أمن المعلومات

Information Security

وسائل تحقيق أمن المعلومات هي مجموعة الآليات والإجراءات والأدوات التي تستخدم للوقاية من المخاطر أو تقليل الخسائر بعد وقوع الحدث على المعلومات وأنظمتها.وتتعدد وسائل الحماية من حيث الطبيعة والغرض وفيما يلي بعض هذه الآليات:

- نظم الإنذار المبكر Awareness system
- التوثق من شخصيات المستخدمين Authentication
- التحكم في الوصول Access Control
- تشفير البيانات Encryption
- برمجيات كشف ومعالجة الفيروسات Antivirus
- أمن شبكات الاتصال Network Security

a. نظام المراقبة وسجلات الدخول Monitoring and Logging in
b. نظام سجلات مراجعة الأداء Audits

نظام الإنذار المبكر:

يستخدم في هذه الآلية أجهزة حساسة (Sensors) للإنذار المبكر ضد السرقة والحريق والكوارث الطبيعية مثل الزلازل والبراكين والفيضانات ،وأخرى أجهزة 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 Confidentiality المعلومات وربما صحتها واتاحيتها والذي يؤدي بدوره للخسارة المالية والقانونية وفقدان ثقة الزبائن.وتتكون هذه الآلية من عمليتين هما (1)Identification(٢)Authentication

وتستخدم عملية التحقق من المستخدمين التقنيات التالية :

- بطاقات الهوية العادية Identity Cards
- كلمات السر Passwords
- الشهادات الرقمية Certificates
- البطاقات الذكية المستخدمة للتعريف Smart Cards
- وسائل التعريف البيولوجية Biological Identification التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي مثل بصمة اليد fingerprint أو الجلد Skin print أو بصمة العين Iris أو الصوت Voice .
- مختلف أنواع الأنظمة التي تولد generate كلمات سر آنية أو وقتية متغيرة الكترونيا
- المفاتيح المشفِرة Encryption Keys
- الأقفال الإلكترونية Electronic Locks التي تؤمن بوابات الدخول والخروج .

وسائل التعريف السابقة كما هو لاحظ تختلف تبعا للتقنية المستخدمة في القطاع والتي تختلف من طريقة عادية تستخدم موظف الاستقبال وموظف الأمن المسلح (Armed Guard) إلى استخدام النظم و الشبكات ونظم قواعد البيانات و قطاعات الأعمال الإلكترونية عن طريق الانترنت وبشكل عام ، فان هذه الوسائل تتوزع إلى ثلاثة فئات هي عوامل التحقق من المستخدمين:-

- **شيء ما تملكه مثل البطاقة الذكية (Smart Card) .**
  (Some thing you have)
- **شيء ما تعرفه مثل كلمات السر (Password)أو الرقم الشخصي(PIN)**
  (Some thing you know)
- **شيء ما يرتبط بك أو موجود فيك مثل بصمة الإصبع أو بصمة العين والصوت**
  . (fingerprint, iris scan ,voice)
  (Some thing you are)

ومن أقوى وسائل التعريف والتوثق تلك التي تجمع بين عاملين أو أكثر من العوامل السابقة . مثل استخدام بطاقة الصراف الآلي (ATM) والتي تتبع لفئة (some thing you have) مع الرقم المعرف (PIN) والذي يتبع لفئة (some thing you know).

وأيا كانت وسيلة التعريف التي سيتبعها نظام التوثق authentication ، فإنها تخضع لنظام أمن وشروط وإرشادات أمنية يتعين مراعاتها ، فكلمات السر على سبيل المثال وهي الأكثر شيوعا من غيرها من النظم ، تتطلب أن تخضع لسياسة مدروسة وإرشادات يمكن تلخيصها في الآتي:

- كل كلمات المرور حتى الابتدائية منها(Initial Password)
  ١. يجب أن يتم تغيرها 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 تركب من خليط من الحروف(كبيرة وصغيرة) والأرقام والرموز
  ٤. يجب أن لا ترتبط بأي معلومات خاصة بالمستخدم أو اسم الحساب(Account)مثل اسم المستخدم ،اللقب،تاريخ الميلاد...الخ

وهناك عبارة سهلة يمكن إتباعها وهي(Password must be difficult to guess easily remembered) أي بمعنى صعب على الآخرين تخمينها وفي نفس الوقت سهلة التذكر على صاحبها لان نسيان كلمة المرور في حد ذاته خرق لعنصر الفائدة Utility حسب نموذج "دون باركر"

٥. يجب حفظ أرشيف بكلمات المرور حتى لا يعاد استخدامها من جديد

- يجب تشفير كلمات المرور المحفوظة(Stored Password)
- يجب عدم إفشاء اسم المستخدم وكلمة المرور مهما كان السبب
- الرخصات الأمنية (مثل البطاقات الذكية)يجب إعادتها عند إنهاء العمل
- إذا كان هناك أدنى شك في تفشي كلمة المرور يجب تغيرها فورا
- مدير النظام يجب أن يستخدم كلمات مرور قوية (Strong Password)
- يجب عدم تفعيل الدخول التلقائي(auto logon) لأنظمة الحاسب أو تذكير كلمات المرور(Password remembering) في حالات الأنظمة الحساسة
- يجب استخدام شاشات التوقف المحمية بكلمات المرور(password protected) ونظام الإغلاق التلقائي(auto logoff).

أخيرا وفيما يتعلق بنظام التوثق من المستخدمين والذي يستخدم عمليتي المطابقة Identification والتوثق Authentication تجدر الإشارة هنا للتفريق بين العمليتين فعملية المطابقة هي مثلا أن

تسأل " من أنت؟" فتقول مثلا "أنا أحمد علي محمد" عملية التوثق تثبت ذلك مثلا أن يقال لك "ابرز بطاقتك" أو "أدخل كلمة المرور".

التحكم في الوصول Access Control

عن طريق هذه الطريقة يتم تحديد مستخدمي النظام والموارد Resources المسموح لهم بها وغير المسموح لهم بها وإعطائهم صلاحيات الوصول إليها عن طريق نظام الترخيص Authorization.احد النماذج المستخدمة في تحديد عملية الوصول وتحديد الصلاحيات ما يعرف بمصفوفة التحكم في الوصول Access Control Matrix والمعتمدة لتطبيق القواعد الأمنية في نظم التشغيل وقواعد البيانات اليوم وفيما يلي وصف لهذه المصفوفة:

جدول١ (مصفوفة التحكم في الوصول)

تنظم المصفوفة العلاقات بين أجزاء النظام على هيئة ترتيب ثلاثي يتضمن الكيانات Entities والموارد Resources وصلاحيات الوصول Access Privileges انظر الجدول الآتي:

حيث:

Object / Subject	O1 (File1)	O2 (File2)	O3 (File3)	O4 (printer)
S1	Read		Read	
S2	Execute	Read		Print
S3	Execute			Print
S4	Read/write	Read	Read	

- Subject تمثل صفوف المصفوفة وهي مجموعة مستخدمي النظام والعمليات
- Object تمثل الأعمدة وهي مجموعة موارد النظام ملفات ،مجلدات،عناصر قاعدة البيانات،طابعات ...الخ.
- Access Privileges وتعرف أيضا بـ Access Type وتمثل الخلايا (تقاطع الصفوف مع الأعمدة) وهي طريقة الوصول للموارد مثلا قراءة ،كتابة ،تنفيذ ،طباعة ...الخ

تعرف المصفوفة السابقة بقانون الترخيص Authorization Rule كما تعرف بالترتيب الثلاثي لان كل حالة فيها تتكون من ثلاث عناصر (S,O,T) أو (Subject, Object, Access Type) فمثلا قانون الترخيص للمستخدم S1 على الملف file3 تكتب هكذا (S1,File3,Read).

وعليه عند إنشاء عملية معينة على كائن (Object) معين بواسطة المستخدم Subject فانه يتم البحث عن الثلاثية السابقة في جدول الصلاحيات العام فإذا أشارت الثلاثية لجواز العملية يتم تنفيذها فورا وان لم تشير لذلك يتم منع العملية من التنفيذ.

تشفير البيانات Data Encryption

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

أهداف التشفير (Cryptographic Objectives):

١- الوثوقية (Confidentiality) : هي عبارة عن خدمة معينة تمنع من خلالها معرفة محتويات المعلومات عن جميع المشتركين عدا الأشخاص المخولين بامتلاك هذه المعلومات . يعتبر مفهوم الأمنية (Secrecy) مرادفا لكل من الوثوقية والخصوصية (Privacy).

٢- تكامل البيانات (Data Integrity): عبارة عن خدمة موجهة لإغراض احتواء التغييرات الغير مسموح بها (Unauthorized) للبيانات ولتحقيق هذا الهدف يجب تمتلك الإمكانية لكشف معالجة البيانات من قبل الأطراف الغير مخولة. تشمل معالجة البيانات عمليات مثل الحشر (Insertion)، الحذف(Deletion) والإحلال (Substitution). يجب أن يكون مستقبل الرسالة قادرا على إثبات أن العبارة لم يتم تحويرها أثناء الإرسال و أن العدو يجب أن لا يكون قادرا على إحلال عبارة كاذبة بدلا من عبارة شرعية.

٣- إثبات الشخصية (Authentication) :عبارة عن خدمة أو وظيفة تتعلق بتحقيق التعريف (Identification) ،هذه الوظيفة تطبق على كل من المشتركين في الاتصال (Two Parties) وعلى المعلومات أيضا حيث أن الأطراف المشتركة عند الاتصال عليها أن تعرف بعضها إلى

البعض الأخر . أما ما يخص المعلومات المستلمة فيجب أن تطابق شخصياً المعلومات الأصلية التي أرسلت وكذلك تاريخ إرسال المعلومات ومحتويات المعلومات ووقت الإرسال، لهذه الأسباب يقسم التشفير اعتماداً على الخاصية أعلاه إلى صنفين رئيسين هما :

أ – إثبات شخصية الكينونة (Entity Authentication) .

ب – إثبات شخصية مصدر البيانات (Data Origin Authentication).

أن طريقة إثبات شخصية مصدر البيانات تزودنا ضمنياً بتكامل البيانات (Data Integrity).

نستنتج من هذا انه في إثبات الشخصية يجب أن يكون ممكنا لمستقبل العبارة أن يتحقق من مصدرها ; وان العدو يجب أن لا يكون قادرا على التنكر بأنه شخص معين أخر.

٤–عدم الإنكار (Non- Repudiation) : عبارة عن خدمة أو وظيفة والتي تمنع أي كينونة (Entity) من أن ينكر أي تعهد أو عمل سابق تم أجرائه . لذلك عند حصول مثل هذا النزاع (Dispute) بين الأطراف المشتركة في إنكار ما تم اتخاذه من أعمال فيجب توفير وسيلة معينة لحل هذا النزاع. يتم توفر هذه الوسيلة من خلال أجراء معين يتضمن إشراك طرف ثالث موثوق. يجب على المرسل أن لا يكون قادرا على الإنكار الكاذب بعد فترة ويدعي انه قد أرسل عبارة.

خوارزميات التشفير Encryption Algorithm

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

وصف الدالة الرياضية لعملية التشفير : **C=E(P,K)** وهي تعني تشفير الرسالة الأصلية لتحويلها إلى نص مشفر باستخدام المفتاح K

وصف الدالة الرياضية لعملية فك التشفير : **D(E(P,K),K)** وهي تعني إعادة الرسالة المشفرة إلى أصلها بعد تحويلها بواسطة المفتاح K الثاني

حيث :

- C تعني الرسالة المشفرة Ciphered
- E تعني عملية التشفير Encryption
- P تعني نص الرسالة Plaintext
- K ترمز لمفتاحي التشفير وفك التشفير
- D تعني عملية فك التشفير Decryption

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=ABCDEFGHJKLMNOPQRSTUVWXYZ

Ciphertext=DEFGHIJKLMNOPQRSTUVWXYZABC

خوارزمية الإزاحة Transportation:

حيث يتم إزاحة الحروف الموجودة في النص تبعا لمفتاح معين وبمعنى آخر يتم إعادة ترتيب الرسالة الأصلية مما يؤدي لإخفائها.

مثال:

Plaintext=call home

Ciphertext=local eohm

هنالك أمثلة كثيرة لخوارزميات التشفير منها RSA,DES

أنواع التشفيرEncryption Types

يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين تشفير متماثلSymmetric Encryption وتشفير غير متماثل Asymmetric Encryption:

تشفير متماثل Symmetric Encryption:

يعرف أيضا بتشفير المفتاح الخاص Private Key Encryption حيث يستخدم فيه نفس المفتاح لتشفير الرسالة ولفك 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 Public Key Encryption حيث يستخدم فيه زوج من المفاتيح أحدهما لتشفير الرسالة والآخر لفك التشفير يعرف الأول بالمفتاح العام Public Key سمي بذلك لأنه يكون معروف للمستخدمين في البيئة المعينة ويستخدم لتشفير الرسائل ،أما الثاني فيعرف بالمفتاح الخاص Private Key سمي بذلك لأنه معروف لمستخدم واحد فقط هو مالكه ويستخدم لفك الرسائل المشفرة بالمفتاح العام المقابل له.يعاب على هذه الطريقة كثرة المفاتيح المستخدمة في التشفير وفك التشفير.

مثلا:

إذا أراد المستخدم A إرسال رسالة مشفرة إلى المستخدم B باستخدام طريقة **التشفير غير المتماثل** فان A عليه التحصل على المفتاح العام لـ B ثم تشفير الرسالة وإرسالها له وطالما الرسالة تم تشفيرها بالمفتاح العام لـ B فان المفتاح الخاص له فقط هو الذي يمكنه فك تشفير الرسالة.وبالمثل إذا أراد B إرسال رسالة إلى A فعليه أن يتحصل على المفتاح العام لـ A ثم تشفير الرسالة وإرسالها إلى A الذي يستخدم مفتاحه الخاص لفك تشفير الرسالة.

برمجيات كشف ومقاومة الفيروسات Antivirus

مضادات الفيروسات Virus countermeasures

يقصد بها البرمجيات التي تستخدم لمكافحة البرامج المصممة خصيصاً للإضرار بنظام الحاسب الآلي وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط بل هو اصطلاح يطلق على هذا النوع من البرمجيات.وفي كثير من الأحيان يطلق على كل البرامج الضار اسم فيروس بغض النظر عما إذا كان فيروس فعلاً أو دودة أو Trojan horse أو أي نوع آخر من أنواع البرمجيات الضارة.

هناك سباق مستمر بين مطوري البرامج الضارة وبرامج مضادات الفيروسات،فكلما وجد برنامج فعال لمكافحة الفيروسات الحالية،يتم إنتاج نوع جديد من الفيروسات لا يعالجها البرنامج الحالي.

العلاج الناجع للفيروسات هو منعها أو عدم السماح لها بالدخول لنظام الحاسب إلا أن تحقيق ذلك يعد من الصعوبة بمكان ولكن إذا حدثت الإصابة بالفيروس فهناك إجراءات يمكن اتخاذها في مواجهة الفيروس أو لمعالجته وتقليل عواقبه هي عبارة عن خيارات يتم اختيار الأنسب منها والذي يوفر أعلى حماية وأقل تكلفة .تتلخص أهداف مضادات حماية الفيروسات في الآتي:

- **الاكتشاف Detection** هو تحديد حدوث الإصابة بالفيروس وتحديد مكانه
- التعرف على الفيروس **Identification** عند اكتشاف الإصابة تأتي مرحلة التعرف على نوع الفيروس الذي سبب الإصابة وذلك من خلال علامات معينة في كود الفيروس أو بسلوكه الذي يقوم به في النظام.
- **إزالة الفيروس Virus Removal** بعد التعرف على نوع الفيروس تتم إزالته من الملف المصاب وإرجاع الملف إلى وضعه الأصلي وتَعَقُّب كل النسخ الأخرى من الفيروس للحد من انتشاره مرة أخرى.

إذا أسفرت مرحلة الاكتشاف عن وجود فيروس لم يتم التعرف على نوعه يجب اللجوء لخيار التخلص discard من البرنامج المصاب ثم إعادة تركيبه مرة أخرى باستخدام النسخ الاحتياطية.

هناك سباق سريع في تصميم وتطوير الفيروسات ومضادات الفيروسات ،وبعكس الأنواع القديمة من المضادات، التي كانت بسيطة،فان تعقيدا كبيراً قد طرأ على مضادات الفيروسات نسبة لتعقيد الفيروسات التي تعالجها.

يمكن التعرف على الأجيال التي تطورت خلالها الفيروسات في العرض التالي:

الجيل الأول الماسحات البسيطة Simple Scanner التي تتميز بالآتي:

- يحتاج البرنامج المضاد الفيروس علامة معينة signature للتعرف على الفيروس
- في بعض أنواعها يحتاج البرنامج لقياس حجم الملف واكتشاف التغير في الطول

الجيل الثاني الماسحات الموجهة Heuristic Scanner وهي تتميز بالآتي:

- استخدام طرق موجهة للبحث عن الإصابات المتوقعة
- بعضها يبحث عن كود فيروسي معين داخل الملفات فإذا وُجد فهذا يعني إصابة الملف المحدد.
- يمكن أيضا اختبار صحة Integrity الملفات باستخدام قيمة الـ Checksum[1] الموجودة مع الملفات فإذا كان الفيروس قد عدل الملف دون أن يعدل قيمة الـ Checksum فان البرنامج المضاد للفيروسات سيكتشف أن هناك إصابة نسبة لاختلاف قيمة checksum المخزنة مع بيانات الملف.

الجيل الثالث الماسحات البسيطة Activity Trap يتم اكتشاف فيروسات الذاكرة بالأفعال التي تقوم بها في النظام وليس بتركيبها

الجيل الرابع الحماية الكاملة Full-featured protection

تستخدم كل التقنيات السابقة في حزمة واحدة وتحتوي مقدرات كبيرة تحد من انتشار الفيروسات ونشاطها التخريبي.

تقنيات متقدمة لمضادات الفيروساتAdvanced antivirus technique:

Generic Decryption

وهذه التقنية تمكن مضادات الفيروسات من التعرف بسهولة على الفيروسات المعقدة (مثل الدودات متعددة الأشكال) وتحتوي ثلاثة عناصر هي:

- CPU emulator وهو برنامج يعمل كحاسب ظاهري يقوم بتنفيذ البرامج بدلا من تنفيذها بواسطة المعالج الأصلي
- Virus signature scanner وتبحث عن الفيروسات المعروفة
- Emulation control module يتحكم في تنفيذ الكود الهدف

تعمل الوحدات الثلاث في التعرف على الفيروس في تحكم تام لمكافحة الفيروسات

أمن شبكات الاتصال Network Security

المقصود به الوسائل التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة ، وتشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين ، أو قوائم المستخدمين ، أو تحديد الميزات وأنواع الصلاحيات أو غير ذلك من الإجراءات والأدوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة ويمكن تفصيلها في الآتي:

- مجموعة الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المصدق لهم بذلك وتهدف إلى تحقيق سرية المعلومات وتشمل تقنيات تشفير المعطيات والملفات , وإجراءات حماية النسخ الاحتياطية والحماية المادية للأجهزة ومكونات الشبكات devices واستخدام الفلترات والموجهات Routers .
- مجموعة الوسائل الهادفة لحماية التكاملية (سلامة المحتوى) وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مصدق لها بذلك ، وتشمل من بين ما تشمل تقنيات الترميز والتواقيع الإلكترونية Digital signature وبرمجيات مضادات الفيروسات وغيرها .
- مجموعة الوسائل المتعلقة بمنع الإنكار (إنكار التصرفات الصادرة عن الشخص) وتهدف هذه الوسائل إلى ضمان عدم قدرة شخص المستخدم من إنكار انه هو الذي قام بالتصرف ، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط ، وترتكز هذه الوسائل في الوقت الحاضر على تقنيات التوقيع الإلكترونيDigital signature وشهادات التوثيق Certificate .
- وسائل مراقبة الاستخدام وتتَّبِع طريقة سجلات الدخول والأداء (الاستخدام) وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين ، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام مثل سجلات الـ Audits والذي تمتت مناقشته في درس التطفل والهجوم Intrusion & Attack.

يمكن تلخيص الوسائل السابقة في الآليات الآتية:

- **الجدران النارية Firewall :**

هي عبارة عن أجهزة hardware وبرامج Software تعمل على أسلوب فلترة وتصفية حركة البيانات الواردة والصادرة من والى الشبكة اعتمادا 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 .

وقد تم استخدام أول الجدران النارية لتحقيق الأمن في أوائل التسعينات ، وكانت عبارة عن موجهات لبروتوكول **IP** مع قوانين فلترة كانت بسيطة كما في السيناريو التالي :

اسمح لفلان بالدخول والنفاذ إلى الملف التالي . أو امنع فلان (أو برنامجا) من الدخول من المنطقة (أو المناطق) التالية .

ورغم أنهالا تزال تقوم بنفس الوظيفة الرئيسية(تصفية الحركة) إلا انه أضيفت إليها خصائص جديدة هذه الخصائص الجديدة استفادت من الميزة الأساسية للجدران النارية وهي وقوعها على بوابة الشبكة.

جاءت الأجيال التالية من الجدران النارية أكثر قدرة وأكثر مرونة للتعديل وأدى ذلك إلى المزيد من الابتكارات ، ليس فقط في مجال تسريع أداء الجدران النارية وتقديم خدماتها ، بل وأيضا في تضمينها قدرات متعددة تفوق ما كان متوفرا في تلك الأيام ، وتتمثل هذه القدرات في ما يلي :-

- **التحقق من هوية المستخدمين**

التحقق من الهوية يعني التأكد من صحة هوية المستخدم بشكل يتجاوز التحقق من اسم المستخدم والكلمات السرية (التي لا تعتبر وسيلة قوية للتحقق من هوية المستخدمين لأنه يمكن التقاطها من الشبكة) إلى أساليب قوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية **Certificates** ، أو برمجيات حساب الشفرات الرقمية الخاصة . وبواسطة الشهادات الرقمية يمكن تفادي التقاط كلمات المرور.

- **وسائل مراقبة الاستخدام وتتبع سجلات الدخول والخروج للشبكة Logging and Monitoring**

وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين ،ومراقبة العمليات، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد

الاستخدام مثل **Log File** و **Audit Record** (الذي تمت مناقشته في درس التطفل والهجوم)،تشمل كذلك برامج مراقبة الشبكة مثل **Sniffing Program** وأوامر **Dumb**.

- **الشبكات الافتراضية الخاصة Virtual Private Networks**

أما الإضافة الثالثة إلى الجدران النارية للإنترنت فكانت التشفير البيني للجدران النارية firewall to firewall - والتي تعرف اليوم بالشبكات الافتراضية الخاصة Virtual Private Networks . وسميت هذه الشبكات بالخاصة لأنها تستخدم التشفير ، وسميت بالافتراضية الخاصة لأنها تستخدم الإنترنت وشبكات عامة لنقل المعلومات الخاصة .

رغم أن الشبكات الافتراضية الخاصة كانت متوفرة قبل برمجيات الجدران النارية باستخدام المودمات Modems و الموجهات Routers للتشفير لكنها أصبحت تستخدم فيما بعد ضمن برمجيات الجدران النارية .

- **مراقبة المحتوى Content Screening**

يقصد به تحليل محتويات الحزم Packets الواردة للشبكة ومعرفة واختبار محتواها .وخلال الأعوام القليلة الماضية أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة المحتوى الوارد إلى الشبكة للبحث عن الفيروسات والبرمجيات الضارة، ومراقبة عناوين الإنترنت.

- **الجدران النارية الخاصة Private Firewall :**

وهو جيل جديد من الجدران النارية الذي بدأ المزودون بطرحه هذه الأيام،هذا الجيل يحتوي على عدد من التقنيات بما في ذلك حلول جدران نارية جاهزة لا تحتاج لإعداد من قبل المستخدم ويمكن البدء باستخدامها فور الحصول عليها دون الحاجة إلى إجراء أية تعديلات خاصة على نظام التشغيل أو البنية التحتية المستخدمة .

- **التشفير Encryption**

من الإضافات للجدران النارية أيضا التشفير.حيث استفادت الجدران النارية من تقنيات التشفير في إعداد الشهادات الرقمية الخاصة Certificates والتي استخدمت في عمليات التحقق من المستخدمين بدلا عن طريقة التحقق القديمة التي كانت باسم المستخدم وكلمات المرور .كما استخدمت في التوقيع الرقمي Digital Signature .تمت مناقشة التشفير كتقنية عامة في أول هذا الدرس.

- **برمجيات كشف ومقاومة الفيروسات Antivirus واستخدامها في الجدران النارية**

استفادت الجدران النارية من ميزة مراقبة المحتوى وعملت على خلق تركيبة من هذه الميزة مع برامج مضادات الفيروسات لمنع دخول المحتويات الضارة Manlius contents إلى الشبكات. تمت مناقشة آليات مضادات الفيروسات في الدرس الخاص بالبرمجيات الضارة من ضمن موضوعات هذا الكتاب.

قد انتقلت وسائل حماية الشبكات من مستويات الحماية الفردية أو ذات الاتجاه الفردي ، التي تقوم على وضع وسائل الحماية ومنها الجدران النارية في المنطقة التي تفصل الشبكة الخاصة عن الموجهات routers التي تنقل الاتصال إلى الشبكة العالمية (الإنترنت) ، إلى مستويات الأمن المتعددة والتي تقوم على فكرة توفير خطوط إضافية من الدفاع بالنسبة لنوع معين من المعلومات أو نظم المعلومات داخل الشبكة الخاصة ، وتعتمد وسائل الأمن متعددة الاتجاهات والأغراض آليات مختلفة لتوفير الأمن الشامل للنظام يمكن تقسيمها إلى ثلاثة مناطق أساسية هي:

الأولى إدارة خطوات الأمن وتشمل الخطط والاستراتيجيات وأغراضها والقواعد والبحث والتحليل.

الثانية أنواع الحماية وتشمل الوقاية أو الحماية والتحقيق والتحري والتصرف .

الثالثة وسائل الحماية وتشمل حماية النظم والخوادم Servers وحماية البنية التحتية للشبكة .

التواقيع الرقمية

تعتبر التواقيع الرقمية (Digital Signatures) أحد الأدوات الأساسية المستخدمة في أمنية المعلومات. وهذه هي الكتلة التي تبنى عليها العديد من الخدمات والتي منها على سبيل المثال لا الحصر عدم الإنكار، إثبات صحة مصدر البيانات، التعرف (Identification)، والشهادة (Witness). بعد تعلم أساسيات الكتابة، بالامكان التعلم على كيفية عمل توقيع كتابي (Handwritten) لغرض التعرف (Identification). وفي عمر التعاقد مع الاتصال فان التوقيع يتطور لكي يكون جزء متمم للهوية الشخصية (Identity). يرمي هذا التوقيع إلى إن يكون جزء مميز (Unique) للشخص ويخدم وسيلة للتعرف، التخويل (Authorization)، التثبت أو (Validation). باستخدام المعلومات الالكترونية فان فكرة التوقيع تحتاج إلى إعادة تحديد ; وهي إن تكون ببساطة شئ ما مميز للموقع (Signer) وتكون مستقلة عن المعلومات الموقع عليها. يعتبر الاستنساخ الالكتروني (Electronic Replication) للتوقيع هو أمر في منتهى البساطة بحيث إن إضافة توقيع إلى وثيقة غير موقعة من قبل منشأ التوقيع أمر في غاية التفاهة (Triviality).

يستخدم التوقيع الرقمي لغرض التعريف (Identification) بالأجزاء (مثل شخص معين، جهاز معين،.....) المطلوب التثبت من صحة تخويلها. اعتاد المستفيدون على استخدام التواقيع اليدوية و التي أصبحت تمثل غرض تعريفي لذلك الشخص. يجب أن يكون التوقيع الرقمي مميز وفريد للمستفيد ويعتبر وسيلة للتعريف، التخويل وكذلك التحقق (Validation). في المعلومات الرقمية فإن فكرة التوقيع تحتاج إلى إعادة نظر، إنها ليست ببساطة عبارة عن شئ مميز للموقع (Signer) وغير معتمداً على المعلومات الموقعة.

لغرض الوصول إلى أمنية المعلومات في الوسط الإلكتروني فإن ذلك يحتاج لعدد هائل من التقنيات و المهارات القانونية.

حماية البيانات

المحاور الاساسية لحماية البيانات

١. حماية جهاز الحاسب و ملحقاته من التأثيرات الكهربية الغير مرغوب فيها.
٢. حماية جهاز الحاسب الالي من حدوث خلل بسبب ظروف بيئة التشغيل المحيطة بالجهاز
٣. حماية البيانات عن طريق القيام بعملية التخزين الاحتياطي كل فترة زمنية و بصفة دورية
٤. حماية بيانات شبكة الحاسب من الإضرار بها

فيروسات الحاسب

في ظل تنامي استخدام الانترنت و استخدمها كأداة لنقل البيانات، اصبح من السهل اصابة العديد من اجهزة الحاسب بالفيروسات.

تعريف الفيروس:

- الفيروس هو برنامج كمبيوتر يتكون من عدة برامج فرعية مكتوبة بأحد لغات البرمجة مثل أي برنامج تطبيقي اخر علي الحاسب، ليس هناك اختلاف إلا في الغرض منه و هو اصابة الحاسب الالي و اتلاف برامجه و بياناته.
- يمكن للفيروس ان يكون في شكل ملف مستقل او ملتصقا بأحد الملفات.
- عند انتقال الملف المصاب بالفيروس الي ذاكرة الحاسب للتعامل معه يقوم الفيروس بنسخ نفسه و وضع نسخ اخرى منه في ذاكرة الحاسب.

خصائص الفيروس

١. **القدرة علي الاختفاء :**
   - قد يدخل مرتبط ببرنامج شائع
   - يدخل كملف مخفي ضمن مجموعة برامج و لا يمكن استعراضه عند استعراض اسماء البرامج.
   - تستقر الفيروسات في الذاكرة في اماكن يصعب ملاحظتها
   - بعضها يظل ساكن لفترة طويلة ثم يبدأ في التكاثر بسرعة.
٢. **التكاثر :**
   - يقوم الفيروس بنسخ نفسه سواء في الذاكرة او داخل كل ملف يصيبه.

٣. **التنقل :**

- يتنقل الفيروس داخل الذاكرة من مكان الي اخر حيث يصعب ازالته.

٤. **البصمة :**

- لكل فيروس بصمة يضعها ضمن البرنامج المصاب بالفيروس من خلالها يمكن التعرف عليه.

٥. **التدمير:**

- لكل فيروس ما يسمى المفجر الذي يقوم بتدمير البيانات بمجرد تشغيله و هو اما ان يكون مرتبطا بتاريخ او عند ضغط مفتاح معين او عند تنفيذ امر وعين.

أشباه الفيروسات

- الدودة :

هو برنامج يعيد انتاج نفسه لكن لا يلوث برامج اخرى و هي نوعان:

- الدودة المضيفة: تستخدم الشبكة لنسخ نفسها الي اجهزة الكمبيوتر المتصلة بالشبكة
- الدودة الشبكية: توزع اجزائها على عدة كمبيوترات و تعتمد علي الشبكة فيما بعد لتشغيل اجزائها.

- حصان طرواده :

- يختبئ ضمن برامج تظهر بريئة و عندما يشغل المستخدم احد هذه البرامج ينشط حصان طرواده و يقوم بعمل معين هو مصمم من اجله، و في الغالب يقوم بعمل بوابة خلفية تمكن المتسللين من الدخول لجهاز الكمبيوتر المصاب و العبث به.
- لا يستطيع حصان طرواده اعادة انتاج نفسه.

الاضرار التي تنتج عن الفيروسات

١. فقدان بعض الملفات التطبيقية الهامة و توقف عمل التطبيق.
٢. امتلاء الذاكرة نتيجة نسخ الفيروس نفسه.
٣. فقدان جدول توزيع الملفات FAT مما يصعب الوصل الي الملفات على الحاسب.
٤. فقدان قطاع القلاع Boot Sector بالتالي يفقد الجهاز القدرة علي تحميل نظام التشغيل.
٥. تلف بعض الاقراص المصابة بالفيروس.
٦. توقف الجهاز فجاة عن العمل مما يؤدي الي فقد البيانات التي يتم العمل عليها.
٧. تغيير مواضع حروف لوحة المفاتيح مما يصعب العمل علي الحاسب.
٨. يعطل تنفيذ بعض التطبيقات و البرامج.

أعراض الفيروس

- عدم تحميل نظام التشغيل او القدرة علي التعامل معه بشكل سليم.
- توقف النظام عن العمل اثناء التشغيل.
- زيادة او نقصان حجم ملف بصورة ملحوظة.
- تغيير عدد الملفات.
- عدم ظهور اسماء الملفات عند استعراض محتويات القرص.
- عرض رسائل خطاء فجائية و غير متوقعة مثل: "لا توجد ذاكرة كافية للتشغيل".
- ظهور ملفات جديدة لها اسماء و امتدادات غريبة.
- تغيير مظهر العلامات الدالة عن الملفات.
- بطء تشغيل النظام بصورة ملحوظة.
- عدم قدرة بعض التطبيقات علي العمل.
- نقص شديد في سعة الذاكرة.
- و جود تناقص مستمر في المساحة الخالية علي القرص الصلب.
- عدم القدرة علي التعامل مع بعض الوحدات الطرفية مثل مشغل الاقراص و الطابعات.
- انهيار النظام بالكامل و عدم قدرة الجهاز علي العمل.

مراحل عمل الفيروس

١. **مرحلة الدخول:**

- يدخل الفيروس الي الجهاز مختبئا في ملف ملوث.

٢. **مرحلة بداية العودة و الانتشار:**

- يبدأ مختفيا في ثنايا برنامج اخر و ينشط معه.
- يضيف الفيروس شفرته الي البرنامج الاصلي و يعدل تعليماته بحيث ينتقل التنفيذ الي شفرة الفيروس و عند تشغيل الملف التنفيذي المصاب، يقفز البرنامج الي تعليمات الفيروس فيشغلها ثم يعود لتنفيذ تعليمات البرنامج الاصلي. عند هذه النقطة يكون الفيروس نشطا و الجهاز مصاب.
- يصبح البرنامج المصاب مصدرا للعدوى و يصيب بدور غيره من البرامج.
- معظم الفيروسات تمر بمرحلة كمون بعد العدوى مباشرتا لا يظهر التلف علي البرامج التي تمت اصابتها جديدا مما يتيح للفيروس الوقت اللازم لنسخ نفسه دون ملاحظته.

٣. **مرحلة التنفيذ:**

- هي مرحلة شرطية يعتمد تنفيذها علي شرط معين يحدده مصمم الفيروس مثل تاريخ معين، عدد محدد من مرات التكاثر .

طرق و اسباب انتشار الاصابة بالفيروسات

١. مشاركة الملفات عن طريق شبكة الحاسب.
٢. نسخ البرامج من النشرات الالكترونية.
٣. تثبيت برنامج جديد في الحاسب.
٤. من خلال نقل الاجهزة نفسها.
٥. استخدام اسطوانات مصابة بالفيروس.
٦. من خلال مرفقات البريد الالكتروني.
٧. التداول السيئ للبرامج.

الوقاية من الفيروس

- استخدام البرامج الاصلية و عدم استخدام النسخ.
- تجهيز عدة نسخ احتياطية من البرامج الاصلية.
- الاحتفاظ بسجل لكل عمليات التعديل في برامج التطبيقات.
- عدم تحميل أي برنامج مجلوب من الخارج.
- يجب فحص البرمجيات و اختبارها قبل استخدامها
- حماية الاقراص عن طريق فتحة الحماية للأقراص المرنة
- اختبار الملفات من وقت لأخر لملاحظة حجمها.
- مراقبة الملفات التنفيذية و ملفات التهيئة من حين للأخر.
- اجراء عملية مسح شاملة للجهاز بصفة دورية.
- الكشف الدوري علي الاقراص المرنة و الممغنطة.
- استخدام الاقراص الضوئية للكتابة فقط.
- عدم الدخول علي مواقع غير معروفة.
- تجنب التصفح بشكل عشوائي.
- تحميل برامج داخل الحاسب للكشف عن وجود الفيروسات.

البروكسي Proxy

البروكسي

البروكسي هو برنامج (Software) يتم تركيبه على أجهزة خادمة. و لذلك يسمّى مجازاً باسم خادم البروكسي . مثله في ذلك مثل خادم الويب . الذي هو أيضاً عبارة عن خادم برمجي .

الكثير من الشبكات الداخلية ومزودي خدمة الإنترنت يستعملون بروكسي خوادم الويب ، و خوادم البروكسي عبارة عن حلقة وصل بينك وبين الإنترنت . على الرغم من أن بعض الناس ترى مشاكل في استعمال البروكسي ، إلا أن فوائدها تفوق مشاكلها بكثير

كيفية العمل :

يعمل البروكسي سيرفر كبوابة أمنية لشبكة الانترنت للحواسيب المتصلة به , (Clients)وهذا لا يؤثر بأي شكل على استخدام الشبكة من خلال هذا السيرفر , فالمستخدم للانترنت عبر البروكسي يتعامل معها بشكل طبيعي بدون أي تأثير من البروكسي، في ماعدا أن المستخدم إذا قام بطلب محتوى ما من الانترنت و كان هذا المحتوى ممنوع من البروكسي ففي هذه الحالة لا يمكن عرض هذا المحتوى سواء كان صفحة انترنت أو وسائط متعددة أو أي محتوى .أما بالنسبة للـ Web Serverفالأمر سواء، فعندما يستقبل مزود موقع الانترنت طلبات التصفح يعالجها كأنها جاءت مباشرة من أجهزة الزبائن.كذلك يمكن لخوادم البروكسي أن تستخدم لتامين الشبكات الخاصة المرتبطة بشبكات عامة اكبر غير آمنة كشبكة الانترنت، ففي هذه الحالة، تتصرف بفعالية اكبر من موجهات فلترة الحزم (Packet Filtering Routers) على مستوى مراقبة وإدارة الدخول إلى الشبكة، وهذا النوع من مزودات البروكسي يدعى Firewall .

هناك نوعان من مزودات البروكسي تستخدم في بيئات حماية الشبكات , Firewall هما :

- **مزودات الارتباطات : Circuit – Level Gateways :**

وتعمل هذه المزودات بواسطة إنشاء ارتباطات افتراضية بين الأجهزة على الشبكة الداخلية وبين مزود البروكسي لهذه الشبكة، وفي هذه الحالة على سبيل المثال، إذا قام مستخدم ما بطلب تصفح لموقع معين، يقوم مستعرض الانترنت بإنشاء حزمة طلب , HTTP بعد ذلك تنتقل هذه الحزمة إلى مزود البروكسي، ثم يقوم البروكسي بتغيير رقم الـ IP لهذه الحزمة من رقم الجهاز في الشبكة الداخلية إلى رقم الـ IP الخاص به ويقوم بإرسال الحزمة إلى الانترنت، عندها يستقبل مزود الـ HTTP البعيد هذه الحزمة ويرسل الرد عليها إلى مزود البروكسي ومن ثم يقوم هذا المزود بتوجيهها إلى الجهاز الذي قام بطلبها.

- **مزودات التطبيقات : Application – Level Gateways :**

مزودات التطبيقات تستطيع تطبيق إجراءات أمنية بواسطة تحليل الحزم القادمة من الشبكات العامة الغير أمنة ، هذه الإجراءات الأمنية تستطيع فحص عناوين الحزم ومعلومات الترويسات ,(Header) السماح لهذه الحزم أو حظرها بناء على محتواها وتعديل هذه العناوين أو الترويسات أو المحتوى لحظر معلومات هامة عن المستخدم لشبكة الانترنت .

مزودات التطبيقات توفر خدمات البروكسي فقط لعدد من التطبيقات و البروتوكولات مثل HTTP, FTP, SMTP, TELNET,أما بالنسبة لبقية التطبيقات والبروتوكولات فيمكن لها أن تستخدم خدمات البروكسي ولكن بشرط تنصيب وإعداد خدمة بروكسي خاصة بها على مزود

البروكسي .

مثال على مزودات البروكسي هو Microsoft Proxy Server

- **POP3 (Post Office Protocol):هو بروتوكول كيفية تخزين البريد الوارد في ملقم البريد، وجميع موفري الخدمة يدعمونه.**
- **SMTP (Simple Mail Transfer Protocol): بروتوكول لنقل البريد البسيط عبر الانترنت وعادة ما يستخدم للبريد الصادر.**
- **IMAP (Internet Message Access Protocol): هو أفضل وأحدث بروتوكول يستخدم للبريد وبعض موفري الخدمة يدعمونه، ويتيح لك استخدام ملقم البريد لتنظيم رسائلك والوصول إليها من أي مكان.**

ما هي وظائف خادم البروكسي ؟

1-العمل كجدار ناري وللتنقيح .

2-المشاركة في الوصل بالإنترنت .

3-الذاكرة المخبئة caching .

الخلاصة :

مميزات استخدام البروكسي سيرفر تتضمن التالي :

(1)توفير إمكانية إدارة بوابة موحدة آمنة إلى الشبكات العامة.

(2)توفير طرق دخول متعددة إلى شبكة الانترنت.

(3)إمكانية مراقبة وتتبع دخول كل مستخدم إلى شبكة الانترنت.

(4)يمكن لعدة مستخدمين مشاركة ارتباط انترنت سريع واحد.