Els dispositius mòbils

Existeixen molts tipus de dispositius mòbils. Fins fa poc, en les universitats s'utilitzaven els **ordinadors portàtils**, però actualment, gairebé la totalitat dels treballadors utilitzen **telèfons intel·ligents**, sigui per l'ús personal o corporatiu, i també existeix una tendència creixent en l'ús de **tauletes**.

Els riscs més habituals dels dispositius mòbils són la pèrdua, el robatori i el trencament, destrucció i avaria. tot i que en molts casos aquesta tecnologia té un cost alt, el problema més grans dels quals se'n deriven aquests incidents no és la pèrdua econòmica, sinó la **pèrdua o robatori d'informació**.

Per evitar aquests riscos hem d'implementar diverses mesures de seguretat que es descriuen a continuació.

1. Xifrat

Habitualment, els dispositius mòbils s'utilitzen fora de les dependències de la nostra organització.

Per aquest motiu, hem de xifrar la informació emmagatzemada en aquests suports. Així aconseguirem reduir l'impacta que podria ocasionar la pèrdua o robatori d'un dispositiu mòbil. Per exemple, la pèrdua d'un ordinador portàtil o la pèrdua d'un telèfon intel·ligent corporatiu.

Existeixen múltiples eines pel xifrat d'informació, i la major part dels fabricants d'eines de seguretat tenen aplicacions per fer-ho. A més, moltes aplicacions de compressió i ofimàtica disposen de funcionalitats específiques pel xifrat, que poden ser útils per a l'intercanvi d'informació entre dues parts i suficients en la majoria dels casos.

2. BYOD

El BYOD, anomenat així per les sigles en anglès Bring Your Own Device, és una tendència que es basa en el fet que els treballadors fan un ús dels seus dispositius personals en l'entorn de treball.
Per exemple, cada cop és més habitual que els treballadors puguin accedir al seu compte de correu o agenda corporativa des del seu telèfon intel·ligent personal, o fins i tot gestionar informació corporativa des dels seus portàtils personals.
Tot i això, aquest tipus de pràctiques BYOD tenen importants implicacions des del punt de vista de la seguretat de la informació, donat que tot i que els dispositius que utilitzem estiguin personalitzats segons les nostres preferències, això no necessàriament significa que tingui les mesures de seguretat necessàries. Per tant, hem de posar en marxa i instal·lar diferents mesures de

seguretat en els dispositius personals, que permeten treure el màxim profit al BYOD d'una forma segura.
Per tant, sempre que desitgem fer un ús d'un dispositiu personal per emmagatzemar o accedir a informació corporativa, hem de considerar tots els requisits de seguretat que aplicarem a qualsevol equip corporatiu per aquesta tasca: utilització de xifrat, contrasenyes robustes, accés per clau, ús d'eines de connexió remota en l'oficina (VPN), etc.
En alguns casos pot ser necessari fins i tot implementar mesures de seguretat addicionals, donat que en moltes ocasions aquests dispositius són gestionats per altres persones (parelles, fills) o s'utilitzen sovint fora de les instal·lacions de la universitat (per exemple, un mòbil personal).

3. Connexions a xarxes sense fils públiques

És freqüent fer un ús de xarxes sense fils públiques quan ens trobem en llocs públics, com aeroports, cafeteries, comerços, restaurants o biblioteques. En general, ho fem per evitar l'ús de connexió 3G o per velocitat, si no tenim suficient cobertura de dades.
Tot i això, les xarxes sense fils públiques presenten diferents riscos, sent el principal no saber qui controla la WiFi. Això no significa que l'amo d'un local tingui males intencions, sinó que un usuari malintencionat pot atacar la xarxa i obtenir-ne el control, si aquesta no té les mesures de seguretat adequades, sense que el propietari del local (i el proveïdor de connexió) ho sàpiguen.
Si això passa, és possible que les nostres dades siguin interceptades per un ciberdelinqüent, capturant tot el nostre flux d'informació. Per exemple, seria possible que aquest obtingues l'usuari i la contrasenya que utilitzem per accedir a la xarxa de la nostra universitat o fins i tot les claus per a gestionar els nostres comptes bancaris en línia.
No és recomanable fer ús d'aquest tipus de xarxes si anem a utilitzar informació sensible o confidencial, accedir als nostres comptes bancaris, accedir a la xarxa de la nostra universitat o similars. Hem d'utilitzar únicament en un context lúdic (llegir notícies, veure contingut multimèdia, etc.) sense oblidar, tanmateix, que en els telèfons intel·ligents, moltes aplicacions com les xarxes socials o el correu electrònic fan tasques de sincronització sense que l'usuari se n'adoni.
Per tant, si necessitem connectivitat fora de les nostres oficines, hem de buscar alternatives de connexió, com per exemple, "pinxos USB" que els operadors de telefonia quan fem ús de portàtils, les connexions 3G quan utilitzem telèfons intel·ligents o tauletes, o eines de connexió segura en la nostra organització.

4. Configuracions de seguretat vs per defecte

Per norma general, les configuracions de seguretat per defecte en els dispositius mòbils no tenen activades totes les mesures de seguretat que ofereix el sistema, ja que aquestes poden introduir massa complexitat per alguns usuaris bàsics.
Tot i això, quan es tracta de dispositius que anem a utilitzar en l'entorn corporatiu, sigui el BYOD o dispositius de l'organització, és imperatiu que apliquem a qualsevol dispositiu les mesures necessàries de seguretat.
Entre les mesures que podem destacar estan les següents:

- Xifrat dels suports d'emmagatzematge.
- Contrasenya d'accés al sistema.
- Funcionalitat que permeti restablir la configuració per defecte del dispositiu via remota (també anomenat *Wipe* remot).
- Còpies de seguretat periòdica.

Addicionalment, aquells dispositius que disposen d'un mode administrador poden portar configurades contrasenyes d'accés genèric, com admin o 1234. Aquesta informació és pública i és explotada per delinqüents.
Per tant, és necessari que abans d'utilitzar l'equip per accés remot a l'entorn corporatiu, li apliquem les principals mesures de seguretat, de mode que davant una pèrdua del dispositiu o robatori, l'impacte sigui mínim.

5. Geoposicionament

Anomenem geoposicionament a la capacitat d'alguns dispositius d'ubicar-se geogràficament. Aquesta funcionalitat és utilitzada per exemple pels GPS per a guiar a l'usuari en el seu trajecte.
Tot i això, la informació de geoposicionament també és utilitzada per altres serveis i aplicacions. Per exemple, en diverses xarxes socials existeix la possibilitat que autoritzem a la xarxa a posicionar-nos, i les aplicacions per capturar i editar imatges també guarden informació sobre la ubicació en què s'ha fet la foto.
El principal risc associat a aquestes dades de localització és que estem recaptant, emmagatzemant i pot ser, difonent, més informació de la necessària. Això passa en la major part de cops de forma involuntària.
Donat que la major part dels dispositius mòbils permeten habilitar i deshabilitar les funcions de geoposionament, segons les preferències i necessitats de l'usuari, es recomana deshabilitar aquesta funcionalitat sempre que no sigui estrictament necessari.