Fonaments de seguretat informàtica

PID_00269889

Amadeu Albós Raya

Temps mínim de dedicació recomanat: 5 hores

Universitat Oberta de Catalunya

Amadeu Albós Raya

Enginyer informàtic per la Universitat Oberta de Catalunya.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats per la professora: Helena Rifà (2019)

Primera edició: setembre 2019
© Amadeu Albós Raya
Tots els drets reservats
© d'aquesta edició, FUOC, 2019
Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars dels drets.

Índex

Introducció

La tecnologia s'ha tornat ubiqua amb el pas del temps, no només perquè els serveis que ofereix són cada vegada més nombrosos i accessibles des de gairebé qualsevol lloc, sinó perquè la societat l'ha acceptat de ple i l'explota cada dia amb objectius i en situacions diferents.

Les tecnologies de la informació i la comunicació faciliten que la informació pugui fluir contínuament en totes direccions, sense gaires complicacions tècniques o fronteres que siguin perceptibles. Però la informació és un actiu valuós que cal protegir, perquè amb aquesta omnipresència està exposada contínuament a tot tipus de riscos. De vegades caldrà assegurar que la informació no hagi estat modificada sense autorització, altres vegades que només puguin accedir determinats usuaris i altres garantir que s'hi pugui accedir en tota circumstància. Els sistemes informàtics són el mitjà per a processar la informació i extreure'n el màxim profit, però també poden materialitzar tots els riscos amb aquelles tecnologies que no disposen dels mecanismes de seguretat adequats.

La complexitat dels sistemes informàtics i l'evolució constant de les amenaces imposen que la seguretat no sigui ni estàtica ni centrada en un sol element, sinó basada en un conjunt coherent de mesures dinàmiques que pretenen reduir (i si pot ser, eliminar completament) l'impacte que puguin tenir.

Al llarg de les properes seccions veurem com és un sistema informàtic i quines són les mesures habituals per a garantir, d'una banda, la seguretat física i perimetral, i d'una altra banda, la seguretat dels serveis i les comunicacions.

Objectius

1. Conèixer el sistema informàtic, els components i el funcionament.

2. Identificar els riscos de seguretat de la informació que processa el sistema informàtic.

3. Comprendre les mesures de seguretat física i perimetral d'un sistema informàtic.

4. Comprendre les mesures de seguretat dels serveis i les comunicacions d'un sistema informàtic.

5. Entendre la cohesió i complementarietat de les mesures de seguretat informàtica.

6. Reflexionar sobre l'evolució dels riscos i la dinàmica de la seguretat informàtica.

1. El sistema informàtic

La tecnologia és essencial per a automatitzar el procés de la informació. Tots els elements que intervenen en el sistema han d'estar ben organitzats i actuar conjuntament per a assolir aquest objectiu, però les tecnologies són diverses per naturalesa i tenen diferents ritmes evolutius, la qual cosa genera un ventall ampli d'escenaris possibles.

Totes les mesures per a garantir la seguretat de la informació recauen sobre els components del sistema informàtic i en la interacció que hi ha entre ells, per tant, no es podran implementar adequadament sense conèixer-ne el funcionament i l'organització.

1.1. El context informàtic

Avui dia, difícilment es poden concebre tecnologies basades en elements aïllats els uns dels altres. Si bé es poden trobar situacions concretes que poden justificar aquest plantejament,[1] els requisits actuals per al tractament de dades imposen cada vegada més la cooperació i la comunicació entre tots els elements.

(1)Per exemple, un ordinador que es dediqui exclusivament al càlcul no té gaires més requisits per l'acompliment del seu objectiu que el programa de càlcul i les dades que s'han de processar.

Un **sistema informàtic** és un conjunt organitzat de recursos humans, materials i lògics que actuen en el procés automàtic de la informació.

Vegem aquesta definició amb més detall:

- El sistema informàtic requereix una estructura adequada i coherent que permeti integrar, amb eficàcia, la capacitat i la funció que pot aportar cadascun dels recursos al procés de la informació.

- Els recursos materials són tots aquells elements tangibles que es poden trobar en el sistema. Seria el cas dels ordinadors, les tauletes, els servidors, el cablejat, els commutadors, els projectors, els encaminadors, les impressores, etc.

- Els recursos lògics són tots els elements intangibles que són necessaris per a utilitzar el maquinari i obtenir les prestacions que ofereix, el programari (per exemple, els sistemes operatius o les aplicacions d'usuari) o les configuracions que defineixen el comportament del sistema (per exemple, les regles de filtratge d'un tallafocs o la definició dels permisos d'accés a una carpeta compartida).

- Els recursos humans són totes aquelles persones que interactuen amb el sistema per a realitzar diferents tasques, com els usuaris, els administradors, els desenvolupadors, els tècnics, etc.

- L'acció conjunta dels diferents recursos del sistema és necessària per a aconseguir el resultat esperat. Per exemple, per a consultar la bústia de correu, un usuari haurà d'utilitzar un ordinador connectat a la xarxa que tingui instal·lat el sistema operatiu i l'aplicació necessària per a connectar amb el servei de correu electrònic.

En general, es considera que qualsevol dels recursos pot suposar una amenaça per la seguretat del sistema. Per exemple, un usuari pot comprometre l'accés a la informació emmagatzemada si deixa a la vista les claus d'accés al sistema, un sistema operatiu pot presentar vulnerabilitats[2] dins del codi que podrien ser explotades per a obtenir privilegis d'execució[3] o els errors en el disseny d'un processador poden facilitar l'accés no autoritzat a dades d'altres processos.

[2] Sovint, les vulnerabilitats s'anomenen amb el terme anglès *bugs*.

[3] Les accions que s'executen en un sistema estan emmarcades en el propi context, a excepció d'aquelles d'administració o de supervisió que poden tenir privilegis en altres contextos diferents del propi.

1.2. La infraestructura del sistema

La **infraestructura d'un sistema informàtic** és el conjunt de suports i dispositius que processen, transmeten o emmagatzemen la informació. Representen els recursos essencials sobre els quals es duran a terme les accions, per la qual cosa l'absència impedeix que el sistema informàtic pugui portar a terme una o més de les funcions.

Formen part de la infraestructura tots aquells suports materials sobre els quals se sustenta el sistema, com podrien ser el cablejat i els armaris de xarxa, també tots aquells dispositius electrònics que, juntament amb el programari de base, fan una o més funcions, com, per exemple, els ordinadors i els servidors amb el sistema operatiu o les impressores i els projectors amb el microprogramari[4] que incorporen.

[4] El microprogramari (*firmware* en anglès) implementa les funcions bàsiques de control d'un dispositiu, per la qual cosa està relacionat amb les característiques físiques i electròniques del maquinari sobre el qual està integrat.

A grans trets, es poden distingir tres grups de recursos dins de la infraestructura: aquells que tenen relació amb els usuaris, els serveis i les comunicacions.

1.2.1. Els recursos d'usuari

Tots els usuaris necessiten utilitzar el sistema informàtic amb els dispositius adequats, de manera que puguin completar una o més de les accions entorn del procés de la informació que hagin de realitzar.

Els **recursos d'usuari** són tots aquells dispositius que materialitzen la interfície entre l'home i la màquina, de manera que la interacció condueixi a la realització d'alguna tasca concreta amb el sistema informàtic.

Per exemple, son recursos d'usuari els ordinadors, les tauletes, els telèfons intel·ligents, les impressores, els projectors o les pissarres digitals, entre d'altres. Aquests dispositius disposen d'un suport electrònic (maquinari) sobre el qual s'executa la lògica de funcionament (programari) que facilita l'operació amb l'usuari i la realització de les accions. Es poden classificar segons diversos criteris, però, des de la perspectiva de la seguretat, se'n distingiran principalment els tipus següents:

- Els **dispositius corporatius**, que adquireix i administra l'organització mateixa per tal que els usuaris puguin realitzar les tasques que tenen encomanades. Es consideren confiables perquè l'organització n'elegeix les especificacions, n'instal·la el programari adequat i en determina la configuració necessària per integrar-se en el sistema amb garanties de seguretat.

- Els **dispositius de tercers**, que tot i estar presents en el sistema i accedir a un o més dels serveis que ofereix, són propietat dels usuaris (com treballadors o col·laboradors) o, inclús, d'altres organitzacions (com clients, proveïdors o convidats), per tant, normalment, es troben fora del control administratiu de l'organització. De fet, cada vegada són més les organitzacions que accepten aquesta política, anomenada BYOD[5], tot i els riscos per la seguretat que pot suposar la integració de dispositius desconeguts o poc confiables dins del sistema. D'aquests dispositius se'n desconeix l'estat de manteniment i de protecció, i també els riscos als quals pot haver estat sotmès o les amenaces que poden generar dins del sistema.

[5]BYOD és l'acrònim de l'anglès *bring your own device*, una filosofia que proposa la incorporació al sistema dels dispositius que aporten els usuaris.

Els recursos d'usuari s'ubiquen a l'extrem del sistema informàtic i acostumen a ser la porta d'entrada per trencar la cadena de seguretat, per exemple, amb la introducció de programari maliciós[6] que exploti vulnerabilitats, el robatori de dispositius que continguin informació no xifrada o l'obtenció il·lícita de les claus d'accés al sistema. Moltes vegades, l'actuació dels usuaris pot ser determinant a l'hora de controlar els riscos i evitar la propagació d'incidents cap a la resta del sistema. Per exemple, evitant l'acció de programari maliciós analitzant sistemàticament les claus de memòria o evitant la retransmissió de missatges fraudulents.

[6]El programari maliciós (*malware* en anglès) és tot aquell programari que té objectius nocius per als dispositius, com, per exemple, corrompre el sistema operatiu o segrestar dades.

1.2.2. Els recursos de servei

La implantació d'un sistema informàtic suposa un increment del cost, la complexitat, el manteniment i els riscos per la seguretat, per la qual cosa no té sentit si no s'explota per a prestar serveis de valor afegit a l'organització.

Els **recursos de servei** són tots aquells dispositius que proveeixen d'alguna funcionalitat específica a la resta del sistema, tant si els clients del servei són recursos d'usuari com d'altres recursos de servei (que poden necessitar altres serveis per a proporcionar el seu propi).

Per exemple, és un recurs de servei un directori d'usuaris que organitza els permisos d'aquests i dona servei a un servidor de fitxers per autoritzar l'accés a determinades carpetes compartides.

En termes generals, es poden considerar dos grans grups de recursos de servei:

- Els **dispositius compartits**, que són recursos que ofereixen funcionalitats limitades i específiques d'acord amb la capacitat o les característiques que tenen en particular, com podrien ser les impressores en xarxa, les càmeres de vigilància, els projectors connectats a la xarxa, els sensors ambientals, etc. En general, aquestes funcionalitats són ofertes pel microprogramari que incorporen, tot i que poden necessitar la instal·lació de programari en el recurs que vol accedir al servei (per exemple, per visualitzar les imatges o el vídeo d'una càmera de vigilància pot ser necessària la instal·lació d'un navegador web o d'una aplicació específica).

- Els **servidors**, que són els recursos per excel·lència a l'hora de proveir la resta del sistema de serveis d'alt nivell atesa la capacitat de procés i d'adaptació a qualsevol context. Amb el programari adequat, els servidors poden oferir serveis web, de correu electrònic, de bases de dades, d'aplicacions, de temps, de compartició de fitxers i un llarg etcètera. Els servidors disposen de maquinari i programari específic capaç de suportar la càrrega de treball que se'ls pugui exigir però mantenir les prestacions i el funcionament al llarg del temps[7].

(7)La redundància dels components físics (com les fonts d'alimentació o els discos d'emmagatzematge) és una manera habitual de mantenir l'estabilitat de funcionament en cas de fallades.

Els recursos de servei, especialment els servidors, centralitzen informació que és valuosa per a l'organització, per la qual cosa acostumen a ser un dels centres d'atenció a l'hora d'implantar mesures de seguretat. Per exemple, la sobretensió elèctrica pot malmetre un servidor i aturar els serveis que presta (inclús corrompre les dades en procés) o les vulnerabilitats presents en el sistema operatiu (o en l'hipervisor[8]) poden facilitar l'accés a dades sense autorització.

(8)L'hipervisor (també anomenat monitor de màquines virtuals) permet l'execució simultània de diversos sistemes operatius amb el seu propi context de funcionament (anomenades màquines virtuals) sobre el mateix servidor físic.

1.2.3. Els recursos de comunicació

Per a que tots els recursos presents en la infraestructura puguin cooperar en el procés de la informació, és imprescindible establir canals que permetin l'enviament i la recepció de dades entre els diferents components.

El **recursos de comunicació** són tots aquells suports, dispositius, programes i protocols que permeten la transmissió o l'intercanvi de dades entre els diferents elements del sistema (que normalment seran recursos d'usuari o de servei, però també altres recursos de comunicació).

La infraestructura de comunicacions pren la forma de xarxa informàtica. Els recursos (nodes) es connecten amb una interfície adequada al suport de transmissió[9] que habilita al programari instal·lat per transferir paquets de dades[10] utilitzant protocols de comunicació estàndards.

(9)Els suports o mitjans de transmissió més utilitzats són el parell trenat de coure (sobretot per al cablejat intern), la fibra òptica (sobretot en les connexions a internet) i el buit (per a les connexions sense fils).

Les xarxes informàtiques requereixen la instal·lació de caixes o punts de connexió (amb fils) i de punts d'accés (sense fils) per connectar els nodes, dispositius per transmetre les comunicacions entre els nodes (commutadors[11]) i dispositius per connectar amb els nodes ubicats en altres xarxes (encaminadors[12]), com, per exemple, internet. També és necessari implantar alguns serveis bàsics per al bon funcionament de la xarxa, com, per exemple, el servei d'adreçament de recursos (per a assignar a cada node una adreça identificativa que permeti localitzar-lo) o la resolució dels noms dels nodes (per a obtenir les adreces que tenen assignades a partir del nom comú, i viceversa).

(10)El paquet de dades és la unitat bàsica de transferència i conté tant la informació que es vol transmetre com altres dades de control (emissor, receptor, marca de temps, ordre del paquet, etc.).

(11)El commutador és un dispositiu que transmet paquets de dades entre els nodes que hi estan directament connectats.

(12)Els encaminadors són dispositius que permeten intercanviar paquets de dades entre dues o més xarxes diferents.

Com la resta d'elements de la infraestructura, els recursos de comunicació també són un dels objectius habituals per a trencar la seguretat del sistema, atesa la funció de facilitar la transmissió de dades en totes direccions[13]. La intercepció de dades, la modificació indeguda d'informació, la suplantació de l'emissor o del receptor, la redirecció de paquets de dades o la denegació de serveis són riscos inherents a les comunicacions, que poden comprometre la seguretat de qualsevol dels nodes presents en el sistema.

(13)Per defecte, les dades es transmeten per la xarxa en clar (sense xifrar) i els commutadors no filtren ni els nodes que s'hi connecten ni els paquets de dades que envien o reben.

1.3. Els serveis del sistema

Els **serveis d'un sistema informàtic** són totes aquelles funcionalitats que proporciona el sistema que tenen un valor directe[14] per als usuaris i per a l'organització en general. Representen l'objectiu principal pel qual s'implanta el sistema i justifiquen l'augment de costos, riscos i complexitat amb beneficis concrets en un o més aspectes del procés de la informació dins de l'organització.

(14)Cal diferenciar els serveis que ofereix el sistema als usuaris (que tenen l'objectiu d'afegir valor a les seves tasques) dels que són necessaris per al funcionament de la infraestructura de suport (que són de gestió i explotació dels recursos i no impliquen directament l'usuari).

Formen part dels serveis del sistema tot el programari que proveeix els usuaris de processos, capacitats o funcionalitats d'alt nivell que són rellevants per a l'objecte de negoci de l'organització, com, per exemple, la manipulació, l'emmagatzematge, la presentació o la comunicació d'informació. A diferència

del programari instal·lat en els recursos d'usuari, (per exemple, processadors de text, fulls de càlcul, eines de presentació, etc.), els serveis requereixen d'una infraestructura completa per tal d'accedir a les prestacions que ofereixen. El correu electrònic, la compartició de fitxers, la transmissió de veu o de vídeo, els serveis web, la missatgeria instantània o els jocs en línia són exemples de serveis d'ús habitual entre els usuaris.

Des de la perspectiva de la seguretat, es diferencien aquells serveis que es presten localment des del sistema mateix de l'organització, aquells que s'ofereixen des de l'exterior (com, per exemple, des d'internet) i aquells que combinen les característiques anteriors.

1.3.1. Els serveis locals

Tradicionalment, l'opció per defecte de qualsevol organització ha estat implantar tots els serveis necessaris en la infraestructura local, la qual cosa permet tenir el control total dels processos i dels serveis corporatius.

Els **serveis locals** són totes aquelles funcionalitats que es dissenyen, s'implanten, s'exploten i es mantenen dins de la infraestructura de l'organització. Aquest plantejament no implica necessàriament que sigui l'organització mateixa qui realitza les tasques d'administració o de gestió dels serveis[15], sinó que representa un objectiu en la concepció, ubicació i utilització d'aquests serveis.

[15] L'organització pot delegar les tasques d'administració del sistema a un tercer (per exemple, una empresa especialitzada) quan no pot (o no vol) assumir la gestió del seu sistema.

Vegem les particularitats d'implantar els serveis en el sistema de l'organització:

- L'organització manté el control total dels serveis que ofereix i pot ajustar de manera directa, dinàmica i precisa qualsevol dels aspectes de seguretat a qualsevol nivell (des dels components físics fins als d'aplicació).

- La implantació local dels serveis requereix la infraestructura necessària per a funcionar amb garanties de seguretat[16] i del personal capaç de construir-los i mantenir-los al llarg del temps[17], amb les implicacions econòmiques i organitzatives que això comporta.

- Les mesures de seguretat dels serveis locals han de ser proporcionals al context, coherents amb les solucions informàtiques implantades i administrades de manera proactiva per a garantir la consistència del servei i la protecció de la informació.

[16] Alguns serveis poden necessitar maquinari amb molta capacitat o amb configuracions específiques, i programari amb costos de llicència que depenen de la màquina on s'instal·la o del nombre d'usuaris que l'utilitzen.

[17] Si bé les eines actuals faciliten part de les tasques, és necessari un coneixement aprofundit per a garantir la seguretat i la coherència de la configuració.

És força habitual considerar el sistema local com un entorn segur i confiable per a desplegar els serveis de l'organització, però és un error que ha propiciat multitud d'incidents de seguretat (com, per exemple, el segrest, el robatori o

[18] La tendència actual a l'hora d'implantar mesures de seguretat en les organitzacions és considerar que el sistema local és un entorn poc o gens confiable.

la destrucció de dades) perquè els riscos i les amenaces no tenen fronteres i el sistema local pot no ser tant confiable com s'espera que sigui a efectes de seguretat informàtica[18].

1.3.2. Els serveis remots

La democratització de l'accés a internet de banda ampla ha propiciat la proliferació de l'oferta de serveis fora de les organitzacions, la qual cosa facilita, cada vegada més, la substitució o l'ampliació de tots aquells serveis que tradicionalment s'han implantat localment en el sistema mateix de les organitzacions.

Els **serveis remots** són tots aquells serveis que s'utilitzen des de l'organització (tot i que també podrien ser accessibles des de qualsevol altre lloc) però que no estan implantats en el seu sistema. Normalment, són oferts per proveïdors amb qui es contracta la prestació d'aquests serveis amb unes condicions específiques.

Les condicions poden estar relacionades amb el programari o les funcionalitats proveïdes, el suport i l'atenció a l'usuari, el manteniment i les mesures de seguretat, el cost dels serveis principals i complementaris, etc.

D'entre els exemples possibles, segurament els serveis de portal web i correu electrònic corporatiu són dels més habituals, però se'n podrien afegir molts més, com la connexió a escriptoris remots[19], els sistemes d'informació empresarials, les eines cooperatives i de treball en grup, la missatgeria instantània o la televisió sota demanda. En general, es pot considerar que els sistemes informàtics actuals estan preparats per utilitzar serveis remots a qualsevol nivell, com, per exemple, actualitzar el sistema operatiu d'un ordinador a partir dels dipòsits de programari remots que aprovisiona el fabricant mateix, o enviar i rebre missatges amb l'aplicació de missatgeria instantània d'un telèfon intel·ligent.

[19] L'accés a escriptoris remots és una tecnologia que permet interactuar amb un ordinador que es troba físicament distant com si s'estigués al davant, és a dir, es visualitza la mateixa interfície d'usuari i es poden executar les mateixes accions (inclús amb la redirecció d'impressores o de discos locals).

Si bé en la decisió d'externalitzar serveis s'acostumen a tenir en compte diversos factors (com els costos, el manteniment, la responsabilitat, etc.), la seguretat del servei i de la informació que processa és un aspecte d'especial importància. De fet, l'aprovisionament extern d'un servei no l'exclou dels riscos i les amenaces de seguretat, més aviat al contrari, perquè l'exposició als atacs augmenta pel fet de ser directament accessible des de qualsevol node d'internet. Per a mitigar aquesta situació, els proveïdors de servei implementen en els centres de dades[20] un ventall de mesures altament efectives per a garantir els seus serveis davant de riscos físics (com les intrusions, els incendis o els talls elèctrics) o lògics (com la protecció de vulnerabilitats, la salvaguarda de la informació, la prevenció contra atacs organitzats o el programari maliciós) amb tecnologies específiques i professionals qualificats que difícilment són abordables per moltes organitzacions.

[20] Els centres de dades (en anglès, *data centers*) són instal·lacions preparades per a allotjar una gran quantitat de recursos destinada a proveir de serveis els clients que els contracten.

Si bé l'externalització de serveis augmenta la dependència amb els proveïdors de tecnologia (entre altres aspectes), la ubicació real del servei no es considera actualment un factor determinant a l'hora de garantir la protecció de la informació. En qualsevol cas seran les mesures que es puguin implantar juntament amb el servei (ja sigui local o remot) les que el dotaran de garanties de seguretat reals[21].

(21)No és difícil trobar serveis en centres de dades més segurs i protegits que els equivalents implantats en sistemes locals. L'emmagatzematge i la compartició de fitxers n'és un bon exemple.

1.3.3. Els serveis híbrids

La implantació de serveis locals i remots acostumen a donar resposta a bona part dels requisits habituals de les organitzacions, però es poden donar circumstàncies que necessitin solucions que es trobin a mig camí entre totes dues opcions.

Els **serveis híbrids** són aquells serveis que necessiten disposar de recursos locals i remots per a acomplir la seva funció, eventualment, de manera distribuïda o descentralitzada. Si bé aquesta dualitat estableix dependències perquè el servei sigui efectiu, obre un ventall de possibilitats noves que poden ajudar a resoldre requisits particulars de l'organització.

Vegem alguns exemples d'aquests serveis:

- És possible que sigui necessari publicar a l'exterior algun servei de l'organització amb l'objectiu que altres usuaris o serveis hi puguin accedir. Els casos més habituals corresponen als serveis de portal web i correu electrònic corporatiu amb domini de l'organització, però n'hi pot haver molts d'altres. L'exposició de serveis a l'exterior suposa un risc elevat per al sistema, tant per l'augment de requisits de seguretat com per l'ampliació de la superfície d'atac[22].

(22)Els serveis web i de correu electrònic se situen habitualment entre els més atacats, i moltes vegades serveixen de plataforma per atacar altres sistemes, siguin locals o remots.

- De vegades caldrà que els usuaris que es troben a l'exterior de l'organització puguin utilitzar els recursos del sistema local com si es trobessin físicament dins de les instal·lacions, com seria el cas dels comercials que visiten els clients (i han d'accedir als serveis interns) o també del teletreball dels empleats d'una organització (que accedeixen des de casa, sovint amb tecnologies de connexió a escriptoris remots). La implementació d'aquests serveis també suposa un risc elevat per a l'organització perquè permeten l'accés al sistema (i a una informació que pot ser privilegiada o confidencial) des de l'exterior, per no esmentar les facilitats que s'obren per a la propagació de programari maliciós.

- De vegades serà necessari connectar permanentment dos sistemes informàtics que es troben físicament distants l'un de l'altre però accessibles a través d'un mitjà que pot ser hostil (com internet). Seria el cas d'una organització que tingui diferents oficines, seus o sucursals repartides al

llarg del territori i que, per les circumstàncies del seu funcionament, han d'intercanviar dades de manera automàtica i permanent. Com en el cas anterior, els riscos per la seguretat augmenten a causa de l'ampliació de la superfície d'atac i de la facilitat de propagació d'incidents entre tots els sistemes connectats (que actuen com si fos un de sol).

- També és possible que un servei necessiti distribuir el processament de la informació entre recursos interns i externs, de manera que una part del procés es realitzi en remot i l'altra en local. Per exemple, seria el cas d'aquells serveis de computació distribuïda on es divideix i reparteix la resolució d'una tasca (eventualment complexa) entre dos o més recursos, com les aplicacions d'igual a igual[23] o projectes com SETI@Home[24]. Els riscos per la seguretat es mantenen elevats a causa de la necessitat d'interacció entre sistemes distants (i potser desconeguts) i l'automatització d'aquesta interacció (no sempre és fàcil detectar les accions que realitza), però a la vegada variable en funció del servei que s'estigui executant (per exemple, els serveis de compartició de fitxers poden comprometre més fàcilment la informació que els serveis dedicats al càlcul massiu de dades).

(23)El paradigma de computació d'igual a igual (en anglès *peer-to-peer*, P2P) es fonamenta en una xarxa de nodes que poden actuar com a client o servidor a la vegada. Un dels usos més populars és la compartició de fitxers.

(24)El projecte SETI@Home és una gran xarxa de nodes particulars (tothom s'hi pot adherir lliurement) que utilitza els moments d'inactivitat dels equips informàtics per a processar senyals de ràdio de l'espai exterior a partir de les dades en brut obtingudes per les antenes.

(25)La internet de les coses, més conegut com a IoT (la sigla de l'anglès d'*Internet of things*) representa la connexió dels dispositius quotidians o comuns a la xarxa (eventualment internet), de manera que puguin interactuar amb altres i ser controlats o monitorats en remot. Són exemples d'aquests dispositius les càmeres de vigilància, els tancaments de portes, els diferents sensors (de temperatura, pressió, etc.) i un llarg etcètera cada vegada més nombrós.

Tot i que aquests serveis (o possibles variants) són força utilitzats atès que són relativament fàcils d'implementar amb el maquinari i el programari actuals, cada vegada és més recurrent la reconversió en serveis remots oferts per proveïdors de servei. Això és així perquè la indústria de l'externalització de serveis informàtics és un mercat que no deixa d'enginyar tecnologies noves que faciliten cada vegada més la ubiqüitat dels serveis i reivindiquen facilitats tant en l'explotació dels serveis com en la contractació i la gestió del cost, a la vegada que mantenen les garanties de funcionament pròpies dels serveis remots. Per exemple, seria el cas de la connexió remota al sistema de l'organització o a les plataformes per a administrar o centralitzar els dispositius de la internet de les coses[25].

No cal oblidar que la utilització d'aquests serveis suposa l'establiment d'una dependència amb el proveïdor que s'ha de plasmar en un contracte de prestació de serveis, on hauria d'haver una menció especial per la seguretat i la protecció de la informació que s'hi processa.

1.4. L'estructura i el funcionament del sistema

L'estructura d'un sistema informàtic pot ser tant simple o complexa com els requisits que ha de resoldre. El sistema ha de ser un reflex de l'organització i evolucionar al mateix ritme, sense menystenir les possibilitats que, al seu torn, poden oferir els avenços tecnològics per a afavorir o millorar els objectius, el funcionament o la capacitat de l'organització.

Tot i la diversitat d'escenaris possibles, els sistemes informàtics segueixen una estructura funcional comuna, tant des del vessant d'infraestructura com del de serveis.

1.4.1. El disseny i la operativa de la infraestructura

A continuació es presenta, de manera simplificada, el funcionament general de la infraestructura dels sistemes informàtics:

- En general, els recursos d'usuari (per exemple, ordinadors) i els recursos de servei (per exemple, servidors) es connecten als recursos de comunicació (per exemple, commutadors) creant un segment de xarxa que habilita la comunicació entre tots ells. Connectant dos o més commutadors s'estén o s'amplia el segment de xarxa cap a més nodes.

- En els segments de xarxa sense fils (com, per exemple, wifi[26]), els nodes es connecten a la xarxa (que s'identifica amb un SSID[27]) a través de punts d'accés[28]. Com qualsevol altre recurs, per a habilitar la comunicació amb la resta de nodes només cal connectar els punts d'accés als commutadors.

- La interfície de xarxa de cada dispositiu té dues adreces: l'adreça física (anomenada MAC[29]), que identifica el dispositiu però no habilita la comunicació a nivell global, i l'adreça lògica, que s'assigna d'acord amb la ubicació real del node connectat i les característiques de la xarxa on es troba, la qual cosa habilita l'enviament i la recepció de paquets de dades amb altres nodes, ja siguin locals o remots.

- En el model de comunicacions més estès avui dia en tot tipus de xarxes, el model TCP/IP[30], l'adreçament lògic reposa sobre les adreces IP[31], que juntament amb la màscara de xarxa[32], habiliten la comunicació directa entre els nodes que es troben en la mateixa xarxa[33] o a través d'un encaminador si es troben en xarxes diferents. En general, la majoria de sistemes tenen un recurs de servei (per exemple, un encaminador o un servidor) que distribueix automàticament les adreces lògiques als dispositius que s'hi connecten utilitzant protocols específics d'assignació d'adreces (el més habitual és DHCP[34], tot i que n'hi ha d'altres, com BOOTP[35]).

(26)Wifi és l'abreviatura de *wireless fidelity*, un tipus de xarxa sense fils molt estesa i que s'utilitza habitualment per a connectar dispositius d'usuari a la xarxa d'una organització.

(27)SSID és l'acrònim anglès de *service set identifier*.

(28)Els punts d'accés sense fils es coneixen popularment com AP, l'acrònim anglès d'*access point*.

(29)L'adreça física o adreça MAC (acrònim de l'anglès *media access control*) és un identificador de 48 bits únic per cada interfície de xarxa, que es representa amb un nombre en format hexadecimal (per exemple, 12:34:56:78:9A:BC) i s'assigna en funció del fabricant i del tipus de dispositiu.

(30)TCP/IP és el model de comunicacions resultant de la creació d'internet, i deu el seu nom a la conjunció dels seus dos protocols principals: TCP (*transport control protocol*) i IP (*internet protocol*).

(31)L'adreça IP és un identificador de 32 bits que es representa amb quatre números decimals (entre 0 i 254) separats per punts (per exemple, 192.168.21.37). S'estructuren en classes i alguns rangs estan reservats a propòsits específics.

- Sota la perspectiva general de la seguretat, l'adreçament IP pot ser públic o privat. Les adreces públiques s'assignen a nodes connectats a internet, perquè s'hi pugui accedir directament des de qualsevol altre node. En canvi, les adreces privades estan reservades i els paquets amb aquestes destinacions no surten mai de la xarxa local (els encaminadors no els transfereixen cap a internet), per la qual cosa tots els particulars i les organitzacions poden utilitzar-les per a les comunicacions internes[36]. D'acord amb l'estàndard, les adreces privades que s'exclouen de l'àmbit d'internet són 10.0.0.0/8, 172.16.0.0/12 i 192.168.0.0/16.

(32)La màscara de xarxa actua com a filtre d'una adreça IP per a identificar el node dins de la xarxa. Per exemple, 192.168.21.37/24 indica que els 24 primers bits corresponen a la xarxa (màscara) i la resta al node. És a dir, l'adreça correspon a l'ordinador 37 de la xarxa 192.168.21.0/24.

(33)Els nodes 192.168.12.77/24 i 192.168.21.78/24 no es podran comunicar directament entre si perquè es troben en xarxes diferents: el primer està a la xarxa 192.168.12.0/24 i el segon a 192.168.21.0/24.

(34)DHCP és la sigla de l'anglès *dynamic host configuration protocol*.

(35)BOOTP és l'acrònim de l'anglès *bootstrap protocol*.

(36)Molts encaminadors estan configurats de fàbrica amb l'adreçament privat 192.168.1.0/24 per a la xarxa interna.

- Per a connectar el sistema a internet és necessari un encaminador, que és el dispositiu que assegura l'intercanvi de paquets entre les xarxes d'àmbit públic (internet) i el privat de l'organització. Per a realitzar la seva funció, disposa d'una adreça IP privada en la interfície de xarxa local i d'una adreça IP pública en la interfície connectada a internet (que assigna el proveïdor de telecomunicacions[37]). Per tal que els nodes de la xarxa local es puguin connectar amb recursos externs, cal que tinguin configurada l'adreça IP de l'encaminador com a porta d'enllaç[38] a d'altres xarxes (que és una de les opcions de configuració dels protocols d'assignació d'adreces).

(37)De vegades es fa referència al proveïdor de telecomunicacions amb l'acrònim anglès ISP (*internet service provider*).

(38)La porta d'enllaç es coneix popularment per l'anglès *gateway*.

- Per a localitzar els recursos d'internet és habitual utilitzar el servei DNS[39], que resol les adreces públiques dels nodes als quals es vol accedir a partir del seu nom de domini[40]. En general, el proveïdor de telecomunicacions assigna els serveis DNS a la interfície pública de l'encaminador (tot i que es poden utilitzar altres servidors diferents als assignats), per a que pugui retransmetre les peticions dels nodes de la xarxa local (per a fer-ho, cal que els nodes interns tinguin configurada l'adreça privada de l'encaminador com a servidor DNS, un altra de les opcions de configuració dels protocols d'assignació d'adreces).

(39)DNS és l'acrònim de l'anglès *domain name system*.

(40)El nom complet de domini es coneix com FQDN, l'acrònim anglès de *fully qualified domain name*, que consisteix en el nom del node seguit dels dominis als quals pertany, per ordre jeràrquic i separats per punts.

1.4.2. El disseny i l'operativa dels serveis

Vegem ara com és el funcionament habitual de la prestació de serveis en els sistemes informàtics:

- Tot i que hi ha diferents paradigmes de prestació de serveis, un dels més utilitzats és l'anomenat *client/servidor*, on un dels recursos (el servidor) està a l'espera de rebre les peticions dels altres recursos (els clients), que són els qui prenen la iniciativa de sol·licitar el servei i assumeixen la part activa de la connexió. Un cop rebuda la petició, el servidor pot analitzar-ne la conveniència i l'adequació abans de prestar (o no) el servei. Per exemple, la navegació web segueix el paradigma client/servidor perquè és l'usuari (client) qui demana al servidor web que li transmeti el contingut d'algun dels recursos web que posseeix.

- La majoria de vegades, per a poder accedir i interactuar amb els serveis que s'ofereixen és necessari disposar d'una aplicació adequada (ja sigui estàndard o creada *ad hoc*), sense la qual o bé no serà possible accedir al servei, o bé serà complicat o feixuc interactuar-hi. Per exemple, seria el cas del navegador web, que permet descodificar el llenguatge HTML[41] de les pàgines web per a mostrar visualment el resultat de manera amigable per als humans. També seria el cas dels clients de correu electrònic, que presenten de manera organitzada la llista de missatges i el contingut d'aquells que es volen visualitzar.

- En el model TCP/IP, cada servei té associat un protocol d'aplicació que estableix els requisits necessaris per interactuar amb el servei i obtenir el resultat esperat. Aquests protocols són estàndards i molt propers a l'usuari, com, per exemple, HTTP[42] (per a la transferència de pàgines web), FTP[43] (per a la transferència de fitxers), NTP[44] (per a sincronitzar el rellotge dels equips), POP3[45] (per a recuperar els missatges de la bústia), SMTP[46] (per a transmetre missatges electrònics) i un llarg etcètera de protocols que resolen multitud situacions concretes.

- Els protocols d'aplicació requereixen utilitzar protocols de transport per a establir la comunicació entre ambdós extrems. De protocols de transport n'hi ha dos en el model TCP/IP, el TCP[47], que és un protocol que s'assegura que tots els paquets de dades que s'envien arriben a destinació (entre altres mesures), i l'UDP[48], que és més lleuger i ràpid però no garanteix que el receptor rebi tots els paquets que s'envien. Si bé la majoria de protocols d'aplicació utilitzen TCP en les comunicacions per a garantir el servei, d'altres han optat per l'UDP per la rapidesa que ofereix en la transmissió tot i que es perdi algun paquet (per exemple, els serveis en temps real).

(41)HTML és l'acrònim de l'anglès *hypertext markup language*, el llenguatge utilitzat per crear i distribuir pàgines web.

(42)HTTP és l'acrònim de l'anglès *hypertext transfer protocol*.

(43)FTP és l'acrònim de l'anglès *file transfer protocol*.

(44)NTP és l'acrònim de l'anglès *network time protocol*.

(45)POP3 és l'acrònim de l'anglès *post office protocol*, en la tercera versió del protocol.

(46)STMP és l'acrònim de l'anglès *simple mail transfer protocol*.

(47)TCP és l'acrònim de l'anglès *transport control protocol*.

(48)UDP és l'acrònim de l'anglès *user datagram protocol*.

- Cada servei té assignat un port concret sobre el qual presta la seva funció, és a dir, una porta d'entrada oberta en la qual espera les peticions de servei. Els ports prenen la forma d'un número entre 0 i 65535 (ambdós inclosos) i estan associats als protocols de transport. Per exemple, el servei DNS utilitza el port 53 dels protocols TCP i UDP (TCP/53 i UDP/53), el servei HTTP utilitza el port 80 del protocol TCP (TCP/80), el servei SMTP utilitza el port 25 del protocol TCP (TCP/25), el servei RDP[49] utilitza el port 3389 del protocol TCP (TCP/3389), el servei SSH[50] utilitza el port 22 del protocol TCP (TCP/22), el servei SMB[51] utilitza el port 445 del protocol TCP (TCP/445) o el servei IPP[52] utilitza el port 631 del protocol TCP (TCP/631).

- Si bé els estàndards defineixen els ports que ha d'utilitzar cada servei (com els vistos anteriorment), a la pràctica res no impedeix que es puguin canviar per d'altres. Per exemple, no és estrany trobar servidors web que ofereixin el servei HTTP des del port TCP/8080, enlloc de l'estàndard TCP/80.

- Per a poder accedir a un servei cal conèixer l'adreça IP del servidor, els protocols d'aplicació i de transport que utilitza, i també el port sobre el qual està a l'espera de peticions[53]. Amb aquesta informació, cal enviar els paquets de dades necessaris amb l'estructura, el format i les dades que requereixin els protocols al port concret de l'adreça IP del servidor. Si tot és correcte, el servidor retornarà una resposta d'acord amb la definició dels protocols a l'adreça IP del client que ha sol·licitat el servei, i així successivament fins a completar tota la interacció.

(49)RDP és l'acrònim de l'anglès *remote desktop protocol*, un protocol que permet la connexió a escriptoris remots basat sobretot en MS Windows.

(50)SSH és l'acrònim de l'anglès *secure shell*, una interfície d'administració pròpia dels sistemes GNU/Linux.

(51)SMB és l'acrònim de *server message block*, un protocol per a compartir fitxers en una xarxa local.

(52)IPP és l'acrònim d'*internet printing protocol*, un protocol per a imprimir documents en una impressora en xarxa.

(53)Un servidor tindrà tants ports oberts com serveis està prestant.

1.4.3. La seguretat del sistema informàtic

Com es pot entreveure en les seccions anteriors, difícilment pot haver cap mecanisme de seguretat que pugui cobrir totes les necessitats de seguretat (ni tan sols la majoria) d'un sistema informàtic que pot ser tan divers i complex com les amenaces i els riscos als quals està exposat.

Per a garantir la seguretat de la informació no hi ha cap altra via que no sigui combinar múltiples mecanismes de seguretat al llarg i ample de tot el sistema informàtic de manera adequada, coherent i proporcional.

Moltes vegades, la implantació de mesures de seguretat segueix un model per capes o nivells (des del suport físic fins al factor humà), però amb independència del desplegament que se'n faci (que haurà de ser connex amb el context), l'important és garantir tota la cadena de seguretat de la informació de principi a final (per exemple, creació, emmagatzematge, accés, modificació i destrucció).

Tot i amb això, també caldrà tenir en compte altres aspectes que poden influir en la definició i plantejament de la seguretat del sistema:

- L'evolució (o l'actualització) de la tecnologia implantada en el sistema pot comportar canvis en el funcionament o l'operativa dels components, i requerir l'ajustament de les mesures de seguretat (o inclús promoure'n la implantació de noves). Per exemple, l'actualització del programari de serveis pot descartar la utilització dels protocols d'aplicació que es considerin insegurs, obsolets o compromesos. És el cas de les primeres versions dels protocols SMB o SSH, entre molts d'altres.

- En general, les noves tecnologies presenten requisits de seguretat més exigents, per tant la incorporació al sistema pot provocar la necessitat d'ajustar o d'implementar noves mesures per a garantir-ne la cohesió i el funcionament global. Per exemple, els serveis de compartició de fitxers[54] s'estan substituint progressivament per serveis en línia als quals s'accedeix per mitjà d'un navegador web.

(54)Els serveis de fitxers utilitzen normalment protocols orientats a una xarxa local, com SMB o NFS.

- L'organització evoluciona amb el temps i el sistema informàtic ha de reflectir alguns d'aquests canvis. De vegades només serà necessari realitzar ajustaments en la configuració de seguretat (per exemple, l'actualització dels permisos d'accés a la informació), però en d'altres potser caldrà donar resposta a noves necessitats que requereixin la reavaluació completa de la política de seguretat del sistema (per exemple, implantar nous serveis que hagin de ser accessibles des de l'exterior de l'organització).

- Els riscos i les amenaces contra la seguretat de qualsevol dels components del sistema també evolucionen (i perfeccionen) amb el temps, per tant haurà de ser habitual la revisió periòdica de la política de seguretat del sistema per a considerar les novetats que van sorgint. Per exemple, és ben coneguda la capacitat que té el programari maliciós d'explotar les vulnerabilitats de dia zero[55].

(55)Els atacs de dia zero aprofiten la finestra de temps existent entre la identificació d'una vulnerabilitat i la publicació de l'actualització que la corregeix.

Sovint, quan es tracta la seguretat dels sistemes informàtics s'acostuma a citar una frase que, amb el temps, s'ha convertit en tota una referència:

> «L'únic sistema segur és aquell que està apagat i desconnectat, enterrat en un refugi de ciment, envoltat per gas verinós i custodiat per guardians ben pagats i molt ben armats. Tot i així, jo no apostaria la meva vida per ell».
>
> Prof. Eugene Spafford (Universitat Purdue)

Certament, aconseguir que un sistema informàtic sigui completament segur és impossible, però decididament es poden implementar polítiques i mecanismes que ofereixin garanties suficients, com veurem en les properes seccions.

2. La seguretat física i perimetral

Sense cap mena de dubte, un dels primers aspectes que cal considerar a l'hora de protegir la informació és l'accés al sistema informàtic. De res no serveix implementar les tecnologies i les mesures de seguretat més eficaces si es descuiden aspectes tant bàsics com, per exemple, negligir el tancament amb clau de la sala de servidors o deixar a la vista les credencials d'usuari.

En les properes seccions s'abordaran tant els aspectes físics de seguretat com tots aquells aspectes lògics relacionats amb l'accés i la connexió a la infraestructura del sistema.

2.1. Els conceptes bàsics de seguretat

Els mecanismes de seguretat de la infraestructura estan orientats a protegir els diferents recursos presents en el sistema, tant en el vessant material com en el d'explotació (això és, la capa bàsica de programari que habilita la utilització dels recursos).

Sovint, moltes d'aquestes mesures estan encaminades a controlar l'accés (físic o lògic) als diferents recursos (d'usuari, de servei o de comunicacions), de manera que tots els intents fraudulents[56] per accedir siguin detectats, controlats i filtrats, i s'eviti, en la mesura del possible, la propagació dels incidents cap a la resta del sistema.

[56] L'establiment de polítiques de seguretat ha de permetre, precisament, l'establiment de criteris clars, coherents i ben definits respecte a l'accés als recursos.

Les actuacions que es poden portar a terme per a protegir la infraestructura del sistema no estan exclusivament lligades a la implementació de mesures tècniques en un o més dels components, sinó que també poden requerir les accions dels usuaris o, inclús, donar forma a l'estructura física o lògica del sistema informàtic. Per exemple, es poden crear zones amb diferents requisits de seguretat, on l'intercanvi de comunicacions pot estar filtrat o directament bloquejat.

2.2. La seguretat física del sistema

Un dels principis bàsics de la seguretat de tota infraestructura és la protecció física dels recursos, no solament davant d'accessos no autoritzats, sinó també davant dels riscos físics i naturals inherents a la localització on es troben ubicats.

Vegem alguns d'aquests riscos:

- El lliure accés a la zona on es troben els recursos per part de persones no autoritzades és un risc de robatori, manipulació o destrucció que es pot resoldre tancant l'espai i limitant-ne l'accés. La sala de servidors[57] és un dels exemples més habituals, però l'accés als armaris de dades o de comunicacions (entre d'altres) també hauria d'estar controlat perquè són accessos directes al sistema.

(57)Quan la importància de la informació emmagatzemada ho requereix, les sales de servidors es poden protegir amb controls biomètrics d'entrada i amb materials i aïllaments de tot tipus.

- La protecció contra els riscos inherents a tot espai físic, com, per exemple, els incendis o les inundacions. Si bé el maquinari té un valor econòmic tangible, el que realment té valor (potser incalculable) és la informació emmagatzemada en el sistema (la pèrdua total de la informació podria comprometre l'activitat de l'organització). Els servidors acostumen a centralitzar la informació més important, per tant són un dels principals objectius que cal protegir.

- Les fluctuacions o els talls en el subministrament elèctric són un dels riscos físics per a qualsevol sistema. Els pics de tensió poden ser nefastos per a qualsevol material electrònic i poden requerir la substitució d'algun dels components perquè tornin a funcionar (per exemple, la font d'alimentació). En general, es considera que s'haurien de protegir els recursos de servei (principalment, servidors) i de comunicacions (principalment, commutadors, encaminadors i punts d'accés) amb sistemes d'alimentació ininterrompuda[58].

(58)Els sistemes d'alimentació ininterrompuda (SAI) són dispositius que filtren les sobretensions del corrent elèctric. Poden incorporar bateries per a mantenir l'alimentació durant un temps en cas de tall en el subministrament elèctric.

- Els components interns dels dispositius també poden fallar per molts motius i deixar el recurs fora de servei ràpidament. Els servidors són, una vegada més, el primer objectiu que cal protegir aprofitant la capacitat que tenen per redundar els components més susceptibles de fallada (com, per exemple, la font d'alimentació i els discos d'emmagatzematge) i així mantenir la continuïtat dels serveis.

- La pèrdua o la fallada total del sistema també és un escenari que s'ha de preveure, per molt fatalista que pugui semblar (de fet, el funcionament de l'organització en pot dependre completament). Realitzar regularment còpies de seguretat[59] de la informació més important és una mesura imprescindible i totalment ineludible en qualsevol sistema (ja sigui domèstic o corporatiu). Les exigències i els plantejaments poden ser molt diversos en funció del context i de la informació que cal salvaguardar, però una estratègia simple i popular és l'anomenada 3-2-1, que sosté el manteniment de tres còpies de les dades (la dades del sistema en producció i dues més) en dos suports diferents, amb una d'elles fora de les instal·lacions de l'organització[60].

(59)Les còpies de seguretat es coneixen popularment per l'anglès *backup*.

(60)Cal tenir en compte que, amb la proliferació dels serveis remots (sovint anomenats «al núvol»), també s'han diversificat les estratègies de còpies de seguretat (algunes d'elles reinterpretant la 3-2-1).

Segurament, els centres de dades són l'exemple més clar de com s'ha de protegir un sistema contra tot tipus de riscos, atès que implementen les bones o millors pràctiques del sector (per exemple, controls d'accés a les instal·lacions,

materials específics contra degradacions diverses, regulació tèrmica de temperatura i d'humitat, protecció contra alteracions en el corrent elèctric, múltiples sistemes d'alta disponibilitat, etc.), a costa de contrapartides econòmiques molt importants.

La implementació de totes les mesures de seguretat possibles pot ser que la majoria d'organitzacions no la pugui assumir, per tant, s'imposa el principi de proporcionalitat a l'hora de ponderar els requisits que té el sistema i seleccionar els mecanismes adequats, necessaris i coherents amb la casuística de l'organització.

2.3. La seguretat dels recursos

Mantenir la informació segura al llarg de la cadena de procés és responsabilitat de tots els recursos implicats, de principi a final. Considerar que el sistema és segur per haver implantat mecanismes en alguns dels recursos és negligir la concepció global del que ha de ser un entorn segur i confiable tot facilitant la materialització dels riscos i la proliferació dels incidents de seguretat.

Els mecanismes que pretenen assegurar els recursos del sistema persegueixen un doble objectiu, d'una banda, protegir el propi recurs del procés que realitza, i d'una altra banda, protegir-lo del sistema o dels altres recursos amb els quals pugui tenir interacció.

2.3.1. Els recursos d'usuari

Els recursos d'usuari són un dels objectius a l'hora de protegir la cadena de seguretat de la informació, perquè s'ubiquen a l'extrem (l'inici i el final) de bona part de les transaccions del sistema, executen diversitat d'aplicacions que connecten amb serveis d'entorns molt diferents que manipulen tot tipus de dades, no sempre disposen de tots els mecanismes de seguretat necessaris per a protegir la informació, i l'usuari que utilitza el recurs no té perquè conèixer totes les actuacions que ha de realitzar per a garantir, en tot moment, la seguretat de les transaccions que realitza.

La diversitat de riscos que han d'afrontar els recursos d'usuari són ben coneguts i alimenten la proliferació de tot tipus d'amenaces que els exploten. La formació dels usuaris en matèria de seguretat i el control dels recursos que utilitzen són dos dels pilars fonamentals per a assegurar aquest extrem de la cadena, però l'adopció ràpida de les polítiques BYOD en les organitzacions promou la implantació de mesures específiques per a contenir aquest nou es-

(61)MDM és la sigla de *mobile device management*, un programari que permet gestionar, assegurar i monitorar dispositius mòbils.

cenari (per exemple, la segmentació de la xarxa sense fils de convidats o la implantació de sistemes MDM[61] per acceptar dispositius que hagin d'accedir als serveis del sistema).

Vegem algunes de les mesures de seguretat habituals que són aplicables a gairebé qualsevol dispositiu d'usuari:

- Mantenir el sistema operatiu i totes les aplicacions sempre actualitzades.
- No descarregar ni instal·lar aplicacions d'orígens desconeguts.
- Utilitzar el compte de supervisor únicament per a realitzar tasques administratives, com, per exemple, la configuració del dispositiu o la instal·lació d'aplicacions.
- Utilitzar claus d'accés robustes[62].
- Si és possible, implementar controls d'accés a la informació o a les aplicacions.
- Bloquejar la interfície d'interacció amb el sistema quan no s'hagi d'utilitzar.
- Instal·lar i configurar mecanismes de protecció contra atacs (per exemple, un tallafocs local[63]) i programari maliciós (per exemple, un antivirus).
- Realitzar còpies de seguretat de la informació en dispositius externs de manera regular.
- Mantenir la prudència a l'hora d'interactuar amb els serveis, especialment amb aquells implantats al núvol. Cal revisar detingudament el contracte de prestació dels serveis remots per a garantir que les dades que es confien no són objecte d'activitats inadequades.
- Xifrar amb claus i algoritmes robustos[64] la informació que s'hagi d'emmagatzemar en els dispositius (especialment aquells que siguin mòbils).
- Si escau, fixar els dispositius mòbils amb cadenes o altres suports per a evitar els possibles robatoris.

(62) Els mínims que es consideren per a la robustesa de les claus és cada vegada més alt. Actualment, es considera robusta una clau formada per una frase que inclogui tot tipus de símbols.

(63) En aquest context, el tallafocs és un programari que filtra les connexions de la xarxa cap al dispositiu (i viceversa), i en descarta aquelles que puguin ser sospitoses o fraudulentes.

(64) Per exemple, el sistema operatiu pot xifrar completament un volum de dades, o alguns llapis de memòria incorporen zones protegides dins de l'espai d'emmagatzematge.

Aquestes mesures són genèriques i no exclouen la consideració d'altres que puguin ser aplicables a contextos específics, com podria ser el cas d'alguns àmbits públics (per exemple, els sectors educatiu, sanitari o l'Administració pública en general) o privats (per exemple, organitzacions d'investigació i desenvolupament o empreses d'alta tecnologia).

Tot i que alguns mecanismes de seguretat es poden automatitzar, com, per exemple, la cerca de virus, l'actualització del sistema o la realització de còpies de seguretat, l'usuari es manté en la primera línia de protecció de la cadena de seguretat i les actuacions que realitza poden ser determinants. La formació dels usuaris és tant decisiva com la creació d'hàbits i costums en matèria de seguretat i protecció de la informació dins de l'organització.

2.3.2. Els recursos de servei

Els recursos de servei comparteixen la funcionalitat amb la resta del sistema, per la qual cosa estan més exposats als riscos i que fallin genera un impacte més gran en l'organització que la disrupció eventual d'altres recursos (com els d'usuari). Garantir l'estabilitat i la disponibilitat del recurs, i preservar les característiques i les propietats dels serveis que presta són objectius essencials.

Els riscos als quals pot estar sotmès un recurs de servei poden ser molt diversos, des de la fallada d'algun dels components materials del recurs que aturin completament el funcionament (com la fallada de la font d'alimentació o d'un disc d'emmagatzematge), fins a la vulneració d'un o més dels components lògics que puguin comprometre la informació que processa (per l'acció de programari maliciós present en els recursos d'usuari).

Els dispositius compartits (com les impressores o els projectors) acostumen a tenir poques opcions de seguretat perquè la seva funció és limitada i no acostumen a suposar un gran risc ni per a la seva pròpia seguretat ni per a la del sistema en general. La majoria de vegades, les opcions es limiten a l'activació d'unes poques mesures, com el bloqueig de la interfície de configuració amb una clau d'accés, la restricció de la prestació del servei a un conjunt de recursos concret o la limitació de les funcions segons el perfil d'usuari.

En canvi, els servidors són els recursos de servei que més riscos de seguretat acumulen, atesa la centralització de dades i les funcions dins del sistema. Vegem algunes de les mesures més habituals:

- En el pla físic, els servidors tenen caixes amb ventilació i fonts d'alimentació millorades, i també un pany per tancar amb clau l'accés als components interns. A més, n'hi ha tant en el format torre, per a situar-se preferentment al terra o sobre una plataforma, o en format *rack*, per a ser

instal·lats dins d'un armari de dades (que estan tancats amb clau i ubicats en espais menys accessibles). Alguns servidors de torre també es poden instal·lar en aquests armaris gràcies a unes guies opcionals.

- Respecte al maquinari, les mesures de seguretat principals se centren a redundar els components crítics del servidor per tal que siguin tolerants a les fallades (quan un component falla, n'hi ha un altre que permet mantenir el funcionament sense interrupcions). Per exemple, és habitual disposar de més d'una font d'alimentació elèctrica instal·lada o més d'una interfície de connexió a la xarxa. També disposen de diversos discos (controlats per maquinari o per programari) sobre els quals es distribueixen les dades[65] de tal manera que, si un falla, no només no s'atura el servei ni es perden les dades, sinó que si se substitueix el disc problemàtic per un de nou, s'hi escriuen les dades que hauria de tenir (a partir de la informació de la resta de discos) i es recupera l'estabilitat que s'havia perdut.

(65)Un dels mecanismes de redundància més utilitzats és RAID, acrònim de l'anglès *redundant array of inexpensive disks*, que tant es pot implementar per maquinari com per programari. Ofereix diversos nivells de redundància d'acord amb els discos disponibles i els objectius que es vulguin aconseguir (rendiment, protecció, etc.).

- Les dades no sempre han d'estar físicament en el mateix servidor que processa les transaccions, sinó que poden ubicar-se en altres recursos de servei accessibles a través de la xarxa (i que poden estar en ubicacions encara més segures). Seria el cas de l'emmagatzematge en xarxa[66] o de les xarxes d'emmagatzematge[67], que si bé pot semblar un joc de paraules, són dos conceptes completament diferents: mentre que el primer actua com un servidor de fitxers, el segon es presenta com un disc local però l'accés es redirigeix cap a la xarxa d'emmagatzematge. Ambdues opcions afegeixen complexitat al sistema i, com qualsevol altre servei, requereixen de mesures de seguretat específiques (especialment les xarxes d'emmagatzematge, on és fàcil cometre errors de configuració que puguin comprometre la seguretat).

(66)L'emmagatzematge en xarxa és conegut per la sigla NAS, de l'anglès *network attached storage*.

(67)Les xarxes d'emmagatzematge es coneixen amb la sigla SAN, de l'anglès *storage area network*.

- Pel que fa al programari, implantar solucions de proveïdors contrastats i que ofereixin un bon suport, adequades a la funció que han de realitzar i descartant qualsevol opció que no formi part de l'àmbit empresarial són aspectes essencials per a garantir-ne la seguretat. Si bé l'actualització regular del programari és vital per a corregir vulnerabilitats, també és important que la configuració (especialment del sistema operatiu o de l'hipervisor) no deixi marge a la explotació de riscos (per exemple, amb mecanismes d'aïllament i control dels processos en execució[68]), per la qual cosa és possible requerir els coneixements de professionals de l'àrea per a garantir aquests aspectes de seguretat.

(68)Els sistemes operatius de nivell empresarial poden controlar l'activitat que realitzen els processos que s'hi executen i bloquejar-los si les accions que pretenen realitzar no corresponen amb el seu perfil (per exemple, si intenten accedir a un fitxer de configuració que no és propi).

(69)Hi ha llistes de recursos d'internet que són coneguts perquè són l'origen d'atacs o de la difusió de correu brossa o de programari maliciós.

- Un dels serveis imprescindibles que tot servidor ha de mantenir sempre actiu i ben configurat és el tallafocs. El filtratge que proporciona de les connexions garanteix que només siguin accessibles els ports dels serveis que s'estan prestant, que es descarten els paquets de dades corruptes o fraudulents i que les comunicacions dels clients segueixen els patrons d'interacció previstos. El tallafocs permet el filtratge de les connexions en

qualsevol sentit de la comunicació, de manera que també és possible evitar que la instal·lació d'un servei fraudulent en el servidor pugui contactar o enviar dades a sistemes desconeguts, eventualment hostils[69].

Els recursos de servei són l'objecte habitual de múltiples amenaces de seguretat però, en general, hi ha suficients mecanismes de seguretat en pràcticament tots els nivells com per a oferir garanties de protecció de la informació, amb el benentès d'adequar-les i configurar-les d'acord amb el context i l'exposició que tenen.

2.3.3. Els recursos de comunicació

Els recursos de comunicació estableixen canals per a la transmissió de dades entre extrems, però aquesta facilitat també exposa els recursos del sistema i les dades que s'intercanvien entre ells a diversitat de riscos. Evitar els accessos il·lícits i el control fraudulent dels recursos de comunicació són objectius habituals de la política de seguretat.

Vegem algunes de les disfuncions que poden patir els components bàsics de les comunicacions i les implicacions per a la seguretat de la informació:

- El cablejat es pot malmetre amb el temps, especialment els connectors i els cables dels recursos. No sempre és fàcil identificar l'element que genera la fallada (de vegades, poden ser parcials o intermitents), però poden provocar la corrupció de les dades que es transmeten o inclús la pèrdua total de la transmissió.

- Les interfícies de xarxa també poden presentar problemes de funcionament, sobretot a causa d'una fallada dels components electrònics que les integren. A més de la possibilitat de pèrdua o corrupció de les dades que es transmeten, també poden propagar problemes cap al commutador a causa de la transmissió de senyals disruptives (per exemple, la repetició en bucle del procés d'activació i la desactivació de la línia) que poden afectar la seva funció si no disposen dels mecanismes de detecció i desactivació de línies problemàtiques[70] (la qual cosa deixaria el recurs sense accés a la xarxa).

- Els commutadors o els punts d'accés poden deixar de funcionar per fallada elèctrica o electrònica (com el cas de les interfícies de xarxa). De vegades, aquests problemes no aturen completament el dispositiu, sinó que es tradueixen en un comportament erràtic que pot provocar la corrupció de les dades que es transmeten, la pèrdua parcial o total de la connectivitat dels recursos o la disfunció del segment de xarxa que controlen (per exemple, impedint la comunicació amb altres segments).

[70] Cada vegada és més freqüent trobar commutadors que implementen la desactivació de línies problemàtiques. Sovint, el protocol d'activació no es desencadena fins que es desconnecta i reconnecta el recurs.

Més enllà de les disfuncions en un pla físic (que són inherents a l'electrònica dels suports), el focus d'atenció principal acostuma a recaure en la capa de programari dels diferents recursos que implementen les funcionalitats pròpies de la comunicació:

- El principi de mantenir actualitzat el microprogramari de cada dispositiu és garantia de correcció d'errors i de prevenció de vulnerabilitats, com en qualsevol altre recurs del sistema informàtic.

- Un altre principi bàsic de tots els dispositius que s'adquireixen és la necessitat de canviar les claus d'accés que el fabricant estableix en els productes per defecte, en favor d'unes de pròpies suficientment robustes com per a resistir els atacs habituals de força bruta[71].

(71)Els atacs de força bruta consisteixen en provar sistemàticament totes les combinacions possibles de contrasenyes fins a aconseguir la credencial vàlida.

- Protegir la interfície de configuració del dispositiu, tant de l'accés des d'ubicacions no autoritzades (per exemple, internet) com dels usuaris no autoritzats (controlant els permisos d'administració o supervisió) i de la captura il·lícita de transmissions (activant les variants segures dels protocols, com, per exemple, HTTPS[72]). Canvis fraudulents en la configuració d'alguns recursos de comunicació (especialment en els encaminadors) poden redirigir la transmissió de dades cap a sistemes il·legítims.

(72)HTTPS és la variant segura del protocol HTTP, protocols àmpliament utilitzats per a configurar dispositius de xarxa.

- Per defecte, la connexió física de qualsevol dispositiu a la xarxa ja l'habilita a establir comunicació amb la resta de recursos que hi són presents, la qual cosa pot suposar un risc per a la seguretat. Per mitigar aquesta situació és necessari desactivar totes aquelles interfícies dels commutadors i encaminadors que no tenen cap recurs assignat, o bé imposar filtres d'accés per adreça física (MAC) en aquells casos que sigui necessari mantenir un control estricte del dispositiu[73].

(73)Les opcions de filtratge per adreça física són habituals d'encaminadors i punts d'accés sense fils.

- L'accés físic als recursos de comunicació, com els commutadors i els encaminadors, pot facilitar la manipulació fraudulenta de les connexions de la resta de dispositius o inclús la connexió al sistema de dispositius externs que podrien realitzar qualsevol activitat il·legítima, com l'escolta de les comunicacions[74], la introducció de programari maliciós o el bloqueig de serveis[75]. Les mesures de seguretat principals se centren en ubicar els recursos de comunicació en armaris tancats amb clau i limitar-ne l'accés al personal autoritzat.

(74)Les eines d'escolta poden recuperar els paquets de dades que circulen per la xarxa per analitzar-ne el contingut.

(75)Els atacs de denegació de servei són coneguts popularment per la sigla en anglès DoS (*denial of service*).

Les organitzacions depenen cada vegada més dels recursos de comunicació per accedir als serveis que sustenten la seva activitat, per tant, qualsevol disfunció pot aturar parcialment o total la seva activitat. Protegir la infraestructura de comunicacions resulta essencial avui dia, tant per a garantir els recursos que s'hi connecten com la informació que transfereixen.

2.3.4. La internet de les coses

La internet de les coses representa tot un repte de seguretat perquè proveeix d'alguna funcionalitat que pot ser important o confidencial per a l'organització a partir d'un dispositiu que és relativament simple (o inclús limitat) que es connecta directament a la xarxa (sigui local o internet). Per exemple, amb aquests dispositius es pot controlar l'obertura i el tancament de portes, monitorar sensors ambientals de sales o proporcionar imatges o vídeos d'ubicacions concretes (entre moltes altres possibilitats).

Vegem algunes de les particularitats entorn de la seguretat de la informació que suposa l'explotació d'aquests dispositius:

- Utilitzen diversitat de tecnologies tant per al maquinari com per al programari. L'ampli ventall de possibilitats que en resulta dificulta tant l'estandardització de l'administració com la implementació de mesures de seguretat generals.

- Sovint, els dispositius s'han d'implantar en la mateixa ubicació on és necessària la seva funció, la qual cosa, de vegades, origina que tant el dispositiu mateix com la connexió a la xarxa siguin físicament accessibles i manipulables.

- La senzillesa de molts d'aquests dispositius es tradueix en prestacions limitades, tant en el maquinari (dificultat per realitzar càlculs complexos, com els necessaris per al xifratge) com en el microprogramari (amb interfícies de control amb poques opcions de seguretat disponibles).

- Els proveïdors d'aquests dispositius no sempre mantenen una línia d'actualització del microprogramari dels dispositius que comercialitzen (com sí és costum amb les aplicacions o els sistemes operatius), la qual cosa pot deixar els dispositius desprotegits davant d'atacs que explotin les vulnerabilitats detectades però no corregides.

La forta implantació que estan tenint aquests dispositius (tant en particulars com en tot tipus d'organitzacions), les mancances o limitacions que poden presentar en matèria de seguretat i l'accessibilitat de molts d'ells des d'internet han propiciat que aquests dispositius siguin un dels objectius habituals per trencar la cadena de seguretat de la informació.

A continuació es plantegen algunes mesures generals per a millorar la seguretat d'aquests dispositius:

- Seleccionar dispositius amb suficient capacitat de procés i prestacions de seguretat, de fabricants implantats sòlidament en el mercat que puguin

proveir d'actualitzacions de microprogramari els productes que comercialitzen.

- Actualitzar regularment el microprogramari per a corregir errors i prevenir vulnerabilitats, com qualsevol altre recurs del sistema.

- Canviar la clau d'accés per defecte per una de pròpia amb robustesa suficient. Si és possible, diferenciar l'accés d'administració del dispositiu (que permet realitzar canvis en la configuració) del d'operador (que permet consultar i executar la funció que realitza).

- Habilitar les funcions de xifratge disponibles en el dispositiu, tant per a protegir les comunicacions amb la interfície de configuració com per a transmetre les dades que genera la seva funció.

- Habilitar el filtratge de connexions per a assegurar que el dispositiu només dóna servei als equips o sistemes legítims per així protegir-lo de possibles atacs o d'accessos il·lícits des d'altres sistemes.

- Intercalar un recurs nou que asseguri les funcions bàsiques de seguretat si el dispositiu no n'és capaç. A més, aquest recurs també pot ajudar en el procés de totes les dades que genera el dispositiu[76] (que, de vegades, poden ser en temps real).

[76] El terme *edge computing* fa referència als recursos que centralitzen i processen les dades dels dispositius IoT abans d'enviar els resultats al sistema de l'organització.

La internet de les coses és una àrea que continua en curs de desenvolupament, especialment quant als aspectes de seguretat de la informació. La implementació real dels mecanismes de seguretat dependrà en gran mesura dels dispositius concrets que s'hagin de protegir i del seu context.

2.4. La seguretat de la xarxa

Les organitzacions depenen, cada vegada més, de les comunicacions per donar suport a tot el flux d'informació que generen i consumeixen els recursos del sistema. Amb raó, bona part de les actuacions de seguretat que s'acostumen a implantar globalment se centren en els recursos de comunicació.

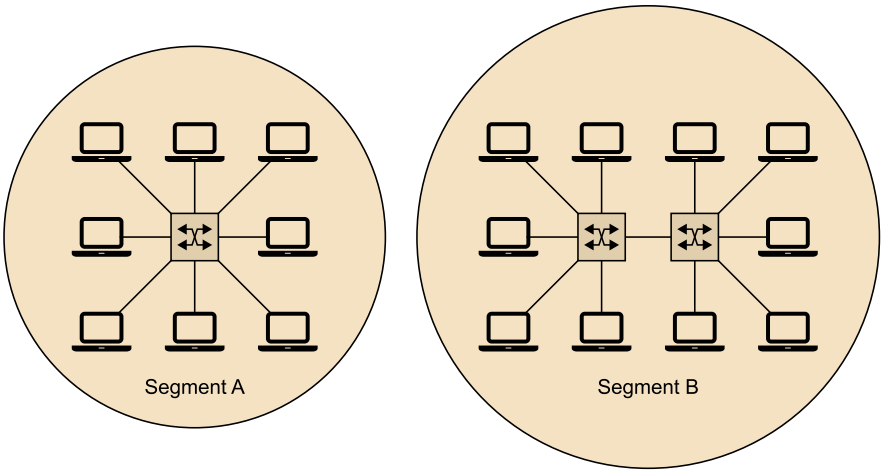
Els mecanismes de seguretat de la xarxa persegueixen protegir els accessos i mantenir el control de les comunicacions per a minimitzar els riscos que suposa tenir una infraestructura permanentment activa i connectada. En els apartats següents se'n fa un recorregut dels més habituals.

2.4.1. La segmentació de la xarxa

El principi fonamental de totes les xarxes és facilitar la comunicació entre tots els nodes que hi estan connectats. En la topologia en estrella[77], el commutador és el dispositiu central que permet enllaçar els extrems de la comunicació i, si es vol ampliar la xarxa, en general, només cal afegir més commutadors i connectar-los entre si de manera que existeixi un camí entre qualsevol parell de nodes.

(77)La topologia en estrella és l'estructura de xarxa més utilitzada avui dia, i consisteix en connectar cada node a un punt central pel qual passen totes les comunicacions.

Figura 1. Dos segments de xarxa en estrella aïllats, un d'ells (B) amb dos commutadors que amplien el segment cap a més nodes



Vegem les mesures de seguretat que es poden implementar en aquest nivell:

- Per defecte, el commutador permet la comunicació sense restriccions entre tots els recursos que s'hi connecten. De vegades, es poden donar situacions que facin necessari l'aïllament d'un o més grups de nodes, de manera que únicament es puguin comunicar dins de cada grup. Per a fer possible aquesta situació cal segmentar o dividir la xarxa, ja sigui de manera física o virtual.

- La segmentació física consisteix en aïllar els commutadors que connecten els nodes de cada grup, descartant qualsevol enllaç físic amb els commutadors d'altres grups de nodes. Si bé la segmentació física compleix amb l'objectiu, és complexa d'organitzar i costosa d'implantar per què s'han d'aprovisionar almenys tants commutadors com grups de nodes es vulguin segmentar.

- Per a resoldre els inconvenients de la segmentació física, alguns commutadors implementen l'estàndard IEEE 802.1Q[78] que dóna suport a la creació de segments virtuals en la xarxa, anomenats VLAN[79], associant cada interfície del commutador amb un segment determinat i etiquetant cadascun dels paquets que transmet amb el número de VLAN al qual pertany. Tot i

(78)L'estàndard IEEE 802.1Q defineix la segmentació amb l'etiquetatge dels paquets de dades, inserint un camp que identifica el segment al qual pertany el paquet.

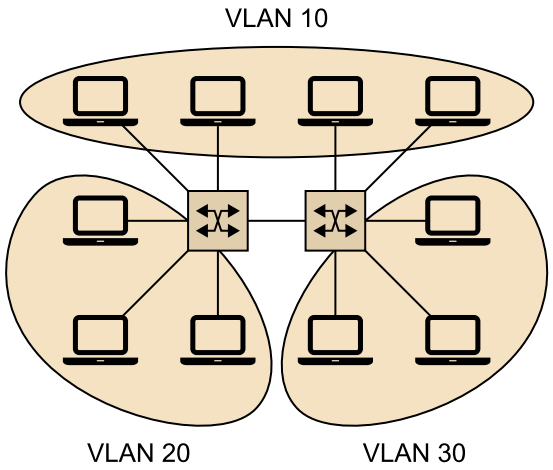
que comparteixen el mateix recurs físic, es considera que les VLAN garanteixen l'aïllament dels nodes al mateix nivell que la segmentació física.

(79)VLAN és l'acrònim anglès de *virtual local area network*.

- En el cas que sigui necessari comunicar els diferents segments d'una xarxa, ja siguin físics o virtuals, és imprescindible que cada segment tingui un adreçament diferent[80] i que un encaminador asseguri la comunicació entre cada segment. En aquest punt, si escau, l'encaminador pot establir els filtres necessaris per a deixar passar únicament els paquets que compleixen els criteris que s'han definit (per exemple, habilitar únicament un sentit de la comunicació o filtrar els serveis que se sol·liciten en la transmissió).

(80)La manera més fàcil de crear adreçaments diferents és ajustar la màscara de xarxa. Per exemple, les xarxes 192.168.21.0/24 i 192.168.73.0/24 són dues xarxes privades diferents.

Figura 2. Segmentació virtual (VLAN) d'una xarxa en estrella amb dos commutadors



Segmentar la xarxa interna en diversos segments presenta l'avantatge de poder gestionar diversos perfils de seguretat (un per a cada zona), a costa d'augmentar la complexitat del disseny, el cost econòmic i la dedicació per a crear i mantenir la infraestructura.

2.4.2. Les xarxes sense fils

En l'actualitat, la connexió dels dispositius sense fils és un aspecte tant important per a l'organització com ho és la connectivitat per cable, malgrat els riscos que suposa mantenir una zona oberta on qualsevol pot intentar introduir-se en el sistema[81]. De vegades, bona part d'aquests dispositius sense fils poden estar associats al fenomen BYOD, la qual cosa augmenta encara més els riscos de seguretat per al sistema.

(81)Si la cobertura de la xarxa sense fils s'estén més enllà de les instal·lacions de l'organització, res impedeix que no pugui ser atacada per dispositius externs.

(82)És l'acrònim anglès de *wireless fidelity*, un tipus de xarxes sense fils que desenvolupa la família de protocols estàndard IEEE 802.

Vegem algunes de les particularitats habituals entorn de la seguretat de les xarxes sense fils (com, per exemple, les xarxes wifi[82]):

- Els punts d'accés són dispositius connectats a la xarxa del sistema que difonen una xarxa sense fils que pot estendre la xarxa cablejada (utilitzant el mateix adreçament) o pot ser independent (creant un nou segment de la xarxa amb un adreçament específic per als dispositius sense fils). En aquest

últim cas, el mateix punt d'accés actuaria com a encaminador entre ambdues xarxes.

- Alguns dels paràmetres de configuració de la xarxa sense fils pretenen mitigar els riscos inherents a la tecnologia mateixa, com la capacitat de crear una xarxa invisible, limitar el nombre màxim d'equips que es poden connectar, definir portals captius[83] per a utilitzar la xarxa, habilitar un filtre de dispositius vàlids basat en adreces MAC, definir una contrasenya per accedir a la xarxa, establir algun tipus de xifratge[84] a l'hora de transmetre les dades o, en alguns recursos, inclús la possibilitat de limitar la comunicació directa entre els diferents dispositius connectats a la xarxa sense fils del punt d'accés[85], entre altres.

- Si bé alguns punts d'accés poden incorporar serveis de gestió de la xarxa com DHCP i DNS, és força habitual delegar aquesta tasca als recursos que aprovisionen la xarxa cablejada. De la configuració d'aquests serveis dependrà la difusió que es fa cap als clients sense fils de les particularitats de la xarxa interna del sistema, com, per exemple, conèixer el nom de domini o les adreces dels serveis implantats.

- Els punts d'accés no acostumen a incorporar la capacitat de filtrar els paquets de dades que es transmeten entre la xarxa sense fils i la xarxa cablejada. Serà necessari segmentar la xarxa sense fils i establir regles de filtratge entre ambdues xarxes per mitjà de l'encaminador si es vol controlar el flux de les comunicacions (com qualsevol altre segment de xarxa).

Cada vegada és més fàcil garantir les connexions sense fils dins de l'organització gràcies a l'evolució de la tecnologia, però l'adopció del BYOD requereix aprofundir amb deteniment en la complementarietat del conjunt de mesures per a garantir la seguretat del conjunt.

(83) Els portals captius són mecanismes per a autoritzar l'accés a la xarxa, per exemple, amb nom d'usuari i contrasenya.

(84) D'entre els mètodes de seguretat wifi que estan estandarditzats per la indústria, el WPA2 ja no es considera suficientment segur i s'opta per la utilització de WPA3 sempre que estigui disponible.

(85) De vegades, aquesta funcionalitat s'anomena *xarxa de convidats* (en anglès, *guest network*).

2.4.3. El tallafocs

Pel que fa a la xarxa, un tallafocs és un dispositiu que implementa les funcions d'encaminador i que pot examinar els paquets de dades que rep per a determinar si n'accepta o en rebutja la retransmissió.

Els tallafocs s'ubiquen a la frontera entre dues o més xarxes (ja sigui entre segments interns o entre el sistema i internet), de manera que pugui filtrar les comunicacions des del perímetre de cada xarxa.

Vegem les particularitats principals del seu funcionament:

- Els tallafocs analitzen els paquets de dades en funció de les regles de filtratge definides: quan els atributs d'un paquet coincideixen amb els definits en una regla, s'executa l'acció que s'ha definit (s'accepta, es denega

o es rebutja el paquet). Per exemple, «accepta tots els paquets de dades provinents de la xarxa interna que sol·liciten el servei DNS (UDP/53)». En general, el paquet de dades es descarta si no coincideix amb cap de les regles definides.

- Les regles de filtratge poden examinar diversos atributs i propietats dels paquets. Per exemple, l'adreça d'origen o de destinació del paquet, el protocol utilitzat i el número de port, si el paquet està iniciant una connexió nova o forma part d'una comunicació ja establerta, el sentit i la direcció de la comunicació, etc. A més, les regles poden combinar diverses d'aquestes característiques a la vegada per a ajustar al màxim el filtratge a la situació que s'accepta, es rebutja o es denega, però cal tenir en compte que, com més atributs es verifiquin i com més regles hi hagi, més cost computacional haurà de suportar el tallafocs i més alentirà el trànsit de paquets.

- La seguretat que proporciona el tallafocs és proporcional a com d'adequades són les regles del filtratge. En aquest sentit, és costum partir d'una configuració que denega totes les connexions (tant d'entrada com de sortida del sistema) i només acceptar les estrictament necessàries (delimitant les adreces, els protocols, els ports, etc.). Evidentment, la configuració s'haurà d'adaptar al context exacte de l'organització (per exemple, si l'organització publica el seu propi servei web caldrà habilitar les connexions entrants per a prestar el servei a l'exterior).

- Una de les funcions interessants que tenen els tallafocs és la capacitat de registrar l'activitat que realitzen en forma de diaris[86], d'aquesta manera es pot saber de primera mà quin és el comportament del tallafocs davant les diverses situacions amb les quals s'ha d'enfrontar dia a dia (per exemple, la quantitat i les característiques dels atacs que s'estan filtrant).

[86]Els diaris (en anglès, *logs*) és una de les utilitats més interessants i útils dels tallafocs.

- Com que és un dispositiu de xarxa, el tallafocs també pot realitzar altres funcions, com, per exemple, assignar adreces als dispositius de la xarxa, resoldre els noms dels recursos, encaminar els paquets entre els diferents segments de xarxa (siguin físics o virtuals) o connectar cadascun dels segments a internet. Si bé són funcions que habitualment s'assignen al tallafocs, en instal·lacions grans es deleguen a d'altres dispositius per alliberar-lo de qualsevol tasca que no sigui la pròpia (amb l'inconvenient que afegeix cost i complexitat a la instal·lació).

- El mercat ofereix moltes solucions basades en tallafocs que amplien les funcions ja comentades amb altres serveis, com la protecció antivirus, els servidors intermediaris[87], els filtres d'aplicació[88] o inclús la integració de punts d'accés sense fils en el dispositiu mateix. Tota aquesta combinació de funcionalitats trenquen la finalitat primera que ha de tenir el tallafocs, i

[87]El servidor intermediari actua de mitjancer entre el client i el servidor per tal de protegir el primer dels continguts oferts pel segon. El cas més habitual és el servidor intermediari de serveis web.

les bones pràctiques de l'àrea recomanen segregar aquests serveis a d'altres dispositius.

El tallafocs és un element crític per a la seguretat del sistema informàtic. Si bé l'objectiu principal és protegir de riscos externs, no cal oblidar que també hi ha riscos a l'interior del sistema, per tant també es poden establir regles per a limitar les connexions que surten cap a internet (i així potser detectar possibles aplicacions fraudulentes operant dins del sistema).

(88)Els filtres del nivell d'aplicació (sovint anomenats *Layer 7* o simplement *L7*) intenten identificar l'aplicació o el servei que hi ha al darrera d'una connexió mitjançant el seu comportament, de manera que es pugui filtrar (cosa que no és possible realitzar a nivell de xarxa).

(89)Les xarxes privades virtuals són conegudes popularment com a VPN, l'acrònim anglès de *virtual private network*.

2.4.4. Les xarxes privades virtuals

De vegades, les organitzacions han de permetre la connexió remota al seu sistema per tal que un usuari (o tot un altre sistema informàtic) s'hi pugui connectar i utilitzar els recursos dels que disposa com si estigués present localment. Per a garantir la seguretat d'aquestes connexions s'utilitzen les xarxes privades virtuals[89]:

- Una xarxa privada virtual es fonamenta en la creació d'un canal de comunicacions segur a través d'un mitjà insegur (com podria seria internet). Aquest canal és com un túnel d'extrem a extrem on la informació es transmet protegida.

- Dins del sistema, el dispositiu que normalment s'encarrega d'establir les connexions de xarxa privada virtual és el tallafocs, gràcies a la seva ubicació a la frontera amb internet i la capacitat d'encaminar paquets de dades. En instal·lacions grans, de vegades es deriven aquestes funcions a servidors específics.

- Hi ha diferents implementacions de xarxes privades virtuals, probablement, una de les més utilitzades arreu és IPSec[90] ja que bona part dels sistemes operatius (i moltes vegades, també del microprogramari) l'incorporen per defecte.

(90)IPSec és la contracció d'IP (*internet protocol*) i Sec (*security*).

- En general, per a establir el canal segur cal que els extrems coneguin o comparteixin alguns paràmetres de la connexió, com, per exemple, la passarel·la[91], la clau compartida de la connexió, les credencials de l'usuari que es connecta o els certificats digitals per a autenticar els extrems. El número de paràmetres depèn del tipus de connexió i dels mecanismes de seguretat exigits per a establir el canal segur (alguns d'ells són acumulables).

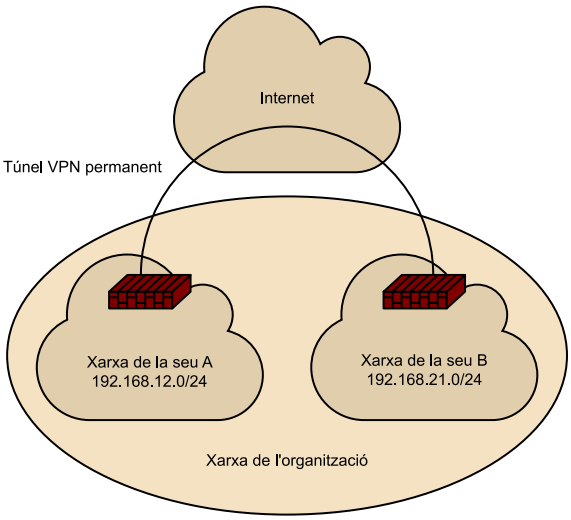
(91)La passarel·la del túnel VPN és l'adreça del sistema al qual es vol connectar, és a dir, l'adreça IP pública de l'encaminador.

- Un cop s'ha establert el túnel, tota la informació que s'envia o es rep per aquest canal està xifrada de tal manera que qualsevol que en pugui capturar els paquets de dades no en podrà conèixer el contingut si desconeix les claus utilitzades.

- Els usos més habituals de les xarxes privades virtuals són la connexió d'usuaris remots[92] o la interconnexió de sistemes informàtics. En el primer cas es crea i es destrueix el túnel (i el segment de xarxa virtual associat) sota demanda de l'equip remot. En el segon cas s'estableix un canal segur, permanent i xifrat entre els sistemes, la qual cosa permet l'accessibilitat continua entre tots els nodes presents en les xarxes connectades. En ambdós casos es poden establir regles de filtratge en les comunicacions, tot i que no és l'habitual.

(92)En l'argot propi, a l'usuari remot que es connecta a un sistema a través d'una xarxa privada virtual se l'anomena *road warrior*.

Figura 3. Xarxa privada virtual (VPN) permanent entre dues seus d'una mateixa organització



- L'objectiu principal de les xarxes privades virtuals és estendre la xarxa a tots els equips o sistemes remots, la qual cosa augmenta la superfície d'atac i els riscos de seguretat en general. Per defecte, es considera que els equips remots que es connecten a través d'una xarxa privada virtual han de ser igual de confiables que els equips locals, tot i que és recomanable implantar filtres per a controlar els accessos i evitar la propagació de riscos.

- La utilització de xarxes privades virtuals suposa més cost computacional en els equips que estableixen el túnel a causa de les operacions criptogràfiques que s'han de realitzar per a assegurar els paquets de dades que es transmeten, però també per les possibles regles de filtratge que es puguin haver establert.

Les xarxes privades virtuals són una de les opcions més utilitzades per a connectar equips o sistemes de manera segura a través d'internet, però cada vegada són més les alternatives que proposen externalitzar les connexions segures a través de serveis de tercers[93] o inclús directament reconvertir cap al núvol tots aquells serveis als quals han d'accedir els usuaris remots (així s'evita qualsevol actuació en el sistema local).

(93)Normalment, aquests serveis de connexió segura a través d'un servei externalitzat requereixen la instal·lació de programari específic en els dos extrems de la connexió (per exemple, el servei d'escriptori remot).

2.4.5. La detecció i la protecció contra intrusos

No sembla fàcil detectar les intrusions que puguin haver en uns sistemes que estan orientats plenament a facilitar la utilització i la comunicació entre els recursos. A més, als possibles atacants també els interessa fer prova de discreció si aconsegueixen introduir-se en el sistema, i eviten (o eliminen) qualsevol rastre que puguin deixar.

Els sistemes de detecció i de protecció contra intrusos[94] intenten mantenir sota control aquesta situació, vegem-ne com funcionen:

(94)Els sistemes de detecció d'intrusos són coneguts popularment per l'acrònim anglès IDS (*intrusion detection system*) i els sistemes de protecció contra intrusos per IPS (*intrusion protection system*).

- El sistema de detecció d'intrusos monitora l'activitat del sistema buscant patrons o comportaments que puguin ser sospitosos i, en cas de trobar-los, emetre una alerta.

- En general, la detecció consisteix en monitorar diversos elements buscant patrons de comportament ja coneguts (com els del programari maliciós) o anòmals (com l'acció repetitiva d'accions contra un mateix recurs o l'enviament de paquets mal estructurats). La detecció es pot realitzar en diversos nivells, els més habituals són en la xarxa, en el sistema operatiu i en les aplicacions. Per exemple, que una aplicació intenti accedir o modificar a fitxers que no formen part del seu context d'execució podria activar una alerta que indiqui que potser es tracta de programari maliciós.

- El sistema de protecció contra intrusos pot actuar sobre els elements del sistema per a contenir l'impacte que pugui tenir una alerta prèviament detectada (com, per exemple, activar regles específiques del tallafocs) i així evitar que es pugui produir un incident de seguretat.

- Hi ha la possibilitat que la monitorització generi falsos positius i identifiqui com un atac o incident una situació que no té perquè ser-ho. En general, es recomana realitzar una primera fase de detecció per tal d'ajustar el comportament de les eines abans de posar en marxa la protecció (que activaria els mecanismes necessaris per bloquejar els elements que han generat l'alerta).

En el mercat hi ha moltes utilitats que realitzen les funcions de detecció i protecció davant d'intrusions, si bé moltes vegades fan servir nomenclatures diverses per a referir-se a aquestes funcionalitats. Per exemple, la majoria de sistemes operatius controlen el nombre d'intents fallits a l'hora d'introduir les credencials d'usuari, i bloquegen durant uns minuts l'entrada a partir d'un cert nombre d'errors consecutius.

2.4.6. Les zones desmilitaritzades

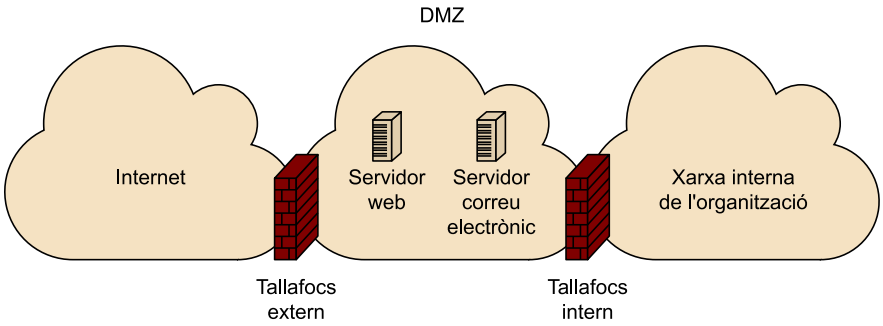
De vegades, l'organització necessita publicar algun dels serveis que ofereix el seu sistema, ja sigui per a que el públic en general hi pugui accedir (com un portal web) o per necessitats de funcionament del servei mateix (com seria el cas d'un servidor de correu electrònic, al qual es necessita accedir des de l'exterior per rebre el correu entrant dels dominis que administra).

Oferir aquests serveis suposa un risc per al sistema, per la qual cosa s'acostuma a crear una zona desmilitaritzada[95] per garantir-ne la seguretat:

[95]La zona desmilitaritzada, de l'anglès *demilitarized zone* (DMZ), es basa conceptualment en el seu homònim de la vida real per a indicar una zona d'exclusió que pretén evitar riscos majors.

- La zona desmilitaritzada és un segment de la xarxa del sistema que es crea quan es dupliquen els tallafocs. És a dir, l'espai de xarxa resultant entre el tallafocs extern (que fa de frontera amb internet) i l'intern (que fa de frontera amb el sistema local) actua com una zona desmilitaritzada. També és possible crear la zona amb un sol tallafocs dedicant una de les interfícies de xarxa disponibles per a crear aquest segment nou.

Figura 4. Zona desmilitaritzada (DMZ) basada en dos tallafocs (intern i extern) amb dos serveis accessibles des de l'exterior (web i correu electrònic)



- En la zona desmilitaritzada s'ubiquen els recursos als quals s'ha de poder accedir des de l'exterior. El tallafocs extern permetrà l'accés remot als recursos de la zona, mentre que el tallafocs intern mantindrà aïllat el sistema local i limitarà així l'impacte dels possibles incidents de seguretat.

- La implantació d'una zona desmilitaritzada és costosa en termes econòmics perquè suposa l'adquisició del material per a implementar la zona (tallafocs, commutadors, servidors, etc.), però també per la inversió en hores de professionals per a garantir la seguretat global de tota la infraestructura, que estarà més exposada.

- La publicació de serveis augmenta els riscos i facilita l'explotació de vulnerabilitats que no només poden afectar als propis serveis, sinó també servir de plataforma per a atacar els tallafocs o el sistema local (o inclús altres sistemes[96]).

[96]Les xarxes de zombis són xarxes d'ordinadors que estan sota el control dels atacants i serveixen de plataforma per a cometre atacs contra altres sistemes.

Si bé les zones desmilitaritzades continuen tenint sentit en organitzacions mitjanes i grans que tenen necessitat de publicar serveis a l'exterior i capacitat suficient per a garantir el funcionament i la seguretat, cada vegada és més habitual migrar aquests serveis a centres de dades especialitzats, de manera que siguin ells els qui assumeixin tots els requisits de seguretat necessaris per a publicar els serveis.

3. La seguretat dels serveis i de les comunicacions

El sistema es crea i es manté per a processar la informació que requereix el funcionament de l'organització, per tant, a més de les mesures necessàries per a assegurar la infraestructura del sistema, també cal protegir l'explotació dels serveis i de les comunicacions d'alt nivell.

En aquest sentit, les activitats diàries dels usuaris de l'organització, com, per exemple, accedir al sistema, modificar fitxers compartits, accedir al sistema d'informació de l'organització o consultar la bústia de correu electrònic han de tenir la cobertura necessària per a garantir que la informació es mantingui segura en tota circumstància.

Al llarg dels propers apartats es veuran els mecanismes més habituals que s'implementen per a assegurar les accions que els usuaris, els dispositius i els processos realitzen en el sistema, tant pel que fa als serveis com pel que fa a les comunicacions.

3.1. Els conceptes bàsics de seguretat

Els mecanismes de seguretat dels serveis i de les comunicacions se centren en protegir tota aquella informació que és productiva per a l'organització i que, en conseqüència, forma part del seu objecte de negoci.

D'acord amb l'estàndard ISO/IEC 27001[97], **la seguretat de la informació** consisteix en preservar les tres propietats essencials de la informació: la confidencialitat, la integritat i la disponibilitat[98].

[97] L'estàndard ISO/IEC 27000 és la normativa de referència per definir, desplegar i mantenir mesures de seguretat en un sistema informàtic.

[98] La propietats de seguretat de la informació són fàcilment extensibles segons el context on s'aplica, i poden incloure aspectes com l'autenticitat, la traçabilitat, la responsabilitat i el no repudi.

Vegem els mecanismes principals que s'implementen habitualment per a garantir la seguretat de cadascuna d'aquestes propietats.

3.1.1. La confidencialitat

Mantenir la informació accessible per a un conjunt de persones i secreta per la resta ha estat des de sempre un dels aspectes fonamentals a l'hora de protegir la informació. Si la informació és poder, tal com resa la dita, mantenir-la secreta sembla un requisit indispensable per a tot aquell que la posseeix.

La **confidencialitat** és la propietat que garanteix que la informació és únicament accessible per a aquells que hi estan autoritzats.

[99] Avui dia, tots els mètodes per a xifrar i desxifrar la informació són públics i àmpliament coneguts, per tant la qualitat de la protecció recau exclusivament en la clau de xifratge.

En general, per a garantir la confidencialitat d'una informació (tant si està emmagatzemada com en circulació per la xarxa) s'utilitzen mecanismes criptogràfics que transformen un text en clar en un text xifrat (i viceversa) gràcies a la utilització d'algoritmes i claus criptogràfiques, de manera que el text només és accessible si se'n posseeix la clau utilitzada per xifrar[99].

Pel context que ens ocupa, hi ha dos grans mètodes de xifratge (o criptosistemes):

- Els **criptosistemes de clau privada**, també anomenats *criptosistemes de clau simètrica o compartida*, utilitzen la mateixa clau de xifratge tant per a xifrar com per a desxifrar la informació (per tant, la clau ha de ser compartida entre ambdós usuaris, dispositius o processos que han d'accedir a la informació xifrada). L'algorisme més representatiu és l'AES[100], que és l'estàndard actual, mentre que DES[101] i triple DES[102] (o 3DES) ja no són recomanables tot i haver estat àmpliament utilitzats en diversitat d'àmbits.

- En els **criptosistemes de clau pública**, també anomenats *criptosistemes de clau asimètrica*, cada usuari posseeix un parell de claus: una de pública accessible per a tothom i una de privada que només coneix cada usuari. Ambdues claus tenen la particularitat de poder desxifrar el que ha xifrat l'altra i, a la vegada, impedir que es pugui obtenir la clau privada a partir de la pública. Els algorismes més utilitzats són RSA[103], ElGamal[104] i la criptografia de corba el·líptica (CCE[105]). El funcionament és simple: si es vol que un usuari pugui accedir a una informació, es xifra amb la seva clau pública per a que després la pugui desxifrar amb la seva clau privada i així recuperar la informació original.

Vegem algunes particularitats d'aquests criptosistemes:

- Els processos de xifratge i desxifratge de dades tenen un cost computacional elevat per als dispositius a causa de la intensitat dels càlculs matemàtics dels algoritmes. En aquest sentit, els criptosistemes de clau pública són clarament més costosos que els de clau privada.

- La distribució de claus compartides en els criptosistemes de clau privada és un procés molt costós perquè per a cada usuari nou és necessari generar una clau nova amb cadascun dels altres usuaris del sistema. Aquest procés segueix una progressió exponencial respecte al nombre d'usuaris que no és escalable a la pràctica.

- Sovint s'utilitzen els criptosistemes de clau pública per a intercanviar de manera segura una clau compartida que servirà per a xifrar l'intercanvi d'informació. En general, aquesta clau compartida s'utilitza exclusivament durant un període de temps limitat i després es destrueix (per exemple, la sessió d'un usuari en el sistema). La clau és llarga i s'obté de funcions alea-

(100) AES és l'acrònim anglès d'*advanced encryption stantard*.

(101) DES és l'acrònim anglès de *data encryption standard*, un algorisme de xifratge que ha estat estàndard durant anys i molt utilitzat en serveis informàtics i de telecomunicacions.

(102) El Triple DES és una variant del DES que encadena tres vegades l'algoritme, es va introduir al demostrar que el DES es podria trencar fàcilment i obtenir la informació en clar.

(103) RSA és la sigla de Rivest, Shamir i Adleman, els seus creadors, i es basa en les matemàtiques dels nombres primers.

(104) El sistema d'encriptació ElGamal es basa en l'intercanvi de claus de Diffie-Hellman.

(105) La criptografia de corba el·líptica es basa en les matemàtiques homònimes.

tòries, pel que es considera suficientment segura com per poder-se obtenir de manera fraudulenta durant el temps de la interacció. Amb aquest plantejament s'eviten tant els problemes de la distribució de claus compartides com del sobrecost computacional que requereix el xifratge de clau pública.

Els criptosistemes de clau pública encara tenen una altra problemàtica per resoldre, que no és altra que garantir que les claus públiques són efectivament de qui diuen ser. És a dir, que la clau pública que es pot obtenir d'un usuari (o d'un dispositiu) sigui la que correspon realment amb la seva clau privada, i no amb la de ningú altre que n'hagi pogut suplantar la identitat. Per a resoldre aquesta situació es va crear la infraestructura de clau pública.

La **infraestructura de clau pública**[106] és el conjunt de recursos físics, lògics, humans, polítics i procedimentals necessaris per a crear i gestionar certificats digitals basats en criptografia de clau pública.

(106)La infraestructura de clau pública es coneix popularment per l'acrònim anglès PKI (*public key infrastructure*).

La infraestructura consta de diversos elements que interactuen per a garantir-ne l'objectiu, els més rellevants són els següents:

- El **certificats**[107] són el centre de tota la infraestructura, contenen dades identificatives de l'usuari, el servei o l'organització a la qual fan referència i també la clau pública i la data de validesa del certificat (entre altres dades). La clau privada no s'emmagatzema en el certificat, sinó en una estructura o fitxer de dades separat.

(107)El format de certificat més habitual segueix l'estàndard internacional X.509 en la seva tercera versió (v3).

- L'**autoritat de certificació**[108] és l'entitat de confiança que garanteix que els certificats que emet (i revoca) corresponen als usuaris, serveis o organitzacions legítims (la qual cosa en comporta la verificació real). Si es confia en una autoritat de certificació i es disposa del certificat (perquè s'ha obtingut per canals segurs), es podrà garantir la identitat de qualsevol dels usuaris, serveis o organitzacions als quals hagi emès un certificat només comprovant-ne la validesa. Aquesta confiança s'estructura de manera jeràrquica: si es confia en l'autoritat de certificació, es confia en tots els certificats que hagi emès (i així en endavant, per a tots els nivells).

(108)L'autoritat de certificació es coneix per la sigla CA de l'anglès *certification authority*.

- Els **repositoris** són les estructures on s'emmagatzema tota la informació de la infraestructura de clau pública, en especial els certificats i les llistes de revocació de certificats[109] (que són llistes que inclouen els certificats que han deixat de ser vàlids abans de la data prevista).

(109)Les llistes de revocació de certificats es coneixen com a CRL, acrònim de l'anglès *certification revocation list*.

La infraestructura de clau pública proporciona totes les garanties de confiança que són necessàries per a implementar el xifratge de clau pública en multitud d'entorns, tant del sector públic (per exemple, en l'Administració pública amb la generació del DNI electrònic) com del privat (per exemple, el sector bancari o financer en general).

3.1.2. La integritat

Una altra de les propietats essencials per a dotar de garanties la informació és que representi la realitat de manera fidedigna. És a dir, que la informació no hagi estat creada o manipulada per un tercer sense autorització i, en conseqüència, hagi deixat de tenir el valor original o, pitjor encara, que condueixi a una interpretació errònia.

La **integritat** de la informació és la propietat que garanteix la correspondència respecte a la realitat original que representa, sense alteracions fraudulentes de cap tipus.

Per a garantir la integritat de la informació s'utilitzen funcions de resum[110], que són funcions matemàtiques que estableixen una correspondència unidireccional entre la informació i una representació simbòlica de mida fixa. És a dir, qualsevol alteració o modificació en la informació original generarà un resum diferent[111] que delataria la pèrdua d'integritat.

(110)Les funcions de resum es coneixen habitualment com a funcions *hash*.

(111)Tot i que el resum té mida fixa, és molt difícil que el resum de dues informacions sigui el mateix.

Els algorismes de resum SHA-1[112] i MD5[113] han estat habituals durant molt de temps, però ja no són recomanables perquè presenten algunes vulnerabilitats. Actualment, els algorismes de resum recomanables per a ser utilitzats són els de la família SHA-2 i SHA-3, que presenten novetats respecte a les versions anteriors i diverses variants en funció de la llargada del resum que es vol obtenir.

(112)SHA és la sigla de l'anglès *secure hash algorithm*.

(113)MD és la sigla de l'anglès *message digest*.

Quan es fa referència a la integritat d'una informació cal considerar dues dimensions:

- La **integritat del contingut**, que garanteix que la informació representa realment allò que ha de representar, és a dir, que és exacta, fidedigna, creïble i confiable en tots els aspectes. Per a garantir la integritat del contingut d'una informació, l'emissor n'ha de calcular la funció resum i fer-la accessible per al receptor, que, per la seva banda, calcularà el resum de la informació que hagi obtingut i comprovarà que ambdós resums coincideixin per a validar que la informació no s'hagi alterat. Un exemple habitual de la integritat del contingut és la descàrrega de programari des de mitjans insegurs (com internet), on el productor publica el resum dels fitxers en el seu portal de descàrrega per tal que els usuaris el puguin contrastar amb els de la còpia descarregada.

- La **integritat de la font** té com a objectiu garantir que la informació prové de l'entitat que l'ha de proporcionar, i no de cap entitat il·legítima que hagi suplantat l'original. Per a garantir la integritat de la font s'utilitza el xifratge de clau pública: l'emissor calcula el resum de la informació i el xifra amb la seva clau privada, de manera que el receptor pugui desxifrar-lo amb la clau pública de l'emissor i comprovar si correspon amb el resum que ha calculat de la informació obtinguda (només coincidirà si la informació no ha estat alterada i la clau pública utilitzada és la de l'emissor). Un exemple d'integritat de la font és l'autenticació d'un missatge de correu o d'un document electrònic[114], on l'emissor vol garantir que n'és efectivament l'autor.

[114] Algunes aplicacions d'ofimàtica incorporen funcions de xifratge per a garantir la confidencialitat i la integritat de missatges, documents, etc. utilitzant certificats.

Una conseqüència directa de superar la verificació de la integritat és que l'emissor no pot repudiar la informació a posteriori. Per exemple, el fabricant de programari no pot eludir la seva responsabilitat si els fitxers descarregats del seu portal són íntegres però contenen programari maliciós (per exemple, un virus o un troià). De fet, la propietat d'integritat de la informació assenta les bases necessàries per a la signatura digital de documents gràcies als mecanismes tècnics per a vincular diferents entitats (integritat de la font) amb una mateixa informació (integritat del contingut).

3.1.3. La disponibilitat

Avui dia, la informació és més necessària que mai, perquè sense ella ni es poden realitzar les activitats previstes ni es poden prendre les decisions adequades. La informació sempre ha d'estar disponible per a aquelles entitats que hi tenen ple dret d'accedir.

La **disponibilitat** és la propietat que garanteix que la informació sempre sigui accessible per a tots els usuaris o processos que hi estan autoritzats.

Garantir l'objectiu de disponibilitat pot requerir un ampli ventall de mesures tècniques, moltes d'elles pròpies dels àmbits físic i d'infraestructura, revisem-ne les més rellevants:

Vegeu també

Per a més detall, vegeu el mòdul dedicat a la seguretat física i d'infraestructura.

- Protegir el suport físic de la informació dels accessos no autoritzats o dels riscos físics i naturals.

- Redundar els components crítics del sistema per a evitar interrupcions del servei.

- Realitzar còpies de seguretat de manera regular per a poder restablir els serveis com més ràpid millor.

- Segregar els dispositius potencialment perillosos a segments de xarxa controlats.
- Implantar mesures de prevenció contra amenaces i vulnerabilitats.
- Controlar l'accés i la utilització dels dispositius que contenen dades.
- Implantar polítiques i controls per a assegurar que no es pot alterar lliurement l'accés a la informació (per exemple, aturant els serveis).
- Implantar polítiques i controls per a assegurar que la informació no s'elimina de manera fortuïta o deliberada per part d'usuaris o processos no autoritzats.
- Establir mecanismes de detecció i de protecció d'amenaces que segrestin les dades o n'impedeixin l'accés (per exemple, els atacs de denegació de servei[115]).

[115]Els atacs de denegació de servei són coneguts per la sigla DoS, de l'anglès *denial of service*. Hi ha una variant que explota encara més els recursos de la xarxa anomenada DDoS, *distributed denial of service*.

A diferència de les mesures tècniques per a garantir les altres propietats de seguretat de la informació, segurament la pèrdua de la disponibilitat de la informació és possiblement la menys fàcil d'assolir perquè es poden donar circumstàncies que queden fora de l'abast de les actuacions previstes. Per exemple, un tall en el subministrament elèctric prou llarg pot acabar amb la capacitat de les bateries del sistema d'alimentació ininterrompuda i aturar els servidors, la fallada de més d'un disc del servidor pot provocar l'aturada immediata del servei (o inclús la pèrdua de les dades emmagatzemades) o que el centre de dades on s'hagi ubicat el sistema d'informació empresarial sigui atacat per una xarxa de zombis[116] que alenteixi o desatengui les peticions de servei que s'hi realitzen.

[116]Una xarxa de zombis (*botnet*) és un conjunt de dispositius connectats a la xarxa (com ordinadors, telèfons intel·ligents o dispositius IoT) que estan sota el control de tercers gràcies a programari maliciós i que s'utilitzen per a perpetrar atacs com la denegació de servei distribuïda (DDoS), enviar correu brossa o robar dades.

Implantar mesures de seguretat per a preveure totes les circumstàncies possibles és complex i costós. Una vegada més, el principi de proporcionalitat s'imposa per a seleccionar la informació que és crítica per a l'organització i els mecanismes que poden assegurar-la d'acord amb el context i la situació particular.

3.2. La seguretat dels usuaris

Moltes vegades, la seguretat d'un sistema informàtic (i de la informació que processa) es fonamenta en controlar els accessos i les accions que es realitzen. Per a aconseguir-ho, primer cal verificar que els usuaris són efectivament qui diuen ser, i segon que poden realitzar les operacions que pretenen.

Les mesures de **seguretat d'usuari** agrupen tots aquells mecanismes que permeten definir i controlar les accions que pot fer cadascun d'ells, cosa que requereix la verificació prèvia de la seva identitat.

En aquest context, es consideren usuaris tant les persones que interactuen amb el sistema com els processos que s'hi executen. De fet, tots els processos estan lligats a un usuari del qual reprenen el context de seguretat que necessiten per a realitzar les seves accions, amb independència de si aquest usuari representa una persona física o una funció dins del sistema[117].

(117)La creació d'usuaris impersonals amb permisos limitats a la funció que realitzen és una mesura de seguretat habitual en els sistemes.

En les properes seccions es revisaran els mecanismes principals tant per a garantir la identitat de l'usuari com per a controlar la seva interacció amb el sistema.

3.2.1. L'autenticació

Bona part de la seguretat del sistema (especialment la dels serveis que executa) es basa en saber qui l'està utilitzant, perquè no tots els usuaris han de poder realitzar les mateixes accions o accedir a la mateixa informació. Aquesta necessitat va més enllà de la distribució de tasques o de funcions pròpia dels departaments d'una organització, perquè està regulada per la legislació nacional i internacional. Per exemple, està tipificat que un usuari únicament ha de poder accedir a la informació que requereix per a realitzar les seves tasques fins que les completi.

L'**autenticació** és el procés pel qual es valida la identitat d'un usuari, és a dir, es verifica que l'usuari és efectivament qui diu ser abans d'utilitzar el sistema.

En funció dels requisits de seguretat que pugui imposar l'organització, el sistema pot exigir l'autenticació en diferents nivells:

- A l'hora d'engegar un recurs, ja sigui a la BIOS[118] o al suport d'arrancada del sistema.
- Quan es vol utilitzar el sistema operatiu del recurs i s'inicia així una nova sessió de l'usuari que es valida.
- Per a accedir i utilitzar una aplicació, programa o servei, ja sigui local o remot.

(118)BIOS és l'acrònim de *basic input output system*, que és un microprogramari que controla el maquinari.

Aquestes mesures són acumulables, és a dir, que és possible que el sistema requereixi l'autenticació en només un, en dos o en tots tres nivells abans que es pugui utilitzar.

El procés d'autenticació de l'usuari es basa en diferents factors complementaris, de manera que el sistema en pot exigir més d'un per a validar la identificació. Vegem quins són aquests factors:

- Els **factors que coneix l'usuari**, com, per exemple, una contrasenya, una frase, la resposta a una pregunta o un PIN[119].

- Els **factors que posseeix l'usuari**, com les targetes intel·ligents[120], els testimonis d'autenticació[121] o inclús dispositius implantats (com microxips sota la pell).

- Els **factors que té l'usuari**, com, per exemple, els identificadors biomètrics com l'empremta digital, el patró de la retina o de l'iris de l'ull, la veu, l'escriptura, la geometria de la mà o de la cara, la seqüència d'ADN de l'individu, etc.

(119) PIN és la sigla de l'anglès *personal identification number*.

(120) Les targetes intel·ligents (en anglès, *smartcards*) tenen la capacitat d'emmagatzemar informació protegida amb mecanismes criptogràfics.

(121) Els testimonis d'autenticació permeten calcular contrasenyes d'un sol ús o emmagatzemar claus de xifratge, es poden implementar en maquinari (un clauer) o en programari que s'instal·la en un dispositiu (un telèfon intel·ligent).

Els factors que coneix l'usuari acostumen a ser els més vulnerables perquè moltes vegades s'acaben apuntant en algun lloc (perquè la contrasenya és difícil de recordar), són excessivament simples (com un seguit de lletres de l'abecedari o del teclat) o bé són deduïbles a partir de la informació de l'usuari (com una data d'aniversari o el nom de familiars). A continuació es revisen algunes de les mesures recomanades a l'hora de seleccionar les credencials:

- Utilitzar contrasenyes llargues (frases) i fàcils de recordar, evitant paraules o sèries de caràcters que puguin ser deduïbles (dates, noms, seqüències, etc.).

- Establir un període de validesa i de reutilització de la contrasenya coherent amb el risc que té el servei al qual dóna accés.

- Memoritzar la contrasenya, no deixar-la mai per escrit i evitar que altres persones la puguin veure. No llençar papers amb contrasenyes que altres puguin llegir.

També es pot pensar que els factors que posseeix l'usuari (com, per exemple, les targetes intel·ligents) són vulnerables pel risc de pèrdua de l'objecte o inclús de robatori, però cal tenir en compte que aquests elements acostumen a tenir proteccions addicionals per a accedir al contingut. Per exemple, a les targetes només s'hi pot accedir si s'introdueix correctament el PIN i moltes d'elles tenen capacitat de procés, de manera que la informació emmagatzemada no surt mai de la pròpia targeta.

Es considera que com més factors d'autenticació requereixi el sistema d'autenticació, més garanties tindrà de la identitat de l'usuari.

Per exemple, avui dia és habitual que els serveis tinguin la possibilitat de requerir dos factors d'autenticació[122]: primer s'introdueixen les credencials en el sistema o el servei que es vol utilitzar (normalment, usuari i contrasenya) i, un cop comprovades, el sistema envia al telèfon intel·ligent de l'usuari una alerta (a través d'un missatge o d'una aplicació específica) per a validar l'intent de connexió al sistema. A més d'afegir factors a l'autenticació, aquest sistema també permet detectar quan les credencials de l'usuari han estat compromeses i és necessari canviar-les d'immediat (per exemple, si es rep la notificació per a validar una connexió que no s'ha realitzat). Una variant d'aquest exemple consisteix en la utilització de contrasenyes d'una sola vegada[123], on el sistema és capaç de transmetre a l'usuari (a través d'un missatge o d'una aplicació) una contrasenya que únicament és vàlida per a una sessió o per a un temps determinat.

(122)L'autenticació basada en dos factors és popularment coneguda com a 2FA, la sigla de *two factors of authentication*.

(123)L'autenticació basada en contrasenyes d'un sol ús es coneix per la sigla en anglès OTP (*one-time password*).

3.2.2. L'autorització

La identificació de l'usuari és el primer pas per a establir una interacció segura, però això no implica que automàticament tingui accés a la informació o que pugui realitzar qualsevol operació en el sistema.

L'**autorització** és el procés pel qual es verifica que l'usuari té el permís per a realitzar les operacions que pretén dur a terme, com, per exemple, accedir a informacions determinades o executar accions o programes concrets.

Per exemple, els clients de banca electrònica es poden autenticar amb èxit en el portal perquè han introduït correctament els factors d'autenticació que s'exigeixen, però cadascun d'ells només podrà accedir al comptes bancaris que tenen associats al seu usuari i no als de la resta.

Tot i que l'autorització acostuma a ser un procés que depèn de l'autenticació, hi poden haver serveis (com, per exemple, els serveis web o de fitxers) en els quals un usuari anònim[124] (no autenticat) pot accedir a determinades informacions o executar un conjunt d'operacions al sistema de manera legítima i sense trencar la política de seguretat establerta.

(124)Sovint, als usuaris anònims se'ls coneix com convidats (*guest*) i utilitzen el context de seguretat de comptes d'usuari homònims.

En termes generals, l'autorització defineix el context de seguretat d'un usuari per mitjà de polítiques de control d'accés als recursos o als serveis del sistema.

Les polítiques de control d'accés defineixen amb concreció i determinisme les accions que pot realitzar cada usuari (sovint, aquesta definició s'aplica a grups d'usuaris per a facilitar-ne la gestió). La implementació d'aquestes polítiques és molt diversa perquè depèn fortament del context d'utilització, però se'n poden identificar dues tendències majoritàries:

- El **control d'accés per usuari o per dispositiu**, que defineix el context de seguretat en el perfil mateix de cada usuari o dispositiu, és a dir, totes aquelles operacions que ha de ser capaç de realitzar en el sistema. Aquesta implementació és habitual dels sistemes operatius (entre d'altres), que permeten definir la pertinença dels usuaris o dispositius a determinats grups, de manera que el simple fet de pertànyer a un grup concret sigui suficient per realitzar un conjunt determinat d'operacions. Per exemple, podran connectar-se a l'ordinador de manera remota[125] tots aquells usuaris que pertanyin al grup d'usuaris remots per als quals està habilitat el permís per a establir aquest tipus de connexió. Tots els usuaris que no pertanyin a aquest grup no podran establir cap connexió remota amb l'ordinador, tot i que mantindran l'inici de sessió local (si el tenen activat).

[125] La connexió remota a l'ordinador utilitza programari i protocols específics, que de vegades són propis de cada sistema operatiu. Per exemple, SSH per als entorns GNU/Linux i RDS per a MS Windows.

- El **control d'accés per recurs** es defineix per als recursos o per als serveis del sistema als quals es pot accedir de manera que cadascun d'ells pugui tenir la seva pròpia llista de control d'accés[126], que és una matriu on es defineixen les operacions que pot realitzar cada usuari (o grup) per aquell recurs o servei concret. Aquesta implementació és habitual del nivell de serveis del sistema i es pot considerar un estàndard de facto a causa de la seva implementació en multitud d'entorns. Per exemple, els servidors de fitxers poden establir una llista de control d'accés en cadascuna de les carpetes compartides, definint quins usuaris (o grups d'usuaris) poden realitzar les operacions de lectura i/o d'escriptura dins de la carpeta i en les subcarpetes que conté. Alguns serveis poden ser més granulars a l'hora de definir els permisos. Per exemple, la creació, la modificació, la visualització, l'eliminació, etc.

[126] Les llistes de control d'accés són conegudes per l'anglès *access control list* (ACL).

En el context dels serveis d'un sistema, és habitual acumular i combinar els controls d'accés per usuari (o dispositiu) i per recurs per tal de garantir que l'ajustament de la seguretat sigui l'òptim respecte al context d'utilització.

Cal tenir en compte que la majoria de solucions, per defecte, implementen el principi de mínim privilegi[127], que determina que cada usuari només haurà de tenir aquells permisos que són estrictament necessaris per a realitzar les seves tasques. A la pràctica, aquest principi es tradueix amb l'activació dels permisos més baixos que té l'usuari; per exemple, si l'usuari hereta del grup un permís de lectura en una carpeta i un permís d'escriptura a nivell de recurs, el servidor de fitxers únicament activarà el permís de lectura seguint el principi de mínim privilegi.

(127)En anglès, *principle of least privilege*.

3.2.3. La gestió de la identitat

La verificació de la identitat dels usuaris i el control dels seus accessos sempre ha estat un aspecte essencial de la seguretat de tot sistema informàtic. Amb el pas del temps s'han desenvolupat (i es continuen desenvolupant) diversitat de mètodes i protocols per a cobrir aquests requisits, que tant es poden utilitzar de manera independent com integrats de múltiples maneres.

En general, és força habitual implementar un **servei d'identitat o de directori** en el sistema que tant centralitzi la informació i l'administració dels usuaris com proveeixi d'autenticació i/o d'autorització a la resta de serveis i dispositius del sistema.

Vegem algunes de les característiques que poden tenir aquests serveis d'identitat:

- El servei d'identitat pot emmagatzemar tot tipus d'informació dels usuaris, com dades generals (nom, cognoms, telèfons, domicili, etc.), credencials diverses (comptes d'usuari i contrasenyes), certificats de seguretat i claus de xifratge (claus públiques i privades), atributs biomètrics (empremta digital, geometria de la cara o de la mà, etc.), pertinença a grups d'usuari o inclús és capaç d'emmagatzemar autoritzacions, drets o permisos en tot el sistema. Algunes d'aquestes característiques només estan disponibles en determinades solucions que integren múltiples funcionalitats en un sol producte.

- La informació s'emmagatzema en estructures de dades específiques guardades en fitxers o en bases de dades, a les quals s'hi pot accedir mitjançant el servei d'identitat utilitzant un o més protocols, com, per exemple, LDAP[128], Kerberos[129], RADIUS[130] o inclús SQL[131] en el cas de bases de dades relacionals.

- En general, cada servei del sistema requereix completar el procés d'autenticació de l'usuari, la qual cosa pot ser feixuga si l'usuari ha

(128)LDAP és la sigla en anglès de *lightweight directory access protocol*, un protocol per accedir i mantenir un servei de directori d'usuaris.

(129)Kerberos és un protocol per a validar la identitat d'usuaris i serveis mitjançant tiquets de durada limitada.

d'accedir a molts serveis diferents. Una manera de resoldre aquesta situació és el servei d'inici de sessió únic[132], on l'usuari ha de realitzar el registre de la sessió una sola vegada en el servei d'identitat i tots els serveis que en depenen n'accepten automàticament la validesa. Kerberos és un dels protocols més habituals per proveir l'inici de sessió únic dins d'un sistema informàtic local, però els serveis accessibles des d'internet utilitzen altres estàndards i protocols, algunes de les tecnologies que s'utilitzen habitualment són OpenID[133], OAuth[134] o SAML[135], entre moltes d'altres.

Amb la implementació conjunta d'aquestes tecnologies s'assoleix un dels requisits essencials per a la seguretat de tot el sistema, que no és altre que identificar els usuaris que realitzaran les accions en el sistema i gestionaran la informació que s'hi processa. A més, les diferents solucions de gestió de la identitat que s'ofereixen al mercat també permeten materialitzar les polítiques de seguretat definides en l'organització, com, per exemple, el període de validesa de la contrasenya dels usuaris o els requisits de complexitat que han de tenir quan s'imposa el canvi, però també altres funcions que són invisibles per als usuaris però útils per a la gestió de la seguretat, com, per exemple, l'establiment de relacions de confiança entre diferents dominis de seguretat i permetre així la interoperabilitat dels usuaris entre ambdós sistemes.

(130)RADIUS és l'acrònim de *remote authentication dial-in service*, un protocol que pot autenticar usuaris contra diverses fonts locals o remotes.

(131)SQL és l'acrònim de *structured query language*, un llenguatge per a manipular bases de dades relacionals.

(132)El servei d'inici de sessió únic s'anomena, en anglès, *single sign-on* (SSO).

(133)OpenID és un estàndard i un protocol per a l'autenticació descentralitzada.

(134)OAuth és un estàndard per a la delegació de l'autenticació àmpliament utilitzat a internet.

(135)SAML és la sigla de *security assertion markup language*, un llenguatge estàndard per a intercanviar dades d'autenticació i d'autorització entre entitats.

3.3. La seguretat dels serveis i les comunicacions

La finalitat principal de tot sistema informàtic és, d'una banda, proveir serveis d'alt nivell per a l'organització, i, d'una altra banda, facilitar l'accés dels usuaris a aquests serveis. Sovint, aquests serveis processen, emmagatzemen i transmeten informació de valor que ha de mantenir-se segura, la qual cosa suposa una exposició del servei i de les comunicacions a diversitat d'atacs, riscos i amenaces.

Les mesures de **seguretat de serveis i comunicacions** agrupen tots aquells mecanismes per a garantir les propietats de seguretat de la informació en la prestació del servei, és a dir, tant en el procés de la informació que realitzen com en la comunicació amb l'usuari.

La relació entre servei, usuari i comunicacions és indissoluble perquè els usuaris (o els processos) interactuen amb els serveis que s'ofereixen en el sistema (siguin locals o remots) a través de la xarxa de comunicacions implantada. Mantenir la seguretat al llarg de tota aquesta cadena d'elements tan diversos i susceptibles de ser atacats de múltiples maneres suposa un esforç important per a l'organització.

En les properes seccions es veuran alguns dels mecanismes més habituals per a garantir aquesta cadena de seguretat de la informació.

3.3.1. Els serveis

Sense cap mena de dubte, tots els serveis són un possible objectiu d'atacs pel simple fet d'existir, amb independència de si són públics o privats, interns o externs a un sistema, etc. De serveis n'hi ha de molts tipus, però tots tenen en comú que d'alguna manera permeten o bé l'accés a les dades subjacents, o bé el control d'algun mecanisme, la qual cosa els posiciona en el punt de mira de qualsevol atacant o programari maliciós.

La **seguretat dels serveis** se centra en garantir que el servei no es pugui comprometre a cap nivell, especialment quant al funcionament i les dades que processa.

Els serveis estan sotmesos permanentment a tot tipus de riscos i amenaces de seguretat per la seva pròpia idiosincràsia, vegem-ne alguns dels habituals:

- L'existència de portes ocultes[136] o vulnerabilitats no corregides en les solucions informàtiques que proveeixen el servei podrien habilitar l'accés d'usuaris il·legítims sense l'autenticació necessària, obtenir el control administratiu del servei o inclús espiar o segrestar la informació que es processa.

- En el cas que les solucions que proveeixen el servei no estiguin preparades per a controlar o contenir situacions de funcionament anòmales (per exemple, la recepció d'un gran nombre de sol·licituds de servei[137], eventualment mal formatades[138]), es podria produir l'aturada del servei, l'exposició d'informació confidencial o facilitar la inserció de programari maliciós en la memòria de treball de la solució informàtica.

- Les possibles deficiències en les interfícies o en la configuració de les solucions, i les limitacions per a suportar les mesures de seguretat més actuals, també poden ser l'objectiu d'atacs o de programari maliciós, i poden permetre el robatori, el segrest o la destrucció de dades, o inclús la redirecció fraudulenta del servei, ja sigui parcial o total, cap als equips dels atacants. Sovint, aquests aspectes de seguretat es relacionen amb els dispositius IoT, però en cap cas en tenen l'exclusivitat.

(136) Les portes ocultes, en anglès, s'anomenen *backdoors*.

(137) Inundar de peticions un servei forma part dels atacs de denegació de servei més comuns (en anglès, *denial of service*, DoS).

(138) L'enviament de peticions mal formatades (o amb codis específics) són habituals dels atacs d'injecció de codi (els més populars són els atacs *SQL Injection*).

Tots aquests aspectes depenen en gran mesura de la qualitat i l'adequació de les solucions informàtiques que proveeixen el servei, especialment del disseny i la construcció. Vegem ara algunes de les característiques que afavoreixen la seguretat d'aquestes solucions i que en poden determinar l'adopció:

- Les solucions es poden assegurar des del disseny, establint mesures de seguretat per defecte, implementant el principi de mínim privilegi, revisant el codi font per tercers[139], mantenint diaris d'activitat o reduint el temps de resposta en la correcció d'errors o vulnerabilitats[140].

- L'arquitectura interna de les solucions també pot afavorir els aspectes de seguretat quan es prioritzen les mesures que es materialitzaran en les diferents funcionalitats previstes, com, per exemple, la implementació de bones pràctiques[141] del sector o de normatives de seguretat vigents.

- La incorporació de funcionalitats de seguretat dins de les mateixes solucions també facilita el procés d'assegurar la informació, com, per exemple, els mecanismes per autenticar i autoritzar els usuaris, el suport de criptosistemes per a protegir la informació o la inclusió de mecanismes de filtratge de les connexions (tallafocs) o de detecció d'intrusions (per exemple, quan un usuari intenta iniciar sessió reiteradament sense èxit).

- Les solucions han de permetre configurar les opcions de seguretat incorporades alertant o evitant opcions que puguin obrir bretxes de seguretat[142] en el sistema, però l'organització també ha de preveure professionals qualificats que puguin extreure el màxim profit de les possibilitats de seguretat que ofereixen les solucions instal·lades.

(139)El programari lliure no només utilitza comunitats de desenvolupadors per a fer evolucionar el codi font, sinó que es publica en obert i tothom el pot revisar i notificar incidències o problemes de seguretat.

(140)Una vegada més, la importància de la correcció del programari i l'actualització permanent dels sistemes resulta vital per a la seguretat de la informació.

(141)ITIL (*information technology infrastructure library*) és una biblioteca de bones pràctiques àmpliament reconeguda i utilitzada en la gestió de serveis de tecnologies d'informació.

(142)Algunes aplicacions avisen l'usuari quan vol canviar una configuració que podria tenir efectes negatius en la seguretat.

Tots aquests plantejaments incideixen en la necessitat de disposar de solucions sòlides i de proveïdors confiables, que tinguin capacitat per a dissenyar i construir eines que incorporin els mecanismes necessaris per a garantir la seguretat de la informació que processen.

3.3.2. Les comunicacions

Actualment, les xarxes de comunicacions són imprescindibles per a poder explotar els serveis, però la circulació permanent de dades entre clients i servidors genera un risc constant i sostingut per a la seguretat de la informació.

La **seguretat de la comunicació** agrupa totes aquelles mesures orientades a protegir la informació que es transmet entre extrems a través de les xarxes informàtiques.

Cal tenir en compte que bona part dels protocols del model de comunicacions TCP/IP[143] no estan concebuts tenint en compte la seguretat, així que a menys que s'utilitzin les variants segures, cal considerar que la informació viatja a través de la xarxa en clar[144] per defecte. Per exemple, el protocol HTTP és insegur, mentre que el protocol HTTPS n'és l'equivalent segur.

(143)La pila TCP/IP és el model de comunicacions que utilitza internet i el més habitual en tot tipus de sistemes, tot i que el seu desenvolupament data dels anys seixanta del segle passat.

Amb els serveis permanentment exposats a la xarxa i la transmissió de dades en clar, les possibilitats d'atacar les comunicacions d'un sistema són àmplies. Vegem una classificació simple dels tipus d'atac:

- Els **atacs passius** se centren sobretot en capturar les dades que circulen per la xarxa (amb el monitoratge o l'anàlisi del trànsit[145]) o determinar els serveis que proveeix un sistema (amb l'escaneig de ports oberts o la transmissió de paquets fraudulents[146]).

- Els **atacs actius** són molt variats, però tots tenen en comú la voluntat de corrompre el funcionament normal de les comunicacions o directament aconseguir accés a qualsevol node present en la xarxa. Aquests atacs utilitzen programari maliciós, l'escolta il·legítima de comunicacions, els atacs de denegació de servei[147], la redirecció de paquets a un tercer[148] o els atacs d'intercepció[149]. Molts d'aquests atacs disposen de múltiples variants que exploten vulnerabilitats conegudes en sistemes que no estan actualitzats.

El mecanisme de seguretat principal per a garantir les comunicacions dels serveis d'un sistema i prevenir bona part dels atacs actius és la utilització de la criptografia:

- Xifrant les dades d'usuari dels paquets que es transmeten per la xarxa es garanteix que, tot i capturar-los i analitzar-los, es manté la confidencialitat sempre que no es disposi de la clau de xifratge.

- Amb el xifratge de les dades es pot detectar fàcilment la manipulació dels paquets, gràcies al control de la integritat de les dades que proporciona, i també comprovar l'autenticitat de l'emissor, especialment si s'utilitzen certificats digitals.

- La utilització de la infraestructura de clau pública afegeix garanties d'identitat entre extrems i de robustesa si s'empren claus asimètriques (que acostumen a ser llargues). Addicionalment, també hi ha mètodes per a compartir claus de xifratge a través d'un mitjà insegur, com, per exemple, l'intercanvi de claus Diffie-Hellman (que normalment s'utilitzen per a generar claus de sessió).

- La criptografia no pot prevenir o evitar els atacs contra la disponibilitat dels serveis, que és una qüestió deslligada de la protecció de les dades i s'ha de gestionar amb els mecanismes ja vistos.

(144) Que un paquet de dades contingui informació en clar vol dir que qualsevol que sigui capaç de capturar-lo en podrà llegir el contingut sense restriccions majors.

(145) Una connexió entre dispositius o sistemes de telecomunicacions no autoritzats s'anomena, en anglès, *wiretapping*.

(146) L'escaneig dels ports que manté oberts un servidor es coneix com a *port scan*, mentre que la transmissió fraudulenta de paquets per a esbrinar els serveis s'anomena *idle scan*.

(147) Els atacs de denegació de servei tenen variants, una de les més habituals és la versió distribuïda (DDoS), en la qual un conjunt d'equips (normalment sota control fraudulent) envia paquets de sol·licitud de servei o de control (ICMP) de manera massiva a un mateix servei.

(148) Un dels atacs de redirecció és el *DNS spoofing*, que consisteix en corrompre el servei de resolució de noms canviant l'adreça IP d'un servei per a redirigir-lo cap al sistema de l'atacant, de manera que li puguin arribar tots els paquets que emet l'usuari cap al que creu que és el sistema legítim.

(149) L'atac d'intercepció és conegut per l'anglès *man-in-the-middle*, i consisteixen a redirigir la comunicació entre dos extrems cap a un intermediari sense el seu consentiment, de manera que la pugui escoltar i, si vol, alterar.

Hi ha diferents llibreries i protocols que implementen mètodes criptogràfics per a garantir la seguretat de les comunicacions, però sense cap mena de dubte, el més utilitzat és TLS.

TLS (*transport layer security*[150]) és un conjunt de protocols criptogràfics dissenyats per a proporcionar confidencialitat i integritat en la transmissió de dades a través d'una xarxa.

(150)La majoria de llibreries i referències mantenen el nom SSL (*secure sockets layer*), l'antecessor ja obsolet de TLS, tot i implementar els nous protocols.

Vegem les característiques principals de TLS:

- Proporciona una connexió privada o confidencial entre extrems perquè xifra les dades utilitzant una clau per a cada sessió (que es negocia a l'inici de cada connexió amb un protocol d'intercanvi segur de claus).

- S'autentiquen els extrems de la connexió mitjançant certificats provinents de la infraestructura de clau pública, que si bé és optativa, normalment es requereix per almenys un dels extrems de la connexió (normalment el servidor).

- Es manté la integritat de les dades que es transmeten perquè s'envien acompanyades d'un codi d'autenticació de missatge[151], que controla tant l'alteració de les dades transmeses com la pèrdua d'algun paquet durant la transmissió.

(151)El codi d'autenticació de missatge s'anomena, en anglès, *message authentication code* (MAC).

- Pot garantir que qualsevol reutilització de les claus de xifratge no pugui desxifrar comunicacions anteriors. Aquesta propietat s'anomena *forward secrecy*.

- Pot suportar diferents mètodes d'intercanvi de claus, de xifratge i d'autenticació de missatges, però no totes les combinacions possibles generen les propietats anteriors.

La majoria de variants segures dels protocols del model de comunicacions TCP/IP utilitzen TLS per a assegurar les connexions. A més del canvi en el nom del protocol (per exemple, HTTPS és la versió segura d'HTTP), molts protocols segurs també canvien el número de port del servei (per exemple, HTTPS utilitza el port TCP/443 enlloc del TCP/80 del protocol insegur HTTP). D'altres protocols no canvien el port (o tenen ambdues variants, com LDAP) però utilitzen una sol·licitud específica per a iniciar la connexió segura anomenada «STARTTLS».

Cal destacar que TLS (com altres protocols criptogràfics) proporciona un túnel segur d'extrem a extrem, per la qual cosa garanteix que cap dels dispositius o recursos a través dels quals es transmeten les dades poden accedir al contingut dels paquets de dades. Però aquesta privacitat també s'aplica a qualsevol dispositiu de seguretat perimetral que hi pugui haver en el sistema (com, per exemple, un tallafocs o un servidor intermediari[152]), per tant, si es transmet qualsevol atac o amenaça a través de la connexió segura, l'equip final serà l'únic element capaç de contenir-los o mitigar-los (la qual cosa hauria de motivar la implantació de mesures de seguretat en aquest extrem de la connexió).

(152)Els servidors intermediaris es coneixen popularment com a *proxy* i l'exemple més habitual és el *proxy* de serveis HTTP, que a més de fer les funcions d'intermediació, també poden filtrar els continguts o verificar la presència de programari maliciós, entre d'altres.

3.3.3. Els usuaris

De poca cosa serveix la implantació de tots els mecanismes tècnics per a garantir la seguretat del sistema si els usuaris finals no prenen consciència que també formen part de la cadena per a assegurar la informació.

La **seguretat dels usuaris** agrupa totes aquelles actuacions que pretenen integrar les accions dels usuaris dins de la política de seguretat del sistema.

Tradicionalment, la seguretat informàtica s'ha volgut resoldre des d'una perspectiva tècnica, però amb el pas del temps s'ha demostrat que resulta imprescindible implicar tots els actors que interactuen amb el sistema, especialment els usuaris finals, perquè han de garantir l'extrem de la cadena de procés de la informació. Per exemple, alguns usuaris poden tenir dificultats per a gestionar correctament les diferents credencials que tenen o per a reconèixer pàgines web fraudulentes o adjunts de missatges potencialment perillosos (entre altres), la qual cosa pot suposar un risc per a la seguretat de tot el sistema.

En aquest sentit, són ben coneguts els atacs d'enginyeria social, l'objectiu dels quals és convèncer els usuaris perquè revelin secrets que permetin als atacants aconseguir qualsevol tipus d'informació que puguin utilitzar contra el sistema o contra ells mateixos (com, per exemple, credencials d'accés a serveis, els números i codis de targetes de crèdit, etc.). Probablement, un dels casos més coneguts són els atacs de pesca de credencials, que pretenen enganyar els usuaris[153] presentant un portal web aparentment conegut però que redirigeix la informació proporcionada (per exemple, les credencials d'accés a un servei) cap als servidors dels atacants.

(153)L'engany s'implementa per mitjà de correu electrònic o missatgeria instantània (*spoofing*) i crea una situació que requereix l'atenció de l'usuari, com, per exemple, un descobert bancari.

Aquest tipus d'atacs són difícils de preveure (inclús des del punt de vista tècnic), per tant la millor manera de gestionar-los és amb la formació dels usuaris i la promoció d'una cultura de la seguretat en l'organització que fomenti tant la identificació d'aquestes situacions com la prudència a l'hora d'actuar.

3.4. La seguretat dels continguts

Si bé tots els mecanismes de seguretat són benvinguts per donar suport a la cadena de seguretat, de vegades el que interessarà és garantir alguna de les propietats de seguretat en elements d'informació individuals (com un document o un missatge).

La **seguretat del contingut** pretén aplicar mecanismes de seguretat a elements o suports d'informació particulars, que sovint estan associats al treball que realitzen els usuaris per a garantir-ne alguna de les propietats.

Per exemple, de vegades es voldrà protegir un llapis de memòria d'accessos indeguts o bé garantir la validesa de documents (com contractes o acords). En ocasions, aquests elements d'informació es queden al marge de les polítiques de seguretat general implantades en el sistema, però la seva cobertura és necessària per a assegurar algunes de les situacions que es poden donar en l'organització. En les properes seccions es revisen alguns casos interessants.

3.4.1. El xifratge

Com s'ha vist en apartats anteriors, el mecanisme principal per a garantir la confidencialitat de la informació és el xifratge de les dades, ja sigui mitjançant criptosistemes de clau privada o pública. Amb les solucions existents, avui dia és relativament fàcil poder xifrar la informació:

- Molts sistemes operatius permeten el xifratge dels discos de l'ordinador (inclús d'aquells on s'instal·la el sistema) amb una contrasenya, de manera que dels intents de recuperar directament les dades del disc no se'n pugui obtenir resultat en clar.

- En suports extraïbles (com els llapis de memòria) es poden crear àrees privades utilitzant el mateix programari de xifratge que proporciona el fabricant del suport o bé per mitjà del programari de tercers.

- Algunes aplicacions ofimàtiques permeten bloquejar determinades accions en els documents que manipulen o xifrar completament el contingut amb contrasenyes (o inclús amb certificats digitals).

- El correu electrònic permet el xifratge i desxifratge dels missatges amb criptosistemes de clau pública, tenint en compte que és necessari haver configurat prèviament els certificats dels usuaris implicats en la comunicació[154], ja sigui amb la instal·lació directa dels certificats o l'accés als repositoris on estan emmagatzemats.

(154)Normalment, la clau pública i privada que correspon a un usuari s'empaqueta en un fitxer amb format PKCS#12 (extensió .p12) protegit amb una contrasenya d'accés.

El nombre d'aplicacions amb suport per al xifratge dels continguts continua en creixement (sobretot aquelles que implementen la infraestructura de clau pública), símptoma inequívoc de la importància que té protegir la informació.

3.4.2. La signatura digital

La integritat de la informació és una de les propietats de seguretat importants en sistemes informàtics on el cost de còpia o de modificació és pràcticament inexistent[155]. Una de les aplicacions més interessants de la criptografia aplicada a la integritat és la signatura digital de documents o missatges:

(155)En qualsevol sistema informàtic, copiar una dada d'un lloc a un altre o modificar-la directament no es considera costós, ni en termes computacionals ni temporals.

- La signatura digital utilitza la infraestructura de clau pública, on cadascun dels usuaris o entitats que signen el document tenen el seu parell de claus (pública i privada).

- Del document que cal signar (un contracte, un acord, un missatge, etc.) se n'extreu un resum (*hash*), que es xifra amb la clau privada de cada usuari[156] i s'afegeix al document per tal que la resta pugui desxifrar-lo amb la clau pública corresponent i verificar la coincidència amb el resum del document (la qual cosa significaria que s'ha signat el document original).

(156)Enlloc de xifrar tot el document només s'acostuma a xifrar el resum per a reduir el cost computacional de l'operació. El resultat és, a efectes pràctics, perfectament equivalent.

- En general, cada vegada que s'obre el document se'n comproven les signatures, per tant requereix disposar dels certificats instal·lats en el sistema o l'accés als repositoris que els contenen.

- Amb la signatura digital s'assoleix també una altra de les propietats de la seguretat de la informació (si bé no essencial), que és el no repudi. Un cop verificada la signatura del document o del missatge, l'usuari no pot negar la seva acció perquè tècnicament es pot demostrar el contrari.

- La signatura digital es pot combinar amb el xifratge del contingut, però cal tenir en compte que es tracta de dues operacions diferents: el xifratge del contingut es realitza amb la clau pública del destinatari (per a que el pugui desxifrar amb la seva clau privada) i la signatura digital utilitza la clau privada de l'emissor (per a que el receptor la pugui desxifrar amb la clau pública de l'emissor).

- Les administracions públiques (entre altres organismes) poden proporcionar certificats digitals legalment vàlids a les persones físiques i jurídiques per a realitzar les operacions anteriors amb els mateixos efectes legals que una signatura física (per exemple, els documents d'identitat electrònica).

De la mateixa manera que amb el xifratge, el nombre d'aplicacions que donen suport a les operacions de signatura digital continua creixent, especialment aquelles destinades a validar la informació que pot tenir implicacions legals (per exemple, la signatura de contractes o les declaracions d'impostos).

3.4.3. L'esteganografia

Si l'objectiu de la criptografia és modificar la informació per a que només puguin accedir aquells que tenen la clau de xifratge, l'esteganografia agrupa totes aquelles tècniques que serveixen per a ocultar la informació privada entre dades públiques (sense alterar la percepció del conjunt).

Els casos més habituals consisteixen en introduir un text dins d'un fitxer d'imatge o de so, modificant els bits menys significatius (aquells que no produeixen alteracions destacables en el resultat) per a incloure la informació desitjada. La mida i l'aparença del fitxer seran el mateix, per tant serà molt difícil constatar les diferències entre el fitxer original i el modificat, excepte en el resultat de la funció resum, que serà diferent perquè la codificació interna del fitxer ha estat alterada.

Tot i que l'ús de l'esteganografia requereix tècniques i programari especialitzat per a introduir les dades en els fitxers i poder recuperar-les, és una bona manera de protegir la informació amb mitjans aparentment irrellevants.

Resum

No sembla fàcil garantir les propietats de seguretat de la informació en un món com l'actual. L'omnipresència de la informació, la complexitat de la tecnologia, l'exposició constant dels serveis, l'evolució ràpida dels riscos o la contenció dels atacs són només algunes de les situacions a les quals s'ha de fer front per a assegurar la informació.

Si bé aconseguir que el sistema sigui completament segur en tota circumstància és una fita difícilment assolible, la tecnologia ofereix suficients mecanismes de seguretat per a protegir la informació en la majoria de situacions. La implantació de mesures requereix l'anàlisi de l'organització, la identificació correcta dels requisits de seguretat, la bona selecció i combinació dels mecanismes (tècnics, organitzatius, etc.), i la implantació coherent i el manteniment proactiu posterior de totes mesures per tal que la seguretat sigui una realitat efectiva i durable.

De fet, en el context de seguretat informàtica no es pot perdre mai la visió de conjunt, perquè un sistema és tant segur com ho és la cadena de procés de la informació que suporta. Aquest cicle de vida és el que ha de guiar totes les actuacions dirigides a garantir les propietats de seguretat de la informació.

Bibliografia

Codolà, S. *Seguridad y auditoría de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Colobran, M. *Gestión de incidentes de seguridad*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Colobran, M.; Morón Lerma, E. (2004). *Introducción a la seguridad informática*. Barcelona: Planeta UOC.

Cruz, A. *Análisis de riesgos*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Domingo, J.; Herrera, J.; Rifà, H. *Criptografía*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

García, J.; Perramon, X. *Seguridad en redes de computadores*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Introducción a la seguridad de la información*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Garre, S. *Implantación de un sistema de gestión de la seguridad de la información (SGSI)*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Jimeno, M. T.; Míguez, C.; Matas, A. M.; Pérez, J. (2008). *Guía práctica hacker*. Madrid: Anaya Multimedia.

Perramon, T. *Sistemes de comunicacions*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Prieto, J. *Comunicacions sense fils*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

Rifà, H. *Infraestructura de clave pública*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.