Introducere

Dispozitivele mobile, smartphone-uri și tabletele, trebuie să îndeplinească anumite cerințe de securitate considerate de bază: confidențialitate, integritate și disponibilitate. Pentru a atinge aceste obiective, telefoanele și tabletele trebuie securizate pentru o largă varietate de amenințări.

Scopul prezentei lucrări este de a oferi organizațiilor soluțiile adecvate pentru a centraliza și gestiona eficient dispozitivele mobile.

Prezenta lucrare cuprinde recomandări și bune practici necesare organizațiilor care utilizează telefoane inteligente și tablete în desfășurarea activităților de business și care dețin deja sau au nevoie să implementeze un sistem centralizat de management al acestora. Lucrarea exemplifică, de asemenea, riscurile de securitate pe care dispozitivele mobile le ridică și propune soluții de mitigare a acestora.

Recomandările legate de siguranța acestor dispozitive pot fi aplicate atât celor aparținând unei companii, cât și celor personale. Accentul ar trebui să fie însă asupra celor de companie, având în vedere că peste 66% dintre companii pun la dispoziția angajaților dispozitive mobile – smartphone-uri și/sau tablete (conform OpenDNS citat de SC Magazine http://www.scmagazine.com/mobile-security-stats/slideshow/805/#0).

Dispozitivele mobile: caracteristici

Telefoanele inteligente și tabletele sunt printre cele mai dinamice dispozitive și, cel mai probabil, punctul central al dezvoltării tehnologice a electronicii moderne. Analizând această dinamică, este dificil de conferit o definiție finală a termenului. Totuși, odată cu schimbarea dispozitivelor mobile se modifică și amenințările de securitate, devenind astfel important să stabilim o bază a caracteristicilor ce definesc dispozitivele mobile:

- Dispozitiv compact
- Înglobează cel puțin un receptor wireless ce poate fi conectat la Internet- WI-FI, rețea celulară de date sau orice altă tehnologie care permite conectarea la Internet
- Deține o modalitate de stocare internă a datelor
- Utilizează un sistem de operare diferit de cele utilizate pentru laptop-uri și/sau desktop-uri
- Aplicațiile sunt disponibile din surse multiple: odată cu instalarea sistemului de operare, accesibile din browser web, achiziționate și instalate de la terți.
- Include elemente de sincronizare cu alte dispozitive: desktop/laptop, servere ale organizației, servere ale providerului de servicii de comunicații, alte servere, etc.
- Una sau mai multe camere video/foto
- Microfon
- Suport pentru dispozitive de memorie externă

Principalele riscuri si amenințări

Dispozitivele mobile trebuie sa asigure îndeplinirea a cel puțin 3 obiective majore de siguranță:

Confidențialitate
datele accesate și/sau transmise/recepționate nu sunt citite de terți

Integritate
detectarea oricăror schimbări ale datelor transmise / recepționate, intenționate sau neintenționate

Disponibilitate
utilizatorul poate accesa date și resurse atunci când are nevoie de acestea

De cele mai multe ori, dispozitivele mobile necesită elemente de securitate suplimentare față de cele clasice utilizate de specialiștii IT, în primul rând pentru că, prin natura lor, dispozitivele mobile sunt mult mai expuse. Înainte de a defini un plan de securizare a dispozitivelor mobile, organizațiile ar trebui să definească modele de mitigare a amenințărilor. Principalele amenințări sunt detaliate mai jos.

Lipsa controlului asupra securității fizice

Dispozitivele mobile sunt utilizate în locații externe ce nu se află sub controlul direct al organizației, fiind astfel expuse pierderii, furtului sau accesului neautorizat. În procesul de planificare a strategiei de securizare a telefoanelor și tabletelor, organizațiile trebuie să ia în considerare faptul că aceste dispozitive vor fi în posesia unor terți rău intenționați care vor încerca sa obțină date sau să acceseze resursele organizației.

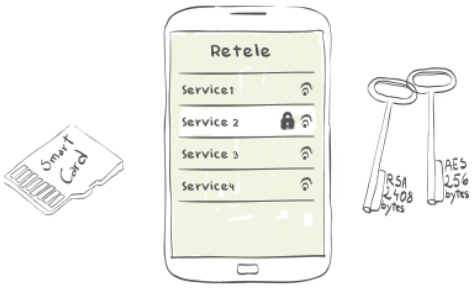
Strategia de protecție pentru aceste cazuri este una stratificată:

Protejarea datelor sensibile prin criptarea datelor de pe dispozitiv sau eliminarea stocării datelor în memoria telefonului (cazul extrem, foarte dificil de pus în practică, care elimină avantajele dispozitivului mobil).

Al doilea nivel de protecție vizează utilizarea autentificării în momentul accesării dispozitivului mobil și mai ales a resurselor. Majoritatea dispozitivelor mobile utilizează un simplu PIN – se pot însă implementa metode de autentificare bazate pe certificate digitale sau autentificare în domeniu (domain authentication).

Utilizarea de rețele ce nu sunt sub controlul organizației

Un studiu al VoiceVault atestă ca 51% dintre utilizatorii de dispozitive mobile se conectează la rețele nesecurizate (http://voicevault.com/three-frightening-mobile-security-statistics-will-make-believer-voice-biometrics/). Deoarece dispozitivele mobile utilizează în principal rețele non-organizaționale pentru comunicații de voce, text și pentru conectarea la Internet, organizațiile nu au niciun control asupra rețelelor utilizate. Aceste sisteme de comunicație sunt susceptibile la atacuri *man in the middle* ce compromit atât integritatea comunicației, cât și confidențialitatea, anulând astfel 2 dintre cele 3 obiective de bază ale dispozitivelor mobile.



Riscurile generate de utilizarea unor rețele externe se elimină prin utilizarea de tehnologii puternice de criptare și prin utilizarea de semnături electronice.

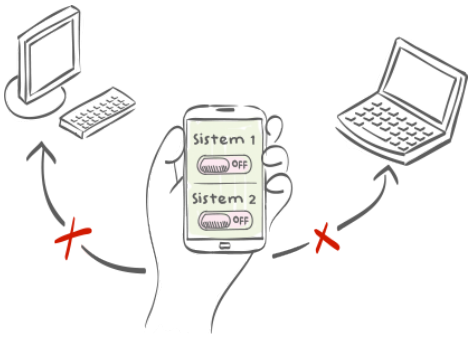
Utilizarea de aplicații dezvoltate de terți ce nu prezintă încredere

Dispozitivele mobile sunt astfel construite încât sa permită obținerea, instalarea și găsirea rapidă de aplicații dintre cele mai diverse. Acest lucru deschide ușa larg pentru o multitudine de riscuri de securitate, în special pentru dispozitivele ce nu au niciun fel de restricții sau limitări de interacțiune cu aplicații terțe.

Aceste riscuri pot fi reduse în mai multe feluri, începând cu limitarea accesului către astfel de aplicații. O astfel de soluție nu este 100% eficientă, deoarece utilizatorii încă pot accesa aceste aplicații prin intermediul browser-ului care nu poate fi blocat complet deoarece va elimina unul dintre scopurile dispozitivelor mobile. În schimb, se poate instala un alt browser ce include un sandbox securizat pentru accesarea resurselor organizaționale, lăsând browserul standard liber pentru uz.

Integrarea cu alte sisteme

Dispozitivele mobile pot interacționa cu alte sisteme prin sincronizarea sau stocarea de date. Interacțiunea locală înseamnă, de cele mai multe ori, conectarea dispozitivului la un laptop sau desktop printr-un cablu. Interacțiunea remote presupune instalarea de actualizări sau backup-ul într-un sistem cloud.



Evitarea riscurilor se poate face destul de simplu prin dezactivarea posibilității de a sincroniza un dispozitiv mobil deținut de companie cu un computer personal. De asemenea, un alt filtru de securitate ce ar trebui avut în vedere este eliminarea utilizării unor servicii externe de back-up.