Continguts Formatius
de Suport al Projecte acTIC

Nivell C3: Navegació i comuniació en el món digital

Mòdul 5: La seguretat al món digital

1. OBJECTIUS

- Ser conscient de la importància de la seguretat al món digital

2. VIRUS INFORMÀTICS I PROGRAMARI MALICIÓS

- Un sistema informàtic està format per tres elements: l'ordinador (hardware), els programes (software) i les dades (la informació).
- Un sistema segur ha de complir tres condicions: la confidencialitat, la integritat i la disponibilitat.
- Si alguna d'aquestes característiques no es compleix, pot ser degut a:
  - La debilitat del sistema informàtic, o vulnerabilitat.
  - La pèrdua potencial de recursos del sistema, o amenaça.
  - La probabilitat que el sistema sigui atacat a causa del risc d'una amenaça.
  - El mal que es produeix al sistema, o atac.
- Hi ha dos tipus d'amenaces: els virus i el programari maliciós

Un sistema informàtic està format per tres elements: l'ordinador (maquinari), els programes (programari) i les dades (la informació). Qualsevol dels elements del sistema pot fer fallida per l'acció d'un virus o d'un programari maliciós que hi arribi a entrar. Per això és molt important que el sistema sigui segur i que estigui suficientment protegit.

Un sistema segur ha de complir tres condicions: la confidencialitat, la integritat i la disponibilitat.

La confidencialitat vol dir que l'accés al sistema només es permet a persones autoritzades. La integritat significa que les modificacions que es facin a les dades o altres recursos del sistema, únicament poden ser realitzades per aquestes persones autoritzades. La disponibilitat implica que tots els recursos del sistema han d'estar a l'abast d'aquestes mateixes persones.

Si alguna d'aquestes característiques no es compleix, pot ser:

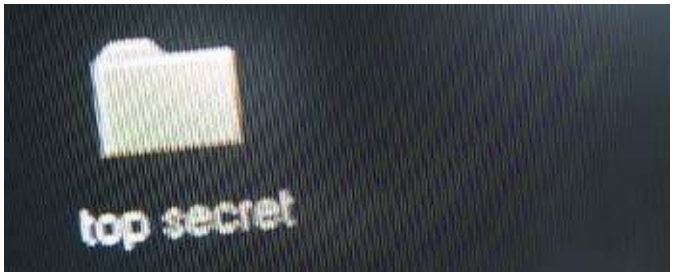
1. Per la debilitat del sistema informàtic, o vulnerabilitat. Si tenim instal•lat un antivirus a l'ordinador, però no el tenim actualitzat, pot ser atacat per virus nous.
2. Per la pèrdua potencial de recursos del sistema, o amenaça: Si es

produeixen fallades internes del hardware o el software, hi ha l'amenaça d'un atac al sistema.

3. Per la probabilitat que el sistema sigui atacat a causa del risc d'una amenaça: Si l'ordinador conté dades confidencials, es corre un risc molt alt de perdre-les en cas que sigui atacat.

4. Pel mal que es produeix al sistema, o atac: És el mal immediat o posterior que pot afectar la confidencialitat, la integritat o la disponibilitat dels recursos del sistema.

Per tant, hem de protegir el sistema amb una sèrie de controls adequats que n'eliminin les debilitats.



Els virus informàtics ataquen a la confidencialitat de les dades que tenim al nostre ordenador personal

Els virus

Un virus informàtic és un programa que s'executa a l'ordinador tot utilitzant-ne el sistema operatiu. Tenen uns components bàsics:

- L'agent infecciós: És la part del virus que utilitza qualsevol vulnerabilitat del sistema per introduir-se a l'ordinador.
- El duplicador: Permet que el virus es copiï dintre de programes de l'ordinador o que s'enviï automàticament a través del correu electrònic.
- El codi maligne: És la part del virus que produeix el mal al sistema. S'activa en determinades situacions, com ara quan s'engega l'ordinador, quan s'executa un programa concret o quan s'arriba a una determinada data de l'any.

Hi ha diversos tipus de virus. Cadascun utilitza un mecanisme diferent per estendre's i atacar. Entre els més habituals destaquen:

- Bombes lògiques: S'activen quan es compleix una condició determinada, com quan s'arriba a una data en concret. El virus Divendres 13, s'activava cada dia 13 que coincidia en divendres.

- Cucs: Creen còpies de si mateixos i s'autoenvien a d'altres ordinadors connectats en xarxa (per exemple, via correu electrònic).
- Troians: Són programes que contenen un virus. Quan s'executa el programa, el virus s'estén i executa el seu codi maligne.
- Exploits: Aprofiten la vulnerabilitat del sistema operatiu, o dels programes, per infectar la resta de l'ordinador i expandir-se.
- Virus polimòrfics: Canvien de forma després de cada infecció; és a dir, canvien el seu codi maligne, el tipus d'arxius que ataquen, etc.
- Virus ocults: Una vegada s'han activat i han infectat un arxiu, romanen actius i eviten la seva detecció mitjançant l'enviament d'informació falsa.
- Virus autoencriptats: Són virus que encripten el codi maligne cada vegada que infecten un arxiu per tal de dificultar-ne la detecció.
- Virus per correu: Són virus que envien missatges a d'altres ordinadors per infectar-los.

La consola d'un antivirus mostra la presència de troians

Programari maliciós

El programari maliciós (spyware) és un programa espia que té l'objectiu d'obtenir informació sobre els nostres hàbits de navegació per Internet. Amb aquesta informació, ens poden enviar publicitat (finestres emergents), missatges no desitjats, o aconseguir dades confidencials.

Hi ha dos tipus de programari maliciós: Quan descarreguem un programa o un joc gratuït, podem instal•lar un programa maliciós al nostre ordinador sense saber-ho. És important llegir les pantalles prèvies abans de descarregar el programa, ja que a vegades ens informen que se'ns instal•larà un programari maliciós que ens omplirà l'ordinador de publicitat, com a forma de retribució per al creador del programa. Hi ha altres tipus de programari maliciós que s'instal•len al nostre sistema sense adonar-nos-en.

Alguns dels sistemes per protegir-nos dels virus i del programari maliciós són els antivirus i els programes antispyware (antiespia).

3. CONÈIXER I CONFIGURAR SISTEMES DE PROTECCIÓ

- Per protegir-nos dels diferents tipus d'atacs al nostre sistema informàtic, disposem d'una gran quantitat d'eines que el faran més segur.
- Aquestes eines són els antivirus, els antiespies i els tallafocs.

Per protegir-nos dels diferents tipus d'atacs al nostre sistema informàtic, disposem d'una gran quantitat d'eines de protecció que el faran més segur.

Tanmateix, hem d'aprendre i posar en pràctica una sèrie de normes de seguretat bàsiques, com ara no obrir ni respondre missatges de correu electrònic de desconeguts, utilitzar contrasenyes d'accés alfanumèriques, o, quan naveguem per Internet, no clicar qualsevol enllaç o botó d'una pàgina web.

Antivirus

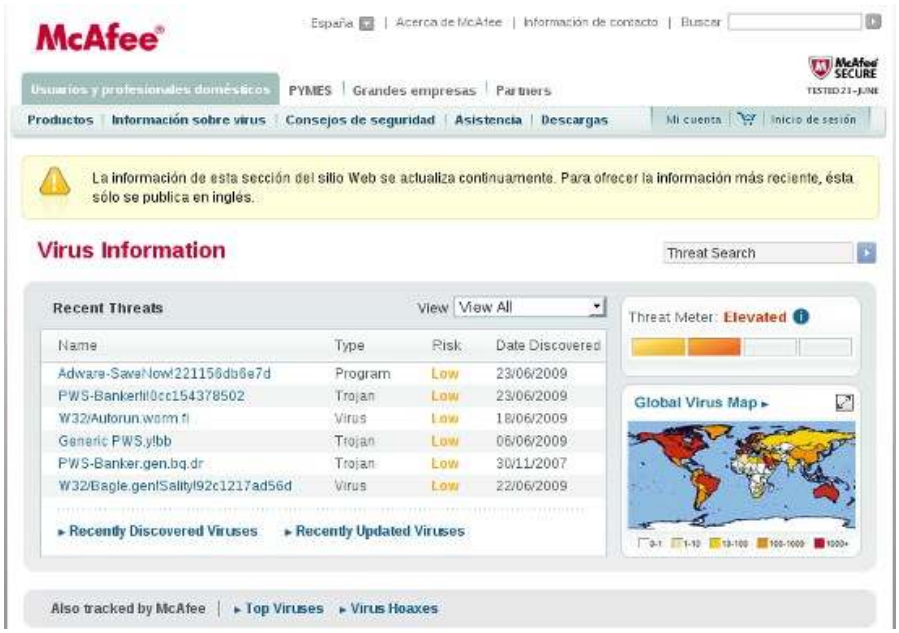
Un antivirus és un programa que presenta diverses funcions:

- Analitza el disc dur, o qualsevol suport d'emmagatzematge de l'ordinador, per tal de trobar arxius infectats per virus. El programa compara parts d'un arxiu amb els continguts d'arxius de virus coneguts. Per això és tan important mantenir actualitzat l'antivirus.
- Elimina els virus trobats. Segons com estigui configurat l'antivirus, el programa elimina el virus o el posa en quarantena.
- Evita que el virus estigui actiu.
- Analitza el correu electrònic.
- Analitza les pàgines web que es visiten quan naveguem per Internet.

El sistema adverteix que l'antivirus de l'ordinador no està actualitzat o hi ha algun problema. Existeix perill d'entrada de virus

Els antivirus es poden obtenir en línia, tot i que alguns d'ells són de pagament, i també les actualitzacions (programes com Norton o McAfee). Altres programes són gratuïts, especialment per a usuaris domèstics, com per exemple Avast!, AVG Antivirus o CLAM AV.

Per instal•lar un antivirus en línia, normalment s'ha de descarregar i executar l'arxiu setup.exe. Una vegada executat, apareixen diferents finestres (llicència, ubicació del programa, configuració, etc.) fins que el programa queda instal•lat.



McAfee, fabricant d'antivirus, detecta la creació i actualització de virus a tot el món

És molt important mantenir actualitzat el programa. L'actualització es pot fer de forma manual o de forma automàtica, quan l'ordinador està connectat a Internet.

Normalment, els sistemes operatius de programari lliure pateixen menys problemes de seguretat que el sistema operatiu Windows.

Antiespies

Els programes espies s'instal•len al nostre ordinador mentre naveguem per Internet, l'omplen de publicitat i obtenen dades nostres sense permís. Podem eliminar-los utilitzant un programa antiespia.

El navegador detecta la presència de virus i recomana la instal·lació d'un programa antivirus.

Hi ha antivirus que porten aquesta funció incorporada. Alguns programes antiespies que es poden descarregar gratuïtament d'Internet són Ad-aware o Spybot.

El procediment per descarregar-los és el mateix que seguim amb els antivirus en línia.

Tallafocs

Un tallafoc és un programa que filtra i bloqueja les comunicacions en xarxa (per Internet o per xarxa local) no desitjades; és a dir, que protegeix la informació d'intrusions externes i optimitza l'accés per nivells als diferents programes i aplicacions que diversos usuaris d'un ordinador poden utilitzar.

El sistema operatiu Windows XP inclou per defecte un tallafoc. La configuració permet activar-lo, amb excepcions o sense, o desactivar-lo.

La pestanya d'opcions avançades permet activar o desactivar el tallafoc per a una connexió en concret.

A la pestanya d'excepcions, podem seleccionar-hi els programes o serveis que no quedaran bloquejats pel tallafocs.

Quan s'utilitza un encaminador (router) per connectar-nos a Internet, també hem d'utilitzar un tallafoc.

4. ENLLAÇOS RELACIONATS

Virus informàtics (Cassificació) http://www.network-press.org/?virus_informaticos_concepto
Fòrums sobre antivirus http://alerta-antivirus.red.es/foros/

Enllaços a programes d'antivirus:
McAfee http://www.mcafee.com/es
Norton http://www.symantec.com/
Avast http://www.avast.com/
AVG Antivirus http://www.grisoft.com/

Enllaços a programes antiespies:
Ad-aware http://www.lavasoft.com/
SpyBot http://www.spybot.info/
Windows AntiSpyware http://www.microsoft.com/

Enllaços a programes tallafocs:
Norton personal firewall http://www.symantec.com/
Sygate personal firewall http://www.sygate.com/