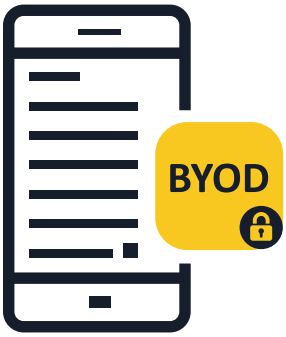
ZLONAMJERNI PROGRAMI ZA MOBILNE UREĐAJE

KORISNI SAVJETI ZA TVRTKE

1 Obavijestite zaposlenike o mobilnim rizicima

- Mobilni rad zamućuje granicu između poslovne i osobne upotrebe. Tvrtke mogu pretrpjeti značajnu štetu napadom koji je inicijalno bio usmjeren na mobilni uređaj pojedinca. Mobilni uređaj je računalo i potrebno ga je zaštititi kao što štitite računala.



2 Uvedite korporativnu politiku 'donesi svoj uređaj' (Bring-Your-Own-Device, BYOD)

- Zaposlenici koji koriste svoje mobilne uređaje da bi pristupali korporativnim podacima i sustavima (čak i ako je riječ samo o bazama podataka e-pošte, kalendaru ili kontaktima), moraju slijediti pravila tvrtke. Pažljivo odaberite tehnologije koje ćete koristiti za upravljanje mobilnim uređajima i njihovo osiguravanje i uputite zaposlenike da budu oprezni.

3 Uključite pravila mobilne sigurnosti u ukupni sigurnosni okvir

- Ako uređaj nije sukladan sigurnosnim pravilima, ne bi mu se smjelo dopustiti spajanje s korporativnom mrežom te pristup korporativnim podacima. Tvrtke bi trebale implementirati rješenja za upravljanje mobilnim uređajima (MDM) ili upravljanje mobilnošću tvrtke (EMM).
- Uz to sve, ključno je instalirati rješenje za obranu od mobilnih prijetnji. To će osigurati povećanu vidljivost i kontekstualnu svijest o aplikacijama, mreži te prijetnjama na razini operacijskog sustava.

4 Budite oprezni pri korištenju javnih Wi-Fi mreža kod pristupa podacima tvrtke

- Općenito govoreći, javne Wi-Fi mreže nisu sigurne. Ako zaposlenik pristupa korporativnim podacima koristeći javnu Wi-Fi mrežu u zračnoj luci ili u kafiću, podaci mogu biti izloženi zlonamjernim korisnicima. Savjetuje se da tvrtke razviju pravila „učinkovitog korištenja“ kad je o tome riječ.

5 Neka operacijski sustavi i aplikacije uređaja budu ažurirani

- Savjetujte osoblju da preuzme ažuriranja softvera za operacijske sustave uređaja čim ih se to zatraži. Posebno za Android, istražite davatelje mobilnih usluga i proizvođače uređaja da biste saznali njihovu politiku ažuriranja. Najnovija ažuriranja zajamčit će veću sigurnost uređaja, ali i njegove bolje performanse.

6 Instalirajte aplikacije samo s provjerenih izvora

- Kod mobilnih uređaja koji se povezuju s korporativnom mrežom, tvrtke bi trebale dopustiti instalaciju samo aplikacija sa službenih izvora. Možete i razmisliti o izradi korporativne trgovine aplikacijama putem koje krajnji korisnici mogu pristupati aplikacijama koje je odobrila tvrtka, preuzimati ih i instalirati. Obratite se davatelju usluga sigurnosti i zatražite savjet ili izradite svoj sustav sigurnosti unutar tvrtke.

7 Spriječite „otvaranje“ uređaja (jailbreak postupak)

- „Otvaranje“ je postupak uklanjanja sigurnosnih ograničenja koja nameće davatelj operacijskog sustava kako bi se dobio potpun pristup operacijskom sustavu i značajkama. Otvaranje uređaja može značajno oslabiti njegovu sigurnost i otvoriti sigurnosne rupe koje možda nisu bile vidljive. Upotreba uređaja kojima je otvoren sustav ne bi smjela biti dopuštena u okruženju tvrtke.

8 Razmislite o alternativama pohrane u oblaku

- Mobilni korisnici često žele pristupiti važnim dokumentima, ne samo putem službenih računala, nego i putem privatnih mobitela ili tableta izvan ureda. Tvrtke bi trebale pristupiti izradi sigurne pohrane u oblaku te uslugama sinkronizacije datoteka, kako bi riješili te potrebe na siguran način.

9 Potaknite osoblje da instalira aplikaciju za mobilnu sigurnost

- Svi operacijski sustavi podložni su riziku od zaraze. Ako je dostupno, pazite da koristite rješenje za mobilnu sigurnost koje otkriva i sprječava zlonamjerni i špijunski softver te zlonamjerne aplikacije, uz druge značajke zaštite privatnosti i zaštite od krađe.