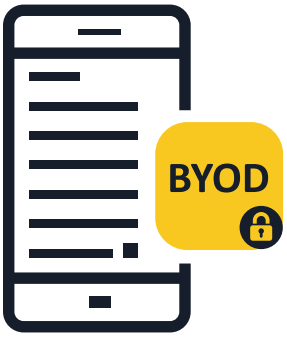
MOBILO IERĪČU ĻAUNPROGRAMMATŪRA

PADOMI UN IETEIKUMI UZŅĒMUMIEM

1 Informējiet savus darbiniekus par riskiem, kas saistīti ar mobilo ierīču drošību

- Darbā izmantojot mobilās ierīces, tiek izpludinātas robežas starp šo ierīču lietošanu darba un privātajām vajadzībām. Uzņēmumu darbību var ievērojami ietekmēt uzbrukums, kas ticis sākotnēji veikts konkrētas personas mobilajai ierīcei. Mobilā ierīce ir dators, tāpēc tai ir jānodrošina attiecīga aizsardzība.



2 Ieviesiet uzņēmuma darbinieku personisko ierīču izmantošanas (bring-your-own-device (BYOD)) politiku

- Darbiniekiem, kuri izmanto savas personiskās ierīces, lai piekļūtu uzņēmuma datiem un sistēmām (pat ja tas ir tikai e-pasts, kalendārs vai kontaktpersonu datu bāze), ir jāievēro uzņēmuma politika. Uzmanīgi izvēlieties, kuras tehnoloģijas tiks izmantotas, lai pārvaldītu un padarītu drošas mobilās ierīces, un iesakiet saviem darbiniekiem ievērot piesardzību.

3 Savā vispārīgajā drošības sistēmā iekļaujiet mobilo ierīču drošības politikas

- Ja ierīce neatbilst drošības politiku prasībām, to nedrīkst atļaut pievienot uzņēmuma tīklam un tai nedrīkst atļaut piekļūt uzņēmuma datiem. Uzņēmumiem ir jāievieš savi Mobile Device Management (mobilo ierīču pārvaldības) (MDM) vai Enterprise Mobility Management (uzņēmumu mobilitātes pārvaldības) (EMM) risinājumi.
- Papildus tam noteikti ir jāinstalē aizsardzības risinājumi pret mobilo ierīču apdraudējumu. Tādējādi tiks nodrošināta lietotņu, tīkla un operētājsistēmas apdraudējuma līmeņa redzamība un kontekstuālā izpratne.

4 Ievērojiet piesardzību, izmantojot publiski pieejamos Wi-Fi tīklus, lai piekļūtu uzņēmuma datiem

- IKopumā publiski pieejamie Wi-Fi tīkli nav droši. Darbiniekam lidostā vai kafejnīcā piekļūstot uzņēmuma datiem ar Wi-Fi tīkla savienojuma starpniecību, dati var tikt atklāti ļaunprātīgiem lietotājiem. Uzņēmumiem ir ieteicams šajā sakarā izstrādāt „efektīvas izmantošanas” politikas.

5 Vienmēr atjauniniet ierīces operētājsistēmu un lietotnes

- Iesakiet saviem darbiniekiem lejupielādēt viņu mobilo ierīču operētājsistēmas programmatūras atjauninājumus, tiklīdz viņiem tas tiek lūgts. Īpaši attiecībā uz Android — iepazīstieties ar mobilo sakaru operatoru un tālruņu ražotāju atjauninājumu politiku. Pēdējie atjauninājumi nodrošinās, ka ierīce ir ne vien daudz drošāka, bet ka ir uzlabots arī tās sniegums.

6 Instalējiet lietotnes vienīgi no uzticamiem avotiem

- Uzņēmumiem tādās mobilajās ierīcēs, kas tiek pieslēgtas uzņēmuma tīklam, būtu jāļauj instalēt lietotnes tikai no oficiāliem avotiem. Vai arī apsveriet izveidot uzņēmuma lietotņu veikalu, ar kura starpniecību galalietotāji var piekļūt lietotnēm un lejupielādēt un instalēt lietotnes, kuras ir akceptējis uzņēmums. Konsultējieties ar savu drošības risinājumu nodrošinātāju, lai saņemtu padomu par šāda veikala izveidi, vai arī izveidojiet to uzņēmuma iekšienē.

7 Nepieļaujiet ierīces drošības uzstādījumu rediģēšanu

- Drošības uzstādījumu rediģēšana ir operētājsistēmas izplatītāja uzstādīto drošības ierobežojumu atcelšanas process, kas nodrošina pilnīgu piekļuvi operētājsistēmai un tās funkcijām. Jūsu ierīces drošības uzstādījumu rediģēšana var ievērojami samazināt tās aizsardzību, oatklājot drošības caurumus, kas iepriekš nebija skaidri saredzami. Uzņēmuma vidē nedrīkst izmantot ierīces, kuru lietotājiem ir piešķirtas administratora (Root) tiesības.

8 Apsveriet mākoņkrātuves izmantošanu

- Mobilo ierīču lietotāji bieži vien vēlas piekļūt svarīgiem dokumentiem ne vien ar darba datoru starpniecību, bet arī ar privāto tālruņu vai planšetdatoru starpniecību, atrodoties ārpus biroja. Uzņēmumiem ir jāapsver drošas mākoņkrātuves izveide un failu sinhronizēšanas pakalpojumu nodrošināšana, lai izpildītu šīs prasības drošā veidā.

9 Iedrošiniet savus darbiniekus instalēt mobilo ierīču drošības lietotni

- Visas operētājsistēmas ir pakļautas inficēšanās riskam. Ja iespējams, pārliecinieties, ka viņi izmanto mobilo ierīču drošības risinājumu, kas atklāj ļaunprogrammatūras, spiegprogrammatūras un ļaunprātīgas lietotnes un pasargā no tām, kā arī citas privātuma aizsardzības un zādzību novēršanas funkcijas.

EUROPOL EC3 European Cybercrime Centre

LATVIJAS VALSTS POLICIJA

#MobileMalware