Pautes d'actualització del sistema informàtic

La protecció del sistema informàtic és crítica per assegurar que l'accés a la informació personal es fa només per les persones autoritzades. No n'hi ha prou amb assegurar la seguretat física per garantir la seguretat del sistema informàtic. Un punt de xarxa lliure pot facilitar la intrusió al nostre sistema; el pas del temps fa que apareixen forats no descoberts abans o errors de maquinari en els equips que poden deixar el sistema informàtic vulnerable. Pitjor encara, una actualització del sistema (servidors, encaminadors, estacions de treball), que suposem que millora la seguretat, en realitat pot obrir noves esquerdes en el nostre sistema sense que ens adonem. També podríem parlar de contrasenyes insegures o febles, rotació de personal dins de l'organització, etc., aspectes que hem de comprovar periòdicament per a assegurar que el nostre sistema es manté segur.

Per tots aquests motius és necessari protegir i tenir actualitzats tant els elements *hardware* com els elements *software* del sistema informàtic. Altrament persones no autoritzades, de dins i fora de l'organització, podrien accedir a dades personals, amb els consegüents perjudicis econòmics i d'imatge que pot representar.

Aquestes són alguns dels punts que haurem de tenir presents per mantenir la xarxa i el sistema protegit:

- **Sistema de** fitxers: s'ha de garantir que només puguin accedir als fitxers o modificar-los els usuaris autoritzats a fer-ho.

- **Codi maliciós**: s'anomena codi maliciós el codi que s'insereix dins d'un programa "autoritzat" i que fa una sèrie d'accions desconegudes per a l'usuari, les quals actuen normalment en detriment seu.

  Els exemples més coneguts de codi maliciós són els virus i els troians.

- **Autenticació d'usuaris**: procés de verificació de la identitat d'una persona a l'hora d'accedir a un recurs. Habitualment els usuaris s'autentiquen mitjançant un nom d'usuari i una contrasenya (hi ha diferents tipus d'autenticació i diferents polítiques d'assignació de contrasenyes, els quals pot determinar un administrador).

- C**riptografia**: l'ús d'eines criptogràfiques permet de garantir la confidencialitat de les dades que circulen per la xarxa o es troben emmagatzemades en un sistema informàtic.

- **Eines de seguretat**: l'administrador pot fer ús de diverses eines amb la finalitat de comprovar i mantenir la seguretat de la xarxa. En general, podem diferenciar les següents:

  - Eines per a comprovar la vulnerabilitat de les mateixes màquines (per exemple, un escàner de ports).

- Eines que ofereixen serveis segurs (per exemple, l'ús de *Secure Shell* en lloc de l'habitual *Telnet*).

- Eines que garanteixen la integritat del sistema (com ara *Tripwire*).

- **Monitorització del sistema**: s'anomena *logging* el procediment mitjançant el qual s'enregistren en un fitxer les activitats que tenen lloc en un sistema operatiu o en una aplicació. La importància dels fitxers *log* és evident i ens permetrà d'esbrinar **què** ha passat en un sistema informàtic i, si cal, prendre les mesures adients. És molt important plantejar *quines* aplicacions han d'enregistrar *log* i *quan* ho han de fer, i també quan s'han d'eliminar o migrar a un dispositiu d'emmagatzemament per a poder tenir espai en el sistema.

- **Seguretat del** maquinari **de xarxa**: pel que fa a la seguretat dels commutadors, concentradors i encaminadors, cal tenir en compte els aspectes següents:

  - Activació del xifratge (en cas que els dispositius ho admetin).

  - En cas que no sigui necessari, cal desactivar el control remot d'administració.

  - Canviar les contrasenyes d'administració predeterminades d'aquests dispositius.

Aquests són alguns dels punts que haurem de tenir presents per mantenir la xarxa i el sistema actualitzat:

- **Actualització del maquinari de xarxa**: pel que fa al maquinari de xarxa (commutadors, concentradors i encaminadors), cal tenir present que són elements que necessiten periòdicament actualitzacions del seu programari base.

- **Actualització de les estacions de treball**. L'actualització de les estacions de treball, pel que fa al sistema operatiu, es pot fer de manera centralitzada per assegurar que estan sempre correctament actualitzats amb els darrers pedaços de seguretat.

  En el cas de Microsoft, existeix una aplicació gratuïta anomenada Windows Server Update Servides (WSUS) que permet manegar de manera centralitzada la distribució de pedaços en una xarxa corporativa. http://technet.microsoft.com/es-es/wsus/default(en-us).aspx

- **Actualització de l'antivirus**. L'antivirus representa també un punt molt important en el sistema informàtic. A l'igual que les estacions de treball, existeixen solucions per part dels fabricants que fan una actualització dels ordenadors de la xarxa corporativa a partir d'un punt central. Aquests productes permeten saber quins ordenadors estan actualitzats, quan, en quina versió, i així com obtenir un petit informe de la seva situació en matèria d'incidències.

- **Actualització del servidor**. Els servidors necessiten actualitzacions de software i hardware, igual que la resta del sistema informàtic. Al ser els elements que proporcionen recursos a la resta (a les estacions de treball), és important que estiguin disponibles el major temps possible. Per això cal que les actualitzacions

es facin periòdicament per prevenir forats de seguretat que podrien comprometre tot el sistema informàtic. Tindrem present:

> Una **acció** o **actualització programada** és aquella que es fa en elements de la xarxa o en servidors. S'avisa als usuaris amb un temps d'antelació (hores, dies o inclús setmanes) dels serveis que afecta i de la durada prevista.

- Saber prèviament com afecten les actualitzacions al servidor. Si aquestes afecten al normal funcionament de l'equip o necessiten reiniciar el servidor s'haurà de fer una actualització programada.

- Si l'actualització és important, caldrà fer una còpia de seguretat del servidor. La política de copies de seguretat se'n pot veure afectat, i per tant s'ha de preveure abans de fer-la.

- Especialment en el cas dels servidors, cal mirar que l'actualització opera correctament (fa el que suposem) durant un període (que pot ser de hores a setmanes en funció del que s'hagi actualitzat). Sobretot si les actualitzacions han modificat serveis importants.