SANS SECURITY AWARENESS
CERT.LV Information Technologies Security Incident Response Institution
OUCH! | 2018.gada janvāris
Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

- **Bezvadu tīkls**
- **Ierīces**
- **Paroles**
- **Rezerves kopijas**

Mājas kiberdrošība

Ievads

Pirms vairākiem gadiem kiberdrošība mājās bija vienkārša: vairumā māju bija tikai bezvadu tīkls un daži datori. Šodien tehnoloģijas ir kļuvušas sarežģītākas un ir integrētas visos mūsu dzīves aspektos, no mobilajām ierīcēm un spēļu konsolēm līdz mājas termostatam un, iespējams, ledusskapim. Turpmāk daži padomi jūsu mājas drošībai.

Viesredaktors
Matt Bromiley savā darbā apstrādā incidentus, palīdzot dažāda lieluma klientiem tikt galā ar datu noplūdes gadījumiem. Viņš arī pasniedz SANS kursus FOR508 – Padziļināta digitālā izmeklēšana un incidentu apstrāde. Sekojiet Matt **@mbromileyDFIR**.

Bezvadu tīkls

Gandrīz katrā mājā ir bezvadu (Wi-Fi) tīkls. Tas pieslēdz jūsu ierīces internetam. Vairumu mājas bezvadu tīklu kontrolē jūsu interneta maršrutētājs vai bezvadu piekļuves punkts. Abi strādā līdzīgi, izmantojot bezvadu signālus, ar kuriem savienojas arī mājas ierīces. Tas nozīmēm, ka drošs bezvadu tīkls ir jūsu mājas aizsardzības pamats. Aizsargāt bezvadu tīklu palīdzēs šie ieteikumi.

- Nomainiet interneta maršrutētāja vai bezvadu piekļuves punkta noklusēto administratora paroli. Administratora konts ir tas, kas kontrolē bezvadu tīkla iestatījumus.
- Ļaujiet pieslēgties savam bezvadu tīklam tikai cilvēkiem, kam jūs uzticaties. To var izdarīt, uzstādot tīkla drošības iestatījumus. Šobrīd labākais mehānisms ir WPA2. Izvēloties šo, cilvēkiem, kas vēlas pieslēgties tīklam, tiks prasīta parole, un, pieslēdzoties tīklam, visas aktivitātes tiks šifrētas.
- Pārliecinieties, ka parole, kas tiek izmantota, lai pieslēgtos jūsu bezvadu tīklam, ir izvēlēta droša, un, ka tā ir atšķirīga no administratora kontam piešķirtās paroles. Vairumā gadījumu jums parole ir jāievada tikai vienu reizi katrai ierīcei, jo tās saglabā un atceras pieslēguma paroli.
- Daudzi bezvadu tīkli atbalsta tā saucamo viesu tīklu. Tas ļauj ciemiņiem pieslēgties internetam, vienlaikus aizsargājot jūsu mājas tīklu, jo viesi nevar pieslēgties citām ierīcēm, kas ir šajā tīklā. Arī šim Viesu tīklam izvēlieties WPA2 un unikālu paroli.

© SANS Institute 2018

Mājas kiberdrošība

Ja neesat pārliecināts, kā izdarīt iepriekšminēto – vaicājiet savam interneta pakalpojumu sniedzējam vai izpētiet maršrutētāja vai piekļuves punkta dokumentāciju, vai apmeklējiet attiecīgā produkta vai ražotāja mājas lapas.

Šie vienkāršie pasākumi ļaus jums padarīt jūsu māju kiberdrošu – aizsargājiet bezvadu tīklu, izmantojiet automātisku atjauninājumu iespēju, izmantojiet unikālas paroles un veidojiet rezerves kopijas.

Ierīces

Nākamais – jums jāzina, kādas ierīces ir pieslēgtas bezvadu tīklam, un jāpārliecinās par to drošību. Tas bija samērā vienkārši, kad tie bija atsevišķi datori. Mūsdienās bezvadu tīklam var pieslēgties praktiski jebkas, ieskaitot jūsu viedtelefonus, televizorus, spēļu konsoles, mazuļu uzraudzības ierīces, skandas, iespējams, pat jūsu automašīna. Kad esat identificējis ierīces, pārliecinieties par to drošību. Labākais ir iespējot automātisku atjauninājumu uzstādīšanu, ja tas ir iespējams. Ļaundari nepārtraukti meklē jaunas ievainojamības ierīcēs un operētājsistēmās. Automātiska atjaunināšana nodrošina, ka jūsu datoru un ierīces darbinas jaunākā programmatūra, kas apgrūtina to uzlaušanu.

Paroles

Nākamais solis ir izmantot drošu unikālu paroli katrai ierīcei un tiešsaistes kontiem. Atslēgas vārdi ir unikāla un droša. Ja atcerēties daudzas paroles kļūst apgrūtinoši, izmantojiet paroļu frāzes. Tās ir paroles, ko ir vieglāk atcerēties un kas satur vairākus vārdus vai frāzi, piemēram, “Kur ir mana kafija?” vai “saule-pīrāgi-laimīgs-pazudis”. Jo garāka frāze, jo tā ir drošāka. Unikāla parole nozīmē atšķirīgu paroli katrai ierīcei un tiešsaistes kontam – tādā veidā, ja tiek kompromitēta viena no parolēm, pārējās ierīces un konti joprojām ir drošībā. Tāpat ieteicams ir izmantot paroļu pārvaldnieku, kas ir drošības programma, kas droši uzglabā jūs paroles šifrētā virtuālā seifā.

Visbeidzot, iespējojiet divu faktoru verifikāciju jūsu tiešsaistes kontiem, kad vien iespējams. Divu faktoru verifikācija ir daudz drošāka. Tā izmanto paroles, bet papildus piedāvā otru soli, piemēram, kodu, kas tiek nosūtīts uz jūsu viedtālruni, vai aplikāciju, kas ģenerē kodu. Divu soļu verifikācija ir pats labākais mehānisms, kā aizsargāt jūsu kontus, un tas ir daudz vienkāršāk, kā jūs domājat.

© SANS Institute 2018

Mājas kiberdrošība

Rezerves kopijas

Dažkārt, lai cik piesardzīgs jūs būtu, jūsu kontu vai ierīci var uzlauzt. Šādā gadījumā bieži vienīgais veids, kā atgūt jūsu personīgo informāciju, ir to atjaunot no rezerves kopijām. Ļoti svarīgi ir veidot regulāras rezerves kopijas svarīgākajai informācijai . Papildus vienmēr pāraudiet, vai jūs varat tiešām atjaunot informāciju. Vairums mobilo ierīču atbalsta rezerves kopiju veidošanu "mākonī". Arī datoriem ir pieejami rezerves kopiju veidošanas risinājumi vai pakalpojumi, kas ir samērā lēti un vienkārši izmantojami.

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

Paroļu frāzes:	https://securingthehuman.sans.org/ouch/2017#april2017
Paroļu pārvaldnieks:	https://securingthehuman.sans.org/ouch/2017#september2017
Divu faktoru autentifikācija:	https://securingthehuman.sans.org/ouch/2017#december2017
Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2017#august2017

License

OUCH! izdod SANS institūts programmas "Securing The Human" ietvaros un tas tiek izplatīts saskaņā ar Creative Commons BY-NC-ND 3.0 licences nosacījumiem. Jūs varat izplatīt šo biļetenu vai izmantot to savā informācijas tehnoloģiju drošības izglītošanas programmā ar nosacījumu, ka biļetens netiek izmainīts Papildu informācijai vai jautājumiem par tulkošanu izmantojiet www.securingthehuman.org/ouch e-pasta adresi.

Redakcija: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Tulkojums: Edgars Tauriņš