Consell Assessor del Parlament sobre Ciència i Tecnologia

Informe de ciberseguretat i privadesa per al Parlament de Catalunya

Resum executiu

Aquest document respon a una petició del Consell Assessor del Parlament sobre Ciència i Tecnologia (CAPCIT) amb l'objectiu de fer un informe sobre ciberseguretat i privadesa per al Parlament de Catalunya. Aquest informe no pretén donar informació exhaustiva ni rigorosa sota un punt de vista analític dels diferents tipus d'atacs i mecanismes per a protegir-nos, sinó que intenta oferir una visió general que no requereixi una formació específica en l'àmbit de les enginyeries de les TIC.

El document s'estructura en dos grans blocs: el primer corresponent a la ciberseguretat i el segon adreçat a la privadesa. Posteriorment s'afegeix una guia de bones pràctiques i unes conclusions.

Respecte al bloc de ciberseguretat, es fa una classificació dels tipus d'atacs més comuns (enginyeria social, vulnerabilitats a les aplicacions, APT, programari de segrest) indicant les característiques, l'impacte i els mecanismes per a poder mitigar aquests atacs. També s'ha afegit a petició del sol·licitant informació de l'atac Pegasus.

Respecte al bloc de privadesa, en primer lloc s'ha establert una classificació de les dades en funció de la seva sensibilitat i s'ha introduït de forma senzilla les tecnologies que es fan servir per a protegir la privadesa. Posteriorment s'ha indicat quines d'aquestes tecnologies s'han de fer servir en les diferents etapes del cicle de vida de la informació. Finalment s'indica quines són les lleis que permeten regular la privadesa en el nostre entorn.

Introducció

La ciberseguretat consisteix en la protecció de sistemes, xarxes i dades digitals contra atacs informàtics. Es tracta d'una disciplina crítica i indispensable que protegeix les nostres dades, la nostra privadesa i la nostra societat en conjunt. Els atacs a la ciberseguretat poden ser realitzats per una àmplia gamma d'actors, inclosos *hackers* ètics, ciberdelinqüents, grups de *hackers* estatals i altres. Així doncs, la ciberseguretat esdevé una necessitat vital per a empreses, governs i individus.

La societat actual depèn cada vegada més de les TIC i això obliga a posar més focus en la resiliència. Mentre que la ciberseguretat tradicional es focalitza en protegir la informació, la ciberresiliència, entesa com l'habilitat per a preparar-se, respondre i recuperar-se d'un ciberatac, serà bàsica per a limitar l'impacte dels ciberatacs i garantir la continuïtat dels serveis essencials.

La ciberseguretat és una responsabilitat compartida: tant els individus com les organitzacions han de prendre mesures per a protegir-se dels atacs informàtics. La despesa mundial en ciberseguretat durant el 2022 ha estat superior a 260.000 milions d'euros i s'espera que tingui un creixement del 15% anual fins al 2025. L'augment dels pressupostos en ciberseguretat és conseqüència de la rellevància que aquest àmbit està assolint en el desenvolupament de la societat digital.

Un ciberatac és una acció o sèrie d'accions realitzades per un atacant amb l'objectiu de comprometre o danyar un sistema informàtic, una xarxa, un dispositiu o les dades que s'hi emmagatzemen. Existeixen diversos tipus de classificacions de ciberatacs en funció de l'objectiu, metodologia o el seu impacte. Segons l'objectiu aquests atacs poden tenir diverses finalitats, com l'accés no autoritzat, el robatori d'informació, el sabotatge o destrucció de dades, la denegació de servei, entre d'altres. Malauradament, cap sistema és immune als atacs. Qualsevol entitat que gestioni, transmeti, emmagatzemi o manipuli dades d'alguna altra manera ha d'instituir i fer complir mecanismes per a monitorar el seu entorn informàtic, identificar vulnerabilitats i tancar els forats de seguretat tan aviat com sigui possible. Però no només les institucions han de prendre mesures per a vetllar per la ciberseguretat; a nivell individual també es poden fer una sèrie d'accions per a protegir les dades i dispositius, com poden ser utilitzar contrasenyes fortes i úniques, mantenir el programari actualitzat, evitar fer clic en enllaços o obrir fitxers de fonts desconegudes, utilitzar un programa antivirus de confiança i ser conscient dels riscos de la ciberseguretat.

Una disciplina complementària a la ciberseguretat i íntimament lligada és la privadesa. La privadesa és el dret d'una persona a controlar la informació sobre ella mateixa. Aquest dret inclou el dret a decidir qui té accés a la informació personal, com s'utilitza i si s'ha de compartir. La privadesa és un dret fonamental que protegeix la llibertat, la seguretat i la dignitat de les persones en un món cada vegada més digital i connectat. Mantenir l'equilibri entre la utilització de dades per a fins legítims i la protecció de la privadesa és un repte important per a la societat actual.

La privadesa és important per una sèrie de raons. En primer lloc, permet als individus protegir la seva intimitat. En segon lloc, promou la llibertat d'expressió. En tercer lloc, protegeix els drets humans bàsics, com ara el dret a la llibertat d'opinió i el dret a la protecció contra la discriminació. La privadesa es pot veure amenaçada per la recollida i compartició de dades entre entitats, la venda de dades personals a tercers i els atacs informàtics que poden robar dades personals.

Hi ha una sèrie de lleis i regulacions de privadesa que protegeixen els drets de privadesa de les persones, que estableixen requisits per a les entitats sobre com poden recopilar, utilitzar i compartir dades personals.

Tipus d'atacs més comuns

En l'actualitat la diversitat dels atacs existents és molt diversa, i cada cop, més complexa, ja que, a mesura que els sistemes de protecció van millorant, els atacants es van professionalitzant i dediquen ingents quantitats de temps a formar-se i a aprofitar el mínim error per a poder realitzar els seus actes cibercriminals. Molts d'aquests atacants s'han professionalitzat fins al punt de crear estructures i sistemes de gestió pròpies de règims militars o empresarials.[1] Així doncs, ens trobem davant d'una nova era, on el cibercrim organitzat s'ha de prendre molt seriosament.

Tot i aquest avanç que ha sofert el cibercrim cal remarcar que generalment es poden observar patrons repetibles en els atacs, per la qual cosa a la pràctica de la gran diversitat existent s'acaben trobant atacs relativament similars.

Així, encara avui dia els tipus d'atacs més usats estan basats en enginyeria social i en errades de seguretat a les aplicacions utilitzades. Per això aquest capítol se centra en la descripció dels atacs per enginyeria social, per continuar amb una detallada explicació dels atacs causats per vulnerabilitats del programari, passant després la discussió sobre dues derivades d'aquests atacs més bàsics, els atacs amb programari de segrest i Pegasus, que no deixen de ser una combinació dels anteriors.

Enginyeria social

Tot i que en una primera instància es podria pensar que l'enginyeria social no és un atac, en realitat els efectes que pot aconseguir fa que s'hagi de replantejar aquesta premissa. Amb enginyeria social s'aconsegueix violar un dels primers pilars de la ciberseguretat, la privacitat, i això s'aconsegueix a través d'un dels punts més importants quan es parla d'entorns cibersegurs, la recollida d'informació de la víctima.

Què és doncs l'enginyeria social? És l'atac pel qual s'enganya la víctima a través de trucs psicològics per, a través d'una falsa sensació d'urgència, revelar informació sensible o forçar la víctima a compensar econòmicament l'atacant.

1. https://www.kelacyber.com/wp-content/uploads/2022/03/KELA-Intelligence-Report-ContiLeaks-1.pdf

L'enginyeria social és considerada un dels vectors d'atac més comuns actualment; tant és així que l'enginyeria social es considera l'atac més utilitzat durant el 2022, especialment amb una de les formes més comunes, el *phishing*, que s'estima que causa el 33% del total d'atacs realitzats. Cal esmentar que l'enginyeria social rarament és el fi d'un atac, més aviat n'és el mitjà, per a posteriorment poder obtenir un rèdit d'aquesta informació obtinguda.

En general un atacant buscarà informació personal d'algú per tal de:

— **Impersonar** la víctima per tal de lucrar-se'n econòmicament o bé per a poder utilitzar-la com a palanca per a aconseguir més informació d'algú altre.

— Aconseguir que la víctima realitzi alguna **acció**, com ara una transferència bancària o atorgar permís per a permetre que l'atacant pugui realitzar alguna operació, generalment econòmica.

Característiques i impacte

Hi ha molts tipus i variants d'enginyeria social depenent del mecanisme utilitzat per a guanyar-se la confiança de la víctima i així aconseguir realitzar l'atac. Els mecanismes més típics són:

— ***Phishing***: on l'atacant envia un missatge fent-se passar per algun conegut. El conegut pot ser algú de la nostra agenda de contactes, però també pot ser algun proveïdor de serveis. En aquesta categoria són coneguts[2] els missatges fent-se passar per una entitat bancària, alguna empresa de lliurament de mercaderies o una oficina de correus.

  Hi ha diversos tipus de *phishing* i cada cop són més evolucionats. El més perillós és *Spear Phishing*, on l'atacant prèviament fa una anàlisi exhaustiva de la víctima o la seva organització, i crea llavors un missatge personalitzat, inclús suplantant algú conegut de la víctima, que és molt més creïble que un correu genèric d'alguna entitat externa. Tenim exemples coneguts d'aquest tipus d'atacs com el que va sofrir l'Ajuntament de Barcelona, on, a través de la impersonació d'un proveïdor, es va aconseguir canviar el número de compte dels seus pagaments per un controlat per un atacant, aconseguint desviar aproximadament uns 350.000 euros.

— ***Whaling***: és una variant del *phishing* molt comuna on l'objectiu són els directius d'empreses o caps polítics. En aquest cas l'atacant, a través del correu electrònic, es fa passar per un altre executiu o polític d'alt rang d'una altra entitat. El missatge generalment conté alguna emergència falsa o una gran oportunitat que durarà poc temps i que requereix una acció ràpida de la víctima. Generalment l'objectiu és aconseguir informació sensible.

— ***Honey trap***: aquesta variant típicament utilitza xarxes socials conegudes, com ara Instagram, WhatsApp o Telegram. L'objectiu és enviar un missatge impersonant algú que vol mantenir una relació sentimental, i, un cop guanyada la confiança, demanar algun tipus d'ajut immediat a través d'un problema inventat, demanant urgència per tal de no donar temps a pensar en la veracitat del missatge.

— ***Baiting***: l'objectiu en aquest cas és obtenir informació sensible de la víctima, per això es busca que la víctima ompli algun qüestionari o document amb aquesta informació o la redirigeix a una pàgina de *login* de Google o Microsoft falses per a robar-li les credencials.

— ***Pretexting***: l'atacant crea un escenari fictici, per exemple pretenent ser del servei tècnic d'alguna empresa i dient que per a poder arreglar un problema, també fictici, en què la víctima ha de proporcionar dades personals, com ara targetes de crèdit o contrasenyes, per tal de poder continuar utilitzant un servei.

L'impacte que tenen aquest tipus d'atacs és difícilment quantificable, principalment perquè moltes de les víctimes, o bé per vergonya o bé per falta d'informació, no denuncien l'acte. Tot i així, com es pot observar a l'informe de l'*Internet Crime Complaint Center* (IC3), es calcula que durant el 2022 es van realitzar més de 300.000 atacs.

A banda d'això i com a punt crític dels atacs per enginyeria social, cal esmentar que és un dels *vectors d'atac* més habituals per grups de ciberdelinqüents organitzats per tal d'aconseguir un accés inicial dins d'un sistema. Un cop dins mira d'expandir-se a tota la xarxa abans de realitzar un atac coordinat contra la víctima. Un exemple d'això el tenim en l'atac que va sofrir la Universitat Autònoma de Barcelona, on els atacants inicialment van utilitzar *phishing* per a aconseguir les credencials d'un empleat per a posteriorment realitzar un atac amb programari de segrest.

Com mitigar els atacs per enginyeria social

Hi ha diverses formes de poder mitigar, o almenys minimitzar, l'impacte d'aquest tipus d'atacs, però això sempre implica dos pilars fonamentals: per una banda, és necessari disposar de les eines tecnològiques

2. Campañas de suplantación de entidades bancarias con falsos cargos y bloqueo de cuentas

necessàries, generalment aplicatius de monitoratge de la seguretat dels nostres sistemes, però també, i igualment important, conscienciant els empleats i els usuaris dels nostres sistemes de com actuar i com detectar aquest tipus de frau. Aquesta conscienciació generalment passa per proporcionar als empleats cursos de ciberseguretat amb casos pràctics per a poder observar de primera mà el funcionament d'aquest tipus d'atacs.

Aquesta conscienciació generalment passa per la verificació d'una llista de punts a considerar abans de publicar qualsevol tipus d'informació a la xarxa. Els més importants són:

— **Determinar** si el correu rebut és de l'interlocutor que diu ser. Per això es recomana observar amb detall el domini des del qual s'ha enviat el correu. Això és, des de la «@» del correu fins al final: allà s'ha de veure exactament el domini esperat, sense cap error ni lletra diferent al que hauria de ser (no és el mateix user@microsoft.com que user@micosoft.com).

— **Sospitar** de qualsevol interlocució, especialment si no es coneix l'emissor del missatge.

— **Evitar** descarregar adjunts dels correus quan vinguin de fonts desconegudes i continguin aplicacions. Per a saber si un adjunt és una aplicació, cal veure el tipus de fitxer. Les aplicacions són: fitxers EXE, MSI i inclús VBA.

— **Assegurar-se** de la correcció dels enllaços dels correus. Això s'ha d'observar passant el ratolí per sobre de l'enllaç i veure quin és el domini al qual portarà l'enllaç: s'ha d'inspeccionar que el domini apunti cap allà on toca. Per a fer-ho cal observar tot el contingut de la URL, especialment des de «https://» fins a la primera «/» del nom; així, el domini de la URL https://www.gencat.cat.in/noticies/2023-07-22/ no apunta a la web de la Generalitat. Per això es recomana que, en comptes de clicar als enllaços, s'accedeixi a la pàgina web teclejant directament al navegador la pàgina que es vol visitar.

— **Verificar** la identitat de l'interlocutor a través de mètodes alternatius, com ara amb una trucada telefònica o validant la llibreta de direccions.

Per tal de poder fer-se una idea de la conscienciació dels empleats o usuaris de les TIC convé de tant en tant fer campanyes d'atacs de *phishing* controlats per a permetre que els empleats aprenguin a detectar-los i a actuar en conseqüència, sobretot creant un clima en què es pugui reportar lliurement si algun atac d'aquestes característiques s'ha produït, sense represàlies per a la possible víctima, que pot amagar el fet per vergonya o per por a conseqüències disciplinàries.

Atacs causats per vulnerabilitats a les aplicacions

Amb la gran quantitat de dispositius que actualment estan connectats a Internet, amb la gran quantitat de programari que tenen, i l'enorme quantitat d'usuaris, és normal que aquest programari pugui contenir errades. Aquestes errades poden ser funcionals, on l'aplicació no actua com s'espera, però d'altres poden ser senzillament errors de programació o configuració que no són perceptibles pels usuaris, però que poden ser aprofitats per un atacant maliciós per a forçar que l'aplicació es comporti de forma no esperada, i causar, així, potencial exfiltració d'informació o permetre a l'atacant prendre control dels recursos afectats.

Aquest segon grup d'errades es coneixen com a vulnerabilitats i són una enorme font d'atacs, especialment amb aplicacions no actualitzades o aplicacions no validades que poden contenir molts d'aquests errors.

Característiques

Si bé els atacs per enginyeria social impliquen una acció per part d'un o més usuaris, les vulnerabilitats d'aplicacions, al contrari, es manifesten a través de fallades d'una aplicació que permeten a l'atacant realitzar accions malicioses a l'equip de la víctima, sigui un mòbil, un ordinador d'escriptori o el servidor hostatjat en un centre de dades. Això implica que molts cops aquests tipus d'atacs no requereixen cap acció per part de la víctima. Només cal un atacant amb suficients coneixements tècnics i un equip vulnerable connectat a la xarxa.

Procedència dels atacs

Generalment aquests atacs venen a través de dues vies: a través d'atacs automàtics o bé a través d'atacs dirigits.

Atacs automàtics

Un atac automàtic fa referència a aquells atacs en què l'atacant, en comptes de buscar activament una víctima per a atacar-la, posa un sistema automàtic que busca errors coneguts al programari de totes les màquines connectades a Internet. Aquest atac sistemàtic mira d'identificar aquestes vulnerabilitats i un cop trobades avisa l'atacant indicant la llista d'equips vulnerables que s'han trobat. Un cop fet això, l'atacant aprofita aquesta vulnerabilitat per a prendre control de l'equip que té el programari vulnerable.

Com es pot observar, aquest tipus d'atacs no van dirigits a algú en particular, sinó que van dirigits a usuaris amb aplicacions vulnerables independentment de qui són i què fan.

Atacs dirigits

Un altre tipus molt important d'atacs que aprofiten errors del programari és quan un atacant es fixa en una víctima i, un cop decidit a atacar-la, es fa una anàlisi personalitzada on s'estudien tots els seus recursos públics. Un cop identificats tots, es veu el que es coneix com a «superfície d'atac», que fa referència al conjunt de recursos atacables d'un individu o empresa. Un cop identificada aquesta superfície d'atac, es fa un estudi de quin sistema es fa servir i es prova de forma personalitzada d'atacar cada un d'aquests recursos. En aquest punt es posa a prova la seguretat i la configuració de tota la infraestructura que la víctima té en el sistema.

Objectius aprofitant vulnerabilitats a les aplicacions

Si bé hi ha moltes possibles classificacions de formes d'aprofitar-se de vulnerabilitats, una de les més rellevants és la que considera la víctima de l'atac, que principalment pot ser-ne un usuari final, o bé el propi servei ofert per una empresa.

Atacs contra els usuaris

Generalment aquest tipus d'atacs es beneficien d'accions incorrectes realitzades per usuaris aprofitant problemes a l'aplicació que fan servir. En aquesta categoria es poden trobar, per exemple, problemes al navegador o bé problemes a aplicacions empresarials, com ara Microsoft Office o d'altres.

Aquí l'objectiu és fer que l'usuari realitzi alguna acció que fa que l'aplicació en qüestió es comporti de forma incorrecta.

Un exemple clàssic és quan la víctima obre un adjunt que ha rebut d'un correu electrònic. Aquest adjunt conté un document Word amb un contingut forjat per un atacant que fa que l'aplicació es comporti de forma inadequada, per exemple, obrint una connexió cap a l'exterior que permet a l'atacant prendre el control de la màquina de la víctima. Això es coneix com a atac del tipus *backdoor*.

Un altre cas clàssic és quan un atacant maliciós aconsegueix que la víctima obri un enllaç amb el navegador, que està forjat de manera que permet robar les galetes del navegador, la qual cosa, a la pràctica, vol dir que l'atacant tindrà accés a tots els recursos en línia a què la víctima accedeix des d'aquell navegador.

Com es pot observar, aquest tipus d'atacs, al contrari del que s'ha presentat als atacs automàtics, requereix accions concretes per part dels usuaris.

Per fer-nos una idea, des de la creació del navegador Google Chrome el 2009, se li han trobat un total de **3.243 vulnerabilitats**,[3] de les quals, en els primers vuit mesos del 2023, n'hi ha hagut un total de **31**. Això no vol dir que aquest navegador estigui mal implementat, el que vol dir és que és un dels més usats i, per tant, hi ha molt interès a trobar-li errades que permetin als atacants tenir èxit en els seus atacs.

Atacs contra els serveis

En el cas d'atacs realitzats contra serveis, l'objectiu generalment és aconseguir les dades que hi ha al darrere del servei en particular, però la gran diferència amb els atacs contra usuaris és que en aquest cas la víctima no ha de realitzar cap acció. El que procura l'atacant en aquests casos és enviar dades invàlides al servei o analitzar-ne el funcionament buscant alguna mala configuració que li permeti accedir al sistema.

L'enviament de dades invàlides acostuma a provocar un mal funcionament de l'aplicació que en segons quins casos pot proporcionar accés total a l'atacant. Aquest tipus de vulnerabilitats tenen el mateix impacte que les dels atacs contra usuaris, en el sentit que són errors de programació que es podrien arreglar. De nou, com més coneguda i usada és una aplicació, més errades s'hi troben i més impacte potencial tenen contra els nostres sistemes.

Tenim exemples d'aquest tipus d'atacs amb gestors de contingut (coneguts com a *Content Management Systems - CMS*), que són aplicacions que permeten la introducció de forma molt senzilla a pàgines web per a gestionar-ne el contingut per usuaris no experts. Aquests sistemes sempre han estat el focus d'atacs, ja que estan presents a gairebé tot arreu; un dels més famosos és WordPress, del qual, des de la seva creació el 2003, s'han reportat un total de **6.830 vulnerabilitats diferents**, algunes de les quals han tingut impacte mediàtic, com ara el cas dels Papers de Panamà,[4] que el 2016 va dur al que es coneix com la filtració periodística més gran de la història.

Tot i així, cal esmentar que, igual que amb els atacs contra aplicacions d'usuaris, les empreses al darrere d'aquestes aplicacions, generalment, tenen equips de desenvolupadors grans, dedicats exclusivament a arreglar aquestes errades en el mínim temps possible.

Pel que fa a les errades a la configuració del sistema, típicament es troben sistemes amb contrasenyes per defecte o molt fàcils d'endevinar, pàgines d'administració accessibles per tothom o bé serveis innecessaris amb accés obert per a possibles atacants.

3. https://www.opencve.io/cve?product=chrome&vendor=google
4. https://www.xataka.com/seguridad/un-plugin-de-wordpress-y-un-drupal-antiguo-causantes-de-la-filtracion-de-los-papeles-de-panama

Tipus de vulnerabilitats per antiguitat

La darrera classificació que es mostrarà en aquest document és la classificació de les vulnerabilitats segons l'antiguitat. Això és especialment important, ja que, a la pràctica, per a poder arreglar un problema, se n'ha de conèixer l'existència. Per això, en distingim dos tipus: les vulnerabilitats conegudes – o «antigues»– i els atacs de dia zero (*0-day*), que són les vulnerabilitats que encara no estan reportades i que, per tant, encara no són conegudes pels desenvolupadors.

Vulnerabilitats conegudes

Hi ha equips d'empreses grans i conegudes, i altres experts *freelance*, que dediquen el seu temps a buscar vulnerabilitats. Quan se'n troba una, aquesta és reportada als desenvolupadors i se'ls dona un temps abans de fer-la pública. Aquest procediment serveix, per una banda, per a obligar els desenvolupadors a arreglar els problemes i, per l'altra, donar-los prou temps perquè ningú que no conegui la vulnerabilitat pugui aprofitar-se'n mentre s'arregla. En qualsevol cas, arreglar la vulnerabilitat no és suficient; falta que els administradors de les aplicacions les actualitzin a la versió segura al més aviat possible.

La base de dades de vulnerabilitats conegudes s'anomena Common Vulnerabilities and Exposures (CVE)[5] i és una llista realitzada per Mitre i finançada pel govern dels Estats Units. Actualment té un total de **211.265** entrades de totes les aplicacions existents des de la creació de la base de dades, al setembre del 1999.

0-day

Si les vulnerabilitats conegudes i registrades poden durnos molts problemes, amb els atacs de dia zero (*0-day*) el problema és encara molt més gran, ja que, com ja s'ha dit, els atacs de dia zero són vulnerabilitats recentment descobertes, o bé per experts reconeguts o bé per atacants maliciosos.

Quan qui descobreix la vulnerabilitat és un atacant maliciós, aquest pot aprofitar l'error trobat durant molt més temps, ja que la víctima i els desenvolupadors de les aplicacions no en són coneixedors. Així doncs, són un tipus de vulnerabilitats extremadament delicades. Durant la història hi ha hagut atacs de dia zero famosos, però el més conegut recentment, com es veurà més endavant en aquest document, és l'aplicació Pegasus, que s'aprofita d'errades al sistema de missatgeria de IOS a l'iPhone per a descarregar l'aplicació de forma totalment transparent a l'usuari del dispositiu mòbil.

Impacte

Juntament amb els atacs per enginyeria social, els atacs que aprofiten vulnerabilitats de programari són els més habituals actualment. Hi ha nombrosos estudis que miren de quantificar l'impacte d'aquest tipus d'atacs, però tots coincideixen que l'impacte econòmic i de prestigi vers la víctima d'aquests atacs és enorme.

El 2023,[6] segons IBM, el cost mitjà als Estats Units d'un atac es quantifica en **4,45 milions** de dòlars, la qual cosa suposa un increment del 2,3% respecte al 2022.

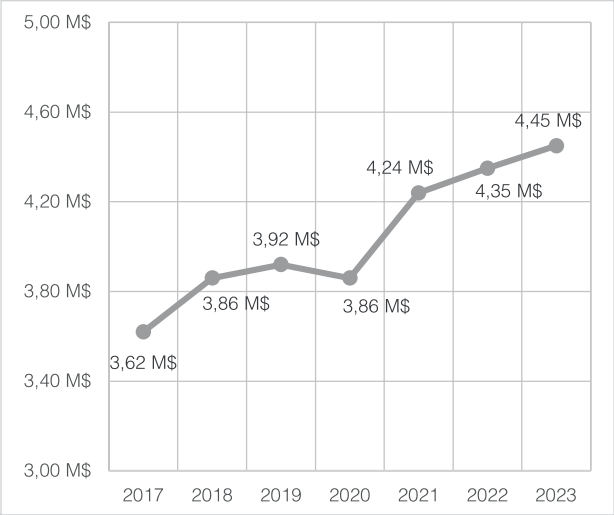

Figura 1: Evolució del cost (milions de dòlars)

D'altra banda, el mateix informe fa palès que de mitjana les empreses triguen **182 dies** a ser conscients que s'ha realitzat un atac de forma exitosa, i gairebé **60** a solucionar el problema. Això posa de manifest la gran necessitat de tenir un bon equip de ciberseguretat a l'empresa, així com coneixement de les eines necessàries per a poder mitigar aquest tipus d'atacs i solucionar-los.

Un punt important que cal tenir en compte és que aquest impacte econòmic considera, entre altres coses, l'impacte en la reputació de l'empresa, que, generalment es veu molt afectada amb la pèrdua de clients i amb la publicitat negativa que suposa; però també considera el cost que suposa el filtratge o la destrucció d'informació que pot realitzar l'atacant. Més endavant es veuran els atacs amb programari de segrest, que en molts casos es beneficien de vulnerabilitats a les aplicacions per tal de guanyar accés a la informació de la víctima.

Com mitigar els atacs per vulnerabilitats del programari

Cal esmentar que la mitigació d'aquest tipus d'atacs pot impactar a diversos nivells. Bàsicament es poden veu-

5. https://cve.mitre.org/cve/
6. Cost of data Breach Report 2023

re des de dos punts de vista, el del desenvolupador de l'aplicació o el de l'usuari (bé sigui un administrador de sistemes o bé un usuari final).

Com a desenvolupador

Detallar les diverses bones pràctiques de desenvolupament surt fora de l'objectiu d'aquest document, però és important, quan s'utilitza una aplicació, que l'usuari tingui en compte l'històric de l'empresa que la proporciona. Així, s'han de mirar coses com ara si l'empresa va millorant l'eina i treu noves versions de forma regular, i també quantes vulnerabilitats crítiques s'han trobat a l'eina i el temps que es triga a resoldre-les.

Com a usuari final

Estrictament com a usuari final, tant si és un administrador d'un servei com si és un usuari final sense coneixements tècnics, la lògica és força similar. Com es pot veure en informes sobre estadístiques de vulnerabilitats,[7] la immensa majoria d'atacs (75%) es realitzen amb vulnerabilitats reportades des de fa més de 6 anys, i en gairebé tots els casos la solució seria tan senzilla com actualitzar l'aplicació a una versió estable. Això porta a la gran bona pràctica en aquest aspecte: un bon usuari hauria de monitorar l'estat de les eines que utilitza i actualitzar-les quan sigui necessari. Com que això no és senzill *a priori*, la millor forma de fer-ho és a través d'eines que proporciona el mateix sistema operatiu, generalment en la forma d'avís per a actualitzar, o bé el sistema o alguna eina que es té instal·lada, i, en la mesura que sigui possible, tenir el sistema al dia.

Amenaces persistents avançades

Abans de continuar amb altres atacs, es vol dedicar aquesta secció a veure com el crim organitzat està, cada cop més, perpetrant cibercrims que cada cop impacten més en la vida de les persones. En particular aquesta secció es dedica a discutir sobre les amenaces persistents avançades (*Advanced Persistent Threats*, APT).

Què són les APT?

Les APT són grups organitzats de cibercriminals, sovint autònoms amb estructures empresarials complexes, molts cops finançats per governs i amb objectius molt diversos, però generalment amb motivacions econòmiques o polítiques per tal de portar la guerra a nivell cibernètic.

Les accions que generalment realitzen aquests grups són, en general, robar, espiar o senzillament pertorbar un servei, equip o empresa.

Generalment, en aquests atacs realitzats per aquests tipus de grups, la víctima és curosament seleccionada, estudiada, i només quan es té suficient informació es passa a l'ofensiva. És important remarcar que un atac realitzat per una APT no és un atac ràpid. Aquest tipus d'amenaces poden durar dies, setmanes o inclús mesos, en què l'atacant primer estudia la víctima. Un cop trobades possibles vulnerabilitats, es traça un pla d'atac del tipus *Land and Expand,* on primer es mira de prendre control de forma sigil·losa d'una part de la infraestructura, per a, a poc a poc, anar expandint-se, fins que es considera que s'ha pogut prendre control de tots els recursos de la víctima i es fa un atac coordinat. En aquest punt, depenent de l'objectiu de l'atac, poden passar diverses coses, però normalment, i com es veurà posteriorment en els atacs amb programari de segrest, s'inhabiliten els serveis que ofereix la víctima i es xifren totes les dades i, si es pot, les còpies de seguretat. Un cop arribats en aquest punt, s'informa la víctima de l'atac i dels passos que ha de realitzar per tal de recuperar la informació. Normalment, la recuperació passa pel pagament mitjançant bitcoins o altres criptomonedes per a evitar ser trobats per les autoritats competents.

S'ha de remarcar que generalment aquests tipus de grups de ciberterroristes organitzats, un cop pagat el rescat, i per un tema purament de màrqueting, no tornen a atacar la víctima i, en segons quins casos, inclús li donen idees sobre com millorar la seguretat del seu sistema.[8] L'objectiu és, principalment, que les futures víctimes no tinguin dubtes a l'hora de pagar el rescat, donada la serietat de l'atacant. Aquest punt de prestigi ha estat un dels grans canvis des que existeixen aquest tipus de cibercriminals organitzats.

Amb aquests grups de cibercrim organitzat, el que es veu és que segons quins governs els observen com una forma més d'atac contra els seus enemics, i els utilitzen quan cal per a fins polítics i per a fer trontollar l'estabilitat dels països atacats.

Grups d'APT

Els grups d'APT són constantment monitorats per empreses i autoritats. Se n'han identificat més de 250, entre els quals, en un moment donat, pot haver-n'hi uns 50 d'actius. Per tal d'identificar-los, normalment se'ls assigna un nom amb la forma **APT[Número]**, on, per exemple, APT1 correspon a *PLA Unit 61398*,[9] un grup

7. https://www.getastra.com/blog/security-audit/cyber-security-vulnerability-statistics/
8. Ransomhouse group
9. https://en.wikipedia.org/wiki/PLA_Unit_61398

cibercriminal xinès. A banda, cada grup es coneix a si mateix amb algun tipus de pseudònim, per exemple Double Dragon[10] (també conegut com APT41), Winnti Group, Barium o Axiom.

Aquesta diversitat de noms ve donada per l'evolució d'aquests grups, que van canviant d'integrants o de *modus operandi* i es van batejant a si mateixos utilitzant diferents noms, de vegades per màrqueting, de vegades per a despistar les autoritats.

Quant a països, Xina és el lloc on hi ha més grups d'APT, seguit de Rússia i els països de l'est, tot i que també n'hi ha als Estats Units. Un punt important és que, donat el bon finançament d'aquests grups, avui dia molts d'ells tenen integrants arreu del món, on els contracten a través del web fosc i els paguen amb criptomonedes per a evitar-ne el seguiment.

Programari de segrest (*ransomware*)

Els atacs amb programari de segrest són, sens dubte, un dels tipus d'atac més mediàtic a causa del gran increment d'atacs a empreses[11] i institucions públiques[12, 13] que els han sofert.

Però en realitat l'atac amb programari de segrest és només la darrera etapa d'un atac que prèviament hi ha hagut per a guanyar accés a un sistema. Això generalment es realitza a través d'enginyeria social o bé a través de vulnerabilitats a les aplicacions existents a l'entitat atacada.

Aleshores, el programari de segrest és un atac pel qual, un cop l'atacant ha guanyat accés a un sistema, xifra totes les dades importants de la víctima utilitzant una clau criptogràfica molt robusta i reclama un rescat per les dades. En segons quins casos, per a forçar el pagament del rescat, s'amenaça amb filtrar i publicar les dades en el web fosc o a través d'altres mètodes, com ara Telegram, tot amb l'objectiu de treure'n rèdit econòmic o polític.

Cal indicar que tant l'enginyeria social com les vulnerabilitats a les aplicacions vistes anteriorment en molts casos són tipus d'atacs perpetrats per atacants que normalment no tenen cap interès particular en el lloc o la persona atacats; en molts casos ni tan sols saben de qui es tracta i troben la víctima utilitzant mecanismes automàtics. En el cas del programari de segrest, en general, l'atac té un caire diferent: generalment es realitza amb un objectiu molt clar, on la víctima ha estat elegida a consciència per una APT.

Característiques i impacte

La gran majoria d'atacs que acaben amb programari de segrest acostumen a utilitzar un vector d'atac força similar. En general, primer s'investiga la víctima, tant des del punt de vista tècnic, mirant els recursos digitals accessibles des de l'exterior, especialment aquells que tinguin potencials vulnerabilitats, com des del punt de vista social, investigant i intentant, a través d'enginyeria social, obtenir credencials que permetin a l'atacant iniciar el control de la infraestructura de la víctima.

Un cop s'ha arribat a controlar un recurs de l'empresa, el següent pas generalment es basa a mirar d'expandir aquest control a altres recursos. Això normalment es realitza a través de sistemes d'elevació de privilegis, o sigui, l'atacant es transforma en administrador i, quan sigui possible, de tot el domini, i així anar expandint el control. Un cop es té control sobre gran part dels sistemes, es realitza un atac coordinat que generalment està format de dues parts: la primera és l'exfiltració de dades cap a un equip extern i la segona és el seu posterior xifratge, si és possible inclús de les còpies de seguretat per a fer més complicada la restauració de la informació.

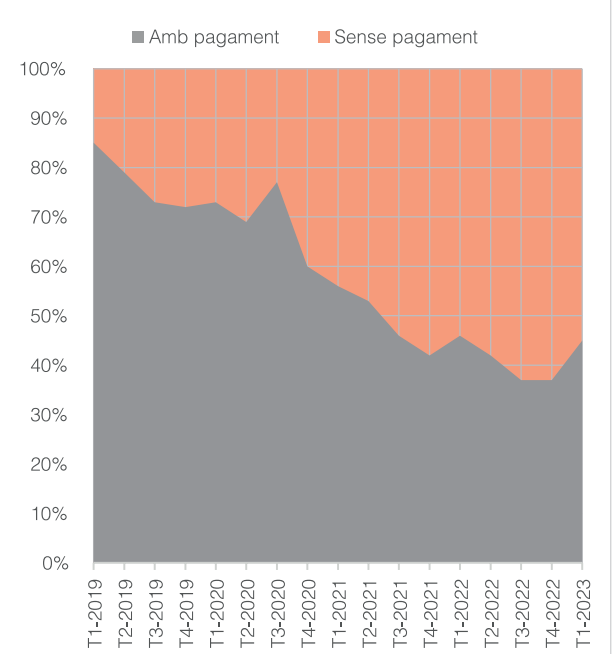

Figura 2: Evolució dels pagaments a cibercriminals per rescat de la informació [Font]

Un cop realitzat el xifratge del sistema, s'avisa la víctima de l'acció i se li dona un enllaç per a fer efectiu un pagament que li donarà accés a les dades novament i li restaurarà el sistema a l'estat original. Normalment aquest missatge conté també l'amenaça per la qual, si

10. https://content.fireeye.com/apt-41/rpt-apt41/
11. Ciberatacs a empreses catalanes
12. Atac informàtic a la UAB
13. https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona

no es paga el rescat, es publicaran les dades. Tot i així, la desconfiança amb l'atacant fa que sovint la víctima no vulgui realitzar el pagament, la qual cosa ha portat els atacants, en molts casos, a canviar el seu model de negoci: ara dosifiquen la informació que es publica sobre la víctima maximitzant així el seu benefici. Això cada cop és més habitual, ja que en els darrers anys, com mostra la Figura 2, s'ha anat decrementant la quantitat de víctimes que paguen el rescat.

Cal notar que un atac per programari de segrest té dues característiques importants, per una banda utilitza altres mecanismes vistos anteriorment per a poder fer l'atac, i per l'altra, generalment està perpetrat per grups de ciberdelinqüents organitzats.

Com mitigar els atacs amb programari de segrest

Aquest tipus d'atacs són dels més complicats d'evitar, principalment perquè al darrere hi ha un equip organitzat amb grans coneixements i moltes eines per a poder identificar i explotar possibles errades o vulnerabilitats del sistema.

Tot i així, es recomana tenir en compte un conjunt de bones pràctiques que poden minimitzar la possibilitat de ser vulnerats:

- Realitzar i validar còpies de seguretat, deixant-ne alguna sempre fora de línia per tal d'evitar-ne el xifratge
- Conscienciar els usuaris en l'ús dels recursos digitals:
  - Tenir una bona política de contrasenyes
  - Ser observadors amb els correus fraudulents
  - Vigilar a qui es dona accés als recursos

Impacte polític dels atacs amb programari de segrest

Inicialment els ciberatacs eren un motiu de prestigi entre els actors maliciosos. Amb l'aparició del programari de segrest es va veure ràpidament el canvi cap a un model de negoci on els atacs podien donar rèdit econòmic ràpidament. Tot i així, donada l'alta especialització i coneixements dels APT, s'està veient un canvi de motivació en els atacs, on molts cops la part econòmica és secundària comparada amb la desestabilització que causa l'atac en si, especialment quan el grup de cibercriminals té finançament de governs o altres tipus d'avantatges, com, per exemple, protecció contra l'extradició, com és ben sabut que fa Rússia.[14]

Aquest canvi de paradigma fa que ara les víctimes dels atacs per programari de segrest es busquin entre universitats, hospitals o altres infraestructures crítiques, amb l'objectiu de desestabilitzar governs o bé ajudar en temes militars, tal com s'observa amb la invasió d'Ucraïna, on es pot veure com la quantitat de ciberatacs després de la primera ofensiva es va multiplicar per 2,5 contra Ucraïna i per 3 contra els països de l'OTAN.[15]

Amb tot, aquest canvi de paradigma hauria de fer reflexionar els governs a invertir en formació cap a la ciutadania per tal de mirar de mitigar al màxim possible l'impacte d'aquest nou model de negoci.

Pegasus

Pegasus, si bé ha tingut un ressò mediàtic molt important des de fa un temps, no és un atac informàtic *per se*, però, com amb la gran majoria d'eines, sempre se'n pot fer un ús incorrecte. Aquest document recull una visió objectiva de què proporciona Pegasus i quines característiques té i fins on pot arribar, sense entrar en judicis de la legitimitat de l'ús que un actor en pugui fer.

Característiques

Pegasus és una eina coneguda com de recollida d'informació (*information gathering*), creada per una empresa israeliana anomenada NSO Group, que es dedica a aconseguir intel·ligència d'un dispositiu. En aquest sentit, Pegasus ha estat dissenyat per uns experts en ciberseguretat i es ven als governs per a poder realitzar espionatge de delinqüents i persones que potencialment poden posar en perill la seguretat nacional. No és un sistema pensat per a ser usat amb dissidents polítics que no tinguin un registre criminal.

Això és així perquè Pegasus s'aprofita de vulnerabilitats en sistemes operatius Android i IOS (iPhone), però també suporta altres sistemes operatius com Blackberry o Symbian (Nokia). Aleshores, l'objectiu final de Pegasus és, de forma personalitzada per a cada un dels sistemes operatius i de les víctimes, estudiar el dispositiu i, de forma totalment transparent per a la víctima, instal·lar-li un agent que permet exfiltrar, sense que la víctima se n'adoni, les dades del seu dispositiu. Així, Pegasus és capaç d'enviar un gran ventall d'informació a l'atacant. Les dades més importants són:

- Ubicació de la víctima: es pot conèixer en tot moment la ubicació
- Totes les dades d'aplicacions: correus electrònics, imatges, missatges de WhatsApp...

14. How the Kremlin provides a safe harbor for ransomware
15. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

— Registre de trucades

— Àudio de les trucades per a poder ser reproduïdes per l'atacant

Si bé les accions que realitza Pegasus són molt útils per a l'atacant, cal dir que el punt que el fa únic és la forma que té d'infectar els dispositius. Pegasus permet ser instal·lat pràcticament en qualsevol dispositiu mòbil de forma transparent i sigil·losa i, tot aprofitant vulnerabilitats de cada un dels dispositius, prendre el control del sistema executant-se com a administrador i, per tant, permetent l'adquisició de totes les dades rellevants del sistema.

Per tal d'evitar al màxim la detecció, Pegasus aprofita sempre que sigui possible el que es coneixen com a vulnerabilitats sense clic (*0-click*), que són aquelles vulnerabilitats que no requereixen cap acció per part de la víctima per a ser infectada. L'exemple més conegut és una vulnerabilitat existent al sistema de missatgeria MMS d'iPhone que permet a Pegasus infectar aquest tipus de dispositius. De fet, vulnerabilitats d'aquest tipus continuen sent trobades i explotades actualment.[16]

El fet que Pegasus pràcticament no deixi rastre als dispositius el fa extremadament difícil de detectar per antivirus o altres sistemes; tant és així que el mateix sistema té un mecanisme per a desinstal·lar-se del dispositiu quan l'atacant ho decideix o quan està a punt de ser detectat.

Com mitigar els atacs tipus Pegasus

Sent realistes, no hi ha una forma fàcil ni clara de mitigar aquest tipus d'atacs tan sofisticats, principalment perquè els qui han creat aquestes eines són experts en vulnerabilitats de programari i tenen al seu abast una enorme quantitat de recursos que els permeten investigar i descobrir molts atacs de dia zero que acaben garantint la infecció de nous dispositius.

L'efecte col·lateral d'això és que altres grups també són potencialment descobridors d'aquests problemes de seguretat i poden estar explotant-los sense el coneixement de les seves víctimes.

En qualsevol cas, per tal de minimitzar l'èxit d'atacs com Pegasus, es recomana mantenir els dispositius mòbils actualitzats i, com sempre, dubtar de tots els missatges rebuts d'orígens desconeguts.

Altres tipus d'atacs

Atacs DoS i DDoS

Un atac de denegació de servei (DoS) està dissenyat per a sobrecarregar els recursos d'un sistema fins al punt que sigui incapaç de respondre a les sol·licituds de servei legítimes. Un atac de denegació de servei distribuït (DDoS) és similar, ja que també busca esgotar els recursos d'un sistema, però en aquest cas és executat per una gran quantitat d'ordinadors infectats amb programari maliciós que estan controlats per l'atacant. Aquests atacs s'anomenen *atacs de denegació de servei* perquè el servidor víctima no pot proporcionar servei a aquells que hi volen accedir. És a dir, en els atacs de xarxa DoS i DDoS, l'objectiu és simplement interrompre l'efectivitat del servei del servidor atacat, mitjançant un allau de sol·licituds il·legítimes. Atès que el lloc ha de respondre a cada sol·licitud, els seus recursos s'esgoten amb totes les respostes. Això fa que sigui impossible que el lloc serveixi als usuaris com ho fa normalment i sovint provoca un tancament complet del lloc.

Una manera habitual de prevenir els atacs DoS és utilitzar un tallafoc que detecti si les sol·licituds enviades al servidor són legítimes. Les sol·licituds atacants es poden descartar, cosa que permet que el trànsit normal flueixi sense interrupcions. Un exemple d'un gran atac a Internet d'aquest tipus es va produir al febrer de 2020 contra Amazon Web Services (AWS).

Atacs de contrasenya

Les contrasenyes són l'eina de verificació d'accés preferida per la majoria de la gent, per la qual cosa descobrir la contrasenya d'una persona o servei és una proposta atractiva per a un atacant. Això es pot aconseguir mitjançant uns quants mètodes diferents, alguns d'ells fent servir tècniques d'enginyeria social.

Un atacant també pot utilitzar un atac de diccionari per a esbrinar la contrasenya d'un usuari. Un atac de diccionari és una tècnica que utilitza paraules i frases comunes, com les que es troben en un diccionari, per a intentar endevinar la contrasenya de l'objectiu. Un mètode eficaç per a prevenir els atacs de força bruta i de diccionari contra contrasenyes és configurar una política de bloqueig. Això bloqueja l'accés a dispositius, llocs web o aplicacions automàticament després d'un cert nombre d'intents fallits. Amb una política de bloqueig, l'atacant només té uns quants intents abans de ser bloquejat i no poder accedir.

Una altra possibilitat d'atac de contrasenya es basa en l'ús dels enregistradors de teclat (*keyloggers*). Es tracta d'un tipus de programari maliciós dissenyat per a rastrejar cada pulsació de tecla i informar-ne un atacant. Normalment, un usuari es descarrega el programari creient que és legítim, però aquest instal·la un enregistrador de teclat sense que l'usuari en sigui conscient. Per a protegir-se d'aquests atacs, cal executar un escàner de virus. Les empreses d'antivirus mantenen registres dels enregistradors de teclat més comuns i els marcaran com a perillosos.

16. Blastpass - CitizenLab

Privadesa de la informació

Tot i que pràcticament tothom té una idea més o menys clara del que és la privadesa, no hi ha una definició àmpliament acceptada per la comunitat acadèmica. Un aspecte específic és la privadesa de la informació, que aborda concretament la informació personal d'un individu i la divulgació d'aquesta informació personal. En altres paraules, la privadesa de la informació és «el dret dels individus, grups o institucions a determinar per ells mateixos quan, com i en quina mesura es comunica a d'altres informació sobre ells».

L'aparició i els avanços de les tecnologies de tractament de la informació, el pas d'un món analògic a un altre digital centrat en les dades i la tendència a recopilar i emmagatzemar dades personals han portat a entendre la importància, ara més que mai, de la preservació de la privadesa. Els dispositius electrònics actuals permeten als éssers humans generar i enregistrar una quantitat extraordinària d'informació en diverses formes: fotos, àudios, clips de vídeo, documents electrònics. A més, cada vegada es fan servir més les xarxes de telecomunicacions per a un gran ventall d'activitats i serveis: llegir el diari, anar de compres, mantenir-se en contacte amb altres persones, operacions bancàries, reservar vacances, xarxes socials, agenda en línia, etc. A tot això cal afegir la presència cada vegada més freqüent dels dispositius de la Internet de les coses (dispositius IoT, *Internet of Things*), que generen una gran quantitat de dades per a la seva aplicació en diferents àmbits. Els telèfons mòbils, els rellotges intel·ligents i altres dispositius portàtils augmenten dràsticament la cobertura i la rapidesa amb la qual les dades biomètriques i de comportament de les persones estan disponibles per al seu processament. En alguns casos, aquestes dades són compartides amb el coneixement de les persones afectades, per exemple, quan els usuaris publiquen vídeos, fotos o opinions sobre productes i temes d'actualitat. Una quantitat molt major es recopila de manera inadvertida quan les persones naveguen per pàgines web, utilitzen serveis de localització i aplicacions similars, o simplement entren en espais intel·ligents enriquits amb qualsevol cosa, des d'assistents de veu fins a càmeres de circuit tancat de televisió.

Les dades de comportament són molt descriptives de l'individu i posen de manifest multitud d'atributs. Contenen forts indicadors de rutines, hàbits i també afeccions mèdiques i «tics». Les correlacions conegudes entre trets fisiològics i afeccions mèdiques inclouen la detecció de depressió o consum d'antidepressius en imatges facials, la detecció d'insuficiències orgàniques a causa de la coloració dels ulls (hepatitis) o de la pell (abús d'alcohol, estat físic general, i altres). Aquestes dades també es poden utilitzar per a identificar individus de manera única; per exemple, la forma de caminar s'ha utilitzat de forma molt rellevant per a identificar individus i revela atributs individuals com l'edat, el gènere i condicions fisiològiques.

Una altra amenaça de privadesa pot provenir de l'ús de dispositius portàtils per a serveis basats en la ubicació (LBS) o monitoratge de la salut. Els dispositius que permeten monitorar el cos poden recopilar informació com són el ritme cardíac, la ubicació i trajectòria, i emmagatzemar-la al núvol del dispositiu o al telèfon intel·ligent local. En conseqüència, la protecció de la privadesa esdevé cada vegada més important, ja que una gran quantitat d'informació privada pot ser utilitzada indegudament per tercers no desitjats sense les corresponents mesures de protecció i el consentiment dels usuaris.

Es considera que unes dades són sensibles si la seva divulgació, accés o ús sense autorització pot causar danys, perjudici, vergonya o discriminació a una persona. Algunes normatives de privadesa, com el Reglament general de protecció de dades (GDPR) de la Unió Europea proporcionen definicions específiques d'informació sensible i exigeixen que les organitzacions incorporin mesures adequades per a protegir aquestes dades, com el xifratge, els controls d'accés i la minimització de dades.

L'estudi de la privadesa es pot dividir en dues categories: privadesa del contingut i privadesa de la interacció. En la primera classe, els atacants poden identificar una persona a partir d'un conjunt de dades anonimitzades o xifrades amb cert coneixement sobre les persones afectades. En el segon cas, mentre es realitza una activitat en línia, encara que la confidencialitat de la informació que es transmet estigui protegida mitjançant xifrat, l'origen i la destinació de la comunicació són fàcilment traçables. La informació sobre qui es comunica amb qui pot revelar informació crítica que podria ser utilitzada. Per exemple, algú que accedeixi a un lloc web amb informació sobre una malaltia potencialment mortal pot no obtenir una assegurança mèdica o perdre el seu treball si aquesta informació arriba a la companyia d'assegurances o a l'ocupador. La possibilitat de relacionar tota la informació de trànsit generada per un usuari d'Internet (per exemple, a través de l'adreça IP, el número d'identificació nacional o el número de la seguretat social) permet elaborar perfils sofisticats de cada usuari.

Així doncs, cal establir un balanç entre la necessitat d'utilitzar les dades personals i el dret de les persones a la privadesa de les dades. La privadesa de les dades està estretament relacionada amb la protecció de les dades. La privadesa de les dades i la protecció de les dades comparteixen el mateix objectiu: protegir les dades sensibles de les violacions, els ciberatacs i la pèrdua accidental o intencionada de dades. No obstant això, mentre que la privadesa de la informació es centra

en les normes sobre com les organitzacions poden recopilar, emmagatzemar i processar informació personal, la protecció de les dades es centra en els controls de seguretat que garanteixen la confidencialitat, la integritat i la disponibilitat de la informació. A més, la protecció de les dades sovint implica protegir no només la informació personal, sinó altres dades crítiques per al negoci, com secrets comercials de l'empresa i dades financeres.

Tipus i sensibilitat de les dades

A fi i efecte d'explorar els diferents tipus d'informació sensible que diverses normatives defineixen i supervisen, en primer lloc cal introduir els conceptes bàsics d'*informació identificable de persona* (PII, *Personally Identifiable Information*) i d'*informació personal* (PI, *Personal Information*).

La PII o informació identificable de persona es defineix com aquella informació que, o bé per si sola o bé quan es combina amb una altra informació, pot utilitzar-se per a identificar o rastrejar la identitat d'una persona. La PII constitueix el tipus de dades disponible més habitualment i de forma menys regulada. En termes més generals, el NIST (National Institute of Standards and Technology), en el *document Guide to Protecting the Confidentiality of Personally Identifiable Information*, ofereix els següents exemples d'informació que poden considerar-se PII:

— Nom: com pot ser el nom complet o àlies.

— Número d'identificació personal: com el número del document nacional d'identitat, número de seguretat social (SSN), el número del passaport, el número del permís de conduir, el número d'identificació fiscal, el número d'identificació del pacient o el número del compte financer o de la targeta de crèdit.

— Dades d'adreça: com l'adreça postal o l'adreça de correu electrònic.

— Característiques personals, incloses imatges fotogràfiques (especialment de la cara o una altra característica distintiva), radiografies, empremtes dactilars o altres imatges biomètriques o dades de plantilles (per exemple, escàners de retina, signatura vocal, geometria facial).

— Informació sobre una persona vinculada o vinculable a una de les anteriors (per exemple, data de naixement, lloc de naixement, raça, religió, pes, activitats, indicadors geogràfics, informació laboral, informació mèdica, informació educativa, informació financera).

La PI o informació personal és una categoria més àmplia. En altres paraules, tota la PII es considera PI, però no tota la PI és PII. Així doncs, la PI es defineix com aquella informació que identifica, es refereix, descriu, pot associar-se o podria raonablement vincular-se, directament o indirectament, amb una persona concreta. La PI, per tant, pot incloure dades que estan òbviament associades a una identitat –com un nom o una data de naixement, que sovint també és PII– o interpretar-se d'una manera legal extremadament àmplia. La PI pot i sol incloure aspectes com origen racial o ètnic, afiliacions o opinions polítiques, creences religioses o filosòfiques, afiliació sindical, orientació sexual, antecedents penals, informació mèdica o genètica, dades biomètriques, informes de localització, adreces IP…

També és útil exposar quins tipus de dades NO estan subjectes a preocupacions sobre la privadesa de les dades. N'hi ha dos tipus principals:

— Dades de caràcter personal no sensibles (PII): informació que ja es troba en registres públics, com una guia de telèfons i un directori en línia.

— Informació no identificable personalment (no-PII): dades que no es poden utilitzar per a identificar una persona. Els exemples inclouen identificadors de dispositius o galetes (*cookies*). No obstant això, algunes lleis de privadesa consideren que fins i tot les galetes podrien ser considerades dades personals, ja que poden deixar rastres que podrien ser utilitzats en combinació amb altres identificadors per a establir la identitat d'una persona.

La definició d'*informació sensible* –també coneguda com a «dades sensibles»– és una mica diferent depenent de les lleis de privadesa aplicables. Com a definició global es pot assumir que la informació sensible són aquelles dades personals que la majoria de jurisdiccions consideren que haurien de ser tractades amb un estàndard de cura més elevat. Es considera que unes dades són sensibles si la seva divulgació, accés o ús sense autorització pot causar danys, perjudici, vergonya o discriminació a una persona. Tot sovint, la informació sensible inclou dades d'identificació personal així com informació financera, mèdica, antecedents penals i qualsevol altra dada que pugui utilitzar-se per a identificar o rastrejar una persona. La PII pot o no ser sensible –o pot considerar-se sensible només en determinades circumstàncies. Per exemple, alguns PII com ara noms, números de telèfon o una altra informació que pot ser de domini públic no sol considerar-se sensible (encara que podria ser-ho en determinats contextos), mentre que altres PII com ara números de la seguretat social, números de registre d'estrangers sí que ho serien. Algunes normatives de privadesa, com el Reglament general de protecció de dades (GDPR) de la Unió Europea, proporcionen definicions específiques d'informació sensible i exigeixen que les organitzacions incorporin mesures adequades

per a protegir aquestes dades, com el xifratge, els controls d'accés i la minimització de dades.

Per tant, les dades sensibles requereixen un nivell més alt de protecció a causa de la seva naturalesa delicada i personal, com la informació mèdica, l'orientació sexual, la religió, la raça, entre altres. Per a protegir-la, cal aplicar mesures de seguretat més rigoroses. I, depenent de la llei, és possible que es requereixin diferents tipus de consentiment per a recopilar-la.

A continuació s'indiquen alguns dels tipus d'informació comunament considerats sensibles, tant pel públic en general com pels mandats legals:

— **Informació sanitària personal** (PHI, *Personal Health Information*): historial mèdic, informació sobre assegurances i altres dades privades que recullen els proveïdors d'assistència sanitària i que podrien vincular-se a una persona determinada.

— **Informació financera personal identificable** (PIFI, *Personally Identifiable Financial Information*): números de targetes de crèdit, detalls de comptes bancaris o altres dades relatives a les finances d'una persona.

— **Expedients acadèmics:** qualificacions, expedients acadèmics, horari de classes, dades de facturació i altres registres relatius a la formació acadèmica d'una persona.

Els registres d'una base de dades poden contenir informació, que, segons la seva naturalesa o tipologia, poden classificar-se en:

— **Atributs clau o identificadors:** són camps que identifiquen unívocament els subjectes de les dades (nom, DNI, núm. de passaport, telèfon…). Aquest tipus de dades han d'eliminar-se dels registres anonimitzats.

— **Quasiidentificadors:** són camps que, si bé per si mateixos i de forma aïllada no identifiquen un individu (com ara edat, ocupació, codi postal), agrupats amb altres atributs quasiidentificadors poden assenyalar de manera unívoca un subjecte. Les tècniques d'anonimització treballen sobre aquestes dades, eliminant camps que no són necessaris per al tractament (en aplicació del principi de minimització), agregant-los o generalitzant-los.

— **Atributs sensibles:** són els camps que contenen dades que podrien tenir un major impacte en la privadesa d'un individu concret, entre ells les categories especials de dades, i que no han de ser vinculats amb el subjecte de dades al qual pertanyen (malalties, tractaments mèdics, nivell de renda…). Aquesta informació pot ser de gran interès en l'objecte del tractament de dades, però, tret que existeixi una legitimació per a això, ha de mantenir-se dissociada d'un subjecte concret.

— **Altres:** la informació que no pertany a les tres categories anteriors.

A continuació, es presenten algunes mesures per a tractar les dades sensibles sota un punt de vista de privadesa:

— **Minimització de dades:** es tracta de recol·lectar només les dades necessàries i rellevants per al propòsit específic de la recol·lecció. És a dir, s'han de recollectar només les dades necessàries per a complir amb un propòsit específic i no més del necessari.

— **Consentiment informat:** és important obtenir el consentiment explícit i lliure de la persona per a recol·lectar i utilitzar les seves dades sensibles. El consentiment ha de ser informat, específic i atorgat de manera voluntària.

— **Protecció de dades:** les dades sensibles han de ser emmagatzemades i protegides adequadament per a evitar l'accés no autoritzat o l'ús inadequat. Es poden utilitzar mesures tècniques, com el xifratge, i mesures organitzatives, com a polítiques de seguretat i accés restringit a les dades.

— **Eliminació de dades:** és important que les dades sensibles siguin eliminades de manera segura una vegada que ja no siguin necessàries per al propòsit per al qual van ser recollides.

— **Responsabilitat i transparència:** les organitzacions que gestionen dades sensibles han de ser transparents quant a la recol·lecció, ús i protecció de les dades, i han d'assumir la responsabilitat de garantir la privadesa i seguretat de les dades.

En resum, el tractament de les dades sensibles des d'un punt de vista de privadesa requereix mesures de protecció i seguretat específiques, així com transparència i responsabilitat per part de les organitzacions que manegen aquestes dades.

En els darrers anys la preservació de la privadesa ha despertat un interès considerable entre tota la comunitat i per tant també entre els acadèmics i els dissenyadors. En conseqüència, s'han desenvolupat diversos mètodes per a protegir la privadesa o s'han establert polítiques amb un àmbit ampli per a la protecció de dades sensibles. En l'actualitat, no hi ha solucions genèriques que puguin gestionar tots els problemes de privadesa relatius a la protecció de la informació sensible contra la divulgació no desitjada mentre es conserva la utilitat de les dades. Les tècniques tradicionals es basaven únicament en l'anonimització, és a dir, eliminant tots els identificadors –atributs

que identifiquen sense ambigüitat els participants, com ara el número de seguretat social, el passaport, el nom-cognom). No obstant això, cal tenir en compte que les combinacions úniques de valors d'atributs poden utilitzar-se per a tornar a identificar sense ambigüitat un individu en una base de dades sense identificadors explícits, i en tornar a identificar un participant d'una base de dades, se li poden revelar els atributs confidencials (sensibles) com ara el salari, malalties, ideologia, etc.

Tecnologies de protecció de la privadesa

Les tecnologies de protecció de la privadesa (en anglès, *Privacy-Enhancing Technologies*, PET) són un conjunt d'eines tècniques dissenyades per a protegir la privadesa de les dades personals en diverses aplicacions i sistemes d'informació. Aquestes tecnologies proporcionen un conjunt de mecanismes per a minimitzar la quantitat d'informació personal que es recopila, processa i divulga, garantint que es compleixin els principis fonamentals de privadesa. En la darrera dècada s'han proposat nombroses eines PET relacionades amb l'anonimització del trànsit de xarxa (per exemple, la xarxa TOR), la gestió d'identitats, l'emmagatzematge anònim de dades, a més de les tècniques criptogràfiques i de separació de la informació.

Bàsicament les tècniques de privadesa de dades es poden classificar en tècniques de pertorbació de dades i tècniques d'emmascarament o anonimització, tal com s'indica a la següent figura. A grans trets es tracta d'eliminar o modificar determinades dades personals d'una persona, d'un conjunt de dades, de manera que la persona no pugui ser identificada directa o indirectament a partir d'aquestes dades. D'aquesta manera es redueix el risc que les dades siguin utilitzades de manera inapropiada o es divulguin sense autorització. Aquest procés es realitza a través de diverses tècniques, com l'eliminació de certs camps de dades, la substitució dels valors reals de les dades per valors ficticis o l'agregació de les dades en categories més generals.

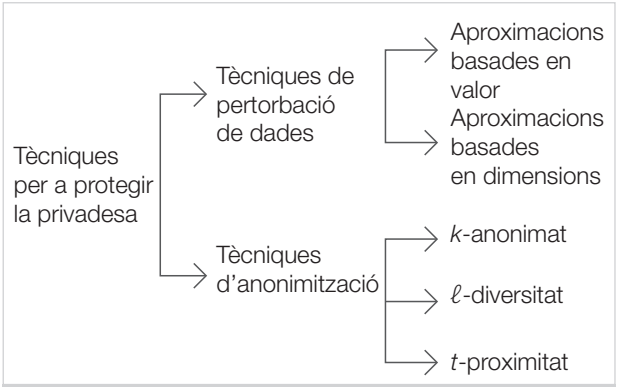

Figura 3: Tècniques per a protegir la privadesa

Les tècniques de pertorbació de dades són un conjunt de mètodes consistents a introduir canvis deliberats en les dades abans de la seva anàlisi o divulgació. Aquestes tècniques són especialment rellevants en el context de la ciència de dades, l'aprenentatge automàtic i la mineria de dades, on es busca utilitzar dades per a obtenir informació valuosa sense revelar informació sensible o identificable sobre les persones o organitzacions involucrades. El resultat és equivalent a afegir «soroll» a les bases de dades que permet la confidencialitat individual del registre. La pertorbació de dades s'aplica típicament als registres electrònics de salut (EHR) per a protegir la informació sensible, tot i que el seu ús no es limita a la indústria sanitària. Aquestes tècniques de pertorbació poden tenir dos enfocs diferents: basats en valors i basats en dimensions.

— Les aproximacions basades en valor fan referència a mètodes que modifiquen o pertorben els valors de les dades, alhora que preserven les propietats estadístiques generals o les característiques del conjunt de dades. Aquestes tècniques dificulten la reidentificació de persones específiques en un conjunt de dades, però encara permeten obtenir informació i coneixements significatius a partir de les dades pertorbades. Bàsicament, en comptes d'utilitzar directament els valors originals de les dades, les aproximacions basades en valors modifiquen aquests valors d'una manera que conserva la utilitat de les dades per a l'anàlisi, però redueix el risc de violacions de la privadesa. Les aproximacions basades en valors es fan servir sovint en escenaris on cal analitzar dades a nivell individual mentre es protegeix la privadesa. Alguns exemples poden ser recerca mèdica, anàlisi de dades del cens i aplicacions d'aprenentatge automàtic. Aquestes tècniques ajuden les organitzacions i els investigadors a adherir-se a les regulacions de privadesa i als estàndards ètics, tot i obtenir coneixements amb valor de dades sensibles.

— Les aproximacions basades en dimensions fan referència a mètodes que es centren a pertorbar o alterar les dades en dimensions o atributs específics del conjunt de dades, mentre es preserva l'estructura global i les propietats estadístiques de les dades. Aquestes tècniques s'utilitzen per a millorar la protecció de la privadesa afegint soroll o fent modificacions en determinades característiques, reduint així el risc de reidentificació de les persones. Entre altres possibilitats, es poden fer servir tècniques d'aleatorització per a introduir soroll controlat o alteracions a les dimensions seleccionades, de manera que sigui més difícil vincular punts de dades específics a persones mentre es permet l'anàlisi significativa. Les aproximacions basades en dimensions són especialment útils quan es treballa amb conjunts de

dades on només un subconjunt d'atributs conté informació sensible, i és essencial protegir aquests atributs mentre es permet l'anàlisi en dimensions no sensibles. Aquestes tècniques troben l'equilibri entre la preservació de la privadesa i la utilitat de les dades, assegurant que encara es puguin obtenir coneixements significatius de les dades pertorbades mentre es redueix el risc de vulneracions de la privadesa.

Les tècniques d'anonimització per a la privadesa es refereixen a mètodes i processos utilitzats per a eliminar o ocultar la informació personalment identificable (PII) de conjunts de dades, fent que sigui més difícil identificar o relacionar persones específiques amb les dades. No obstant això, cal tenir en compte que l'eficàcia d'aquestes tècniques depèn de diversos factors, com la qualitat del procés d'anonimització, els requisits específics de privadesa i el model d'amenaces. En alguns casos, fins i tot les dades ben anonimitzades poden ser vulnerables a atacs de reidentificació si hi ha altres informacions externes disponibles per als atacants. A continuació s'indiquen alguns tipus de tècniques d'anonimització.

— ***k*-anonimat**: El *k*-anonimat és una tècnica de privadesa de dades que s'utilitza per a protegir la identitat dels individus en conjunts de dades que es comparteixen públicament. La idea principal darrere del *k*-anonimat és que una entitat que publica un conjunt de dades ha de garantir que cada individu en el conjunt de dades sigui indistingible d'almenys *k*-1 altres individus en el mateix conjunt de dades. En altres paraules, el *k*-anonimat assegura que no es pugui identificar un individu específic en un conjunt de dades compartit. Es diu que un individu és *k*-anònim dins del conjunt de dades en el qual es troba inclòs si, i només si, per a qualsevol combinació dels atributs quasiidentificadors associats, existeixen almenys uns altres *k*-1 individus que comparteixen amb ell els mateixos valors per a aquests mateixos atributs. Cal tenir en compte que el *k*-anonimat no es centra en els atributs sensibles dels registres, sinó en els atributs quasiidentificadors que poden permetre la vinculació.

  Per a aplicar la tècnica del *k*-anonimat, s'agrupen les dades per atributs que permeten identificar una persona, com el nom, l'adreça, el número d'identificació personal, etc. Després, s'eliminen els atributs identificadors i s'agrupen les dades en conjunts que contenen almenys *k* individus que comparteixen el mateix conjunt de valors d'atributs. Per a garantir el *k*-anonimat, es poden utilitzar tècniques de generalització, agrupació o supressió de dades.

  Per exemple, suposant que es té un conjunt de dades de pacients que inclou informació sobre la seva edat, gènere, ciutat de residència i resultat d'una prova mèdica. Per a aplicar el *k*-anonimat, es podrien agrupar les dades per edat, gènere i ciutat de residència, i després eliminar els identificadors com a noms o números d'identificació personal. Després, es poden generalitzar o suprimir uns certs valors per a garantir que cada grup contingui almenys *k* pacients que comparteixen el mateix conjunt de valors d'edat, gènere i ciutat de residència.

  Suposant que un hospital té una base de dades de pacients que inclou el seu DNI, informació sobre la seva edat, gènere, codi postal i malaltia:

DNI	Edat	Gènere	Codi postal	Malaltia
21057841	22	H	25036	Cardiovascular
74323432	23	H	25012	Respiratori
23489343	18	H	25600	Cardiovascular
44648948	47	D	08870	Osteoporosi
78489455	42	D	08630	Respiratori
61154615	50	D	08292	No malaltia
54687897	23	H	17256	Pàncrees
87879873	25	H	17800	Paget
91584168	19	D	17424	COVID
21548710	41	D	43008	Glaucoma
33728590	41	H	43001	Diabetis
09342859	41	D	43004	No malaltia

  Per a aplicar la tècnica d'agregació mitjançant *k*-anonimat en aquesta taula, es podria procedir de la següent manera:

  – **Definir el valor de *k***: *k* representa el nivell d'anonimat que es desitja aconseguir, és a dir, el nombre mínim d'individus que han de ser presents en cada grup d'atributs identificatius perquè no sigui possible identificar a cap d'ells. En aquest cas, se suposa que es desitja un nivell d'anonimat de *k*=3.

  – **Eliminar els atributs identificadors** (en aquest cas el DNI) i identificar els atributs quasiidentificadors: són aquells atributs que combinats poden permetre la identificació d'un individu en la taula original. En aquest cas, són l'edat, el gènere i el codi postal.

  – **Agrupar les dades:** s'han d'organitzar les dades per cada combinació d'atributs identificatius, de manera que a partir de la malaltia no es pugui identificar qui és el pacient i que almenys hi hagi *k* possibilitats.

Edat	Gènere	Codi postal	Diagnosi
<25	H	25***	Cardiovascular
<25	H	25***	Respiratori
<25	H	25***	Cardiovascular
40-50	D	08***	Osteoporosi
40-50	D	08***	Respiratori
40-50	D	08***	No malaltia
<25	*	17***	Pàncrees

Edat	Gènere	Codi postal	Diagnosi
<25	*	17***	Paget
<25	*	17***	COVID
41	*	4300*	Glaucoma
41	*	4300*	Diabetis
41	*	4300*	No malaltia

Les columnes sensibles d'interès no poden revelar informació que hagi estat retallada a les columnes generalitzades. Per exemple, algunes malalties són úniques d'homes o dones, cosa que podria revelar un atribut de gènere que havia estat retallat, i per tant, podria comprometre l'anonimat.

Els valors a les columnes sensibles no són tots iguals per a un grup particular de *k*. Si els valors sensibles són tots iguals per a un conjunt de *k* registres que comparteixen atributs quasiidentificadors, aleshores aquest conjunt de dades encara és vulnerable a un atac anomenat *atac d'homogeneïtat*. En un atac d'homogeneïtat, l'atacant fa servir el fet que és suficient trobar el grup de registres al qual pertany la persona si tots tenen el mateix valor sensible. Per exemple, si tots els homes majors de 60 anys del conjunt de dades tenen càncer, si se sap que en Joan té més de 60 anys i està en el conjunt de dades, es té la certesa que en Joan té càncer. A més, fins i tot si no tots els valors són iguals per a un grup de *k*, si no hi ha prou diversitat, encara hi ha una alta probabilitat que s'aprengui alguna cosa més sobre en Joan. Si aproximadament el 90 per cent dels registres del grup tenen el mateix valor sensible, un atacant pot inferir amb una gran certesa quin és l'atribut sensible de la persona. Mesures com la ℓ-diversitat i la *t*-proximitat (que seran explicades posteriorment) es poden utilitzar per a especificar que entre qualsevol *k* registres coincidents ha d'haver-hi una certa quantitat de diversitat en els valors sensibles. Per a il·lustrar-ho, imaginant que les tres persones que formen part del darrer bloc haguessin tingut la mateixa malaltia, si se sap que una de les persones que han format part d'aquell estudi viu al codi postal 43004, ja es pot saber quina malaltia té, i per tant, s'hauria compromès la seva privadesa.

— **ℓ-diversitat:** aquest concepte es va introduir per a evitar els atacs d'homogeneïtat indicats en el paràgraf anterior. La ℓ-diversitat és una tècnica que permet ampliar el *k*-anonimat assegurant que cada grup de registres indistingibles tingui com a mínim ℓ valors diferents per a atributs sensibles. Això afegeix una capa addicional de protecció contra atacs basats en atributs. Es procedeix a il·lustrar la ℓ-diversitat amb un exemple. Suposant que es té un conjunt de dades que conté els expedients mèdics dels pacients, i un dels atributs és «Diagnosi», que indica la condició mèdica de cada pacient. Es vol publicar una part d'aquest conjunt de dades amb fins de recerca al mateix temps que es preserva la privadesa dels pacients.

Assumint que el conjunt de dades original és

Edat	Gènere	Codi postal	Diagnosi
29	H	90216	Diabetis
29	D	90219	Asma
31	H	90217	Asma
22	D	94105	Hipertensió
39	H	94117	Asma
24	D	94109	Asma
37	H	94126	Diabetis
26	D	90216	Diabetis
21	H	90213	Diabetis
36	H	94105	Hipertensió
27	H	90217	Hipertensió
28	D	90211	Hipertensió
22	H	90211	Hipertensió
34	H	90211	Hipertensió
23	D	94102	Diabetis
32	H	90213	Diabetes
24	H	90218	Asma
28	H	90214	Asma

una possible modificació de la base de dades, després d'aplicar la ℓ-diversitat amb ℓ=3, seria

Edat	Gènere	Codi postal	Diagnosi
30-34	H	9021*	Diabetes
30-34	H	9021*	Hipertensió
30-34	H	9021*	Asma
20-24	D	9410*	Hipertensió
20-24	D	9410*	Diabetis
20-24	D	9410*	Asma
25-29	D	9021*	Hipertensió
25-29	D	9021*	Diabetis
25-29	D	9021*	Asma
35-39	H	941**	Hipertensió
35-39	H	941**	Diabetis
35-39	H	941**	Asma
20-24	H	9021*	Hipertensió
20-24	H	9021*	Diabetis
20-24	H	9021*	Asma
25-29	H	9021*	Hipertensió
25-29	H	9021*	Diabetis
25-29	H	9021*	Asma

– En aquest conjunt de dades modificat, s'ha assegurat una 3-diversitat per a l'atribut «Diagnosi». Per a la categoria «Diabetis», hi ha cinc pacients diferents. Això fa que sigui més difícil per a un adversari determinar la condició mèdica d'un individu específic basant-se únicament en l'atribut «Diagnosi» compartit.

– La ℓ-diversitat és una manera de reforçar la protecció de la privacitat dels atributs sensibles dins d'un

conjunt de dades, particularment quan es lliura o es comparteixen dades per a investigació o anàlisi, alhora que es redueix el risc d'atacs d'inferència basats en atributs. El valor específic de ℓ en la ℓ-diversitat pot variar en funció del nivell desitjat de protecció de la privacitat i la naturalesa del conjunt de dades.

— ***t*-proximitat**: La *t*-proximitat és una mesura de privadesa que té com a objectiu assegurar que la distribució dels atributs sensibles en un grup de registres indistingibles no sigui significativament diferent de la distribució general en el conjunt de dades.

Privadesa en les etapes de cicle de vida de la informació

Les tècniques i mecanismes de privacitat varien segons la fase del cicle de vida de les dades. A continuació, es presenten les tècniques i mecanismes de privacitat en les fases de recopilació, generació, emmagatzematge i processament de dades:

Etapa 1: recopilació d'informació personal

La primera etapa del cicle de vida de la informació és la recopilació de dades personals. Aquí, les entitats han d'assegurar-se d'obtenir el consentiment adequat dels individus abans de recopilar les seves dades. A més, s'han d'establir polítiques clares i transparents per a informar els usuaris sobre com s'utilitzarà la seva informació personal.

Etapa 2: emmagatzematge i gestió de la informació personal

Una vegada que es recopila la informació personal, és crucial garantir-ne l'emmagatzematge segur i la seva correcta gestió. Això implica implementar mesures tècniques i organitzatives per a protegir les dades contra accessos no autoritzats, pèrdues o filtracions. A més, és essencial establir polítiques i procediments clars sobre qui té accés a la informació personal i com es gestiona internament. Entre altres tècniques es fan servir les següents:

— **Xifratge:** El xifratge de les dades implica transformar-les en una seqüència de caràcters incomprensible per a qualsevol persona que no tingui la clau de desxifratge. Això ajuda a protegir les dades emmagatzemades en cas que siguin robades o s'hi hagi accedit de manera no autoritzada.

— **Accés restringit:** Es poden establir mesures per a limitar l'accés a les dades emmagatzemades només a les persones que tenen permís. Això inclou la implementació de sistemes d'autenticació i autorització per a garantir que només les persones autoritzades tinguin accés a les dades.

Etapa 3: ús i processament de la informació personal

Durant aquesta etapa, les organitzacions utilitzen la informació personal recopilada per als fins previstos. No obstant això, és important garantir que l'ús i processament de les dades es realitzin de manera compatible amb les lleis i regulacions de privacitat aplicables. Les organitzacions han d'establir restriccions i controls adequats per a assegurar-se que la informació personal només s'utilitzi d'acord amb els consentiments atorgats pels individus. Entre altres tècniques es fan servir les següents:

— **Anonimització o perturbació:** es modifiquen els conjunts de dades recopilades per a publicar-los garantint la privadesa. D'aquesta forma es permet el processament de les dades per a fins específics sense revelar la identitat de l'individu.

— **Minimització de dades:** com s'ha esmentat anteriorment, la minimització de dades implica publicar només la informació necessària per al propòsit específic de l'ús.

Etapa 4: retenció i eliminació de la informació personal

La retenció i eliminació de la informació personal és una etapa crítica en el cicle de vida de la informació. Les entitats han de definir períodes de retenció clars i complir amb les obligacions legals i reguladores. A més, han d'implementar procediments adequats per a eliminar de manera segura i permanent les dades personals quan ja no siguin necessaris per als fins per als quals es van recopilar.

En resum, les tècniques i mecanismes de privacitat en les fases de generació, emmagatzematge i processament de dades inclouen l'anonimització, la perturbació, la minimització de dades, l'encriptació, l'accés restringit, el consentiment informat. És important implementar aquestes mesures per a garantir la privacitat i seguretat de les dades en cada fase del cicle de vida de les dades.

Aspectes de la privadesa

Distingim tres tipus de privadesa: la privadesa de les dades, la privadesa de l'usuari i la privadesa de la localització. La privadesa de dades, la privadesa d'usuaris i la privadesa de localització són conceptes diferents però relacionats en el context de la privadesa en línia. La privadesa de dades es refereix a la protecció de les dades personals, la privadesa d'usuaris es refereix a la protecció de la identitat en línia d'un individu, i la privadesa de localització es refereix a la protecció de la informació de localització d'un individu.

A mode de resum es podria dir :

— La privadesa de dades fa referència al dret d'una persona a controlar la informació personal que comparteix amb els altres. Aquesta informació pot incloure el seu nom, adreça, número de telèfon, adreça de correu electrònic, historial de navegació, historial de compres, etc.

— La privadesa d'usuaris fa referència al dret d'una persona a controlar la seva identitat en línia. Aquesta identitat pot incloure el seu nom d'usuari, contrasenya, perfils de xarxes socials, etc.

— La privadesa de localització fa referència al dret d'una persona a controlar la seva informació de localització. Aquesta informació pot ser recopilada per agències governamentals, empreses tecnològiques o altres tercers.

Privadesa de les dades

Es refereix a la protecció de les dades personals d'un individu, com el seu nom, adreça, número d'identificació, informació financera, historial mèdic, entre d'altres. La privadesa de dades implica que aquestes dades només siguin recopilades, emmagatzemades i utilitzades de manera legal i ètica, i que s'implementin mesures adequades per a garantir la seva seguretat. La privadesa de dades s'enfoca en la protecció de les dades com a entitat en si mateixa.

Alguns exemples pràctics de privadesa de les dades:

— Una empresa de comerç electrònic ha d'obtenir el consentiment informat d'un client abans de recopilar les dades personals, com el seu nom, adreça de correu electrònic i detalls de pagament.

— Una empresa d'anàlisi de dades ha d'utilitzar tècniques d'anonimització de dades per a eliminar qualsevol informació que pugui identificar un individu de les dades recopilades abans d'utilitzar-les per a l'anàlisi.

— Una empresa de serveis financers ha de limitar l'accés a les dades personals a només aquells empleats que necessiten tenir accés per a fer les seves funcions laborals.

— Un servei de correu electrònic ha d'utilitzar tècniques de xifratge per a protegir les dades mentre es transmeten d'un servidor a un altre.

Privadesa d'usuari

Es refereix a la protecció de la identitat en línia d'un individu, incloent el seu nom d'usuari, contrasenya, adreces de correu electrònic i altra informació personal que el pugui identificar. La privadesa d'usuari implica que aquesta informació només es comparteixi amb tercers amb el consentiment de l'usuari i que s'implementin mesures de seguretat per a protegir-la de l'exposició no autoritzada. La privadesa d'usuari s'enfoca en la protecció de la identitat de l'usuari i de la manera com s'utilitza en línia.

Alguns exemples pràctics de la privadesa de l'usuari:

— Un lloc web de xarxes socials ha de permetre als usuaris configurar les seves preferències de privadesa, com qui pot veure el seu perfil i qui pot veure les seves publicacions.

— Una aplicació de missatgeria ha de permetre als usuaris controlar qui pot veure la seva informació de contacte, com ara el número de telèfon o l'adreça de correu electrònic.

— Un servei de correu electrònic ha de permetre als usuaris controlar qui els pot enviar correus electrònics i qui pot veure la safata d'entrada.

— Un servei de transmissió de vídeo ha de permetre als usuaris controlar qui pot veure el seu historial de visualització i quines recomanacions de contingut se'ls mostren.

Privadesa de localització

La privadesa de localització és el dret d'una persona a controlar la informació sobre la seva ubicació geogràfica, històric de localitzacions i patrons de desplaçament. Aquesta informació pot ser recopilada per diversos dispositius i aplicacions, com ara telèfons mòbils, ordinadors, sistemes de navegació GPS i aplicacions de seguiment d'activitat.

La privadesa de localització és important per diverses raons. En primer lloc, pot ser utilitzada per a rastrejar els moviments d'una persona, i en segon lloc, la informació de localització pot ser utilitzada per a crear perfils de comportament, i en conseqüència ser utilitzada amb objectius de màrqueting o fins d'espionatge.

Moltes de les accions que es fan a través d'Internet, com trucar algú per telèfon mòbil, fer un apunt sobre un esdeveniment, utilitzar el sistema de navegació d'un cotxe o pagar amb targeta de crèdit, van deixant un rastre ininterromput de les nostres activitats quotidianes. Aquestes accions es registren fàcilment i s'emmagatzemen de manera persistent en bases de dades. La privadesa de la ubicació requereix que aquesta informació només es recopili i comparteixi de manera transparent i legal, i que els usuaris tinguin control sobre com s'utilitza i es comparteix.

La pràctica comuna adoptada pels recopiladors i propietaris de dades per a protegir la privadesa dels in-

dividus que monitoren és la pseudonimització, també coneguda com a *despersonalització*. Aquest enfocament senzill consisteix a eliminar tots els identificadors personals (per exemple, informació que estigui directament relacionada amb la identitat de la persona, com ara el nom, el número de telèfon, l'adreça precisa, el número de matrícula, etc.) i substituir-los per algun pseudoidentificador. Malauradament, la pseudonimització només proporciona un nivell molt baix de protecció, per exemple, la correlació creuada naïf de les dades pseudonimitzades amb informació addicional (obtinguda, per exemple, de dades de xarxes socials d'accés públic) pot permetre la reidentificació, és a dir, la revelació de les identitats dels usuaris amb una alta probabilitat. Així doncs, la primera mesura que cal prendre per a protegir la privadesa de localització es desactivar la ubicació del telèfon mòbil quan no sigui necessària.

Regulació de la protecció de dades

A causa de les creixents preocupacions públiques, els governs estan ocupats creant i adaptant lleis de protecció de dades i privadesa. De fet, la necessitat d'abordar els problemes actuals de privadesa i protegir els drets de privadesa de les dades és una tendència global. El Reglament general de protecció de dades de la UE (RGPD) és la llei més coneguda, però molts països, inclosos el Brasil, l'Índia i Nova Zelanda, han promulgat noves regulacions de privadesa o han reforçat les lleis existents per a regular com es poden recopilar, emmagatzemar, utilitzar, divulgar i transmetre dades personals.

A Espanya, la regulació de la protecció de dades està composta per dos documents principals:

— El Reglament general de protecció de dades (RGPD), que és una normativa europea que s'aplica a tots els estats membres de la Unió Europea, inclosa Espanya.

— La Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD), que és una llei espanyola que desenvolupa el RGPD.

El RGPD és una norma europea que estableix un marc de protecció de dades personals a tota la Unió Europea. Aquesta normativa s'aplica a totes les empreses que processen dades personals de ciutadans de la Unió Europea, independentment de la ubicació de l'empresa. El RGPD defineix les dades personals com «tota informació sobre una persona física identificada o identificable». Això inclou informació com el nom, l'adreça, el número de telèfon, l'adreça de correu electrònic, l'historial de navegació i l'historial de compres. El RGPD estableix una sèrie de principis que han de ser respectats per les persones que tracten dades personals. Aquests principis inclouen:

— Lleialtat i transparència: les persones han de ser informades sobre com es tracten les seves dades personals, i aquestes només es poden tractar amb un propòsit determinat i lícit.

— Minimització de dades: només es poden recopilar aquelles dades personals que són necessàries per a la finalitat prevista.

— Limitació de la conservació: les dades personals només es poden conservar durant el temps necessari per a la finalitat prevista.

— Integritat i confidencialitat: les dades personals han de ser protegides contra l'accés, la modificació, la divulgació o la destrucció no autoritzada.

— Responsabilitat: les persones que tracten dades personals han de ser responsables de complir amb els principis del RGPD.

La LOPDGDD complementa el RGPD i estableix una sèrie de mesures específiques per a la protecció de les dades personals a Espanya. Aquestes mesures inclouen:

— La creació de l'Agència Espanyola de Protecció de Dades (AEPD), que és l'organisme encarregat de vetllar pel compliment de la normativa de protecció de dades a Espanya.

— El dret dels ciutadans a sol·licitar l'accés, la rectificació, la supressió, la limitació del tractament, la portabilitat de les dades i l'oposició al tractament de les seves dades personals.

— El deure de les empreses de notificar a l'AEPD qualsevol incidència de seguretat que pugui afectar les dades personals dels seus clients.

Addicionalment, a Catalunya hi ha una autoritat de control específica, l'Autoritat Catalana de Protecció de Dades (APDCAT), que és l'entitat encarregada fonamentalment de supervisar i garantir l'aplicació de les dues normatives esmentades. També té altres funcions com promoure la sensibilització i la comprensió del públic respecte dels riscos, les normes, les garanties i els drets relacionats amb el tractament, i assessorar, de conformitat amb el dret dels estats membres, el parlament nacional, el govern i altres institucions i organismes, sobre les mesures legislatives i administratives relatives a la protecció dels drets i les llibertats de les persones físiques pel que fa al tractament de la normativa de protecció de dades a Catalunya. L'APDCAT treballa de manera coordinada amb l'Agència Espanyola de Protecció de

Dades (AEPD) per a garantir una protecció efectiva dels drets dels ciutadans en relació amb les seves dades personals.

Guia de bones pràctiques

Durant tot el document s'han estat donat recomanacions; aquest capítol en proporciona un recull i n'afegeix alguna més, combinant tant la part de ciberatacs com la part de la privadesa de la informació.

Recomanacions generals

S'ha vist que la ciberseguretat és un tema complex; cada dia es sofreixen més atacs. Si bé no existeix un sistema totalment segur, aplicar el sentit comú i fer cas d'unes directrius molt clares pot ajudar a minimitzar l'impacte de possibles atacs. Per tant, es recomana seguir aquests punts generals de seguretat:

— **Conscienciació i formació:** és important que les persones que manegen dades personals siguin conscients de la importància de la privadesa i sàpiguen com protegir-la. Cal formar els empleats i els usuaris en bones pràctiques de privadesa.

— **Verificació de la font:** cal verificar la font abans de proporcionar informació personal o financera, i evitar respondre a correus electrònics, trucades telefòniques o missatges sospitosos.

— **Privadesa en xarxes socials:** cal revisar la configuració de privadesa en els comptes de xarxes socials i ajustar les opcions per a protegir la informació personal, permetent compartir només l'estrictament necessària.

— **Navegació segura:** cal utilitzar un navegador web segur i configurar-lo per a bloquejar galetes de tercers i evitar-ne el seguiment. Garantir també que les pàgines web que es visitin siguin segures i utilitzin el protocol HTTPS.

— **Correu electrònic segur:** cal utilitzar un servei de correu electrònic segur i xifrat, i evitar enviar informació confidencial a través del correu electrònic.

— **Compra en línia segura:** cal verificar que el lloc web sigui segur abans de fer una compra en línia, i utilitzar una targeta de crèdit virtual o un servei de pagament segur.

— **Protecció de la identitat:** cal mantenir la informació personal segura i protegir la identitat en línia mitjançant la utilització d'eines com el bloqueig de crèdit i el monitoratge de la identitat.

Com guardar la informació personal

Com ja s'ha vist, les dades i la informació en general són tant l'objectiu dels atacants dels sistemes com una preocupació per als serveis en línia que s'acostumen a utilitzar. Per tant, tant quan es tenen dades de tercers com quan s'està oferint un servei, s'han de tenir en compte els següents punts:

— **Utilització de xifratge:** tant a nivell de les dades que es transmeten cap a un destinatari com les dades que es guarden a qualsevol dispositiu d'emmagatzematge.

— **Minimització de dades:** cal recopilar i emmagatzemar només la informació necessària per a complir el propòsit específic de la recopilació de dades. No cal recopilar dades innecessàries.

— **Consentiment informat:** cal obtenir el consentiment explícit i informat de les persones abans de recopilar les dades. El consentiment ha de ser lliurement donat i les persones han de saber exactament què s'està fent amb les seves dades.

— **Seguretat de les dades:** és important garantir la seguretat de les dades personals mitjançant la implementació de mesures de seguretat tècniques i organitzatives adequades, com ara el xifratge, l'autenticació d'usuaris, el control d'accés i el monitoratge de l'activitat.

— **Transparència:** cal informar les persones sobre l'ús de les seves dades personals, incloent-hi qui són els responsables del tractament de les dades, el propòsit de la recopilació de dades i com s'utilitzaran les dades.

— **Drets dels usuaris:** les persones tenen drets en relació amb les dades personals, com el dret d'accés, rectificació, supressió, limitació del tractament i portabilitat de dades. És important garantir que es respectin aquests drets.

— **Avaluacions d'impacte:** cal dur a terme avaluacions d'impacte de la privadesa per a identificar i minimitzar els riscos per a la privadesa en la recopilació i tractament de dades personals.

— **Revisió i actualització:** cal revisar i actualitzar les polítiques i pràctiques de privadesa de forma regular per a assegurar-se que se segueixen les millors pràctiques i s'adapten als canvis en la normativa i la tecnologia.

Com utilitzar els dispositius

Si bé aprendre a guardar les dades de forma correcta és important, també ho és com es controlen i s'uti-

litzen els dispositius personals, que, al cap i a la fi, proporcionen l'accés a les dades que es vol protegir. D'aquesta manera es poden donar les següents recomanacions:

- **Contrasenyes segures:** cal fer servir contrasenyes fortes i diferents per a cada dispositiu i compte de serveis en línia. Cal canviar les contrasenyes periòdicament.
- **Autenticació de dos factors:** és molt convenient habilitar l'autenticació de dos factors sempre que sigui possible. Això afegeix una capa addicional de seguretat per a protegir els dispositius i els comptes.
- **Actualitzacions de programari:** cal mantenir els dispositius i aplicacions actualitzats amb les últimes versions de programari i actualitzacions de seguretat per a evitar vulnerabilitats.
- **Antivirus i tallafocs:** cal fer servir programes d'antivirus i tallafocs per a protegir els dispositius de virus, programari maliciós i altres atacs informàtics.
- **Xarxes segures:** s'ha d'evitar en la mesura que es pugui la connexió a xarxes wifi obertes, ja que poden ser vulnerables a atacs informàtics.
- **Privadesa de la càmera i el micròfon:** és necessari prendre mesures per a protegir la privadesa de la càmera i el micròfon dels dispositius, com tapar la càmera o desactivar el micròfon quan no estiguin en ús.
- **Còpies de seguretat:** cal fer còpies de seguretat periòdiques de les dades importants emmagatzemades als dispositius, per a protegir-les en cas de pèrdua, robatori o fallada del dispositiu.
- **Configuració de privadesa:** cal revisar i ajustar la configuració de privadesa dels dispositius i aplicacions per a garantir que la informació personal es protegeix adequadament i s'evita l'accés no autoritzat.
- **Limitació de la informació personal:** cal limitar la informació personal que es comparteix en els dispositius personals, especialment en xarxes socials i aplicacions de missatgeria.
- **Revisió de permisos d'aplicacions:** cal revisar regularment els permisos que s'han concedit a les aplicacions i revocar els que no necessitin accedir a la informació personal.
- **Ús de VPN o d'infraestructura confiança zero (Zero Trust):** cal utilitzar una xarxa privada virtual (VPN) per a xifrar la connexió a Internet i protegir la privadesa en línia, especialment quan la connexió sigui des de fora de la xarxa corporativa.

Conclusions

Aquest document ha mostrat els grans problemes de forma resumida, els grans punts a tenir en compte tant des del punt de vista de ciberatacs com des del punt de vista de privadesa de les dades que s'utilitzen en el dia a dia.

Pel que fa als ciberatacs, el que es troba és que, de forma més o menys activa, un actor maliciós busca fer un ús il·legítim d'un sistema o robar certa informació per a rebre'n algun benefici. S'ha vist que la gran majoria dels atacs se centren en l'enginyeria social o bé s'aprofiten de vulnerabilitats en el programari existent per tal d'apropiar-se de la informació o dels sistemes amb els errors. Com a conseqüència d'aquests atacs, s'ha vist que hi ha grups de cibercrim organitzat, coneguts com APT, que per motius econòmics o polítics realitzen atacs dirigits a víctimes curosament seleccionades. Aquests atacs, avui dia, en una proporció molt elevada són amb programari de segrest, on l'atacant té per objectiu extorsionar la víctima xifrant les dades existents als seus sistemes i amenaçant de publicar-les en el web fosc.

Referent a ciberatacs, s'ha mostrat també, si bé no es pot considerar un atac per si, el sistema Pegasus, un programari de ciberespionatge que es fa servir per a observar grups terroristes, però que ha sigut notícia en els darrers temps pel mal ús que n'han fet certs governs.

Pel que fa a la privadesa de les dades, s'ha pogut observar l'impacte i les implicacions que té compartir dades privades (siguin personals o no) a Internet. S'ha pogut veure quins tipus de dades es tenen segons la seva sensibilitat, i què cal fer per a poder-les emmagatzemar i tractar amb el nivell de privadesa que correspongui. Per tal d'aconseguir això s'han vist també les tecnologies existents actualment per a poder protegir les dades personals.

Complementant això, s'ha estudiat també l'impacte de la privadesa en les etapes del cicle de vida de la informació, on s'ha pogut veure com la privadesa és important en tots els nivells d'emmagatzemament de la informació. El darrer punt important de la privadesa que s'ha estudiat han estat els diferents aspectes de privadesa que afecten la informació. Així, s'ha pogut observar la privadesa des del punt de vista de les dades mateixes, però també considerant els usuaris i la localització de les dades.

Finalment, a mode de sumari, s'han presentat una sèrie de bones pràctiques per a mirar de mitigar al màxim possible la presència de ciberatacs als sistemes, així com el procediment que cal seguir per a garantir que les dades publicades a la xarxa compleixen les garanties de privadesa necessàries.

Consell Assessor del Parlament sobre Ciència i Tecnologia

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Informe de ciberseguretat i privadesa per al Parlament de Catalunya

Autors: Miquel Soriano, René Serral-Gracià
Universitat Politècnica de Catalunya

El Consell Assessor del Parlament sobre Ciència i Tecnologia (CAPCIT) és un òrgan del Parlament creat el 2008 amb l'objectiu de coordinar la informació i l'assessorament en matèria científica i tecnològica que necessitin els diputats i els òrgans del Parlament. El CAPCIT és un òrgan de composició mixta, format pels diputats que en són membres i per representants de les principals institucions científiques i tecnològiques de Catalunya: l'Institut d'Estudis Catalans (IEC), la Fundació Catalana per a la Recerca i la Innovació (FCRI), el Consell Català de la Comunicació Científica (C4), la Reial Acadèmia de Ciències i Arts de Barcelona (RACAB), l'Associació Catalana d'Entitats de Recerca (ACER) i una representació de les universitats públiques i privades. Per a més informació: http://www.parlament.cat/capcit.