة التي تحمي النظام ليبقى متاحا دائما (ومن هنا يطلق عليه أحيانا "الديمومة")

ومن الأمثلة على الخروقات الممكنة لأمن المعلومات التي يمكن أن تتم في حال عدم توفر عنصر "توفر المعلومة" :

- إمكانية تدمير أنظمة المنشأة باستخدام برنامج تدمير (أو فيروس تدميري) حديث الإنتاج لا يوجد له برامج حماية أو تحديثات (Patches) تلغي فاعليته.
- ففي هذه الحالة إذا لم تكن هناك أنظمة احتياطية يتم استخدامها بدل التي تم تدميرها وتضمن توفر المعلومة فسيكون هناك توقف تام في عمل المنشأة ولو لوقت محدود.

سياسات أمن المعلومات

مقدمة : تبدأ خطة أمن المعلومات بإنشاء السياسات الأمنية (Security Policies) والاجراءات القياسية (Standards) والإجراءات المتخذة (Practices) من أجل الحصول على معلومات تفصيلية مطبوعة عن كل واحد منها والتي تكون في مجموعها خطة تفصيلية لأمن المعلومات.

١) ماهية السياسات الأمنية

هي الطريقة أو الخطوات المكتوبة التي تحدد كيفية أداء الأعمال ذات العلاقة بأمن المعلومات وكيف تتم معالجة أي حدث يخص المعلومة وكيف يتم استخدام التقنية المتوفرة لمعالجة ذلك.

وتعتبر السياسة الأمنية هي حجر الزاوية للتخطيط لأمن المعلومات والتي يمكن الانطلاق منها لتطبيق الخطة على أرض الواقع.

وتجدر الإشارة إلى أن هناك جانبا كبيراً من أمن المعلومات هو في حقيقته جانب إداري وإجرائي بالدرجة الأولى يتمثل في السياسات الأمنية.

السياسات الأمنية هي إجراءات إدارية يتم تطبيقها على أرض الواقع من خلال الأنظمة والبرامج المتاحة.

- مثال ذلك ، يمكن وضع سياسة أمنية تنص على أنه في حال عدم إدخال كلمة المرور بشكل صحيح لثلاث مرات متتالية فأنه يتم تعطيل حساب ذلك المستخدم ولا يفتح مرة أخرى إلا عن طريق مدير الشبكة. وهذا إجراء إداري يتم تطبيقه من خلال التحكم بكلمات المرور.

ويمكن القول بأن السياسات الأمنية هي بمثابة قانون للمنشأة يحدد التعريفات والإجراءات المقبولة على كافة المستويات الإدارية من مدراء ومتخذي القرارات والمنفذين.

وعلى هذا، فإن السياسة الأمنية لا بد أن تكون واضحة ودقيقة وتحدد ما هو الشيء الصحيح وما هو الشيء الخاطئ وما هو الإجراء في حاله الصواب والإجراء في حالة الخطأ. ومما لاشك فيه يجب أن يكون هناك سياسة أمنية عامة للمنشأة بدءً من إجراءات منح الصلاحيات للموظف، مروراً بسياسة كلمات المرور، ثم استخدام شبكة الإنترنت، وانتهاءً بخطة مواجهة الكوارث؟

خصائص وثيقة السياسة الأمنية العامة

يجب أن تكون السياسية الأمنية العامة مكتوبة على شكل وثيقة تفصيلية تتصف بالخصائص التالية :

١. أن تكون منظمة ومرتبة ومبوبة وفق مهام المنشأة الأساسية.
٢. أن تكون مكتوبة بلغة واضحة سهلة الفهم والتطبيق.
٣. أن يتم فيها تحديد المسؤوليات والصلاحيات بكل دقة، فمثلاً، يجب تحديد من لديهم صلاحية حرمان المستخدم من الدخول على الشبكة عند مخالفته للسياسة الأمنية، وتحديد الأشخاص المسئولين عن إيقاف خدمة معينة إذا كانت تضر بشبكة المنشأة.
٤. تحديد الإجراءات التي يجب إتباعها عند ظهور أي مشكلة بشكل تفصيلي وعدم ترك الموظف في حيرة من أمره.

ما يجب ان تحتويه وثيقة السياسة الأمنية العامة

يجب أن تحتوي وثيقة السياسة الأمنية العامة (على الأقل) على البنود التالية:

١. الإجراءات اللازم اتخاذها فيما يخص أمن المعلومات وموارد المنشأة لدى تعيين موظف جديد أو عند إنهاء خدمات موظف سابق.
٢. تحديد صلاحيات المستخدمين وتقسيمهم إلى مجموعات وتحديد صلاحيات كل مجموعة.
٣. وضع الشروط والقيود اللازمة لكلمات المرور لضمان أمن وحماية حسابات المستخدمين.
٤. تحديد متى يجب أيقاف حساب المستخدم ومنعه من الدخول على شبكة المنشأة أو تعطيل حسابه لفترة محدودة، ومتى يجب إعادة تفعيله.
٥. الإجراءات اللازم إتباعها والشروط اللازم استيفائها قبل توصيل أي جهاز جديد بشبكة المنشأة.
٦. إجراءات أمن المعلومات التي يجب تطبيقها على الشبكة بشكل عام، وعلى كل جهاز على حده كقفل منافذ الاتصال وتفعيل التحديث التلقائي لأنظمة التشغيل والبرامج وتحديد الأوقات المناسبة لذلك.
٧. الإجراءات اللازم إتباعها لحماية شبكة المنشأة من الفيروسات.
٨. تحديد المستخدمين أو المجموعات الذين يسمح لهم بتركيب أجهزة برامج إضافية على أجهزتهم.
٩. شروط وقيود استخدام شبكة الإنترنت وإجراءات الاتصال بها.
١٠. الإجراءات اللازم اتخاذها للحصول على بريد إلكتروني وشروط وقيود استخدامه.
١١. آلية النسخ الاحتياطي وتحديد مسؤوليات وصلاحيات عمل ذلك.

يمكن القول بأنه لا توجد سياسة أمنية تغطي كافة جوانب أمن المعلومات في جميع إجراءات المنشأة فلا بد من وضع طريقة مناسبة للتعديل أو الإضافة على السياسة الأمنية، وترك مجال لذلك وفق ضوابط وشروط محدده.

يجب مراعاة إمكانية مراجعة السياسة الأمنية والتعديل فيها مع مرور الزمن أثناء التطبيق.

حالات تطبيقية لسياسات أمنية

الهدف من تقديم حالات تطبيقية لبعض السياسات الأمنية (من الناحية الإدارية كدليل أمني) هو توفير التوجيهات الأمنية اللازمة التي تعكس قواعد السياسة الأمنية لكل حالة تطبيقية وعرضها في شكل تسهل قراءته وفهمه.
والحالات التطبيقية التي سيتم استعراضها هي: السياسة الأمنية لكلمات المرور، السياسة الأمنية لاستخدام الإنترنت والبريد الإلكتروني.

السياسة الأمنية لكلمات المرور

من أقدم الأدوات المستخدمة لحماية المعلومات هي استخدام كلمة المرور)كلمات السر(للدخول على الأنظمة أو المعلومات. وبذلك فإن جانبا هاما من حماية المعلومات يقع بالكامل في أيدي المستخدمين.

لذلك ظهرت الحاجة إلى إيجاد سياسة أمنية تحكم كلمات المرور وتضمن رفع المستوى الأمني لها وتتلخص أهم بنود السياسة الأمنية لكلمات المرور في صيغة افعل لا تفعل فيما يلي:

- **افعل ما يلي:**

١. استخدم كلمات مرور تكون خليط من الأحرف (أ...ي) والأرقام (صفر...٩) والرموز (%، @، &...إلخ).
٢. غيّر كلمة المرور الخاصة بك بشكل دوري.
٣. استخدام حد أدنى من طول كلمات المرور، وينصح بشدة أن لا يقل عن عشر خانات مكونة من أرقام وحروف ورموز.
٤. غيّر كلمة المرور المقدمة إليك عند فتح حساب جديد أو إعطائك صلاحية الدخول على نظام خاص بالمنشأة لأول مرة.
٥. وضع حد معين لعمر كلمة المرور بحيث يجب استخدام كلمة المرور طوال فترة (عمر) معينة ولا يسمح للمستخدم بتغييرها قبل اكتمال تلك الفترة.
٦. استخدام كلمات مرور عشوائية للأنظمة عالية الحساسية.
٧. تعطيل (أو إلغاء) كلمة المرور بعد ثلاث محاولات خاطئة.

- **لا تفعل ما يلي:**

١. استخدام كلمات مرور مكونة من كلمات موجودة في المعجم. بمعنى يجب أن لا تكون كلمات عادية يمكن لطرق الاختراق المتعمدة على المعاجم أن تكسرها.
٢. استخدام اسم المستخدم أو أي جزء منه أو أي جزء من الاسم العادي للمستخدم ككلمات مرور.
٣. كتابة كلمات المرور على ورق أو ملصقات من أجل تذكرها.
٤. استخدام كلمات المرور التلقائية (Default) ككلمات مرور أساسية.
٥. استخدام أي كلمة مرور من آخر خمس كلمات مرور تم استخدامها في الماضي.

٦. إطلاع غيرك على كلمة المرور الخاصة بك حتى ولو كان مدير النظام.
٧. استخدام كلمة المرور نفسها في عدة حسابات وأنظمة. (مثال ذلك: استخدام كلمة المرور نفسها للبريد الإلكتروني "العام" وللدخول على شبكة الحاسب الآلي المحلية للمنشأة).
٨. تخزين كلمة المرور على الحاسب الآلي.

السياسة الأمنية لاستخدام شبكة الإنترنت والبريد الإلكتروني

يتم توفير شبكة الإنترنت والبريد الإلكتروني للعاملين في المنشأة لتسهيل القيام بأعمالهم والتواصل فيما بينهم ومع الجهات الخارجية.

هناك بعض المخاطر المتأصلة في استخدام الإنترنت والبريد الإلكتروني من أجل ذلك يتم وضع السياسة الأمنية لاستخدام شبكة الإنترنت والبريد الإلكتروني في صيغة افعل لا تفعل لعدد من التوجيهات المنظمة لذلك كما يلي:-

- **افعل ما يلي:**

١. التأكد من عنوان الموقع أو الصفحة المراد زيارتها على شبكة الإنترنت.
٢. التأكد من موثوقية مصادر الروابط المستخدمة للدخول على المواقع.
٣. تخزين الروابط المهمة وكثيرة الاستخدام في قائمة المفضلة للرجوع لها وقت الحاجة وكذلك لضمان صحتها عند استخدامها.
٤. المعرفة التامة بأنواع الملفات التنفيذية التي تحمل أكواد ضارة مثل (ActiveX) .
٥. التأكد من أن رسائل البريد الإلكتروني الصادر منك تتضمن عناوين الاتصال الخاصة بك.
٦. التأكد من صحة عنوان البريد الإلكتروني للمرسل إليه وكذلك عنوان من تريد أن تزودهم بصورة كربونية (CC) أو صورة معماة (BCC)، حيث أن الأخطاء في مثل ذلك قد تؤدي إلى عواقب وخيمة.
٧. التأكد من أن مرفقات البريد الإلكتروني هي نفسها ما قصدتها وليس غيرها. الإهمال في ذلك قد يؤدي إلى بعث معلومات هامة وحساسة إلى جهات ليس لها الحق في الاطلاع عليها.
٨. ضغط الملفات والمجلدات كبيرة الحجم قبل إرفاقها بالبريد الإلكتروني.
٩. تشفير المحتويات والمرفقات الهامة قبل إرسالها، (لاحظ انه يفضل بشدة ضغط الملفات قبل تشفيرها حتى يمكن الاستفادة من عملية الضغط أقصى ما يمكن).
١٠. التأكد من أن جميع الرسائل الواردة إليك بتم فحصها من البرامج الضارة.
١١. حذف الرسائل الغير ضرورية سواءً المرسلة أو المستقبلة والرسائل غير موثوقة المصدر خاصة التي بها روابط دعائية.
١٢. ترتيب الرسائل وحفظها في مجلدات حسب طبيعة عملك واحتياجك.

١٣.الإبلاغ عن أي خطأ ارتكبته أو موقع تمت زيارته واتضح أنه موقع ضار أو بريد الكتروني استقبلته وبه روابط غير موثوقة أو به برامج ضارة

- **لا تفعل ما يلي:**

١. استخدام روابط غير متأكد من صحتها أو التي تكون من مواقع أخرى غير موثوقة.
٢. استخدام النوافذ المنبثقة الغير موثوقة.
٣. تخطي رقابة الشبكة للدخول على مواقع محجوبة
٤. قضاء أوقات طويلة في تصفح مواقع ليس لها علاقة بعمل المنشأة
٥. ترك الإنترنت مفتوح طوال اليوم لأغراض ليس لها علاقة بعمل المنشأة
٦. تنزيل الصور والفيديو والصوتيات التي ليس لها علاقة بعمل المنشأة.
٧. تنزيل المواد والبرامج بطريقة تنتهك حقوق ملكية الآخرين.
٨. تنزيل البرامج وتشغيلها أو تثبيتها على الأجهزة بدون إذن مسبق.
٩. تنزيل أو تثبيت البرامج الضارة وبرامج الاختراق والتجسس بأي شكل من الأشكال.
١٠.القيام بأي نشاط تخريبي أو تجسسي أو وصول غير مشروع من خلال أجهزة وشبكة المنشأة.
١١.استخدام البريد الإلكتروني لأشخاص آخرين والقيام بقراءة محتواه أو إرسال الرسائل منه.
١٢.إرسال رسائل بريد إلكتروني أو مرفقات غير مصرح بها كالرسائل الدعائية والنكت وأخبار الأندية الرياضية.
١٣.تفعيل التمرير الآلي للبريد الإلكتروني إلى خارج المنشأة أو الجهات الغير مصرح لها داخل المنشأة.
١٤.فتح رسائل البريد الإلكتروني مجهولة المصدر والمواضيع.
١٥.إرسال أو فتح الرسائل أو المرفقات الغير لائقة أو التي بها محتويات غير مناسبة.