ConnectPay

Atmintinė apie sukčiavimą

Tuo metu, kai visas pasaulis kovoja su pasauline pandemija, organizacijos ir įmonės susiduria su kitokiu rimtu ir vis agresyvesniu priešu – sukčiavimu. Nuo sukčiavimo nėra apsaugota nė viena pasaulio bendrovė, nuo jo nėra ir vakcinos. Be to, bendrovės turėtų tikėtis, kad 2022 m. nusikalstamos veiklos ir sukčiavimo apimtys ir toliau augs. **„ConnectPay“** nori jus informuoti apie naujausias sukčiavimo tendencijas ir padėti jums kovoti su šiuo blogiu.

1. Kokios yra aktualiausios sukčiavimo tendencijos?

Sertifikuotų sukčiavimo tyrėjų asociacijos (angl. *Association of Certified Fraud Examiners*, ACFE) atlikto tyrimo duomenimis, **51 proc.** organizacijų nuo pandemijos pradžios aptiko daugiau sukčiavimo atvejų, o **71 proc.** įmonių ir organizacijų mano, kad sukčiavimo apimtys jų organizacijose iki 2022 m. turėtų išaugti.

2021 m. **38 proc.** organizacijų nusprendė didinti investicijas į kovai su sukčiavimu skirtas technologijas. Reaguodamos į pandemiją, **80 proc.** apklaustųjų organizacijų jau yra vienaip ar kitaip pakoregavusios savo kovos su sukčiavimu programas.

Vidaus ir išorės sukčiavimo atvejų skaičius pasiskirstė beveik po lygiai – maždaug po **40 proc.**, o likusią dalį iš esmės sudarė mišraus – vidinio ir išorinio – sukčiavimo atvejai.

Bendrovės „PwC“ 2020 m. atlikto pasaulinio nusikalstamos veiklos ir sukčiavimo tyrimo duomenimis, beveik pusė organizacijų susidūrė bent su vienu sukčiavimo atveju, o šios statistikos vidurkis – šeši sukčiavimo atvejai vienai bendrovei. Dažniausiai pasitaiko tokios sukčiavimo rūšys:

- klientų sukčiavimas;
- kibernetiniai nusikaltimai;
- neteisėtas turto pasisavinimas;
- kyšininkavimas ir korupcija;
- sukčiavimas apskaitoje / finansinėse ataskaitose.

2. Kokia yra sukčiavimo daroma žala?

Nuostolius dėl sukčiavimo įvertinti sunku. Kai kurias sąnaudas galima apskaičiuoti – tai tiesioginiai finansiniai nuostoliai arba išlaidos baudoms, nuobaudoms sumokėti, atsakomiesiems veiksmams vykdyti ir žalai atlyginti. Tačiau kitas sąnaudas pamatuoti nėra taip paprasta. Tarp jų – žala prekių ženklui, prarasta padėtis rinkoje, kritusi darbuotojų motyvacija ir prarastos galimybės.

Vidutiniai finansiniai nuostoliai gali sudaryti nuo 0,5 iki 5 proc. visų įprastinių organizacijos įplaukų. Bendrovės „Javelin“ 2021 m. atlikto tapatybės klastojimo tyrimo duomenimis, nuostoliai dėl tapatybės klastojimo 2020 m. sudarė 56 mlrd. JAV dolerių. Kaip rašoma 2020 m. ACFE ataskaitoje

tautoms, tipinis sukčiavimo darbo vietoje atvejis trunka 14 mėnesių iki jis būna aptinkamas ir per mėnesį gali padaryti 8 300 JAV dolerių nuostolių. Šiuo atveju itin svarbus laiko veiksnys – kuo vėliau aptinkamas sukčiavimo atvejis, tuo didesnis nuostolis patiriamas.

3. Kokios yra dažniausiai pasitaikančios sukčiavimo formos?

- **Sukčiavimas darbo vietoje** – tai sukčiavimo atvejis, kai sukčiauti bendrovės atžvilgiu imasi jos darbuotojas, vadovas, tarnautojas arba savininkas. Trys pagrindinės sukčiavimo darbo vietoje kategorijos yra korupcija, neteisėtas turto pasisavinimas ir ataskaitų klastojimas. ACFE duomenimis, dėl tokio sukčiavimo bendrovės patiria didžiausius nuostolius – iki 5 proc. visų savo įplaukų.

- **Tapatybės vagystė** – tai ataka, kai įgyjama nukentėjusiojo asmeninė informacija, kuri neteisėtai naudojama sukčiavimo tikslais.

- **Artimųjų sukčiavimas** – ši sukčiavimo rūšis yra panaši į tapatybės klastojimą, tačiau nusikaltėlis priklauso artimai nukentėjusiojo aplinkai. Dėl to sukčiaujantis asmuo turi galimybę įgyti nukentėjusiojo asmeninę informaciją, kurią jis neteisėtai naudoja, siekdamas sukčiauti. Nusikaltėlis gali būti šeimos narys, artimas bičiulis, kartu gyvenantis draugas, kolega ir pan.

- **Sąskaitos perėmimas** – tapatybės vagystės ir sukčiavimo rūšis, kai piktų kėslų turinti trečioji šalis gauna prisijungimo prie vartotojo sąskaitos duomenis.

- **Kompiuterinis įsilaužimas** – dvi dažniausiai pasitaikančios kompiuterinio įsilaužimo rūšys yra įsilaužimas į el. pašto paskyrą ir vartotojo sistemą. Su tokiais incidentais susiduriama, kai kibernetiniai nusikaltėliai įgyja neteisėtą prieigą prie jūsų el. pašto ar sistemos ir gali peržiūrėti juose esančią informaciją ir (arba) ja manipuliuoti.

- **Duomenų vagystė (angl. *phishing*)** – labai dažnai sutinkama kibernetinės vagystės rūšis. Tokios atakos patiriamos, kai kibernetiniai nusikaltėliai pavagia nukentėjusiojo asmens duomenis naudodami suklastotą svetainę, kuri atrodo kaip tikra. Nieko neįtariantys asmenys į tokias svetaines dažniausiai nukreipiami el. paštu.

- **Socialinis programavimas** – socialinio programavimo atveju nusikaltėliai gali įgyti asmens pasitikėjimą, su juo bendraudami tam, kad surinktų informaciją apie tą asmenį, sistemą arba atitinkamą organizaciją.

- **Vadovų sukčiavimas** arba vadinamasis įmonės el. pašto kompromitavimas (angl. *Business Email Compromise*, BEC) – tai sukčiavimas pasitelkiant socialinį programavimą. Sukčiai apsimeta aukšto rango vadovu (paprastai generaliniu direktoriumi), kad įtikintų darbuotojus atlikti mokėjimą, suteikti konfidencialios informacijos ir pan.

- **Kenksminga programinė įranga** – kompiuteriniai įsilaužėliai, siekdami pasiekti jūsų asmeninę informaciją, į jūsų prietaisus ar internetines platformas gali perduoti

kenksmingą programinę įrangą. Nors tokia programinė įranga jūsų sistemų ar įrenginių technologinei įrangai ir nekenkia, dėl jos gali rimtai nukentėti tokioje įrangoje saugomi duomenys ir programos.

4. Kokių prevencinių priemonių derėtų imtis?

- Savo organizacijoje įgyvendinkite tinkamą sukčiavimo aptikimo, atsakomųjų veiksmų ir prevencijos strategiją, kad galėtumėte užkirsti kelią sukčiavimui ir netinkamam elgesiui, aptikti sukčiavimo ir netinkamo elgesio atvejus ir imtis atitinkamų atsakomųjų veiksmų. Turėtų būti aiškiai nustatytos darbuotojų pareigos ir atsakomybės ribos, įmonėje turėtų būti puoselėjama nepakantumo sukčiavimui kultūra. Įgyvendinant kovos su sukčiavimu priemones patiriami mažesni nuostoliai dėl sukčiavimo, o sukčiavimo atvejai aptinkami greičiau.

- Didinkite savo darbuotojų sąmoningumą sukčiavimo atžvilgiu. Supažindinkite darbuotojus su geriausiomis sukčiavimo prevencijos praktikomis ir perspėjamaisiais ženklais, taip pat procedūromis, kuriomis būtina vadovautis atakos atveju. ACFE teigimu, 33 proc. sukčiavimo darbo vietoje atvejų buvo aptikti, nes bendrovėse buvo įdiegtas pranešimų apie vidinius pažeidimus procesas, su kuriuo buvo supažindinti darbuotojai.

- Jei įmanoma, naudokite dviejų veiksnių tapatybės patvirtinimo procesą ir neperduokite vienkartinių prisijungimo kodų trumposiomis žinutėmis ar telefonu. O jeigu jūsų svetainėje negalima įdiegti dviejų veiksnių tapatybės patvirtinimo funkcijos, stenkitės naudoti sudėtingus slaptažodžius arba slaptažodžių valdymo priemonę.

- Apsaugokite savo prietaisus. Vartotojai turėtų apsaugoti savo prie interneto prijungtus ir mobiliuosius prietaisus, koduodami juose saugomus duomenis, nesinaudodami viešaisiais belaidžio interneto (WiFi) tinklais, naudodami virtualiuosius privačius tinklus (VPN) ir kovos su kenksminga programine įranga priemones. Apsauga nuo kenksmingos programinės įrangos turėtų būti įdiegta visuose prietaisuose.

5. Svarbi informacija

Daugiau informacijos apie tai, kaip galite apsisaugoti ir užkirsti kelią sukčiavimui, rasite mūsų svetainėje https://connectpay.com/security/

Apie įtartiną veiklą prašome visuomet informuoti bendrovę **„ConnectPay“** el. paštu security@connectpay.com.

Informacijos šaltiniai

„Javelin“ https://www.javelinstrategy.com/content/Javelin-2021-Identity-Fraud-Study
Sertifikuotųjų sukčiavimo tyrėjų asociacija (ACFE) https://www.acfe.com/covidreport.aspx &
2020 ACFE Report to the Nations
„PwC“ https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
„UK Finance“ https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf
Murray Goldstein straipsnis https://www.coxblue.com/4-ways-small-businesses-can-protect-themselves-from-cyber-attacks/