OUCH! | 2016 m. liepos mėn.

Mėnesinis informacinio saugumo naujienlaiškis kompiuterių naudotojams

OUCH!

ŠIAME LEIDINYJE…

- **Kaip sukčiaujama apsimetant įmonės vadovu?**
- **Kaip apsisaugoti?**

Sukčiavimas apsimetant įmonės vadovu

Kaip sukčiaujama apsimetant įmonės vadovu?

Kibernetiniai nusikaltėliai veikia patylomis, nuolat sugalvodami naujų būdų, kuriais galėtų gauti norimus dalykus. Vienas iš veiksmingiausių būdų yra nusitaikyti į tokius žmones kaip jūs. Kibernetiniai nusikaltėliai žino, kad silpniausia bet kurios organizacijos grandis yra nieko neįtariantys žmonės, tačiau jie pamiršo, jog geriausia organizacijos apsauga gali būti tokie sumanūs žmonės kaip OUCH! skaitytojai.

Kviestinė redaktorė

Angela Pappas yra „Thomson Reuters“ mokymo ir informavimo apie informacijos saugumą direktorė. Savo darbe Angela yra atsakinga už atstovų programą, elektroniniu būdu mokydama ir lavindama darbuotojus apie sukčiavimą.

Kibernetiniai nusikaltėliai sukūrė naują puolimo būdą, vadinamą sukčiavimu apsimetant įmonės vadovu (angl. CEO Fraud), kuris dar yra žinomas kaip kompromitavimas elektroniniais verslo laiškais (angl. Business Email Compromise arba BEC). Šių puolimų metu, kibernetinis nusikaltėlis apsimeta jūsų įmonės generaliniu direktoriumi arba kitu vyresniuoju vadovu. Nusikaltėliai tokiems darbuotojams kaip jūs atsiunčia el. laišką, bandydami jus įtikinti padaryti ką nors tokio, ko neturėtumėte daryti. Tokių puolimų rūšys yra ypač efektyvios, kadangi kibernetiniai nusikaltėliai prieš tai būna atlikę tyrimą. Pirmiausiai, jie jūsų organizacijos svetainėje randa informaciją, nusakančią kur yra įmonės buveinė, kas yra jūsų vadovai ir su kokiomis organizacijomis jūs dirbate. Tuomet kibernetiniai nusikaltėliai tokiose svetainėse kaip LinkedIn, Facebook ar Twitter pasidomi jūsų bendradarbiais. Žinodami organizacijos struktūrą jie pradeda tyrimą ir nusitaiko į konkrečius darbuotojus. Savo taikinius jie renkasi pagal savo konkrečius tikslus. Jei kibernetiniai nusikaltėliai siekia gauti pinigų, tuomet jie gali nusitaikyti į darbuotojus dirbančius buhalterijos skyriuje. Jei jie ieško mokesčių informacijos, jie gali nusitaikyti į žmogiškųjų išteklių skyrių. Jei jie nori gauti prisijungimą prie duomenų bazės serverio, tuomet jie gali nusitaikyti į ką nors, dirbantį IT skyriuje.

Nusprendę koks yra siekis ir į ką nusitaikyti, jie pradeda regzti puolimą. Dažniausiai jie naudoja konkrečiam asmeniui skirtą suklastotą elektroninį laišką. Sukčiaujama tuomet, kai nusikaltėlis milijonui žmonių išsiunčia el. laišką, siekdamas juos įtikinti imtis kokių nors veiksmų, pavyzdžiui, atidaryti užkrėstą priedą arba apsilankyti kenkėjiškoje svetainėje. Sukčiavimas

Sukčiavimas apsimetant įmonės vadovu

naudojant konkrečiam asmeniui skirtą suklastotą elektroninį laišką yra panašus į įprastą sukčiavimą, tačiau vietoj bendro laiško išsiuntimo milijonams žmonių, jie išsiunčia po individualų laišką mažai, rinktinių žmonių grupei. Šie konkretiems asmenims skirti suklastoti elektroniniai laiškai atrodo ypač tikroviškai, be to juos sunku aptikti. Dažnai atrodo, jog jie atėjo iš jums pažįstamo arba jūsų įmonėje dirbančio asmens, pavyzdžiui, jūsų bendradarbio, o gal net paties vadovo. El. laiškai atrodo tikroviškai, kadangi juose naudojamas tas pats žargonas, kuriuo įprastai kalba bendradarbiai, juose taip pat gali būti naudojamas jūsų organizacijos logotipas ar net oficialus vadovo parašas. Dažnai šiuose el. laiškuose jaučiamas didžiulis skubinimas, reikalaujant nedelsiant imtis veiksmų ir išlaikyti konfidencialumą. Kibernetinių nusikaltėlių tikslas yra jus priversti neapgalvotai suklysti. Pateikiame tris dažniausiai pasitaikančias situacijas:

Sukčiavimas apsimetant įmonės vadovu tai galingas puolimas, kuriuo galima apeiti daugumą mūsų saugumo priemonių. Galiausiai, geriausia mūsų apsauga esate jūs patys.

- **Bankinis pavedimas**. Kibernetiniai nusikaltėliai siekia gauti pinigų. Tai reiškia, kad jie ieškojo informacijos ir sužinojo, kas dirba buhalterijos skyriuje arba kokia komanda tvarko jūsų organizacijos finansus. Tuomet nusikaltėliai parašo ir išsiunčia el. laišką apsimesdami tų asmenų vadovu, el. laiške nurodydami, jog tai skubus atvejis ir kad pinigai į tam tikrą sąskaitą turi būti pervesti nedelsiant.

- **Sukčiavimas mokant mokesčius**. Kibernetiniai nusikaltėliai siekia pasisavinti informaciją apie jūsų bendradarbius, kad galėtų apsimesti darbuotojais, siekdami įgyvendinti sukčiavimo planą mokant mokesčius. Jie susiranda informaciją apie jūsų organizaciją ir sužino, kas tvarko darbuotojų informaciją, pavyzdžiui, nusitaiko į kažką, kas dirba žmogiškųjų išteklių skyriuje. Tuomet kibernetiniai nusikaltėliai išsiunčia netikrą el. laišką, apsimesdami vyresniuoju vadovu arba kuo nors iš teisės skyriaus, reikalaudami nedelsiant pateikti konkrečius dokumentus.

- **Apsimetimas teisininku**. Ne visada sukčiavimas apsimetant įmonės vadovu vyksta naudojant el. laiškus. Kartais gali būti naudojami ir tokie būdai, kaip skambučiai telefonu. Tokiu atveju, nusikaltėliai jums išsiunčia el. laišką, apsimesdami vyresniuoju vadovu, pranešančiu, jog jums žada paskambinti teisininkas dėl skubaus klausimo. Tuomet jums paskambina teisininku apsimetęs nusikaltėlis. Kalbėdamas apie konfidencialius dalykus, kuriuos reikia įvykdyti per konkretų laiką, nusikaltėlis sukuria didelės skubos pojūtį. Dėl spaudimo paskubėti, jūs patikite, jog veiksmų turite imtis nedelsiant.

Sukčiavimas apsimetant įmonės vadovu

Kaip apsisaugoti?

Taigi kaip galėtumėte apsisaugoti ir kartu apsaugoti savo organizaciją? Geriausia jūsų apsauga yra sveikas protas. Jei iš savo vadovo arba kolegos gavote pranešimą, kuris neskamba ir neatrodo patikimai, tai gali būti puolimas. Užuominomis gali būti didžiulės skubos jausmas, keistai atrodantis parašas, tam tikras tonas, kurio iš šių žmonių nesitikėtumėte arba jei el. laiške naudojamas vardas skiriasi nuo to, kaip esate to žmogaus vadinamas. Dar viena užuomina galėtų būti nusikaltėlių naudojamas el. pašto adresas arba telefono numeris, kurio niekada prieš tai nesate matę, o galbūt jų naudojamas el. pašto adresas atrodo labai panašiai, bet nėra identiškas jūsų bendradarbio arba vadovo el. pašto adresui. Kilus abejonėms, paskambinkite tam asmeniui patikimu telefono numeriu arba susitikite su juo akis į akį (tik nerašykite atsakymo el. paštu) ir įsitikinkite, kad šį el. laišką siuntė būtent jis. Niekada nebandykite išvengti saugumo politikos ar procedūrų. Jūsų organizacijoje gali būti laikomasi tam tikros politikos, kuria apibrėžiamos tinkamos procedūros, kurias naudojant galima pervesti lėšas arba atskleisti konfidencialią informaciją. Prašymai šias procedūras apeiti, nepaisant akivaizdaus šaltinio, turėtų būti laikomi įtartinais, todėl prieš imantis bet kokių veiksmų, tai derėtų patikrinti. Jei gavote tokį prašymą ir nežinote ką daryti, nedelsiant susisiekite su savo prižiūrėtoju, pagalbos skyriumi arba informacijos saugumo komanda.

SUŽINOKITE DAUGIAU

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

Šaltiniai

Socialinė inžinerija:	https://securingthehuman.sans.org/ouch/2014#november2014
Sukčiavimas:	https://securingthehuman.sans.org//ouch/2015#december2015
Kas yra kenkimo programa?:	https://securingthehuman.sans.org/ouch/2016#march2016
Dviejų etapų tapatybės patikrinimas:	https://securingthehuman.sans.org/ouch/2015#september2015
Dienos patarimas:	https://www.sans.org/tip-of-the-day

Licencija

Redaktoriai: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Lietuvišką vertimą finansavo „Perlo“ įmonių grupė.