CFGM-SMX

Mòdul professional: ***Seguretat informatica***
Codi: ***0226***
Durada: ***110 hores***

índex

Xavi Blanes 2025

Tema 1: Conceptes sobre seguretat informàtica

1. Per què cal protegir?

Parar atenció a la seguretat informàtica és crucial per diverses raons fonamentals, ja que afecta tant a individus com a empreses i organitzacions de tot tipus. Aquí tens algunes de les raons més importants per les quals és essencial preocupar-se per la seguretat informàtica:

1. Protegir la informació personal: La informació personal, com ara dades bancàries, números de la seguretat social, adreces i altres dades sensibles, es troba a les xarxes i dispositius digitals. Si aquesta informació cau a mans equivocades, pot ser utilitzada per al robatori d'identitat o altres tipus d'estafes.
2. Prevenir la pèrdua de dades: Les empreses i organitzacions emmagatzemen grans quantitats de dades importants. Un atac informàtic o una falla de seguretat poden provocar la pèrdua d'aquestes dades, amb conseqüències greus per a la continuïtat de les operacions i la confiança dels clients.
3. Evitar atacs cibernètics: Les amenaces cibernètiques, com ara virus, malware, ransomware i atacs de phishing, estan en constant augment. Protegir els sistemes i les xarxes contra aquests tipus d'atacs és essencial per evitar pèrdues de dades i danys financers.
4. Mantenir la confiança dels clients: Si una empresa no pot protegir les dades dels seus clients, això pot danyar la seva reputació i la confiança dels clients. La pèrdua de confiança pot tenir un impacte negatiu a llarg termini en els resultats financers i la continuïtat del negoci.
5. Cumpliment de la normativa: Molts països i sectors tenen regulacions específiques sobre la seguretat de la informació i la privacitat dels usuaris. No complir amb aquestes normatives pot comportar sancions legals i multes considerables.
6. Preservar la propietat intel·lectual: Les empreses i les institucions de recerca poden tenir propietat intel·lectual valuosa, com ara patents i secrets comercials. Protegir aquesta informació és essencial per mantenir la seva competitivitat i valor.
7. Previndre interrupcions de servei: Atacs informàtics com els atacs de denegació de servei (DDoS) poden interrompre els serveis en línia i causar molèsties als usuaris o clients. La seguretat informàtica adequada pot ajudar a prevenir aquest tipus d'interrupcions.
8. Protegir la infraestructura crítica: La seguretat informàtica també és important per protegir la infraestructura crítica, com ara les xarxes elèctriques, les xarxes de transport i les instal·lacions de producció. Un atac informàtic a aquestes àrees podria tenir conseqüències devastadores.

La seguretat informàtica és essencial per protegir la informació, els negocis i la societat en general contra amenaces cibernètiques. Ignorar la seguretat informàtica pot tenir conseqüències greus i costoses, per la qual caldrà prendre mesures actives per mantenir-se protegit.

Malgrat tota la nostra preocupació i totes les mesures que prenguem, la seguretat completa és impossible. Hem d'assumir que hem desplegat la màxima seguretat possible amb el pressupost assignat i la formació actual dels nostres tècnics i usuaris:

- Amb més diners podríem replicar els servidors, les connexions, el subministrament elèctric o tot alhora.

- Amb més formació en els tècnics podríem desplegar sistemes avançats de protecció, com els NIPS (Network Intrusion Prevention System).

- Amb més formació en els usuaris podríem estar tranquils perquè no compartirien la seua contrasenya amb altres usuaris, no entrarien en pàgines potencialment perilloses i, quan arribaren a casa, el portàtil o el mòbil d'empresa no l'usaria cap altre component de la seua família.

D'altra banda, podem estar segurs que en la nostra casa o en la nostra empresa estem aplicant totes les mesures, però no sabem què fan les altres persones amb les quals ens comuniquem. En l'àmbit personal, possiblement enviem imatges a algú que no sap que té un troyà en el seu ordinador, i que aquest troyà està especialitzat a difondre en Internet qualsevol imatge que troba. En el fons, tot és informació: siguen els escassos 140 caràcters d'un tweet, siguen fitxers de diversos megaoctets, estan en el nostre equip i algú pot intentar obtenir-los. La clau és la motivació: qui està interessat en la nostra informació. És poc probable que algun superhàcker intente entrar en el nostre ordinador portàtil a per les nostres fotos descarregades de la càmera o les nostres anotacions de classe, segurament no li costaria molt, però l'esforç no paga la pena.

En canvi, les empreses sí són molt més atractives per a aquestes activitats delictives. Fins a tal punt que existeixen les auditories de seguretat: contractem a una empresa externa especialitzada en seguretat informàtica perquè revise els nostres equips i els nostres procediments. Un exemple d'aquestes empreses són els tiger teams (equips tigre): intenten accedir a les nostres instal·lacions com ho faria un hàcker, per a confirmar si podem estar tranquils. D'altra banda, els mecanismes de seguretat han d'estar adaptats a cada cas particular: una contrasenya de 20 caràcters que utilitza majúscules, minúscules, nombres i signes de puntuació és molt segura, però si obliguem a que siguen així les contrasenyes de tots els empleats, la majoria l'apuntarà en un paper i la apegarà en el monitor. Qualsevol que sega en l'ordinador tindrà accés als recursos d'aquest usuari.

2. Què protegir?

A causa del pressupost, no podem aplicar totes les mesures de seguretat possibles a tots els equips de l'empresa. Hem d'identificar els actius que cal protegir: quins equips són més importants i quines mesures apliquem en cadascun. Per exemple, tots els equips han de portar antivirus i firewall. No obstant açò, l'ocupació del disc dur solament ens preocuparà en els servidors, no en els llocs de treball. De la mateixa manera, el control del programari instal·lat és molt més exhaustiu en un servidor que en un ordinador personal.

No obstant açò, el major actiu és la informació continguda en els equips, perquè un equip danyat o perdut es pot tornar a comprar i podem tornar a instal·lar i configurar totes les aplicacions que tenia. És car, i tenim el mateix ordinador o millor. Per contra, les dades de la nostra empresa són nostres, ningú pot retornar-nos-les si es perden. En aquest punt, l'única esperança són les còpies de seguretat i l'emmagatzematge redundant.

2.1. Equips

Quant a la seguretat física dels equips:

- És fonamental que no es puguen sostreure, ni l'equip sencer ni alguna peça d'aquest (principalment el disc dur).

- En el cas dels portàtils no podem evitar que isquen de l'empresa, per a que els treballadors visiten les dependències del client o es porten treball a casa. Però hem de procurar que aquests ordinadors apliquen xifrat en el disc dur i tinguen contrasenyes actualitzades, sobretot en els usuaris amb perfil d'administrador.
- És important que no es puguen introduir nous equips no autoritzats. Un hàcker no necessita trencar la seguretat d'un servidor si pot connectar-se a la xarxa de la empresa amb un equip seu. Amb el programari adequat pot realitzar l'atac. Pot introduir un troyà en algun ordinador d'un empleat...
- Aplicarem manteniment preventiu per a evitar avaries. Per exemple, en cada ordinador, una vegada a l'any, obrir la caixa per a netejar els dissipadors i els ventiladors, perquè la pols acumulada pot anul·lar la seua funció de rebaixar la temperatura del sistema.

2.2. Aplicacions

Els ordinadors d'una empresa han de tenir les aplicacions estrictament necessàries per a dur a terme el treball assignat: ni més ni menys. Menys és evident perquè impediria complir la tasca, però també hem d'evitar instal·lar programari extra ja que pot contenir vulnerabilitats que puguen danyar al sistema complet. Quan una empresa adquireix un nou equip, el personal de sistemes procedeix a maquetar-lo: instal·la les aplicacions utilitzades en aquesta empresa, cadascuna en la versió adequada per a aquesta empresa, amb la configuració particular requerida. Fins i tot pot arribar a substituir el sistema operatiu que portava l'equip per la versió que s'utilitza en l'empresa. L'objectiu perseguit és múltiple:

- Estalviar a l'usuari la tasca d'instal·lar i configurar cada aplicació (i de manera afegida evitem donar-li massa privilegis).
- Assegurar que el programari instal·lat respon a les llicències comprades en l'empresa.
- Homogeneïtzar l'equipament, de manera que solament haurem d'enfrontar-nos als problemes en una llista reduïda de configuracions de maquinari. La solució proposada s'aplica ràpidament a tots els equips afectats.

Però hem d'estar preparats perquè altres aplicacions intentaran instal·lar-se:

- Intencionadament. L'usuari llança un instal·lador del programa que ha descarregat d'Internet o ho porta de casa en un USB.
- Innocentment. L'usuari entra en una pàgina pirata que fa la descàrrega sense que ho sàpia, o introdueix un USB que desconeix que està infectat per un virus.

En tots dos casos, l'antivirus serà una barrera i l'absència de privilegis d'administració també ajudarà. Però convé aplicar altres mesures per a no posar-los a prova:

- A l'hora de crear un usuari, evitar que tinga privilegis d'administració del sistema. Encara que pot instal·lar determinades aplicacions, solament afectaran a aquest usuari, no a tots els d'aquesta màquina.
- Desactivar el mecanisme de autoarranc d'aplicacions des d'USB (en algunes empreses, en maquetar els equips d'usuari, fins i tot lleven els lectors de CD i desactiven els USB de la màquina).

La primera garantia que hem de tenir a l'hora d'instal·lar una aplicació és el seu origen: si ha arribat en un CD del fabricant o si la descarreguem del seu lloc web, o si està inclosa en el mecanisme d'actualitzacions automàtiques de la versió actual. Si el CD no és original, o si descarreguem de la web d'un altre, hem de desconfiar. Per exemple, en els telèfons

mòbils i tàblets la majoria de les aplicacions procedeixen de Google Play en Android, o App Store en iPhone). Utilitzem la seua opció de cerca, mirem que el nombre de descàrregues siga elevat i la baixem. Durant la instal·lació ens demana permís per a fer algunes coses en l'equip, encara que no té molt sentit perquè el 99 % dels usuaris no sap què li està preguntant i sempre accepta. En el fons, confiem que l'aplicació no és perillosa perquè l'hem trobat en el lloc oficial, on se suposa que la proven abans de penjar-les.

2.3. Dades

Com hem dit abans, les màquines i les aplicacions es compren, però les dades de la nostra empresa són exclusivament d'ella. Cal protegir-les per dos aspectes:

- Si desapareixen, l'empresa no pot funcionar amb normalitat.
- Si arriben a les mans de la competència, l'estratègia empresarial i el futur de la companyía estaran en risc.

Les empreses modernes responen a l'esquema de «oficina sense papers»: estan informatitzades totes les dades que entren, les generades internament i les que comuniquem a l'exterior. La infraestructura necessària és àmplia i complexa perquè els nivells de seguretat són elevats:

- Tots els equips han d'estar especialment protegits contra el programari maliciós que puga robar dades o alterar-les.
- L'emmagatzematge ha de ser redundant: gravem la mateixa dada en més d'un dispositiu. En cas que ocórrega una fallada de maquinari en qualsevol dispositiu, no hem perdut la informació.
- L'emmagatzematge ha de ser xifrat. Les empreses tracten informació molt sensible, tant les dades personals de clients o proveïdors com els seus propis informes, que poden ser interessants per a la competència. Si, per qualsevol circumstància, perdem un dispositiu d'emmagatzematge (disc dur, pendrive USB, cinta de backup), les dades que continga han de ser inútils per a qualsevol que no puga desxifrar-les.

2.4. Comunicacions

Les dades no solen estar recloses sempre en la mateixa màquina: en molts casos ixen amb destinació a un altre usuari que les necessita. Aquesta transferència (correu electrònic, missatgeria instantània, disc en xarxa, servidor web) també cal protegir-la. Hem d'utilitzar canals xifrats, fins i tot encara que el fitxer de dades que estem transferint ja estiga xifrat (doble xifrat és doble obstacle per a l'atacant). A més de protegir les comunicacions de dades, també és tasca de la seguretat informàtica controlar les connexions a la xarxa de l'empresa. Sobretot amb l'expansió del teletreball, que permet aprofitar Internet per a treballar en la xarxa interna com si estiguérem asseguts en una taula de l'oficina. Ara les xarxes de les empreses necessiten estar més obertes a l'exterior, després estaran més exposades a atacs des de qualsevol part del món.

El perill també està en la pròpia oficina: no pot ser que qualsevol visitant entre en la nostra xarxa amb solament connectar el seu portàtil a una presa de la paret o a través de la wifi de la sala d'espera. Un hàcker segurament no coneix els usuaris i contrasenyes dels administradors de cada màquina, però pot introduir programari maliciós que prove de endevinar-ho, aprofitar vulnerabilitats no resoltes en les nostres aplicacions per a desplegar cucs que resten rendiment a la xarxa, etc. Un segon objectiu de la supervisió de les comunicacions és evitar l'arribada de correu no desitjat (spam) i publicitat en general.

Amb açò alliberem part de la ocupació de la connexió a Internet, reduïm la càrrega dels servidors de correu (així com l'ocupació de disc), els nostres usuaris no patiran distraccions i finalment evitem atacs camuflats en aquests correus.

La tendència actual en les empreses és migrar els seus sistemes a Internet (cloud computing). Les més endarrerides encara es limiten a disposar del servei de correu electrònic amb el seu propi domini (@lameuaempresa.com) i penjar la pàgina web en algun servidor compartit (hosting), però moltes ja utilitzen l'emmagatzematge en web (per exemple, Dropbox i Google Drive per a usuaris individuals, S3 de Amazon per a empreses) i algunes estan desplaçant tota la seua infraestructura informàtica a servidors virtuals situats en algun punt del planeta amb connexió a Internet (de nou Amazon amb el seu EC2).

Realment fa molt que utilitzem cloud computing: tots els webmail (Gmail, Hotmail, etc.) són serveis de correu electrònic que no estan en els nostres ordinadors, sinó que ens connectem a ells mitjançant un navegador per a enviar, rebre i llegir els missatges, sense importar-nos quants servidors o equips de xarxa ha necessitat desplegar aquesta empresa perquè tot funcione amb normalitat. Quan s'opta pel cloud computing en una empresa, la primera premissa ha de ser la seguretat en les comunicacions, perquè tots aquests serveis estan en màquines remotes a les quals arribem travessant xarxes de tercers.

3. Definicions

Per a fixar els conceptes relacionats amb la seguretat informàtica anem a intentar elaborar un xicotet diccionari. Utilitzarem exemples de la vida real per a comprovar que la seguretat està a tot arreu, no solament en els ordinadors.

3.1. Seguretat física/lògica, activa/passiva.

La seguretat física s'ocupa dels equips informàtics: ordinadors de propòsit general, servidors especialitzats i equipament de xarxa. La seguretat lògica es refereix a les diferents aplicacions que s'executen en els equips.

Les amenaces contra la seguretat física són:

- Desastres naturals (incendis, inundacions, enfonsaments, terratrèmols). Els tenim en compte a l'hora de situar l'emplaçament del centre de processament de dades (CPD), on allotgem els principals servidors de l'empresa. Però, encara que tinguem el millor sistema d'extinció d'incendis o la sala estiga perfectament segellada, sempre hauríem de tenir un segon CPD per a que l'activitat no pare.
- Robatoris. Els nostres equips, i sobretot la informació que contenen, resulten valuosos per a altres individus o organitzacions. Hem de protegir l'accés a la sala del CPD mitjançant múltiples mesures de seguretat: vigilants, targetes d'accés, identificació mitjançant usuari i contrasenya, etc.
- Fallades de subministrament. Els ordinadors utilitzen corrent elèctric per a funcionar i necessiten xarxes externes per a comunicar-se amb altres empreses i amb els clients. Aquests serveis els contractarem amb determinats subministradors, però hem d'estar preparats per a les ocasions en què no puguen proporcionar-lo: unes bateries o un grup electrògen per si falla el corrent, una segona connexió a Internet (fins i tot podem optar per una solució sense fil) per a estar protegits davant un tall en el carrer.

Les amenaces contra la seguretat lògica són:

- Virus, troyans i malware en general. Com ocorre amb el spam en el correu electrónic, el malware és programari no desitjat i que hem d'eliminar.
- Pèrdua de dades. Un defecte en el codi font d'una aplicació, o una configuració defectuosa de la mateixa, pot ocasionar modificacions inexplicables en la informació emmagatzemada, fins i tot la pèrdua de dades. Per a reduir aquest risc, les empreses proven molt bé una aplicació abans de decidir utilitzar-la i, sobretot, realitzen còpies de seguretat en diversos punts del processament de la informació per a poder recuperar-se sense perdre-ho tot.
- Atacs a les aplicacions dels servidors. Els hàckers intentaran entrar a per les dades aprofitant qualsevol vulnerabilitat del sistema operatiu o de les aplicacions que executen en aquesta màquina (per açò convé tenir instal·lat el programari mínim imprescindible).

D'altra banda, podem parlar de seguretat activa i seguretat passiva. La seguretat passiva són tots els mecanismes que, quan patim un atac, ens permeten recuperar-nos raonablement bé. Per exemple, les bateries davant una caiguda de tensió o la còpia de seguretat quan s'ha desbaratat la informació d'un disc. La seguretat activa intenta protegir-nos dels atacs mitjançant l'adopció de mesures que protegisquen els actius de l'empresa, com vam veure en l'epígraf anterior: equips, aplicacions, dades i comunicacions.

3.2. Confidencialitat, disponibilitat, integritat i no repudi

La confidencialitat intenta que la informació solament siga utilitzada per les persones o màquines degudament autoritzades. Per a garantir la confidencialitat necessitem disposar de tres tipus de mecanismes:

- Autenticació. L'autenticació intenta confirmar que una persona o màquina és qui diu ser, que no estem parlant amb un impostor.
- Autorització. Una vegada autenticat, els diferents usuaris de la informació tindran diferents privilegis sobre ella. Bàsicament dos: solament lectura, o lectura i modificació.
- Xifrat. La informació estarà xifrada perquè siga inútil per a qualsevol que no supere l'autenticació.

Vegem alguns exemples del món real:

- Per a entrar a un estadi de futbol es necessita una entrada (autenticació), però uns aniran a tribuna i uns altres a una llotja VIP (autorització).
- Per a traure diners d'un caixer necessites una targeta i el PIN d'aquesta targeta (autenticació).
- En arreplegar un enviament certificat necessites portar el DNI, perquè comproven que eres tu (autenticació).
- En els parcs temàtics cal portar una entrada (autenticació) i, si pagues una mica més, tens un fast-pass para no fer cua en les atraccions (autorització).

L'objectiu de la integritat és que les dades queden emmagatzemats tal com espera l'usuari: que no siguen alterats sense el seu consentiment. Un exemple seria l'identificador del compte bancari, que té quatre grups de nombres:

- Quatre dígits del codi del banc.
- Quatre dígits del codi de la sucursal del banc on hem obert el compte.
- Dos dígits de control.

- Deu dígits per al codi del compte, dins de totes les obertes en aquesta sucursal.

Els dígits de control s'obtenen per combinació numèrica dels altres 18 nombres. Aquesta combinació és una operació matemàtica que ens assegura que qualsevol xicotet canvi en algun dels 18 nombres generaria uns dígits de control diferents. És a dir, si volem fer una transferència bancària per telèfon i, en dictar el número de compte, canviem sense voler algun dels dígits (és igual qualsevol dels 20), qui apunta aquest número de compte no podrà operar amb ella perquè és un nombre invàlid, ja que els dígits de control no corresponen als altres 18.

La disponibilitat intenta que els usuaris puguen accedir als serveis amb normalitat en l'horari establert. Per a açò s'inverteix en sobredimensionar els recursos:

- Una tenda té dues datáfonos amb dos bancs diferents. Així sempre pot oferir el cobrament per targeta.
- Un equip de futbol té diversos suplents en la banqueta. Així sempre pot intentar mantenir onze jugadors quan algun es lesiona.
- Els avions porten pilot i copilot.
- Quan es fan obres entre dues estacions de metro, hi ha una línia d'autobusos que porta d'una a l'altra per superfície, i el tiquet és el mateix.

El no repudi es refereix al fet que, davant una relació entre dues parts, intentarem evitar que qualsevol d'elles puga negar que participara en aquesta relació. Hi ha molts exemples de la vida real:

- Els contractes se signen per les dues parts. Per exemple, la hipoteca d'una casa.
- Signem l'imprès de matriculació en un cicle formatiu.
- En algunes targetes de crèdit cal signar un paper amb les dades de la compra, i la tenda es queda una còpia.
Conservem el tiquet de compra per a poder sol·licitar la devolució.
- Quan fem una reserva de vol obtenim un localitzador i a l'hora de retirar el bitllet no poden negar que vam fer la reserva.

3.3 Saps tens eres

L'autenticació és especialment important en temes de seguretat. Hem d'estar molt segurs de la identitat de la persona o sistema que sol·licita accedir a nostra informació. Un esquema molt utilitzat per a analitzar l'autenticació és classificar les mesures adoptades segons tres criteris:

- Alguna cosa que saps. Per a accedir al sistema necessites conèixer alguna paraula secreta: la típica contrasenya.
- Alguna cosa que tens. En aquest cas és imprescindible aportar algun element material: generalment una targeta.
- Alguna cosa que eres. El sistema sol·licita reconèixer alguna característica física de l'individu (biometria): empremta dactilar, escàner de retina, reconeixement de veu, etc.

L'autenticació serà més fiable quants més criteris diferents complisca:

- Per a entrar a casa solament ens cal una clau (alguna cosa que tens). Però en alguns països europeus els portals tenen un codi (alguna cosa que saps).

- Per a entrar a un ordinador, generalment necessitem un usuari (alguna cosa que saps) i una contrasenya (alguna cosa que saps).
- Per a traure diners d'un caixer necessitem una targeta (alguna cosa que tens) i introduir un PIN (alguna cosa que saps). En canvi, en la web del banc solament necessitem un usuari (que sol ser nostre DNI, relativament fàcil de localitzar) i un PIN (alguna cosa que saps).
- Per a arreplegar en Correus un enviament certificat o per a identificar-te a la Policia, cal aportar el teu DNI (alguna cosa que tens) i que siga la teua cara la que apareix (alguna cosa que eres).

Els sistemes biomètrics no sempre s'apliquen en entorns de molt alta seguretat. Per exemple, poden estar en el menjador de l'empresa, comprovant qui és emprat i qui no per a decidir sol·licitar el pagament del menú.

3.4. AAA

La sigla AAA es refereix a autenticació, autorització i accounting. Les dues primeres ja les hem vist amb anterioritat, la tercera es refereix a la informació interna que els sistemes generen sobre si mateixos. Concretament, l'ús que es fa dels seus serveis. Aquesta informació serveix per a revisar el dimensionament dels equips i, degudament associada a cada departament de l'empresa, permet establir limitacions i penalitzacions. Però la informació del accounting també permet comprovar l'eficàcia de les mesures d'autenticació i autorització, sobretot en una anàlisi forense després d'un atac. Seguint el rastre podrem localitzar per on ha entrat i intentar resoldre-ho. Per aquest motiu, és important que el registre del accounting es faça en una màquina diferent: si el hàcker ha aconseguit entrar, podria fàcilment esborrar les seues petjades. Per contra, si el registre es fa simultàniament en una altra màquina, ja són dues les màquines que ha d'atacar (i generalment la màquina de registre es carrega amb el mínim programari possible, per a reduir les opcions d'entrada).

3.5. i2i

i2i significa extrem a extrem: la seguretat ha de controlar-se en l'origen de les dades, en la destinació de les dades i en el canal de comunicació utilitzat entre origen i destinació:

- En l'origen i en la destinació intentarem que l'equip i les aplicacions no hagen sigut modificats. Si algun no està sota el nostre control, hem de desconfiar.
- En el canal intentarem limitar qui accedeix i, sobretot, xifrarem, perquè les nostres dades travessaran les xarxes d'altres companyies. Sobre els seus equips i el personal que opera amb ells no tenim cap control, aleshores: hem de desconfiar.

3.6. Vulnerabilitat, malware, exploit

El programari està fet per humans, després hem d'estar preparats per a patir els errors introduïts durant la seua programació. Poden ser lleus (algun missatge mal traduit), greus (corrupció de dades) i crítics (un forat de seguretat dóna accés lliure a dades confidencials).

Una vulnerabilitat és un defecte d'una aplicació que pot ser aprofitat per un atacant. Si ho descobreix, l'atacant programarà un programari (anomenat malware) que utilitzarà aquesta vulnerabilitat per a prendre el control de la màquina (exploit) o realitzar qualsevol operació no autoritzada. Hi ha tres tipus de vulnerabilitats:

- Vulnerabilitats reconegudes pel subministrador de l'aplicació i per a les quals ja té un pegat que les corregeix. Si la nostra empresa utilitza aquesta aplicació, ha d'aplicar el pegat immediatament.

- Vulnerabilitats reconegudes pel subministrador, però encara no hi ha un pegat. En alguns casos es proporciona una solució temporal (workaround), però, generalment, és millor desactivar el servei fins a haver aplicat el pegat.
- Vulnerabilitats no reconegudes pel subministrador. És el pitjor cas, perquè podem estar exposats a un atac durant un temps llarg sense saber-ho.

Els fabricants de programari intenten reaccionar ràpidament davant qualsevol informe que demostre una vulnerabilitat en els seus programes. Gràcies a Internet, de manera programada, els programes connecten amb la web del seu subministrador per a comprovar si hi ha algun pegat pendent d'aplicar (actualitzacions automàtiques). És a dir, no esperen al fet que l'administrador de la màquina comprove un a un l'estat de tots els programes instal·lats, perquè pot passar temps des que s'allibera el pegat fins que l'administrador s'assabenta, el descarrega i l'aplica.

Hi ha molts tipus de malware:

- Virus. Intenten deixar inservible l'ordinador infectat. Poden actuar aleatòriament o esperar una data concreta (per exemple, Divendres 13).
- Cucs. Van acaparant tots els recursos de l'ordinador: disc, memòria, xarxa. L'usuari nota que el sistema va cada vegada més lent, fins que no hi ha forma de treballar.
- Troyans. Solen habilitar portes posteriors en els equips: des d'un altre ordinador poden connectar amb el troyà per a executar programes en l'ordinador infectat. Realment no és tan important quin malware ens ha entrat: cal eliminar-lo perquè és una aplicació que no hem volgut instal·lar i que no ens portarà res bo (fins i tot pot mutar: un cuc convertir-se en troyà, etc.).

Tots tenen en comú el seu afany de replicació: intenten contaminar el màxim nombre d'ordinadors possible per a continuar la infecció. També cal anar amb compte amb els falsos antivirus. En algunes pàgines web perilloses (serveis de descàrregues il·legals, per exemple) apareix un missatge que ens avisa que estem infectats i s'ofereixen amablement per a descarregar un antivirus que ens netejarà l'ordinador. Si premem en l'enllaç i descarreguem i instal·lem aquest programa, probablement hem deixat entrar un malware que, des d'aquest instant, pot fer qualsevol cosa: llançar anuncis sense parar, instal·lar altres virus, obrir una porta posterior per a convertir-nos en ordinador zombi en algun atac organitzat, robar dades personals (imatges, vídeos), etc. En alguns casos, el virus dóna la cara i directament ens diu que ha segrestat el nostre ordinador. Efectivament: ja no podem fer res amb el teclat ni el ratolí. Per a recuperar la màquina cal introduir una contrasenya que solament ens la proporcionen després d'efectuar un pagament econòmic (és a dir, demanen un rescat).

Hi ha programes que ens asseguren que acceleraran el rendiment de l'ordinador, o el disc dur, o la connexió a Internet. Aquests programes existeixen, però hem de descarregar-los des de fonts de tota confiança, com les webs dels autors d'aquest programari o un lloc amb bona reputació (Softonic, CNET, etc.). Per a evitar que ocórrega, és millor tenir sempre activat l'antivirus (i tenir-ho actualitzat, clar). I, si per qualsevol raó, l'ordinador ja està segrestat, alguns antivirus tenen l'opció d'executar-se des d'un LiveCD. És a dir, descarreguem des de la web del fabricant de l'antivirus una imatge i fem un USB d'arrancada. Aquesta imatge porta un minisistema operatiu i el programa de l'antivirus.

Arranquem l'ordinador amb l'USB i podem fer una neteja a fons, amb la tranquil·litat que el virus no s'ha activat perquè no està funcionant el sistema operatiu del disc dur.

4. Tipus d'atacs

Una vegada que algú està decidit a atacar-nos, pot triar alguna d'aquestes formes:

- Interrupció. L'atac aconsegueix provocar un tall en la prestació d'un servei: el servidor web no està disponible, el disc en xarxa no apareix o solament podem llegir (no escriure), etc.

- Intercepció. L'atacant ha aconseguit accedir a les nostres comunicacions i ha copiat la informació que estàvem transmetent.

- Modificació. Ha aconseguit accedir, però, en lloc de copiar la informació, l'està modificant perquè arribe alterada fins a la destinació i provoque alguna reacció anormal. Per exemple, canvia les xifres d'una transacció bancària.

- Fabricació. L'atacant es fa passar per la destinació de la transmissió, per la qual cosa pot conèixer l'objecte de la nostra comunicació, enganyar-nos per a obtenir informació valuosa, etc.

Per a aconseguir el seu objectiu pot aplicar una o diverses d'aquestes tècniques:

- Enginyeria social. A l'hora de posar una contrasenya, els usuaris no solen utilitzar combinacions aleatòries de caràcters. En canvi, recorren a paraules conegudes per a ells: el mes del seu aniversari, el nom del seu carrer, la seua mascota, el seu futbolista favorit, etc. Si coneixem bé a aquesta persona, podem intentar endevinar la seua contrasenya.

També constitueix enginyeria social demanar per favor a un company de treball que introduïsca el seu usuari i contrasenya, ja que el nostre sembla que no funciona. En aquesta sessió podem aprofitar per a introduir un troyà, per exemple.

- Phishing. L'atacant es posa en contacte amb la víctima (generalment, un correu electrònic) fent-se passar per una empresa amb la qual tinga alguna relació (el seu banc, la seua empresa de telefonia, etc.). En el contingut del missatge intenta convèncer-lo perquè prema un enllaç que li portarà a una (falsa) web de l'empresa. En aquesta web li sol·licitaran la seua identificació habitual i des d'aquest moment l'atacant podrà utilitzar-la.

- Keyloggers. Un troyà en la nostra màquina pot prendre nota de totes les tecles que premem, cercant el moment en què introduïm un usuari i contrasenya.

- Força bruta. Les contrasenyes són un nombre limitat de caràcters (lletres, nombres i signes de puntuació). Una aplicació malware pot anar generant totes les combinacions possibles i provar-les una a una. Tard o d'hora, encertarà. Fins i tot pot estalviar temps si utilitza un diccionari de paraules comunes i aplica combinacions d'aquestes paraules amb nombres i signes de puntuació. Contra els atacs de força bruta hi ha diverses mesures:

* Utilitzar contrasenyes no trivials. No utilitzar res personal i inserir enmig de la paraula o al final un nombre o un signe de puntuació. En alguns sistemes ens avisen de la fortalesa de la contrasenya triada.

* Canviar la contrasenya amb freqüència (un mes, una setmana). Depenent del maquinari utilitzat, els atacs poden tardar bastant. Si abans hem canviat la clau, li ho posem difícil.

* Impedir ràfegues d'intents repetits. El nostre programari d'autenticació que sol.licita usuari i contrasenya fàcilment pot detectar diversos intents consecutius en molt poc de temps. No pot ser un humà: hem de respondre introduint una espera. Aquest retard allarga moltíssim el temps necessari per a completar l'atac de força bruta. Establir un màxim d'errades i després bloquejar l'accés. És el cas de les targetes SIM que porten els mòbils: al tercer intent fallit en introduir el PIN ja no en permet cap més. Com el PIN és un nombre de quatre xifres, la probabilitat d'encertar un nombre entre 10 000 en tres intents és molt baixa.

- Spoofing. Alterem algun element de la màquina per a fer-nos passar per una altra màquina. Per exemple, generem missatges amb la mateixa adreça que la màquina autèntica.

- Sniffing. L'atacant aconsegueix connectar-se en el mateix tram de xarxa que l'equip atacat. D'aquesta manera té accés directe a totes les seues converses.

- DOS (Denial of Service, denegació de servei). Consisteix a tombar un servidor saturant-lo amb falses peticions de connexió. És a dir, intenta simular l'efecte d'una càrrega de treball moltes vegades superior a la normal.

- DDoS (Distributed Denial of Service, denegació de servei distribuïda). És el mateix atac DOS, però ara no és una única màquina la que genera les peticions falses (que és fàcilment localitzable i permet actuar contra ella), sinó moltes màquines repartides per diferents punts del planeta. Açò és possible perquè totes aquestes màquines han sigut infectades per un troyà que les ha convertit en ordinadors zombis (obeeixen les ordres de l'atacant).

4.1. Tipus d'atacants

Se sol parlar de hàcker de manera genèrica per a referir-se a un individu que se salta les proteccions d'un sistema. A partir d'ací podem distingir entre:

- Hàcker. Ataca la defensa informàtica d'un sistema sol pel repte que suposa fer-ho. Si té èxit, moralment hauria d'avisar als administradors sobre els forats de seguretat que ha utilitzat, perquè estan disponibles per a qualsevol.

- Cràcker. També ataca la defensa, però aquesta vegada sí que vol fer mal: robar dades, desactivar serveis, alterar informació, etc.

- Script kiddie. Són aprenents de hacker i cracker que troben en Internet com fer un atac i el llancen sense conèixer molt bé què estan fent i, sobretot, les conseqüències derivades de la seua actuació (açò els fa especialment perillosos).

- Programadors de malware. Experts en programació de sistemes operatius i aplicacions capaços d'aprofitar les vulnerabilitats d'alguna versió concreta d'un programari conegut per a generar un programa que els permeta atacar.

- Sniffers. Experts en protocols de comunicacions que poden processar una captura de tràfic de xarxa per a localitzar la informació interessant.

- Ciberterrorista. Cracker amb interessos polítics i econòmics a gran escala.

5. Bones pràctiques

És molt dura la tasca del responsable de seguretat informàtica en una empresa gran: hi ha molta informació que protegir i múltiples portes per on patir intrusions. Les seues funcions són:

- Localitzar els actius que cal protegir: equips, aplicacions, dades i comunicacions. Sobretot, revisar la política de còpies de seguretat: què copiem, quan copiem, on ho copiem, on guardem de manera segura els dispositius de còpia, com verifiquem que la còpia s'ha fet bé, quan fem una prova de recuperació d'una còpia, etc.

- Redactar i revisar regularment els plans d'actuació davant catàstrofes, contemplant totes les possibilitats: atac intencionat, desastre natural, arrencada parcial de serveis (pocs serveis o tots els serveis però amb menor capacitat).

- No instal·lar res que no siga estrictament necessari, i revisar la configuració dels sistemes i aplicacions per si estem atorgant més permisos dels imprescindibles.

- Activar els mecanismes d'actualització automàtica de les aplicacions que tenim instal·lades. Excepte sistemes delicats (hem de provar molt bé cada actualització abans d'aplicar-la), en general els fabricants alliberen actualitzacions que no donen problemes.

- Donar formació als usuaris perquè utilitzen la seguretat i la vegen com una ajuda, no com una molèstia.

- Revisar els log del sistema (el accounting que hem vist abans). Algunes eines ens ajuden perquè arrepleguen els fitxers de log i apliquen fàcilment molts patrons coneguts (cercar la paraula error o warning, etc.).

- Considerar l'opció de contractar una auditoria externa, perquè si hem comès un error de concepte, és molt difícil que el trobem per nosaltres mateixos.

- Revisar la llista d'equips connectats: poden haver introduït equips no autoritzats.

- Revisar la llista d'usuaris actius: pot ser que algun empleat ja no estiga en la empresa però el seu usuari i tots els privilegis associats segueixen disponibles per a ell o per a algú de la seua confiança.

- Encara que els navegadors ens intenten facilitar la vida oferint recordar la contrasenya que introduïm en una pàgina web, no és recomanable fer-ho per que, si algú seu davant del nostre ordinador, entrarà directament en aquestes pàgines amb la nostra identitat i privilegis.

6. Legislació

Com en el món real, trencar la seguretat informàtica d'una empresa per a robar les seues dades és un delicte perseguit per la llei. També el desenvolupament d'Internet ha permés l'aparició de lleis completament noves, com la que regula el comerç electrònic.

6.1. Reglament General de Protección de Datos (RGPD)

El Reglament General de Protección de Datos (RGPD), conegut com a General Data Protection Regulation (GDPR) en anglès, és una regulació de la Unió Europea (UE) que va entrar en vigor el 25 de maig de 2018. El GDPR és una normativa de protecció de dades personals que estableix un conjunt de regles i requisits per a la recopilació, el tractament i la protecció de les dades personals de les persones residents a la UE. Aquesta regulació va ser dissenyada per garantir que les dades personals siguin tractades amb privacitat, transparència i seguretat adequades.

Ací hi ha alguns dels aspectes clau del GDPR:

1. **Àmbit d'aplicació**: El GDPR s'aplica a totes les empreses i organitzacions que processen dades personals de persones residents a la UE, independentment d'on es trobi la pròpia organització.
2. **Consentiment**: Les organitzacions han de sol·licitar un consentiment clar i explícit per recopilar i processar les dades personals de les persones. Aquest consentiment ha de ser lliure i informat.
3. **Drets de les persones afectades**: El GDPR confereix una sèrie de drets a les persones afectades, incloent-hi el dret a accedir a les seves dades, el dret a la portabilitat de dades, el dret a rectificar dades inexactes i el dret a ser oblidat (que implica l'eliminació de les seves dades en certes circumstàncies).
4. **Responsabilitat i transparència**: Les organitzacions han de ser transparents en relació amb com tracten les dades personals i han d'implementar mesures de seguretat adequades per protegir-les.
5. **Notificació d'incidents de seguretat**: Les organitzacions han de notificar a les autoritats de protecció de dades i a les persones afectades qualsevol violació de seguretat de les dades en un termini determinat.
6. **Delegat de protecció de dades (DPO)**: Algunes organitzacions han de designar un DPO, que és responsable de supervisar el compliment de les normatives de protecció de dades.
7. **Sancions i multes**: El GDPR preveu sancions econòmiques significatives per a les organitzacions que no compleixin amb les seves disposicions, podent arribar a multes de fins a 20 milions d'euros o el 4% del volum de negoci anual global de l'organització, la quantitat que sigui més elevada.

El GDPR va ser dissenyat per estandarditzar les regulacions de protecció de dades a tota la UE, oferint a les persones un major control sobre les seves dades i establint un marc més robust per a la privacitat de les dades en l'era digital. Les organitzacions que tracten dades personals de persones a la UE han de complir amb les disposicions del GDPR, i les autoritats de protecció de dades de cada país de la UE supervisen el seu compliment.

6.2. LPI

La Llei de Propietat Intel·lectual (LPI) és una llei espanyola que regula els drets relacionats amb la propietat intel·lectual, incloent-hi els drets d'autor, els drets d'interpretació i execució, els drets dels productors de fonogrames i altres aspectes vinculats a la creació i la difusió d'obres culturals i artístiques. Aquesta llei té com a objectiu protegir els drets dels creadors i incentivar la creació cultural i artística a Espanya.

La Llei de Propietat Intel·lectual proporciona un marc legal per a la protecció i la regulació dels drets de propietat intel·lectual en diverses àrees, incloent els drets d'autor, els drets d'interpretació i execució amb l'objectiu de protegir els interessos dels creadors i fomentar la creació cultural i artística.

6.3. Administració electrònica

L'Administració electrònica fa referència a l'esforç de tots els estaments públics per a adaptar els seus procediments a les noves tecnologies. Així eviten la manipulació de papers, i els ciutadans i empreses poden relacionar-se amb l'Administració de manera telemàtica.

Poder resoldre els tràmits per Internet té múltiples avantatges:

- Disponibilitat les 24 hores del dia. No cal demanar permís en el treball, fins i tot podem fer-ho en dies festius i caps de setmana.

- Facilitat d'accés. Els portals de l'Administració incorporen múltiples assistents que proporcionen tota l'ajuda necessària.

- Estalvi de temps. No cal desplaçar-se fins a una oficina i esperar torn per a ser atès.

- Fiabilitat. Els procediments ja no depenen de persones, sinó de sistemes.

El DNI electrònic i el certificat digital va suposar un punt d'inflexió perquè ara el ciutadà sí que disposa d'una autenticació fiable. Però encara està lluny de ser àmpliament utilitzat.

Tema 2: Criptografia

1. Per què cal encriptar?

L'encriptació de la informació és fonamental en seguretat informàtica per diverses raons importants:

- Confidencialitat: L'encriptació protegeix la confidencialitat de la informació en convertir-la en un format il·legible per a qualsevol que no tinga la clau de desencriptació adequada. Això assegura que només les persones autoritzades puguen accedir i comprendre la informació.

- Protecció contra l'accés no autoritzat: L'encriptació dificulta significativament l'accés no autoritzat a la informació. Encara que un atacant puga accedir a les dades, no podrà utilitzar-les sense la clau de desencriptació correcta.

- Integritat de les dades: L'encriptació també contribueix a garantir la integritat de les dades. Si algú intenta modificar la informació encriptada sense la clau adequada, el procés de desencriptació detectarà l'alteració i rebutjarà les dades.

- Seguretat en trànsit: L'encriptació s'utilitza àmpliament per protegir la informació mentre es transmet a través de xarxes, com ara l'encriptació SSL/TLS en transaccions en línia. Això evita que els atacants intercepten i accedisquen a les dades durant la transferència.

- Compliment normatiu: En molts sectors i països, hi ha regulacions i lleis que exigeixen l'encriptació de certs tipus de dades, especialment les que contenen informació sensible o personal. No complir aquestes regulacions pot resultar en sancions legals i multes.

- Protecció en cas de pèrdua o robatori de dispositius: Quan s'encripta la informació emmagatzemada en dispositius com ara ordinadors portàtils, telèfons mòbils o unitats USB, es protegeix contra l'accés no autoritzat en cas de pèrdua o robatori. Les dades estan segures i no es poden utilitzar sense la clau de desencriptació.

- Privacitat personal: L'encriptació també protegeix provacitat personal en el món digital. Evita que els proveïdors de serveis en línia, les empreses o fins i tot el govern accedisquen a les teues dades personals sense el teu consentiment.

- Protecció contra ransomware: L'encriptació pot ajudar a protegir contra el ransomware en dificultar que els atacants xifren els fitxers i exigisquen un rescat per desbloquejar-los.

Podem dir que l'encriptació és una pràctica essencial en seguretat informàtica perquè garanteix la confidencialitat, la integritat i la seguretat de la informació, tant en repòs com en trànsit. Ajuda a prevenir l'accés no autoritzat, protegeix contra la pèrdua de dades i és una part crítica de qualsevol estratègia de seguretat informàtica.

2. Criptografia

La criptografia és l'estudi i la pràctica de tècniques i mètodes que s'utilitzen per protegir la informació mitjançant la transformació de dades llegibles en un format il·legible, conegut com a "text xifrat," i després tornar-lo a convertir en la seua forma original, "text clar," mitjançant un procés anomenat "desxifrat."

La criptografia s'utilitza amb el propòsit principal de garantir la confidencialitat, la integritat i l'autenticitat de la informació en diverses aplicacions, com la seguretat de la comunicació, l'emmagatzematge de dades i la protecció de la privadesa.

Hi ha dos tipus principals de criptografia:

1. **Criptografia de xifrat simètric**: En aquest enfocament, s'utilitza una única clau per xifrar i desxifrar les dades. Tant l'emissor com el receptor han de conèixer i compartir aquesta clau prèviament. El xifrat simètric és eficient i ràpid, però presenta el desafiament de la gestió de claus, ja que les claus han de mantenir-se segures i compartir-se de manera segura.

2. **Criptografia de clau pública (asimètrica)**: Aquest enfocament utilitza un parell de claus matemàticament relacionades: una clau pública i una clau privada. La clau pública s'utilitza per xifrar les dades, mentre que la clau privada s'utilitza per desxifrar-les. La clau privada es manté en secret, mentre que la clau pública es pot compartir lliurement. La criptografia de clau pública és fonamental per a la seguretat de la comunicació a Internet i per a funcions com l'autenticació i la signatura digital.

La criptografia juga un paper crucial en la seguretat informàtica i s'aplica en una àmplia varietat de situacions, com ara:

- **Comunicacions segures**: Garanteix que les comunicacions en línia, com les transaccions bancàries i les comunicacions per correu electrònic, siguen onfidencials i segures.

- **Emmagatzematge segur de dades**: Permet el xifrat de les dades emmagatzemades en dispositius, com ara ordinadors i telèfons mòbils, per protegir la informació en cas de pèrdua o robatori.

- **Autenticació**: S'utilitza en processos d'autenticació per verificar la identitat d'un usuari o sistema.

- **Signatures digitals**: Permet la creació de signatures digitals per verificar l'autenticitat d'un document electrònic.

3. Criptografia simètrica

Com ja hem dit abans, la criptografia simètrica és una tècnica de criptografia en la qual es fa servir una única clau, anomenada "clau de xifrat," per tant per xifrar com per desxifrar la informació. Tant l'emissor com el receptor han de conèixer i compartir aquesta mateixa clau prèviament per poder comunicar-se de manera segura. En el procés de xifrat, la clau de xifrat pren les dades originals, anomenades "text clar," i les converteix en un format il·legible conegut com "text xifrat." Quan les dades xifrades arriben al receptor, aquest utilitza la mateixa clau de xifrat per desxifrar el text xifrat i tornar-lo a la seva forma original de text clar.

La criptografia simètrica és eficient i ràpida, però presenta el desafiament de la gestió de claus, ja que les claus han de ser compartides de manera segura entre les parts que desitgen comunicar-se de manera segura. Aquest tipus de criptografia es fa servir en molts contextos, com ara el xifrat de dades emmagatzemades en dispositius o el xifrat de comunicacions punt a punt en sistemes que requereixen un alt rendiment i una latència baixa.

4. Criptografia asimètrica

La criptografia asimètrica, també coneguda com a criptografia de clau pública, és un mètode de seguretat informàtica que utilitza dues claus diferents, una clau pública i una clau privada, per a xifrar i desxifrar la informació.

Clau pública: Aquesta clau és coneguda per tots i es fa servir per xifrar la informació abans d'enviar-la. És com tancar la informació en una capsa forta amb una clau que tots poden veure, però només la clau privada pot obrir la capsa i accedir a la informació.

Clau privada: Aquesta clau és totalment secreta i només la coneix el propietari. Es fa servir per desxifrar la informació xifrada amb la clau pública. És com tenir la clau exclusiva per obrir la capsa forta i llegir el contingut.

Aquest sistema permet a les persones i les empreses comunicar-se de manera segura a través d'Internet i protegir les seves dades.

Per exemple, quan fas una compra en línia o accedeixes al teu compte bancari, el teu navegador utilitza la clau pública del lloc web per xifrar les teves dades. Només el lloc web, que té la clau privada corresponent, pot desxifrar i llegir les dades. Això assegura que les teves dades siguen confidencials i no puguen ser llegides per tercers mentre viatgen per Internet.

També s'utilitza per verificar la identitat en línia i protegir la privadesa digital.

5. Signatura digital i certificat digital

La signatura digital i el certificat digital són dos conceptes importants en el camp de la seguretat informàtica que es fan servir per garantir la autenticitat i la integritat de la informació en entorns digitals.

Signatura digital: Una signatura digital és una representació electrònica d'una signatura manuscrita que es fa servir per autenticar un document o un missatge electrònic. Es crea utilitzant una clau privada i s'afegeix al document o al missatge. Quan algú rep un document amb una signatura digital, pot utilitzar la clau pública del signant per verificar la signatura i assegurar-se que el document no ha estat alterat i que prové del signant autèntic. Les signatures digitals són molt segures i es fan servir en transaccions en línia, contractes electrònics, i altres situacions on es requereix una prova de la autenticitat i la integritat dels documents electrònics.

Certificat digital: Un certificat digital és una eina que ajuda a garantir la autenticitat d'una persona o d'una entitat en línia. Conté la informació de la persona o l'entitat, així com la seua clau pública. El certificat és emès per una autoritat de certificació de confiança (CA) i es fa servir per verificar la identitat i la clau pública d'una persona o d'una entitat. Quan algú vol enviar-te un missatge amb una signatura digital, pot utilitzar el certificat digital per verificar que realment eres tu qui has signat el missatge. El certificat digital també es fa servir en connexions segures a Internet (com ara HTTPS) per garantir que estàs connectant-te al lloc web autèntic i no a una pàgina web fraudulenta.

Podem dir que la signatura digital és una manera d'autenticar i protegir la integritat de documents i missatges electrònics, mentre que el certificat digital és una eina que ajuda a verificar la identitat en línia i a protegir la connexió segura a Internet. Ambdós són essencials per garantir la seguretat i la confiança en les comunicacions i les transaccions en línia

6. PKI

PKI (Infraestructura de Clau Pública, per les seues sigles en anglès) és un sistema que s'utilitza per gestionar claus públiques i privades i certificats digitals en entorns de seguretat informàtica. Aquesta infraestructura és essencial per a la seguretat i la gestió de les comunicacions i les transaccions en línia.

La PKI utilitza certificats digitals emesos per una autoritat de certificació (CA) de confiança per garantir la identitat de les parts i la seguretat de les comunicacions en línia. Les parts principals d'una PKI inclouen:

1. **Certificats digitals**: Aquests són documents electrònics que contenen la informació d'una persona o d'una entitat, juntament amb la seua clau pública. El certificat digital és emès per una CA de confiança i serveix per verificar l'identitat del titular i la validesa de la seva clau pública.

2. **Autoritats de certificació (CA)**: Les CA són organitzacions de confiança que emeten, gestionen i revoquen certificats digitals. Les CA verifiquen l'identitat dels titulars de certificats, i quan emeten un certificat, també signen el certificat amb la seua pròpia clau privada per acreditar la validesa del certificat.

3. **Entitats de registre**: Les entitats de registre són les responsables de recopilar la informació dels titulars dels certificats i enviar-la a la CA perquè puga emetre els certificats. Aquestes entitats asseguren que la informació continguda en els certificats siga precisa i que els titulars són qui diuen ser.

4. **Entitats de validació**: Aquestes entitats verifiquen i validen certificats digitals, confirmant que són vàlids i no han estat revocats.

La PKI s'utilitza en molts contextos, com ara connexions segures a Internet (HTTPS), signatures digitals, xifrat de dades i autenticació d'usuaris. La PKI és una infraestructura essencial per garantir la seguretat i la confiança en les comunicacions i les transaccions en línia mitjançant l'ús de certificats digitals i autoritats de certificació de confiança.

Tema 3: Seguretat passiva: equips

1. Ubicació del CPD

Les empreses col·loquen els equips d'usuari prop de l'usuari (un ordinador sobre la seua taula, un portàtil que es porta a casa), però els servidors estan tots junts en una mateixa sala. Aquesta sala té diversos noms: CPD (centre de processament de dades), centre de càlcul, DataCenter, sala freda, «peixera», etc. Centralitzant s'aconsegueix:

- Estalviar en costos de protecció i manteniment. No necessiten duplicar la vigilància, la refrigeració, etc.

- Optimitzar les comunicacions entre servidors. Com estan prop uns dels altres no calen cables llargs ni altres elements intermedis que redueixen el rendiment.

- Aprofitar millor els recursos humans del departament d'informàtica. No han de desplaçar-se a diferents edificis per a realitzar instal·lacions, substituir targetes, etc.

Tan important com prendre mesures per a protegir els equips és tenir en compte què fer quan aquestes mesures fallen. Totes les empreses han de tenir documentat un pla de recuperació davant desastres, on es descriga amb el màxim detall (en una crisi no hi ha temps per a reflexionar) què fer davant una caiguda de qualsevol dels serveis que presta el CPD. Aquest pla ha de ser actualitzat quan s'efectue un canvi en el CPD (nou servei, nou equip). El pla ha d'incloure:

- Maquinari. Quins models de màquines tenim instal·lats (tant servidors com equipament de xarxa), quins models alternatius podem utilitzar i com s'instal·laran (connexions, configuració).

- Programari. Quin sistema operatiu i aplicacions estan instal·lats, amb el nombre de versió actualitzat i totes les opcions de configuració (permisos, usuaris, etc.).

- Dades. Quins sistemes d'emmagatzematge utilitzem (discos locals, prestatgeria de discos), amb quina configuració i com es fa el respatller de dades (còpies de seguretat).

1.1. Protecció

La informàtica és vital per a l'empresa: si els servidors es paren, l'empresa es para. Succeeix en tots els sectors: en una empresa de telefonia, en una companyia aèria, en uns grans magatzems...

El CPD ha d'estar protegit al màxim:

- Triarem un edifici en una zona amb baixa probabilitat d'accidents naturals (terratrèmols, ciclons, inundacions).

- També evitarem la proximitat de rius, platges, preses, aeroports, autopistes, bases militars, centrals nuclears, etc.

- Evitarem ubicacions on els edificis veïns al nostre siguen empreses dedicades a activitats potencialment perilloses: gasos inflamables, explosius, etc.

- Preferentment seleccionarem les primeres plantes de l'edifici. La planta baixa està exposada a sabotatges des de l'exterior (impacte de vehicles, assalts, etc.). Les plantes

subterrànies serien les primeres afectades per una inundació. Les plantes superiors estan exposades a un accident aeri i, en cas d'incendi iniciat en plantes inferiors, és segur que ens afectarà.

- Es recomana que l'edifici tinga dos accessos i per carrers diferents. Així sempre podrem entrar en cas que una entrada quede inaccessible (obres, incident, etc.).

- És recomanable evitar senyalitzar la ubicació del CPD per a dificultar la seua localització a possibles atacants. La llista d'empleats que entren a aquesta sala és molt reduïda i saben perfectament on està.

-Els passadissos que porten fins al CPD han de ser amples perquè alguns equips són bastant voluminosos. Fins i tot convé dotar-lo d'un moll de descàrrega.

- L'accés a la sala ha d'estar molt controlat. Els servidors solament interessen al personal del CPD.

- En les parets de la sala s'haurà d'utilitzar pintura plàstica perquè facilita la seua neteja i s'evita la generació de pols.

- En la sala s'utilitzarà fals sòl i fals sostre perquè facilita la distribució del cablejat (per a electricitat i comunicacions) i la ventilació.

- L'altura de la sala serà elevada tant per a permetre el desplegament de fals sòl i fals sostre com per a acumular molts equips en vertical, perquè l'espai d'aquesta sala és molt valuós.

- En empreses d'alta seguretat, la sala del CPD es recobreix amb un cofre de formigó per a protegir-la d'intrusions des de l'exterior.

- Instal·larem equips de detecció de fums i sistemes automàtics d'extinció d'incendis.

- El mobiliari de la sala ha d'utilitzar materials ignífugs.

1.2. Aïllament

Les màquines que situem en el CPD utilitzen circuits electrònics. Per tant, cal protegir-les davant:

- Temperatura. Els circuits dels equips, especialment els processadors, treballen a alta velocitat, per la qual cosa generen molta calor. Si, a més, li sumem la temperatura de l'aire els equips poden tenir problemes.

- Humitat. No solament l'aigua, també un alt percentatge d'humitat en l'ambient pot danyar-nos. Per a evitar-ho utilitzarem deshumidificadors.

- Interferències electromagnètiques. El CPD ha d'estar allunyat d'equips que generen aquestes interferències, com a material industrial o generadors d'electricitat, siguen nostres o d'alguna empresa veïna.

- Soroll. Els ventiladors de les màquines del CPD generen molt soroll (són moltes màquines treballant a alt rendiment), tant que convé introduir aïllament acústic per a no afectar als treballadors de les sales adjacents.

1.3. Ventilació

Els CPD no solen tenir finestres. La ventilació que aconseguiríem amb elles seria mínima per a tota la calor que es genera, i el risc d'intrusions des de l'exterior (o simplement la pluja) no és admissible en una instal·lació de tanta importància.

La temperatura recomanable en la sala estaria al voltant dels 22 graus. Les màquines no ho necessiten, però cal pensar que ací també van a treballar persones. Per a aconseguir-ho instal·larem equips de climatització. Se solen instal·lar per duplicat, per a estar coberts davant l'avaria d'un dels equips.

En els CPD grans s'adopta la configuració de passadissos calents i passadissos freds. Les files d'equips es col·loquen en blocs formant passadissos, de manera que tots els ventiladors que extrauen la calor de la màquina (font d'alimentació, caixa de la CPU) apunten cap al mateix passadís. En aquest passadís es col·loquen els extractors de calor de l'equip de climatització.

1.4. Subministrament elèctric i comunicacions

El nostre CPD no està aïllat: necessita certs serveis de l'exterior. Els principals són l'alimentació elèctrica i les comunicacions. En tots dos casos convé contractar amb dues empreses diferents, de manera que si una companyia subministradora falla podem seguir treballant.

El subministrament elèctric del CPD hauria d'estar separat del que alimenta a la resta de l'empresa per a evitar que un problema en qualsevol despatx de l'edifici afecte als servidors, perquè estan sent utilitzats per empleats d'altres edificis, fins i tot per clients i proveïdors. Per als sistemes crítics, en els quals l'empresa no pot permetre's cap interrupció del servei, haurem d'instal·lar generadors elèctrics alimentats per combustible.

Quant a les comunicacions, convé que el segon subministrador utilitze una tecnología diferent al primer. Per exemple, si tenim una connexió ADSL, el segon no hauria de ser ADSL també, perquè comparteixen el mateix cable fins a arribar a la central: una fallada en aques cable ens desconnectaria dels dos subministradors. En qualsevol cas, sempre convé tenir una tercera opció de connexió sense fil, per si el problema ocorre en el carrer (obres en la vorera, etc.).

1.5. Control d'accés

Les màquines del CPD són vitals per a l'empresa i solament necessiten ser utilitzades per un reduït grup d'especialistes. L'accés a aquesta sala de màquines ha d'estar especialment controlat. No podem consentir que algú s'emporte cap màquina o algun component d'ella (discos durs, cintes de backup), ni deixar-lo romandre dins intentant tenir accés des de les consoles dels servidors. Les identificacions habituals (contrasenyes, targetes d'accés) es complementen amb mesures més segures, com la biometria, que veurem en la una altra unitat. En instal·lacions importants, el CPD pot tenir el seu propi equip de vigilants de

seguretat. En la sala se sol instal·lar també una xarxa de sensors de presència i càmeres de vídeo per a detectar visites inesperades.

Nota: molt interessants aquests 2 videos:

- Google Data Center 360° Tour (https://youtu.be/zDAYZU4A3w0?si=jnUCOq84paoieRl4)

- Un SUPERORDENADOR con 165.888 NÚCLEOS
(https://youtu.be/nctTZplQY-o?si=pXFFM48aE9RX9tu5)

2. Centre de suport en seguretat informàtica

Un "centre de suport en seguretat informàtica" es refereix generalment a una instal·lació o infraestructura secundària dissenyada per recolzar i garantir la continuïtat de les operacions de seguretat informàtica d'una organització en cas que passe un esdeveniment advers, com un ciberatac, un desastre natural o una fallada al sistema.

Aquests centres de suport solen formar part de l'estratègia de recuperació davant de desastres d'una organització i tenen com a objectiu mantenir la disponibilitat i la integritat dels sistemes d'informació crítics i les dades confidencials.

Ací hi ha alguns aspectes clau d'un centre de seguretat en informàtica:

- Respatller de dades i sistemes: El centre de seguretat està equipat amb còpies de seguretat de les dades essencials i rèpliques de sistemes crítics per garantir que, en cas d'un incident, l'organització puga continuar operant amb una interrupció mínima.

- Ubicació geogràfica alternativa: sovint aquests centres es troben en ubicacions geogràfiques diferents o allunyades de la ubicació principal de l'organització per reduir el risc que un desastre afecte tant la ubicació principal com la de suport.

- Infraestructura redundant: Els centres de seguretat solen comptar amb servidors, sistemes d'emmagatzematge i xarxes redundants per garantir la disponibilitat contínua dels serveis essencials.

- Recuperació davant de desastres: En cas d'un incident, el centre de suport està dissenyat per facilitar la ràpida recuperació dels sistemes i dades crítiques.

- Proves regulars: És fonamental realitzar proves regulars dels procediments de recuperació davant de desastres per garantir que el centre de respatller estiga preparat i funcione correctament en cas de necessitat.

La implementació d'un centre de seguretat en seguretat informàtica és una part important de l'estratègia de seguretat cibernètica i ajuda a garantir que una organització puga mantenir la continuïtat de les operacions fins i tot en situacions adverses.

3. SAI

El corrent elèctric és vital en qualsevol ordinador. Com no podem confiar que mai va a fallar l'empresa amb la qual hem contractat el subministrament elèctric, hem de pensar en alternatives. En aquesta mateixa unitat hem suggerit contractar un segon subministrador o disposar d'un generador propi (grup electrògen). Sense abandonar aquestes solucions, en un CPD mai ha de faltar un SAI (sistema d'alimentació ininterrompuda), en anglès UPS (Uninterruptible Power Supply).

Un SAI és un conjunt de bateries que alimenten una instal·lació elèctrica (en el nostre cas, equips informàtics).

En cas de tall del corrent, els equips connectats al SAI segueixen funcionant perquè aconsegueix electricitat de les bateries. La capacitat d'aquestes bateries és reduïda depèn del SAI triat i del consum dels equips, encara que el mínim garantit sol ser deu minuts. Aquest és el factor més important a l'hora d'adquirir un SAI: quants watts consumeixen els equips que ha de protegir i quant temps necessitem que els protegisca.

Igual que ocorria amb els equips de climatització, si el pressupost ho permet, convé aplicar redundància i instal·lar un doble joc d'equips SAI, per a estar coberts en cas que un d'ells fallara. Açò és possible perquè la majoria dels servidors vénen amb doble font d'alimentació i connectaríem una font a cada grup de SAI.

Quan ocorre un tall de llum, el SAI procedeix d'aquesta manera:

Espera uns minuts per si el tall ha sigut puntual i el subministrament es recupera immediatament per si mateix. Si no és així, executa una parada ordenada dels equips connectats al SAI. Sempre és millor sol·licitar una parada al sistema operatiu i les aplicacions que executa que perdre el corrent i confiar que no es genere cap inconsistència.

Connectar els equips al SAI té altres avantatges:

- Solen portar un estabilitzador de corrent que protegix de les pujades de tensió, que també poden ser molt nocives.

- També solen poder-se configurar per a enviar e-mails en cas que no funcionen bé o tall de subministrament elèctric.

3.1. Tipus

Tradicionalment, s'han considerat dos tipus d'equips SAI:

- SAI en estat d'espera (stand-by). Els equips informàtics prenen corrent del subministrament principal, mentre el SAI es limita a vigilar que aquest subministrament fluïsca. Quan ocorre un tall, el SAI activa immediatament les seues bateries perquè els equips no es vegen afectats (el temps de resposta sol ser suficient). A partir d'aquest moment, el SAI aplica els temps d'espera assenyalats en el punt anterior. Quan torna el corrent, desactiva la generació de corrent propi i comença a carregar les bateries.

- SAI en línia (on-line). Els equips sempre estan prenent corrent de les bateries del SAI. Quan ocorre un tall, el SAI es limita a aplicar els temps d'espera. Quan torna el corrent, comença a carregar les bateries.

L'avantatge del SAI en línia és que no depenem del temps de resposta per a activar les bateries; en canvi, l'avantatge del SAI en espera és que podem substituir les bateries sense detenir el subministrament als equips connectats.

3.2. Monitoratge

Quan tenim un SAI confiem que està bé i que respondrà quan siga necessària la seua intervenció. Però convé revisar regularment l'estat del SAI. Aquests equips solen incorporar uns indicadors lluminosos en el frontal si està carregant o descarregant les bateries, percentatge de bateria restant, etc.

No obstant açò, és una informació puntual i solament disponible si s'està davant de l'equip. Per a millorar la seua gestió, els SAI solen incorporar un port de connexió amb un ordenador. Per a testar de manera interactiva el bon funcionament.

4. Node Tirant

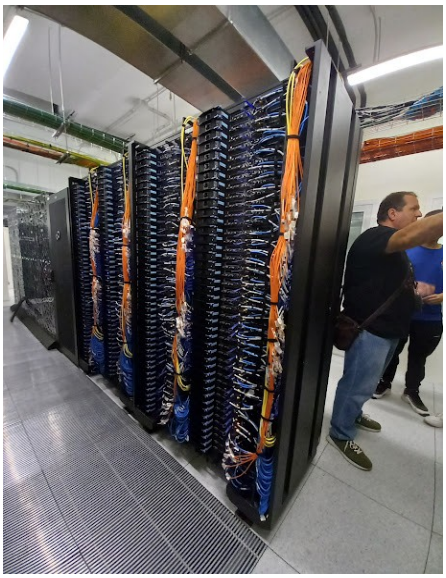
La Universitat de València (UV) acull el supercomputador Tirant, una gran oportunitat de veure de prop les mesures de seguretat que s'implementen en aquesta infraestructura a través de les seues visites guiades.

Forma part de la RES (xarxa espanyola de supercomputació) i està instal·lat al campus de Burjassot i és gestionat pel Servei d'Informàtica (SIUV). El SIUV s'encarrega de gestionar tant la infraestructura esmentada com el propi sistema (a nivell de maquinari i programari). El personal ofereix, a més, el servei de suport a l'usuari.

El supercomputador Tirant va ser inaugurat l'any de 2008. En la seva configuració actual, després de l'última actualització (juliol 2018), Tirant queda format per 336 nodes cadascun d'ells amb dos processadors Intel Xeon SandyBridge E5-2670 a 2,6 Ghz i 32 GB

de RAM DDR3 (5376 nuclis). Aquesta configuració proporciona a Tirant un rendiment màxim tècnic de 111,8 Tflops.

Ací teniu una foto del Tirant 3 poc abans de ser desmuntat. A hores d'ara ja està funcionant la versió 4 del superordinador Tirant.



Tema 4: Seguretat passiva: emmagatzenament

1. Estratègies d'emmagatzematge

Per a una empresa, la part més important de la informàtica són les dades: les seues dades. Perquè:

- El maquinari és car, però es pot tornar a comprar.

- Un informàtic pot acomiadar-se, però és possible contractar-ne un altre.

- Si una màquina no arranca perquè s'ha corromput el sistema de fitxers, pots instal·lar de nou el sistema operatiu i les aplicacions.

En tots els casos anteriors es recupera la normalitat en un termini de temps raonable. No obstant açò, les dades d'aquesta empresa són únics: no es poden comprar, no es poden contractar, no hi ha originals. Si es perden, no els podem recuperar.

Bé, ja que les dades són tan importants, cal esforçar-se en millorar la seua integritat i disponibilitat:

- Podem comprar els millors discos del mercat en qualitat i velocitat, però mai hem d'oblidar que són màquines i poden fallar. En un lloc d'usuari ens ho podem permetre (e canviem i ja està) però en un servidor hem vist que no.

- Podemos concentrar els discos en uns servidors especialitzats en emmagatzematge.

- Podemos replicar la informació diverses vegades i repartir-la per ciutats diferents.

- Podemos contractar el servei de respatller de dades a una altra empresa, connectats per Internet, per a no dependre dels nostres equips i personal.

A continuació estudiarem cadascuna d'aquestes alternatives. Cada empresa triarà implementar una o vàries, segons les seues necessitats i possibilitats.

1.1. Rendiment i redundància. RAID

Els ordinadors poden connectar diversos discos interns perquè les plaques base solen portar integrada una controladora de discos per a dues o tres connexions. I si punxem més controladores, podrem connectar més dispositius. Però per a què volem diversos discos en un ordinador? Per la mateixa raó per la qual comprem CPU de diversos nuclis o plaques base amb diverses CPU. Podemos aprofitar diversos discos d'un ordinador per a:

- Crear unitats més grans. Dos discos de 500 GB junts ens poden donar una unitat d'1 TB. Amb tres discos tenim 1,5 TB, etc. Si volem 2 TB i solament tenim discos de 640 GB, podem ajuntar tres. Crear unitats més ràpides. Si tenim dos discos de 500 GB i configurem el sistema perquè, en cada fitxer, els blocs parells s'escriguen en un disc i els senars en un altre, després podrem fer lectures i escriptures en paral·lel.

- Crear unitats més fiables. Si configurem els dos discos anteriors perquè, en cada fitxer, els blocs s'escriguen alhora en tots dos discos, podem estar tranquils perquè, si falla un disc, les dades estaran fora de perill en l'altre. Doncs una de les tecnologies que ho aconsegueix es diu RAID.

Hi ha diversos nivells de RAID. Els més importants són:

- RAID 0. Agrupem discos per a tenir un disc més gran, fins i tot més ràpid. Des d'aquest moment, els blocs que arriben al disc RAID 0 s'escriuran en algun dels discos del grup. Per descomptat, per a l'usuari aquest procés és transparent: ell solament veu un disc d'1 TB on abans hi havia dos discos de 500 GB. En el RAID 0 podem triar entre spanning i striping (que és el més comú). En qualsevol cas, si falla un dels discos, ho perdem tot.

- RAID 1. Se'l sol anomenar mirror o espill. Agrupem discos per parelles, de manera que cada bloc que arribe al disc RAID 1 s'escriurà en els dos discos alhora. Si falla un dels discos, no perdem la informació, perquè estarà en l'altre. A canvi, sacrifiquem la meitat de la capacitat (l'usuari ha connectat dos discos de 500 GB i solament té disponibles 500 GB, en lloc d'1 TB) i no guanyem rendiment.

- RAID 5. (Redundant Array of Independent Disks 5) és una configuració d'emmagatzematge que utilitza almenys tres discs durs per proporcionar redundància i rendiment. Funciona distribuint dades i paritat (informació de comprovació d'errors) a través dels discos. Si un dels discs falla, les dades es poden reconstruir utilitzant la informació de paritat dels altres discs. Això proporciona tolerància a fallades i millora la velocitat de lectura, però l'escriptura pot ser més lenta a causa dels càlculs de paritat.

1.2. Emmagatzematge en xarxa: NAS i SAN. Clústers

Hem vist que podem millorar el rendiment i la fiabilitat de l'emmagatzematge d'un ordinador connectant diversos discos i configurant-los en RAID. Però en les empreses se sol treballar amb equip, compartint fitxers entre diversos ordinadors. Hem de pensar com compartir fitxers i com fer-ho amb seguretat (qui pot llegir aquests fitxers i qui pot modificar-los, esborrar-los o incloure'n de nous).

La millor alternativa és posar-ho en un servidor dedicat i, si pot ser, especialitzat en emmagatzematge. D'aquesta manera:

- Podem instal·lar el programari estrictament necessari i tenir-ho actualitzat (menor risc d'infeccions).

- Estarà sota la supervisió del personal del CPD (centre de procesament de dades), la qual cosa garanteix estar encès tot el temps, formar part de la política de còpies de seguretat de l'empresa, detectar quan el disc està pròxim a omplir-se, etc.

- Si, a més, és un servidor especialitzat en emmagatzematge, disposarà de maquinari suficient per a desplegar configuracions RAID, una memòria caché d'alt rendiment, etc.

Si un equip de la xarxa ofereix discos a altres equips connectats a ella. És el que es coneix com NAS (Network Attached Storage, emmagatzematge connectat a la xarxa). En aquest esquema tenim un equip amb emmagatzemament local. Aquest equip servidor executarà un determinat programari servidor que respon a un determinat protocol. Aquell equip que necessite accedir a aquesta carpeta compartida, executarà un programari client capaç d'interactuar amb el servidor d'acord amb el protocol del servidor. Com la majoria dels equips d'usuari són Windows, el protocol més comú és CIFS (Common Internet File System), que és una evolució de SMB (Server Message Block).

En un entorn privat pot ser suficient amb un xicotet equip que faça de servidor NAS; però en un entorn empresarial necessitem molt més rendiment i seguretat, per la qual cosa l'equip servidor necessitarà potència de processament, àmplia memòria caché, targetes de xarxa d'alta capacitat i configuracions RAID. Si altres servidors també ho necessiten, segurament optarem per una solució SANT (Storage Area Network). En un SAN els discos estan en el que es diu una «prestageria», on es realitza la configuració RAID. La prestageria disposa de cachés d'alt rendiment per a reduir els temps d'operació. Els servidors es connecten a la prestageria a traves de commutadors de fibra òptica (per açò parlem de network). La configuració dels les prestageries és flexible: per a cada equip es poden assignar uns discos concrets i reservar-li certa quantitat de caché. I canviar-ho quan siga necessari.

L'emmagatzematge compartit és especialment important en els clústers. Un clúster és un conjunt de màquines (anomenades nodes) coordinades per a realitzar una tasca en comú. Pot ser una base de dades, un servidor web, un sistema de gestió de xarxes, cerca de vida extraterrestre (SETI), emmagatzematge compartit en Internet etc. Cada màquina executa una part de la funcionalitat i està coordinada amb la resta de les màquines. Per a açò necessiten un determinat programari de clúster instal·lat en totes elles i, sobretot, un emmagatzematge fiable i d'alt rendiment, perquè els nodes intercanvien molta informació.

1.3. Emmagatzematge en el núvol

Suposem que la nostra empresa ja té en les seues instal·lacions NAS (disc en xarxa) i SANT (discos d'alt rendiment, capacitat i seguretat). Però hi ha més necessitats:

- Volem penjar fitxers per als nostres clients i proveïdors.
- Quan estem fora de l'oficina podem necessitar algun fitxer (un pressupost, un contracte).
- Anem a continuar a casa un treball que tenim a mig fer.
- Simplement volem una còpia d'uns documents importants en un altre lloc que no siga l'oficina.

Per a un empleat, una solució simple és guardar-ho tot en un pendrive USB. Però es perden amb massa facilitat (i la informació que va pot ser molt important: convé haver-la xifrat) i a més no podríem treballar simultàniament amb altres companys (encara que cadascun porte el seu pendrive, els següents canvis no estarien sincronitzats). La solució habitual era obrir un accés directe des d'Internet fins als discos de l'empresa. Funciona, encara que és delicat, perquè al final és una «porta posterior» per on poden intentar entrar hackers, i arribar fins a aquests discos o qualsevol altre servidor nostre.

Com a alternativa, en els últims anys han aparegut multitud de serveis d'emmagatzemament en el núvol:

La primera generació (Megaupload, FileServe, etc.) consisteix que un usuari puja un fitxer a una web perquè ho descarreguen altres usuaris connectats a aqueixa web. Però resulta incòmode, primer perquè solament emmagatzema fitxers, sense una estructura de carpetes, i, segon, perquè si volem tots els fitxers d'una carpeta, cal anar d'un en un, o comprimir-los en un zip i pujar-ho.

La segona generació (Dropbox, OneDrive, Skydrive, GoogleDrive) és més simple: directament sincronitzen carpetes dels dispositius (ordinador personal, mòbil, tableta)

entre si i amb els servidors del proveïdor. Qualsevol canvi que faces en qualsevol dispositiu automàticament ocorre en els altres dispositius i en el disc del proveïdor.

Tots aquests serveis tenen avantatges i inconvenients:

- Les nostres dades estan fora de les nostres instal·lacions, per la qual cosa podem accedir a ells a qualsevol hora, sense estar allí, i amb la tranquil·litat que qualsevol desastre que ocórrega en l'oficina no els afectarà.

- L'empresa proveïdora del servei d'emmagatzematge en el núvol es preocupa per fer còpies de seguretat de les dades que pugem. Fins i tot solen conservar versions anteriors de cada fitxer que modifiquem.

- La connectivitat a Internet d'aquestes empreses sol ser molt superior a la nostra, per la qual cosa l'accés és ràpid. I al mateix temps no ocupem ample de banda de la nostra connexió.

No obstant açò, perdem el control sobre l'accés a la nostra informació. Hem de confiar en la capacitat tècnica i humana del proveïdor d'emmagatzematge en el núvol per a evitar atacs sobre els seus servidors (de nou, convé xifrar els arxius que pugem al núvol). I confiar també en què no incorre en pràctiques delictives, com el cas Megaupload, que tanca el servei a tots els clients, innocents o no.

2 Backsups de dades

Ni el RAID 1 ni el RAID 5 ens permeten dormir tranquils. Estem protegits davant la errada d'un dels discos, però no si fallen dos. O si s'incendia la sala i crema el servidor. O si algú accedeix a la màquina i la formata. Podem veure el RAID com una forma de seguir funcionant, encara que haja mort un dels discos. Però les nostres dades són més importants i cal seguir protegint-les. Per açò farem còpies i les portarem el més lluny possible.

1) Primer anem a distingir entre:

– Backup de dades. Còpia de seguretat de les dades de l'usuari o empresa que estan emmagatzemats en un ordinador.
– Imatge del sistema. Còpia de seguretat dels programes (sistema operatiu i aplicacions) que estan instal·lats en un ordinador.

Normalment es fa una imatge del sistema just després d'instal·lar-ho i configurar-lo, o després de la instal·lació d'una aplicació important. En canvi, el backup de dades cal fer-lo diàriament, fins i tot amb més freqüència, depenent de l'activitat de l'empresa.

2) El segon pas és identificar les dades que hem de salvar. Ací hem de distingir entre:

– Fitxers. Poden ser unitats senceres, la típica carpeta Els meus Documents, etc. Existeix la complicació de detectar els fitxers que estan sent modificats precisament quan s'ha llançat la còpia.
– Sistemes complexos, com les bases de dades, on la concurrència de canvis sol ser molt més alta que amb fitxers, perquè una operació afecta a diverses taules. Per aquest motiu, els servidors de base de dades tenen els seus propis mecanismes d'exportació del contingut de les taules.

3) Finalment, per a cada tipus d'informació identificada en el pas anterior, cal acordar la freqüència de respatler. En un supermercat, per a la base de dades d'empleats pot ser suficient efectuar una còpia diària o setmanal, però la base de dades de vendes no pot esperar tant.

2.1. Tipus de dispositius locals i remots. Robot de cintes

Una vegada hem confirmat quina informació del disc dur volem conservar i amb quina freqüència, cal decidir on fem la còpia: suport físic i ubicació d'aquest suport físic. Quant al suport físic, podem pensar en:

- Usar una altra partició del mateix disc dur. No és bona idea, perquè si falla el disc, ho perdem tot.

- Usar un altre disc d'aquesta màquina, però si es destrueix la màquina, ho perdem tot.

- Passar-ho a un disc dur extraïble per a emportar-nos-ho, o potser el disc dur d'una altra máquina al que accedim per FTP. Seria acceptable, però els discos durs són relativament cars.

- Si podem triar entre cintes i discos, millor les cintes perquè tenen més capacitat i són més fiables i reutilitzables.

En qualsevol cas, i sobretot si anem a utilitzar suports extraïbles, que es poden extraviar, hem de preocupar-nos per xifrar el contingut. Açò ja ho fan la majoria dels programes de backup.

La facilitat d'extraure un suport i posar un altre és vital. Primer perquè evitem estar sempre utilitzant el mateix element, la qual cosa accelera la seua deterioració, i sobretot perquè les còpies de seguretat, si podem, cal conservar-les el més allunyades possible del disc copiat, per a evitar que un desastre en la sala d'ordinadors també acabe amb les còpies. Per açò:

- Si la nostra empresa té dues seus, convé que les cintes d'una seu s'intercanvien amb les cintes de l'altra per missatgeria.

- Si solament hi ha un edifici, en la part oposada al CPD.

- Han d'estar sempre en una sala amb control d'accés, per a evitar que qualsevol arribe fins a les nostres dades.

- Dins de la sala, cal ficar-les en una aprestageria ignífuga.

Una vegada triat el suport, cal decidir on posar-ho. Podríem comprar un per a cada servidor com a dispositiu local, però resulta car i laboriós, atès que anem a utilitzar diverses cintes (per exemple, una per a cada dia de la setmana) i algú hauria d'anar màquina per màquina canviant les cintes, i etiquetant perfectament de quina màquina són i a quin dia corresponen.

Interessa centralitzar aquestes tasques repetitives i que les facen màquines, no persones.

En les empreses se sol instal·lar una llibreria de cintes (robot de cintes), on es fa el backup de tots els servidors de l'empresa i també aquells llocs de treball que ho necessiten. Cada cinta està etiquetada i el robot manté una base de dades on registra quina cinta va utilitzar a cada moment

Aquest dispositiu remot està connectat a la LAN de l'empresa o directament als servidors mitjançant SAN. Executa un programari servidor que connecta amb un programari client instal·lat en cada equip seleccionat. Normalment, la xarxa que utilitza és una LAN o VLAN diferent a la LAN de treball (els ordinadors amb funció de servidor solen portar dues interfícies de xarxa). En utilitzar una LAN diferent, l'activitat de l'empresa no es veu afectada pel tràfic de backup, i viceversa

2.2. Tipus de còpies

Com hem vist abans, cada empresa ha d'identificar quines dades vol protegir amb la còpia de seguretat. Hi ha tres tipus de còpia:

- Completa. Inclou tota la informació identificada. Si era una unitat de disc, tots els arxius i carpetes que conté; si era una base de dades, l'exportació de totes les seues taules.

- Diferencial. Inclou tota la informació que ha canviat des de l'última vegada que es va fer una còpia de seguretat completa. Per exemple, si el dilluns es va fer una completa i el dimarts sol ha canviat el fitxer a.txt, en la cinta del dimarts solament s'escriu aquest fitxer. Si el dimecres sol ha canviat el fitxer b.doc, en la cinta del dimecres s'escriuran a.txt i b.doc.

- Incremental. Inclou tota la informació que ha canviat des de l'última còpia de seguretat, siga completa o incremental. En l'exemple anterior, la cinta del dimarts portarà el fitxer a.txt, però la cinta del dimecres sol b.doc.

Una empresa podria decidir fer tots els dies copia completa. Però, si hi ha moltes dades, és un procés lent i alguna cosa arriscat, perquè cal vigilar que s'estiga fent una còpia consistent de la informació (mentre es fa la còpia, el sistema segueix funcionant i en qualsevol moment algú pot introduir canvis). Amb la còpia diferencial o incremental tenim les mateixes garanties, perquè recuperem la informació aplicant l'última cinta completa i l'última diferencial (o l'última completa i totes les incrementals).

En una empresa mitjana és habitual l'esquema de deu cintes:

- Una per a un backup complet (els divendres).

- Quatre per a un backup parcial diari (diferencial o incremental) de dilluns a dijous.

- Cinc per a backups complets anteriors: quinzenal, mensual, trimestral, semestral i anual.

Triar entre diferencial o incremental per al backup diari depèn de cada empresa. Si hi ha poca activitat diària, es pot permetre el diferencial, perquè aporta l'avantatge que cada cinta diària té tota la informació necessària per a recuperar aqueix dia (en l'incremental, si perdem la cinta d'un dia, pot ser que tinga fitxers que no estiguen en les cintes següents). Però si hi ha molta activitat, estem de nou davant el problema de mantenir la consistència de la còpia.

3. Imatge del sistema

La imatge del sistema no és tan important com les dades, perquè si no hi ha altre remei podríem instal·lar des de zero, amb una ISO del sistema operatiu i les aplicacions necessàries, i després apliquem a tots dos les opcions de configuració que tenim documentades. Però aquest procés és lent i generalment necessita que un tècnic estiga present (i també es pot equivocar). Una imatge ens ajudarà a recuperar el sistema ràpidament i sense errors.

La imatge d'un sistema és un bolcat del contingut del disc dur. Amb tot: executables i dades del sistema operatiu, executables i dades de les aplicacions instal·lades i dades personals dels usuaris. Generalment es comprimeix en un únic fitxer que ocupa molts GB, depenent de la grandària del disc, l'ocupació i el tipus de continguts. Aquest fitxer sol estar xifrat i s'emmagatzena lluny del sistema original, com fem amb les cintes del backup.

Com hem explicat abans, la imatge no és un mètode adequat de fer còpies de seguretat en una empresa. És cert que copiem tot, programes i dades, però és un procés lent durant el qual el sistema no està operatiu, la qual cosa és incompatible amb la missió crítica que la informàtica exerceix en una empresa.

3.1. Creació i recuperació. LiveCD

Existeixen diverses eines en els diferents sistemes operatius per a crear i recuperar imatges (Norton Ghost, Acronis True Image), però presenten l'inconvenient de ser formats propietaris, de manera que per a recuperar-les necessites el mateix programa (fins i tot la mateixa versió), la qual cosa pot ser un problema en determinades circumstàncies.

Nosaltres anem a estudiar una solució senzilla i genèrica, disponible per a qualsevol plataforma maquinari habitual. Consisteix en la utilització d'un LiveCD Linux, amb el qual arrancarem l'ordinador el disc del qual volem clonar. Una vegada dins, triarem el dispositiu local o remot on emmagatzemar la imatge (generalment, un disc USB) i procedirem a executar la còpia. Per descomptat, una solució alternativa és apagar l'ordinador, extraure el disc dur, punxar-lo en un altre ordinador i fer la còpia allí. El LiveCD ens estalvia aquestes manipulacions. Els avantatges del LiveCD són:

- És una solució vàlida per a clonar sistemes Windows o Linux en qualsevol de les seues versions, perquè treballem directament amb el disc, sense importar què hi ha dins.

- És una solució vàlida per a qualsevol maquinari convencional, perquè Linux funciona en quasi totes les plataformes.

- És una solució interoperable: el format del fitxer és estàndard, de manera que un fitxer creat amb un LiveCD es pot recuperar amb un altre LiveCD diferent.

Els inconvenients són:

- Com qualsevol imatge, cal recuperar-la sencera, no hi ha opció de triar carpetes o fitxers.
- Durant la recuperació estem escrivint en tot el disc, un error en un sector pot interrompre l'operació.

- La grandària del disc on recuperem ha de ser el mateix o superior al del disc original.

- No inclou opcions avançades, com deixar la imatge en el mateix disc i instal·lar un gestor d'arrencada que permeta recuperar-la fàcilment, com ocorre en els ordinadors actuals. Encara que és una opció poc fiable, perquè el dany del disc que ens porta a recuperar la imatge li pot haver afectat a ella.

3.2. Congelació

En alguns entorns interessa donar una configuració estable a l'ordinador i després impedir qualsevol canvi, tant si ve de l'usuari o d'algun intrús (virus, troyans, etc.). L'exemple més típic són les sales d'ordinadors d'un cibercafé: quan s'acaba el temps de lloguer del lloc, cal esborrar qualsevol rastre (fitxers personals, programes instal·lats) perquè el següent client trobe l'ordinador «net». Aquesta és la missió del programari de congelació: una vegada instal·lat, pren nota de com està el sistema (snapshot) i, des d'aqueix instant, qualsevol canvi que ocórrega en el sistema podrà ser anul·lat quan l'administrador ho sol·licite (en el cas del cibercafé es configura perquè ocórrega de manera automàtica en la pròxima arrencada).

Els sistemes Windows també inclouen aquesta funcionalitat de crear punts de restauració, però la funcionalitat és limitada, perquè solament es preocupen de programes, no de dades. Les eines de congelació solen permetre mantenir diversos snapshots, per a facilitar tornar a altres situacions passades. L'espai ocupat en el disc pot arribar a ser un problema.

El principal inconvenient d'aquesta solució apareix quan volem instal·lar un programa nou. En alguns programes cal descongelar, instal·lar i tornar a congelar. En altres simplement recordar que, si alguna vegada recuperem un snapshot anterior, caldria tornar a instal·lar-ho. I açò s'agreuja amb el fet que la majoria dels sistemes operatius i les aplicacions s'actualitzen amb molta freqüència (el famós Patch Tuesday). Per tant, les solucions de congelació tenen una aplicabilitat bastant limitada perquè és difícil administrar els diferents snapshots.

3.3. Registre de Windows i punts de restauració

Els sistemes Windows inclouen una funcionalitat similar al programari de congelació de l'apartat anterior: es diuen punts de restauració i arrepleguen l'estat dels executables i la configuració del sistema operatiu (no s'inclouen els documents dels usuaris). És important crear un punt de restauració abans d'efectuar canvis importants en el sistema, com la instal·lació o substitució de drivers o l'aplicació de pegats.

El **Registre de Windows** és una base de dades jeràrquica que emmagatzema configuracions i opcions del sistema operatiu Windows i de les aplicacions instal·lades. Conté informació sobre controladors, programes, configuració d'usuari i més.

Els **Punts de Restauració** són còpies de seguretat automàtiques que el sistema operatiu crea abans de fer canvis importants, com actualitzacions o instal·lacions de programari. Aquests punts permeten tornar a un estat anterior del sistema en cas de problemes.

Diferències clau:

- Registre de Windows → Conté configuracions i paràmetres del sistema.

- Punts de Restauració → Serveixen per recuperar l'estat anterior del sistema si hi ha errors.

3.4. Eines de revisió mèdica de discos

Ja sabem com protegir les nostres dades davant d'una fallada en un disc (RAID, backup, emmagatzematge en el núvol, etc.). Però no hauríem d'esperar asseguts fins que un disc falle i confiar que entrarà en funcionament el mecanisme de respatler. Sempre és aconsellable prendre mesures preventives, en aquest cas la detecció primerenca de la fallada.
En Windows 7 ens situem sobre la unitat i, en el menú de botó dret, triem Propietats. Apareix una finestra i punxem en la pestanya Eines. Ací tenenim l'eina de comprovació d'errors.

Com estem usant aquesta unitat per al sistema operatiu, ens trobem davant un problema similar a la còpia consistent que vam veure amb anterioritat. L'eina ens adverteix que no pot fer els canvis i que ho prepara tot per a fer-ho en la propera arrencada. S'aconsegueix el mateix executant el comando chkdsk /f des del cmd. En Linux tenim el comando fsck per a comprovar la integritat del sistema de fitxers. Per a comprovar el disc podem utilitzar la utilitat de discos.

En aquesta eina apareixen en el costat esquerre totes les unitats connectades al equip. En seleccionar alguna, en el costat dret obtenim tota la informació (model, capacitat, volums) i podem llançar diverses operacions (formatar, editar particions, comprovar el sistema d'arxius).

Hi ha una operació especial anomenada Dades SMART. Es refereix a un estàndard utilitzat en els discos durs per a analitzar detalladament el seu estat. Si en aquesta eina l'estimació general és que el disc no està sa, hem de substituir-ho com més aviat millor.

Tema 5: Seguretat activa: sistema operatiu i aplicacions

1. Carrera d'obstacles

Per moltes mesures de control d'accés que posem, un hàcker pot asseure's davant d'un equip de la nostra empresa. O directament robar un portàtil a un dels nostres directius. Anem a intentar posar-li-ho difícil per a que el seu «treball» siga una carrera d'obstacles i, segurament, davant alguna barrera, desistisca.

1.1. La caixa de l'ordinador

En primer lloc evitarm que puga obrir la caixa de l'ordinador per a endur-se el disc dur i a casa. La majoria de les caixes dels ordinadors de sobretaula porten un parell d'ancoratges on col·locar un cadenat normal. També està l'opció de canviar un caragol normal per un caragol amb clau. Per als portàtils tenim el famós cadenat Kensington que té un cap que s'introdueix per una ranura especial de la caixa del portàtil. El cap continua en un cable d'acer perquè l'enrotllem en alguna part fixa (la taula o algun ancoratge especial). El cap pot utilitzar una clau o una combinació de nombres.

Els cadenats són poc efectius, però almenys obliguem al lladre a portar alguna eina més i li fem perdre un temps valuós. Fins i tot si s'obri, la majoria de les caixes d'ordinador professionals porten un detector que grava en la memòria de la BIOS la data i hora en què s'ha produït l'obertura. L'endemà, quan l'empleat encenga l'ordinador, apareixerà un missatge en pantalla avisant-lo.

1.2. La BIOS de l'ordinador

Amb el cadenat, el hàcker ja no es podrà emportar-se el disc. Però existix la tècnica de l'arrencada amb LiveCD, muntar el disc dur local i fer una còpia del mateix en un dispositiu extern. Per a evitar que un hàcker faça el mateix, cal entrar en la BIOS per a modificar l'ordre d'arrencada. Per defecte sol estar posat primer el CD/DVD i després el disc dur local HDD (Hard Disk Drive). Hem de canviar-ho perquè el primer i únic siga el HDD (si algun dia cal una altra cosa, sempre podrem tornar ací). Aquesta tasca se sol fer quan arriba un nou equip a l'empresa. Tampoc convé oblidar canviar les contrasenyes de l'administrador, perquè si no en posem cap o deixem els valors per defecte, el hàcker pot entrar a la BIOS i modificar l'ordre d'arrencada. En algunes empreses fins i tot activen una contrasenya d'ús de l'ordinador. És a dir, en arrancar la BIOS sempre demana una contrasenya, no solament quan volem accedir a la seua configuració. Si hem oblidat les contrasenyes de la BIOS, la solució típica és retirar la pila que manté aquests valors en memòria. En les plaques base modernes directament hi ha un jumper que, si està tancat quan l'ordinador arranca, esborra aquests valors. Per tots dos motius (pila o jumper) cal seguir evitant l'accés a l'interior de la caixa de l'ordinador.

1.3. El boot manager

Ja hem aconseguit que l'hàcker no es puga emportar res i que només arranque la màquina des del nostre disc local. En aquest disc pot ocórrer que tinguem instal·lats diversos sistemes operatius (o diverses versions del mateix sistema, com sol ocórrer en Linux), de manera que, en arrancar, un programa anomenat boot manager (gestor d'arrencada) ens permeta triar un d'ells. Ara cal establir qui accedeix a cada opció.

1.4. Xifrat de particions

Amb les barreres que hem posat fins ara, el hàcker no pot endur-se res; només pot arrancar des del disc local i només pot triar una de les entrades del boot manager. Però si alguna d'aquestes mesures falla, encara podem evitar que accedisca a les nostres dades: anem a xifrar el contingut, de manera que siga il·legible.

2. Autenticació en el sistema operatiu

Hem aconseguit que el nostre hàcker no puga evitar que la màquina arranque amb un sistema operatiu instal·lat per nosaltres. Comparat amb el que hem vist fins a ara (BIOS, boot manager), els sistemes operatius permeten incloure molt més programari d'autenticació i més complex. Veurem múltiples mecanismes per a assegurar-nos que el nostre sistema solament l'usa qui està autoritzat.

2.1. Usuari/password

És el mecanisme més típic. Aplicant l'estratègia «alguna cosa que saps», la pantalla inicial del sistema espera que la persona introduïsca el nom d'un usuari i la contrasenya associada a aquest usuari. Mentre tecleja, el nom de l'usuari és visible però amb traseña no (se sol substituir per asteriscos, guions, etc.), per a evitar que la veja algú que es trobe a la nostra esquena.

Si ens equivoquem, bé perquè l'usuari no existeix, bé perquè la contrasenya no és la correcta, el sistema ens impedeix l'entrada i ens deixa intentar-ho de nou. En alguns sistemes ens ofereix una pista sobre la contrasenya (si la vam posar l'última vegada que canviem la contrasenya), i la majoria té un límit d'intents. Si consumim aquest límit, el sistema es pot bloquejar durant un temps o definitivament (per exemple, els mòbils tenen un límit de tres intents per a introduir el PIN). Amb aquest límit evitem atacs per força bruta que proven una a una totes les combinacions de lletres, nombres i caràcters especials.

Per a posar les coses més difícils als hàckers, una bona mesura és canviar el nom per defecte dels usuaris amb més privilegis sobre el sistema. Així no solament hauran d'aplicar la força bruta sobre la contrasenya, sinó també sobre el nom de l'usuari. Per exemple, en els primers sistemes Unix es treballava des de l'usuari root amb tots els privilegis (superusuari), en l'actualitat, encara que l'usuari root segueix existint, el sistema no permet usar-lo per a entrar al sistema, en canvi, els privilegis s'administren mitjançant el mecanisme su, com veurem més endavant. Així i tot, sempre convé utilitzar contrasenyes no trivials: paraules que no apareguen en el diccionari de cap llengua, combinar lletres majúscules amb minúscules, nombres, signes de puntuació, etc. I canviar la contrasenya regularment. Els sistemes operatius permeten obligar a l'usuari a complir totes aquestes normes.

2.2. Targetes

En algunes ocasions, el mecanisme d'usuari i contrasenya no és suficient: és insegur (algú pot espiar les tecles que premem) o simplement molest (per exemple, en els torns d'accés a l'entrada de l'empresa no podem perdre el temps teclejant). Per a aquests casos aplicarem l'estratègia «alguna cosa que tens» i repartirem targetes entre els usuaris. Per exemple, els caixers automàtics dels bancs apliquen una seguretat doble: la targeta més un nombre PIN.

Les targetes amb xip són més segures però més cares, per la qual cosa s'utilitzen en ocasiones especials, encara que ja estan estenent-se Hi ha dos tipus: Les que són simplement un dispositiu d'emmagatzematge: contenen les nostres claus perquè les llija el dispositiu on introduïm la targeta. Les que contenen un dispositiu de processament (xip): contenen les nostres claus, però mai ixen de la targeta. El xip es limita a xifrar amb elles algun desafiament que llança el dispositiu per on introduïm la targeta.

2.3. Biometria

La seguretat del mecanisme usuari/contrasenya és suficient per a la majoria de les aplicacions. La targeta és còmoda. Però qualsevol podria asseure's en el nostre ordenador, inserir la nostra targeta (robada o duplicada), introduir el nostre usuari i amb la contrasenya (ens pot haver espiat, o li la vam dir en anar-nos-en de vacances) i accedir al sistema suplantant-nos. Si la informació que manipulem és important, aplicarem l'estratègia «alguna cosa que eres», per a complementar el mecanisme usuari/contrasenya amb un control més: la biometria.

La biometria consisteix a identificar alguna característica física del subjecte: la petjada dactilar, l'ull, la veu. La persona o persones autoritzades han de gravar primer la seua característica física. Per exemple, en la petjada es graven dits de les dues mans, per si es pateix un accident en una d'elles. Després, cada vegada que vulguen utilitzar l'ordinador, hauran de situar el dit damunt del sensor. Com hem dit abans, el control biomètric no és substitutiu de l'usuari/contrasenya, sinó complementari: convé tenir els dos per a augmentar la seguretat (estratègia «alguna cosa que saps, alguna cosa que eres»). Encara que en algunes ocasions sí que s'utilitza per a estalviar la molèstia d'estar prement tecles: per exemple, per a accedir a alguna zona vip de l'empresa.

Actualment els mòbils de gama alta i mitjana ja n'incorporen.

2.4. Elevació de privilegis

Ja estem autenticats en el sistema operatiu i podem treballar amb ell, però sempre limitats als privilegis associats a l'usuari amb el qual ens hem presentat. En les empreses, la majoria dels empleats utilitzen usuaris que no tenen permís per a realitzar tasques d'administració de la màquina (usuaris limitats, no administradors), així es redueix el dany que puguen causar, ja siga per error o perquè s'ha colat un virus. Però hi ha determinades situacions (instal·lació de nous programes, modificació de paràmetres del sistema) per a les que sí que necessitem ser administradors. Una solució és eixir de l'usuari actual i entrar com a administrador, però és més senzill sol·licitar, de manera puntual, una elevació de privilegis. Consisteix a demanar-li al sistema executar un determinat programa amb permisos d'administrador. S'aplica solament a de forma puntual i solament a aquesta execució: no afecta a les aplicacions obertes abans o després, ni quan obrim aquest mateix programa més endavant. Quant a l'usuari, depenent de la configuració del sistema, simplement apareixerà una finestra de confirmació o ens demanarà una nova autenticació.

Abans de realitzar l'elevació de privilegis, el sistema ens demanava confirmació. Tradicionalment açò no ocorria en els sistemes Windows, fins a XP inclusivament: una vegada entràvem com a administrador, no hi havia cap control més. Com a conseqüència, qualsevol virus podia dominar la màquina. I com en els ordinadors d'ús personal se sol utilitzar sempre l'usuari administrador perquè és el propi usuari el que realitza les tasques

de manteniment de la seua màquina, ací tenim la principal causa de la mala fama dels sistemes Windows quant a seguretat. Per a mitigar-ho, en la versió Vista es va afegir el famós UAC (User Access Control). Ara el sistema avisa a l'usuari quan un programa sol·licita executar una operació de administració. Si no estàvem fent res especial, com una instal·lació de nou programari, podem suposar que és un atac i detenir-ho ací.

Però al final va resultar ser molt molest, perquè moltes eines necessiten fer operacions especials en el sistema i no per açò són perilloses (per exemple, canviar l'hora). A més, la majoria dels usuaris no saben a priori si el que va a fer l'aplicació és nociu o no i, per defecte, sempre accepten (amb la possible entrada de virus) o sempre neguen (llavors, les noves aplicacions no s'instal·len bé). El resultat final va ser que molta gent no ho va entendre com una millora i es va queixar. Microsoft es va veure obligat aleshores a introduir una modificació en Vista que permetia desactivar el UAC, de manera que tornàvem al funcionament de XP. En Windows 7 i Windows 2008 s'ha millorat el UAC en permetre certa configuració.

3. Quotes

Fins ara hem protegit els nostres sistemes evitant l'accés de persones no autoritzades. Ara anem a protegir-los de les persones que sí que estan autoritzades. Perquè els nostres usuaris, amb intenció o no, també poden danyar el sistema. Per exemple, poden descarregar molts arxius pesats, de manera que omplin el disc i el sistema comença a fallar perquè sempre necessita escriure en alguns fitxers (el típic error filesystem full). També poden llançar processos molt pesats, que ralentizen la CPU i no permeten treballar als altres usuaris. Per a evitar-ho, els sistemes es configuren per a aplicar quotes. Per al disc, s'estableix que cada usuari pot ocupar un nombre determinat de GB. Quan excedeix aqueix límit, podem configurar de manera que el sistema no li permeta estendre's més.

Cal assignar les quotes amb cura: Si són molt baixes, tindrem als usuaris queixant-se tots els dies perquè no els deixem treballar. Cal tenir especial cura amb els usuaris que es creen perquè són necessaris per a arrancar una aplicació, com el www-data del servidor web Apatxe: si excedeixen la quota, l'aplicació es pararà. Si són molt altes, no tindran l'efecte dissuassori que s'espera d'elles i, al final, acabarem comprant més discos.

4. Actualitzacions i pegats

Ja tenim el sistema protegit contra l'accés d'estranys i contra el mal ús dels propis. Però estem parlant de programari: fet per humans i, per tant, subjecte a errades. El CD/DVD que hem utilitzat per a instal·lar Windows conté una versió concreta alliberada en una data concreta, des de llavors, els programadors de Microsoft han seguit treballant. El resultat són les actualitzacions: paquets de programari on s'introdueixen millores i, sobretot, corregeixen defectes. Com a administradors responsables del sistema, hem d'instal·lar aquestes actualitzacions.

Per sort, no cal esperar al fet que ens arribe un altre CD amb cada actualització: es descarrega automàticament des d'Internet. Microsoft allibera actualitzacions de forma rutinària, i Service Pack, cada dues setmanes, els dimarts a la nit, però si troben la solució a un problema urgent, l'alliberen immediatament, sense esperar al següent dimarts.

Les actualitzacions són configurables. Podem triar entre:

- No cercar actualitzacions ni instal·lar-les (no recomanable).

- Comprovar si hi ha actualitzacions, però no descarregar-les ni instal·lar-les. Açò només té sentit en equips amb poc disc o accés limitat a Internet.
- Descarregar i instal·lar sempre. És el més habitual.

Els pegats són semblats a les actualitzacions, però s'utilitzen solament per a corregir defectes i solen necessitar que l'usuari el descarregue i l'instal·le. És a dir, quan algú (el propi fabricant o algun client) detecta un problema en una aplicació, el fabricant avisa a tots els clients afectats, els escriu un workaround i, quan té el pegat que ho arregla, els avisa perquè el descarreguen del seu lloc web. Per aquest motiu és important tenir còpies originals de les aplicacions i registrar-se en la web del fabricant per a estar al dia dels problemes que apareguen.

5. Antivirus

Podem tenir el sistema actualitzat, però hi ha molt de programador maliciós que vol instal·lar programari en el nostre sistema per al seu profit (diversió, espionatge industrial, etc.). Són els anomenats virus informàtics, que són de molts tipus (cucs, troyans, etc.), però, en qualsevol cas, estem parlant de malware (programari maligne) i cal evitar-los.

Els virus poden instal·lar-se en la nostra màquina sense que ens enterem, aprofitant algun defecte del sistema operatiu o les aplicacions instal·lades (defectes que encara no s'han resolt, o s'han resolt i no ens hem assabentat). Però també els podem «obrir la porta» perquè estem fent la instal·lació d'una aplicació que hem aconseguit d'algun lloc no oficial. Per a combatre tots dos casos hem d'instal·lar un antivirus. L'antivirus és un programa que està vigilant contínuament el que ocorre en la nostra màquina. Concretament, qualsevol programari que s'intenta executar (executables .exe, llibreries .dll) primer passa per l'antivirus. Ell el compara amb la seua base de dades de virus i, si el troba, impedix que s'execute i avisa a l'usuari. Encara que l'antivirus sempre va per darrere del virus, és important tenir-ho actualitzat. L'actualització afecta tant a la base de dades de virus coneguts com al programari del propi antivirus.

6. Monitoratge

Hem evitat l'accés a estranys, hem aplicat quotes als interns, tenim activades les actualitzacions automàtiques del sistema operatiu i totes les aplicacions instal·lades, tenim antivirus actualitzat... Estem tranquils? Doncs no. Hem vist que qualsevol de les mesures aplicades és imperfecta. La nostra tasca és instal·lar-les, formar als usuaris i, tots els dies, vigilar que tot estiga normal. Aquesta vigilància consisteix en: Revisar els log del sistema i les aplicacions. Qualsevol succés anòmal quedarà anotat en algun lloc. Si el sistema ho permet, activar la còpia sincronitzada del log en una altra màquina. És a dir, cada avís s'escriu alhora en la nostra màquina i en una altra. D'aquesta forma podrem analitzar un desastre, evitarem que un hàcker esborre les seues petjades, etc.

Revisar l'ocupació del sistema, principalment el disc i la CPU. Allò més habitual és programar una tasca per a revisar-ho regularment (cada cinc minuts, per exemple) i generar una alarma que alerte a l'administrador quan se supere algun límit (90 % del disc, per exemple).
Subscriure's a les newsletters dels fabricants del nostre maquinari i programari per a tenir a mà la informació oficial: actualitzacions, pegats, nova funcionalitat, workarounds, etc.

Participar en fòrums d'usuaris de les mateixes aplicacions que nosaltres, per a estar al dia dels problemes que apareixen (pot ser que ens passe el mateix) i per a poder demanar ajuda si alguna cosa ens sobrepassa (en paral·lel amb la consulta al suport oficial).

El monitoratge dels log consisteix primer a diferenciar què és un problema i què no ho és. El text de log ajuda perquè sol tenir un indicador de gravetat (crítica, alt, mitjà, baix o simple avís), encara que és la classificació del fabricador: solament nosaltres coneixem el nostre sistema i sabem les conseqüències de cada avís. Per a conèixer l'ocupació de recursos d'una màquina podem entrar en ella i llançar eines locals, o el comando top en Linux.

Però si tenim al nostre càrrec el monitoratge de molts equips, no podem estar tot el dia entrant en cadascun d'ells cada cinc minuts. Convé instal·lar una eina d'inventari i monitoratge. L'inventari és la llista d'equips i connexions i la configuració de tots dos. El monitoratge és la supervisió en tot moment de l'estat dels elements de l'inventari. Aquestes eines faciliten molt el treball de l'administrador perquè:

- Rastregen la xarxa periòdicament cercant noves altes i baixes d'equips en l'inventari. Són capaços d'identificar diferents tipus d'equips, no sol ordinadors, sinó també equipament de xarxa. Per a açò és necessari que els equips oferisquen interfícies estàndard, com SNMP (Simple Network Management Protocol). Obtenen la configuració per a tots els equips de l'inventari i la registren en una base de dades per a generar informes, avisar de canvis, etc. Incorporen alertes sobre ocupació de disc, inactivitat d'una interfície, etc. Podem monitoritzar en directe l'activitat de les interfícies de xarxa, ús de CPU, etc. La implantació d'una d'aquestes eines representa la frontera entre una administració artesanal de la xarxa i sistemes, i una administració moderna i professional.

El punt d'inflexió sol ser un límit en la proporció entre el nombre d'equips i el nombre d'integrants del departament de suport informàtic. Quan el personal ja està desbordat de treball, introduir aquestes eines permet automatitzar les tasques rutinàries i així deixar temps lliure a les persones que atenen els problemes complicats. Per exemple, localitzar els equips de la xarxa que tenen un determinat programari instal·lat, detectar nous equips connectats però no autoritzats, etc.

7. Aplicacions web

L'arquitectura d'aplicacions ha evolucionat amb el temps: En els anys seixanta i setanta eren monolítiques: tota la funcionalitat, tant la interfície d'usuari com la lògica de procés, estava en la mateixa màquina. Els usuaris utilitzaven terminals «simples» connectats a l'ordinador principal. La protecció d'una aplicació monolítica se centrava a protegir la màquina on executaven tots els programes. En els anys vuitanta i noranta apareixen els ordinadors personals i les xarxes de comunicacions dins de les empreses. Aquests dos avanços permeten implementar les aplicacions seguint l'arquitectura client-servidor: la interfície d'usuari i part de la lògica de procés estan en l'ordinador de l'usuari, i la resta de la lògica de procés està en un ordinador central, al que connecten els ordinadors d'usuari mitjançant la xarxa local. La protecció es complica: ara cal protegir a cada client, el servidor i la xarxa local de l'empresa. A partir dels anys noranta, l'èxit d'Internet permet estendre les aplicacions web (que segueixen el model client-servidor) a qualsevol punt de connexió del planeta. Hi ha un parell de diferències amb els anys vuitanta: el client sol ser sempre mateix (el navegador) i la comunicació utilitza xarxes públiques, sobre les quals l'empresa té nul control. La protecció és més difícil que mai.

Ningú dubta dels avantatges d'implementar una aplicació mitjançant tecnologies web: No necessitem instal·lar res en el client: solament es necessita el navegador (que s'inclou amb el sistema operatiu i que té altres usos, com navegar per Internet). Amb açò evitem instal·lar un client nou que puga entrar en conflicte amb altres aplicacions de la màquina, l'usuari no necessita privilegis especials per a instal·lar programes, etc.

Qualsevol actualització generada pels nostres programadors (més funcionalitat, pegats que arreglen defectes) està immediatament disponible per als usuaris perquè sempre descarreguen la pàgina actualitzada de l'última versió. No cal esperar al fet que tots els usuaris siguen avisats de l'actualització, la descarreguen, instal·len, etc. Per aquesta raó estan àmpliament esteses en Internet (Google Apps, Twitter, WordPress YouTube, etc.), i també dins de les empreses, les intranets. Però hem d'anar amb compte amb: La màquina que allotja el servidor web i les seues aplicacions accessòries (base de dades i unes altres). Si un hàcker pren aquesta màquina, té accés a tota la informació i totes les connexions dels usuaris. Cal aplicar les mesures de protecció que hem estudiat en aquest tema.

Si la màquina del servidor web no és nostra, sinó llogada (hosting web), no tenim control sobre les mesures de protecció. Hem de confiar en la professionalitat del proveïdor i repassar el contracte, especialment l'apartat dels nivells de servei (SLA [Service Level Agreement]). Per exemple, podem exigir al proveïdor que si el servidor web està caigut més de dues hores a l'any, ens faça un descompte del 25 % en la següent quota. La transmissió entre el client web (navegador) i el servidor web. Moltes aplicacions encara utilitzen el protocol HTTP. En algun tram de xarxa pot estar escoltant un hàcker i conèixer què fem, fins i tot modificar-ho per al seu profit. Hem d'optar per HTTPS.

La màquina d'un usuari connectat pot haver estat hackeada i el seu navegador també. Per exemple, s'ha instal·lat un keylogger que envia totes les contrasenyes fora del nostre control. En aquest punt és important l'antivirus.

8. Cloud computing

Després de les aplicacions web, la següent evolució de les aplicacions en Internet és el cloud computing (computació en el núvol). Convé diferenciar entre computació en el núvol i emmagatzematge en el núvol (cloud storage: iCloud, Dropbox, Amazon S3). L'emmagatzematge també aporta flexibilitat (nombre variable de GB reservats, backup automàtic), però es limita a guardar arxius i carpetes. La computació és més àmplia perquè executa programes que treballen amb arxius, bases de dades, altres servidors, etc. No obstant açò, es complementen perquè la computació en el núvol pot treballar amb arxius d'emmagatzematge en el núvol. A les empreses ja no els interessa connectar a Internet un servidor web del seu CPD perquè necessiten dedicar recursos a proveir QoS (Quality of Service, qualitat de servei), bona connectivitat, servidors potents, administradors eficaços, etc. A més, obrir a l'exterior les connexions del CPD és una font de problemes per la quantitat d'atacs que ens poden arribar.

8.1. IaaS: Infrastructure as a Service

Un primera solució de cloud computing és el IaaS (Infrastructure as a Service). La nostra empresa vol posar una màquina sencera (un Linux, per exemple) en un proveïdor, però amb una diferència respecte del hosting dedicat: aquesta màquina s'executarà en un entorn virtualizado, de manera que podem regular la potència. Si l'aplicació està ralentint-se per un excés de càrrega, contractem temporalment més CPU i més RAM (i assumim l'increment de cost associat). Quan ja no tinguem tanta càrrega, tornarem a la

configuració bàsica. Fins i tot es pot sol·licitar que arranquen més màquines (es diuen instàncies). El procediment és similar al de les màquines virtuals: generem un disc virtual (fitxer vdi, per exemple), instal·lem el que necessitem (generalment Linux RedHat o Ubuntu, però també Windows Server) i ho pugem a la web del proveïdor. Des d'un panell de control en aquesta web modifiquem l'execució de la màquina segons ens convinga en cada moment.

Però en aquesta opció seguim necessitant personal especialitzat per a administrar aquestes instàncies, generar-les, actualitzar-les, configurar la seguretat, vigilar la virtualització, etc.

8.2. SaaS: Programari as a Service

Les empreses que no volen invertir en aquesta despesa (una fàbrica de formatges sap de formatges, no de programari) trien SaaS (Programari as a Service), aplicacions completes on el mateix proveïdor s'encarrega del desenvolupament de l'aplicació, el seu manteniment i també posa les màquines i la connectivitat (o en les màquines d'un IaaS, però mai en les nostres). Per exemple, per al correu de la fàbrica de formatges, en lloc d'utilitzar una màquina nostra (el que suposa contractar una bona connexió a Internet i assumir els recursos humans necessaris per a realitzar la configuració, administració, monitoratge (24 x 7...), podem simplement contractar el servei Google Apps de Google.

De cara a la protecció de les aplicacions, en els dos casos (IaaS, SaaS), com ja passava amb el hosting, perdem el control sobre la seguretat de la màquina i el programari que executa en ella: hem de confiar en la professionalitat del proveïdor i redactar molt bé els SLA del contracte del servei.

Tema 6: Seguretat activa: accés a xarxes

1. Xarxes cablejades

En les dues unitats anteriors hem estudiat a fons com protegir la nostra màquina juntament amb les dades i el programari que s'executa en ella. Però en una empresa és estrany trobar una màquina aïllada. Generalment estan connectades a una xarxa d'àrea local LAN per a utilitzar els recursos d'altres màquines i per a que altres màquines aprofiten els seus (per exemple, el disc en xarxa NAS). La mateixa cura que hem tingut vigilant l'activitat que ocorre dins de la màquina cal mantenir-la quan les dades ixen i entren per alguna de les seues interfícies de xarxa.

També cal protegir-se dels atacs que vinguen per la xarxa. Una màquina que ofereix serveis TCP/IP ha d'obrir certs ports. A aquests ports poden sol·licitar connexió màquines fiables seguint el protocol estàndard, o màquines malicioses seguint una variació del protocol que provoca una fallida en el nostre servidor. El resultat d'aquesta fallida seran, com a mínim, que el servei queda interromput, però en alguns casos l'atacant pot prendre el control de la màquina (per açò, cada vegada més, els serveis s'executen amb els mínims de privilegis).

Les primeres xarxes LAN cablejades eren molt insegures, perquè tots els ordinadors estaven connectats al mateix cable (arquitectura en bus), de manera que qualsevol podia posar la seua targeta de xarxa en mode promiscu i escoltar totes les converses, no solament aquelles en les quals participava. Actualment, aquesta por pràcticament ha desaparegut, perquè utilitzem la topologia en estel: cada equip té un cable directe a un port d'un commutador de xarxa (switch) i per ací envien els seus paquets. El switch els rep i decideix per quin port va a enviar-los per a que arriben a la destinació. A més de millorar la seguretat, estem millorant el rendiment, perquè no malgastem recursos pel fet de enviar paquets a equips que no els interessen.

No obstant açò, les xarxes commutades tenen les seues pròpies vulnerabilitats:

- Cal protegir el switch físicament: tancar-ho en un armari/rack amb clau dins d'una sala amb control d'accés. Així evitem no només el robatori, sinó que algú accedisca al botó de réset i el configure a la seua manera.
- Cal protegir el switch lògicament: posar usuari/contrasenya per a accedir a la seua configuració.
- Cal fer grups de ports, perquè en un switch solen estar connectats grups de màquines que mai necessiten comunicar-se entre si. Hem d'aïllar-les per a evitar problemes de rendiment i seguretat.

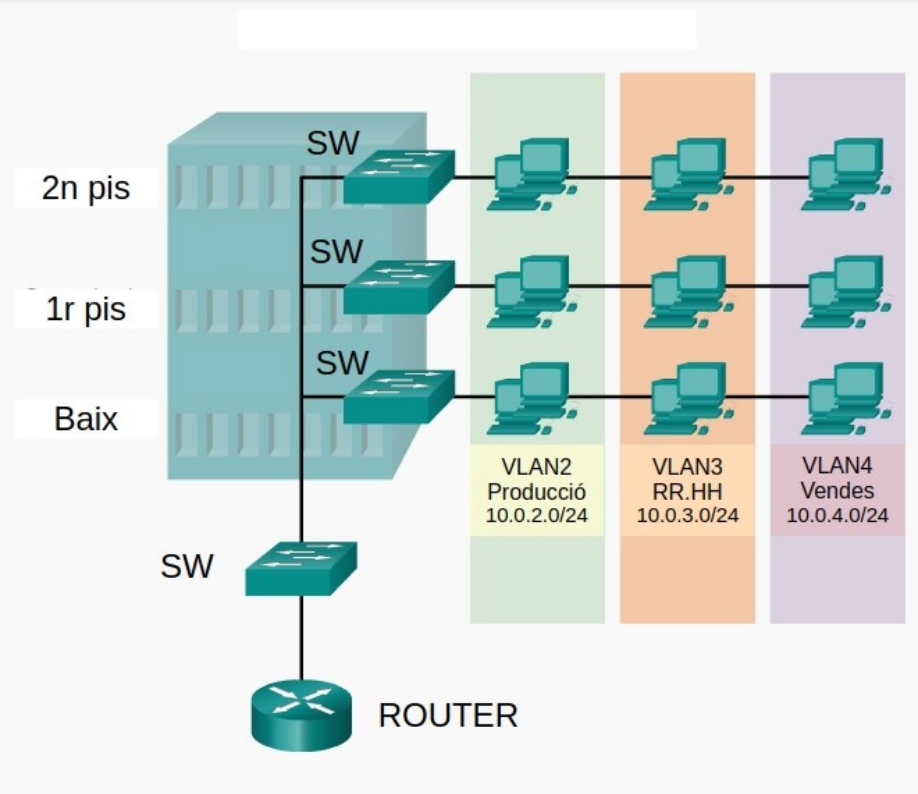
1.1. VLAN

Una VLAN (Virtual Local Area Network) és una xarxa lògica dins d'una xarxa física que permet agrupar dispositius en segments virtuals, independentment de la seva ubicació física. Això significa que els dispositius que pertanyen a una VLAN poden comunicar-se entre si com si estagueren connectats al mateix switch, encara que estiguen en diferents parts de la xarxa física.

Tot açò oferix uns avantatges de seguretat si usen les VLANs:

1. **Segmentació de la xarxa**: Les VLANs permeten dividir una xarxa en segments més xicotets i aïllats. Això reduix el risc que un atacant puga accedir a tota la xarxa si compromet un sol dispositiu.
2. **Control d'accés**: Es pot configurar el trànsit entre VLANs mitjançant llistes de control d'accés (ACLs) o firewalls, la qual cosa permet restringir la comunicació entre diferents VLANs. Això és útil per limitar l'accés a zones sensibles de la xarxa.
3. **Aïllament de trànsit**: El trànsit dins d'una VLAN no es transmet a altres VLANs, la qual cosa impedeix que els usuaris no autoritzats intercepten dades sensibles.
4. **Contenció de brots de malware**: Si un dispositiu dins d'una VLAN es veu compromès, el malware o l'atac es pot contenir dins d'aquesta VLAN, evitant que es propague a altres parts de la xarxa.
5. **Gestió de polítiques de seguretat**: Les VLANs faciliten l'aplicació de polítiques de seguretat específiques per a diferents grups d'usuaris o dispositius. Per exemple, es poden aplicar regles diferents per a empleats, convidats o dispositius IoT.
6. **Reducció de l'àmbit de difusió (broadcast)**: Les VLANs limiten l'àmbit dels dominis de difusió, la qual cosa redueix el risc d'atacs de tipus "broadcast storm" o l'ús indegut de protocols de difusió.

Per tant, l'ús de VLANs oferix una major flexibilitat i seguretat a les xarxes, permetent una millor gestió del trànsit i la contenció de possibles amenaces.



Una VLAN basada en grups de ports no queda limitada a un switch. Si ens fixem en la figura anrerior, un dels ports pot estar connectat al port d'un altre switch, i, al seu torn, aquest port forma part d'un altre grup de ports, etc. Per exemple, quan el departament de producció té part de la seua personal en la primera planta i part en la segona, i part en la planta baixa, cal deixar un port en cada switch per a interconnectar-los.

En la figura tenim diversos equips en cada planta i un switch. No obstant açò, és extrany que les VLAN estiguen completament aïllades de la resta del món. Com a mínim, necessitaran accés a Internet, així com connectar-se amb altres servidors interns de l'empresa (intranet, discos, backup, etc.). Per a interconnectar VLAN (capa 2) generalment utilitzarem un router (capa 3).

Capa 2. En el model TCP/IP la capa 2 o capa d'enllaç té una visió local de la xarxa: sap com intercanviar paquets de dades (trames) amb els equips que estan en la seua mateixa xarxa. La comunicació és directa entre origen i destinació (encara que creue un o diversos switch). Capa 3. La capa 3 o capa de xarxa té una visió global de la xarxa: sap com fer arribar paquets de dades fins a equips que no estan en la seua mateixa xarxa. La comunicació és indirecta, necessita passar per una màquina més: el router.

El router necessitarà connectivitat amb cadascuna de les VLAN que interconnecta. Una forma d'aconseguir-ho es amb el trunk port.

Un **port troncal** (o **trunk port**) en una configuració de múltiples VLANs és un port en un switch que pot transportar tràfic de diverses VLAN alhora. A diferència d'un **port d'accés** (access port), que només pertany a una única VLAN, un port troncal permet la comunicació entre VLANs en diferents switches.

Principals característiques:

1- Transporta tràfic de múltiples VLANs – Un port troncal pot portar tràfic de diverses VLAN usant etiquetatge de trames.
2- Usa protocols d'encapsulació – Normalment utilitza IEEE 802.1Q, que afegeix una etiqueta VLAN a cada trama Ethernet per identificar a quina VLAN pertany.
3- Connecta switches i altres dispositius – Sol ser utilitzat per interconnectar switches, routers o servidors que necessiten accés a múltiples VLANs.
4- Evita la necessitat de múltiples connexions físiques – Sense troncalització, caldria un cable independent per a cada VLAN entre switches.

1.2. Autenticació en el port. MAC i 802.1X

L'autenticació en el port és una tècnica de seguretat de xarxa que restringeix l'accés als ports d'un switch per evitar connexions no autoritzades. Les dues maneres més comunes d'implementar-la són mitjançant l'autenticació basada en MAC i l'autenticació IEEE 802.1X.

1.2.1. Autenticació basada en MAC (Port Security)

Aquest mètode controla l'accés a la xarxa basant-se en l'adreça MAC del dispositiu connectat. Funciona de la següent manera:
Com funciona? Al switch se li configuren manualment les adreces MAC permeses en un port específic. Si es connecta un dispositiu amb una MAC no autoritzada, el switch pot:

- Descartar el tràfic de la MAC no autoritzada.
- Deshabilitar el port (shutdown).
- Registrar una alerta sense bloquejar el dispositiu.

1.2.2. Autenticació IEEE 802.1X (Network Access Control - NAC)

L'estàndard 802.1X proporciona un mecanisme d'autenticació més avançat basat en credencials d'usuari en lloc de només adreces MAC.

Com funciona? Requereix un servidor RADIUS que valide els dispositius abans de permetre l'accés.

- Els dispositius han d'enviar nom d'usuari i contrasenya o certificat digital.
- Si l'autenticació és correcta, el switch permet el tràfic; si no, es bloqueja.

Components principals d'802.1X:

- Supplicant (Client) → El dispositiu que intenta accedir (exemple: ordinador, impressora).
- Authenticator (Switch o Punt d'Accés) → Controla l'accés al port.
- Authentication Server (RADIUS Server) → Verifica les credencials i aprova o rebutja la connexió.

1.2.3 Diferències clau entre MAC Authentication i 802.1X

Característica	Autenticació per MAC	IEEE 802.1X
Seguretat	Baixa (fàcil de suplantar una MAC)	Alta (usuari + contrasenya/certificat)
Necessita servidor RADIUS?	No	Sí
Flexibilitat	Baixa (es basa només en MAC)	Alta (pot fer autenticació per usuaris)
Ideal per a...	Xarxes menudes, dispositius sense suport 802.1X	Empreses, universitats, entorns segurs

2. Xarxes sense fils

L'ús de tecnologia WiFi en una empresa pot comportar diversos problemes de seguretat, ja que una xarxa sense fil és més vulnerable a atacs externs en comparació amb una xarxa cablejada. A continuació, es detallen els principals riscos i com mitigar-los:

Principals riscos de seguretat en WiFi d'empresa:

1- Atacs d'Intercepció i Eavesdropping. Sense encriptació adequada, un atacant pot capturar el tràfic WiFi amb eines com Wireshark o Kismet, llegint dades confidencials (contrasenyes, correus, documents).

La solució pot ser utilitzar xifrat fort (WPA3 o almenys WPA2-Enterprise). O implementar VPN per protegir les connexions remotes.

2- Atacs de "Man-in-the-Middle" (MitM). Un atacant pot crear un punt d'accés fals (Evil Twin Attack) amb el mateix nom que la xarxa real i interceptar dades.

Una solució és utilitzar certificats digitals i autenticació 802.1X. O bloquejar dispositius no autoritzats amb lístes de control d'accés (ACLs).

3. Atacs per força bruta i cracking de contrasenyes. Si la contrasenya WiFi és dèbil, pot ser descoberta mitjançant atacs de força bruta o diccionari.

Una solució és utilitzar contrassenyes robustes (més de 12 caràcters, lletres, números i símbols). O canviar periòdicament les claus d'accés.

4- Dispositius no autoritzats a la xarxa (Rogue APs). Un empleat o atacant podria instal·lar un punt d'accés no autoritzat, obrint una porta insegura a la xarxa.

Una solució és utilitzar sistemes de detecció d'intrusions sense fils (WIDS) per identificar punts d'accés desconeguts. O desactivar SSID broadcasting per evitar xarxes visibles.

5- Denegació de Servei (DoS/DDoS). Atacs com la inundació de tràfic (Deauthentication Attack) poden desconnectar tots els dispositius de la xarxa.

Podem Utilitzar 802.11w Management Frame Protection (MFP) per evitar atacs de desautenticació o implementar firewalls i monitorització de trànsit.

6- Mal ús per part d'empleats (Shadow IT). Els empleats poden connectar dispositius no autoritzats (smartphones, USB WiFi) o accedir a xarxes públiques insegures amb dispositius corporatius.

Solució: aplicar polítiques de seguretat WiFi amb accés segmentat (VLANs per a convidats i empleats). Formació en ciberseguretat per evitar males pràctiques.

7- Vulnerabilitats en dispositius IoT connectats. Dispositius IoT (càmeres de seguretat, sensors) sovint tenen seguretat feble i poden ser objectiu d'atacs.

Solució: mantenir el firmware actualitzat. O segmentar la xarxa IoT en una VLAN independent.

Bones pràctiques per millorar la seguretat WiFi:

- Xifrat WPA3 (o WPA2-Enterprise amb RADIUS).
- Desactivar WPS, ja que és vulnerable a atacs de força bruta.
- Filtrar adreces MAC per limitar els dispositius autoritzats.
- Crear VLANs per separar tràfic corporatiu, IoT i convidats.
- Monitoritzar la xarxa amb eines com Cisco ISE, Aruba ClearPass o WiFi IDS/IPS.
- Implementar 802.1X amb autenticació RADIUS per seguretat d'accés.

2.1. Associació i transmissió

L'associació i transmissió en xarxes WiFi es refereix als processos mitjançant els quals un dispositiu sense fils (com un ordinador, un mòbil o una tauleta) es connecta a una xarxa WiFi i com es transfereixen les dades dins d'aquesta xarxa.

El procés d'Associació en una Xarxa WiFi d'un dispositiu que vol connectar-se a una xarxa WiFi. Ha de seguir els següents passos:

1. Escaneig (Scanning)
    - El dispositiu cerca xarxes disponibles a l'entorn, escoltant les trames de balisa (beacons) enviades pels punts d'accés (AP).
    - Alternativament, pot enviar una petició de sonda (probe request) per buscar una xarxa específica.
2. Autenticació
    - En una xarxa oberta, aquest pas és automàtic.
    - En xarxes protegides (WPA2/WPA3), el dispositiu ha de proporcionar les credencials adequades (com una contrasenya).
3. Associació
    - Un cop autenticat, el dispositiu envia una sol·licitud d'associació al punt d'accés.
    - Si la sol·licitud és acceptada, es concedeix una connexió formal.
4. Obtenir una Adreça IP
    - Si la xarxa utilitza DHCP, el dispositiu obté automàticament una adreça IP.
    - Si la configuració és manual, l'usuari ha d'introduir l'adreça IP, la passarel·la i els servidors DNS.

Pel que fa a la transmissió de Dades en Xarxes WiFi, un cop establerta la connexió, la transmissió de dades seguix aquests passos:

1. Enviament i Recepció de Paquets
    - Les dades es divideixen en paquets i s'envien en forma de trames WiFi (802.11).
    - Els paquets poden ser dirigits a un altre dispositiu dins la mateixa xarxa o cap a Internet a través del router.
2. Mecanismes de Control
    - Es fan servir protocols com CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) per evitar col·lisions entre paquets de diferents dispositius.
    - En cas de pèrdua de paquets, es retransmeten fins que es reben correctament.
3. Seguretat i Cifratge
    - En xarxes segures, les dades es transmeten xifrades amb protocols com WPA2/WPA3.

- Això impedeix que dispositius no autoritzats puguen llegir la informació enviada.

4. Gestió del Roaming (Mobilitat)
    - Si el dispositiu es mou i troba un punt d'accés amb una millor connexió (dins la mateixa xarxa), pot canviar-hi automàticament sense perdre la connexió.

Per tant, el procés d'associació en una xarxa WiFi permet als dispositius establir una connexió amb un punt d'accés, mentre que la transmissió de dades assegura una comunicació eficient i segura. Per millorar la qualitat de la connexió, es poden utilitzar xarxes WiFi 6 (802.11ax), que ofereixen més velocitat, menys interferències i millor gestió de dispositius connectats.

2.2. Xifrat: WPA2 i WPA3

El xifrat WPA2 i WPA3 són mecanismes de seguretat utilitzats en xarxes WiFi per protegir la informació i evitar accessos no autoritzats. Aquests protocols es basen en diferents tècniques de xifratge per garantir que només els usuaris autoritzats puguen connectar-se i transmetre dades de manera segura.

2.2.1. WPA2 (Wi-Fi Protected Access 2)

Introduït el 2004 com a millora de WPA (Wi-Fi Protected Access). Utilitza el protocol de xifrat AES (Advanced Encryption Standard), que és molt segur i resistent a atacs.

Existeixen dues modalitats:

- WPA2-Personal (WPA2-PSK) → Utilitza una clau precompartida (PSK), normalment una contrasenya.

- WPA2-Enterprise (WPA2-EAP) → Usa servidors d'autenticació (com RADIUS) per a xarxes corporatives.

Vulnerabilitats:

- Pot ser atacat mitjançant atacs de força bruta si la contrasenya és fluixa.

- És vulnerable a l'atac KRACK (Key Reinstallation Attack), que pot interceptar la comunicació entre dispositius.

2.2.2. WPA3 (Wi-Fi Protected Access 3)

Introduït el 2018 per millorar la seguretat de WPA2. Protecció contra atacs de força bruta: Utilitza SAE (Simultaneous Authentication of Equals), que substitueix WPA2-PSK i fa que les contrasenyes siguen més segures.

- Xifrat individualitzat: Cada connexió entre un dispositiu i el router està xifrada individualment per millorar la privacitat.

- Més seguretat en xarxes obertes: WPA3 implementa Opportunistic Wireless Encryption (OWE) per xifrar les dades fins i tot en xarxes sense contrasenya.

- Millora en seguretat per IoT i dispositius sense pantalla, permetent connexió segura mitjançant QR o altres mètodes.

Diferències clau entre WPA2 i WPA3:

Característica	WPA2	WPA3
Xifratge	AES-CCMP	AES-GCMP (més segur)
Autenticació	PSK (Pre-Shared Key)	SAE (Protecció contra força bruta)
Protecció en xarxes obertes	No	Sí (OWE)
Vulnerabilitats conegudes	KRACK i força bruta	Millor protecció contra KRACK i atacs per diccionari
Compatibilitat amb dispositius antics	Sí	No sempre (pot requerir

2.3. WPA empresarial: RADIUS

El WPA Empresarial amb RADIUS és una solució de seguretat avançada per a xarxes WiFi que ofereix autenticació centralitzada mitjançant un servidor RADIUS (Remote Authentication Dial-In User Service). S'utilitza principalment en empreses, institucions educatives i organitzacions on es requereix un control més estricte de l'accés a la xarxa.

WPA Empresarial és una versió millorada del protocol WPA que permet una autenticació individual per a cada usuari en lloc d'una única contrasenya compartida.

- Més seguretat → Cada usuari té les seves pròpies credencials (usuari/contrasenya o certificat digital).
- Gestió centralitzada → L'administrador pot controlar l'accés a la xarxa i revocar permisos fàcilment.
- Autenticació dinàmica → Les claus de xifratge canvien contínuament, reduint el risc d'atacs.

Què és el servidor RADIUS?

El servidor RADIUS (Remote Authentication Dial-In User Service) és el sistema encarregat de verificar les credencials dels usuaris quan intenten connectar-se a la xarxa WiFi.

- Actua com a intermediari → El router WiFi (punt d'accés) envia les credencials al servidor RADIUS per a la seva verificació.
- Suporta diversos mètodes d'autenticació, com contrasenyes o certificats digitals.
- Permet gestió avançada d'usuaris, controlant qui pot connectar-se i quan.

Alguns exemples de servidors RADIUS són:

- FreeRADIUS (gratuït i de codi obert)
- Microsoft NPS (Network Policy Server)

- Cisco ISE
- Cloud RADIUS (Autenticació al núvol)

Els protocols d'autenticació compatibles amb RADIUS (EAP – Extensible Authentication Protocol):

- EAP-TLS → Utilitza certificats digitals per a màxima seguretat.
- PEAP (Protected EAP) → Usa contrasenya xifrada per evitar atacs d'intercepció.
- EAP-TTLS → Similar a PEAP, però amb més compatibilitat.

Els avantatges de WPA Empresarial amb RADIUS poden ser:

- Cada usuari té credencials pròpies → No es comparteix una sola contrasenya com en WPA2-PSK.
- Difícil d'atacar → Sense una base de dades robada, és molt difícil accedir il·legalment.
- Es pot integrar amb Active Directory (AD) per a autenticació d'usuaris d'empresa.
- Les claus de xifrat canvien constantment, reduint el risc de hackeig.

Diferència entre WPA-Personal (PSK) i WPA-Empresarial (RADIUS)

Característica	WPA-Personal (PSK)	WPA-Empresarial (RADIUS)
Autenticació	Una única contrasenya compartida	Cada usuari té el seu propi usuari/contrasenya
Seguretat	Menys segura (risc de filtració de la contrasenya)	Més segura (autenticació centralitzada i xifrat dinàmic)
Ús recomanat	Xarxes domèstiques o petites empreses	Empreses, universitats, organitzacions grans
Gestió d'usuaris	No permet control individual	Control total d'accés per usuari
Protecció contra atacs	Vulnerable a atacs de força bruta	Protecció contra atacs de força bruta i intercepció

3. VPN

Una VPN (Virtual Private Network) és una tecnologia que permet als empleats connectar-se de manera segura a la xarxa interna (intranet) de l'empresa des de qualsevol lloc amb accés a Internet. Això és especialment útil per a empreses amb teletreballadors o empleats en mobilitat, ja que garanteix seguretat, accessibilitat i privacitat en la comunicació de dades.

Què fa una VPN en una empresa? Una VPN permet que un usuari es connecte a la xarxa de l'empresa com si estigués físicament a l'oficina, encriptant el trànsit entre el seu dispositiu i la xarxa corporativa. Això té diversos avantatges:

- Accés segur a la intranet → Els empleats poden accedir a fitxers, servidors, aplicacions internes, correu electrònic corporatiu, bases de dades, etc.

- Xifratge de dades → La informació viatja de manera encriptada, protegint-la de hackers i atacs d'intercepció.

- Evita restriccions geogràfiques → Els empleats poden treballar des de qualsevol lloc, independentment de la seva ubicació.

- Protecció contra xarxes públiques → Si un empleat es connecta des d'una xarxa WiFi pública (cafeteria, aeroport, hotel), la VPN impedeix que tercers intercepten la seva connexió.

Com funciona una VPN corporativa? Passos per a la connexió d'un empleat a la intranet mitjançant VPN:

- L'empleat inicia sessió en la VPN des del seu dispositiu (ordinador, mòbil, tauleta) mitjançant una aplicació VPN o una configuració específica.

- Es crea un túnel xifrat entre l'usuari i el servidor VPN de l'empresa.

- El servidor VPN autentica l'usuari i li assigna una adreça IP interna de l'empresa.

- L'empleat pot accedir a la intranet, als servidors i als recursos compartits com si estigués físicament a l'oficina.

Depenent de la necessitat de l'empresa, es poden utilitzar diferents tipus de VPN:

- VPN d'accés remot. Permet als empleats connectar-se a la xarxa interna de l'empresa des de qualsevol lloc. Exemple: Un comercial accedeix als servidors de l'empresa mentre viatja.

- VPN de lloc a lloc (site-to-site VPN). Connecta dues o més oficines per a compartir la mateixa xarxa de manera segura. Exemple: Una empresa amb oficines a Barcelona i València pot unificar la seva xarxa interna.

- VPN basada en la núvol. Proveïdors com Azure VPN, AWS VPN o Google Cloud VPN ofereixen connexions segures a servidors al núvol. Exemple: Una empresa amb servidors en AWS permet als seus empleats accedir de manera segura.

Protocols VPN. Alguns dels més utilitzats són:

Protocol	Seguretat	Velocitat	Ús habitual
OpenVPN	Molt segura (AES-256)	Bona	Empreses i ús general
IPSec (IKEv2/IPSec, L2TP/IPSec)	Molt segura	Ràpida	VPN d'empresa i mòbils
WireGuard	Molt segura	Molt ràpida	VPN modernes i optimitzades
SSL VPN (TLS/SSL)	Seguretat web	Mitjana	Accés a VPN via navegador

Podem dir que una VPN corporativa és essencial per a empreses amb teletreballadors, oficines remotes o empleats en mobilitat. Permet accedir de manera segura i privada als recursos de la intranet des de qualsevol lloc, protegint la informació contra atacs externs i millorant la productivitat dels empleats.

4. Serveis de xarxa. Nmap i netstat

4.1. Nmap

Nmap (Network Mapper) és una eina de codi obert utilitzada per explorar, escanejar i analitzar xarxes. És àmpliament utilitzada per administradors de sistemes i experts en ciberseguretat per detectar dispositius, serveis actius i vulnerabilitats dins d'una xarxa.

Funciona en Windows, Linux i macOS. Pot escanejar xarxes locals i remotes. És utilitzat per pentesters i administradors per a detectar forats de seguretat.

Les principals funcions de Nmap en ciberseguretat són:

Funció	Explicació
Escaneig de ports	Identifica ports oberts en servidors i dispositius
Identificació de serveis (Service Fingerprinting)	Detecta quin programari s'està executant en cada port
Detecció de sistemes operatius (OS Fingerprinting)	Determina el tipus i versió del sistema operatiu d'un dispositiu
Exploració de xarxes	Descobreix dispositius i nodes en una xarxa
Auditoria de seguretat	Ajuda a detectar vulnerabilitats i possibles punts d'entrada per a atacants
Detecció de dispositius ocults	Permet trobar dispositius que no responen a pings convencionals

🔹 Exemple d'ús: Un administrador de xarxes pot utilitzar Nmap per comprovar quins ports té oberts un servidor i si algun d'ells és vulnerable a atacs.

Comandes bàsiques de Nmap:

Escaneig bàsic d'una IP o domini. Llista els ports oberts i serveis actius.

```
nmap 192.168.1.1
```

Escaneig de tota una xarxa. Mostra tots els dispositius connectats a la xarxa.

```
nmap 192.168.1.0/24
```

Detecció de sistema operatiu i serveis. Identifica el sistema operatiu i els serveis en execució.

```
nmap -O -sV 192.168.1.1
```

Escaneig de ports específics. Revisa si els ports 80 i 443 (web) estan oberts.

```
nmap -p 80,443 192.168.1.1
```

Escaneig agressiu (més informació i detecció d'OS). Escaneig profund que inclou sistema operatiu, serveis i versions.

```
nmap -A 192.168.1.1
```

Detecció de vulnerabilitats amb scripts de Nmap (NSE). Busca vulnerabilitats conegudes en el dispositiu escanejat.

```
nmap --script=vuln 192.168.1.1
```

Com pot ajudar Nmap a la seguretat?

- Identificació de ports oberts → Tanca ports innecessaris per reduir la superfície d'atac.
- Detecció de serveis vulnerables → Actualitza versions de programari per evitar exploits.
- Identificació de dispositius sospitosos → Descobreix dispositius desconeguts en la xarxa.
- Escaneig de vulnerabilitats → Utilitza scripts per detectar problemes de seguretat.
- Simulació d'atacs per pentesting → Comprova si la teva xarxa pot ser explotada per hackers.

Diferències entre Nmap i altres eines similars:

Eina	Funció principal	Avantatge respecte a Nmap
Nmap	Escaneig de xarxes i ports	Pot detectar sistemes operatius i vulnerabilitats

Eina	Funció principal	Avantatge respecte a Nmap
Wireshark	Anàlisi de trànsit de xarxa	Permet veure el contingut dels paquets en temps real
Nessus	Detecció de vulnerabilitats	Ofereix informes detallats i recomanacions de seguretat
Metasploit	Test de penetració	No només detecta vulnerabilitats, sinó que també les explota

4.2. netstat

Netstat (Network Statistics) és una eina de línia de comandes disponible en Windows, Linux i macOS que permet monitoritzar les connexions de xarxa d'un dispositiu. Es fa servir per identificar connexions actives, ports oberts, processos associats i tràfic de xarxa.

- Ajuda a detectar connexions sospitoses o malicioses
- Permet veure quins ports estan escoltant a la xarxa
- Identifica processos que utilitzen la xarxa i el seu estat

Comandes bàsiques i la seva aplicació en ciberseguretat:

- Veure totes les connexions actives i ports oberts. Mostra totes les connexions actives i els ports TCP/UDP que estan escoltant.
  `netstat -a`

- Veure processos associats a cada connexió. Permet veure el PID (Process ID) associat a cada connexió.
  `netstat -ano` (Windows)
  `netstat -p` (Linux/macOS)

- Investigació: Si detectes una connexió sospitosa, pots trobar quin programa l'està utilitzant amb:
  `tasklist | findstr <PID>` (Windows)
  `ps -aux | grep <PID>` (Linux)

- Detectar connexions establertes a servidors remots. Mostra les connexions remotes actives amb adreces IP en lloc de noms de domini.
  `netstat -n`

- Investigació: Si veus una connexió a una IP desconeguda, pots comprovar-la amb:
  `whois <IP>`

- Monitoritzar connexions en temps real. Actualitza la informació en temps real per veure si apareixen connexions sospitoses.
  `netstat -c` (Linux/macOS)

- Veure connexions actives d'un port específic (Ex: Port 80 – HTTP). Permet veure totes les connexions establertes amb un port concret.

```
netstat -an | findstr :80  (Windows)
netstat -an | grep :80  (Linux)
```

Identificar connexions sospitoses i atacs. Identificació d'un possible malware o troià

Si detectes una connexió a una IP estranya en ESTABLISHED, pot ser que un malware estiga enviant dades al teu servidor.

Protecció contra atacs amb Netstat. Evitar atacs de força bruta

Si veus moltes connexions en un mateix port (Ex: 22 per SSH), podria ser un atac de força bruta.

Tema 7: Seguritat activa: control de xarxes

1- Espiar la nostra xarxa

En la unitat anterior hem après a delimitar qui pot usar la nostra xarxa. Per això establim controls en els punts de connexió, tant cablejats com inalámbrics o en una VPN a través d'Internet. En aquesta unitat aprendrem a conèixer què està passant a la nostra xarxa, què estan fent els usuaris autoritzats. Es per això que necessitarem espiar-nos a nosaltres mateixos buscant garantir la disponibilitat de la xarxa (localitzarem enllaços saturats) i detectar atacs en curs.

Si ens centrem en la nostra pròpia xarxa i en els perills interns, el monitoratge del trànsit és clau per detectar i prevenir amenaces internes que podrien comprometre la seguretat. Aquests perills poden provenir tant de treballadors malintencionats com d'errors humans o dispositius compromesos.

1.1. Per què és útil el monitoratge del trànsit en la nostra xarxa?

1. Detecció d'activitats sospitoses dels usuaris
    - Identificació d'accessos no autoritzats a recursos sensibles.
    - Monitoratge de moviments sospitosos de dades (per exemple, una gran quantitat d'arxius transferits fora d'hores de feina).
    - Control de l'ús d'eines de compartició de fitxers o d'emmagatzematge al núvol (com Google Drive, Dropbox).

2. Prevenció d'atacs interns i negligències
    - Amenaces internes: Un empleat descontent pot intentar robar o esborrar informació.
    - Errors humans: Un usuari pot accedir a un enllaç maliciós o instal·lar sense voler un programa amb malware.
    - Ús indegut de recursos: Monitorar l'ús excessiu de la xarxa per part d'usuaris no autoritzats o per activitats no relacionades amb la feina (streaming, descàrregues il·legals).

3. Identificació de dispositius compromesos
    - Detecció de trànsit anòmal generat per malware que podria haver infectat un ordinador dins de la xarxa.
    - Identificació de comunicacions amb servidors sospitosos, possiblement relacionats amb atacs com ransomware o troians.

4. Control de privilegis i moviments laterals
    - Monitoratge dels privilegis dels usuaris per detectar si algú intenta obtenir permisos elevats de forma fraudulenta.
    - Identificació de moviments laterals dins la xarxa, indicant que un atacant intern (o un hacker amb accés) està intentant accedir a altres sistemes.

El monitoratge del trànsit intern permet protegir la nostra xarxa no només de perills externs, sinó també d'amenaces internes. Ens ajuda a detectar comportaments sospitosos, evitar pérdues de dades, i identificar dispositius o usuaris compromesos abans que causin danys greus.

1.2. Eines de monitoratge

Eina	Funció principal	Avantatges	Inconvenients	Cas d'ús ideal
Suricata (NGIPS)	IDS/IPS de nova generació per detectar i prevenir atacs en temps real.	✅ **Més ràpid que Snort** gràcies a **suport multi-thread**. ✅ Suport per a **protocols diversos** (HTTP, DNS, etc.).	× Requereix **bons recursos de hardware** per funcionament òptim. × Configuració més complexa.	Anàlisi de trànsit en temps real i detecció avançada d'amenaces.
Zeek (Bro)	Monitoratge i anàlisi de trànsit de xarxa amb focus en metadades.	✅ **Enregistra metadades detallades**, útil per a **anàlisi forense**. ✅ Detecta **comportaments sospitosos**.	× No és un **IDS/IPS complet** (no bloqueja trànsit). × Requereix més configuració per integració amb altres eines.	Monitorització passiva i anàlisi forense de trànsit de xarxa.
SIEM	Recopilació, correlació i anàlisi d'alertes de seguretat.	✅ **Correlació d'alertes de múltiples fonts** (xarxa, endpoints, sistemes). ✅ Automatització de detecció i resposta.	× **Costós** i pot ser **complex de configurar**. × Requereix una gran infraestructura.	Gestió centralitzada de seguretat i resposta a incidents.
NDR	Monitoratge de xarxa amb IA i Machine Learning per detectar amenaçes.	✅ Detecta **amenaces desconegudes** mitjançant **anàlisi de comportament**. ✅ Visibilitat completa del trànsit en temps real.	× Pot ser **costós** i generar **falsos positius** si no està ben configurat.	Detectar atacs desconeguts i anòmales mitjançant Machine Learning.
tcpdump	Captura i visualització de paquets de xarxa en línia de comandes.	✅ Eina **lleugera** i fàcil d'usar per a **captura ràpida de trànsit**. ✅ Permet **capturar tot el trànsit** en xarxa.	× **No analitza paquets** (només captura). × No proporciona una vista gràfica.	Anàlisi ràpida de trànsit i captura de pacs en temps real.
Wireshark	Anàlisi profunda de trànsit de xarxa amb	✅ **Anàlisi detallada de paquets**, facilita la inspecció de	× Pot ser **molt lent** per xarxes grans.	Anàlisi en profunditat de paquets per

Eina	Funció principal	Avantatges	Inconvenients	Cas d'ús ideal
		trànsit. ✅ **Visualització gràfica** fàcil d'entendre.	× Requereix **coneixements tècnics** per interpretar dades.	detectar vulnerabilitats i atacs.
Port Mirroring	Duplica trànsit d'un switch per a monitorització passiva.	✅ Permet **capturar tot el trànsit** sense afectar el rendiment de la xarxa. ✅ **Ideal per eines d'anàlisi de trànsit** (Wireshark, Zeek).	× Pot afectar el **rendiment** si hi ha una gran quantitat de trànsit. × No detecta ni bloqueja atacs per si mateix.	Monitorització passiva del trànsit per a anàlisi posterior.
Snort	IDS/IPS basat en signatures per detectar atacs.	✅ **Gran comunitat** i **gran base de signatures** d'atacs coneguts. ✅ Configurable i gratuït.	× No és tan ràpid ni escalable com **Suricata** en xarxes grans. × Configuració més tècnica.	Detecció d'intrusions i atacs coneguts mitjançant signatures.

En forma de resum podem dir:

1. Suricata i Snort són IDS/IPS molt útils per detectar i prevenir atacs en temps real. Suricata és més ràpid i amb millor rendiment gràcies al suport multi-thread.
2. Zeek (Bro) és una eina més passiva que s'utilitza per monitoritzar el trànsit de xarxa i obtenir metadades detallades per a investigacions forenses.
3. SIEM és una solució més centralitzada per gestionar i correlacionar alertes de seguretat de diferents fonts a tota la infraestructura.
4. NDR utilitza Machine Learning i IA per detectar amenaces desconegudes i comportaments anòmals en el trànsit de xarxa en temps real.
5. tcpdump i Wireshark són eines d'anàlisi de trànsit, amb tcpdump per a captures ràpides i Wireshark per a anàlisis detallades.
6. Port Mirroring és útil per duplicar trànsit de xarxa per a una anàlisi passiva sense afectar el flux de dades.

Combinant aquestes eines, pots aconseguir una protecció integral per a la teva xarxa empresarial!

2. Firewall

Un firewall és un sistema de seguretat de xarxa que actua com a barrera entre una xarxa confiable (com la xarxa interna d'una empresa) i una xarxa no confiable (com Internet).

La seua funció principal és monitoritzar, filtrar i controlar el trànsit d'entrada i d'eixida segons unes regles de seguretat predefinides, bloquejant connexions sospitoses o no autoritzades.

Els firewalls poden ser de maquinari, programari o híbrids, i poden utilitzar diferents tècniques de protecció, com filtrat de paquets, inspecció d'estat, inspecció profunda de

paquets (DPI) i detecció d'amenaces avançades. Són essencials per prevenir atacs contra la nostra seguretat, intrusions i trànsit maliciós dins d'una xarxa empresarial o personal.

2.1. Què fa

Un firewall actua com un controlador de seguretat que monitoritza, filtra i regula el trànsit de xarxa segons unes regles predefinides. El seu objectiu és permetre trànsit legítim i bloquejar connexions no autoritzades o sospitoses, protegint així la xarxa contra amenaces com hackers, malware, atacs DDoS o accessos no autoritzats.

Com actua?

1. Monitorització del trànsit
   Escaneja tot el trànsit de dades que entra i surt de la xarxa.
2. Filtrat de paquets
   Examina cada paquet de dades i decideix si permetre'l o bloquejar-lo segons regles definides (adreces IP, ports, protocols, etc.).
3. Inspecció d'estat *(Stateful Inspection)*
   Analitza no només cada paquet individualment, sinó també el context de la connexió per identificar activitats sospitoses.
4. Inspecció profunda de paquets (DPI)
   Examina el contingut dels paquets per detectar malware, virus o trànsit sospitós dins de protocols aparentment segurs.
5. Bloqueig d'amenaces conegudes
   Compara el trànsit amb bases de dades d'amenaces (IPs malicioses, patrons d'atac, signatures de malware, etc.) i bloqueja possibles atacs.
6. Regles personalitzades
   Permet establir polítiques específiques per a diferents tipus de trànsit, com ara bloquejar certes pàgines web o restringir accés a determinats serveis.
7. Registre i alertes
   Guarda registres del trànsit per a auditories i detecció d'anomalies, avisant en cas d'activitat sospitosa.

Podem distingir, pel seu funcionament:

- Firewall de xarxa → Protegeix xarxes senceres (p. ex. empreses, centres de dades).
- Firewall personal → Protegeix dispositius individuals (p. ex. ordinadors, mòbils).
- Firewall basat en host (HIDS) → Instal·lat directament en un servidor o PC.
- Firewall basat en núvol → Implementat en serveis en línia (p. ex. AWS Firewall).

Exemples de firewalls coneguts: IPTables, pfSense, FortiGate, Palo Alto, Cisco ASA, Windows Defender Firewall.

Un bon firewall és una peça clau per a protegir la teva xarxa d'amenaces cibernètiques!

2.2. On situar-lo

La ubicació del firewall en una xarxa és clau per a protegir els sistemes i evitar atacs. La seva posició dependrà de la infraestructura de la xarxa i el nivell de seguretat necessari.

A continuació, es mostren les ubicacions més habituals:

1- Entre Internet i la xarxa interna (Perímetre de xarxa). És la posició més bàsica i essencial

- Filtra tot el trànsit que entra i surt de la xarxa local.
- Protegeix els dispositius interns d'amenaces externes.

Esquema: Internet -> Firewall Perimetral -> Xarxa Interna

2- Entre la xarxa interna i la zona DMZ (Zona Desmilitaritzada). Protecció avançada per a servidors públics

- Es col·loca entre la xarxa interna i els servidors accessibles des d'Internet (web, correu, FTP, VPN).
- Evita que un atac a la DMZ comprometa tota la xarxa interna.
- Útil per empreses amb serveis públics en línia.

Esquema:

Internet -> Firewall Extern -> DMZ (Servidors Públics) -> Firewall Intern -> Xarxa Interna

3- Entre segments interns de la xarxa (Segmentació de xarxa). Protecció interna contra amenaces laterals

- Es col·loca entre diferents subxarxes internes (p. ex. departaments d'una empresa).
- Limita l'accés entre usuaris, servidors i dispositius crítics.
- Evita la propagació d'atacs com ransomware o moviments laterals d'un atacant.

4- En cada dispositiu (Firewall basat en host – HIDS). Protecció individual per ordinadors i servidors

- Actua com un firewall de programari en cada PC o servidor.
- Bloqueja aplicacions sospitoses o connexions no autoritzades.

Exemple: Windows Defender Firewall, UFW en Linux, pfSense en servidors.

Útil per: Protegir portàtils i ordinadors personals o protegir servidors crítics d'amenaces internes.

5- Combinació de Firewalls per una Protecció Completa

La millor estratègia és usar múltiples firewalls en diferents punts de la xarxa per tenir un model de seguretat en capes (Defensa en profunditat).

- Firewall Perimetral per protegir contra Internet.
- Firewall Intern per evitar moviments laterals dins la xarxa.
- Firewall d'Host per protegir cada dispositiu.
- Firewall de DMZ per serveis públics.

Un bon disseny de xarxa amb firewalls adequadament situats millora molt la seguretat!

2.3. Firewall en Linux. Iptables

IPTables és una eina de filtratge de paquets a nivell de xarxa que permet configurar i controlar les connexions de xarxa en sistemes basats en Linux. A través de regles de filtratge definides pel administrador, iptables permet gestionar el trànsit de xarxa i protegir els dispositius contra connexions no autoritzades o malicioses.
Funció principal:

IPTables actua com un firewall de maquinari i filtra el trànsit de xarxa d'entrada i eixida de la màquina o servidor en què està instal·lat, segons les regles establertes. Aquestes regles poden ser configurades per filtrar trànsit a través de adressen IP, ports, protocols, i altres criteris.

Com funciona IPTables?

IPTables treballa amb taules i cadenes. Cada taula conté diverses cadenes que permeten aplicar regles per al trànsit de xarxa.

Avantatges d'IPTables:

- Control complet sobre el trànsit de xarxa.
- Gratuït i de codi obert (fins i tot per a xarxes empresarials).
- Configuració flexible i detallada de regles.
- Potència i escalabilitat, ideal per a xicotetes i grans xarxes.
- Integració amb altres eines (com fail2ban, per bloquejar IPs després d'intents d'intrusió).

Desavantatges d'IPTables:

- Pot ser complicat de configurar per a usuaris poc experimentats.
- No inclou funcionalitats avançades (com inspecció profunda de paquets) que poden ser requerides en xarxes de gran escala.
- Pot generar configuracions lentes si no s'optimitzen bé les regles en xarxes amb molt trànsit.

IPTables és una eina poderosa per gestionar la seguretat de xarxes Linux, permetent un control detallat sobre les connexions. Tot i ser flexible i potent, requereix coneixements tècnics per a la seva correcta configuració i manteniment. Ideal per a administradors de xarxa que volen personalitzar i gestionar l'accés a la xarxa en sistemes Linux.

2.4. Firewall al Windows Server 2025

En Windows Server 2025, el sistema utilitza un Firewall de Windows Defender per proporcionar protecció a la xarxa i controlar el trànsit entrant i sortint. Aquest firewall és una solució integrada que ve activada per defecte en la majoria de les instal·lacions de Windows Server.

Funcions del Firewall de Windows Defender:

- Filtrat de trànsit. El firewall controla el trànsit de dades a través de la xarxa, permetent o bloquejant connexions segons les regles configurades per l'administrador.
- Regles personalitzades. Permet als administradors crear regles per definir el trànsit permès o bloquejat basat en protocols, ports, direccions IP i aplicacions.
- Inspecció de trànsit bidireccional. Realitza una inspecció del trànsit tant entrant com sortint, evitant que programes maliciosos o no autoritzats puguin comunicar-se amb la xarxa.
- Gestió centralitzada. Amb eines com Windows Admin Center o PowerShell, els administradors poden gestionar el firewall de forma centralitzada, aplicant polítiques a nivell de xarxa o per a grups de servidors.
- Protecció contra amenaces conegudes. Windows Defender Firewall està dissenyat per detectar i bloquejar amenaces comunes, com malware, atacs de denegació de servei (DDoS) i intrusions internes.
- Funcionalitat d'alertes i registre. El sistema permet generar registres d'activitat i alertes de seguretat per ajudar a detectar intents d'intrusió o trànsit sospitós.

El Firewall de Windows Defender en Windows Server 2025 és una solució potent i fàcil de gestionar per controlar el trànsit de xarxa i garantir la seguretat de les xarxes internes i externes, amb novetats que el fan encara més eficaç en entorns híbrids i en el núvol.

3. Proxy

Un proxy és un servidor intermediari entre un client (per exemple, un navegador web) i el servidor de destinació (com un lloc web o un servei en línia). Quan un usuari fa una sol·licitud (com accedir a un lloc web), el proxy rep aquesta sol·licitud, la processa i la reenvia al servidor de destinació en nom de l'usuari. Quan el servidor de destinació respon, el proxy torna la resposta al client.

Tipus de Proxy:

- Proxy web: Filtra i redirigeix el trànsit HTTP/HTTPS.
- Proxy revers (Reverse Proxy): S'utilitza per gestionar les sol·licituds entrants a un servidor intern, generalment per equilibrar càrrega o augmentar la seguretat.
- Proxy de cadenes: Utilitza múltiples proxies en seqüència per millorar la seguretat i l'anonimat.

Com aporta un Proxy a la seguretat de la xarxa?

Els proxies ofereixen diversos beneficis per millorar la seguretat i el control en una xarxa. Aquests són alguns dels avantatges clau:

1. Filtrat de trànsit i bloqueig d'accés a contingut perillós:

    - Els proxies poden filtrar sol·licituds web per bloquejar llocs web maliciosos o no desitjats (per exemple, pàgines de phishing o amb contingut perillós).
    - Permeten establir regles per controlar els tipus de trànsit web permès a la xarxa interna.

2. Anonimat i ocultació d'IP:

    - El proxy amaga l'adreça IP real de l'usuari, ja que totes les connexions surten a través del proxy. Això millora l'anonimat i fa més difícil la traçabilitat de la connexió.
    - En el cas de proxies reversos, es poden amagar les adreces IP de servidors interns de l'exterior, dificultant els atacs directes.

3. Control i monitoratge del trànsit:

    - El proxy permet registrar i monitoritzar tot el trànsit de la xarxa, detectant activitats sospitoses i analitzant els patrons de connexió per detectar amenaces com drets d'accés no autoritzats o atacs DDoS.
    - Genera informes detallats per ajudar els administradors a controlar el trànsit i establir polítiques de seguretat més estrictes.

4. Accés controlat i autenticació:

    - Un proxy pot requerir autenticació abans d'accedir a la xarxa, evitant que usuaris no autoritzats facin connexions a llocs web o serveis.
    - Pot integrar-se amb solucions d'autenticació corporatives per controlar qui accedeix a la xarxa i als recursos d'Internet.

5. Acceleració de trànsit i emmagatzematge en caché:

    - El proxy pot emmagatzemar en caché el contingut web sol·licitat sovint, millorant la velocitat de resposta i reduint la càrrega dels servidors web.
    - A més, aquesta tècnica pot ajudar a evitar que informació sensible es torni a descarregar constantment, millorant la seguretat de dades.

6. Equilibrat de càrrega i protecció contra atacs DDoS:

    - Un proxy revers pot distribuir el trànsit entre diversos servidors, equilibrant la càrrega i millorant l'escalabilitat de l'arquitectura de la xarxa.

- Pot actuar com una barrera de seguretat davant d'atacs DDoS, gestionant i filtrant les sol·licituds entrants abans que arribin als servidors interns.

7. Desxifrat i inspecció de trànsit HTTPS:

- Els proxies poden desxifrar trànsit HTTPS per inspecionar-lo a la recerca de malware o altres amenaces abans de re-enviar-lo a la xarxa interna.
- Això permet detectar amenaces que podrien passar desapercebudes si el trànsit fos només HTTPS xifrat.

Exemples de Proxies utilitzats en seguretat de xarxa:

Squid Proxy: Utilitzat per gestionar el trànsit web i el filtrat de contingut a nivell corporatiu.

Nginx o HAProxy: Proxies reversos que proporcionen equilibrat de càrrega i milloren la seguretat dels servidors web.

Blue Coat ProxySG: Un proxy empresarial utilitzat per a la seguretat de trànsit web i la prevenció de pèrdua de dades (DLP).

Privoxy: Un proxy orientat a la privadesa, sovint utilitzat per ocultar la identitat a la xarxa.

Podem dir que un proxy actua com un intermediari per gestionar, controlar i protegir el trànsit entre clients i servidors, augmentar la seguretat, i mantenir l'anonimat. Aporta una gran protecció contra amenaces externes, filtra contingut perillós i ajuda a controlar l'accés a serveis. Amb les funcions de monitoratge i anàlisi de trànsit, és una eina útil per a xarxes corporatives que volen millorar la seguretat i optimitzar el rendiment de la seva infraestructura de xarxa.

3.1. Proxy Squid: configuració i monitorització

Cas pràctic que vorem en video.
