Scurt ghid de utilizare a dispozitivelor mobile cu Android

Ghid destinat companiilor, începând de la alegerea și achiziționarea dispozitivelor, până la oferirea de sfaturi pentru utilizatorii finali.

Configurarea și utilizarea în siguranță a dispozitivelor cu sistem de operare Android

Android este un sistem de operare pentru dispozitivele mobile, dezvoltat și comercializat de Google, pentru a fi utilizat într-o varietate de dispozitive portabile, cum ar fi smartphone-urile, tabletele și nu numai. Deși acest ghid este potrivit pentru mai multe versiuni de Android, a fost conceput folosind un dispozitiv care rulează cu Android 10, configurat pentru modul business.

În continuare, este pusă la dispoziție o listă de politici de configurare care pot fi preluate și folosite ca punct de plecare pentru setarea propriului dispozitiv.

Securizarea dispozitivelor Android

Recomandări generale

◦ Atunci când decideți ce dispozitive Android va utiliza compania din care faceți parte, luați în considerare faptul că dispozitivele Android beneficiază în mod obișnuit de actualizări de software de până la 3 ani după lansarea produsului. Odată ce un dispozitiv este considerat vechi, acesta nu mai beneficiază de actualizări și nu i se mai oferă actualizări de securitate. În acel moment, ar trebui achiziționate dispozitive mai noi. Rețineți că programul de actualizare a sistemului de operare depinde de producătorul dispozitivului - Google a pus la dispoziție o listă cu datele de încetare a asistenței oferite pentru dispozitivele Pixel și Nexus. Pentru celelalte mărci de dispozitive, acest aspect trebuie verificat cu producătorul corespunzător.

◦ Pentru a avea cel mai ridicat nivel de control asupra politicilor aplicate, dispozitivele ar trebui să fie gestionate de companie.

◦ Odată înregistrate, dispozitivele Android ar trebui să fie controlate folosind un serviciu de supraveghere a dispozitivelor mobile (Mobile Device Management), pentru a putea impune restricțiile de securitate necesare.

◦ În funcție de dispozitivele folosite în companie, ar trebui implementat sistemul de gestionare EMM (Enterprise Mobility Management) care permite configurarea de tip OEM (Original Equipment Manufacturers). Standardul OEM a fost introdus de Google pentru a permite producătorilor de echipamente originale OEM să dezvolte aplicații care pot oferi un plus de configurații specifice dispozitivului. Aceste aplicații sunt disponibile în magazinul Google Play și permit administratorilor IT să acceseze politicile de securitate aplicate dispozitivelor, prin intermediul consolei EMM.

◦ Configurați opțiunile de înregistrare a activității și de monitorizare ale serviciului MDM (Mobile Device Management).

◦ Utilizați una dintre arhitecturile de rețea recomandate, pentru a permite utilizatorului accesul de la distanță la serviciile companiei.

◦ Dacă este necesară o rețea privată virtuală (VPN), ar trebui să utilizați o aplicație terță dedicată.

◦ Utilizarea în scop profesional a aplicațiilor terțe („aplicații gestionate”) trebuie aprobată și centralizată într-un catalog de aplicații al companiei. Acestea ar putea fi instalate automat în momentul configurării dispozitivului, sau puse la dispoziție în Magazinul Google Play gestionat de companie.

◦ Luați în considerare opțiunea de a activa conturile Google dedicate activităților profesionale pe dispozitivele utilizatorilor. Astfel, prin intermediul politicilor de pe dispozitiv, pot fi gestionate diferite funcționalități Google.

◦ Nu este recomandată configurarea unui antivirus sau a altor programe de securitate pe dispozitivele mobile.

Aplicații de lucru

Majoritatea companiilor vor dori să le ofere utilizatorilor o serie de aplicații dedicate productivității și businessului, astfel încât aceștia să poată accesa documente, crea conținut și colabora de la distanță. Este recomandată folosirea aplicațiilor integrate în serviciile companiei din care faceți parte. Aceste aplicații au un grad mai ridicat de încredere și de securitate, deoarece producătorii lor oferă o trasabilitate a calităților tehnice pe care le dețin.

Aplicațiile terțe folosite la muncă ar trebui să provină exclusiv din catalogul de aplicații al companiei, care conține doar aplicații pre-aprobate și sunt gestionate printr-un serviciu MDM. Aplicațiile instalate astfel vor putea fi supravegheate, având acces la datele de serviciu. Includerea în catalogul aprobat a unor aplicații cu privilegii ridicate, cum ar fi aplicația de tastatură terță sau extensiile de rețea, trebuie realizată cu precauție, deoarece aceste tipuri de aplicații pot accesa cantități mari de date și, prin urmare, prezintă un risc mai mare pentru companie.

Dacă dispozitivul Android este configurat să fie un unul exclusiv dedicat activității profesionale, magazinul privat Google App al companiei va permite accesul utilizatorului doar la aplicațiile pre-aprobate. Totuși, în configurațiile hibride, atât pentru uz personal cât și pentru uz profesional, unele aplicații instalate din magazinul public Google Play nu vor fi supravegheate de companie și nu trebuie să aibă acces la aceleași date. Pentru mai multe informații referitoare la acest tip de configurație și la riscurile implicate, consultați instrucțiunile puse la dispoziție pentru aplicațiile terțe.

Configurarea dispozitivului

După ce a fost ales un serviciu MDM, o arhitectură și o strategie de gestionare a aplicațiilor, trebuie aleasă o configurație prin care să se poată implementa controlul asupra dispozitivului mobil.

În mod special, configurația trebuie să includă politici care gestionează și supraveghează:

◦ Interfețele externe, inclusiv perifericele cu și fără fir (de exemplu: atunci când dispozitivul este blocat, să fie blocat și accesul USB)

◦ Utilizarea funcțiilor biometrice, a codurilor de acces și a politicilor de autentificare

◦ Serviciile Google Cloud permise

◦ Actualizările sistemului de operare și ale aplicației, inclusiv actualizările automate

◦ Configurarea parolei de dispozitiv pentru a fi în conformitate cu politica de autentificare a companiei.

Sursa: [NCSC UK]

Traducere și adaptare: Adina Lehene, Teodora Dumitrescu și Bogdan Manole (program voluntariat CERT-RO)