IT teenuste juht soovitab: neid kübersoovitusi järgides jätad pätid pika ninaga

6 aastat tagasi - 03.01.2020 Autor: AM

Eesti tehnoloogiaettevõtte Iteraction IT teenuste juht Lauri Sinisaar toob välja mõned olulisemad viisid, kuidas end lihtsate võtetega kübermaailmas kaitsta ning milliseid tegevusi vältida tuleks.

Erinevad küberohud varitsevad tänapäeval sisuliselt iga nurga peal. Alles hiljuti rääkis endaga juhtunud häkkimisintsidendist tuntud Eesti sisulooja ja Youtuber Victoria Villig, kelle Instagrami konto kaaperdasid pahalased ja nõudsid lunaraha. Sealjuures näitavad uuringud, et inimesed ei ole tihti nendest ohtudest teadlikud ja ei oska end ka nende vastu kaitsta.

"Näeme enda igapäevases töös, kuidas küberkaitsesse panustamine on tänapäeval ülioluline. Tavainimene kaotab häkkimise korral enda andmeid ja halvemal juhul ka raha. Ettevõtted võivad ilma jääda sadade või isegi tuhandete klientide andmetest ja pettuse ohvriks langemisel on ka kaotatud rahasummad väga suured," rääkis Sinisaar.

Siin on mõned soovitused igapäevaeluks.

1. Kasuta kaheastmelist tuvastamist

Oma konto üle kontrolli kaotamiseks on väga paljusid erinevaid viise. Kontot haldava teenusepakkuja kaudu võivad paroolid lekkida või võib kasutaja ise õngitsusskeemi ohvriks langeda ja teadmatusest kasutajakonto andmed ise ära anda.

"Kontode kaitsmiseks on mitmeid eri viise, kuid üks on kõige olulisem – kaheastmeline autentimine. See tähendab, et kui keegi sinu parooli teada saab, siis sellest üksinda talle ei piisa, kuna sinu kontole sissepääsemiseks on vaja kaht astet. Üheks on parool ja teiseks näiteks kinnituskiri sinu telefonis või sõnum," selgitas Sinisaar.

Seega kui keegi üritab inimese kontole ligi pääseda, saab inimene ise sellest teada ja rünnak on võimalik nurjata.

2. Ettevaatust piraatlehtedel

Ei ole saladus, et internetis on kohti, kust muidu raha maksvaid asju tasuta kätte saab, näiteks filme ja mänge. Sellele vaatamata on igal asjal oma hind ja mõne filmi või programmiga võib piraatluslehelt kaasa tulla ka pahavara, mis arvutis oma elu elama hakkab.

"On arusaadav, et tasuta filmi vaatamine tundub ahvatlev. Paraku tasub piraatluslehtedel olla ettevaatlik, kuna ei ole haruldane, et selliselt lehelt tuleb kasutajale kaasa *keylogger* ehk tarkvara, mis jälgib ja salvestab seda, mida kasutaja enda arvutisse kirjutab. Nii võivad kaduma minna kontod ja paroolid ning loomulikult kõik muu tundlik ja privaatne info, mida inimene enda arvutiga haldab," ütles Sinisaar.

Sinisaare soovituseks on vähemalt paigaldada oma arvutisse viirusetõrje, mis taolist pahavara ära tunneb ja eemaldada suudab.

3. Väldi piraattarkvara

Sarnaselt tasuta filmidele tasub ettevaatlik olla ka selle suhtes, kui kuskilt internetiavarustest on võimalik muretseda mõnda muidu tasulist tarkvara tasuta.

"Raha maksmata Microsofti teenuseid kasutada sooviksid ilmselt paljud, kuid nagu piraatlusega ikka, kaasnevad ka sel juhul asjaga teatud ohud nagu viirused ja muu pahavara, mis inimese elu keeruliseks teevad," rääkis Sinisaar.

Seetõttu soovitab Sinisaar piraattarkvara vältida ning lisaturvameetmena tasub taas kasutada head viirusetõrjet.

4. Varunda andmeid

Lisaks erinevatele kaitsemeetoditele tasub tähelepanu pöörata teenustele, mis aitavad halba olukorda sattumisel sellest kergemalt pääseda. Nimelt on andmete varundamine hea viis, kuidas andmeid mugavalt kaitsta nii häkkerite kui ka lihtsalt arvutirikke eest.

"Varundamiseks soovitame kindlasti kasutada pilveteenuseid. Nii saab oma andmed mugavalt veebis hoida ja kui arvuti katki läheb, ei juhtu sinu piltidega midagi, vaid need saab uude arvutisse lihtsalt internetist alla laadida. Samuti on pilveteenused heaks heidutusmeetmeks küberpättide vastu. Kui keegi arvuti üle võtab, siis pääsed enda andmetele sellele vaatamata ligi," ütles Sinisaar.

Head pilveteenused andmete varundamiseks on näiteks OneDrive, Dropbox, Google Drive või Amazon Cloud Drive. Mitmed teenused pakuvad ka lahendust, kus kasutaja andmed varundatakse automaatselt, seega pole tarvis ise andmete eest hoolitsemiseks midagi teha.

5. Vali õige parool

Kui kaheastmeline tuvastus on konto kaitsmise juures võtmetähtsusega, siis kindlasti on oluline ka sobiva parooli valik, kuna see aitab vältida olukorda, kus pahalased inimese salasõna üldse teada saavad.

"Hea parool algab 12 märgist, sisaldab numbreid, sümboleid ning suur- ja väiketähti. Siiski tasub meelest pidada, et vaid pikkus ei taga turvalisust. Parooli valikul tuleks jälgida, et sümbolid ja suurtähed ei asetseks paroolis nii-öelda loogiliselt, näiteks salasõna ees või lõpus, kuna sellise loogika suudab ka pahalase tarkvara ära arvata,“ ütles Sinisaar.

Lisameetmena võiks kasutusele võtta paroolihalduri, mis on tarkvara, mis peab kasutaja eest tema paroole ise meeles ning aitab neid valida. Headeks variantideks on näiteks LastPass ja 1Password.

6. Uuenda tarkvara

"Ilmselt on kõik söögi alla ja söögi peale kuulnud sellest, kuidas seadmete tarkvara tuleb uuendada, kuid sellele vaatamata kipub just vananenud tarkvara olema paljude küberintsidentide põhjuseks. Mäletame ilmselt kõik pahavararünnakut mõne aasta eest, mis pani kinni kümneid haiglaid üle maailma ja rünnaku lubas läbi viia just vananenud tarkvara," rääkis Sinisaar.

Lihtne nõuanne, mida tarkvarauuenduste puhul järgida, on muuta see rutiiniks. Täpselt nagu on inimestel kombeks kord nädala-paari jooksul kodu koristada, võiks korra sama perioodi jooksul ka seadmete tarkvara üle vaadata ning ära uuendada.

Hea küberhügieeni järgimiseks tuleks teha järgmist:

- Kasuta kaheastmelist autentimist (inglise keeles *2-factor authentication*), see jätab suurema osa küberpätte pika ninaga
- Kasuta korralikku viirusetõrjet
- Piraatlusega tegelevad leheküljed ja piraattarkvara kasutamine võivad kaasa tuua viiruseid ja pahavara

- Varunda andmed pilveteenusesse, et arvuti kaotamisel või häkkimisel andmed alles jääksid
- Vali turvaline parool, mis on pikk ja sisaldab rohkelt sümboleid ja numbreid. Ideaalis kasuta paroolihaldurit (LastPass ja 1Password)
- Uuenda tarkvara. Tundub lihtne, kuid tegelikult ka seda tehes saab ära hoida väga palju ohte
- Kontrolli, kas sinu parool on lekkinud aadressil Haveibeenpwned.com.

- Tegijad
- Uudised

- Lahendused
- Turvalisus

Pilt

