NOVES AMENACES CIBERNÈTIQUES

La tecnologia domèstica eleva el risc a les xarxes empresarials

Els atacs dels 'hackers' arribaran fins i tot a través dels altaveus intel·ligents

EDUARDO LÓPEZ ALONSO
BARCELONA

La incorporació creixent de les xarxes domèstiques a l'escenari del teletreball obre les empreses a riscos de seguretat informàtica cada vegada més grans. Els experts entreveuen noves amenaces per al 2019 que se sumen a les que ja implica incorporar a la xarxa empresarial els accessoris tecnològics personals (el denominat BYOD o *bring your own device*), i que ha suposat tradicionalment el principal focus d'atacs a les xarxes informàtiques de les empreses en els últims anys.

Internet, les xarxes socials i els dispositius domèstics connectats *online* han multiplicat les vulnerabilitats a les empreses i han donat lloc a una ciberinseguretat creixent. Els empleats tenen en el seu poder l'accés més vulnerable a les xarxes empresarials. Aquesta és alguna de les conclusions de les principals consultores de seguretat, que reconeixen que qualsevol avançament tecnològic augmenta encara més el negoci vinculat a la ciberseguretat.

AFP / GRANT HINDSLEY

►►Dave Limp, vicepresident de dispositius d'Amazon, amb el nou altaveu Echo Dot, a Seattle, al setembre.

Investigadors de Trend Micro ja han demostrat com els altaveus intel·ligents, l'Alexa d'Amazon n'és un exemple, poden filtrar dades personals. Segons aquesta consultora, alguns atacs el 2019 es dirigiran contra aquests altaveus intel·ligents o altres artefactes connectats a la xarxa per accedir a les entranyes empresarials a través de les domotizacions domèstiques dels empleats.

L'augment dels acords de teletreball ja dispara les amenaces, al desafiar amb moviments de dades empresarials des d'aplicacions basades en el núvol i *software* col·laboratiu la integritat de l'anteriorment xarxa tancada empresarial típica. «El paper de l'enginyeria social en l'èxit dels atacs contra les empreses i els individus continuarà augmentant al llarg del pròxim any», asseguren els experts de Trend Micro en el seu últim informe (*Mapping the future*). Aquesta companyia afirma que el nombre d'atacs de *phishing* (suplantació d'identitat) bloquejats per la companyia ha augmentat el 3.800% des del 2015. Paral·lelament, els ciberdelinqüents ja no utilitzen programes semiautomatitzats per accedir a xarxes empresarials. L'ús del kit d'*exploits* ha caigut el 98% des del 2015. És el torn de l'enginyeria social i l'engany a través de *links* en el correu electrònic.

EN EL TOP 3 // Segons Kaspersky, Espanya es va situar en el top 3 de països atacats per *phishing* en el tercer trimestre d'aquest any. El nombre de casos neutralitzats per aquesta firma va arribar als 137 milions d'atacs, un 27,5% més que fa un any. Un terç de tots aquests intents registrats per aquesta companyia de ciberseguretat es van dirigir contra entitats financeres. La base d'aquesta típica estafa cibernètica és l'obtenció de claus mitjançant la suplantació d'identitat (per un correu electrònic fals, per exemple, o per l'ús d'una xarxa wifi pública sense utilitzar solucions VPN de trànsit xifrat). Segons Karspersky, un de cada tres ordinadors (el 30,01%) es va enfrontar a una amenaça *online* durant aquest 2018. D'aquestes, destaquen els atacs de *ramsonware* (també conegut com a *rogueware* o *scareware*), que restringeix l'accés a l'ordinador i exigeix el pagament d'un rescat per eliminar la restricció. Els atacs més perillosos els han causat WannaCry, Petya, Cerber, Cryptolocker i Locky. Aquest tipus d'atacs han augmentat més d'un 40% en un any, segons Kaspersky.

Els experts anuncien un 2019 ple d'amenaces a l'entorn del nostre correu electrònic. Les bases de dades de Check Point ja han detectat la barbaritat d'11 milions de *malewares* i més de 5,5 milions de llocs web infectats. I el fenomen segueix en creixement exponencial. ≡

Programes maliciosos al núvol per a la generació de criptomonedes

►► La utilització creixent d'aplicacions al núvol ha elevat les vulnerabilitats. «Les febles mesures de seguretat del núvol permetran una explotació més gran dels comptes per a la mineria de monedes», expliquen a Trend Micro. Segons Check Point, els tres *malewares* amb més incidències a Espanya són actualment Coinhive, Roughted i XMrig. El primer és un programa que s'introdueix a l'ordinador de l'usuari i es dedica a minar l'equip o a generar la criptomoneda Minero. «Ja ha afectat el 25% de les empreses espanyoles», asseguren els experts de Check Point.