OUCH! | 2016.gada Oktobris

Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

- **Jūs**
- **Paroles**
- **Atjauninājumi**
- **Rezerves kopijas**

Četri soļi drošībai

Pārskats

Tehnoloģijai kļūstot par mūsu ikdienas aizvien nozīmīgāku sastāvdaļu, tā kļūst arvien sarežģītākā. Ņemot vērā izmaiņu ātrumu, turēties līdzi drošības ieteikumiem nav vienkārši. Tā vien šķiet, ka katru reizi ir kādi citi ieteikumi par to ko darīt vai nedarīt. Tomēr, lai arī nianses kā būt drošībā var mainīties laika gaitā, ir pamata lietas, ko Jūs vienmēr varat darīt, lai sevi pasargātu. Neatkarīgi no tā, kādu tehnoloģiju Jūs izmantojat, vai kur Jūs to izmantojat, mēs iesākam ievērot četrus pamata soļus. Lai uzzinātu vairāk par tiem, izmantojiet Resursu sadaļu izdevuma beigās.

Viesredaktors

Rijans Džonsons (Ryan Johnson) cenšas nodrošināt, lai organizācijas būtu gatavas neizbēgamiem uzlaušanas gadījumiem un pasniedz Padziļināto tīkla kriminālistiku SANS institūtā. Rijans ir aktīvs Twitter kā **@ForensicRJ**.

1. **Jūs**: pirmkārt atcerieties, ka tehnoloģija Jūs nekad pilnībā nepasargās. Uzbrucēji ir iemācījušies, ka vieglākais veids, kā apiet vispilnīgāko drošības sistēmu, ir uzbrukt Jums. Ja tie vēlas Jūsu parole, kredītkarti vai personas datus, visvieglākais ir Jūs apmānīt, lai Jūs pats iedotu šo informāciju. Piemēram, viņi var zvanīt Jums izliekoties par Microsoft tehnisko atbalstu un apgalvot, ka Jūsu dators ir inficēts, kamēr patiesībā tie ir tikai kiber noziedznieki, kas vēlas iegūt piekļuvi Jūsu datoram. Vai tie var nosūtīt Jums e-pastu, kurā teikts, ka Jums nav iespējams piegādāt sūtījumu un lūgts uzklikšķināt uz saites, lai apstiprinātu piegādes adresi, kamēr patiesībā viņi vēlas tikai Jūs ievilināt ļaundabīgā mājas lapā, kas kompromitēs Jūsu datoru. Tādā veidā sākas izspiedēj vīrusu vai “CEO” apmānīšanas uzbrukumi. Galu gala labākā aizsardzība pret uzbrukumiem esat Jūs pats. Esat piesardzīgs. Izmantojot veselo saprātu, Jūs varat pamanīt un apturēt vairumu uzbrukumu.

2. **Paroles**: Nākamais solis sevis pasargāšanai ir spēcīgas, unikālas paroles izmantošana Jūsu iekārtām un tiešsaistes kontiem. Atslēgvārdi ir spēcīga un unikāla. Spēcīga nozīmē, ka to nav viegli uzminēt hakeriem vai programmām. Esat noguris no sarežģītām parolēm, ko nav iespējams atcerēties un ir sarežģīti ierakstīt? Pamēģiniet paroļu frāzi. Tā vietā,

Četri soļi drošībai

lai izmantotu vienu vārdu, izmantojiet vairākus vārdus vai teikumu, ko ir vienkārši atcerēties, piemēram “Kur palikusi mana kafijas krūze?” Jo paroles frāze garāka jo labāk. Unikāla parole nozīmē, ka Jūs izmantojat atšķirīgu paroli katrai ierīcei vai tiešsaistes kontam. Tādā veidā, ja viena parole ir kompromitēta, pārējie Jūsu konti un ierīces ir drošībā. Nevarat atcerēties visas tās drošās un unikālās paroles? Neuztraucaties, mēs arī nē. Tādēļ iesakām Jums izmantot paroļu pārvaldnieku - tā ir specializēta programma Jūsu viedtālrunim vai datoram, kas uzglabā Jūsu paroles šifrētā veidā.

Sekojot šiem soļiem, Jūs labāk pasargāsiet sevi, izmantojot jaunāko tehnoloģiju.

Visbeidzot, viens no svarīgākajiem pasākumiem ir divu faktoru verifikācijas izmantošana. Viena pati parole vairs nespēj pasargāt kontus, mums nepieciešams kas spēcīgāks. Divu faktoru verifikācija ir daudz spēcīgāka. Tā izmanto Jūsu paroli, bet pievieno papildus soli (faktoru), vai nu kaut ko kas Jūs esat (biometrija) vai kaut ko kas Jums ir (piemēram, kods, kas tiek nosūtīts uz Jūsu tālruni vai aplikācija tālrunī, kas ģenerē šo kodu). Izmantojiet to katram kontam, kur vien tas, iespējams, ieskaitot paroļu pārvaldnieku. Divu faktoru verifikācija, iespējams, ir svarīgākais pasākums, ko Jūs varat veikt, lai sevi pasargātu un tās lietošana ir iespējama vienkāršāka kā Jūs domājat.

3. **Atjauninājumi**: Pārliecinieties, ka Jūsu datori, mobilās ierīces, aplikācijas un viss pārējais, kas pieslēgts Internetam, izmanto jaunāko programmatūras versiju. Kiber noziedznieki nepārtraukti meklē ievainojamības gan programmatūrā, gan ierīcēs. Kad ievainojamība tiek atrasta, viņi lieto speciālas programmas, lai tās izmantotu un ielauztos ierīcēs. Tajā pašā laikā programmatūras vai iekārtu ražotāji cenšas novērst ievainojamības izlaižot atjauninājumus. Nodrošinot to, ka datori un mobilās ierīces uzstāda atjauninājumus, Jūs apgrūtiniet ļaundariem iespēju Jūs uzlauzt. Vienkārši uzstādiet automātisko atjauninājumu uzlikšanu, kur vien iespējams. Šis likums attiecas uz jebkādu pie tīkla pieslēgtu lietu, ieskaitot televizorus, mazuļu uzraudzības iekārtas, mājas maršrutētājus, spēļu konsoles, iespējams pat automašīnas. Ja Jūsu operētājsistēma vai ierīces ir vecas un tām vairs netiek nodrošināti atjauninājumi, padomājiet par iespēju tās nomainīt pret jaunākām.

Četri soļi drošībai

4. **Rezerves kopijas**: Lai cik piesardzīgs Jūs arī nebūtu, Jūs var uzlauzt. Ja tā ir noticis, bieži vienīgā iespēja ir nodrošināt, ka Jūsu dators vai mobilā ierīce ir tīra no ļaunatūras ir to pilnībā izdzēst un pēc tam atjaunot. Uzbrucējs var pat Jums liegt piekļuvi Jūsu failiem, fotogrāfijām un citai informācijai, kas saglabāta uzlauztajā sistēmā. Bieži vienīgais veids, kā šo informāciju atgūt, ir atjaunot to no rezerves kopijas. Veiciet regulāras rezerves kopijas jebkādai svarīgai informācijai un pārliecinieties, ka Jūs tās varat izmantot, lai atjaunotu informāciju. Vairums operētājsistēmu atbalsta automātisko rezerves kopiju veikšanu. Papildus mēs iesakām glabāt rezerves kopijas vai nu Mākonī vai pie tīkla nepieslēgtā iekārtā, lai pasargātu tās no ļaundariem.

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

Pikšķerēšana:	https://securingthehuman.sans.org/ouch/2015#december2015
Paroļu pārvaldnieki:	https://securingthehuman.sans.org/ouch/2015#october2015
Divu faktoru verifikācija:	https://securingthehuman.sans.org/ouch/2015#september2015
Paroļu frāzes:	https://securingthehuman.sans.org/ouch/2015#april2015
Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2015#august2015

License

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