Estils

El malson de l'internet de les coses

Els experts en ciberseguretat alerten dels perills dels objectes connectats i exigeixen a la indústria més protecció

GETTY

NEREIDA CARRILLO
BARCELONA

El televisor intel·ligent, els sensors dels garatges, la polsera que mesura quant es camina, la cafetera connectada, els cotxes intel·ligents, els vigilanadons... Tots aquests aparells poden recórrer el camí que hi ha entre ser màquines útils i convertir-se en soldats obedients d'una mena d'exèrcit robot. Aquest escenari, opina Jordi Serra, professor dels estudis d'informàtica, multimèdia i telecomunicacions de la UOC, "pot passar, no és ciència-ficció". L'internet de les coses pot convertir-se en un malson.

La prova que fets com aquest són possibles la vam tenir en l'atac massiu de finals d'octubre que va fer caure gegants com Twitter, Netflix, Amazon i *The New York Times*, i que va afectar, durant gairebé onze hores, més de mil milions de clients arreu del món. Va ser un atac que, se sospita, es va produir des de dispositius connectats a la xarxa, principalment càmeres de videovigilància. "Estem connectant moltes coses a internet, però no ho estem fent de manera segura –afirma Gonzalo Asensio, director d'IT Security d'Eurecat–. Els ciberdelinqüents ho aprofiten per fer atacs de denegació de servei amb uns trastos que, tots junts, tenen una força molt gran".

Els experts en ciberseguretat estan preocupats per l'internet de les coses, tota mena de dispositius connectats a la xarxa dels quals no s'ha garantit prou la seguretat. Segons càlculs de la consultora Gartner, l'any 2020 s'arribarà a 20.000 milions d'objectes connectats; una xifra que des de Cisco, més optimistes, eleven als 50.000 milions l'any 2020. Mentre aquests sensors i dispositius s'estenen tant entre usuaris i empreses com en la gestió de les ciutats, els experts alerten de les seves vulnerabilitats. Amb xifres com aquestes, el problema no és intranscendent.

Usuaris massa confiats

Malgrat els missatges d'alerta dels experts, l'usuari sovint és poc conscient dels defectes d'aquestes màquines, sobre les quals només sent bondats. Pocs pensen que l'aparell que els ajuda a veure si el seu nadó està dormint plàcidament pot ser interceptat. Segons el baròmetre del 2015 sobre el risc a internet elaborat per ISACA, una entitat internacional que audita els sistemes d'informació, un 64% dels consumidors dels Estats Units asseguren que confien en les dades transmeses per aquests dispositius. Aquesta xifra contrasta amb una altra: el 78% dels professionals enquestats asseguren que els estàndards de seguretat d'aquests aparells són insuficients.

"Qualsevol problema que puguis trobar en un ordinador o telèfon el pots trobar en els objectes connectats", assegura el professor de la UOC. Serra i Asensio diuen que els problemes de seguretat més freqüents en els objectes connectats són que tenen configuracions per defecte en què hi ha un usuari i una contrasenya molt febles, que no s'actualitzen de forma correcta i que no xifren de manera apropiada les dades que emmagatzemen i transmeten. "Si la comunicació no és xifrada o el xifrat que porten no és del tot segur, es pot agafar la informació i generar conseqüències", adverteix el director d'IT Security d'Eurecat. Per la seva banda, el professor de la UOC explica que "els fabricants no tenen la política d'anar actualitzant el sistema, i a mesura que passa el temps apareixen forats de seguretat".

Emergents
El 2020 al món hi haurà 20.000 milions d'objectes connectats

Risc
Els cotxes connectats són especialment vulnerables

Asensio explica que dispositius com ara el televisor, el *router*, els rellotges intel·ligents i els cotxes connectats es poden utilitzar per atacar webs i serveis i també poden ser *hackejats* per accedir fraudulentament a informació personal. En aquest cas, són especialment sensibles els objectes connectats que es van obrint pas en el camp de la salut i la monitorització personal. Però també és possible atacar infraestructures o sensors de les ciutats. "La indústria és la responsable que aquests dispositius siguin segurs i de mantenir-los segurs amb actualitzacions. Però necessita vendre", lamenta Serra, que es queixa que, sovint, les empreses productores d'objectes connectats sacrifiquin la seguretat per augmentar els beneficis.

Bloquejar cotxes connectats

El director d'IT Security d'Eurecat pronostica que els pròxims anys creixeran els atacs als cotxes connectats: "Manipular un sensor d'IoT d'un cotxe connectat pot tenir un impacte molt negatiu per a la seguretat física, però també, en el cas del *ransomware*, et pot deixar el cotxe bloquejat". El *ransomware* és un programari maliciós que infecta l'ordinador i xifra la informació, de manera que els ciberdelinqüents exigeixen a l'usuari que pagui per recuperar les dades.

Malgrat que, segons vaticina Asensio, aviat veurem un increment dels atacs a cotxes connectats, ara mateix els dispositius més vulnerables són les càmeres de videovigilància. "Set de cada deu càmeres connectades a internet no tenen cap tipus de protecció i la resta la tenen feble", alerta Asensio, que afegeix que "molts cops els ciberdelinqüents poden usurpar-ne les imatges".

Al laboratori de ciberseguretat d'Eurecat han fet un simulacre de com serien aquests atacs adreçats als dispositius de l'internet de les coses i en tenen clares les conseqüències. Per això ajuden les empreses a descobrir i prevenir aquestes amenaces. El laboratori, que s'ha posat en marxa enguany, compta amb un equip multidisciplinari integrat per enginyers de telecomunicacions, electrònics, matemàtics i informàtics, tots ells membres de comitès tècnics internacionals que defineixen estàndards en tecnologies clau.

Coresponsabilitat

Els experts avisen que sovint els usuaris no són conscients dels forats de seguretat en els seus televisors intel·ligents, vigilanadons o bombetes connectades a internet, ni tampoc de la informació que queda desprotegida. "Tothom entra en el joc. No hem de pensar que pel fet de ser anònims no serem atacats o coresponsables d'un atac que han fet des de casa nostra amb els nostres dispositius", adverteix Serra.

Com a mesures per combatre els perills de l'internet de les coses, els experts recomanen introduir un usuari i contrasenya nous que siguin difícils de trencar. També aconsellen actualitzar el programari de manera periòdica i no deixar aquests dispositius contínuament connectats a internet si no els estem fent servir. Tanmateix, recalquen que, tot i la prudència dels usuaris, la màxima responsable de garantir la seguretat és la indústria.

"Quan surt una nova tecnologia, si no s'ha pensat en la seguretat des del principi, al final el resultat és negatiu", afirma Asensio. "La seguretat informàtica s'hauria de regular per llei i obligar les empreses a mantenir els sistemes", conclou sobre aquesta problemàtica Serra. Els experts també alerten que cal més conscienciació entre els ciutadans, que sàpiguen què és ciència-ficció i què es pot convertir en realitat.