Els telèfons intel·ligents, espies a sou dels Estats Units

L'Agència de Seguretat Nacional (NSA) dels Estats Units no ha deixat escapar el 'boom' dels telèfons intel·ligents, i ha desenvolupat la capacitat d'introduir-se en iPhone, dispositius Android i fins i tot dins de BlackBerry, un dispositiu que es creia que era especialment segur.

Michael Hayden, antic director de l'NSA, explica una història interessant sobre els iPhone. Segons va comentar recentment en una conferència a Washington, ell i la seva dona eren en una botiga d'Apple a Virgínia quan un venedor se'ls va acostar i, entusiasmat, els va començar a parlar de l'iPhone i de les "400.000 aplicacions" que ja existien per al dispositiu. Hayden, divertit, es va girar cap a la seva dona i li va dir en veu baixa: "Aquest noi no deu saber qui sóc, oi? 400.000 aplicacions són 400.000 possibilitats d'atac".

Sembla que Hayden només exagerava una mica. D'acord amb documents interns de l'NSA procedents dels arxius d'Edward Snowden als quals *Der Spiegel* ha tingut accés, el servei d'intel·ligència dels EUA no sols ha intervingut ambaixades i ha accedit a les dades de cables submarins de telecomunicacions per obtenir informació. L'NSA també està molt interessada en una nova forma de comunicació que ha tingut un èxit espectacular els darrers anys: els telèfons intel·ligents.

A Alemanya, més de la meitat de tots els usuaris de telèfons mòbils tenen telèfons intel·ligents; al Regne Unit en tenen dues terceres parts dels usuaris de telèfons mòbils. Als EUA, uns 130 milions de persones ja fan servir aquests dispositius. Els miniordinadors s'han convertit en centres de comunicació, assistents digitals i ajudants personals, i sovint saben més sobre els seus usuaris que la majoria d'ells no sospiten.

Per a una agència com l'NSA, les unitats d'emmagatzematge de dades són una mina d'or. En un sol dispositiu es combina gairebé tota la informació que pot interessar a una agència d'intel·ligència, és a dir, els contactes socials, detalls sobre els hàbits i la ubicació de l'usuari, els seus interessos (a través dels termes de cerca que fa servir, per exemple), fotos i, de vegades, fins i tot números de targetes de crèdit i contrasenyes.

Nous canals. Els telèfons intel·ligents, en poques paraules, són una innovació tècnica fantàstica, però també una oportunitat excel·lent per a espiar la gent. Aquests dispositius obren les portes d'allà on fins i tot una organització tan poderosa com l'NSA encara no podia entrar.

Des del punt de vista dels experts en informàtica de la seu de l'NSA a Fort Meade, a Maryland, l'èxit colossal dels telèfons intel·ligents plantejava un gran desafiament. Es van obrir tants nous canals que semblava que els arbres no deixarien veure el bosc als agents de l'NSA.

Segons un informe intern de l'NSA del 2010, "explorant les tendències, els objectius i les tècniques actuals", la propagació dels telèfons intel·ligents es produïa "molt ràpidament", uns fets que "sens dubte compliquen l'anàlisi tradicional dels objectius".

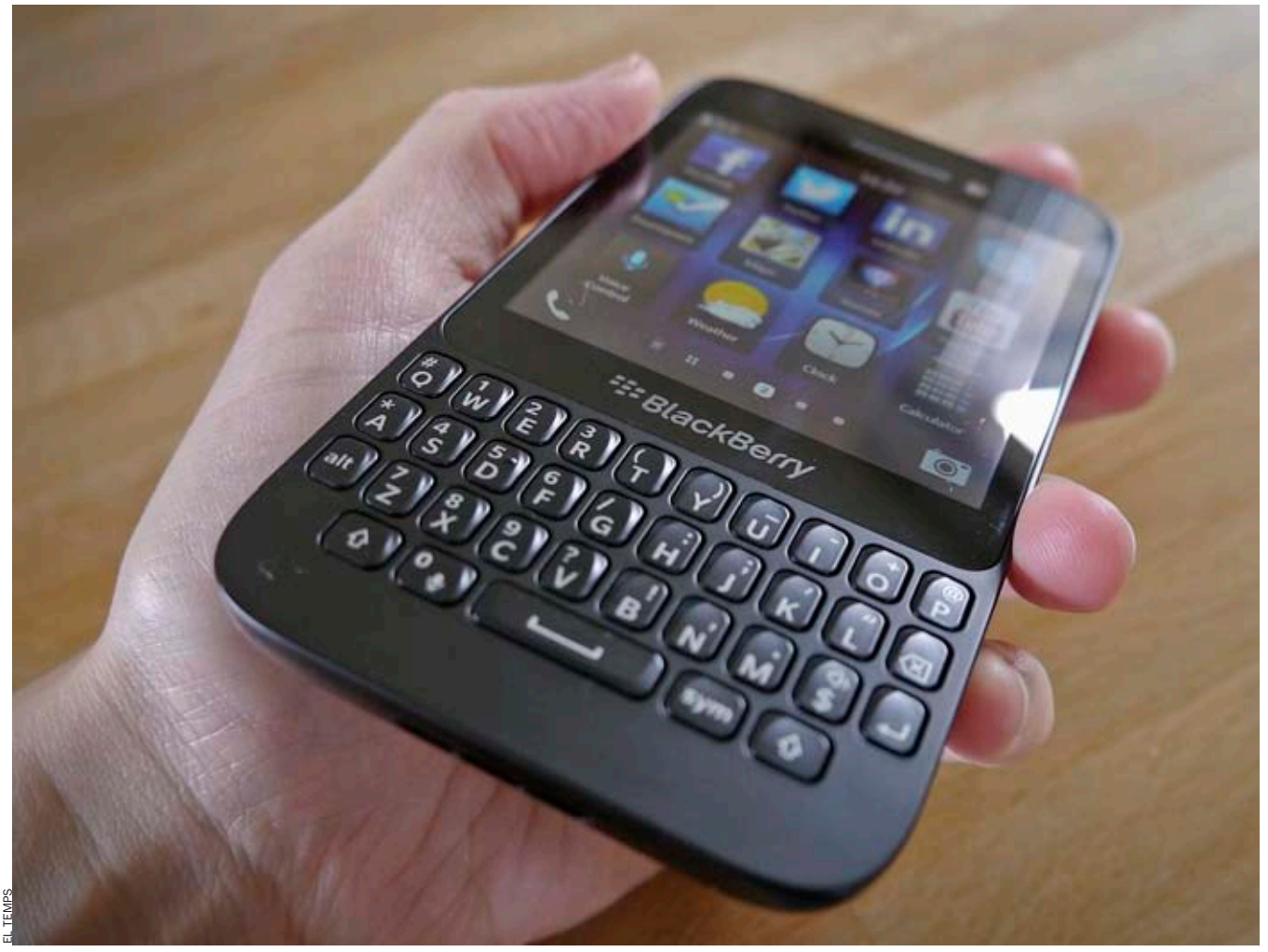
L'NSA va abordar aquest tema amb la mateixa velocitat amb què els dispositius fan canviar els hàbits dels usuaris. Segons els documents, l'agència va establir grups de treball per als principals fabricants de telèfons intel·ligents i sistemes operatius. Equips especialitzats van començar a estudiar intensament l'iPhone d'Apple i el seu sistema operatiu iOS, així com el sistema operatiu Android de Google. Un altre equip va estudiar les maneres d'atacar BlackBerry, que fins aleshores s'havia considerat una fortalesa inexpugnable.

Als documents no hi ha indicis d'espionatge a gran escala sobre els usuaris de telèfons intel·ligents, però no obstant això, mostren clarament que si el servei d'intel·ligència defineix un *smartphone* com a objectiu, trobarà la manera d'accedir a la informació que conté.

Igualment, és un tema molt delicat que l'NSA tingui com a objectiu dispositius fabricats per empreses nordamericanes, com és el cas d'Apple i Google. El cas de BlackBerry no és menys sensible, perquè la seu de l'empresa és al Canadà, un dels països socis de l'aliança "Five Eyes" de l'NSA. Els membres d'aquest grup selecte s'han compromès a no participar en cap activitat d'espionatge contra els altres membres.

Treure profit de la "nomofòbia". De totes maneres, sembla que en aquests casos la política del no-espionatge no s'aplica. Als documents relacionats amb els telèfons intel·ligents que *Der Spiegel* va poder veure no hi ha indicis que les empreses cooperessin voluntàriament amb l'NSA.

Quan *Der Spiegel* s'hi va posar en contacte, responsables de BlackBerry van explicar que la feina de l'empresa no és fer comentaris sobre la suposada



EL TEMPS

Els telèfons intel·ligents són una innovació tècnica fantàstica, però també una oportunitat excel·lent per a espiar la gent.

vigilància dels governs. “Els nostres principis i les nostres declaracions públiques han deixat clar que no hi ha cap mena de *porta del darrere* per accedir a la nostra plataforma”, explicava la companyia en un comunicat. Google va emetre un comunicat que deia: “No coneixem grups de treball d’aquesta mena i no concedim a cap govern l’accés als nostres sistemes”. L’NSA no havia respost a les preguntes de *Der Spiegel* en el moment d’imprimir de la revista.

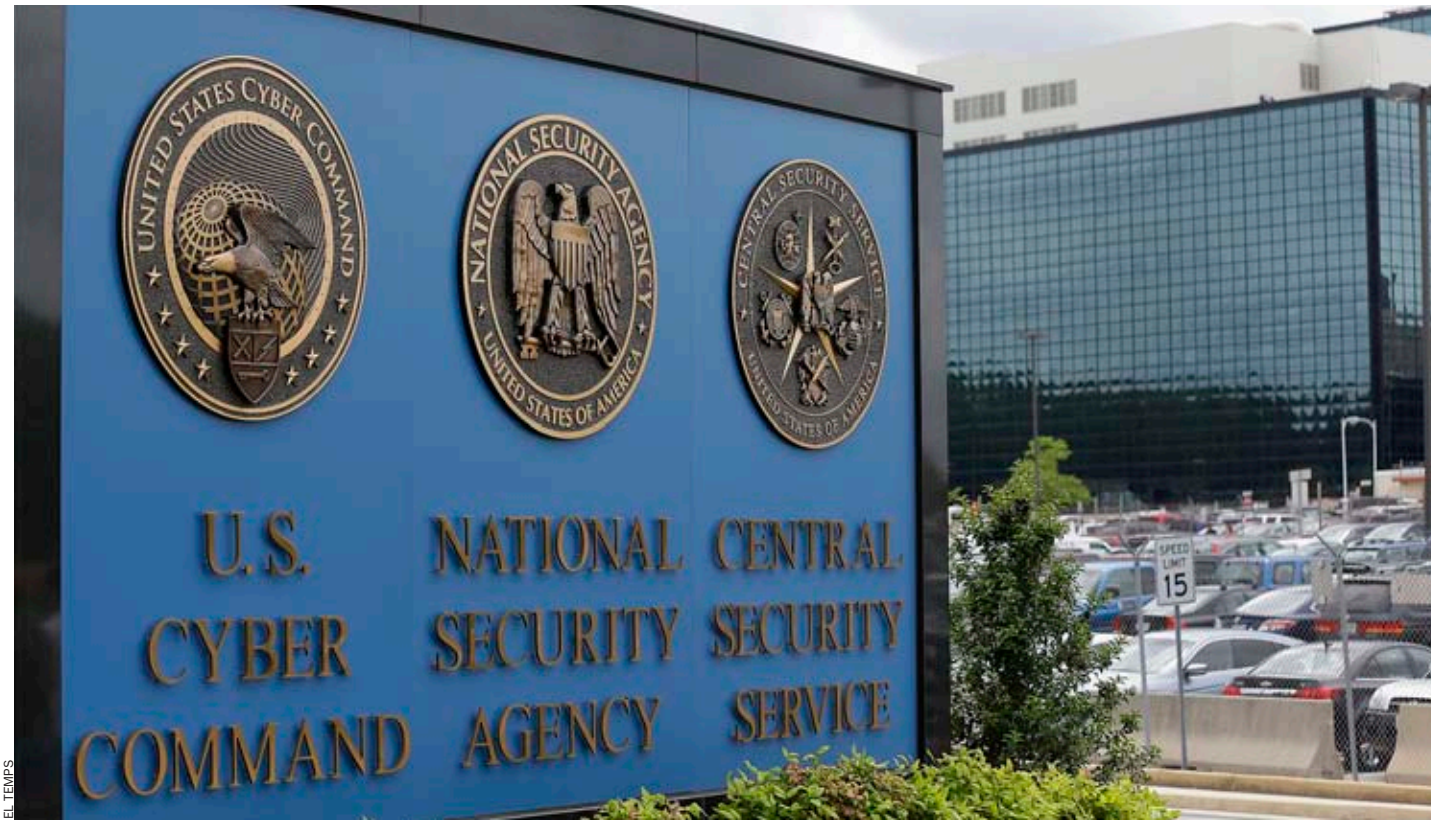
A l’hora d’obtenir informació dels telèfons intel·ligents, l’agència aprofita la despreocupació amb què molts usuaris tracten aquests dispositius. D’acord amb un arxiu de l’NSA, els usuaris de telèfons intel·ligents pateixen una mena de *nomofòbia*, és a dir, por de sortir de casa sense el telèfon mòbil. A molts usuaris, l’única cosa que els preocupa és no tenir cobertura. Una presentació detallada de l’NSA, “El vostre objectiu té un telèfon intel·ligent?”, demostra com d’extensius són actualment els mètodes de vigilància contra els usuaris del popular iPhone d’Apple.

En tres transparències consecutives, els autors de la presentació estableixen una comparació amb “1984”, la clàssica novel·la de George Orwell sobre un estat de vigilància, un fet que posa de manifest la visió que té l’agència dels telèfons intel·ligents i dels seus usuaris. “Qui hauria dit el 1984 que aquest seria el Gran Germà?”, es demanen els autors en referència a una foto del cofundador d’Apple, Steve Jobs. I pel que fa a fotos de clients entusiastes d’Apple i usuaris d’iPhone, l’NSA escriu: “...i que els zombies serien clients?”.

Si fem cas dels documents de l’agència, l’NSA pot seleccionar una àmplia gamma de dades dels usuaris del producte més lucratiu d’Apple segons quins objectius persegueixi.

A partir dels exemples que s’inclouen als documents de l’agència, es pot apreciar que els resultats són impressionants. Inclouen, per exemple, la imatge del fill d’un antic secretari de Defensa abraçant una noia, una foto que va fer amb el seu iPhone. Una sèrie d’imatges mostra homes i dones joves a zones de conflicte, com ara un home armat a les muntanyes de l’Afganistan, un afganès amb amics i un sospitós a Tailàndia.

El potencial de l’iPhone. Totes aquestes imatges es van fer, aparentment, amb telèfons intel·ligents. Una foto del gener de 2012 és especialment pujada de to: s’hi veu un antic alt funcionari del govern d’un país estranger que, d’acord amb l’NSA, es relaxa al sofà davant d’un televisor i es fa fotos a si mateix... amb el seu iPhone. Per protegir la seva privacitat, *Der Spiegel* ha decidit no revelar-ne el nom o d’altres detalls.



EL TEMPS

La gran propagació dels telèfons intel·ligents va fer que l'NSA, segons els documents, creara grups de treball per a estudiar els principals fabricants

L'accés a aquest tipus de materials varia, però una gran part passa a través d'un departament de l'NSA que s'encarrega d'operacions de vigilància a objectius de màxim interès. Una de les eines que els agents dels Estats Units fan servir són els fitxers de còpia de seguretat establerts pels telèfons intel·ligents. Segons un document de l'NSA, aquests fitxers contenen el tipus d'informació que interessa als analistes, com ara llistes de contactes, registres de trucades i esborranys de missatges de text. Per a accedir a aquest tipus de dades, els analistes ni tan sols han de tenir accés a l'iPhone mateix, segons indica el document. Només cal que el departament accedeixi a l'ordinador de l'objectiu, amb el qual el telèfon intel·ligent ha estat sincronitzat prèviament. Sota el títol "Potencial de l'iPhone", els especialistes de l'NSA enumeren els diferents tipus de dades que es poden analitzar en aquests casos. El document assenyala que hi ha petits programes de l'NSA, *scripts*, que poden encarregar-se de la vigilància en 38 funcions diferents dels sistemes operatius de l'iPhone 3 i 4. Entre d'altres, s'hi inclouen la funció de mapatge, el correu de veu i fotos, així com les aplicacions de Google Earth, Facebook i Yahoo Messenger.

Els analistes de l'NSA són especialment optimistes amb les dades de geolocalització emmagatzemades als telèfons intel·ligents i a moltes de les seves aplicacions, dades que els permeten determinar on era un usuari en un moment donat.

D'acord amb una presentació, fins i tot era possible rastrejar la ubicació d'una persona durant períodes de temps molt extensos, fins que Apple va eliminar aquest *error* amb la versió 4.3.3 del seu sistema operatiu mòbil i en va restringir la memòria fins a set dies.

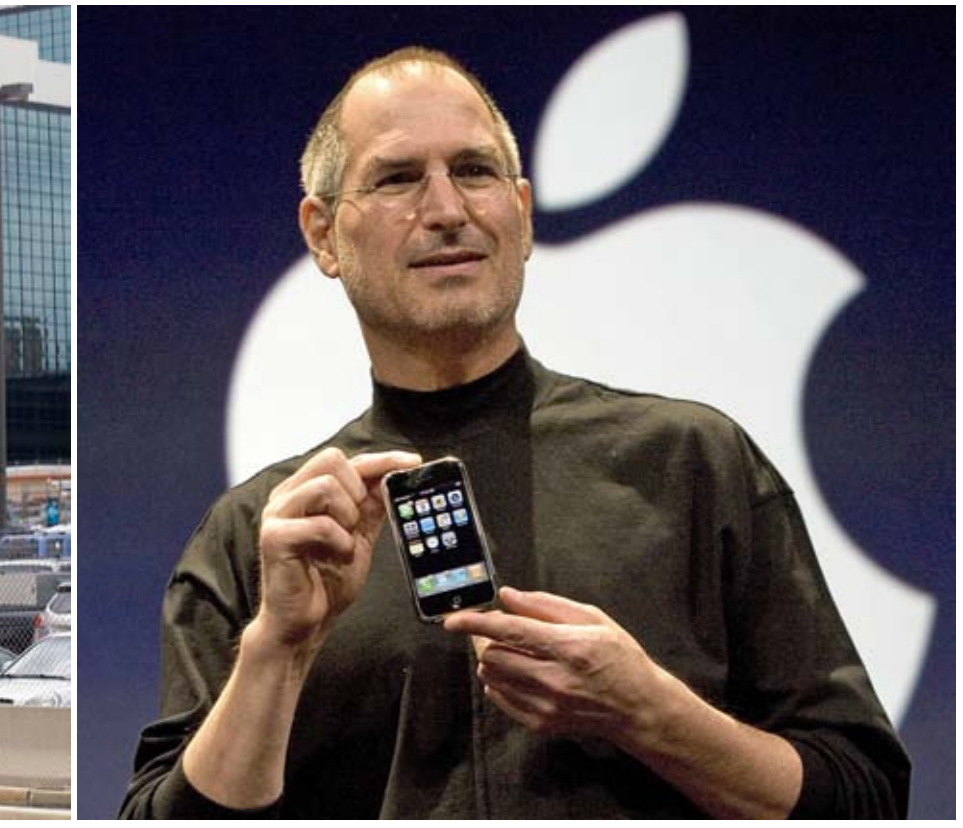
Però, de totes maneres, els "serveis d'ubicació" que fan servir moltes de les aplicacions de l'iPhone, des de la càmera fins als mapes passant per Facebook, són útils per a l'NSA. Als documents d'intel·ligència dels Estats Units, els analistes assenyalen que la "comoditat" dels usuaris garanteix que molt probablement donaran el seu consentiment quan les aplicacions els preguntin si poden utilitzar la seva ubicació actual.

Desxifrar la Blackberry. L'NSA i la seva sòcia, l'agència britànica GCHQ, es van centrar amb una intensitat similar en una altra joguina electrònica: la BlackBerry.

Això és especialment interessant, perquè aquest producte canadenc es dedica a un sector molt específic: les empreses que compren els dispositius als seus empleats. De fet, aquest aparell, que té un petit teclat, sembla més una eina per a fer gestions que l'eina que presumptes terroristes farien servir per a decidir possibles atacs.

L'NSA també comparteix aquest punt de vista, tenint en compte, a més a més, que en fòrums extremistes s'utilitzen sobretot dispositius de Nokia, amb Apple en tercer lloc i BlackBerry en una distant novena posició.

Segons diversos documents, l'NSA va passar anys provant de desxifrar les comunicacions de BlackBerry, que té un grau de protecció elevat, i manté un "Grup de Treball BlackBerry" que es dedica específicament a aquesta tasca. Però el ràpid desenvolupament de la indústria ha mantingut els especialistes assignats al grup en estat d'alerta, com revela un document de GCHQ, "Secret UK".



d'aquests telèfons i sistemes operatius. A la dreta, Steve Jobs, cofundador d'Apple.

Segons aquest document, als mesos de maig i juny de 2009 van aparèixer problemes amb el processament de dades de BlackBerry, uns problemes que els agents atribueixen a un mètode de compressió de dades nou recentment introduit pel fabricant.

Al juliol i a l'agost, l'equip de GCHQ assignat al cas va descobrir que BlackBerry havia absorbit una empresa més petita. Al mateix temps, l'agència d'intel·ligència havia començat a estudiar el nou codi de BlackBerry. Segons un document intern, al març de 2010 finalment es va resoldre el problema. "Xampany!", es van dir els analistes, fent-se copets a l'esquena.

Preocupacions sobre la seguretat. Els documents interns indiquen que aquest no va ser l'únic èxit contra Blackberry, una empresa que comercialitza els seus dispositius dient que són a prova de vigilància i que recentment ha perdut una quota de mercat substancial a causa d'errors estratègics, tal com l'NSA apunta amb interès. Un dels documents interns, en una secció anomenada "Tendències", indica que el percentatge d'empleats del govern dels Estats Units que utilitzen els dispositius BlackBerry va passar d'un 77 per cent a menys del 50 per cent entre agost de 2009 i maig de 2012.

L'NSA conclou que els dispositius ordinaris reemplacen cada vegada més l'únic telèfon intel·ligent certificat pel govern americà, un fet que fa que els analistes expressin les seves preocupacions sobre la seguretat. Pel que sembla, consideren que ells són els únics agents de tot el món que poden accedir a les dades de BlackBerry.

Ja el 2009, els especialistes de l'NSA assenyalaven que podien "veure i llegir" els missatges de text enviats des de dispositius BlackBerry, i que també podien "emmagatzemar i processar correus BIS". Les sigles BIS corresponen als serveis d'Internet de BlackBerry, que operen fora de les xarxes corporatives, i que, en contrast amb les dades que passen a través dels serveis interns de BlackBerry (BES), només comprimeixen però no encripten les dades.

Però fins i tot aquest nivell de seguretat tan elevat no és immune a l'accés de l'NSA, si més no segons una presentació titulada: "El vostre objectiu fa servir una BlackBerry? I ara què?". Aquesta presentació assenyala que l'adquisició de comunicacions BES encriptades requereix una operació "prolongada" per part del departament d'Operacions d'Accés Adaptat de l'NSA per tal de "perseguir plenament l'objectiu". Un correu electrònic d'una agència del govern mexicà, que s'inclou a la presentació sota el títol "Col·lecció BES", demostra que, a la pràctica, tot això s'aplica amb èxit.

Confiar en BlackBerry. Els documents del juny de 2012 indiquen que l'NSA va poder ampliar el seu arsenal contra BlackBerry. Ara també enumera la telefonia de veu entre les seves "capacitats actuals", és a dir, els dos estàndards de telefonia mòbil habituals a Europa i els Estats Units, "GSM" i "CDMA."

Però el grup intern d'experts que s'havia reunit en una "taula rodona sobre BlackBerry", encara no estava satisfet. Segons els documents, també s'hi van discutir quines "millores addicionals caldria incorporar" pel que fa a BlackBerry.

Encara que els materials als quals va tenir accés *Der Spiegel* suggereixen l'ús específic d'aquestes opcions de vigilància de l'NSA, les empreses involucrades no es mostren gaire afectades.

BlackBerry flaqueja i actualment està oberta a ofertes públiques d'adquisició. La seguretat continua sent un dels seus principals punts forts de venda en els models més recents, com ara el Q10. Però si ara es demostra que l'NSA és capaç d'espiar de manera específica els dispositius de BlackBerry i d'Apple, les conseqüències podrien ser de llarg abast.

Aquestes conseqüències s'estenen fins al govern alemany. No fa gaire, el govern de Berlín va convocar un concurs per a l'adjudicació d'un important contracte per a establir comunicacions mòbils segures dins de les agències federals. En va sortir guanyador BlackBerry.

Marcel Rosenbach
Laura Poitras
Holger Stark
© Der Spiegel
Traducció de Paula Arnas Antolín