UNIVERSITATS

Josep Domingo-Ferrer Director en funcions del Cybercat i director de la càtedra UNESCO de privadesa de dades de la Universitat Rovira i Virgili

"Si vols una conversa segura, queda cara a cara i sense mòbil"

MERCÈ RIBÉ
mribe@lrp.cat

Des del seu despatx al campus de Sescelades de la URV, a Tarragona, Domingo parla del naixement del centre de recerca interuniversitari en seguretat informàtica de Catalunya, el Cybercat, i de la nova llei europea de protecció de dades, ja en vigor.

Què és el Cybercat?
És un centre de recerca en ciberseguretat que agrupa tota l'activitat de recerca que es fa a les universitats catalanes en l'àmbit de la seguretat informàtica i la privadesa de dades. Està integrat per set grups de sis universitats: la URV, la UOC, la UdL, la UPC, la UPF i la UAB. Tot i que el centre neix ara, alguns d'aquests grups ja fa més de vint anys que ens coneixem, col·laborem i treballem junts.

Posi'm algun exemple per saber exactament què fan.
Recerca en seguretat en l'automòbil. Els cotxes han passat a ser ordinadors sobre rodes i cada vehicle porta un centenar de petits ordinadors industrials que també poden patir atacs que cal evitar. A més, en el cas del cotxes tenim uns condicionants que ens ho compliquen: duren més que un ordinador de taula i no t'arriben missatges d'actualitzacions de seguretat cada dos per tres. Un altre camp en què treballem és l'internet de les coses, un àmbit en què és molt important garantir seguretat i privadesa. Parlem de dispositius que no són ben bé ordinadors, com poden ser càmeres de seguretat, sensors, neveres... però que estan connectats per recollir dades. Com que la seva finalitat primària no és informàtica, se'n descuida la seguretat i és més fàcil atacar aquests dispositius. El nostre repte és garantir que tinguin un nivell de seguretat suficient sense que això costi gaires diners.

Ciberatacar una nevera?
La persona que té la nevera potser ni ho sap, perquè l'objectiu és fer servir la potència de càlcul d'aquest dispositiu per fer atacs de denegació de servei contra tercers. L'atac que va rebre la Generalitat el 8-N va ser un atac per denegació de serveis i el seu funcionament és molt simple: un pirata va capturant ordinadors per la xarxa mundial perquè passin a ser els seus zombis. Aquests ordinadors no noten cap efecte especial fins que el pirata decideix

> "La ciberseguretat ja és una de les principals preocupacions de les empreses"

fer-los servir, donant-los una ordre que, en el cas del 8-N, va ser enviar missatges a la Generalitat en massa fins a saturar el servei. I és més fàcil convertir en zombis dispositius senzills com els de les neveres o les càmeres de seguretat que els dels ordinadors.

El context actual del país ha accelerat el projecte del Cybercat?
S'estan creant centres de ciberseguretat arreu del món i totes les universitats una mica grans en tenen. Sorprenentment, a Catalunya no existia res semblant i, o ho fèiem nosaltres ara o era qüestió de temps que ho fes algú altre, perquè és una tendència mundial. A Europa, a més, hi ha la necessitat de defensar-se d'atacs que es reben de fora de la Unió, i ja fa temps que la ciberseguretat és una prioritat. Si ampliem el focus veiem que l'intent de manipulació d'eleccions amb atacs de denegació de serveis, amb notícies falses i manipulacions a les xarxes no és exclusiu d'aquí.

Quines empreses corren més risc de ser atacades?
Les que tenen moltes dades i es gasten pocs diners a protegir-les. El 2013 l'atac contra Yahoo va ser la tempesta perfecta, perquè era una empresa que tenia milions de comptes de correu electrònic, però financerament havia anat malament i no es gastaven diners a protegir-los. Hi ha altres empreses, com entitats sanitàries, que potser no són tan atractives, però que han d'estar molt alerta perquè tenen dades molt confidencials. Els bancs també procuren tenir bons sistemes perquè s'hi juguen molt. De fet, la ciberseguretat és, després de la viabilitat financera i la reputació, la principal preocupació de les empreses.

Com a usuari de mòbil o d'ordinador, com em puc protegir dels ciberatacs?
En el cas de l'ordinador cal tenir antivirus i fer les actualitzacions de seguretat que enviï el fabricant del sistema operatiu. Amb el telèfon mòbil la cosa es complica, perquè passar un antivi-

> "L'aplicació que et descarregues gratis acostuma a fer més coses que les que diu que fa "

rus costa més i, a banda, gran part de la feina la fan les aplicacions que la gent es descarrega. I en general aquestes aplicacions acostumen a fer més coses de les que diuen que fan.

Què vol dir?
Tu vols una aplicació per segui un itinerari, però quan te la descarregues dius que sí a tot i li dones accés a agafar les dades dels teus contactes i enviar-les no sé on. Quan s'instal·la una aplicació la gent ha d'estar segura que realment la necessita i ha de ser una mica crítica amb el que et demanen i renunciar-hi si allò que volen no toca. I sobretot quan són aplis de salut, en què és important saber què fan més enllà de mesurar-te els passos i la tensió. A qui més ho expliquen tot això? Perquè potser no cal que a l'altra punta de món algú sàpiga el teu estat de salut.

L'usuari no n'és conscient, de tot això?
No. I el mòbil és bastant més perillós que un ordinador, perquè té molts sensors i capta moltes coses. Per començar, el portes sempre a sobre i la companyia telefònica pot saber on ets en tot moment. Això, d'entrada, ja és un problema, però en el cas dels mòbils intel·ligents moltes aplicacions tenen accés a la localització i ja són més els que saben on ets en tot moment. No ho tenim present, però pel simple fet de portar el mòbil saben amb qui estàs, quanta estona i cada quan hi

Josep Domingo-Ferrer no té xarxes socials perquè creu que tanta hiperconnectivitat interfereix sobre la capacitat de reflexió, d'abstracció i de repòs intel·lectual de la gent. Ell, en lloc d'amics, col·lecciona títols i reconeixements a la seva trajectòria
JOSEP LOSADA

quedes. Tota aquesta informació de contorn, les metadades, són suficients per posar-te la creu a sobre. No cal saber què es diu en una conversa, no-

> "Cal pensar si allò que estàs escrivint vols que s'associï a la teva persona durant molts anys"

més amb qui es té i quan dura, només amb aquestes metadades n'hi ha prou per matar, deia des de la CIA David Cole. Si ets una persona anònima no passa res, però si resultes incòmode per a algú és molt fàcil controlar-te.

Quina és la manera més segura de comunicar-te?
Punxar una trucada de telèfon és molt fàcil i només cal que ho sol·liciti un jutge o la policia. De fet, amb la tecnologia actual es poden fer punxades massives i ni tan sols cal que hi hagi algú escoltant-les. Fer trucades per WhatsApp és més segur, perquè van xifrades i són més difícils de punxar i, en tot cas, la companyia hauria d'estar disposada a filtrar-les. Però si vols tenir una conversa segura, el més prudent és quedar amb algú cara a cara, sense mòbil o amb la bateria fora.

I missatges de WhatsApp o Telegram?
Són segurs sempre que la companyia no decideixi posar-s'hi pel mig. Els usuaris fan servir unes claus per xifrar la conversa, però aquestes claus les genera el servidor de la companyia i no l'usuari.

Acabem d'estrenar una nova llei europea de protecció de dades. Quins canvis suposa?
Fins ara ens regíem per una directiva del 1996 prèvia al desplegament massiu d'internet que no reflectia moltes de les coses que passaven i tothom feia el que li donava la gana. La nova llei era necessària i la posició que ha adoptat Europa ha estat molt garantista pel que fa a la privadesa de les persones i, com que el mercat europeu és molt gran, tindrà poder d'arrossegament en l'àmbit mundial. Ara per recollir dades cal un consentiment explícit. Fàcil d'entendre i només per un propòsit concret. No es poden demanar més dades de les necessàries i hi ha d'haver transparència i obertura en tot el procés. La llei garanteix el dret a l'oblit i que les teves dades desapareguin o que es guardin en un lloc segur mentre siguin vigents. I només es poden transferir a tercers per fer exploracions de dades si són anònimes.

Regalem les dades sense saber que tenen un preu…
Dones dades i reps uns serveis molt atractius i gratuïts a canvi, com els correus electrònics o les xarxes socials, i sí que hi ha algú reticent com jo que no té xarxes socials ni res, però la majoria està encantada de fer-ho sense percebre'n els problemes. El negoci clàssic d'aquestes empreses és enviar anuncis dirigits de coses que t'interessen i la gent ho troba un preu raonable. El problema ve quan s'hi barreja la política o quan les teves aficions es fan servir per a altres coses en lloc d'enviar anuncis. La decisió de comprar o no un producte només t'afecta a tu, però si el que compres és un programa electoral i el votes, la teva decisió afecta tothom, si guanyen!

> "La majoria de gent està encantada de cedir les dades a canvi d'un servei gratuït i d'anuncis"

No té xarxes socials?
Només una pàgina web, un correu electrònic de la universitat i un telèfon que és la mínima expressió d'un telèfon. No considero que necessiti tanta connectivitat i, per tant, no crec que hagi de cedir dades meves a canvi d'una cosa que jo percebo que no necessito. Hi ha gent que potser està en unes condicions diferents i tenir xarxes socials li suposa mantenir contacte amb gent, però en general ens hauríem de preguntar: necessito tota aquesta connectivitat o més aviat m'enreda, tot això? I jo he arribat a la conclusió que més aviat m'enreda.

Per als que som a les xarxes, quines recomanacions ens fa?
Cal pensar si allò que estàs escrivint vols que s'associï a la teva persona durant anys, perquè és com si ho estiguessis picant en pedra i quedarà visible durant molt temps. Encara que la xarxa social et digui que ho ha esborrat, algú pot tenir la informació que has penjat, les piulades que has fet i els "m'agrada" que has clicat, i tot això es pot girar en contra teu. Tenim recent l'exemple amb el president Torra i les piulades del 2012.