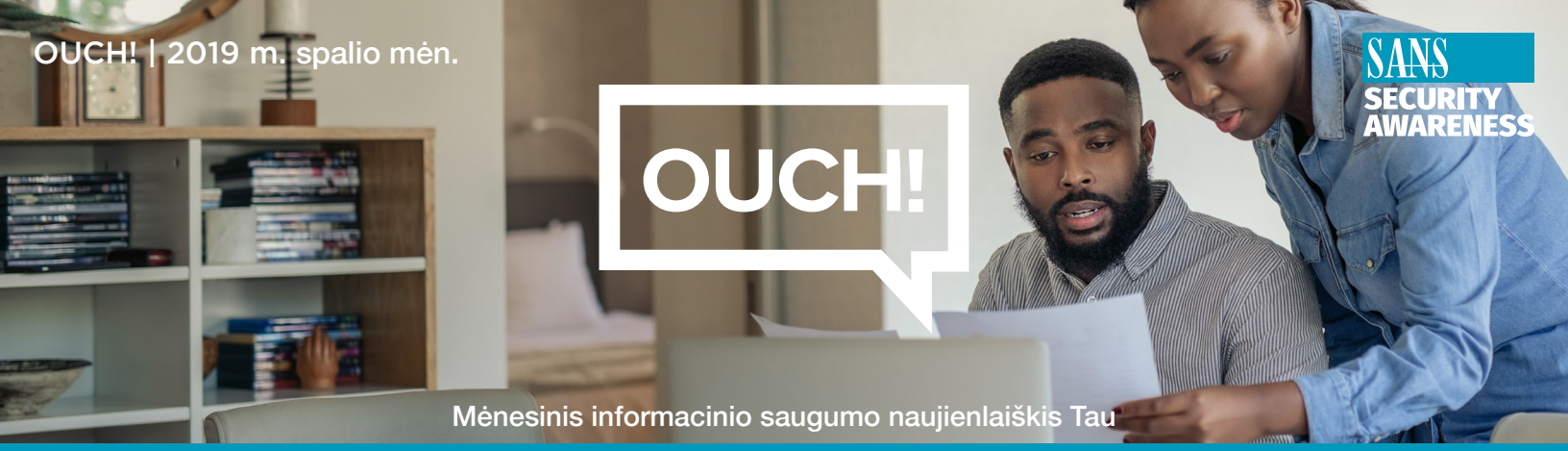

Mėnesinis informacinio saugumo naujienlaiškis Tau

Keturi, paprasti veiksmai, padėsiantys užsitikrinti saugumą

Apžvalga

Maksimalus technologijų išnaudojimas gali atrodyti neįveikiamu ir painiu dalyku. Tačiau, nepaisant naudojamos technologijos ar naudojimo būdo, egzistuoja keturi paprasti veiksmai, galintys padėti užsitikrinti saugumą.

1. Savisauga. Pirmiausia, vien tik technologijos jūsų neapsaugos, nes geriausia apsaugos priemonė yra jūsų savisauga. Nusikaltėliai jau suprato, kad lengviausias būdas gauti norimą dalyką yra nusitaikyti į jus, o ne į jūsų kompiuterį ar kitus įrenginius. Jiems panorėjus sužinoti jūsų slaptažodį, kredito kortelės numerį ar perimti jūsų kompiuterio valdymą, tereikia pasistengti jus įtikinti visa tai jiems atskleisti, o tai dažniausiai yra daroma skubinant imtis veiksmų. Pavyzdžiui, jie gali jums paskambinti, apsimetę „Microsoft“ techninio skyriaus darbuotojais, ir pasakyti, jog jūsų kompiuteris buvo užkrėstas virusu, kai tuo tarpu jie yra paprasčiausi kibernetiniai nusikaltėliai, norintys gauti prieigą prie jūsų kompiuterio. O galbūt jie jums atsiųs el. laišką, kuriame bus rašoma, jog jūsų siuntinio neįmanoma pristatyti, kol nepaspaudėte nuorodos, patvirtinančios jūsų pašto adresą, kai tuo tarpu nuoroda jus nukreips į kenkėjišką svetainę, per kurią bus įsilaužta į jūsų kompiuterį. Galiausiai, geriausia gynybos priemone esate patys. Pasitelkę sveiką protą, galite ne tik pastebėti daugumą tokių atakų, bet ir užkirsti joms kelią.

2. Slaptafrazės. Atsiradus šiuolaikiniams duomenų apdorojimo greičiams, 8 spaudos ženklų slaptažodžiai tapo lengvai įveikiama atgyvena. Svetainei paprašius susikurti slaptažodį, vietoj jo įveskite patikimą ir unikalią slaptafrazę. Slaptafrazė tai tokia slaptažodžio rūšis, kurią sudaro eilė tokių lengvai įsimenamų žodžių, kaip „bitė medus burbonas lietus“. Kuo ilgesnė jūsų slaptafrazė, tuo ji patikimesnė. Unikali slaptafrazė reiškia, jog kiekviename įrenginyje arba internetinėje paskyroje ji yra skirtinga. Tokiu būdu, atspėjus vieną slaptafrazę, visos kitos jūsų paskyros ir įrenginiai liks saugūs. Negalite prisiminti visų susikurtų slaptafrazių? Tuomet naudokite slaptažodžių tvarkytuvę, t. y., specialią programą, kurioje šifruotu formatu būtų patikimai saugomos visos jūsų slaptafrazės (ir kurioje būtų daugybė kitų, puikių funkcijų).

Galiausiai, įjunkite dviejų etapų tapatybės patvirtinimą (dar vadinamą tapatybės patvirtinimu dviem arba keliais veiksmais). Jo metu turi būti įvedamas jūsų slaptažodis ir atliekamas antras veiksmas, pavyzdžiui, įvedamas į jūsų išmanųjį telefoną atsiųstas arba programa sugeneruotas kodas. Dviejų etapų tapatybės patvirtinimas tikriausiai yra pats svarbiausias veiksmas, kurio galite imtis, norėdami apsaugoti savo internetines paskyras. Be to, tai padaryti yra žymiai paprasčiau, nei galvojate.

3. Atnaujinimai. Įsitikinkite, kad kiekviename jūsų kompiuteryje, mobiliajame įrenginyje, programoje ir programėlėje veikia naujausia programinės įrangos versija. Kibernetiniai nusikaltėliai jūsų naudojamuose įrenginiuose nuolat ieško naujų pažeidžiamų programinės įrangos vietų. Aptikę tokias vietas, jie pasitelkia specialias programas, skirtas jomis pasinaudoti ir įsilaužti į jūsų naudojamus įrenginius. Tuo tarpu, šiems įrenginiams programinę įrangą kuriančios įmonės sunkiai dirba, siekdamos tokias pažeidžiamas vietas sutvarkyti, išleidžiant atnaujinimus. Užtikrindami, jog jūsų įrenginiuose ir mobiliuosiuose prietaisuose būtų iškart įdiegiami šie atnaujinimai, jūs stipriai sumažinsite galimybes į šiuos prietaisus įsilaužti. Norėdami visada naudotis naujausia programine įranga, kai tik yra įmanoma, įjunkite automatinio atnaujinimo funkciją. Ši taisyklė galioja beveik bet kokiai technologijai, kurią jungiate prie tinklo, įskaitant prie interneto jungiamus televizorius, vaikų stebėjimo kameras, apsaugos kameras, namų maršruto parinktuvus, žaidimų konsoles ar net automobilį.

4. Atsarginės kopijos ir duomenų atkūrimas. Kartais, nesvarbu, kokie atsargūs bebūtume, į mūsų prietaisus gali būti įsilaužta. Taip nutikus, atsarginės kopijos dažniausiai liks vieninteliu būdu atkurti visą savo asmeninę informaciją. Įsitikinkite, kad reguliariai darote bet kokios svarbios informacijos atsargines kopijas ir patikrinkite ar galite iš jų atkurti savo duomenis. Dauguma operacinių sistemų ir mobiliųjų prietaisų turi automatinę atsarginių kopijų kūrimo į išorinius įrenginius arba debesiją funkciją.

Kviestinis redaktorius

*Sertifikuotas SANS instituto dėstytojas **Steve Anson** konsultuoja tarptautinių IT saugumo komandų narius ir vyriausybių atstovus, siekdamas pagerinti jų saugumo lygį. Steve taip pat yra būsimos knygos „Taikomasis reagavimas į incidentus“ autorius, svetainėje www.AppliedIncidentResponse.com teikiantis nemokamus išteklius IT saugumo specialistams.*

Šaltiniai

Socialinė inžinerija: https://www.sans.org/u/W3G
Individualizuoti apgaulingi laiškai: https://www.sans.org/u/W3Q
Paprastas slaptažodžių kūrimas: https://www.sans.org/u/W3V
Ar pasidarėte atsargines kopijas?: https://www.sans.org/u/W40