SANS SECURITY AWARENESS
PERLAS
OUCH! | 2018 m. sausio mėn.
Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- Jūsų belaidis tinklas
- Jūsų įrenginiai
- Slaptažodžiai
- Atsarginės kopijos

Kaip apsaugoti namus nuo kibernetinių pavojų?

Apžvalga

Prieš keletą metų apsaugoti namus nuo kibernetinių pavojų buvo paprasta, kadangi daugumoje jų buvo tik belaidis tinklas ir keletas kompiuterių. Šiais laikais technologijos tapo žymiai sudėtingesnės ir yra laikomos sudėtine kiekvieno iš mūsų gyvenimo dalimi, pradedant mobiliaisiais prietaisais ar žaidimų pultais ir baigiant namuose esančiais termostatais ar net šaldytuvais. Toliau pateiksime keletą paprastų veiksmų, kurių galite imtis, norėdami apsaugoti namus nuo kibernetinių pavojų.

Kviestinė redaktorė

Matt Bromiley yra dienos metu įvykstančių incidentų sprendėjas, padedantis savo klientams tvarkytis su įvairios apimties duomenų pažeidimais. Taip pat SANS institute jis dėsto FOR508 kursą apie pažangią skaitmeninę teismo ekspertizę ir incidentų sprendimą. Matt veiklą galite stebėti jo paskyroje **@mbromileyDFIR**.

Jūsų belaidis tinklas

Beveik kiekvienuose namuose yra belaidis (Wi-Fi) tinklas. Per jį visus savo prietaisus jungiate prie interneto. Daugumoje namų belaidis tinklas yra valdomas interneto maršruto parinktuvu arba atskiru belaidės prieigos tašku. Jie dirba tokiu pat būdu, siųsdami belaidžius signalus, o namie esantys jūsų prietaisai šiais signalais prie jų jungiasi. Tai reiškia, kad svarbiausia namų apsaugos dalis yra belaidžio tinklo apsauga. Norint jį apsaugoti, rekomenduojame imtis šių veiksmų:

- Pakeiskite numatytąjį savo interneto maršruto parinktuvo arba belaidės prieigos taško (t.y. belaidį tinklą valdančio prietaiso) administratoriaus slaptažodį. Administratoriaus paskyroje galima konfigūruoti jūsų belaidžio tinklo nustatymus.
- Užtikrinkite, kad prie jūsų belaidžio tinklo gali jungtis tik patikimi žmonės. Padarykite tai, įjungdami patikimą apsaugą. Šiuo metu geriausias būdas yra naudoti apsaugos mechanizmą, dar vadinamą WPA2. Jį įjungus, žmonių, norinčių prisijungti prie jūsų namų tinklo, bus reikalaujama įvesti slaptažodį, o jį suvedus, jų internetinė veikla bus šifruojama.
- Įsitikinkite, kad slaptažodis, skirtas prisijungti prie jūsų belaidžio tinklo, yra patikimas ir skiriasi nuo administratoriaus slaptažodžio. Prisiminkite, jog slaptažodį kiekvienam iš įrenginių reikės įvesti tik kartą, kadangi jis bus įsimintas.
- Dauguma belaidžių tinklų palaiko vadinamąjį svečių tinklą. Juo lankytojai gali jungtis prie interneto, tačiau taip jūsų namų tinklas lieka saugus, kadangi jie negali jungtis prie jokių kitų jūsų namų tinklo prietaisų. Jei pridėjote svečių

Kaip apsaugoti namus nuo kibernetinių pavojų?

tinklą, įsitikinkite, jog taip pat įjungėte WPA2 ir šiam tinklui nustatėte patikimą slaptažodį.

Nežinote kaip visa tai atlikti? Tuomet paprašykite, kad tai padarytų jūsų interneto paslaugų teikėjas arba perskaitykite jų svetainėje, taip pat maršruto parinktuvo, belaidės prieigos taško dokumentuose ar atitinkamoje svetainėje pateiktą informaciją.

Pasinaudokite šiais keturiais, paprastais veiksmais, norėdami apsaugoti namus nuo kibernetinių pavojų: apsaugokite savo belaidį tinklą, įjunkite automatinį atnaujinimą, naudokite unikalias slaptafrazes ir įjunkite atsarginių kopijų kūrimą.

Jūsų įrenginiai

Kitas veiksmas yra išsiaiškinti, kokie prietaisai yra prijungti prie jūsų belaidžio namų tinklo ir įsitikinti, jog visi šie prietaisai yra saugūs. Kai turėdavote vieną ar du kompiuterius, tai padaryti būdavo paprasta. Tačiau šiais laikais prie jūsų namų tinklo gali jungtis bet kas, įskaitant ir jūsų išmaniuosius telefonus, televizorius, žaidimų pultus, kūdikių kameras, garsiakalbius ar net jūsų automobilį. Nustatę visus prie jūsų namų tinklo prisijungusius įrenginius, įsitikinkite, kad kiekvienas iš jų yra saugus. Geriausias būdas tai padaryti yra įsitikinti, ar juose (kai tik tai įmanoma) yra įjungtas automatinis atnaujinimas. Kibernetiniai nusikaltėliai įvairiuose įrenginiuose ir operacinėse sistemose pastoviai ieško naujų trūkumų. Įjungus automatinį atnaujinimą, jūsų kompiuteriuose ir kituose prietaisuose visada bus pati naujausia programinės įrangos versija, todėl nusikaltėliams bus žymiai sudėtingiau į juos įsilaužti.

Slaptažodžiai

Sekantis etapas – kiekviename iš savo prietaisų ir internetinių paskyrų naudoti patikimą bei unikalų slaptažodį. Esminiai žodžiai šiame sakinyje yra „patikimą“ ir „unikalų“. Tačiau esate pavargę nuo sudėtingų slaptažodžių, kuriuos sunku ne tik prisiminti, bet ir suvesti? Mes taip pat! Tokiu atveju naudokite slaptafrazes. Tai tokia slaptažodžio rūšis, kurią sudaro keli, lengvai prisimenami žodžiai, pavyzdžiui, „Kur mano kava?“ arba „saulėkaita-spurgos-laimingas-pasiklydęs“. Kuo ilgesnė jūsų slaptafrazė, tuo ji patikimesnė. Unikalus slaptažodis reiškia, kad kiekviename įrenginyje ir internetinėje paskyroje yra nustatytas skirtingas slaptažodis. Tokiu būdu, sužinojus vieną slaptažodį, visos kitos paskyros ir įrenginiai liks saugūs. Nesugebate prisiminti visų tų patikimų ir unikalių slaptažodžių? Nesijaudinkite! Rekomenduojame naudoti slaptažodžių tvarkytuvę, t.y., specialią apsaugos programą, kurioje visi jūsų slaptažodžiai būtų patikimai saugojami užšifruotoje, virtualioje saugykloje.

Kaip apsaugoti namus nuo kibernetinių pavojų?

Galiausiai, kai tik įmanoma, įjunkite dviejų etapų tapatybės patikrinimą, ypač savo internetinėse paskyrose. Dviejų etapų tapatybės patikrinimas yra žymiai saugesnis. Čia turėtumėte suvesti savo slaptažodį ir atlikti dar vieną papildomą veiksmą, pavyzdžiui, surinkti į jūsų išmanųjį telefoną atsiųstą kodą. Arba naudokite išmaniojo telefono programėlę, kuri kaskart sukurtų po atskirą kodą. Dviejų etapų tapatybės patikrinimas tikriausiai yra vienintelis svarbiausias veiksmas, kurio galite imtis, norėdami apsisaugoti internete. Be to, jį naudoti žymiai lengviau, nei įsivaizduojate.

Atsarginės kopijos

Kartais, nesvarbu kokie atsargūs bebūtumėte, į jūsų prietaisus gali būti įsilaužta. Taip nutikus, vienintelis būdas atkurti turėtą informaciją – iš turimų atsarginių duomenų kopijų. Įsitikinkite, kad reguliariai yra daromos bet kokios svarbios informacijos atsarginės kopijos. Be to, nepamirškite patikrinti, jog vis dar galite iš tų kopijų dokumentus atkurti. Dauguma mobiliųjų įrenginių atsargines kopijas gali automatiškai kurti įkeliant jas į debesiją. Didelei daliai kompiuterių jums gali tekti nupirkti kokią nors atsarginių kopijų kūrimo programinę įrangą ar paslaugą, kuri yra santykinai pigi bei paprasta naudoti.

SUŽINOKITE DAUGIAU

Prenumeruokite kas mėnesinį OUCH! naujienlaiškį, gaukite prieigą prie archyvų, sužinokite daugiau apie SANS saugumo sprendimus apsilankę securingthehuman.sans.org/ouch/archives.

Šaltiniai

Slaptafrazės:	https://securingthehuman.sans.org/ouch/2017#april2017
Slaptažodžių tvarkytuvės:	https://securingthehuman.sans.org/ouch/2017#september2017
Dviejų etapų tapatybės patikrinimas:	https://securingthehuman.sans.org/ouch/2017#december2017
Atsarginės kopijos:	https://securingthehuman.sans.org/ouch/2017#august2017

Licencija

Redaktoriai: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.