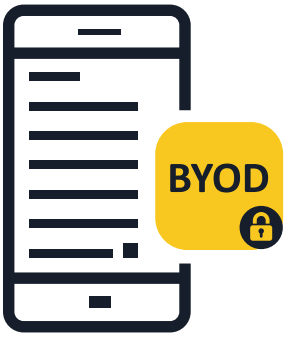
MOBILNA ŠKODLJIVA KODA

UPORABNI NASVETI ZA PODJETJA

1 Svoje zaposlene obvestite o mobilnih tveganjih

- Delo na mobilni napravi zabriše mejo med poslovno in osebno uporabo. Napad, ki je bil usmerjen predvsem na posameznikovo mobilno napravo, lahko močno vpliva na podjetje. Mobilna naprava je računalnik, zato jo morate kot tako tudi zaščititi.



2 Izvajajte poslovno politiko »prinesi svojo napravo« (BYOD – bring your own device)

- Zaposleni, ki uporabljajo lastne mobilne naprave za dostopanje do podatkov in sistemov podjetja (tudi če je to samo elektronska pošta, koledar ali baza stikov), morajo upoštevati politike podjetja. Pozorno izberite, katere tehnologije bodo uporabljene za upravljanje in zaščito mobilnih naprav, in zaposlene spodbudite, naj bodo previdni.

3 Politike mobilne varnosti vključite v splošni varnostni okvir

- Če naprava ni v skladu z varnostnimi politikami, ji ne smeta biti dovoljena povezava v omrežje podjetja in dostop do njegovih podatkov. Podjetja morajo postaviti svoje rešitve za upravljanje mobilnih naprav (MDM – Mobile Device Management) ali upravljanje mobilnosti v podjetju (EMM – Enterprise Mobility Management).
- Za dopolnitev tega je ključna namestitev mobilne rešitve pred grožnjami, s čimer zagotovite zaščito pred tveganji. To bo zagotovilo večjo prepoznavnost in vsebinsko zavedanje o nevarnostih na ravni aplikacij, omrežja in operacijskega sistema glede na stopnje ogroženosti.

4 Bodite previdni pri uporabi javnih omrežij Wi-Fi za dostop do podatkov podjetja

- Na splošno velja, da javna omrežja Wi-Fi niso varna. Če zaposleni dostopa do podatkov podjetja z brezplačno povezavo Wi-Fi na letališču ali v kavarni, so lahko podatki izpostavljeni zlonamernim uporabnikom. Priporočljivo je, da podjetja glede tega razvijejo t. i. politike učinkovite uporabe.

5 Operacijske sisteme naprav in aplikacij je treba nenehno posodabljati

- Svojim zaposlenim svetujte, naj si prenesejo posodobitve programske opreme za operacijski sistem svojih mobilnih naprav, takoj ko so pozvani, da to storijo. Posebej za sistem Android raziščite mobilne ponudnike in proizvajalce slušalk, da se seznanite z njihovo politiko glede posodobitev. Najnovejše posodobitve bodo zagotovile, da bo naprava varnejša in bo bolje delovala.

6 Aplikacije namestite samo iz virov, ki jim zaupate

- Podjetja bi morala dovoliti namestitev aplikacij iz uradnih virov na tistih mobilnih napravah, ki se povezujejo v omrežje podjetja. Premislite o vzpostavitvi trgovine z aplikacijami podjetja, znotraj katere lahko končni uporabniki dostopajo do aplikacij, ki jih je podjetje odobrilo, jih prenašajo in nameščajo. S prodajalcem varnostnih storitev se posvetujte glede namestitve trgovine ali vzpostavite lastno.

7 Preprečite »jailbreaking«

- »Jailbreaking« je postopek odstranjevanja varnostnih omejitev, ki jih je uvedel prodajalec operacijskega sistema, s čimer dobite popoln dostop do operacijskega sistema in funkcij. Izvajanje »jailbreakinga« na vaši napravi lahko znatno zmanjša njeno varnost in razkrije pomanjkljivosti varnostnega sistema, ki niso bile takoj razvidne. Naprave z omogočenim »dostopom root« ne bi smele biti dovoljene v okolju podjetja.

8 Premislite o možnostih shranjevanja v oblaku

- Mobilni uporabniki pogosto želijo dostopati do pomembnih dokumentov ne samo prek svojih službenih osebnih računalnikov, ampak tudi z zasebnih telefonov ali tabličnih računalnikov zunaj pisarne. Podjetja morajo ovrednotiti vzpostavitev varnega shranjevanja v oblaku in storitve sinhronizacije datotek za varno prilagoditev takšnih potreb.

9 Spodbudite svoje zaposlene, da si namestijo aplikacijo za mobilno varnost

- Vsi operacijski sistemi lahko dobijo virus. Če je na voljo, poskrbite, da bodo uporabili rešitev mobilne varnosti, ki zazna in preprečuje zlonamerno programsko opremo, vohunsko programsko opremo in zlonamerne aplikacije poleg drugih funkcij zasebnosti in protivlomnih funkcij.