CFGM-SMX

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

índex

Tema1: Conceptes sobre seguretat informàtica
Tema 2: Criptografia
Tema 3: Seguretat passiva: equips
Tema 4: Seguretat passiva: emmagatzenament
Tema 5: Seguretat activa: sistema operatiu i aplicacions
Tema 6: Seguretat activa: accés a xarxes
Tema 7: Seguretat activa: control de xarxes

Tema 1: Conceptes sobre seguretat informàtica

1. *Per què cal protegir?*
2. *Què protegir?*
3. *Definicions*
4. *Tipus d'atacs*
5. *Bones pràctiques*
6. *Legislació*

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?*
2. *Criptografia*
3. *Criptografia simètrica*
4. *Criptografia asimètrica*
5. *Signatura digital i certificat digital*
6. *PKI*

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*
2. *Centre de suport en seguretat informàtica*
3. *SAI*
4. *Node Tirant*

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.

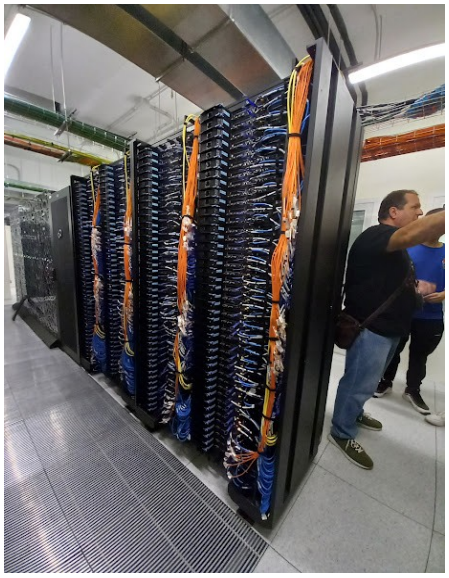
4. Node Tirant

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. En breu es substituirà per la versió 4 del superordinador Tirant.



Tema 4: Seguretat passiva: emmagatzenament

1. Estratègies d'emmagatzematge
- *1.1. Rendiment i redundància. RAID*
- *1.2. Emmagatzematge en xarxa: NAS i SAN. Clústers*
- *1.3. Emmagatzematge en el núvol*

2. Backsups de dades
- *2.1. Tipus de dispositius locals i remots. Robot de cintes*
- *2.2. Tipus de còpies*

3. Imatge del sistema
- *3.1. Creació i recuperació. LiveCD*
- *3.2. Congelació*
- *3.3. Registre de Windows i punts de restauració*
- *3.4. Eines de revisió mèdica de discos*

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. De fet, les actualitzacions automàtiques de Windows sempre creen primer un punt de restauració. Si el canvi aplicat ha sigut un desastre, podem tornar a la situació anterior utilitzant el punt de restauració. És una operació irreversible: una vegada llançat, no podem interrompre-ho i el sistema quedarà amb aquesta configuració.

Si el canvi solament afecta a la configuració, aleshores ens podem limitar a protegir el registre. El registre és una base de dades interna on el sistema operatiu i les aplicacions anoten informació de configuració. Si pateix algun dany o es manipula indegudament, les aplicacions afectades poden deixar de funcionar i necessitar ser instal·lades de nou. Per aquest motiu, abans de la instal·lació d'un pegat complex o si necessitem modificar manualment algun valor del registre, convé fer una còpia del mateix. Per a açò executarem l'aplicació regedit. En la finestra que apareix anem a Arxiu > Exportar.

Podemos triar salvar una clau, una branca o tot el registre (si no sabem què va a canviar, hem de salvar tot). Ens demanarà el nom que li donarem al fitxer, que tindrà l'extensió .reg

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
- *1.1. La caixa de l'ordinador*
- *1.2. La BIOS de l'ordinador*
- *1.3. El boot manager*
- *1.4. Xifrat de particions*

2. Autenticació en el sistema operatiu
- *2.1. Usuari/password*
- *2.2. Targetes*
- *2.3. Biometria*
- *2.4. Elevació de privilegis*

3. Quotes
4. Actualitzacions i pegats
5. Antivirus
6. Monitoratge
7. Aplicacions web
8. Cloud computing.
8.1. IaaS: Infrastructure as a Service
8.2. SaaS: Programari as a Service

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
- *1.1. VLAN*
- *1.2. Autenticació en el port. MAC i 802.1X*

2. Xarxes sense fils
- *2.1. Associació i transmissió*
- *2.2. Xifrat: WEP, WPA, WPA2*
- *2.3. WPA empresarial: RADIUS*

3. VPN
4. Serveis de xarxa. Nmap i netstat

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:

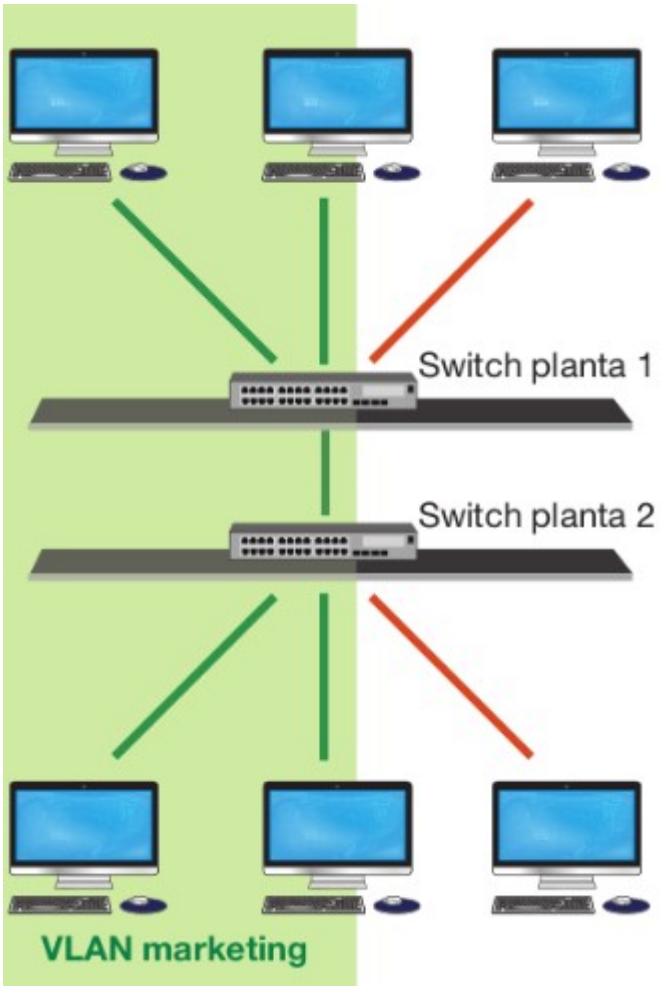
- Cal protegir el switch físicament: tancar-ho en un armari/rack amb clau dins d'una sala amb control d'accés. Així evitem no només el robatori, sinó que algú accedisca al botó de réset i el configure a la seua manera.
- Cal protegir el switch lògicament: posar usuari/contrasenya per a accedir a la seua 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

Els grups de ports que fem en un switch gestionable per a aïllar un conjunt de màquines constitueixen una VLAN (LAN virtual). Se l'anomena virtual perquè sembla que estan en una LAN pròpia, que la xarxa està muntada per a ells sols. Utilitzar VLAN millora el rendiment i la seguretat, perquè aquestes màquines només parlen entre elles i ningú estrany les escolta. Al mateix temps, si ocorre un problema en una VLAN (un atac, un problema d'un servidor DHCP descontrolat), les altres VLAN no es veuen afectades. Però un excés de tràfic en una VLAN sí que afectaria a tots perquè, al cap i a la fi, comparteixen el switch.

Una VLAN basada en grups de ports no queda limitada a un switch. 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 màrqueting té part de la seua personal en la primera planta i part en la segona, cal deixar un port en cada switch per a interconnectar-los.



En la figura tenim dos equips en cada planta, per la qual cosa ocuparien tres ports en cada switch. Switch planta 1 Switch planta 2 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, correu, 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 reservar-li un port en cadascuna.

Una solució alternativa serà utilitzar una VLAN etiquetada (tag). La configuració més simple de VLAN etiquetada manté els grups de ports, però el que els connecta amb el router té una configuració distinta: el switch afegirà una etiqueta (un número) als paquets de dades (trames) que ixen per aquest port. Aquests paquets ja poden viatjar pel mateix cable que els paquets d'altres VLAN sense interferncies entre ells.

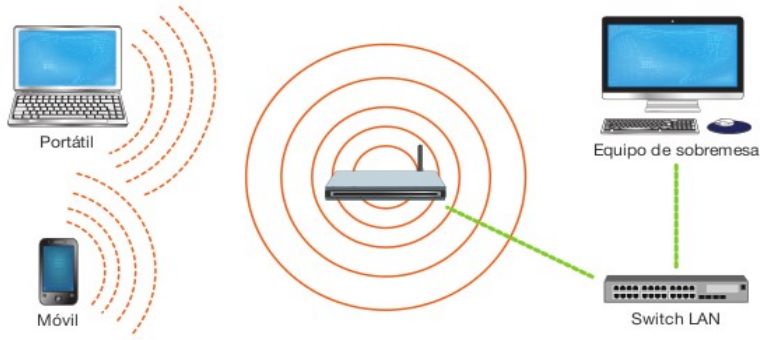
1.2. Autenticació en el port. MAC i 802.1X

Hem protegit l'accés al switch i repartit les màquines de l'empresa en diverses VLAN, interconnectades per routers. Però qualsevol pot ficar-se en un despatx, desconnectar el cable RJ45 de l'ordinador de l'empleat, connectar-ho al seu portàtil i ja estaria en aquesta VLAN. Com seguix sent un switch, no podrà escoltar el tràfic normal dels altres ordinadors de la VLAN, però sí llançar atacs contra ells. Per a evitar-ho, els switch permeten establir autenticació en el port: només podrà connectar aquell que la seua MAC estiga dins d'una llista definida en el propi switch, o, atès que les MAC són fàcilment falsificables (les targetes emeten els paquets que genera el programari de xarxa del sistema operatiu), el que siga autentificat mitjançant RADIUS en l'estàndard 802.1X.

2. Xarxes sense fils

La por al fet que les comunicacions siguen escoltades per tercers no autoritzats han desaparegut en les xarxes cablejades, però estan plenament justificats en xarxes sense fils o WLAN (Wireless LAN), perquè de nou el mitjà de transmissió (l'aire) és compartit per tots els equips i qualsevol targeta en nodalitat promíscua put perfectament escoltar el que no li toca.

Encara que es poden fer xarxes sense fils entre equips (xarxes ad hoc), el més habitual són les xarxes de tipus infraestructura: un equip anomenat access point (AP, punt d'accés) fa de switch, de manera que els altres ordinadors es connecten a ell, li envien els seus paquets i ell decideix com fer-los arribar a la destinació, que pot ser enviar-los de nou a l'aire o traure'ls pel cable que el connecta amb la resta de la xarxa.



Eixir pel cable és la configuració més habitual en les empreses, on la WLAN es considera una extensió de la xarxa cablejada.

Com passava amb el switch en les xarxes cablejades, hem de:

- Protegir l'access point físicament. La protecció física és més complicada que en el cas del switch, perquè l'AP ha d'estar prop dels usuaris perquè puguen captar el senyal sense fil, mentre que per a connectar la presa de xarxa de la taula amb el switch podem utilitzar cable de diverses desenes de metres.
- Protegir el access point lògicament (usuari/contrasenya).
- Controlar quins clients poden connectar-se a ell (autenticació).
- Podem separar dos grups d'usuaris, fent que el mateix AP emeta diverses SSID diferents, amb autenticacions diferents. Aquestes diferents SSID solen tenir associada una VLAN etiquetada.
- Sobretot, cal encriptar la transmissió entre l'ordinador i l'Ap. Així, encara que algú capture les nostres comunicacions, no podrà traure res en clar.

2.1. Associació i transmissió

Per a que un ordinador puga treballar en una xarxa cablejada normal (sense autenticació en el port), n'hi ha prou amb endollar un cable Ethernet entre la targeta de xarxa de l'equip i la presa de xarxa en la paret, per exemple. En wifi s'estableixen dues fases: associació i transmissió. Durant l'associació l'usuari tria la SSID a la qual es vol connectar i aleshores la seua targeta sense fil contacta amb l'AP que ofereix aquesta SSID. Negocien diverses característiques de la comunicació (protocol b/g/n, velocitat, etc.), però sobretot l'AP pot sol·licitar algun tipus d'autenticació per a decidir-hi. Generalment és una clau alfanumèrica que es registra en la configuració de l'AP i que l'usuari ha d'introduir per a poder treballar amb ell.

L'autenticació és més habitual en xarxes sense fils que en xarxes cablejades perquè, per a poder arribar a connectar un cable, primer hem d'entrar en l'empresa, i se suposa que no deixen passar a qualsevol. En canvi, podem captar el senyal inalàmbrica des d'un cotxe aparcat al costat de la façana, asseguts en un bar en la planta baixa, etc. Encara que

l'empresa intente evitar-ho limitant la potència d'emissió de les seues AP, és impossible que no isca res.

Els AP admeten diversos tipus d'autenticació:

- Oberta: no hi ha autenticació, qualsevol equip pot associar-se amb l'Ap.
- Compartida: la mateixa clau que utilitzem per a xifrar la usem per a autenticar.
- Accés segur: usem diferents claus per a autenticar i xifrar. L'usuari sol necesita saber una, la clau d'autenticació: la clau de xifrat es genera automáticament durant l'associació.
- Autenticació per MAC: l'AP manté una llista de MAC autoritzades i solament elles poden associar-se.

Una vegada associats a l'AP, podem començar la fase de transmissió, durant la qual establirem converses amb l'Ap. Si volem evitar que un tercer capture els paquets intercanviats i intente conèixer el que transmetem, el client i l'AP hauran d'activar el xifrat de cada paquet. El tipus de xifrat (algorisme, longitud de la clau, etc.) es negocia durant l'associació.

Per tant, l'AP admet diverses combinacions:

- Autenticació oberta i sense xifrat: s'utilitza en llocs públics (biblioteques, cafeteries, etc.). La intenció és no molestar a l'usuari introduint claus; a més, si les posem, caldria donar a conèixer la clau mitjançant un cartell a l'interior de l'establiment, per la qual cosa la tindrien tots, usuaris i atacants. En aquests casos, el sistema operatiu ens avisa que anem a connectar-nos a una xarxa sense seguretat.
- Autenticació oberta i transmissió xifrada: és l'esquema habitual de les primeres xarxes wifi.

- Autenticació segura i transmissió xifrada: és la millor solució perquè utilitza una clau diferent per a cada cosa. La més coneguda és WPA, com veurem en el següent apartat d'aquesta unitat.

2.2. Xifrat: WEP, WPA, WPA2

La necessitat d'encriptar les comunicacions sense fils va aparèixer des del primer moment. Calia donar als usuaris la garantia de que la seua informació viatjava segura. El primer estàndard es va dir WEP (Wireline Equivalent Privacy), intentant compensar les dues realitats:

- En xarxes cablejades és difícil l'accés al cable, però si algú ho aconsegueix, pot capturar qualsevol comunicació que passe per allí.

- En xarxes sense fils qualsevol pot capturar les comunicacions, però, com que van xifrades, no li servirà de res.

No obstant açò, en poc temps es van trobar febleses a l'algorisme de xifrat utilitzat en WEP. Capturant cert nombre de trames, en poc temps (cada vegada menys, amb l'augment de la capacitat de procés dels ordinadors personals) qualsevol podia obtenir la clau WEP.

Les autoritats d'estandardització van començar a treballar en un nou estàndard: WPA (Wi-Fi Protected Access) que introdueix moltes millores:

- Nous algorismes més segurs (TKIP, AES), tant per l'algorisme en si com per l'augment de longitud de les claus, la qual cosa dificulta els atacs.

- Rotació automàtica de claus. Cada cert temps (diversos minuts) l'AP i el client negocien una nova clau. Per tant, si algun atacant aconseguira encertar amb la clau d'una comunicació, solament li serviria per a desxifrar la informació intercanviada durant aquest interval de temps, però no l'anterior ni el següent.

- Per primera vegada es distingeix entre els àmbits personal i empresarial. En l'àmbit personal és suficient amb l'esquema habitual d'una única clau que coneixen tots (WPA l'anomena PSK [Pre-Shared Key]). En l'àmbit empresarial no té sentit, perque si una persona abandona l'empresa, caldria canviar la clau i comunicar-ho de nou a tots els empleats. Per a resoldre-ho, WPA empresarial introdueix un servidor RADIUS on poder emmagatzemar un usuari i una clau per a cada empleat.

En general convé tenir totes les xarxes en WPA; però en cada cas caldrà éstudiar si l'AP ho té i si tots els possibles equips que volem connectar-li el permeten, tant en maquinari (el xifrat es fa en la targeta) com en programari (el sistema operatiu i el driver han de contemplar-ho). Pot ocórrer que equips vells solament admeten WEP, en aquest cas cal decidir entre actualitzar-los o baixar la seguretat de tots els altres.

2.3. WPA empresarial: RADIUS

Com acabem de destacar, per a les necessitats de seguretat d'una empresa no és sufi cient amb la solució de clau única compartida per tots. A més de l'eixida d'empleats, ja sabem que és una bona pràctica canviar les claus regularment (no sabem quant temps porten intentant conèixer-la), es pot extraviar el portàtil o el mòbil d'un empleat i qui ho trobe pot traure les claus emmagatzemades en el dispositiu, etc.

L'esquema de funcionament de WPA empresarial és el següent:

- Dins de la LAN de l'empresa hi ha un ordinador que executa un programari servidor RADIUS. En aquest servidor hi ha una base de dades d'usuaris i contrasenyes, i el servidor admet preguntes sobre ells.
- Els AP de l'empresa tenen connexió amb aquest ordinador.
- Els AP executen un programari client RADIUS. Aquest programari és capaç de formular les preguntes i analitzar les respostes.
- El servidor RADIUS té la llista de les adreces IP dels AP que li poden preguntar. A més d'estar en la llista, l'AP necessita que li configurem una contrasenya definida en el servidor (una adreça IP és fàcilment falsificable).
- Quan un client vol associar-se a un AP, li sol·licita usuari i contrasenya. Però no les comprova ell mateix, sinó que formula la pregunta al servidor RADIUS utilitzant la contrasenya configurada per a aquest servidor. Depenent de la resposta, l'AP accepta l'associació o no.

A més de millorar la seguretat, perquè cada usuari té la seua contrasenya (amb la seua caducitat) i en qualsevol moment podem afegir o eliminar un usuari, amb WPA empresarial podem portar un registre de qui entra a la xarxa en cada moment.

La rotació de claus que va introduir WPA va ser un pas important per a dissuadir als hackers d'intentar obtenir la clau mitjançant l'anàlisi de la captura de trames de tràfic d'equips ja connectats a l'Ap. Aleshores els hackers van concentrar el seu treball en la clau PSK de la fase d'associació. Van utilitzar la força bruta de dues formes:

- Provant contrasenyes una després d'una altra. Les contrasenyes serien totes les combinacions possibles de lletres i nombres, o una selecció mitjançant un diccionari. Per desgràcia, els AP no solen tenir un control del nombre d'intents fallits, com sí ocorre en altres sistemes d'autenticació que hem vist en aquest llibre (login de Windows, targetes SIM).

- Si aconseguiren capturar les trames d'inici de connexió d'un client, podrien aplicar un atac de diccionari sobre la informació d'aquestes trames. Si no volem esperar al fet que aparega un client nou, podem forçar la desconnexió d'algun.

3. VPN

Les empreses tenen xarxes LAN i WLAN per a les seues oficines, però també solen necessitar que els empleats puguen entrar a aquesta mateixa xarxa des de qualsevol altre lloc d'Internet (la seua casa, la seu d'una altra empresa, etc.), per qualsevol motiu (cercar informació en la intranet, recuperar un fixer del disc compartit, actualitzar una comanda, etc.). Alguna cosa com establir una VLAN entre l'ordinador de l'empleat i la LAN de la empresa, utilitzant Internet com a transport. Estem parlant de muntar una VPN (Virtual Private Network, xarxa privada virtual).

L'objectiu final de la VPN és que l'empleat no note si està en l'empresa o fora d'ella. En tots dos casos rep una configuració IP privada (direcciones 10.X.X.X, per exemple), per la qual cosa no necessita canviar res en la configuració de les seues aplicacions (correu, intranet, etc.). El responsable d'aconseguir aquesta transparència és el programari de la VPN. En el ordinador de l'empleat cal instal·lar un programari client VPN. Aquest programari instal·la un driver de xarxa, de manera que per al sistema operatiu és una targeta més. Aquest driver s'encarrega de contactar amb una màquina de l'empresa, on executa un programari servidor VPN que gestiona la connexió, per a introduir els paquets en la LAN. La gestió consisteix en:

- Autenticar al client VPN. No podem deixar que entre qualsevol, per la qual cosa s'utilitza el típic usuari/contrasenya, targetes intel·ligents, etc.

- Establir un túnel a través d'Internet. El driver de la VPN en el client li ofereix una adreça privada de la LAN de l'empresa (la 10.0.1.45, per exemple), però qualsevol paquet que intente eixir per aqueixa targeta és encapsulat dins d'un altre paquet. Aquest segon paquet viatja per Internet des de la IP pública de l'empleat fins a la IP pública del servidor VPN en l'empresa. Una vegada allí, s'extrau el paquet i s'injecta en la LAN. Perquè algú de la LAN envie un paquet a la 10.0.1.45 el procés és similar.

- Protegir el túnel. Com estem travessant Internet, cal encriptar les comunicacions (sobretot si som una empresa). Els paquets encapsulats aniran xifrats.

- Alliberar el túnel. El client o el servidor poden interrompre la connexió quan ho consideren necessari.

El programari VPN en el client sol portar una opció perquè les connexions a Internet es facen directament en la connexió de l'usuari, sense haver de passar pel túnel i eixir per la connexió a Internet de l'empresa. És a dir, el túnel s'usa solament per a comunicacions internes.

4. Serveis de xarxa. Nmap i netstat

Comencem aquesta unitat parlant dels riscos de connectar un equip a una xarxa. Hi haurà una part del programari instal·lat en aquest equip (els anomenats serveis de xarxa) que vol connectar amb uns equips i que espera connexions d'aquests equips o uns altres. Però poden arribar connexions d'un client atacant, o ens podem estar connectant per error a un servidor atacant.

El programari dels serveis de xarxa és especialment delicat. Hem de vigilar quin programari tenim actiu i quines actualitzacions té pendents. Les actualitzacions arribaran pel mecanisme habitual del sistema operatiu; el programari que tenim actiu (fent connexions o esperant-les) el podem conèixer mitjançant un parell d'eines senzilles: Nmap i netstat.

L'eina **Nmap**, disponible per a sistemes Linux i Windows, s'ha convertit en la navalla suïssa dels hackers de xarxa. A més de l'escaneig de ports per a determinar els serveis disponibles en una màquina, podem demanar a l'eina que intente la connexió a cadascun d'ells. Després analitza els missatges que generen aquests servidors per a identificar la versió concreta del sistema operatiu i la versió concreta del programari de servidor (server fingerprint) que està escoltant en cada port. És a dir, encara que intentem despistar arrancant serveis en ports que no són els esperats (80 para HTTP i uns altres), l'eina reconeix el port com a obert i aconsegueix identificar el servei. La informació de versió és molt útil per a un atacant perquè pot consultar en la seua base de dades les vulnerabilitats de cada versió d'un servei i així triar millor el tipus d'atac que pot llançar contra la màquina. Per a cada port, l'eina ofereix quatre possibles estats:

- open (obert): la màquina accepta paquets dirigits a aqueix port, on algun servidor està escoltant i els processarà adequadament.
- closed (tancat): no hi ha cap servidor escoltant.
- filtered: Nmap no pot dir si aqueix port està obert o tancat perquè algú està bloquejant l'intent de connexió (router, firewall).
- unfiltered: el port no està bloquejat, però no es pot concloure si està obert o tancat.

Netstat: és una ordre de la línia de comandes disponible en sistemas com Unix, GNU/Linux, Mac OS X, Windows y BeOS que s'utilitza per mostrar informació sobre les connexions de xarxa i les estadístiques associades en un sistema informàtic. Aquesta ordre permet als usuaris veure les connexions de xarxa actives, les taules de rutes, els ports que estan escoltant i altres dades rellevants sobre la xarxa. Pot ser útil per diagnosticar problemes de xarxa i supervisar l'ús de la xarxa en un sistema.

Aquesta comanda permet als usuaris veure les connexions de xarxa actives, les taules de rutes, els ports que estan escoltant i altres dades rellevants sobre la xarxa. Pot ser útil per diagnosticar problemes de xarxa i supervisar l'ús de la xarxa en un sistema.

Tema 7: Seguritat activa: control de xarxes

1- Espiar la nostra xarxa
- *1.1. tcpdump*
- *1.2. WireShark*
- *1.3. Port mirroring*
- *1.4. IDS / IPS. Snort*

2. Firewall
- *2.1. Què fa*
- *2.2. On situar-lo*
- *2.3. Firewall en Linux. Iptables*
- *2.4. Firewall al Windows Server 2022*

3. Proxy
- *3.1. Què fa3*
- *3.2. On situar-lo*
- *3.3. Tipus de intermediari*
- *3.4. Proxy Squid: configuració i monitorització*

4. Spam
- *4.1. Què fa*

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. Anem a processar el tràfic de la nostra xarxa mitjançant dos tipus de tècniques:

- El monitoratge del trànsit. Treballa a alt nivell: es limita a prendre mesures, els anomenats comptadors. Per exemple, total de bytes enviats o rebuts en una interfície, agrupats per port d'origen o destinació. El monitoratge és habitual en les empreses perquè:
    a) Resulta fàcil d'activar en tota la xarxa atès que són els propis equips els que faciliten aquesta informació sobre les seus interfícies.
    b) Genera relativament poca informació per transmetre i processar.
    c) És suficient per conèixer la disponibilitat de la xarxa o el tipus de trànsit que transita. Per exemple, conèixer el percentatge de trànsit HTTP de la nostra xarxa ens pot portar a instal·lar un proxy, com veurem en l'apartat 7.3.
- L'anàlisi del trànsit. Treballa a baix nivell: captura tots els paquets que transiten per una interfície (els coneguts sniffer de xarxa). Els paquets només són llegits, no interceptats: el paquet continua el seu camí. El processament d'aquests paquets llegits permet generar mesures agregades, però sobretot interessa analitzar les converses entre els equips, comprovant que s'ajusten al comportament esperat en el protocol estàndard (analitzador de protocols). Encara que aquesta informació és molt més rica que els simples comptadors, la captura és molt costosa d'activar en tota la xarxa, perquè es dispara la quantitat d'informació que cal transmetre i processar (la majoria dels ports ja tenen velocitat gigabit). per aquest motiu, només s'utilitza en situacions concretes que no es poden abordar amb l'estudi de comptadors, com és la detecció d'atacs.

En tots dos casos, com les xarxes de les empreses tenen molts equips utilitzant difents protocols, necessitarem eines que ens ajuden a recollir, processar, analitzar i presentar tota la informació disponible.

Amb aquestes eines cal anar amb compte per aconseguir un equilibri entre els objectius de seguretat i la càrrega extra que suposa tractar aquesta informació (CPU de els equips de xarxa, trànsit que ocupa a la xarxa enviar els comptadors o captures fins l'eina, CPU del servidor de l'eina, cost del programari especialitzat, dedicació de personal de suport a consultar els informes i prendre decisions, etc.).

Els problemes típics que ens faran aplicar aquestes tècniques poden ser tan senzills com una tempesta de broadcast (massa paquets de tipus broadcast), que podem detectar en les estadístiques d'una interfície. I tan complexos com un DoS (Denial of Service, denegació de servei).

Com vam veure en la primera unitat d'aquest llibre, els DoS són un intent de sobrecàrrega d'un servidor saturant de peticions. La nostra missió serà esbrinar si aquestes peticions corresponen a clients reals o als falsos clients (dirigits per l'atacant). Per tant farem una captura puntual en un tram de la xarxa i tractarem d'analitzar els intentsn de connexió a aquest servidor: origen, tipus de petició, nombre de peticions, etc.

A més de la monitorització del trànsit i l'anàlisi del mateix, hi ha un tercer element per a el control de la xarxa: la sonda. Una sonda (en anglès probe) és un equip de la xarxa que està programat per a comportar-se com un client normal d'algun dels serveis que tenim desplegats. La sonda executa les seues operacions periòdicament, de manera que, si alguna falla, podem suposar que també li fallarà a l'usuari i hem de corregir el problema.

Com hem assenyalat anteriorment, el monitoratge del trànsit és relativament fàcil d'activar en una xarxa, perquè els equips solen estar preparats per a facilitar-nos la informació sobre els seus comptadors i n'hi ha prou amb preguntar-los periòdicament. Per contra, la captura de converses és més complexa d'activar. Les opcions són:

- Aconseguir el control sobre algun dels extrems de la connexió per poder utilitzar alguna de les eines que veurem a continuació (tcpdump, wireshark).
- Interceptar la connexió mateixa des d'algun equip de xarxa per on passen els paquets intercanviats. Si aquest equip té certa intel·ligència, segurament incorporarà funcionalitats avançades, com el port mirroring; fins i tot pot ser un router Linux, de manera que tindrem al nostre abast totes les eines que veurem per als extrems.
- Com a últim recurs podríem connectar de manera temporal un hub al port que volem vigilar, però això suposa desplaçaments de personal i equips que no sempre estan disponibles (per exemple, el switch de LAN està en Barcelona, però el departament de suport està a Madrid). Fem servir un hub i no un switch perquè el hub repeteix el trànsit de cada port a tots els altres, just el que necessitem.

1.1. tcpdump

tcpdump és una eina senzilla disponible en Linux que permet fer un bolcat de tot el trànsit que arriba a una targeta de xarxa. Captura tot el trànsit, no només el tràfic TCP, com apareix en el seu nom. Els paquets llegits es mostren en pantalla o es poden emmagatzemar en un fitxer del disc per a ser tractats posteriorment per aquesta mateixa eina o una altra més avançada. Es necessiten privilegis per executar-la, perquè necessitem posar la targeta en mode promiscu perquè accepte tots els paquets, no només els destinats a la seua MAC.

1.2. WireShark

WireShark és l'eina més estesa en Windows per realitzar captures de trànsit i analitzar els resultats. És una evolució d'una eina anterior anomenada Ethereal. Per a la captura de paquets utilitza la llibreria pcap, que també apareix en altres sniffer, com tcpdump. La interfície d'usuari és molt potent, així com el nombre de protocols que és capaç d'analitzar.

1.3. Port mirroring

Els switch gestionables solen incorporar aquesta funcionalitat. Consisteix en modificar la configuració del switch perquè replique tot el trànsit d'un port a un altre. Al segon port agafarem l'sniffer. L'equip o equips connectats en el primer port funcionen amb normalitat, no saben que estan sent espiats. Generalment es pot triar el tipus de trànsit: entrant (des de l'equip fins al switch), eixint (des del switch fins a l'equip) o tots dos. En alguns models podem fer que diversos ports bolquen el seu trànsit a un mateix port, tot i que caldrà vigilar les prestacions del conjunt perquè poden desbordar l'ample de banda

de la interfície o la capacitat de captura del sniffer, el que ocasionaria la pèrdua de paquets, invalidant l'anàlisi posterior.

1.4. IDS / IPS. Snort

Les eines d'anàlisi de trànsit són més o menys senzilles d'instal·lar i configurar, però la complicació ve a l'hora d'interpretar els resultats. Per treure el màxim partit a aquestes eines es necessiten molts coneixements de base i una àmplia experiència en protocols de comunicacions.

Hi ha un segon problema: encara que disposem de personal tan qualificat, no és humanament possible revisar una a una totes les converses que tenen lloc diàriament en una xarxa normal. Sobretot perquè la majoria són interaccions normals, lliures de tota sospita. Els experts cal reservar-los per als casos difícils. Per solucionar dos problemes existeixen els sistemes IDS / IPS (Intrusion Detection System / Intrusion Prevention System). Els IDS detecten els atacs i els IPS actuen contra ells. Tenim dos tipus d'IDS / IPS:

- NIDS / NIPS (Network Intrusion i Network Prevention). Busquen atacs sobre serveis de comunicacions. Es basen en l'anàlisi dels paquets que formen part de la comunicació entre dues màquines, comprovant que s'ajusten al protocol estàndard.
- HIDS / HIPS (Host Intrusion i Host Prevention). Busquen atacs sobre les aplicacions i el sistema operatiu de la màquina. Es basen en l'anàlisi dels processos actuals (Ocupació de CPU i memòria, ports oberts) i la configuració i el registre de cada un dels serveis.

En aquest tema anem a referir-nos als NIDS / NIPS. Aquests sistemes processen un fitxer de captura de trànsit (o la realitzen ells mateixos) i busquen patrons de comportament en els paquets intercanviats entre els equips. No es limiten a revisar les capçaleres del protocol, sinó que també miren en el contingut del paquet (payload). quan detecció tan un possible atac, si és un IDS sol avisa a l'usuari (com a mínim, fitxer de log) i si és un IPS només respon a l'atac (també es pot fer que els IPS avisin).

La resposta d'un IPS pot ser impedir que aquest paquet i els següents d'aquesta connexió arriben al seu destí. En els més avançats es pot configurar que permeten que el paquet arribe, però adequadament modificat perquè no prospere l'atac.

La intel·ligència d'aquestes eines sol residir en un conjunt de regles que es carreguen en el programa des d'un fitxer de configuració. Les regles són elaborades per experts en seguretat que, quan han identificat un nou tipus d'atac, escriuen la regla que permetrà a l'IDS detectar-lo.

Els problemes dels IDS són dos:

- Rendiment. El nombre de regles és creixent (hi ha nous atacs i no podem descartar els antics) i el volum de trànsit també, pel que necessitem un maquinari molt potent per tenir funcionant un IDS sobre captures de trànsit a temps real. En determinats moments, la cua de paquets pendents d'examinar serà tan llarga que la interfície estarà a punt de començar a descartar-los. Per a evitar-ho, l'IDS els deixarà passar, sabent que pot ser un atac (si no els deixa passar, nosaltres mateixos estarem executant un atac). Però si ens limitem a processar fitxers de captura antics, pot ser que trobem atacs que ja han passat i siga tard per reaccionar.

- Falsos positius. Les regles no són perfectes i pot ser que estiguem alertant sobre comunicacions que són perfectament legals. Convé provar molt bé una regla abans de ficar-se en un IPS.

2. Firewall

Hem vist que la tasca dels NIPS és dura: revisar tots els paquets que transiten per la xarxa buscant patrons d'atacs coneguts. Els consegüents problemes de rendiment impedeixen que moltes empreses els utilitzen. Però si efectivament coneixem les característiques de l'atac (port on intenta connectar, tipus d'adreça IP origen invàlida, mida del paquet utilitzat), una altra forma de defensa és prendre mesures en les nostres màquines per a que reaccionen adequadament davant la presència d'aquests paquets sospitosos. És a dir, els paquets que aconsegueixen entrar a la nostra xarxa, enganyar a NIPS (si el tenim) i arribar als nostres equips, o que intenten ixir procedents d'una aplicació no autoritzada (per exemple, un troià ens pot convertir en generadors de correu spam), encara han de superar un control més en cada equip: el firewall o tallafocs.

Per exemple, si tenim un servidor web en la nostra LAN i no volem que siga atacat des de la wifi pública que oferim als clients a la sala d'espera, podem configurar el tallafocs de la màquina del servidor web per a que no accepte connexions de les màquines connectades a aquesta wifi (generalment, les identificarem perquè pertanyen a una subxarxa diferent).

2.1. Què fa

El tallafocs és un programari especialitzat que s'interposa entre les aplicacions i el programari de xarxa per tal de fer un filtrat de paquets:

- En el tràfic entrant, la targeta de xarxa rep el paquet i l'identifica, però abans de lliurar-lo a l'aplicació corresponent, passa pel tallafocs perquè decidixica si prospera o no. En l'exemple del servidor web, la màquina rep un paquet destinat nat al port 80, però abans de lliurar-lo al procés que té obert aquest port (un apache.exe), el firewall decidix.
- En el tràfic d'eixida, les aplicacions elaboren els seus paquets de dades, però abans de lliurar-lo al programari de xarxa perquè l'envie, passa pel tallafocs. Per exemple, si sospitem que una màquina fa spam, podem bloquejar totes les connexions d'eixida al port 25.

En les màquines servidor, generalment el tallafocs actua sobre tràfic entrant: els serveis que s'executen en aquesta màquina obren determinats ports i volem controlar qui es connecta a ells. En les màquines client és més senzill: per defecte, totes les connexions entrants estan prohibides i totes les sortints permeses. Això no vol dir que no puguen entrar paquets, perquè no hi hauria converses, però la conversia l'ha d'iniciar l'equip client.

La intel·ligència del tallafocs s'expressa mitjançant regles de configuració. L'administrador de la màquina pot individualment activar-les, desactivar-les, modificar-les o afegir noves. Aquest procés pot ser automàtic: alguns programes que instal·len en un servidor són capaços de configurar alguns programes del tallafocs, sense necessitar la intervenció de l'administrador.

Les regles del tallafocs són molt més senzilles que les regles d'un IPS i generalment s'apliquen només a les capçaleres TCP / IP de les capes 3 (xarxa) i 4 (transport): el tallafocs

bàsicament mira adreces IP i ports, encara que també pot reconèixer converses entre dos equips i controlar-les.

No ens podem permetre augmentar la complexitat de les regles o mirar el contingut de cada paquet (DPI [Deep Packet Inspection]) perquè els recursos dels equips són limitats. Però si les nostres necessitats de seguretat són superiors, hi ha un tipus de tallafocs més sofisticat, anomenat tallafocs de nivell d'aplicació, on sí s'entra a mirar les dades d'usuari que hi ha més enllà de les capçaleres. S'utilitza sobretot en protocols web (HTTP). Per tant, és més potent (i més lent) que el tallafocs normal, però menys complex (i més ràpid) que tot un IPS.

2.2. On situar-lo

Totes les màquines de l'empresa connectades a la xarxa necessiten activar un tallafocs. Fins i tot encara que no s'execute cap servei: pot ser que el programari de xarxa del sistema operatiu tinga una vulnerabilitat. Igual que amb el malware que cal bloquejar-lo amb l'antivirus perquè és programari no sol·licitat, el tallafocs ens ajuda a bloquejar paquets de xarxa no sol·licitats.

Aquesta mesura seria suficient; però, per evitar que s'inunde la xarxa amb paquets que no arribaran al seu destí, o per ajudar a màquines que no tenen tallafocs (per exemple, una impressora en xarxa, en els punts crítics de la xarxa se solen col·locar màquines independents executant tasques de tallafocs (firewall de xarxa). Per exemple, sempre sol estar en la connexió a Internet perquè per aquí arribaran molts atacs.

Els routers domèstics proporcionats pels ISP (Internet Service Provider) fan funcions cions de tallafocs, perquè per defecte es comporten com equips d'usuari i no permeten connexions entrants. Però una empresa sol necessitar més configuracions, de manera que instal·larà el seu propi tallafocs de xarxa. En empreses petites aquest tallafocs de xarxa segurament s'executarà en una màquina que també fa les funcions de router, fins i tot pot ser que també allotge determinats serveis de l'empresa en Internet (un servidor web o servidor de correu). a les empreses grans hi ha màquines diferents per a cada servei, totes situades en una subxarxa especial anomenada DMZ (Demilitarized Zone, zona desmilitaritzada). El tallafocs d'aquesta zona és menys exigent que el que protegeix la nostra LAN, perquè hem de permetre connexions a aquests serveis; però, com està exposat a més atacs, se sol acompanyar d'un IDS/IPS.

Per exemple, si tenim un servidor web a la DMZ, el tallafoc de la DMZ ha de permetre passar el port 80, però el tallafocs de la LAN, no. No obstant això, convé posar un IPS en el servidor per protegir-los de múltiples atacs HTTP que puguen venir d'Internet.

2.3. Firewall en Linux. Iptables

Quan arriba un paquet a la targeta de xarxa, el sistema operatiu (més concretament, el programari de xarxa) decidix què fer amb ell. El resultat d'aquesta decisió pot ser:

- Descartar-lo. Si el destinatari del paquet no és la nostra màquina o, encara que ho siga, cap procés actual l'espera. Per exemple, arriba una petició http a una màquina que no té un servidor web arrencat: la màquina l'ignora.
- Acceptar-lo, perquè és per a nosaltres i hi ha un procés que sap què fer amb aquest paquet. Seria l'exemple anterior, però ara sí que tenim un servidor web funcionant.

- Acceptar-lo, encara que no siga per a nosaltres, perquè som un router i anem a enviar-lo a una altra interfície. En alguns casos arribarem a modificar les capçaleres del paquet, com veurem més endavant.
- Acceptar-lo, encara que no és per a nosaltres i tampoc som un router: però estem escoltant tots els paquets perquè som un sniffer de xarxa.

En el cas de Linux, la utilitat iptables permet introduir regles en cadascuna d'aquestes fases:

- Quan arriba el paquet per un procés nostre però encara no l'hem entregat, en iptables parlem d'input.
- Quan som un router i estem a punt de passar el paquet d'una interfície a una altra, en iptables parlem de forward.
- Quan un paquet està llest per a eixir per una interfície, en iptables parlem de output.

Hi ha un parell d'etapes més:

- Prerouting. S'executarà abans d'input. 'usa per a obviar l'enrutament perquè sabem exactament que fer amb aquests paquets.
- Postrouting (després d'output i després de forward). S'utilitza per aplicar alguna modificació als paquets que estan a punt d'abandonar la màquina.

Les regles d'iptables tenen una llista de condicions i una acció, de manera que, quan un paquet compleix totes les condicions d'una regla, s'executa l'acció. A les condicions podem definir la interfície per la que va entrar, la interfície per la que ixirà, l'adreca IP o la subxarxa del paquet, el tipus de protocol, el port origen o destí, etc. les accions poden ser simplement acceptar o rebutjar el paquet, o també modificar-lo.

Però no totes les accions estan disponibles en totes les situacions. Per això les regles s'agrupen en tres taules principals:

- filter. És la taula principal. La seua missió és acceptar o rebutjar paquets. És el tallafocs pròpiament dit.
- nat. Les regles d'aquesta taula permeten canviar l'adreca d'origen o destinació dels paquets.
- mangle. En aquesta taula podem alterar diversos camps de la capçalera IP, com el Tos (Type of Service). Se sol utilitzar per aplicar QoS (Quality of Service), marcant els paquets de determinats serveis per després prioritzar-los.

Dins de cada taula, les regles s'agrupen al seu torn per l'etapa del processament de paquets on s'apliquen (prerouting, input, etc.), encara que no totes les taules tenen totes les etapes. Per a cada etapa (també anomenada chain, perquè encadena una regla amb una altra) hi ha una llista de regles que es recorre seqüencialment fins que el paquet acomplix una regla. En aquest moment s'executa l'acció associada a la regla i es deixa d'aplicar la resta de les regles d'aquesta etapa (excepte l'acció LOG, com veurem més endavant). Si el paquet no acompleix cap regla d'aquesta etapa, s'aplica l'acció per defecte de l'etapa.

2.4. Firewall al Windows Server 2022

Configurar un firewall a Windows Server 2022 és una part essencial de l'administració de la seguretat del teu servidor. Pots utilitzar el Firewall de Windows o el Firewall de Windows amb característiques avançades (anteriorment conegut com a Firewall de Windows amb seguretat avançada) per configurar regles i protegir el teu servidor.

Recorda que és important configurar les regles del firewall adequadament per permetre el tràfic necessari per a les aplicacions i serveis que desitges que el servidor oferisca, mentre es bloqueja tot el tràfic no desitjat o no autoritzat.

A més, tingues en compte que la configuració del firewall pot ser complexa i variar segons les necessitats específiques del teu servidor i entorn, per la qual cosa és important comprendre les implicacions de les regles que configures.

3. Proxy

Hem vist que els tallafocs normals permeten controlar les connexions a nivell de xarxa (Filtrat de paquets mirant adreces i ports). Si necessitem alguna cosa més, cal recórrer a un tallafocs d'aplicació o directament a un IPS. Però hi ha una altra forma d'afronta el problema de controlar què estan parlant dos màquines entre si. Podem introduir un nou interlocutor enmig de la conversa: on abans A parlava amb B, ara hi ha un C, de manera que A parla amb C i C l'hi explica a B, i viceversa. Aquest nou intermediari és un servidor intermediari, i com té accés a tots els paquets intercanviats, pot aplicar mesures de seguretat.

Un servidor intermediari és un servei de xarxa que fa d'intermediari en un determinat protocol. El proxy més habitual és el servidor intermediari HTTP: un navegador en una màquina client que vol descarregar-se una pàgina web d'un servidor no ho fa directament, sinó que li demana a un servidor intermediari que ho faca per ell. El servidor no es veu afectat perquè li dóna igual qui consulta les seves pàgines.

No hem de veure sempre la seguretat com una cosa negativa perquè ens impedeix navegar per algunes webs, també pot impedir que entrem en determinats llocs perillosos on podem rebre un atac. A més, en les empreses hi ha altres motius per a instal·lar un servidor intermediari:

- Seguretat per al programari del client. Pot ocórrer que el programari de l'ordinador client estiga fet per a una versió antiga del protocol o tinga vulnerabilitats. Passant per un servidor intermediari actualitzat evitem aquests problemes.
- Rendiment. Si en una LAN diversos equips accedeixen a la mateixa pàgina, fent que passen pel proxy podem aconseguir que fem la primera connexió amb el servidor i la resta rep una còpia de la pàgina que ha estat emmagatzemada pel proxy.
- Anonimat. En determinats països hi ha censura a les comunicacions, de manera que utilitzar un servidor intermediari de l'estranger els permet navegar amb llibertat.
- Accés restringit. Si en la nostra LAN no està activat el routing a Internet, sinó que només pot ixir un equip, podem donar navegació a la resta instal·lant un servidor intermediari en aquest equip.

3.1. Què fa

El servidor intermediari rep d'una màquina origen A un missatge formatat per al servidor B segons un protocol determinat. El processa i genera un nou missatge per la mateixa destinació B, però ara l'origen és P, la màquina del servidor intermediari. Quan el servidor B genera la resposta, l'envia a P. La màquina P processa aquest missatge i genera el seu propi missatge de resposta amb destinació A. Els usuaris no aprecien la diferència perquè les pàgines (en el cas d'un servidor web) arriben al seu navegador amb normalitat, però realment el servidor si que pot saber l'origen de la petició no és un ordinador interessat en el seu servei, sinó un mitjancer de l'ordinador original. Per exemple, nombrosos serveis d'Internet que permeten consultar la IP pública que utilitza el nostre router per connectar a Internet també ens informen de si la nostra connexió està passant per un intermediari.

El processament del servidor intermediari pot portar a decidir no generar cap missatge. És a dir, tallar la comunicació. Aquest comportament es decideix mitjançant regles. En aquestes regles podem filtrar determinades adreces d'origen o destinació, algunes directives del protocol (per exemple, paraules dins de la URL d'una pàgina web), fins i tot continguts (per exemple, imatges). Com podem suposar, com més complexa siga la regla, més tardarà el proxy a aplicar-la a les peticions que li arriben, el que pot ralentir en excés la comunicació.

A més de controlar les connexions web, el proxy millora el rendiment global de la navegació perquè guarda en disc les pàgines que envia als clients. És l'anomenat proxy caché.

3.2. On situar-lo

Si el volum de trànsit que passarà pel proxy és reduït i les regles definides són senzilles, el servidor intermediari necessitarà pocs recursos (CPU, RAM, disc per a la memòria cau), per la qual cosa pot estar implementat en una màquina que ja ofereixi altres serveis (DHCP, DNS, disc en xarxa, correu).

Si el volum és elevat o les regles que hem definit són complexes, no podem permetre'ns afectar altres serveis: necessitarem una màquina en exclusivitat (fins i tot més d'una, formant un clúster). Encara que caldrà dimensionar adequadament l'ample de banda en aquestes màquines dedicades, perquè van a rebre molt de trànsit. En qualsevol cas, el servidor intermediari ha de tenir la millor connectivitat possible amb els servidors per a els que fà d'intermediari (generalment, servidors web en Internet).

3.3. Tipus de intermediari

Si instal·lem un servidor intermediari per a un determinat protocol (per exemple, HTTP), el següent pas és aconseguir que el trànsit dels nostres usuaris passe per aquest intermediari. Tenim dos opcions:

- Proxy explícit. Configurem els navegadors dels usuaris perquè utilitzen el servidor intermediari de l'empresa.
- Proxy transparent. En algun punt de la xarxa un router filtrarà aquest tipus de trànsit (per exemple, comprovant que el destí és el port 80 de TCP) i l'enviarà al servidor intermediari, sense que l'usuari haja de fer res. Si estem utilitzant un router Linux, l'opció òptima és instal·lar-lo en el router, perquè estalviem el trànsit fins a una altra màquina.

Una tercera opció de navegació proxy a l'abast dels usuaris és utilitzar un servidor intermediari web. És a dir, una pàgina web on entrem per introduir l'URL de la pàgina web

que realment volem visitar. El servidor del servidor intermediari web connecta amb aquesta pàgina i ens mostra el resultat. Aquest mecanisme és el més utilitzat per a evitar la censura en alguns ens països. En una empresa no és acceptable perquè el trànsit dels nostres empleats està passant per la màquina d'una empresa desconeguda i no sabem què pot fer amb aquestes dades.
En el cas del servidor intermediari explícit podem incloure un mecanisme d'autenticació, de manera que només alguns usuaris puguen accedir a Internet i només a algunes web. En un proxy transparent no té sentit perquè l'usuari no té cap opció d'introduir usuari i contrasenya.

3.4. Proxy Squid: configuració i monitorització

El programari de servidor intermediari més estès és Squid. Té versió per a Windows, però ací veurem la versió Linux, que és la més utilitzada. Anem a aprendre com s'instal.la, com es configura i com es comprova que està processant trànsit.

4. Spam

A les empreses, el correu electrònic és tan important o més que el telèfon. dels empleats ja que necessiten estar en contacte amb altres empleats de la mateixa empresa, amb els proveïdors i amb els clients. Com a responsables de la infraestructura informàtica hem de garantir que els missatges s'envien i reben amb normalitat, però també que no fem perdre el temps als nostres usuaris amb correus no desitjats (Spam). Aquests correus, com a mínim, porten publicitat, però també són una font de infecció de virus i troians que poden venir en un fitxer adjunt o que aprofiten una vulnerabilitat del programa de correu.

4.1. Què fa

El programari antispam col·labora amb el servidor de correu per detectar missatges indesitjablesbles. Per determinar si un missatge entra en aquesta categoria, l'antispam utilitza:

- La capçalera del missatge, buscant si el servidor de correu origen està en alguna llista negra de spammers reconeguts, si la data d'enviament utilitza un format incorrecte (Suggereix que el correu ha estat generat per un programari d'spam, no per un client de correu normal), etc.
- El contingut del missatge, buscant paraules poc relacionades amb l'activitat de l'empresa (medicines, etc.),
- La pròpia experiència del programa (autoaprenentatge)

Quan es detecta un correu spam, tenim diverses opcions:

- Bloquejar i impedir que arribe fins a l'usuari, així li estalviem molèsties (Llegir-lo, esborrar-ho) i evitem potencials infeccions. No se sol utilitzar perquè mai tindrem la certesa que no hem eliminat algun correu important.
- Deixar-lo passar, però avisant a l'usuari que és un correu sospitós. És l'opció per defecte. L'avís a l'usuari consisteix a afegir text al títol del correu (per exemple, *** SPAM ***), això li servirà a l'usuari per crear els seus propis filtres en el seu programa de correu.
- Deixar passar, però convertint el text del correu en un fitxer adjunt, perquè siga més difícil enganyar l'usuari i només l'obri-lo si està segur que el correu li interessa.

4.2. SpamAssasin: configuració i monitorització

El programari SpamAssasin és un dels més estesos per la seva eficàcia i l'àmplia varietat de filtres que pot arribar a aplicar per determinar si un correu és spam. Els filtres s'especifiquen mitjançant regles. Si un missatge compleix una regla, se li assigna una puntuació. Quan un missatge supera un determinat llindar (per defecte, 5, encara que el podem canviar), es considera que és spam. SpamAssasin, a més, utilitza tècniques d'intel·ligència artificial (xarxes neuronals) per reduir el nombre de falsos positius (correu spam que no ho és) i falsos negatius (corrreu spam que no ha estat detectat com a tal).
