مدونة المناهج السعودية

https://eduschool40.blog

الموقع التعليمي لجميع المراحل الدراسية

في المملكة العربية السعودية

الفصل السابع

أمن نظم المعلومات
مبادئ نظم المعلومات الإدارية
د. آلاء عمر بارفعه

محاور المحاضرة

- امن قاعدة البيانات
- امن الشبكات
- إدارة المخاطرة الامنية

أمن قاعدة البيانات

تعتبر قواعد البيانات من أساسيات العمل في المنظمات لأنها تحتوي على البيانات اللي تعتبر **أصول** المنظمات القيمة اللي يجب أن تكون محمية.

من الضوابط الأساسية المتعلقة بأمن البيانات:

- ضوابط الدخول.
- استبعاد البيانات الزائفة.
-التأكد من هوية المستخدمين وصلاحيتهم.
- الموثوقية.

يمكن تصنيف الإحتياجات اللازمة لأمن قاعدة البيانات إلى:

-سلامة قاعدة البيانات المادية:

يجب ان تكون قاعدة البيانات محصنه ضد المشاكل المادية ، مثلك انقطاع التيار الكهربائي

-سلامة قاعدة البيانات المنطقية:

يجب الحفاظ على هيكلية قاعده البيانات

سرقة البيانات:

-أصبحت معلومات المنظمة هدفاً للسرقة عن طريق نسخها أو نقلها أو أخذها من المنظمة بشكل غير قانوني..

-رغم أن التقنيات الأمنية تتحسن ولكن التهديدات تزداد تطوراً وتعقيداً.

-فإن **التهديدات الداخلية** مصدر القلق الأكبر والمشكلة الأكثر شيوعياً لسرقة البيانات (التهديد من الداخل يمكن أن يكون الأكثر تكلفة والأشد ضرراً بسمعة المنظمة)

-وللسيطرة على مشاكل التهديدات الداخلية يجب أن تولي المنظمة عناية كبيرة بالأمن المتعلق بالأفراد: ويشمل عملية توظيف الموظفين والتأكد من تاريخهم و اتجاهاتهم، والإهتمام بالتدريب الأمني للموظفين، وكيفية التعامل مع الموظفين المستقيلين والمفصولين.

الضوابط الخاصة بقواعد البيانات:

يجب وضع ضوابط لحماية قاعدة البيانات من التخريب، و منها:

-قابلية المراجعة:

إمكانية متابعة من تمكن من الدخول إلى قاعدة البيانات أو من قام بالتعديل على عناصر معينة من قاعدة البيانات.

-ضوابط الوصول:

السماح للمستخدم بالوصول إلى البيانات المصرح له.

-التأكد من هوية المستخدم:

يتم تعريف كل مستخدم بصورة معينة وذلك للمراجعة أو للحصول على إذن للوصول إلي بيانات معينة.

امن الشبكات :

لا تعتبر الكمبيوترات المعزولة أهداف محتملة لكثير من الهجمات . لكنها تصبح اكثر عرضة للخطر عند ربطها مع الشبكات وخاصة الإنترنت ، لانها تصبح متاحه تقريباً لأي شخص على نطاق واسع جداً .
لتتمكن المنظمات من الاستفادة من التجاره الإلكترونية ، وإدارة سلسلة التوريد ، وغيرها من العمليات التجاريه الرقمية يتعين على المنظمات جعل جزء من نظم معلوماتها متاح للعملاء و الموردين .

من الأسباب التي تجعل الشبكات اكثر عرضه لتهديد :

- **صعوبة تحديد هوية المهاجمين** Anonymity
يمكن للمهاجم شن هجوم من على بعد آلاف الاميال وليس على اتصال مباشر مع النظام
- **نقاط كثيره للهجوم** :
تنتقل البيانات او الملفات عبر عديد من الاجهزه المضيفة للوصول الى استخدام تفرض . بعض الاجهزه المضيفة سياسات أمنيه صارمه

- **المشاركة :**
تتميز الشبكات بالتشارك بالموارد وتوزيع العمل الذي يعني ان أعداد كبيره من المستخدمين لديهم القدرة على الوصول الى أنظمة الشبكات

- **حدود غير معروفه :**
امتداد الشبكات يؤدي الى عدم اليقين بشأن حدود الشبكه . بحيث ان جهاز مضيف واحد قد يكون حلقة الربط مع شبكات أخرى .

- **كلما زادت الإجراءات الأمنية المضافه ازدادت صعوبة استخدام الشبكات وازدادت بطأ مما يؤثر على سهولة الاستخدام**

- أنواع التهديدات لأمن الشبكات :

١- الهجوم غير التقني : الهندسة الاجتماعية Social Engineering

تنطوي الهندسة الاجتماعية على استخدام المهارات الاجتماعية والتفاعل الشخصي لجعل شخص ما يكشف عن معلومات ذات صلة أمنيه او تنفيذ إجراءات تعتبر خطر على امن نظم معلومات المنظمة وقد تسهل الهجوم عليها .

وظيفة الهندسة الاجتماعية هي اقناع الضحية على ان يكون مفيد

الأساليب المستخدمة لمكافحة الهندسة الاجتماعية :

١- تعليم و تدريب الموظفين لمواجهة أنواع مختلفة من الهندسة الاجتماعية

٢- وضع السياسات و الإجراءات الواجب اتباعها في حال حدوث خطر

٣- القيام باختبارات للاختراق و الإيقاع بالموظفين

-

٢- الانتحال : Spoofing
استخدام هوية كيان ما (مستخدم ، حساب ، عملية ، جهاز) على الشبكات مما يسمح للمهاجم العمل تحت هوية هذا الكيان .

٣- Session hijacking
هو اعتراض وتولي عملية اتصال بدأت من قبل كيان اخر .

٤- Man-in-the-Middle Attack
هذا الهجوم مشابه لـ Session hijecking، والذي فيه يتطفل كيان واحد بين اثنين اخرين .

٥- Denial-of-service (Dos) attack
يستهدف المهاجم كمبيوتر معين او شبكة الاتصالات او موقع بهدف تعطيل عملهم

٦- Distributed Denial-Of-service (DDoS) Attack
في هاذا النوع من الهجوم يحاول المهاجم الوصول الى العديد من اجهزة الكمبيوتر على شبكة الإنترنت قدر ما يستطيع من خلال الاستفادة من الثغرات الأمنية او الضعف فيها ويقوم المهاجم بالسيطرة على هذه الأجهزة .

حماية الشبكات:

ان الشبكات تتعرض لانواع عديده من الهجمات مما يتطلب العديد من الضوابط لحماية الشبكات.

اهم عناصر حماية الشبكات:

١- التأكد من الهويه:

في البداية يجب تحديد الفرق بين التعريف بالهويه Indentification. والتأكد من الهوية Authentication.

التعريف بالهوية Indentification مصطلح للشخصالذي يقدم هويته الفريده للنظام والتي تفرق بينه وبين الاخرين مثلاً User Name

التأكد من الهوية

مصطلح يتناول جانب "كيف يمكنك اثبات هويتك اللي تدعى أنك هي.

أنواع التأكد من الهوية:

١- شيء يعرفه الشخص (كلمة المرور)

٢- شيء يملكه الشخص (البطاقة الذكية)

٣- شيء يمثل الشخص (بصمات الأصابع/ الصوت)

- ٢- التشفير:

هو عملية تحويل النص العادي الى نص مشفر لا يمكن قراءته من قبل اي شخصّ غير المرسل والمرسل اليه

- الهدف من التشفير هو حماية المعلومات المخزنه و نقل المعلومات بأمان.

ويعتبر التشفير من اهم التقنيات المستخدمة لأمن الشبكات ومن المهم استخدام نظام تشفير قوي.

انواع التشفير:

١- التشفير بالمفتاح الخاص:

يستخدم المرسل والمرسل اليه نفس المفتاح لتشفير Encryptionوفك تشفير Decryptionالرساله حيث يتشاركان المفتاح دون الكشف عنه لاحد.

- مشاكل التشفير بالمفتاح الخاص:

١- يجب ان يحصل المرسل والمرسل اليه على المفتاح ولا يمكن القيام بعملية المبادلة عن طريق شبكة الانترنت ٢- الحاجه الى عدد كبير من المفاتيح اعتماداً على عدد مجموعات من الاطراف للتواصل

٣- عند تلقي رسالة مشفرة بهذه الطريقة لا يمكن للمرء ان يكون متأكداً من هو مرسلها الحقيقي فقد يكون اي شخص يعرف المفتاح السري

٢- مفتاح التشفير العام:

يستخدم هذا الاسلوب مفتاحيين رقميين متصلين رياضياً مفتاح خاص ومفتاح عام
يتم الاحتفاظ بالمفتاح الخاص بصوره سريه من قبل المالك
ويمكن استخدام كلا المفتاحين لتشفير وفك الرساله بشرط عندما يُستخدم احد المفاتيح لتشفير الرساله لا يمكن استخدام نفس المفتاح لفك تشفيرها

الاستخدامات الرئيسيه لهذه التقنيه هي :

١/لتحقيق الخصوصية :
اذا كان العميل يريد ان يرسل رساله الى التاجر بحيث يستطيع التاجر فقط قراءتها
٢/لإثبات هوية المرسل:
إذا كان العميل يريد أن يرسل رساله إلى تاجر ويريد أن يثبت أنه هو فعلا من ارسلها
فوائد استخدام مفتاح التشفير العام:
١/يمكن للمستخدم استخدام نفس زوج المفتاح الخاص والعام لكل نشاطاته، لان المفتاح الخاص به يبقى دائما سري
٢/بما إن المستخدم فقط يعرف المفتاح الخاص به هذا يسمح باستخدام التوقيع الرقمي

٣-الجدار الناري :

هو حاجزا بين شبكتين الشبكه الداخلية للمنظمه (الشبكة الموثوق بها) والشبكه الخارجيه (الانترنت) وتقوم الجداران الناريه بفحص الحزم الوارده والصادره وفقا للسياسات المخزنه في الجدار الناري، و بالتالي يتم السماح لهذه الحزم بالمرور او منعها.

- احدى تقنيات الجدار الناري هي فحص الحزم، حيث يتم فحص عناوين الكمبيوترات المرسل و المرسل اليه و البوابات التي مرت بها الحزم ، و بالتالي تمنع او تسمح دخول الحزم استنادا الى مجموعة من القواعد المحددة سلفا.

- **الجدار الناري الشخصي :**
  هو برنامج يتم تشغيله على الكمبيوتر لمنع حركة المرور غير المرغوب فيها فهو يراقب حركة المرور الوارده والصادره لتلك الشبكه.

٤- أنظمة كشف التسلل:

هو برنامج او جهاز يرصد حركة المرور عبر الشبكه او على الكمبيوتر ويراقب اي نشاط مشبوه غير مرغوب فيه او غير مشروع أو ضار ينتهك سياسة الامن، لتقوم باتخاذ الإجراءات بصورة آلية بناء على سياسات محددة

٥- الشبكات الخاصه الافتراضيه

يمكن للمنظمه بناء شبكه خاصه باستخدام نظام من خطوط الاتصالات المملوكه او المؤجره ولكن مثل هذه الشبكات تكلف كثيرا لذلك تستخدم الكثير من المنظمات الشبكات للخاصه الافتراضيه

الشبكه الخاصه الافتراضيه :

هي شبكه تستخدم شبكه الانترنت العامه لنقل المعلومات ولكن تبدو انها خاصه من خلال استخدام التشفير لتغيير معالم الاتصالات و التوثيق لضمان عدم العبث بالمعلومات و ضوابط الوصول للتحقق من هوية أي شخص يقوم باستخدام الشبكة.

يمكن استخدام الشبكات الخاصه الافتراضيه في ثلاث تطبيقات:

١ الوصول عن بعد :

يتمكن الموظفين العاملين عن بعد الوصول الى الشبكه الداخليه للمنظمه بشكل آمن

٢ المكاتب المتباعده :

انشاء شبكه امنه خاصه بين مكاتب متباعده تابعه للمنظمة

٣ اكسترانت:

تقوم المنظمات باجراء الاعمال التجاريه الالكترونيه مع الشركاء التجاريين والموردين والزبائن عبرها

اداره المخاطر الامنيه

هي عمليه منهجيه لتحديد احتمال وقوع الهجمات الامنيه المختلفه وتحديد الاجراءات اللازمه لمنع او تخفيف تلك الهجمات

مراحل اداره المخاطر الأمنية:

المرحله الاولى التقييم:

عن طريق تحديد الأصول المهمه و نقاط الضعف في نظام البمعلومات و التهديدات المحتملة لهذه الثغرات الأمنية

المرحله الثانيه التخطيط:

الهدف من هذه المرحله هو التوصل الى مجموعة من السياسات التي تحدد نوع التهديدات

المرحله الثالثه التنفيذ:

اختيار و تركيب التقنيات معينه لمواجهة كل من التهديدات ذات الأولوية العاليه

المرحله الرابعه الرصد والمتابعه:

يتم قياس مدى تحقيق الاجرادات الأمنية للاهداف الموضوعه.