مدونة المناهج السعودية

https://eduschool40.blog

الموقع التعليمي لجميع المراحل الدراسية

في المملكة العربية السعودية

تلخيص الفصل السابع (أمن نظم المعلومات)

تعريف أمن نظم المعلومات : هو السياسات والإجراءات والتدابير التقنية المستخدمة لمنع الوصول غير المصرح به إلى المعلومات أو تعديلها أو تدميرها .

أهداف أمن نظم المعلومات (يمكن أن تكون هذه الأهداف مستقلة أو متداخلة) :

١- السرية : أن يتم ضمان الوصول إلى الأصول ذات الصلة بنظام المعلومات فقط من قبل الأطراف المصرح لهم .
٢- السلامة : أنه يمكن معالجة الأصول فقط من قبل الأطراف المصرح لهم تتضمن المعالجة (التغيير - الحذف - الإنشاء - والإضافة) .
٣- التوافر : يعني أن الأصول هي متناول الأطراف المصرح لهم .

- وجود الشبكات والانترنت وانتشار التجارة الإلكترونية أضيف هدفين مهمين :
  - التأكد من الهوية
  - Nonrepudiation : القدرة على الحد من تنصل الأفراد من الالتزام بإتمام معاملة معينة .

يمكن لمالكي نظام المعلومات اختيار عدة إجراءات لتحقيق هذه الأهداف :

- إجراءات وقائية : وهي إجراءات تهدف إلى جعل احتمالية حدوث الخسائر تؤول للصفر .
- إجراءات مخففة : تهدف لتقليل الخسائر لمستوى مقبول .
- إجراءات ناقلة : تتضمن نقل الخسارة في حال حدوثها لطرف ثالث .
- إجراءات استشفائية : تهدف لاستعادة النظام حالته السابقة الطبيعية بعد الحادث. (ولكن تظهر مسألتين مهمة أولا مسألة التكاليف مقابل النفع - ثانيا إيجاد التوازن الصحيح بين هذه الجوانب)

التهديدات : هي مجموعة من الظروف المحيطة التي قد تسبب الخسارة أو الضرر والتي تستغل نقاط الضعف في ذلك النظام .

- يتعرض نظام المعلومات للكثير من التهديدات وهي :

١- الاعتراض : يعني أن بعض الأطراف غير المصرح لهم تمكنت للوصول إلى أحد الأصول.

Scanned with CamScanner

٢- الانقطاع : فقدان أصل من أصول النظام أو عدم توفره أو تحوله لأصل غير قابل للاستخدام .

٣- التعديل : وصول أحد الأطراف غير المصرح لهم تمكنت للوصول إلى أحد الأصول والعبث بها .

٤- التزييف : يمكن لأطراف غير المصرح لهم إنشاء أو تلفيق أمور مزيفة في نظام المعلومات .

لمعالجة هذه المشاكل يمكن الاعتماد على الضوابط التي تستخدم كإجراء وقائي

مكونات أمن نظم المعلومات :

الأمن المادي : يستخدم لوصف الحماية اللازمة للبيئة المحيطة بنظام المعلومات تشمل ضوابط الأمن المادي الحماية من تهديدين :

- تهديدات غير مباشرة : عرضة للكوارث الطبيعية

يتم التعامل معها مع عدة طرق :

- وضع خطط للطوارئ
- التأمين ضد الكوارث على الأصول المادية
- تخزين نسخ احتياطية للبيانات في عدة أماكن آمنة
- توفير مصادر بديلة للتيار الكهربائي
- استخدام جهاز يساعد على حماية الأجهزة

- تهديدات مباشرة : يتعرض نظام المعلومات على تهديدات مباشرة من أشخاص

يمكن اتخاذ واحدة من هذه الأساليب لمنع السرقة :

- منع المرور
- منع إمكانية نقل الأجهزة تمهيدا لسرقتها
- التحقق أثناء الخروج

١- التخلص من المعلومات السرية يتم من طريقتين :

- التخلص من المعلومات المطبوعة التمزيق
- إلغاء البيانات المخزنة على وحدات التخزين

Scanned with CamScanner

أمن البرامج : تشكل البرامج جزءا كبيرا من نظم المعلومات وتشمل نظم التشغيل .

في مجال أمن البرامج تظهر قضيتين مهمتين :

١- كتابة البرامج الخالية من الأخطاء :

- أخطاء البرامج الغير ضارة والغير مقصودة

قد تسبب خلل بسيط في البرامج ولكنها لا تؤدي لثغرات أمنية .

- التعليمات الضارة المقصودة

من الممكن لأي مبرمج إضافة تعليمات برمجية ضارة في نظام أو تطبيق معين وكلما زاد حجم وتعقيد البرامج يمكن للمبرمجين إضافتها أو إخفاءها بسهولة من الأمثلة على ذلك

(Trapdoors) : هي نقطة الدخول إلى البرامج غير الموثوقة .

يحذفه المطورين عادة عند انتهاء الحاجة إليه ومع ذلك يمكن إبقاءه في البرامج للأسباب التالية :

١- نسيان المبرمج إزالتها
٢- تركت عمدا من المبرمج في البرنامج لاختباره
٣- تركت عمدا من المبرمج في البرنامج لصيانة البرنامج النهائي
٤- تركت عمدا من المبرمج في البرنامج كوسيلة خفية للوصول إلى البرنامج بعد تسليمه .

٢-البرامج الضارة : يمكن استخدامها لتكون وسيلة للوصول لتغيير البيانات وغيرها .

- فيروس virus : هو برنامج مخفي داخل برنامج أخر يسمى المضيف بحيث يبدو غير مؤذي (لتفعيل الفيروس يجب أن يتم تشغيل البرنامج المضيف أو فتحه) .

تتفاوت فيروسات الكمبيوتر في شدة تأثيرها فبعها تسبب تأثيرا بسيطا فقط

لا يمكن لفيروس أن ينتشر دون تدخل بشري

- الدودة worm : برنامج مشابه لبرنامج الفيروس من حيث تصميمه ويمكن أن نعتبر أن الدودة صنف فرعي من الفيروس ، هذا البرنامج ينشر نسخ عن نفسه من حاسوب إلى حاسوب من خلال الشبكة دون الحاجة لتدخل بشري .

(الخطر الأكبر من الدودة هو قدرته على تكرار نفسه على النظام)

Scanned with CamScanner

الفرق الأساسي بين الدودة والفيروس :

١- أن الدودة تعمل من خلال الشبكات
٢- يمكن للفيروس أن ينتشر من خلال أي وسيط
٣- تنتشر الدودة من خلال نسخ نفسها كبرنامج قائم بذاته
٤- ينتشر الفيروس بنسخ نفسه كبرنامج يرتبط ويندرج في برامج أخرى

- حصان طروادة : يبدو حصان طروادة كبرنامج شرعي أو ملف من مصدر شرعي ولكن عندما يتم تنشيطه على الكمبيوتر تحصل نتائج مختلفة .

البرامج المضادة للفيروسات : تعتبر البرامج المضادة للفيروسات من أهم طرق الحماية لأجهزة الكمبيوتر المستقلة أو المربوطة بالشبكة .

أمن قاعدة البيانات :تعتبر قواعد البيانات من أساسيات العمل في المنظمات ؟

لأنها تحتوي على البيانات التي تعتبر أصول المنظمات القيمة التي يجب أن تكون محمية

من الضوابط الأساسية المتعلقة بأمن البيانات وقواعد البيانات هي ضوابط الدخول واستبعاد البيانات الزائفة و الموثوقية .

يمكن تصنيف الاحتياجات اللازمة لأمن قاعدة البيانات إلى :

- سلامة قاعدة البيانات المادية .
- سلامة قاعدة البيانات المنطقية .

سرقة البيانات : أصبحت معلومات المنظمات هدفا للقراصنة بحيث يتم سرقة البيانات عن طريق نسخها أو أخذها من داخل المنظمة بشكل غير قانوني .

- التهديدات الداخلية هي مصدر القلق الأكبر والمشكلة الأكثر شيوعا لسرقة البيانات.
- التهديد من الداخل يمكن أن يكون الأكثر تكلفة والأشد ضررا بسمعة المنظمة .

الضوابط الخاصة بقواعد البيانات :

قابلية المراجعة : إمكانية متابعة من تمكن بالدخول إلى قاعدة البيانات .

ضوابط الدخول : السماح للمستخدم الوصول إلى البيانات المصرح فقط الوصول إليها .

Scanned with CamScanner

التأكد من هوية المستخدم : يتم تعريف كل مستخدم بصورة معينة .

أمن الشبكات : من الأسباب التي تجعل الشبكة أكثر عرضة للتهديدات

١- صعوبة تهديد هوية المهاجمين
٢- نقاط كثيرة للهجوم
٣- المشاركة
٤- حدود غير معروفة

(كلما زادت الإجراءات المنية المضافة ازدادت صعوبة استخدام الشبكة وازدادت بطأ مما يؤثر على سهولة الاستخدام)

أنواع التهديدات لأمن الشبكات :

الهجوم غير التقني (الهندسة الاجتماعية) : وظيفة الهندسة الاجتماعية هو إقناع الضحية على أن يكون مفيدا ، في كثير من الأحيان ينتحل المهاجم شخصية شخص من داخل المنظمة.

الأساليب المستخدمة لمكافحة الهندسة الاجتماعية :

١- تعليم وتدريب الموظفين ٢- وضع سياسات وإجراءات ٣- القيام باختيارات للاختراق والإيقاع بالموظفين .

الانتحال :استخدام هوية كيان ما

Session hijacking : هو اعتراض وتولي عملية اتصال بدأت من قبل كيان أخر .

.... Man-in-the : هذا الهجوم مشابه ♦ والذي فيه يتطفل كيان واحد بين اثنين .

.... Denial : يستهدف المهاجم كمبيوتر معين أو شبكة وذلك بهدف تعطيل عملهم .

من الأمثلة على ذلك : استخدام المهاجم رسائل البريد (من أكثر أنواع هذا الهجوم شيوعا هي عندما يغرق المهاجم الشبكة بفيضانات من المعلومات) .

....Distributed : يحاول المهاجم الوصول للعديد من أجهزة الكمبيوتر على شبكة الإنترنت لماذا سمي بذلك ؟ لأن المهاجم يستخدم العديد من أجهزة الكمبيوتر التي تسمى زومبي لشن الهجوم .

Scanned with CamScanner

حماية الشبكات :

- التأكد من الهوية وأنواعها :

١- كلمة المرور أو رقم الـ pin : هو الأسلوب الأكثر استخداما . (من مميزاتها لأنها سهلة الفهم وسهلة التنفيذ وسلبياتها غالبا ما تنسى كلمة المرور وأيضا يميل المستخدم لتدوين كلمة المرور وهذا يجعله أكثر عرضة للخطر)

٢- البطاقة الذكية : المشكلة في إمكانية فقدان المفتاح

٣- القياسات الحيوية : تستخدم هذه النظم الخصائص الفيزيائية (هي جزء من الشخص لا يمكن نسيانها أو سرقتها أو ضياعها)

٤- التشفير : هي عملية تحويل نص أو بيانات إلى نص مشفر و له نوعان :

- التشفير بالمفتاح الخاص : في هذه التقنية يستخدم المرسل والمرسل إليه نفس المفتاح
- التشفير بالمفتاح العام : يستخدم مفتاحين عام وخاص يتم الاحتفاظ بصورة سرية

الاستخدامات الرئيسية لهذه التقنية : تحقيق الخصوصية - للإثبات هوية المرسل .

فوائد استخدام مفتاح التشفير العام :

١- يمكن للمستخدم استخدام نفس زوج المفاتيح الخاص والعام لكافة أنشطته .

٢- بما أن المستخدم فقط يعرف المفتاح الخاص به يسمح له هذا باستخدام التوقيع الرقمي .

الجدار الناري : هو ببساطة حاجز ا بين شبكتين الشبكة الداخلية للمنظمة (الشبكة الموثوق فيها) والشبكة الخارجية (الإنترنت) .

- الجدار الناري الشخصي : هو يراقب حركة المرور الواردة والصادرة لتلك الشبكة .

أنظمة كشف التسلل : هو برنامج أو جهاز يرصد حركة المرور عبر الشبكة أو الكمبيوتر ويراقب أي نشاط مشبوه .

الشبكات الخاصة الإفتراضية : هي شبكة تستخدم شبكة الانترنت العامة لنقل المعلومات

يمكن استخدام الشبكة الخاصة الإفتراضية في ثلاث تطبيقات :

- الوصول عن بعد - المكاتب المتباعدة - إكسترانت .

Scanned with CamScanner

إدارة المخاطر الأمنية : هي عملية منهجية لتحديد احتمال وقوع الهجمات الأمنية .

مراحل إدارة المخاطر الأمنية :

- المرحلة الأولى التقييم : تقييم المخاطر الأمنية
- المرحلة الثانية التخطيط : التوصل لمجموعة من السياسات التي تحدد نوع التهديدات
- المرحلة الثالثة التنفيذ : يتم اختيار وتركيب تقنيات معينة لمواجهة التهديدات
- المرحلة الرابعة الرصد والمتابعة : يتم قياس مدى تحقيق الإجراءات الأمنية للأهداف الموضوعة

Scanned with CamScanner