Introducció

Jordi Serra Ruiz

PID_00200497

Universitat Oberta de Catalunya

Índex

1. La seguretat a l'empresa

Les persones responsables d'administrar els sistemes informàtics d'una empresa, ja sigui una petita empresa o una de molt gran, han de tenir molta pràctica a resoldre problemes derivats de la instal·lació dels equips informàtics de les seves empreses.

El material d'aquesta assignatura us mostra com s'han d'instal·lar i configurar aquests sistemes informàtics, tant el sistema operatiu mateix que es decideixi instal·lar com les eines bàsiques de control i les diferents aplicacions típiques dels servidors, que en molts casos ajuden a fer les tasques diàries, i fins i tot les esporàdiques.

Es veuran les eines i servidors següents en aquesta assignatura:

- Còpies de seguretat
- Plans de risc
- Servidors de fitxers
- Servidor web
- Servidor de xarxes privades virtuals (VPN)
- Servidors de correu electrònic
- Servidors FTP
- Virtualització

1.1. Còpies de seguretat

En molts casos, el més important que té una empresa són les dades. Posem, per exemple, un banc, en què tots suposem que deixem els nostres diners, però en realitat no els té físicament, sinó que té una base de dades amb la quantitat de diners que cada client té dipositat en aquest banc. Per tant, el més valuós que té aquest banc, o en el seu cas una sucursal, són les dades. Si es perd la base de dades, no es perdran els diners, però sí que es perdrà la relació entre els clients i els diners. Per tant, el primer que cal assegurar en una empresa és mantenir les dades costi el que costi. No podem deixar a la seva sort totes les dades que té una empresa, com en l'exemple del banc, les transaccions econòmiques o les dades de clients i proveïdors.

Això implica que s'han de fer còpies de seguretat dels equips informàtics, especialment dels equips que es dediquen a fer tasques de servidor, i tota la informació que tenen en cadascuna de les bases de dades. Tenir còpies dels equips de treball dels usuaris del sistema informàtic farà que una recuperació potencial del lloc de treball es pugui fer molt més ràpidament, però no serà tan crític com perdre les dades dels servidors.

És molt important definir des d'un principi una bona política de realització de còpies de seguretat. Resulta imprescindible poder recuperar tota la informació o la màxima a què puguem optar amb els recursos que es tinguin en un període curt. En una empresa el temps són diners, i com més aviat es recuperin els servidors, menys pèrdues hi haurà.

En general, ja que dependrà molt de les dades i sobretot de la variació d'aquestes i del temps màxim de què es disposi per a poder-les recuperar, les bones polítiques de còpies de seguretat assenyalen que cal fer una còpia completa setmanalment, però el fet de decidir quin tipus de còpia es fa diàriament depèn del tipus de dades i de l'evolució que tinguin aquestes dades. Per exemple, el cas del banc, en què les dades són crítiques, es podria decidir fer una còpia sencera cada dia, ja que és més ràpida de recuperar que no pas recuperar la còpia sencera del dilluns i anar afegint les modificacions de cada dia. Però també s'ha de tenir en compte la mida de la còpia, ja que una còpia sencera és molt gran, i per tant en el cas que no sigui crític en farem servir alguna en què no calgui desar tota la informació.

Depenent de la importància de les dades, del temps que es té per a fer les còpies i dels dispositius físics on s'emmagatzemen les dades, podrem triar entre diverses opcions que ens assegurin que podrem recuperar totes les dades en un temps raonablement curt per a l'empresa.

Les còpies de seguretat s'acostumen a fer sobre el sistema mateix, ja sigui en dispositius de cinta, de DVD, sobre un altre disc dur, etc. Dependrà molt de les dades que s'han de copiar i del pressupost que es tingui per a poder comprar un dispositiu més complex. Una opció és fer la còpia de les dades per mitjà de la xarxa interna de l'empresa o fins i tot de la xarxa Internet. Actualment ja hi ha empreses que disposen de búnquers en què emmagatzemen les dades de les empreses que gestionen les còpies de seguretat, i durant la nit pugen les dades cap als seus servidors.

És important mantenir separades les còpies de seguretat dels dispositius per tal que un error no destrueixi tant el dispositiu del qual fem còpies com les còpies mateixes. S'han donat casos d'empreses privades que han hagut de tancar, i fins i tot institucions públiques que han perdut tant el servidor que contenia les seves dades com la còpia de seguretat a causa d'un incendi.

Còpies de seguretat en xarxa

En el cas de tenir una base de dades amb uns quants gigabytes o fins i tot terabytes de mida, si és una còpia de seguretat de tota la base de dades pot ocupar el sistema i la xarxa durant moltes hores. Fins i tot ens podria passar que en una nit no es pogués fer tota la còpia i les dades ja no fossin les correctes.

Tenint en compte que les còpies de seguretat impliquen accedir a totes les dades en l'espai de temps més petit possible, cal planificar les còpies d'acord amb els ritmes de cada empresa. D'altra banda, s'haurà d'evitar fer circular per la xarxa innecessàriament les dades que hagin de disposar d'un tracte especial per les lleis de protecció de dades i si cal, s'ha de fer amb les mesures suficients perquè terceres persones no les puguin interceptar.

En general, val més dur a terme les còpies a la nit i no en plena jornada laboral, ja que els usuaris veuran com el rendiment del sistema informàtic quedarà afectat seriosament i tant la xarxa com l'accés als discos s'alentirà.

1.2. Plans de risc

Totes les empreses que tinguin algun sistema informàtic una mica gran o que tingui un funcionament crític per a l'empresa, per tal de mantenir el seu negoci han de tenir un pla de risc per a possibles emergències. Les més comunes són la caiguda de la xarxa elèctrica i els pics de tensió, que poden danyar molt seriosament tant les fonts d'alimentació dels equips informàtics com les plaques base mateixes dels ordinadors que funcionen en aquell moment, i deixar completament inservible tot el sistema informàtic. Per exemple, una pujada de tensió en un servidor de fitxers pot deixar tota l'empresa inoperativa, ja que, tot i que els ordinadors de les estacions de treball funcionin, no podran tenir accés als documents de treball.

És molt important protegir-se contra aquestes dues emergències tan comunes (en el mòdul de seguretat passiva es mostrarà com s'ha de fer).

Una altra possible emergència és la pujada de la temperatura a les sales on es tenen ubicats els equips informàtics que fan les feines de servidors. Aquestes màquines, que funcionen contínuament, en molts casos les vint-i-quatre hores del dia i els set dies de la setmana (24 × 7). No s'acostuma a apagar un servidor encara que sigui cap de setmana, ja que s'aprofiten aquestes hores de baix rendiment per a fer les tasques de manteniment i les còpies de seguretat.

Per tant, els equips emeten contínuament calor de les fonts d'alimentació i la resta de components de l'equip com el processador, de manera que cal dissipar-lo col·locant algun sistema de refrigeració a la sala on estiguin ubicats. Si aquest calor no s'extreu, pot provocar que s'aturin automàticament, que es redueixi la vida útil dels components i fins i tot un mal funcionament de l'equip.

D'altra banda, si un servidor ha de funcionar en règim de vint-i-quatre hores del dia i els set dies de la setmana –per exemple, s'ha de mantenir en funcionament una base de dades contínuament–, cal tenir previst què passa quan aquest equip s'avaria o deixa de donar servei per qualsevol anomalia. Cal disposar d'un altre equip amb el qual es pugui garantir el servei les vint-i-quatre hores del dia i els set dies de la setmana, de manera que cal configurar els servidors perquè es passin informació amb la finalitat que si n'hi ha un que deixa de funcionar, l'altre pugui fer de servidor principal, sense que l'organització quedi afectada per aquest fet.

Hi ha diverses maneres de garantir això: servidors de reserva, rèpliques de discos, RAID, etc. Això ho veurem en els mòduls següents.

1.3. Servidors de fitxers

El més usual és que les mitjanes i sobretot les grans empreses tinguin un servidor, o més, per a concentrar en un únic punt tots els documents i l'altra informació de l'empresa. D'aquesta manera es tenen molt més controlades les dades amb la finalitat de fer-ne còpies de seguretat, dur a terme els possibles plans de risc i controlar els accessos a la informació. S'han de tenir en compte les lleis d'accés a les dades personals; una empresa pot tenir dades personals dels seus clients o usuaris en les bases de dades, i no tothom ha de tenir accés a aquestes dades.

Normalment només es fan les còpies de les dades d'aquests servidors, i així s'evita fer còpies de seguretat dels equips dels usuaris, ja que val més garantir la disponibilitat de les dades més importants col·locant-les en un servidor i protegir-les degudament que no pas tenir-les distribuïdes pels equips client i que s'hagin de fer còpies de seguretat de tots els equips. Les dades estarien distribuïdes per molts ordinadors i es faria molt més difícil fer-ne eltractament i control d'accés. A més, seria necessari tenir plans de risc per a cadascun d'aquests equips. Per altra banda, amb la creixent mobilitat dels usuaris es complicaria encara més la realització de còpies de seguretat. Tot i això, en alguns casos molt concrets sí que es fan còpies de seguretat dels sistemes client, però no per a assegurar les dades, sinó per a poder recuperar el sistema molt més ràpidament si és el cas d'un ordinador crític en el seu funcionament.

Amb el servidor de fitxers, per tant, es garanteix de manera centralitzada la privadesa de les dades, i l'accés a les aplicacions i les dades específiques per a cada tipus d'usuari de la xarxa. Per exemple, en una empresa d'arts gràfiques que tingui un departament d'edició gràfica i un altre de comptabilitat, els treballadors que pertanyin al departament d'arts gràfiques no necessiten accedir a les dades del de comptabilitat (no han de tenir accés a les dades dels pressupostos de l'empresa, per exemple). En canvi, els treballadors del departament de comptabilitat poden tenir accés a les edicions gràfiques, als productes finals, per si els fes falta.

D'altra banda, també cal configurar les aplicacions: els dos grups de treballadors no han de veure les mateixes aplicacions, no cal que vegin totes les aplicacions instal·lades en els servidors de fitxers, sinó que n'hi ha prou que cada departament vegi les aplicacions que necessiten. Això només es podrà fer amb les aplicacions que estiguin preparades per a ser instal·lades en servidors i els ordinadors de taula es connectin com a client a aquests servidors per a poder fer servir l'aplicació.

Ocultació d'aplicacions i fitxers

Aquest procediment es pot fer mitjançant perfils o grups d'usuaris. Cada treballador ha de pertànyer a un grup o uns quants grups d'usuaris d'aplicacions. Cada grup s'ha de definir amb un accés específic a un grup d'aplicacions. D'aquesta manera, creem una classificació d'aplicacions i una d'usuaris, cosa que permet crear relacions entre elles.

Així, doncs, relacionant aplicacions amb grups de persones tindrem més ben protegida la informació dins de la mateixa empresa. Molts dels problemes de seguretat que tenen les empreses són deguts pels treballadors mateixos, interns, o externs, que puntualment accedeixen a informació important, de manera que la poden eliminar o modificar, voluntàriament o involuntàriament,

ja sigui perquè tenen permís per a accedir-hi o simplement perquè la política de protecció de dades està mal implementada i ho permet tot. És important tenir en compte això en el moment d'instal·lar el sistema, i tenir molt clar quin tipus d'usuari ha de tenir accés a les dades més crítiques, o simplement les dades a les quals no ha de tenir accés, ja que no és part de la seva feina.

Quan es doni d'alta un nou treballador a l'empresa, només s'ha d'associar a un grup d'usuaris dels que ja s'han creat perquè tingui accés únicament a la informació que sigui necessària per a la seva feina.

Exemple

Seguint amb l'exemple anterior de l'empresa d'arts gràfiques, es pot definir el grup de comptabilitat, al qual s'associaran les aplicacions de base de dades, comptabilitat, fulls de càlcul, recursos humans, etc. I el grup d'edició, al qual s'associaran les aplicacions de retoc fotogràfic, edició de text professional, etc. Els dos grups tindran aplicacions diferents a partir de les tasques que han de fer. A partir d'aquests grups, s'aniran col·locant en un grup o l'altre en funció de les tasques que hagi de fer cada persona.

1.4. Servidor web

Actualment és molt usual que les empreses tinguin un lloc web en què ofereixen els seus serveis i donen informació sobre l'empresa mateixa. Algunes de les pàgines web ofereixen una part privada, on es té accés a les dades més confidencials de l'empresa i que poden ser necessàries per a poder fer alguna tasca fora de l'empresa.

Per a accedir a aquestes pàgines web s'ha d'instal·lar en algun equip informàtic un servidor de fitxers a Internet, més conegut com a servidor web. Aquest servirà cap a Internet els fitxers de la pàgina web a petició dels clients remots que la volen visualitzar.

Evidentment, per a accedir a la informació de l'empresa des de qualsevol punt d'Internet s'ha d'obrir l'accés al servidor, de manera que com a mínim ja hi haurà una porta d'accés oberta al servidor. Per tant, si més no, aquest sistema informàtic tindrà una porta oberta directament a la xarxa Internet, cosa que és un perill si no es configura correctament l'accés a aquestes dades des de l'exterior.

S'ha d'instal·lar el servidor de llocs web de manera segura, és a dir, s'ha de fer de manera que ningú no tingui accés al disc del servidor mitjançant el directori de fitxers del servidor de llocs web i, si és possible, que el servidor de fitxers no sigui el mateix que el servidor de llocs web.

Hi ha maneres molt senzilles de protegir mínimament els documents i directoris als quals no volem que s'accedeixi des de l'exterior; per exemple, es pot fer que l'usuari extern no es connecti al servidor de llocs web com a administrador o superusuari del sistema. I encara que sembli estrany, no és estrany que passi això, ja que la instal·lació del gestor de llocs web es fa des de l'usuari administrador, de manera que, si no es canvia, s'hi accedeix amb aquest perfil,

i es té accés a tota la màquina. Sempre hi ha petits detalls que cal cuidar per a protegir correctament el servidor, tot i que les darreres versions dels servidors web ja han canviat aquest procés d'instal·lació i un cop ha finalitzat el procés canvien l'usuari amb què s'executarà el procés del servidor web.

Un altre problema del servidor web són els accessos al directori d'arxius: cal protegir-nos dels accessos a la recerca de documents, ja que si no desactivem la possibilitat de veure el contingut del directori qualsevol persona pot veure els fitxers que té emmagatzemats el servidor de llocs web. Així, es pot arribar a obtenir informació de l'empresa que no es vol que sigui pública. Molts cops una estructura de fitxers i carpetes pot mostrar els diferents departaments o fins i tot noms d'usuari del sistema i ajudar els atacants que vulguin obtenir dades privades de l'empresa.

Cal assenyalar que en els directoris on hi ha els arxius dels llocs web no s'ha d'emmagatzemar res que no sigui estrictament necessari per a visualitzar correctament la informació pública de l'empresa. No s'ha de col·locar informació no volguda en els directoris públics del web de l'empresa. O, com ha passat algun cop, comentaris que revelen informació en el codi font de les pàgines web.

1.5. Servidor de xarxes virtuals privades

En alguns casos concrets, tot i que cada vegada més, els treballadors de l'empresa s'han de connectar des d'un altre lloc, des de l'ordinador del client, per exemple, situat fins i tot en un altre país. En aquestes empreses caldrà fer servir aquestes xarxes privades virtuals o VPN per a donar servei als comercials o treballadors que necessiten tenir accés de manera segura a les dades de l'empresa des de l'exterior. Fins i tot poden donar servei a l'anomenat *teletreball*, en què els treballadors ja no van a l'oficina, sinó que treballen des de casa o des de qualsevol altra part del món. Aquests treballadors s'han de poder sentir segurs a l'hora de fer servir xarxes insegures per a poder pujar o baixar fitxers dels servidors de l'empresa.

Necessitem instal·lar un canal segur pel qual l'ordinador client es connecti al servidor de manera segura. S'ha de xifrar la informació que circula en tots dos sentits perquè no hi pugui accedir ningú.

Evidentment, aquesta mena de connexió és molt més segura que la que es pot fer mitjançant els famosos Telnet o FTP. Aquestes connexions no ofereixen cap mena de seguretat, de manera que no se'n recomana l'ús en servidors en què la seguretat és primordial. Val més utilitzar qualsevol altre protocol de comunicació segur, com per exemple el *secure shell* (SSH).

1.6. Servidors de correu electrònic

Igual que en el cas dels servidors de llocs web, i especialment de l'SSH, el correu electrònic és una porta d'entrada per a qualsevol persona al servidor, ja que ha de tenir algun port obert per a rebre i enviar els correus electrònics. Cal anar amb compte amb els servidors de sortida de correu, els SMTP, ja que si no els configurem correctament i es tanca únicament el correu de sortida de l'empresa, es pot convertir en una porta de sortida de correus externs a l'empresa que utilitzaran el servidor de sortida del correu com a servidor SMTP propi. És a dir, que terceres persones poden fer servir el servidor d'enviament de correu electrònic de l'empresa com a servidor propi mitjançant la xarxa Internet. Això pot fer que l'empresa tingui innombrables problemes, com per exemple l'enviament mitjançant el servidor de l'empresa de correu perillós (correu brossa, pornografia infantil, etc.) sense que els correus electrònics que s'envien siguin de l'empresa.

El servidor de sortida de correu s'ha de configurar perquè només el puguin utilitzar les persones que estan donades d'alta en l'organització, mitjançant el simple fet d'instal·lar el servidor de correu sortint segur, amb autenticació de l'usuari que accedeix al servei. Això s'aconsegueix enviant els correus del client al servidor de correu sortint pel port 25 (port per defecte de les aplicacions SMTP) amb xifratge de la informació. Antigament era usual que el servidor SMTP no fes cap mena de comprovació i només calia enviar un correu amb el format correcte al port 25 perquè aquest servidor l'encaminés cap a Internet, i evidentment això feia que el servidor SMTP el poguessin fer servir terceres persones alienes a l'empresa.

Per al servidor de correu entrant també hi ha la possibilitat d'activar un canal segur entre el servidor de correu i el client que consulta el correu que ha rebut. Això també és important, ja que permet que la circulació de dades entre els dos punts sigui segura.

Si el client de correu (per exemple, Thunderbird, Kmail, Outlook, Eudora, etc.) (1) accedeix al servidor de correu entrant pel port 110, rebrà els missatges en format normal, de manera que qualsevol intrús que estigui "detectant[1]" la xarxa podrà obtenir les dades que s'estan rebent, ja que viatgen en text pla per la xarxa, interna o fins i tot per Internet.

(1) *Detectar una xarxa* significa accedir-hi mitjançant algun sistema físic i obtenir els paquets d'informació que passen per aquesta xarxa.

Per a augmentar la seguretat de l'empresa, , s'instal·la de manera segura el servidor de correu, mitjançant l'ús del protocol SSL: l'aplicació de correu que tingui el client ha de fer les consultes pel port 995 i donar el nom d'usuari de la xarxa. Mitjançant aquest simple canvi en la instal·lació del servidor de correu ens podem estalviar molts problemes de seguretat a la xarxa, ja que cada dia més s'envia tota mena d'informació (alguna d'important i confidencial) mitjançant el correu electrònic. Pel sol fet d'enviar contínuament informació per la Xarxa, arriba un moment en què ja no som conscients que el correu

s'envia en obert, és a dir, sense xifrar o codificar, de manera que tot el que s'envia com a correu electrònic és susceptible que ho llegeixin fàcilment altres persones.

1.7. Servidors FTP

Com ja s'ha comentat en els apartats anteriors de servidors de llocs web i xarxes virtuals, per a maximitzar la seguretat el millor és treballar sempre amb el protocol SSL, és a dir, que en comptes d'instal·lar el servidor FTP val més instal·lar el servidor SFTP (SecureFTP), que fa servir el protocol SSL per a xifrar la comunicació entre els dos punts de la connexió.

Això ens assegura, a més d'una bona política de claus d'accés dels usuaris, que el canal pel qual circula la informació entre el servidor de fitxers i el client que accedeix a aquest servidor mitjançant FTP sigui segur, és a dir, que una vegada establert el canal no es pugui accedir a les dades que circulen per la xarxa.

1.8. Virtualització

Cada cop més les empreses opten per la instal·lació de servidors virtualitzats, ja que ofereixen molts avantatges i pocs inconvenients. La virtualització consisteix a tenir un únic servidor amb unes prestacions més elevades del que seria necessari per a un servidor convencional, però que en lloc de tenir un únic servidor en té uns quants de manera virtual. Mitjançant un programari específic es creen màquines fictícies que es configuren com a servidors, i d'aquesta manera es disposa d'una única màquina física, però de més d'un servidor dins d'aquesta màquina.

Això permetrà tenir tants servidors com sigui necessari amb l'única inversió en maquinari inicial, amb un sol equip informàtic. Per tant, l'estalvi en maquinari és molt gran, a més de tenir en compte que el grau de dissipació de calor ara només ve d'una única màquina en comptes de tenir-ne moltes. Evidentment, el consum d'electricitat també es reduirà pel mateix concepte.

Un altre avantatge molt important és que si es configura correctament les màquines virtuals són independents del maquinari; per tant, en el cas que un servidor real deixés de funcionar només caldria copiar els fitxers de la màquina virtual a un altre servidor per a tenir, en pocs minuts, un altre cop en funcionament el sistema informàtic virtualitzat. Ara és molt més fàcil fer una còpia de seguretat de tot el sistema, ja que només caldrà fer la còpia dels fitxers del programari de virtualització.

2. Tallafocs

Exemple de tallafoc
Font: (CC). lindztrom

Un dels temes més importants que cal tenir en compte en la seguretat d'un servidor és el dels tallafocs o *firewalls*. N'hi ha de dos tipus: els tallafocs de maquinari i els de programari.

Els primers són un dispositiu físic, normalment petit, que connectem a l'entrada de la xarxa de la companyia, de manera que tota la informació que vol entrar o sortir de la xarxa interna ha de passar per aquest aparell. Realment és com si el cable Ethernet de la xarxa de la companyia, en lloc de connectar-se directament a l'encaminador (*router*) del proveïdor dels serveis d'Internet, posem aquest aparell just al mig, de manera que talla totes les comunicacions que van dels ordinadors cap a la xarxa i només deixa passar les que s'hagin configurat prèviament com a permeses.

És a dir, en el punt de sortida de la xarxa interna (LAN) a la xarxa Internet (WAN), i d'entrada de la WAN a la LAN, hi ha el tallafoc, que ens atura totes les trames de dades d'entrada de la xarxa que no vagin precedides d'una trama interna, és a dir, trames de dades que no s'han sol·licitat des de dins de la LAN mateixa a partir d'una aplicació permesa o d'un port obert.

En canvi, els tallafocs implementats mitjançant programari són programes que s'executen en les màquines client, tant si són els servidors mateixos com els equips informàtics dels treballadors.

Aquest últim cas és el més habitual en empreses petites i en entorn més domèstics, tot i que hi ha molts models de tallafocs petits que donen molt bon rendiment a uns preus molt baixos.

Pel fet de ser programes que no deixen d'estar fets per persones, aquests darrers tallafocs són més vulnerables a atacs i a males configuracions que no pas els tallafocs físics, en els quals, tot i poder-hi haver vulnerabilitats i males configuracions, és més difícil de saltar-se les regles establertes. No deixen de ser programes que s'executen en màquines que tenen accés lliure a Internet. Un mal funcionament del programari del tallafoc o de la màquina mateixa fa que el tallafoc no sigui efectiu.

Evidentment, cadascun té avantatges i inconvenients. Els primers són complicats d'instal·lar i configurar, i a més són considerablement més cars que els segons, que són molt barats, i fins i tot n'hi ha que són completament gratuïts per als equips dels usuaris, i resulten fàcils d'instal·lar i configurar.

En canvi, com a avantatge dels tallafocs maquinari podem trobar la robustesa, ja que si no s'està connectat directament a l'equip real no es pot configurar, o no és aconsellable permetre que es pugui configurar directament des de la xarxa WAN, encara que evidentment sí que s'hauria de permetre fer-ho mitjançant la xarxa LAN de l'empresa.

3. Comparació del Windows respecte del GNU/Linux

En general la seguretat informàtica en els servidors que s'instal·len a les empreses que volen oferir algun tipus de servei per Internet, o simplement que volen tenir emmagatzemades en un lloc segur les seves dades, és, evidentment, un concepte que no entén de marques, ni de filosofies de llicències, ni de termes legals. La seguretat informàtica en els servidors ha d'estar per sobre de tot, fins i tot del sistema operatiu que es decideix instal·lar.

Aquí ens centrarem únicament en els dos sistemes operatius més utilitzats en la instal·lació de servidors: la família de servidors de Microsoft Windows i GNU/Linux.

Entrarem detalladament en la manera com es configuren algunes de les diferents eines de seguretat de tots dos sistemes i, per tant, no veurem en aquest material els altres sistemes operatius, tan vàlids com aquests dos que hem seleccionat. Un exemple de sistema corporatiu que també cuida molt la seguretat és l'AS400 d'IBM, i també el Solaris de SUN, que està basat en Unix, igual que Linux.

És evident que la marca Microsoft, per a algunes persones, representa seguretat i imatge d'empresa solvent competent, i per a d'altres, una empresa que només mira de fer diners a costa de crear productes amb molts errors o *bugs* i molts forats de seguretat.

Tant els primers usuaris com els segons tenen la seva part de raó; la veritat sempre és relativa en aquests casos. El que no es pot negar és que actualment els productes de Microsoft són els més utilitzats en els ordinadors personals, tant els domèstics com els clients terminals de les empreses, i que com a imatge d'empresa té una molt bona presència en el sector; una altra cosa és el que pensen de l'empresa les persones que estan més vinculades al món del programari lliure. No es pot negar, però, que Microsoft és un estàndard *de facto*.

En canvi, GNU/Linux és vist per les empreses grans com un producte fet per molta gent, sense un lideratge seriós, i com un producte que segurament els portarà problemes, ja que la companyia Microsoft ha donat la imatge que el seu sistema operatiu només l'hem de connectar i ja el tenim a punt per a treballar, encara que, en realitat, en alguns casos també es produeixen problemes.

Aquesta visió ja no s'ajusta a la realitat. Actualment el sistema operatiu GNU/Linux es desenvolupa constantment, se'n treuen noves versions i s'arreglen les vulnerabilitats molt més ràpidament que en altres companyies de sistemes operatius. Fins i tot hi ha empreses dedicades a proporcionar suport tècnic i muntar l'estructura del sistema informàtic basat en aquest sistema operatiu

lliure. Les millores en el sistema operatiu que proposen els programadors sempre les ha de supervisar l'equip de persones que s'encarreguen de cada distribució. No és un sistema operatiu que es basi en les aportacions de persones distribuïdes arreu del món, sinó que hi ha organitzacions que s'encarreguen de millorar i validar les successives versions del sistema operatiu GNU/Linux.

Podríem comparar els dos sistemes operatius en dos punts: pel que fa a seguretat i pel que fa a costos, per exemple.

La seguretat en GNU/Linux és una de les primeres coses que es va tenir en compte a l'hora de crear el sistema operatiu, ja que des del principi es va pensar com un sistema operatiu multiusuari, de manera que la seguretat entre usuaris era molt important, i no es permetia que les dades dels usuaris fossin públiques entre ells. Un altre tema que s'ha de considerar pel que fa a la seguretat són els virus. Actualment són gairebé incomptables els virus que ataquen d'una manera o una altra el sistema operatiu de Microsoft, ja sigui un model en concret o tota la família de sistemes operatius de Microsoft; en canvi, per a GNU/Linux es coneixen molt pocs virus que ataquin el sistema o part d'aquest. També s'ha de tenir en compte que els atacs que aprofiten les vulnerabilitats també poden venir per les aplicacions de tercers, que poden deixar d'alguna manera el sistema desprotegit, però d'això no es pot culpar directament el sistema operatiu, ja que no és culpa seva, però en molts casos acaba rebent les conseqüències dels atacs i els forats de seguretat de les aplicacions.

Des d'un punt de vista de la seguretat, sembla que és millor GNU/Linux, però des de fa uns quants anys Microsoft ha millorat molt els seus sistemes i ara ja no permet tenir un sistema nou en el mercat que no hagi passat per totes les proves de qualitat i buscat les vulnerabilitats que s'hagin pogut provar.

Els costos de les llicències és un dels temes més importants per a les empreses. En el cas de les empreses grans, poden tenir milers de punts de treball i, per tant, també treballadors, cosa que fa incrementar considerablement el pressupost de les llicències i formacions. En canvi, en les empreses petites, que poden tenir pocs punts de treball i personal, les llicències representen molts cops un esforç considerable.

Encara que la filosofia del sistema operatiu GNU/Linux és que sigui lliure, això no vol dir que sigui gratuït, de manera que hi ha empreses que es dediquen a instal·lar i configurar els sistemes GNU/Linux. Totes les aplicacions que s'executen en aquest sistema operatiu han d'oferir el codi font perquè els usuaris d'aquests programes els puguin personalitzar segons les seves necessitats. Tot i això, el programari és gratuït.

En canvi, el sistema operatiu de Microsoft té llicències que cal pagar per a instal·lar-lo i utilitzar-lo, i a més és de propietat, és a dir, que no se n'ha fet públic el codi font, tret d'algun cas molt concret, perquè els usuaris el puguin personalitzar segons les característiques pròpies de cada empresa.

Gairebé totes les aplicacions que s'executen en el sistema operatiu de Microsoft són de propietat i tenen algun cost, ja sigui en llicències úniques o anuals, que s'han de pagar per a continuar treballant-hi, o bé no se'n té el codi font per a millorar o localitzar el programari a mida. Cada cop més, però, hi ha programari lliure que es pot fer servir sobre el sistema operatiu Windows. En són un exemple navegadors, gestors de correu, editors de textos i de fotos.

Microsoft ha optat des de fa molts anys per una política d'incloure el seu sistema operatiu en els nous ordinadors personals que es venen. Va arribar a acords, i encara els conserva, perquè els grans fabricants d'ordinadors (HP, Compaq, Dell, etc.) incloguin el seu sistema operatiu en els ordinadors personals que es venien i encara es venen. D'aquesta manera els usuaris finals tenen la sensació que només els cal comprar l'ordinador i que quan l'encenguin aquest ja funcionarà. I de fet és així. D'altra banda, també va arribar a acords amb el fabricant de xips (Intel) perquè les dues empreses intercanviessin més informació amb la finalitat de millorar el rendiment del sistema operatiu amb un processador concret.

Això els ha donat un avantatge molt important pel que fa al nombre de sistemes operatius instal·lats, ja sigui a les cases particulars o a les empreses. Ara hi ha alguna marca d'equips informàtics que ven els seus ordinadors amb els dos sistemes operatius, i és l'usuari el que decideix amb quin es queda; o fins i tot n'hi ha que en venen sense cap sistema operatiu, i és llavors l'usuari, o l'administrador de sistemes en el cas de les empreses, el que opta per comprar el sistema operatiu de Microsoft, per instal·lar GNU/Linux amb un contracte amb alguna empresa de l'estil de Suse o Red Hat, o per baixar gratuïtament d'Internet l'última distribució de GNU/Linux i instal·lar-la.

Evidentment, els costos de les llicències del programari són una bona part dels costos que tenen les empreses, i molts cops els caps no veuen les despeses en seguretat com una inversió rendible, ja que per si soles no generen beneficis per a l'empresa. Per això, actualment hi ha moltes empreses que instal·len en els equips informàtics el sistema operatiu GNU/Linux, ja que té una bona quantitat d'aplicacions que fan el mateix que les aplicacions de propietat.

Però en contrapartida, les empreses que opten per fer servir el sistema operatiu GNU/Linux es troben amb la dificultat que els empleats desconeixen majoritàriament el sistema i, per tant, han de dedicar molts diners als costos de formació i d'organitzar o contractar cursos perquè els usuaris dels ordinadors puguin treballar en un entorn que no han vist mai o gairebé mai.

En canvi, gràcies a la política de Microsoft d'incloure el sistema operatiu des de fa molts anys en els ordinadors personals, i de la facilitat amb què fins ara s'ha fet la còpia pirata d'aquest sistema, quan les empreses contracten nou personal no li han de fer cap curset de formació per a utilitzar l'ordinador.

Actualment és ben conegut el sistema operatiu Windows, i Microsoft el que fa és no sortir d'aquesta línia perquè els empresaris optin per aquest sistema operatiu amb la finalitat de reduir costos de formació en els treballadors.

Malgrat tot, actualment la diferència de funcionament per a un usuari final d'un ordinador entre els dos sistemes operatius és molt petita. Visualment els dos sistemes són molt semblants, i fins i tot les aplicacions tenen interfícies gràfiques molt semblants, com per exemple el Microsoft Office i l'OpenOffice.

4. Seguretat física

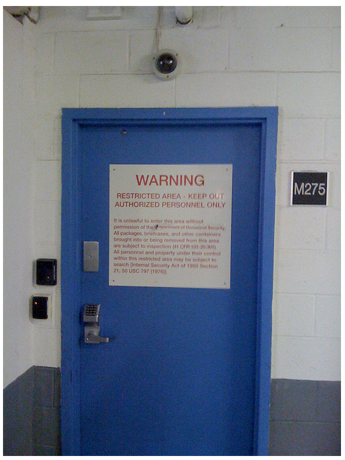
Un dels temes més importants pel que fa a la seguretat d'una empresa és la seguretat física. No serveix de gaire tenir un tallafoc molt potent i car, vigilar les entrades a la xarxa, fer còpies de seguretat de totes les dades, tenir instal·lat i molt ben configurat un bon sistema operatiu, etc., si no es té en compte la seguretat física.

Un simple ordinador en un despatx on sigui fàcil accedir per als lladres ens pot causar problemes seriosos, ja que si hi entren a robar i se l'emporten poden accedir a moltes dades de l'empresa que hi ha desades o que simplement hi ha en el perfil d'usuari que es guarda localment. En aquest ordinador es poden guardar, per exemple, números de comptes corrents, dades personals o adreces.

No seria la primera vegada que en una empresa entren uns lladres en horari laboral i s'emporten un equip informàtic mentre els treballadors són en una reunió o en una altra sala.

Per tant, un aspecte que cal tenir molt en compte és que els equips informàtics no siguin gaire accessibles per a persones no autoritzades, i sobretot els equips que fan les tasques de servidor. Ja no solament perquè els puguin robar persones externes a l'empresa, sinó perquè per distracció o error d'algun treballador es puguin apagar o entrar al sistema operatiu i desconfigurar alguna aplicació.

Per norma general, els equips que es destinen a fer les tasques de servidors s'han d'instal·lar en habitacions separades dels treballadors, tancades amb clau i amb un sistema de refrigeració tot l'any. Així s'evitaran problemes amb l'accés de persones que no estan autoritzades o que no estan familiaritzades amb aquests equips i, per tant, poden tocar el sistema sense saber exactament el que estan fent.



Porta de seguretat amb codi d'entrada
Font: (CC). Salim Virji

Una altra qüestió important pel que fa a la seguretat física és l'emmagatzematge de les còpies de seguretat o *backups*. No serveixen de gaire les cintes, DVD, o qualsevol altre sistema d'emmagatzematge d'aquestes còpies de seguretat guardades en l'oficina mateixa si es declara un incendi a l'edifici i es cremen tots els servidors i les cintes on hi havia les còpies de seguretat. Imaginem-nos els milions de dòlars que es podrien haver perdut en els casos de les torres bessones del World Trade Center, a Nova York, o la torre Windsor, a Madrid, en què el foc ho va destruir absolutament tot, si les empreses grans no haguessin tingut un bon sistema de còpies de seguretat guardat en un altre edifici o fins i tot en una altra ciutat.

Exemple

Recordem un cas més recent, en què un ajuntament d'Espanya va perdre totes les dades informàtiques quan es va cremar tot l'edifici i no tenien guardades les còpies de seguretat fora de l'edifici. Van perdre totes les dades i els històrics.

A causa d'aquests possibles accidents s'ha de desar un joc de còpies dels servidors regularment fora de les instal·lacions de l'empresa, prou lluny i protegides amb sistemes ignífugs per a assegurar que en un incendi no es perdin les dades per les flames o per l'elevada calor a què s'arriba en un gran incendi. En el mercat hi ha caixes de seguretat ignífugues, en les quals no entra el foc, però un altre tema que s'ha de tenir en compte és com pot quedar una cinta de còpia de seguretat si una caixa de ferro eleva la temperatura interior a 1.000 C per un gran incendi. Aquestes coses també les haurem de tenir en compte.

5. Contingut del material

En aquest material es veurà la instal·lació de dos servidors més o menys complets, amb quasi totes les funcionalitats que es poden necessitar. Es mostrarà la configuració de GNU/Linux i un servidor de la família de Microsoft, el gestor de correu electrònic, el servidor de llocs web, el servidor de fitxers i impressió, el servidor de còpies de seguretat, el servidor FTP, els plans de risc, la instal·lació de la xarxa i els clients d'aquesta xarxa, etc.

No es vol sobreposar un sistema operatiu sobre un altre, i per tant s'ha optat per explicar el funcionament de tots dos, de manera que a cada apartat, i després d'explicar el concepte teòric, s'explicarà com s'instal·la i es configura cadascuna de les aplicacions en els dos sistemes operatius. L'administrador de sistemes ha de decidir en cada cas què s'ha d'instal·lar, tant per al servidor com per a les estacions de treball. No és estrany trobar servidors amb GNU/Linux instal·lats i clients Windows en la mateixa xarxa.