



الحاسوب
الكورس الاول
امن المعلومات
والجرائم الالكترونية
الجزء الثاني

م.م. زينة رجب الالوسي
كلية القانون/ جامعة بغداد
المرحلة الثانية

وسائل تحقيق أمن المعلومات

وسائل تحقيق أمن المعلومات هي مجموعة الآليات والإجراءات والأدوات التي تستخدم للوقاية من المخاطر أو تقليل الخسائر بعد وقوع الحدث على المعلومات وأنظمتها.

وتختلف وسائل الحماية من حيث الطبيعة والغرض وفيما يلي بعض هذه الآليات:

- نظم الإنذار المبكر Awareness system
- التوثيق من شخصيات المستخدمين Authentication
- التحكم في الوصول Access Control
- تشفير البيانات Encryption
- برامج كشف ومعالجة الفيروسات Antivirus
- الجدار الناري Firewall
- النسخ الاحتياطية Backup

❖ نظام الإنذار المبكر:

يستخدم في هذه الآلية أجهزة حساسة (Sensors) للإنذار المبكر ضد السرقة والحريق والكوارث الطبيعية مثل الزلازل والبراكين والفيضانات, وأجهزة حساسة ضد المواد المشعة والمواد السامة كما تشمل كاميرات المراقبة الموصلة مع شاشات العرض (Monitors) ومع أنظمة الهاتف النقال.

❖ التوثق من شخصيات المستخدمين

هو وسيلة يتم بها التحكم في الأشخاص المسموح لهم بالوصول للمعلومات والنظم العاملة عليها, إذ أن الوصول للمعلومات بواسطة الأشخاص غير المصرح لهم بذلك يؤدي لفقد سرية المعلومات وربما صحتها واتاحتها والذي يؤدي بدوره للخسارة المالية والقانونية وفقدان ثقة الزبائن. وتتكون هذه الآلية من عمليتين هما:

١. التعرف على الشخص Identification

٢. التحقق من الشخص Authentication

وتستخدم عملية التحقق من المستخدمين التقنيات التالية :

- بطاقات الهوية العادية Identity Cards
- كلمات السر Passwords
- البطاقات الذكية المستخدمة للتعريف Smart Cards
- وسائل التعرف البيولوجية Biological Identification التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنانه البيولوجي مثل بصمة الاصبع أو الوجه أو بصمة العين أو الصوت Voice أو بصمة الاوردة الدموية.
- المفاتيح المشفرة Encryption Keys
- الأقفال الإلكترونية Electronic Locks التي تؤمن بوابات الدخول والخروج .

ومن أقوى وسائل التعرف والتوثق تلك التي تجمع بين تقنيتين أو أكثر من التقنيات السابقة . وأيا كانت وسيلة التعرف التي سيتبعها نظام التوثق authentication ، فإنها تخضع لنظام أمن وشروط

- وإرشادات أمنية يتعين مراعاتها ، فكلمات السر على سبيل المثال وهي الأكثر شيوعاً من غيرها من النظم، تتطلب أن تخضع لسياسة مدروسة وإرشادات يمكن تلخيصها في الآتي:
١. كل كلمات المرور يجب أن يتم تغييرها بشكل دوري (٦٠ يوم على الأقل حسب المواصفات العالمية)
 ٢. يجب أن تلتزم بالحد الأدنى للطول وهو ثمانية حروف (حسب القياسات الدولية).
 ٣. يجب أن تتركب من خليط من الحروف (كبيرة وصغيرة) والأرقام والرموز.
 ٤. يجب أن لا ترتبط بشكل مباشر وسهل التخمين بأي معلومات خاصة بالمستخدم مثل اسم المستخدم، اللقب، تاريخ الميلاد... الخ
 ٥. يجب عدم تفعيل الدخول التلقائي (auto login) لأنظمة الحاسب أو تذكير كلمات المرور في حالات الأنظمة الحساسة.
- وكذلك باقي التقنيات ، حيث كل تقنية تحتوي على شروط أمنية يجب مراعاتها لتحقيق الهدف.

❖ التحكم في الوصول Access Control

حق الوصول هو أحد الوسائل المُستخدمة لحماية البيانات ، وهو عبارة عن حق يُمنح إلى مُستخدم نظام معلومات (جوازات، دوائر أمنية، مرور، أحوال مدنية، وكالات سفر أو خطوط طيران...)، بحيث يمكن للموظف استخدام هذا الحق لخدمة العميل أو المواطن مثل: (عمليات التجديدات، الحجوزات...) أي أن له الحق في القيام بإجراء معين في منطقة معينة من نظام المعلومات لا يمكن له أن يتعداها، ويجب أن تكون العمليات مُسجلة بحيث يمكن معرفة اسم الموظف أو المُستخدم المسؤول عن حدوث خطأ معين في وقت معين على النظام.

❖ تشفير البيانات Data Encryption

يشير مصطلح "تشفير" إلى تحويل النص العادي (Plaintext) من شكل مقروء إلى هيئة نص مرمز (Ciphertext) وغير مقروء بواسطة خوارزميات التشفير ومفاتيح التشفير، ثم إعادة فك الترميز (Decryption) وإعادة النص إلى أصله بواسطة الخوارزميات أيضا ومن قبل الأشخاص المسموح لهم بذلك (الذين يملكون أدوات فك التشفير).

أنواع التشفير Encryption Types

يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين:

- تشفير متماثل Symmetric Encryption

- تشفير غير متماثل Asymmetric Encryption

- تشفير متماثل Symmetric Encryption:

يعرف أيضا بتشفير المفتاح الخاص حيث يستخدم فيه نفس المفتاح لتشفير الرسالة وفك التشفير. يجب أن يتفق الطرفان على مفتاح التشفير مما يسبب مشكلة خاصة عند إرسال المفتاح عبر الشبكات فربما يحدث التقاط لهذا المفتاح وبالتالي كشف المراسلات بين الطرفين لذلك يجب تبادل المفاتيح بطريقة تضمن سريتها.

- تشفير غير متماثل Asymmetric Encryption

يعرف أيضا بتشفير المفتاح العام حيث يستخدم فيه زوج من المفاتيح أحدهما لتشفير الرسالة والآخر لفك التشفير.

- خوارزميات التشفير Encryption Algorithm

هي عبارة عن صيغ رياضية تستخدم لتحويل الرسالة العادية إلى مكونات مشفرة Ciphared ويمكن وصف العمليتين رياضيا بالآتي :

من أمثلة خوارزميات التشفير:

• خوارزمية الإحلال Substitution :

يتم فيها استبدال لمكونات الرسالة الأصلية بتبديل قيمة محل الأخرى مثلا تبديل الحرف الأول بالثالث كما في المثال التالي:

Plaintext=ABCDEFGHIJKLMN**OP**QRSTUVWXYZ

Ciphertext=DEFGHIJKLMN**OP**QRSTUVWXYZABC

• خوارزمية الخط المتعرج (Zig_Zag): في هذه الخوارزمية يقسم النص الواضح الى أطوال ثابتة ويتم توزيع الأحرف بالشكل التالي :

١. حدد عدد الصفوف التي ستستخدم لتشفير النص حيث أن عدد الصفوف يعد مفتاح التشفير ولا يلزمنا معرفة عدد الأعمدة .
٢. إملأ الفراغ في النص الأصلي بمثلث مقلوب (ملاحظة: استخدام المثلث المقلوب بديلا للفراغ لتسهيل الحل فقط).
٣. انشئ جدولاً يعتمد على عدد الصفوف (مفتاح التشفير).
٤. وزع أحرف النص المراد تشفيره بشكل قطري
٥. اضع مثلث مقلوب لتساوي الاطوال

مثال: شفر النص التالي :

I love my country

علما بأن مفتاح التشفير = ٢ (صفين).

I		L		v	▼		y		c		u		t		y	
	▼		o		e		m	▼		o		n		r		▼

هنالك انواع اخرى كثيرة لخوارزميات التشفير منها خوارزمية الإزاحة Transportation RSA,DES وغيرها.

❖ برمجيات كشف ومقاومة الفيروسات Antivirus

يقصد بها البرمجيات التي تستخدم لمكافحة البرامج الخبيثة وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط بل هو اصطلاح يطلق على هذا النوع من البرمجيات بغض النظر عما إذا كان فيروس فعلاً أو دودة أو Trojan horse أو أي نوع آخر من أنواع البرامج الخبيثة. ومن أشهر البرامج المضادة للفيروسات (Norton, McAfee , Kaspersky) ويجب تحميل النسخة الأصلية وذلك لأن هذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة، وتكون عديمة الفائدة في مواجهة الفيروسات الجديدة إلا إذا تم تحديث البرنامج من موقع الشركة المنتجة أو المصنعة له على شبكة الإنترنت، ولا يتم التحديث بشكل صحيح إلا إذا كان البرنامج أصلياً.

❖ الجدران النارية Firewall

هي عبارة عن أجهزة hardware وبرامج Software تعمل على أسلوب فلترة وتصفية حركة البيانات الواردة والصادرة من وإلى الشبكة اعتماداً على قوانين ومعاملات بسيطة. تطورت الجدران النارية بشكل سريع منذ نشأتها وحتى الآن. كانت مثل هذه الجدران النارية توضع في مواقع بين الشبكات للحد من انتشار المشاكل التي يواجهها جزء من الشبكة إلى الأجزاء الأخرى . ظهرت أول الجدران النارية للشبكات في عام ١٩٨٠ وكانت عبارة عن موجهات Routers تستخدم في تقسيم هذه الشبكات إلى شبكات محلية (LAN) صغيرة .

❖ النسخ الاحتياطي Backup

النسخ الاحتياطي عملية اساسية يجب القيام بها بشكل دوري ومنتظم حسب أهمية الملفات، هذا ينطبق على المستخدم المنزلي والملفات على أجهزة الحاسوب في الشركات والمدارس إلى الملفات الحساسة . بسبب عواقب فقدان الملفات نتيجة حادث مثل حريق أو فيضانات، أو تلف أحد مكونات الحاسوب مثل القرص الصلب الحامل للملفات، أو تعرض الحاسوب إلى السرقة أو تخريب متعمد كأن يخترق من قبل قرصنة حاسوب . يصعب على صاحب الملفات استرجاعها وإعادة إنشائها خاصة إذا كانت كبيرة الحجم ومهمة، فيتم عمل نسخ احتياطية من تلك الملفات على وسائط خارجية مثل قرص مضغوط (DVD) أو قرص صلب خارجي ويتم تكرار العملية حسب إستراتيجية تحددها أهمية الملفات وحجمها وتوفر وسائط التخزين الخارجية .