**Pranešimas žiniasklaidai**

2025 m. spalio 17 d.

**Susirašinėjimas su sukčiais įmonei kainavo 60 tūkst. eurų: ekspertas paaiškino, kaip nusikaltėliai pergudrauja verslus**

**Per pirmąjį šių metų pusmetį Lietuvoje užfiksuota beveik 8 tūkst. finansinio sukčiavimo atvejų, rodo Pinigų plovimo prevencijos kompetencijų centro duomenys. Tačiau vis dažniau nusikaltėliai taikosi ne į gyventojus, o į įmones – perimdami jų el. paštus ar susirašinėjimus. „Citadele“ banko plėtros vadovas Romas Čereška įspėja, kad tokie atvejai verslui kainuoja brangiausiai – vienas incidentas gali siekti kelias dešimtis tūkstančių eurų.**

**Iš telefoninių skambučių – į skaitmeninę erdvę**

Verslo aplinkoje sukčiavimo metodai keičiasi itin greitai – vietoje telefoninių skambučių vis dažniau pasitelkiami el. laiškai ar kiti skaitmeniniai kanalai, leidžiantys taikytis į didesnes sumas. Kaip pastebi R. Čereška, tradiciniai telefoniniai sukčiai, kurie anksčiau buvo dažniausias pavojus, šiandien sudaro tik mažą dalį visų bandymų.

„Šiandien vos 5 proc. sukčių bando veikti telefonu – beveik pusė jų persikėlė į skaitmeninę erdvę. Pavojingiausi atvejai – kai perimamas įmonių susirašinėjimas ir pakeičiami sąskaitų rekvizitai. Tokie sukčiai išnaudoja tai, ką verslai vertina labiausiai – pasitikėjimą ilgamečiais partneriais“, – aiškina R. Čereška.

Ekspertai atkreipia dėmesį, kad tokio tipo sukčiavimai dažnai sunkiai pastebimi – nusikaltėliai įsiterpia į realų verslo susirašinėjimą ir veikia itin subtiliai. Pavyzdžiui, neseniai „Citadele“ banko užfiksuotu atveju įmonė patyrė apie 60 tūkst. eurų nuostolį. Nusikaltėliai perėmė tiekėjo el. paštą, pakeitė sąskaitos rekvizitus ir taip nukreipė lėšas į savo sąskaitą.

„Įmonė, tikėdama, kad bendrauja su ilgamečiu partneriu, gavo pasiūlymą, susitarė dėl sąlygų ir apmokėjo sąskaitą. Tačiau tiekėjo el. pašto dėžutė jau buvo nulaužta – visi susirašinėjimai vyko su sukčiais. Tik nesulaukę prekių įmonės atstovai suprato, kad pinigai nukeliavo ne ten, kur turėjo“, – pasakoja R. Čereška.

**El. pašto perėmimai – finansiškai skaudžiausi**

Pinigų plovimo prevencijos kompetencijų centro duomenimis, vien per 2025 m. antrąjį ketvirtį finansiniai sukčiai iš gyventojų ir įmonių bandė išvilioti 19,4 mln. eurų, iš kurių daugiau nei 7 mln. eurų realiai pervesta į sukčių sąskaitas. Iš viso užfiksuota daugiau nei 4,5 tūkst. sukčiavimo atvejų, o daugiau nei pusę jų sudarė suklastoti SMS arba el. laiškai, vadinamieji fišingu (angl. *phishing*)*.*

Vis dėlto, kaip pabrėžia R. Čereška, pavojingiausi yra būtent tie atvejai, kai apgaulė vyksta tyliai ir išmaniai.

„El. pašto perėmimai fiksuojami rečiau, bet vidutinė žala vienam atvejui yra milžiniška – apie 30 tūkst. eurų. Tai reiškia, kad vienas sėkmingas įsilaužimas sukčiams atneša tiek pat, kiek šimtai smulkių atakų prieš gyventojus“, – teigia jis.

Remiantis centro duomenimis, el. pašto perėmimo atvejais per pirmą šių metų pusmetį įmonės prarado apie 900 tūkst. eurų, o vidutinė žala – auga: antrą ketvirtį palyginus su pirmuoju, suma padidėjo nuo 21 iki 30 tūkst. eurų. Tuo metu telefoninio sukčiavimo nuostoliai antrąjį ketvirtį siekė vidutiniškai 11,6 tūkst. eurų vienam atvejui, o suklastotų SMS ar el. laiškų – apie 780 eurų.

**Technologijos svarbios, bet viską lemia žmogaus budrumas**

Augant kibernetinių grėsmių mastui, verslai vis daugiau investuoja į saugumo sistemas, tačiau net ir pažangiausios technologijos neapsaugo nuo žmogiško neatidumo. Sukčiai vis dažniau taikosi ne į sistemas, o į žmones – siekia išprovokuoti skubotus sprendimus ar išnaudoti pasitikėjimą kolegomis ir partneriais.

Pasak R. Čereškos, techninės priemonės yra tik dalis sprendimo – didžiausią reikšmę turi kasdieniai įpročiai ir atsargumas.

„Techninės apsaugos priemonės yra būtinos, bet nepakankamos. Pavojingiausi atvejai įvyksta dėl žmogiškojo faktoriaus – kai neatidžiai patikrinamas laiškas ar skubant priimamas sprendimas. Todėl svarbiausia – įmonės vidinė disciplina ir budrumas, ypač kai kalbama apie pavedimus ar rekvizitų keitimą“, – pabrėžia R. Čereška.

Eksperto teigimu, sumažinti riziką padeda aiškios vidinės procedūros ir nuolatinis darbuotojų švietimas. Todėl rekomenduojama:

* visada atidžiai tikrinti el. paštu gautų sąskaitų rekvizitus ir, kilus abejonių, pasitikslinti duomenis patikimais kontaktais;
* naudoti dvigubą mokėjimų tvirtinimą, ypač apmokant dideles sumas, taip pat įdiegti automatinius įspėjimus, pavyzdžiui, jei vykdomas mokėjimas į naują ar neįprastą sąskaitą.
* įdiegti daugiafaktorę autentifikaciją (MFA) prisijungiant prie el. pašto, banko ir kitų svarbių sistemų;
* atkreipti dėmesį, ar suvesti sąskaitos duomenys sutampa su gavėjo vardu, pavarde ar įmonės pavadinimu – šią patikrą dabar automatiškai atlieka visos finansų įstaigos;
* nesidalinti prisijungimo duomenimis, nespausti įtartinų nuorodų ir interneto banką pasiekti tik per naršyklėje įvestą adresą;
* turėti aiškų incidentų valdymo planą – ką daryti ir su kuo susisiekti, jei įvyko sukčiavimo atvejis;
* reguliariai darbuotojams organizuoti mokymus ir simuliuoti kibernetines atakas, kad būtų išmokta jas laiku atpažinti.

„Ilgainiui veiksmingiausia gynyba – įmonės kultūra, kurioje kiekvienas supranta savo atsakomybę už organizacijos finansinį saugumą“, – sako R. Čereška.