



e-penteo

Seguretat en smartphones i dispositius mòbils

Noemí Batista Maymús, Analista Associada. Penteo.

L'empresa d'avui és mòbil, i seguint aquest precepte, les companyies s'han omplert d'infininitat de dispositius que faciliten la mobilitat dels seus treballadors, de les dades i dels sistemes d'informació. Primer van ser els ordinadors portàtils, però a poc a poc, l'entorn mòbil s'ha anat diversificant i han aparegut nous terminals adaptats a les necessitats dels usuaris, que fins al moment, no eren objectiu prioritari de ciberatacs. Però la penetració i l'ús de telèfons intel·ligents ha crescut enormement en l'últim any, i aquesta massa crítica d'usuaris segurament despertarà l'interès dels atacants.

Malgrat que la indústria porta temps parlant de la seguretat en els dispositius mòbils, fins ara el nombre relativament baix d'usuaris feia molt més interessant seguir centrat en atacs a PCs. Aquesta tendència segurament anirà canviant durant el 2011, i el DTIC haurà de fer més atenció a les condicions de seguretat de tots els dispositius mòbils que tenen accés als sistemes d'informació de l'empresa, o que poden ser utilitzats per l'usuari per guardar documentació confidencial. Hem d'estar atents, sobretot, als *smartphones* i les seves creixents funcionalitats i a la tènue frontera que separa el personal del professional.

El gran creixement dels telèfons intel·ligents, liderats inicialment per la BlackBerry de RIM, en l'entorn empresarial, i seguits de l'auge d'altres sistemes operatius com Android, diversifiquen de manera notable els terminals des dels quals s'accedeix a les dades i sistemes informàtics de les nostres empreses. I és que el creixement dels *smartphones* ha estat espectacular en l'últim any, i s'han sumat de manera decidida a altres dispositius mòbils com PDAs, tablets o portàtils. Les dades de Nielsen indiquen que en el primer quadrimestre de 2010 un 23% dels usuaris de telèfons mòbils

utilitzava un *smartphone* i s'espera que en 2011 els telèfons intel·ligents superin als telèfons tradicionals. Canals ha publicat les últimes dades de venda de *smartphones* a nivell mundial, i les xifres indiquen que l'últim quadrimestre de 2010 es van vendre 100 milions d'unitats, amb un creixement de gairebé el 90% respecte al mateix període de l'any anterior, arribant gairebé als 300 milions d'unitats venudes. Aquest enlairament, a més, s'ha produït tant a nivell empresarial com d'usuari, i els telèfons intel·ligents formen ja part del dia a dia en tots els àmbits.

Alguns riscos en dispositius mòbils

No cal oblidar que els dispositius mòbils presenten riscos addicionals que s'afegeixen als riscos tradicionals de qualsevol dispositiu connectat al sistema d'informació. En utilitzar-se en condicions de mobilitat, i en diversitat d'ambients, són més susceptibles de robatori o pèrdua. A més, les seves alternatives de connectivitat, en ocasions a través de xarxes wi-fi obertes, o de Bluetooth, poden facilitar l'accés no autoritzat al dispositiu.

La combinació de funcionalitats i aplicacions que utilitzen els usuaris pot comportar també que s'estigui oferint informació sense ser conscient d'això. La geolocalització del dispositiu, i per tant de l'usuari, és un clar exemple, que pot facilitar informació d'interès per a potencials atacants sense que l'usuari se n'adoni.

La reutilització o reciclatge dels dispositius, així mateix, sense els procediments de seguretat adequats, facilita la fugida d'informació, especialment dades que permeten identificar als seus usuaris, que sovint s'emmagatzemen en el propi dispositiu.

Altres atacs com el *phishing* poden ser més perillosos en dispositius mòbils, atès que la grandària de la pantalla pot dificultar la lectura de les URLs o la procedència dels missatges, així com la instal·lació de *spyware*, donada la tendència dels usuaris a instal·lar aplicacions.

Smartphones, en el punt de mira

Cisco destaca en el seu informe anual sobre seguretat (Cisco 2010 Annual Security Report) la creixent tendència a atacar dispositius mòbils, especialment *smartphones*. Altres proveïdors de seguretat, com McAfee, consideren també que 2011 serà un any d'inflexió en l'atac a dispositius mòbils, quan per fi es materialitzaran els atacs d'una manera generalitzada. I ofereixen solucions en aquest sentit, que convé avaluar per garantir en els *smartphones* les mateixes condicions de seguretat que apliquem a la resta de dispositius

Si bé és cert que el sistema operatiu dels dispositius mòbils i telèfons intel·ligents està diversificat, la qual cosa dificulta la dispersió generalitzada d'atacs, com per exemple virus, el nombre d'usuaris actuals constitueixen ja una massa crítica que ha començat a atreure l'atenció dels delinqüents. La diversitat al software i al hardware fa més difícil un atac massiu, però aquesta mateixa diversitat dificulta també l'estandardització de mesures de seguretat, i torna els ulls dels atacants cap a plataformes que sí són transversals als dispositius com Java EM.

Usuaris, el punt feble

Però els *smartphones*, vulguem o no, no només s'utilitzen per treballar. A les funcionalitats creixents que tenen aquests dispositius l'àmbit laboral (agenda, gestió de contactes, correu electrònic, connexió

al CRM, etc.), s'afegeix el factor que la seva percepció com a eina de treball no està tan clara com el cas d'un ordinador portàtil. Són molts els empleats que porten el seu *smartphone* sempre damunt, fins i tot en caps de setmana o períodes vacacionals, per la qual cosa ens trobem amb certa dificultat per separar de manera taxativa el professional del personal.

Un estudi recent de Nokia indica que a Espanya un 68% dels usuaris de *smartphones* porta fins a 30 aplicacions en el seu mòbil. I el 47% creuen que les aplicacions milloren les seves vides: en la llar (44%), durant viatges (19%) o en el treball (11%). La instal·lació d'aplicacions de xarxes socials i jocs encapçalen la llista, però fins a un 19% dels usuaris instal·la aplicacions empresarials. Hi ha doncs una coexistència entre les utilitats laborals i els aspectes lúdics i personals en un mateix dispositiu, on sovint s'emmagatzema correus electrònics, documents confidencials o dades de contacte de clients. I sovint els usuaris no són conscients dels riscos que això pot suposa.

Recomanacions de seguretat en dispositius mòbils

Malgrat els riscos que suposen els dispositius mòbils, i de l'actitud inconscient que sovint tenen els usuaris, no sempre hi ha polítiques de seguretat clarament definides. I quan n'hi ha, els usuaris se les salten més habitualment que en els entorns tradicionals. El DTIC, sovint poc inclinat a incorporar diversitat de dispositius i a permetre la seva connexió als sistemes d'informació empresarials, ha acceptat aquesta creixent complexitat, però això no sempre s'ha traduït en l'elaboració i implementació de mesures de seguretat intenses. A més, la reducció de vida dels dispositius, molt especialment els *smartphones*, dificulta encara més les labors de protecció i d'homogeneïtzació de mesures. Si fa un parell d'anys la seva vida mitjana al mercat era d'uns tres anys, avui s'estima que està com a màxim en 9 mesos.

Malgrat tot, tant la seguretat com la mobilitat preocupen a les empreses. Les dades de Penteo ICT Spending 2011 posen de manifest que seguretat i mobilitat són les dues partides d'infraestructura on més empreses concentraran les seves inversions en 2011. Més d'un 64% dels CIOs consideren que en 2011 augmentaran les seves inversions en seguretat, mentre que gairebé un 57% farà el propi amb infraestructures de mobilitat.

Els proveïdors, per la seva banda, ofereixen també productes adaptats a aquestes necessitats, com antivirus per a dispositius mòbils, sistemes de gestió segura de terminals diferents, o programari d'encryptació. L'esforç dels proveïdors per oferir solucions de seguretat mòbil ha augmentat, al mateix temps que els riscos, i caldrà estar atents a les versions i nous productes que es van presentar la setmana passada al Mobile World Congress 2011 de Barcelona.

L'European Network and Information Security Agency (ENISA), organisme de la Unió Europea, ha publicat un informe on recull les principals amenaces a la seguretat, especialment orientat als *smartphones*, així com recomanacions per combatre-les. Entre aquestes es troben consells que poden semblar obvis, però que no sempre s'apliquen als *smartphones*, com configurar el bloqueig automàtic del dispositiu, la realització periòdica de *backups* o l'encryptació de la informació emmagatzemada en la memòria (a més de minimitzar les dades que es guarden localment en el dispositiu). Altres recomanacions que destaquen des de la UE són:

- _ Revisar les configuracions de privacitat de sèrie.
- _ Inspeccionar els permisos en instal·lar aplicacions. Això inclou comprovar la reputació de les aplicacions i dels llocs dels quals es descarreguen. En els casos en els quals es pugui gestionar

informació especialment sensible, és convenient a més configurar els dispositius perquè sigui necessària una contrasenya en cas de voler instal·lar aplicacions. O incloure un llistat que limiti les aplicacions que poden ser instal·lades.

_ Cautela en l'ús d'*hotspots* públics, i especialment, deshabilitar la possibilitat que el dispositiu es connecti de manera automàtica. Utilitzar només els punts fiables per a activitats més conflictives (per exemple, banca electrònica, e-commerce o fins i tot correu electrònic). Per a això convé configurar correctament el dispositiu, però també educar els usuaris sobre pràctiques inadequades.

_ Establir procediments per al reciclatge de dispositius o el seu desfet, que inclogui la neteja de memòria i qualsevol dada emmagatzemada.

_ Encriptació de la informació. Existeixen al mercat diverses solucions que faciliten l'encriptació de les dades, garantint la seva seguretat en cas de pèrdua del dispositiu. McAfee Endpoint Encryption o Check Point Full Disk Encryption són algunes de les alternatives més complertes per a terminals mòbils, encara que existeixen un gran nombre i varietat de solucions, que s'integren amb altres utilitats, com a gestió de dispositius, antivirus, etc.

Conclusions

La ràpida extensió dels telèfons intel·ligents estén a aquesta nova plataforma els problemes de seguretat fins a avui eren més propis dels ordinadors. Si bé la diversitat de sistemes operatius presents en els diferents models dificulta els atacs globals que trobem en els àmbits tradicionals, la veritat és que també fa més complex el desenvolupament de sistemes de seguretat. A més, estem davant d'un nou tipus d'eina que trenca definitivament la barrera entre el món professional i el privat, incrementant els problemes de seguretat associats a la transmissió de la informació.

I malgrat la importància que per a les empreses té la seguretat i la mobilitat (incrementaran el seu pressupost en aquestes àrees en 2011), les polítiques de seguretat sovint no estan a l'altura, i l'actitud dels usuaris dificulta encara més la presa de mesures. Al mercat hi ha eines disponibles que poden ajudar notablement a millorar la seguretat dels dispositius mòbils, com antivirus o sistemes d'informació, però és també imprescindible l'establiment de política per part del DTIC, així com la conscienciació i col·laboració per part dels propis usuaris.

Noemí Batista Maymús és doctorada en comunicació per la Universitat de Navarra, on ha impartit classes de tecnologies de la informació. La seva experiència professional i com a investigadora inclou estades de recerca en diferents universitats dels EUA (Columbia, Northwestern i Berkeley), i comprèn més de deu anys centrats en el coneixement sobre aspectes crítics per a les TIC i el negoci. Actualment és analista associada a Penteo.

Penteo

Madrid
Velázquez 114
28006 Madrid

Barcelona
Córcega 282
08008 Barcelona

T.: +34 902 154 550
www.penteo.com