OUCH! | 2017.gada marts

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Mobilo aplikāciju droša izmantošana

Pārskats

Mobilās ierīces – planšetdatori, viedtālruņi un pulksteņi ir kļuvuši par plaši izmantotu tehnoloģiju gan personīgajā dzīvē, gan darba vajadzībām. Mobilās ierīces ir tik universālas pateicoties miljoniem aplikāciju, ko katrs var izvēlēties. Šīs aplikācijas padara mūs produktīvākus, ļauj zibenīgi sazināties un padalīties ar citiem, apmācīt un izglītot citus vai vienkārši izklaidēties. Tomēr šīs aplikācijas arī rada zināmus riskus. Tālāk apskatīsim dažus soļus, kā droši izmantot jūsu mobilās aplikācijas.

Viesredaktors

Joshua Wright ir Counter Hack tehniskais direktors un vadošais pasniedzējs SANS institūtā. Viņš ir kursa "SEC575: Mobilo iekārtu drošība un ētiskā urķēšana" un grāmatas "Atklātā urķēšana: bezvadu tīkli" autors. Josh var sameklēt Twitter **@joswr1ght**.

Mobilo aplikāciju iegūšana

Pirmais solis ir aplikāciju iegūšana no droša un uzticama avota. Noziedznieki ir iemācījušies radīt un izplatīt inficētas mobilās aplikācijas, kas izskatās kā īstas. Ja jūs instalējat šādu inficētu aplikāciju, noziedznieki var pārņemt kontroli pār jūsu iekārtu. Izvēloties aplikācijas no zināmiem un uzticamiem avotiem, jūs samazināt inficētas aplikācijas instalēšanas iespēju. Jūsu iespējas lejupielādēt kādu noteiktu aplikāciju nosaka tas, kāda zīmola ierīci jūs izmantojat.

Apple ierīcēm – iPad un iPhone aplikācijas lejupielādējat tikai no Apple Aplikāciju veikala (App Store). Šajā veikalā Apple ir veicis drošības pārbaudes visām mobilajām aplikācijām pirms to publiskošanas. Apple nevar "izķert" visas inficētās aplikācijas, taču šāda pārvaldīta vide dramatiski samazina inficēšanās risku. Ja Apple atrod inficētu aplikāciju savā veikalā, tā nekavējoties tiek izņemta no veikala. Windows Phone izmanto līdzīgu pieeju aplikāciju pārvaldīšanā.

Android ierīces ir atšķirīgas. Android dod jums izvēles iespējas lejupielādēt aplikāciju no jebkuras vietas internetā. Taču šāda elastība uzliek jums pašiem lielāku atbildību. Jums ir jābūt piesardzīgākiem attiecībā uz aplikācijām, ko

Mobilo aplikāciju droša izmantošana

jūs instalējat, jo ne visas tās ir pārbaudītas. Google uztur aplikāciju veikalu – Google Play un aplikācijām tajā ir veikta vismaz pamata drošības pārbaude. Tādēļ iesakām izmantot aplikācijas tikai no Google Play. Izvairieties no aplikācijām no citām tīmekļa vietnēm, jo ir salīdzinoši vienkārši izplatīt ļaundabīgas aplikācijas, tā inficējot jūsu mobilo iekārtu. Kā papildu aizsardzību, ja tas ir iespējams, instalējiet mobilajā ierīcē antivīrusa programmatūru.

Aplikāciju drošai izmantošanai, instalējiet tās tikai no uzticamiem avotiem, veiciet atjaunināšanu, kad vien iespējams, un dodiet aplikācijām tikai nepieciešamās atļaujas.

Neatkarīgi no tā, kādas iekārtas jūs izmantojat, papildu drošībai neizvēlieties jaunas aplikācijas, ko tikai daži cilvēki ir lejupielādējuši vai kam nav daudz pozitīvu atsauksmju. Ja aplikācija ir bijusi ilgāk pieejama un vairāk cilvēku ir to izmantojuši un atstājuši pozitīvas atsauksmes, ir mazāka iespēja, ka tā ir inficēta vai neuzticama. Papildus instalējiet tikai aplikācijas, kas jums ir nepieciešamas un ko jūs izmantojat. Vienmēr paprasiet sev – vai tiešām man vajag šo aplikāciju. Jo katra jauna aplikācija ne tikai rada jaunas ievainojamības, bet arī apdraud jūsu privātumu. Beidzot izmantot aplikāciju, izdzēsiet to no ierīces (jūs vienmēr varēsiet atlikt to atpakaļ, ja nepieciešams). Visbeidzot, nekad neurķējiet (jailbreak/root) savu ierīci. Tas ir process, kura laikā jūs uzlaužat ierīces aizsardzību un izmainât iebūvēto funkcionalitāti vai atļaujat instalēt neatļautas aplikācijas. Tas ne tikai izslēdz vai apiet ierīces drošības kontroles, bet arī padara nederīgas garantijas un uzturēšanas līgumus.

Atļaujas

Kad esat instalējis aplikāciju no uzticama avota, konfigurējiet to atbilstoši savām privātuma vēlmēm un vajadzībām. Vienemēr apsveriet pirms dodiet aplikācijai kādu atļauju – vai jūs vēlaties šo atļauju dot un vai aplikācijai tā tiešām ir nepieciešama. Piemēram, aplikācijas izmanto ģeolokācijas pakalpojumu. Ja jūs atļaujat aplikācijai vienmēr zināt savu atrašanās vietu, jūs varat dot iespēju aplikācijas izstrādātājam izsekot jūsu kustību, vai pat pārdot šo informāciju citiem. Ja jūs nevēlaties dot aplikācijai atļaujas, sameklējiet tādu aplikāciju, kas šādas atļaujas neprasa. Atcerieties, ka ir daudz izvēles iespēju.

Mobilo aplikāciju droša izmantošana

Aplikāciju atjaunināšana

Mobilās aplikācijas, tāpat kā datora un mobilās iekārtas operētājsistēma, regulāri jāatjaunina. Noziedznieki vienmēr meklē ievainojamības aplikācijās un tad izveido uzbrukumu, kas izmanto šīs ievainojamības. Aplikācijas izstrādātāji, savukārt, rada atjauninājumus, kas novērš ievainojamības un aizsargā jūsu ierīces. Jo biežāk pārbaudāt, vai aplikācijām nav pieejami atjauninājumi, jo labāk. Vairums iekārtu dod iespēju atjaunināt aplikācijas automātiski. Mēs iesakām izmantot šo iespēju. Ja tas nav iespējams, pārbaudiet aplikāciju atjauninājumus vismaz reizi divās nedēļās. Visbeidzot, kad aplikācija ir atjaunota, vienmēr pārskatiet, kādas ir izmaiņas aplikācijas atļaujām.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Sociālā inženierija:	https://securingthehuman.sans.org/ouch/2017#january2017
Atbrīvošanās no jūsu mobilās ierīces:	https://securingthehuman.sans.org/ouch/2016#december2016
Jūsu planšetdatora drošība:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Arhīvi un tulkojumi:	https://securingthehuman.sans.org/ouch/archives
Mobilo iekārtu drošības kursi:	https://sans.org/sec575

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Tulkojums: Edgars Tauriņš

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus