IBM: mobiilsed seadmed on häkkerite kõige parem sihtmärk

13 aastat tagasi - 06.04.2013 Autor: AM

IBMi IT turvalahenduste seminaril Tallinnas rõhutas IBM Security Systemsi Poola ja Baltimaade müügijuht Zbigniew Szmigiero, et koduarvutid ja mobiilsed seadmed – nutitelefonid-tahvelarvutid – muutuvad ettevõtete andmetele aina suuremaks ohuks ja häkkeritele kõige magusamateks sihtmärkideks.

„Kahjuks on suur osa tänastest infoleketest põhjustatud sellest, et töötaja viib andmed koju, võtab nö tööd koju kaasa ja sealt need siis lekivadki," ütles IBM Security Systems Poola ja Baltimaade müügijuht Zbigniew Szmigiero. „Ning aina suuremaks ohuks muutuvad mobiilsed seadmed – nutitelefonid ja tahvelarvutid."

„Kui aastal 2000 veel võtsid häkkerid oma pahategusid väljakutsena, nad testisid lihtsalt oma oskuseid, siis täna on see terve tööstusharu. Häkkerid muutuvad aina kavalamaks ja neile kõlbavad absoluutselt kõik sihile viivad teed – iga meetod on hea," rääkis Zbigniew Szmigiero.

„Võtame näiteks üsna levinud QR koodi – see on häkkerile ülihea võimalus peita lingis sisalduv ja liigseid kahtlustusi äratada võiv andmerida. Või võtame näite Poolast – seal on maanteel sellised kiiruskaamerad, mis jälgivad, kui kiiresti auto ühe kaamera juurest teiseni jõuab – kui jõudsid liiga kiiresti, tuvastab kaamera auto numbrimärgi ja sind ootab automaatselt trahviteade. Mida häkkerid tegid? Nad kirjutasid autonumbri asemele lihtsa koodijupi, mis sundis kaamerasüsteemil andmebaasi hülgama!"

Szmigiero sõnul on tänavu juba päris palju kõmulisi juhtumeid olnud, näiteks andmehoiustamist pakkuva firma Evernote andmete lekkimine, küberrünnakud Lõuna-Korea pankadele ja telekanalitele, mis viis näiteks sõjalise organisatsiooni NATO nii kaugele, et eile loodi uus sõja-aja reegel – nüüdsest võib häkkeri lihtsalt koha peal maha lasta.

Szmigiero väitel ei toimu suurem osa tänastest küberrünnakuist enam klassikaliselt – keegi paha ja võõras tungib su sisevõrku. „Täna käib hoopis nii – kõigepealt uurin ma häkkerina välja, kes on mind huvitava asutuse IT-pealik, admin. Seejärel vaatan, näiteks Facebookist, kes on tema sõbrad. Nüüd ründan

ma tema sõbra arvutit, hõivan selle ning saadan sealt sellele adminile sõnumi, näiteks mõne talle sobiva kauba sooduspakkumisega. Sooduspakkumine toob admini minu loodud veebilehele – nüüd on mul piisavalt aega, et leida tema arvutist nõrk koht ning sinna oma programmijupike sisestada. Edasi on lihtne – kui mul on pahavara su admini arvutis, hangin ma sealt andmebaasi võtme. Nii on juhtunud, Michelle Obamale näiteks saadeti sõnum, millega anti talle võimalus vaadata lasteaia peol tehtud pilte," rääkis Szmigiero. „Liiga palju töökohaga seotud arvuteid on kodudes."

Szmigiero sõnul ütleb statistika, et enamus rünnakuid tulebki väljaspool turvatud võrku nakatatud koduarvutitest ja mobiilsetest seadmetest. „Jah, Sinu nutitelefon/tahvelarvuti on häkkerile väga väärtuslik sihtmärk – sa käid sellega ju töövõrgus," lisas Szmigiero. „Nutitelefonide/tahvelarvutite puhul ei mõtle inimesed pahatihti turvalisusele – ometi laeti möödunud aastal alla tervelt 45 miljardit äppi – lõviosa neist äppidest on häkitud ning jooksevad seadmetel, mis kasutavad firma turvalist võrku. Vaadake ikka hoolikalt, milliseid andmeid uus äpp kasutada tahab, kontrollige oma mobiilseadmeid!"

- Uudised
- Turvalisus