Universitat d'Alacant
Universidad de Alicante

BIBLIOTECA UNIVERSITARIA

Seguretat Informàtica

Material formativo

BUA
Biblioteca de la Universitat d' Alacant
Biblioteca de la Universidad de Alicante

CI2
COMPETENCIAS INFORMÁTICAS E INFORMACIONALES

SEGURETAT INFORMÀTICA

Seguretat informàtica

Quan parlem de seguretat informàtica ens estem referint, en el fonamental, a la protecció d'informació continguda sota la forma d'arxius informàtics de qualsevol tipus, així com de la infraestructura computacional física (dispositius electrònics i xarxes de connexió) que els suporta enfront de qualsevol tipus d'amenaça, entenent per tal tot aquell factor que puga afectar a l'acompliment directe del sistema informàtic o de la informació i resultats obtinguts del mateix.

Comptat i debatut, la seguretat informàtica té per fi protegir la integritat i privadesa de la informació emmagatzemada o tractada per un sistema informàtic enfront de qualsevol amenaça.

"El únic sistema segur és aquell que està apagat i desconnectat, enterrat en un refugi de formigó, envoltat per gas verinós i custodiat per guardians ben pagats i molt bé armats. Encara així, jo no apostaria la meua vida per ell" (Eugene Spafford, expert en seguretat de dades).

Encara que cap sistema pot considerar-se segur al 100%, sí que podem aplicar una sèrie de protocols, normes, restriccions, polítiques d'accés i plans de contingència que permeten mantenir la seguretat en un nivell òptim. A més, com sol ocórrer en la majoria d'àmbits relacionats amb la seguretat, un dels factors fonamentals a tenir en compte segueix sent la formació de les persones usuàries, perquè coneixent com protegir-se de les amenaces, sàpien utilitzar els recursos que disposa de la millor manera possible.

Altres experts, atès que parlar de seguretat en termes absoluts és impossible, prefereixen parlar de Fiabilitat del sistema.

Fiabilitat és la probabilitat que un sistema es comporte tal com s'espera d'ell.

En el blog del servei d'informàtica de la Universitat d'Alacant hi ha entrades sobre la seguretat que poden resultar-te d'interès com a informació complementària a aquest tema.
Pots consultar les entrades relacionades amb temes de seguretat en el següent enllaç http://blogs.ua.es/si/tag/seguridad/

Característiques d'un sistema segur

1-Integritat

La informació no pot ser modificada per qui no estiga autoritzat. La informació ha de mantenir-se amb exactitud, tal qual va ser generada, sense ser alterada per persones o processos informàtics no autoritzats per a açò.

Es produeix una violació de la integritat quan una persona, aplicació o procés modifica o esborra dades importants, bé accidentalment, bé de forma dolosa.

La modificació de les dades per persones autoritzades ha de quedar registrada, assegurant la seua precisió i confiabilitat.

Com podem assegurar la integritat de la informació continguda en un missatge? Doncs adjuntant un conjunt de dades (metadades) de comprovació d'aqueixa integritat.

La signatura digital és un dels pilars de la seguretat de la informació

2-Confidencialitat

Les dades només han de ser llegibles per als persones autoritzades; la informació no ha de divulgar-se a persones, entitats o processos no autoritzats.

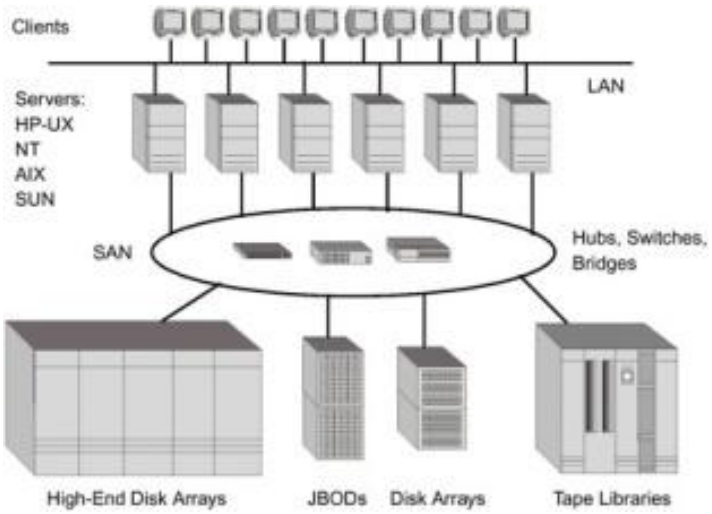
La pèrdua o violació de la confidencialitat de la informació pot adoptar múltiples formes, no totes relacionades amb mitjans informàtics: pot produir-se, per exemple, quan algú mira per sobre dels nostres muscles mentre tenim informació confidencial en la pantalla, o si en una transacció electrònica el nombre de la nostra targeta de crèdit no s'envia xifrat.

3-Disponibilitat

La información ha de estar disponible para las personas, procesos o aplicaciones que deban acceder a ella en el momento en el q La informació ha d'estar disponible per a les persones, processos o aplicacions que hagen d'accedir a ella en el moment en el qual ho requerisquen.

Parlem d'alta disponibilitat quan un sistema està implementat o dissenyat de tal manera que garanteix la continuïtat operacional absoluta durant un període de temps donat, és a dir, que es garanteix que el sistema estiga disponible en tot moment, evitant qualsevol interrupció del servei (ja siga per corts d'energia, fallades del maquinari o problemes de programari)

La gamma de solucions de disseny dependrà del nivell de servei que es vulga proporcionar i de la informació que desitgem protegir, però comprendria, entre uns altres, xarxes de comunicacions redundants, xarxes d'àrea d'emmagatzematge (SAN), clusters d'emmagatzematge en discos durs, servidors espill, equips de xarxa d'alta disponibilitat o servidors de replicació de dades.



Una **SAN** (Storage Area Network, o Red de Área de Almacenamiento) es una red dedicada de almacenamiento que proporciona acceso de nivel de bloques a varios **LUN** (Logical Unit Number, o Número de Unidad Lógica), que viene a ser un disco virtual proporcionado por la SAN.

4-Autenticació

El generador de la informació, o el que accedisca o l'edite, ha d'estar perfectament identificat en tot moment, de forma unívoca i inequívoca.

En els sistemes informàtics, l'autenticació s'implementa mitjançant una combinació de comptes de la persona usuària (que gradua el privilegi d'accés als diferents nivells d'informació) i contrasenya d'accés

5-Irrefutabilitat (No-Rebuig o No-Repudi)

Impossibilitat, per a una persona usuària, programa o procés, de negar (rebutjar) l'autoria d'una acció.

En cas de participar en un procés de comunicació, podem parlar de

- **no repudi d'origen**: la persona emissora no pot negar que va realitzar un enviament perquè la persona receptora té una prova infalsificable de l'origen de l'enviament.
- **no repudi de destinació**: la persona receptora no pot negar que va rebre el missatge perquè la persona emissora té proves de la recepció.

El no repudi evita que la persona emissora o la persona receptora puguen negar la transmissió d'un missatge.

La seguretat informàtica, per tant, protegeix la integritat, confidenciabilidad i disponibilitat de la informació.

Vulnerabilitats

Una vulnerabilitat és la debilitat de qualsevol tipus que compromet la seguretat d'un sistema informàtic.

Podemos agrupar las vulnerabilidades informáticas en función de varios factors:

Factors de Disseny

- Debilitat en el disseny de protocols utilitzats en les xarxes.
- Polítiques de seguretat deficients, pobrament dissenyades o inexistents.

Factors de Implementació

- Debilitat en el disseny de protocols utilitzats en les xarxes.
- Errors de programació no depurats
- Existència de "puertas posteriors" (backdoors) en els sistemes o aplicacions informàtics
- Fallades no corregides dels fabricants

Factors d' Úso

- Configuració incorrecta dels sistemes informàtics
- Desconeixement i falta de compromís de les persones usuàries i de les persones responsables dels serveis TIC
- Disponibilitat d'eines que faciliten els atacs.
- Limitacions oficials (a nivell governamental) de les tecnologies de seguretat.

Factors de Vulnerabilitat del dia zero (0-day o zeroday)

Són aquelles vulnerabilitats conegudes per a les quals encara no s'han creat pegats, revisions o actualitzacions, i que s'empren per a dur a terme un atac.

El nom de 0-day (dia zero) obeeix al fet que no existeix cap revisió o pegat (correcció) per a eliminar o mitigar l'aprofitament d'aqueixa vulnerabilitat per part d'atacants maliciosos.

Fa falta aclarir també que aqueixa vulnerabilitat és usualment desconeguda tant per a les persones programadores del programari com per al gran públic (que ignoren que tenen una bretxa potencialment perillosa en els seus sistemes), però no així per als potencials atacants, entre els quals sí circulen llistats amb aquestes vulnerabilitats.

Llavors, què és exactament una vulnerabilitat?

Per a construir-nos una imatge mental més clara, podem representar-nos el programari informàtic com una malla metàl·lica composta per milions de línies de codi entreteixides. Però ull, en el cas del programari, aquesta malla no seria plana, sinó tridimensional, amb un nivell de complexitat notable.

Aquesta complexitat dificulta la tasca de trobar fallades, punts febles o funcions errònies dins del codi, de tal manera que aquests errors solen escapar a les complexes eines de verificació automatitzada del codi.

Com es troben llavors aquests punts febles, aquestes vulnerabilitats del codi? Doncs

- per una anàlisi minuciosa i detallat
- per un ús indegut
- senzillament, de manera accidental.

Quan es produeix una vulnerabilitat, el punt feble generat pot causar que els programes o els sistemes operatius es comporten de manera estranya, no desitjada o no planificada.

Existeix una varietat quasi infinita de possibles respostes del sistema a aquestes fallades, depenent del tipus d'error i de la gravetat del mateix: des de la fallada molt localitzada i sense major importància, al bloqueig del programa o aplicació o, en els casos més greus, la caiguda total del sistema.

Un atacant que conega aquesta vulnerabilitat pot utilitzar aquest comportament estrany (i, per tant, no desitjat) per a crear una bretxa per on penetrar en el sistema i aconseguir que s'execute el seu codi maliciós, o apoderar-se d'informació sensible.

Classificació de les amenaces informàtiques

De forma general, podem agrupar les amenaces informàtiques en dos blocs principals:

- Amenaces físiques
- Amenaces lògiques

Aquestes amenaces, tant físiques com a lògiques, són materialitzades bàsicament per:

- Persones
- Programes o aplicacions específiques
- Catàstrofes naturals

Els atacs a la baula més feble: les persones

El punt més feble d'un sistema informàtic és, quasi sempre, les persones relacionades en major o menor mesura amb ell.

Mucho más sencillo que acceder a un sistema bien protegido es acceder (y engañar o manipular) a las personas que tienen acceso al mismo.

Enginyeria social

És la pràctica d'obtenir informació confidencial mitjançant la manipulació d'usuaris amb accés al sistema.

Contra el que poguera semblar, el punt més feble en la seguretat dels sistemes informàtics és el factor humà: sol ser molt més fàcil obtenir accés a un sistema gràcies a la manipulació i l'engany de les persones que mitjançant atacs informàtics de força bruta

Recorda: En qualsevol sistema, les persones usuàries sempre són la baula més feble.

Tipus d'atacs d'enginyeria social

1-Hunting: es tracta d'obtenir la informació amb la menor exposició directa possible, amb el menor contacte personal. S'orienten a la consecució d'una dada o acció molt concret (una clau, desactivar una configuració)

2-Farming: cerca mantenir l'enagño el major temps possible, per a explorar al màxim els coneixements, recursos o posició de la víctima. Recorre a granges d'identitats prèviament robades per a crear falsos perfils atractius

Segons el famós hacker Kevin Mitnick, l'enginyeria social té la seua base en quatre elementals principis:

- Tots volem ajudar
- No ens agrada dir No
- La primera actitud sol ser la de confiar en l'altra persona
- A totes les persones ens agrada ser lloades

Tècniques d'Enginyeria Socialocial

1-Pretextos

Es crea un escenari fictici perquè la víctima revele una informació que, en circumstàncies normals, no revelaria.

Normalment la creació d'escenaris ficticis requereix una recerca prèvia de la víctima per a aconseguir dades personals sensibles i fer així més creible la suplantació i fer creure a les víctima que és legítima.

En ocasions, tot el que es necessita per a crear un escenari pretextual és una veu que inspire autoritat, un to seriós i capacitat d'improvisació.

L'atacant pot fingir, per exemple, ser una persona emprada del seu banc, o el director o directora d'una altra sucursal de l'empresa i aconseguir així dades sensibles.

2-Shoulder surfing

Consisteix a espiar físicament a les persones usuàries fins a poder obtenir les claus d'accés al sistema.

El cas típic és el de les persones usuàries que apunten les seues contrasenyes d'accés en un paper al costat del monitor o pegades al teclat.).

3-Phishing (suplantació de personalitat)

L' o l'atacant es fa passar per una persona o empresa de confiança, mitjançant una comunicació oficial electrònica amb aparença de veracitat (mails, missatges de missatgeria instantània, fins i tot cridades telefòniques) per a fer-se amb les contrasenyes, les claus d'accés de la víctima o les seues dades bancàries.

La víctima, en confiar en el remitent, envia les dades a l'atacant.

La identificació dels atacs phishing és complexa si està ben realitzada, ja que els components del missatge enviat són indistinguibles d'un missatge legítim.

4-Masquerading (mascarada)

Consisteix a suplantar la identitat d'una persona usuària legítima d'un sistema informàtic, o de l'entorn del mateix.

Aquesta suplantació pot realitzar-se electrònicament (un usuari o usuària utilitza per a accedir a una màquina un login i password que no li pertanyen) o en persona.

El masquerading és més habitual en entorns on existeixen controls d'accés físic, i on un intrús pot `enganyar' al dispositiu o persona que realitza el control

Dos exemples podrien ser l'accés a un area restringida amb una targeta d'identificació robada que un lector automatitzat accepta, o amb un carnet falsificat que un guàrdia de seguretat dóna per bo.

5-Baiting

Ho podríem traduir de forma més o menys lliure com encebar, o fer picar l'ham.

S'utilitza un dispositiu d'emmagatzematge extraïble (CD, DVD, USB) infectat amb un programari maliciós, deixant-ho en un lloc en el qual siga fàcil de trobar (per exemple, banys públics, ascensors, voreres, etc.) per part de la víctima o víctimes les dades de les quals precisa l'o l'atacant. Quan la víctima trobe aquest dispositiu i ho introduïsca en el seu ordinador, el programari maliciós s'executarà de manera inadvertida i possibilitarà que l'hacker puga accedir a les dades de l'usuari o usuària

6-Scavening (Basureo)

Consisteix a obtenir informació deixada en o al voltant d'un sistema informàtic després de l'execució d'un treball.

El basureo pot ser:

- **Físic**, com cercar en poals de brossa (trashing, traduït també per basureo) llistats d'impressió o còpies de documents
- **Lògic**, com analitzar buffers d'impressores, memòria alliberada per processos, o blocs d'un disc que el sistema acaba de marcar com a lliures, a la recerca d'informació.

7-Vishing

El Vishing (de la unión de voice phishing, o suplantació de veu o telefònica) consisteix a oferir a la víctima un número de telèfon fals per a comunicar-se, fingint ser el vertader, i a continuació obtenir dades sensibles com a nombres de targetes de crèdit o claus i persones usuàries.

Modus Operandi:

- Es realitzen trucades automatitzades aleatòriament fins que algú contesta
- S'informa a l'interlocutor o interlocutora que la seua targeta de crèdit sembla estar sent utilitzada de manera fraudulenta i que cal actualitzar o confirmar les seues dades personals
- Se li facilita un número de telèfon perquè realitze aquestes gestions
- En realitzar la trucada, escolta a l'altre costat un enregistrament idèntic a la d'un servei d'atenció telefònica estandar
- Després, se li sol·liciten dades sensibles, com a números de compte, de targetes de crèdit, dates d'expiració i claus i noms d'usuari.

Una vegada obtinguts aquestes dades, els o les ciberdelincuentes ja poden dur a terme operacions fraudulentes amb la targeta de la víctima.

La forma més senzilla d'evitar el vishing és no oferir informació sensible sense comprovar les vertaderes identitats dels nostres interlocutors, i cridar sempre als nombres oficials que tinguem de les nostres entitats.).

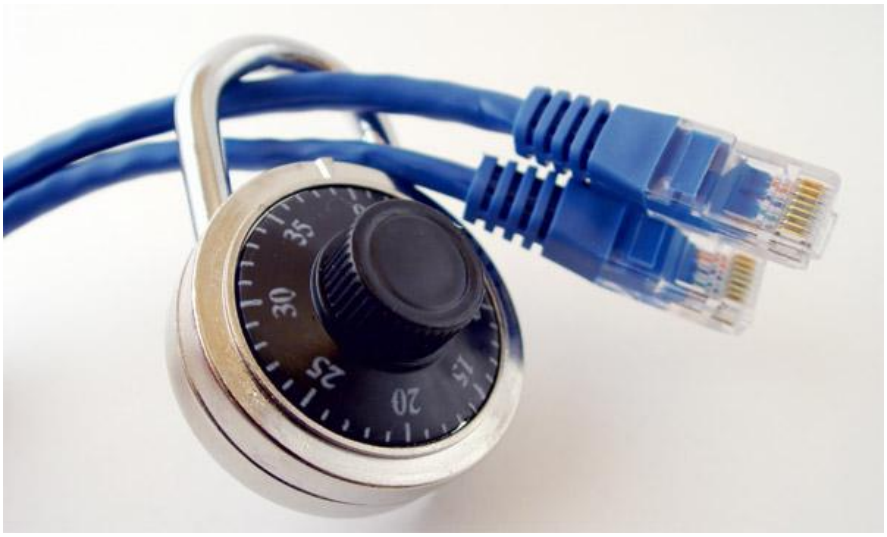
Tipos de amenazas físicas de los sistemas informáticos

Podem caracteritzar els següents tipus d'amenaces físiques:

1-Accés Físic

Sovint es descura la seguretat sobre l'accés, però cal tenir en compte que quan existeix accés físic a un recurs ja no existeix seguretat alguna sobre el mateix, amb el consegüent risc.

Un error típic de seguretat per accés físic és el de preses de connexió a la xarxa informàtica no controlades, d'accés lliure: un atacant amb els suficients coneixements tècnics pot causar greus danys.



Per açò, en el campus de la UA tots els accessos de l'alumnat a la xarxa estan autenticats amb el teu usuari i clau de Campus Virtual, bé mitjançant wifi (has hagut d'autenticar-te prèviament en eduroam), bé mitjançant els ordinadors d'ús públic (que requereixen també identificació prèvia).

Els ordinadors de consulta de catàleg, d'accés lliure, tenen limitades les funcionalitats i la navegació. A més, les xarxes d'accés públic i la xarxa interna de la UA estan virtualizadas i aïllades.

2-Desastres de l'entorn i avaries del maquinari

Dins d'aquest grup estarien inclosos successos que, sense arribar a la categoria de desastres naturals, poden tenir un impacte igual d'important si no s'habiliten les mesures de protecció adequades: parlem, per exemple, de becs de sobretensión que puguen cremar components, apagades que afecten als servidors (i deixen caiguda la web de la UA i tots els seus serveis), incendis, apagades i similars.

Tampoc podem oblidar els errors o danys en el maquinari que es pot presentar en qualsevol moment. Per exemple, danys en processadors, en memòria RAM, en discos durs o, en definitiva, en qualsevol element del maquinari.

Tots aquests factors fan que la información

- deixe d'estar accessible (de manera temporal o, en el pitjor dels casos definitiva)
- deixe de ser fiable

Hem de prevenir al màxim aquests incidents amb les corresponents mesures de protecció contra sobretensiones (sistemes que tallen l'allimentación elèctrica abans que la sobretensión afecte als components informàtics), amb el manteniment operatiu de dispositius SAI (Sistemes d'Alimentació Ininterrompuda, que proporcionen alimentació durant un temps limitat davant caigudes de subministrament elèctric) i amb els sistemes de protecció anti-incendis (detectors de fum, ruixadors automàtics o fire sprinklers)

3-Radiacions electromagnétiques

Sabem que qualsevol aparell elèctric emet radiacions i que aquestes radiacions és poden capturar i reproduir si és disposa de l'equipament adequat.

Per exemple, un possible atacant podria capturar les dades teclejades en un teclat sense fil (no diem que siga fàcil, però és factible), per no parlar de les xarxes wifi obertes, un autèntic coladero de seguretat.

4-Desastres naturals

En la nostra zona geogràfica no són gens rares les gotes fredes, les inundacions per riuades o les pluges torrencials puntuals.

La pròpia Universitat va patir una greu riuada en 1997, que va afectar greument, entre uns altres, a l'edifici de la Biblioteca General, el Dipòsit de la qual va quedar totalment anegado.

Aquestes situacions han de ser sempre previngudes amb les corresponents mesures protectores (recintes estancs a prova d'inundacions, per exemple)

Catàleg de les principals amenaces lògiques dels sistemes informàtics

Les amenaces lògiques comprenen una extensa sèrie d'aplicacions que amenacen la integritat dels sistemes informàtics, i que poden ser de dos tipus principals:

- **Malware** (malicious programari, o programari maliciós): aplicacions dissenyades intencionalmente per a danyar el sistema o per a proporcionar accés al mateix.
- **Bugs o errores de programación**: programari mal dissenyat que, per error, ocasiona un forat de seguretat que pot acabar provocant els mateixos riscos que el malware.

Exploits

Un exploit (d'explotar, o aprofitar) és una aplicació, fragment de programari o arxiu de seqüència de comandos (script) dissenyat per a aprofitar una determinada bretxa de seguretat o vulnerabilitat d'un sistema informàtic per a aconseguir un comportament no previst o no desitjat del mateix.

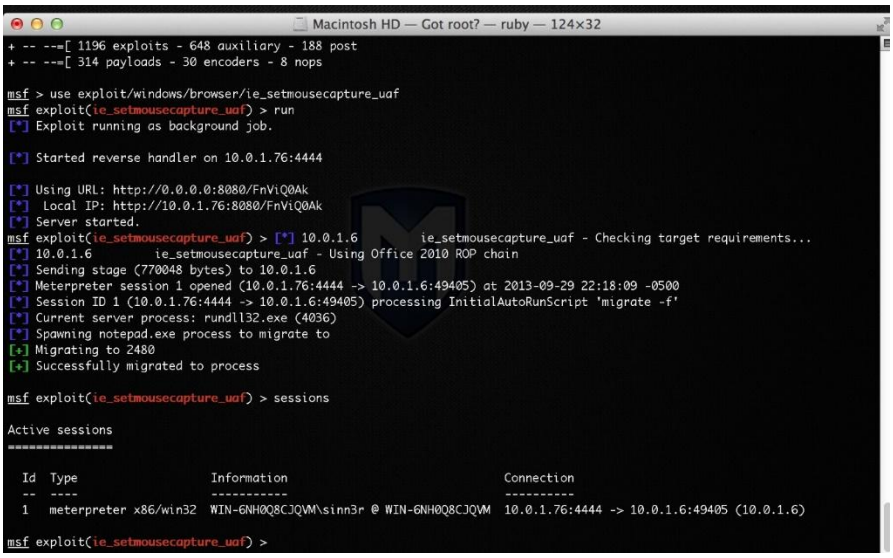
Exemples d'exploits: obtenir un accés no autoritzat, prendre el control de tot el sistema o aconseguir els nivells de privilegi d'usuari o usuària més alts, o aconseguir un atac de denegació de servei.

Podem classificar els exploits, segons la seua forma de contacte amb la vulnerabilitat de softare, com:

- Exploit remots: entra en contacte amb la vulnerabilitat mitjançant una xarxa de comunicacions (bé des d'un altre equip de la mateixa xarxa, bé en una intrusió des d'un sistema extern)
- Exploit local: Abans d'executar l'exploit, necessitem tenir accés al sistema vulnerable. També pot donar-se el cas que un atacant remot tinc accés a la màquina local gràcies a un exploit remot
- ClientSide Exploit, o Exploit del costat del client: En aquest cas, l'exploit aprofita vulnerabilitats d'aplicacions àmpliament utilitzades en els entorns corporatius ofimàticos

Els ClientSide Exploits s'aprofiten de les vulnerabilitats dels navegadors (Internet Explorer, Google Chrome o Mozilla Firefox), lectors de PDF (Tova Acrobat Reader), reproductors Flaix dels navegadors, reproductors multimèdia (Windows Mitjana Player) o aplicacions ofimàtiques (MS Office).

Aquest tipus d'exploit requereix de la intervenció de la persona usuària, ja que l'exploit està en fitxers interpretats que obrin aquestes aplicacions i han de ser carregats (executats) manualment pel propi usuari (que desconeix, per descomptat, el risc al que s'enfronta).



Aquests fitxers arriben a la màquina objectiu principalment mitjançant email o un pendrive infectat.

Una vegada la persona usuària llança l'arxiu, el programa objectiu (per exemple, Word) ho carregarà i executarà i, llevat que siga detectat pel firewall o l'antivirus, aprofitarà la bretxa de seguretat per a aconseguir els seus objectius.

Un exploit pot donar-se en molts tipus de sofware maliciós, com a virus, cucs o scripts.

Els exploits són específics de cada sistema operatiu, de cada configuració particular d'un sistema i del tipus de xarxa en la qual es troben. Poden haver-hi exploits diferents per a atacar la mateixa vulnerabilitat en una aplicació que córrega en diferents sistemes operatius

Virus informàtics

Un virus informàtic és un malware (programari maliciós) que 'infecta' amb el seu codi a altres arxius o executables bàsics del sistema amb la intenció de modificar-los i aconseguir així alterar el funcionament de la màquina atacada sense el coneixement ni el consentiment de la persona usuària.

Els seus objectius poden ser varis, des de ralentir el sistema a destruir tota la informació del mateix o corrompre la partició d'arrencada. En qualsevol cas, els danys se centren en cadascuna de les màquines infectades.

Els virus només infecten al sistema operatiu per al qual van ser dissenyats; hi ha molt pocs casos de virus multiplataforma.

Como funcionen els virus?

- La persona usuària executa el programa infectat (amb el seu desconeixement). En altres ocasions ni tan sols és necessària la intervenció de la persona usuària (per exemple, en carregar una web fraudulenta infectada que executa un script aprofitant una vulnerabilitat del navegador, descarrega l'executable en l'ordinador de l'usuari o usuària i ho executa).

- El codi del virus es queda resident (allotjat) en la memòria RAM del dispositiu. En aquest moment, encara que esborrem el primer executable, el virus seguiria resident en la RAM (llevat que apaguem la màquina)

- Des de la RAM, el virus va prenent el control dels serveis bàsics del sistema operatiu segons aquests vagen sent anomenats (utilitzats) pel sistema

- Finalment, el virus afig el seu codi als programes infectats que han sigut cridats pel sistema i els grava en disc, amb la qual cosa el seu procés de replicacíon s'ha completat. El programa infectat, al seu torn, podrà infectar a altres aplicacions cada vegada que s'execute

Principals vies d'infecció dels virus

- Arxius adjunts en Spam (correu-vos no sol·licitats)
- Llocs web insegurs que han sigut infectats
- Qualsevol dispositiu extern infectat (pendrive USB, CDs, DVDs)
- Xarxes de descàrregues P2P
- Xarxes socials

Mecanismes d'infecció dels virus

Com infecten els virus?

Els virus poden infectar de dues maneres diferents:

- La més usual és la que hem vist: consisteix en "injectar" una porció de codi maliciós en un arxiu executable normal. D'aquesta forma, el virus es manté latent en l'arxiu i quan la persona usuària execute aqueix arxiu, a més de les accions normals codificades, s'executen les instruccions del virus.

- La segona forma d'infectar consisteix a substituir a l'arxiu original i renombrar aquest per un nom conegut només pel virus. Així, en executar l'arxiu primer s'executa el maliciós i, en finalitzar les instruccions, aquest flama a l'arxiu original, ara renombrado.

Cucs informàtics

Un cuc és un programa maliciós que realitza còpies de si mateix en diferents ubicacions de l'ordinador infectat amb l'objectiu de propagar-se a altres ordinadors, contagiar al major nombre possible de màquines i acabar col·lapsant les xarxes informàtiques, impedint el treball de les persones usuàries.

A diferència dels virus clàssics, els cucs no infecten arxius ni precisen de la intervenció de les persones usuàries per a expandir-se. Poden fer-ho de dues formes:

- Utilitzant vulnerabilitats del sistema operatiu per a copiar-se a tots els ordinadors connectats en una xarxa
- Propagant-se per internet a través del correu electrònic, xarxes P2P (peer-to-peer, o comunicació entre parells) o missatgeria instantània.

Una diferència important entre els virus clàssics i els cucs informàtics és que els virus sempre corrompen arxius de la màquina a la qual infecten, mentre que els cucs no necessiten alterar arxius: es copien a si mateixos i es queden residents en memòria.

També esmentarem que els virus solen centrar-se a causar danys a les màquines individuals, mentre que els cucs quasi sempre causen problemes a les xarxes.

L'objectiu dels cucs no és necessàriament provocar un dany al sistema, sinó expandir-se a la major quantitat d'equips que li siga possible.

En alguns casos, els cucs transporten altres tipus de malware, com troyanos o rootkits; en uns altres, simplement intenten esgotar els recursos del sistema com a memòria o ample de banda mentre intenta distribuir-se i infectar més ordinadors.

Troyanos

Un troyano informàtic és un tipus particular de malware que, de cara a l'usuari o usuària, es presenta com un programa inofensiu. En ser executat, no obstant açò, proporciona a l'atacant accés remot a l'equip infectat.

Pren el seu nom, com pots imaginar, de la història del Cavall de Troia narrada per Homer en l'Odissea.

Hi ha multitud de tipus de troyano, però en la seua immensa majoria el que fan és crear una porta posterior (backdoor) perquè l'atacant maliciós pot accedir al sistema de forma remota i realitzar diferents accions sense necessitar permisos. Aquestes accions dependran del nivell de privilegi que tinga l'usuari en la màquina remota, i de les característiques peculiars del troyano.

En els últims temps, els troyanos s'usen, sobretot, per a robar dades confidencials i bancaris de les persones.

Algunes de les accions que poden dur a terme els troyanos:

- Robatori d'informació personal: informació bancària, contrasenyes, codis de seguretat...
- Esborrat, modificació o transferència d'arxius (descàrrega o pujada)
- Monitoratge del sistema i seguiment de les accions de l'usuari o usuària
- Monitorizar les pulsacions del teclat
- Realitzar captures de pantalla
- Utilitzar la màquina com a part d'una botnet (per a realitzar atacs de denegació de servei o enviament de spam).
- Sacar fotos por la webcam (si t Traure fotos per la webcam (si té)

A diferència dels virus i els cucs, els troyanos no poden replicar-se per si mateixos.

Ramsonware

Un ransomware (acrònim de ransom per rescat ware per programari), és un tipus de malware que restringeix l'accés a determinats arxius i carpetes del sistema infectat, o fins i tot al sistema complet, i que demana un rescat monetari a canvi d'eliminar aqueixa restricció d'accés. Els arxius i carpetes solen ser xifrats

El ramsomware es transmet normalment ben com un troyano (camuflat en arxius adjunts, vídeos descarregats, o programes baixats de llocs dubtosos), bé com un cuc (infectant al sistema operatiu a través de les vulnerabilitats del mateix).

Una vegada activat, el ramsonware bloqueja els arxius i llança els missatges d'advertiment, a voltes fins i tot amb fotos tretes amb la nostra pròpia camara web.

L'última infecció important de ransomware ha sigut la de WannaCry, al maig de 2017, que a Espanya va arribar a afectar a grans empreses com a Gas Natural, Iberdrola o la pròpia Telefònica, mentre que en el Regne Unit afecte a una gran part del sistema hospitalari.

Altres infeccions famoses han sigut les de CryptoLocker, CryptoWall o el letal Mamba, un ramsomware de xifrat de disc complet (FDE o Full Disk Encryption: xifra el disc complet i el sistema ni tan sols pot arrancar)

Al ransomware també se li coneix per rogeware o scareware

Rootkits

Un encobridor o rootkit és una aplicació de programari que oculta a altres aplicacions malicioses i a si mateixa evitant la seua detecció tant per part de l'usuari o usuària atacada com dels antivirus.

El seu nom ve de la combinació de les paraules angleses root (arrel, que sol ser el nom del compte d'administrador en els sistemes operatius UNIX / Linux) i kit (conjunt d'eines, en referència al conjunt d'accions que realitza aquest programa).

Els rootkits no poden considerar-se malware per si mateixos lloc que, en realitat, no realitzen accions malicioses, però sí se'ls associa al malware perquè oculten les accions perjudicials que altres aplicacions, processos, arxius, directoris, claus de registre i ports desenvolupen en l'equip atacat.

Procés d'infecció per un rootkit

1- La persona atacant aconsegueix accedir al nivell root (raiz o administrador) del sistema per qualsevol dels mitjans habituals per a açò:

- aprofitant vulnerabilitats conegudes
- crackeando la contrasenya (amb les aplicacions necessàries per a açò)
- mitjançant enginyeria social

2- La persona atacant instal·la i executa el rootkit, que oculta el seu propi rastrol

3- La persona atacant introdueix més malware per a obtenir el control total de l'equip, la qual cosa no és detectat ni pels antivirus ni per l'usuari o usuària en quedar camuflat pel rootkit.

Classificació dels rootkits

Classificació dels rootkits:

- **Els de nucli o kernel**: són, amb diferència, els més perillosos i de detecció més complicada. Afigen o modifiquen part del kernel o nucli, per exemple mitjançant un controlador o un module. Parchean les trucades al sistema amb versions que camuflen i oculten les activitats intrusivas del malware, impossibilitant la seua detecció.

- **Els de nivell d'aplicació**: substitueixen els arxius executables amb versions infectades, o modifiquen les aplicacions existents amb pegats o codi injectat. Són més fàcils de detectar i eliminar que els rootkits de nucli.

Spyware

Són programes espia que recopilen informació de la persona usuària sense el seu consentiment, i després l'envien a la persona atacant.

El terme spyware s'empra de forma laxa per a fer-se extensiu a altres aplicacions que no són estrictament spyware però que recopilen algun tipus d'informació privada, per a després mostrar pop-ups (finestres emergents) no desitjades.

El spayware s'autoinstala en el sistema de tal forma que s'executa cada vegada que s'arranca l'ordinador, consumint recursos de processador i memòria.

Típicament, el spyware recopila dades sobre els hàbits de navegació o comportament en la web de l'usuari o usuària atacada, les webs que visita, amb quina freqüència i el temps que roman en el lloc, o monitorizando les aplicacions que s'executen en l'ordinador.

El spyware provoca inestabilitat en el sistema i ralentització del mateix.

Adware

La combinació de les paraules angleses *Advertising* (publicitat) i *Software* ja ens dóna una pista de les funcions d'aquest malware:

És un programari maliciós que s'instal·la en l'ordinador de la víctima amb la finalitat de descarregar i mostrar en l'ordinador de la víctima tot tipus de continguts publicitaris, en forma de finestres emergents (pop-ups) o bàners i, en els casos més agressius, instal·lant barres d'eines, modificant els favorits dels navegadors i canviant la pàgina d'inici dels mateixos perquè sempre naveguem per les seues xarxes publicitàries.

L'Adware, o **Advertising-Supported Programari** (aplicació recolzada amb publicitat) sol venir camuflat en programes shareware i, s'instal·la en acceptar els termes legals durant la instal·lació dels mateixos.

És un malware més molest que perillós, encara que pot arribar a bloquejar-nos l'ordinador si obri massa finestres emergents.

L'adware no produeix una modificació explícita que danye el sistema operatiu, però sí disminueix el rendiment de l'equip i de la navegació per la xarxa ja que utilitza recursos del processador, la memòria i consumeix de forma notable l'ample de banda.

En general, l'adware utilitza informació recopilada per algun spyware per a decidir què publicitat mostrar, encara que els llocs de joc, apostes i sexe quasi sempre figuren en el seu carrusel publicitari.

Backdoors o portes posteriors.

Les portes posteriors són bretxes de seguretat intencionades implementades en la codificació d'un sistema operatiu o una aplicació, que permeten saltar-se els sistemes de seguretat per a donar accés al sistema.

Comptat i debatut, els backdoors són entrades secretes que permeten entrar al sistema i fer-se amb el control del mateix.

En teoria, els programadors inclouen aquestes dreceres en els sistemes d'autenticació de les aplicacions perquè permeten depurar les fallades amb major velocitat.

Les agències de seguretat nacionals i els governs pressionen als fabricants de programari perquè implementen portes posteriors per a així poder espiar i fer-se amb la informació de les persones usuàries potencialment perilloses (terroristes, delinqüents)

Mesures de protecció

Cadascun de nosaltres som, en última instància, responsables de mantenir els nostres equips en condicions òptimes per a minimitzar el risc d'un atac, la qual cosa impllica, entre altres coses, tenir actualitzat l'antivirus, instal·lar i configurar un firewall o tallafocs (que monitorice les connexions entrants i sortints de l'ordinador), tenir actualitzat el sistema operatiu amb les últims pegats i actualitzacions, evitar navegar per llocs fraudulents, mantenir els navegadors lliures de complements o extensions que no siguen de confiança o ajustar els nivells de privadesa en els nostres perfils de les xarxes socials.

Açò quant a la part tècnica, que és relativament senzilla d'implementar. La part d'enginyeria social és, com ja hem esmentat, la baula més feble de la cadena, i és ací on hem de guiar-nos sempre pel principi de la prudència per a evitar robatori d'identitats o de claus.

A continuació ho veurem amb més deteniment.

Protecció en el correu electrònic

El correu electrònic és una de les eines més utilitzades i un canal molt usat pels atacants. És per açò que has de tractar d'augmentar la seguretat en ell amb l'objectiu de prevenir-te d'atacs deguts a l'ús descurat de l'e-mail.

Spam

Es diu spam (o correu brossa) a l'enviament de missatges massius no desitjats, normalment de remitent desconeggut.

La forma més comuna en la qual pots advertir el spam és en el correu electrònic però també es pot veure de manera semblant en l'ús de missatgeria instantània, cerques en Internet, blogs, mòbils, fòrums d'Internet, etc.

El spam ha resultat sempre econòmic per a les persones atacants ja que realitzar-ho no suposa cost més enllà de la gestió de les llistes de correu. És per açò que existeix una gran quantitat de serveis que tracten de publicitarse, atacants que tracten d'enviar virus i aprofitar les distraccions de les persones usuàries, etc. que fan ús del spam, el volum del qual de correu no desitjat és molt alt (en 2011 s'estima que la xifra de correus no desitjats és d'al voltant de 7 bilions de dòlars).

Actualment el spam és un tema de legislació en moltes jurisdiccions.

Recomanacions per a evitar l'enviament de correu massiu i la propagació de codi:

- No confies en correus que el seu remitent no resulte conegut o puga resultar sospitós; menys encara en arxius adjunts que puguen contenir aquests correus.

- Para esment a l'extensió dels arxius adjunts (indica que tipus d'arxiu és), ja que algunes tècniques d'engany alteren les extensions per a ocultar-se.
- Evita publicar la teua adreça de correu en pàgines web que tinguen una dubtosa reputació. Utilitzar un altre compte de correu electrònic pot ser útil per a protegir el teu compte de correu principal.
- No respongues mai a un correu no desitjat. D'aquesta manera no es perd temps ni es confirma a les persones responsables de fer spam, que el compte de correu està activa.
- Utilitza els filtres anti-spam que proporcione el proveïdor de correu electrònic; filtraran els correus en una altra carpeta i no et molestaran.
- Bloqueja les imatges en correus rebuts i accepta-les només quan consideres que el correu no és nociu (aquesta tècnica la solen utilitzar els proveïdors de correu).

Phishing

El phishing és una forma d'intentar adquirir informació (com a noms de persones, contrasenyes, detalls de targetes de crèdit, etc.) tractant d'emmascarar-se com una entitat de confiança utilitzant una comunicació electrònica.

El seu àmbit principal és **la banca**, i normalment consisteix a obtenir de manera fraudulenta informació confidencial i intentar realitzar algun tipus d'estafa relacionada amb obtenir diners de les persones.

També es pot veure aquesta tècnica d'estafa, encara que en menor mesura, mitjançant missatgeria instantània i fins i tot en trucades telefòniques.

Exemples de phishing són aquells correus que demanen introduir les dades en una pàgina per a evitar que un compte siga cancel·lat, enviar dades personals per correu electrònic, confirmació de dades, etc.

És molt important recordar que les entitats bancàries mai demanen dades personals mitjançant correu electrònic o un altre mitjà com tampoc demanen als persones usuàries que canvien la seua contrasenya. I menys alguna entitat bancària de la qual no s'és client demane dades bancàries.

S'estan realitzant moviments per a crear lleis que castiguen la pràctica de phishing i campanyes per a conscienciar a les persones i siguen advertits del seu perill.

Algunes mesures per a evitar ser víctimes del phishing són les següents:

- Les entitats bancàries no demanen mai dades confidencials per correu electrònic per a minimitzar les possibilitats que la tècnica tinga èxit. Per tant, mai reveles dades confidencials malgrat que el correu tinga un aspecte que puga semblar confiable.
- No faces clic en enllaços que apareixen en el cos del missatge ja que poden portar-te a una pàgina web clonada d'una pàgina d'entitat financera i fer-te creure que et trobes en la vertadera pàgina web.
- Comprova que l'adreça de la pàgina web utilitza un protocol segur. Per a açò fixa't en què l'adreça no comence per http:// sinó per https://, la "s" final en http indica que és una pàgina segura i que la informació que es diposita viatja de manera xifrada.
- Verifica que existeix un certificat digital en la pàgina web. El certificat es pot visualitzar fent clic sobre la icona de cadenat que ha d'aparèixer.
- Si tens dubtes de la legitimitat del correu electrònic, flama a l'entitat financera o acudeix a una oficina per a descartar un possible engany.
- Mai envies contrasenyes, nombres de targeta de crèdit o una altra informació confidencial a través de correu electrònic.
- Examina periòdicament els comptes bancaris, amb la finalitat de detectar possibles irregularitats relacionades amb la manipulació del compte o transaccions no autoritzades.
- Denuncia casos de phishing (quan pugues) a l'entitat de confiança. D'aquesta manera també col·labores amb la seguretat en la navegació en Internet i ajudes a tallar l'activitat del lloc maliciós.

Protecció enfront de finestres emergents (pop-ups)

Durant la navegació, és possible que apareguen finestres emergents (conegudes com popups).

Aquestes finestres emergents resulten poden resultar molestes o bé atraure't perquè faces clic en elles.

Cal anar amb compte ja que l'algunes es tracten de publicitat simplement, però unes altres animen a descarregar un programa (per a veure un video, per exemple) i poden contenir algun tipus de virus.

Existeixen utilitats per a bloquejar les finestres emergents, tant a nivell del propi navegador com de programari extern.

Ús de contrasenyes segures i renovació periòdica

La contrasenya és la forma d'autenticació que utilitzes per a provar la teua identitat o obtenir accés a un recurs.

A causa de la importància de la contrasenya, existeixen diverses **recomanacions** aque pots tenir en compte a l'hora de definir-la:

- Crea una contrasenya que utilitze diferents tipus de caràcters, com a lletres, nombres i símbols. T'aconsellem que tinga una longitud mínima de 8 caràcters i que no puga ser trobada en un diccionari.
- Utilitza una contrasenya creada de manera aleatòria, encara que tinguen l'inconvenient que són més difícils de memoritzar.
- Canvia les contrasenyes de manera periòdica.
- Et recomanem, en la mesura del possible, que utilitzes opcions d'autenticació que oferisquen les entitats bancàries o altres entitats, ja siga mitjançant un certificat digital o DNI electrònic, en lloc d'autenticar-te mitjançant l'ús de contrasenya.

És important que crees una contrasenya difícil d'esbrinar per a altres persones però que siga fàcil de recordar per a tu.

Ajusta la privadesa en navegació i xarxes socials

Navegació

Recomanacions per a millorar la seguretat en la navegació:

- Realitza la descàrrega d'aplicacions de seguretat únicament des de la pàgina web oficial, de manera que s'evita la possibilitat de descarregar arxius que puguen haver sigut prèviament manipulats amb finalitats malicioses.
- En cas d'instal·lar complements extres com a barres de tasques, extensions, protectors de pantalla, comprova prèviament la seua autenticitat.
- Realitza ajustos en la configuració del navegador web per a poder minimitzar el risc d'atacs maliciosos.

- Instal·la un programa antivirus que tinga la capacitat de detectar pàgines web malicioses mentre es navega per Internet i que explora els arxius descarregats; cada vegada són més els antivirus que inclouen aquestes característiques.
- Utilitza un tallafocs (firewall) que bloquege comunicacions entrants i sortints; d'aquesta manera s'evitarà la possibilitat que alguna aplicació maliciosa intente connectar-se amb l'ordinador i fins i tot extraure dades.
- Intenta, si pot ser, no accedir a serveis bancaris o uns altres que utilitzen dades confidencials en ordinadors públics (com cibers, biblioteques, hotels, etc.) fins i tot en xarxes Wi-Fi obertes sense contrasenya.
- En cas de navegar per Internet utilitzant ordinadors públics, et recomanem eliminar els arxius temporals, caché, cookies, historial, contrasenyes i formularis en els quals hages introduït dades per a evitar que una altra persona usuària tinga accés a la teua informació privada.

Xarxes socials

Les xarxes socials actualment són molt populars i massivament utilitzades. Les persones atacants intenten aprofitar-se d'aquelles persones usuàries que són més desprevingudes i utilitzen les xarxes socials amb finalitats malicioses. És per açò que és necessari prendre mesures per a utilitzar-les de la manera més segura possible.

Algunes **recomanacions** són les següents:

- Tracta de no publicar informació privada, ja que persones desconegudes poden aprofitar aquesta informació.
- Cuida, i fins i tot evita, la publicació d'imatges pròpies i dels teus familiars. Les imatges es poden utilitzar fins i tot per a complementar actes delictius de qualsevol àmbit.

- Configura els ajustos de privadesa del perfil d'usuari ; pots configurar-los perquè siga privat i només puguen veure-ho persones a els qui li'l permetes.
- Assegura't de la veracitat de les persones que envien sol·licituds abans d'acceptar-les.
- Canvia les contrasenyes de manera periòdica.

Realitza copies de seguretat regularment

Les còpies de seguretat (o backups) es realitzen per a tenir emmagatzemades còpies d'arxius i fins i tot de l'estat d'un ordinador perquè, en cas de pèrdua d'informació (ja siga per una catàstrofe informàtica o per alguna causa accidental), pugues restablir o restaurar l'estat previ del teu ordinador.

Actualitza el sistema operatiu i les aplicacions

És recomanable que actualitzes el sistema operatiu i les aplicacions instal·lades en el teu ordinador. .

Els sistemes operatius i les aplicacions presenten fallades i errors que poden aprofitar algunes persones amb finalitats malicioses.

Les actualitzacions, a més d'agregar alguna nova funcionalitat, serveixen per a solucionar fallades i agregar noves funcionalitats. Per açò estar al dia amb les actualitzacions de seguretat més importants ajudarà a prevenir atacs maliciosos.

És important que descarregues actualitzacions de llocs que siguen de confiança. Descarregar actualitzacions d'aquells dels quals es dubte la seua reputació o llocs no oficials augmenta el risc d'infecció.

Siempre que sea posible, te recomendamos descargar las actualizaciones a través de los mecanismos que Configura de manera òptima el sistema operatiu

Configura de manera òptima el sistema operatiu

És important que realitzes ajustos el sistema operatiu per a fer-ho més segur.

Alguns **consells** que t'oferim són:

- Deshabilita les carpetes compartides si no les utilitzes. Açò evita la propagació de programes maliciosos que les aprofiten per a infectar l'ordinador.
- Utilitza contrasenyes segures i fàcils de recordar tant en aplicacions com a nivell d'accés a l'ordinador per a evitar que puguen accedir persones no desitjades.

- Crea perfils d'usuari amb privilegis restringits, de manera que es limiten les accions d'algunes persones que puguen provocar un augment de possibilitats d'infecció.
- Deshabilita l'execució automàtica de dispositius d'emmagatzematge extraïbles (com USB), ja que poden contenir aplicacions malicioses que s'executen en segon pla, invisibles a la persona usuària.
- Tingues en compte que el suport tècnic en versions antigues de sistemes operatius i aplicacions rep menys atenció que en el de les últimes versions, per la qual cosa per norma general les versions més antigues estan més exposades a vulnerabilitats.
- Normalment els arxius maliciosos s'amaguen en el sistema com a fitxers ocults, per la qual cosa moltes vegades es troben configurant el sistema perquè es permeten veure els arxius ocults.
- És possible configurar la visualització de les extensions d'arxius perquè pugues identificar les extensions d'arxius que s'hagen descarregat i evitar ser víctima de tècniques com la doble extensió.

Navegació segura, d'incògnit/privada i anònima

Navegació Segura

El protocol **HTTPS** (Hypertext Transfer Protocol Secure, o protocol HTTP segur) garanteix que les sessions de navegació estan xifrades, per la qual cosa la transferència de dades és segura.

Veuràs que et trobes en una sessió de navegació segura quan, en la barra de navegació, et trobes les sigles **https**.

És fonamental que et trobes dins d'una sessió segura quan introduïsques o maneges dades sensibles, com a dades bancàries, acadèmics o de compres.

Si estàs en una pàgina de comerç electrònic i, a l'hora d'efectuar el pagament o introduir els codis de la targeta de crèdit la connexió no és segura, mai has d'introduir les dades.

Navegació privada

Amb la navegació privada, el navegador no deixa en l'ordinador cap rastre de les pàgines que visita (cookies, caché i historial).

No obstant açò, cal tenir en compte que aquest tipus de navegació no oculta la IP (adreça d'internet de l'ordinador) ni proporciona navegació anònima real.

Para quin pugues ser-nos útil la navegació privada?

- Per a obrir sessions paral·leles d'una mateixa aplicació des d'un mateix ordinador: per exemple, podem tenir diversos comptes de GMail obertes, en lloc d'haver de tancar una sessió i obrir una altra, o obrir sessió en un altre navegador
- Per a mantenir la privadesa de cada persona usuària en ordinadors compartits i, evitar, per exemple, que dades personals o privats queden exposats distretament (formularis, claus..)
- Per a visitar pàgines sospitoses o que generen poca confiança: així s'evita que es puga instal·lar 'malware' (aplicacions nocives) per mitjà de cookies

Què fa i què no fa la navegació privada

Si ben cada navegador realitza aquesta funció a la seua manera, en termes generals, la navegació privada implica que el navegador:

- Elimina les cookies després de tancar la sessió
- No es guarda cap tipus d'historial o formularis d'acte-completat
- No es guarden les contrasenyes
- S'esborra la caché automàticament en eixir

D'igual manera, cal recordar **el que no fa:**

- No proporciona connexions segures o xifrades
- No oculta la teua adreça IP
- No evita que les pàgines d'Internet emmagatzemen informació sobre tu
- No impedeix que la teua navegació siga supervisada per l'administrador de la xarxa
- No suposa un anonimat total (aplicacions de tercers com a Flaix poden guardar les seues pròpies cookies, etcètera)

Navegació Anònima: TOR, I2P i proxies gratuïts

Encara quan naveguem en manera privada, seguim sent identificables en la xarxa: nostra IP és visible i a partir d'ací es pot obtenir la nostra posició geogràfica aproximada, el nostre proveïdor de servei o fins i tot el nom de l'empresa en què treballem (si disposem d'una IP institucional).

L'única forma d'aconseguir un anonimat quasi complet quan naveguem és usar una connexió segura a una màquina denominada servidor http proxy.

Un servidor http proxy és un ordinador que funciona com una passarel·la a través de la qual es filtren les nostres peticions de navegació per la web.

Així, si volem connectar-nos a una pàgina web, primer farem la petició al servidor proxy, i serà aquesta màquina la que faça la petició de càrrega a la pàgina a la qual vulguem connectar-nos, quedant el nostre ordinador "ocult" a ulls del servidor d'aqueixa pàgina web, doncs la IP que li consta a aqueix servidor web és la del proxy.

Quan usem aquest mecanisme diverses vegades seguides, és quasi impossible rastrejar la IP original del nostre ordinador, amb el que nostra navegació és totalment anònima.

TOR és el sistema de navegació anònima més popular.

Es tracta d'una xarxa gratuïta gràcies a la qual es pot navegar, xatejar o descarregar arxius de forma totalment anònima. Al mateix temps, és un conjunt de programes que possibilita l'accés a aquesta xarxa.

Per a usar TOR, hem de descarregar l'aplicació i instal·lar-la. Existeixen també complements per a Firefox que faciliten la navegació anònima amb TOR, així com versions portables de la pròpia aplicació (Portable TOR), o basades en el navegador Opera (Opera-TOR)

A més de TOR, existeix una xarxa de servidors proxy no xifrats i túnels VPN anònims a través dels quals poder fer la nostra connexió, però la fiabilitat és variable.

I2P i Freenet són xarxes P2P privades, que serveixen a comunitats anònimes a través dels quals s'intercanvien grans volums de dades. La xarxa I2P és una xarxa dins d'internet, de tal forma que les seues comunicacions són invisibles per a la resta d'usuaris d'internet.

Per a acabar

En aquest tema hem après:

- Que la seguretat informàtica al 100% no existeix
- Que el punt crític de la seguretat en els sistemes sol ser el factor humà
- les característiques dels sistemes segurs
- Què són les vulnerabilitats informàtiques i com poden afectar-nos
- L'amenaça que representa l'enginyeria social, i quines tècniques s'utilitzen per a enganyar a les persones usuàries
- El catàleg d'amenaces lògiques als sistemes informàtics i com actuen
- Els riscos potencials d'usar el correu electrònic i navegar per internet, i com protegir-se enfront d'ells
- Les diferències entre navegació segura, privada i anònima