**Pranešimas žiniasklaidai**

2024 m. kovo 21 d.

**Finansinių apgavysčių mastai auga: kieno naudai veikia dirbtinis intelektas – sukčių ar el. verslų?**

**Finansinės institucijos ir elektroninis verslas nuolat tobulina sistemų saugumą, aktyviai užsiima vartotojų informacinio raštingumo edukacija, o auganti dirbtinio intelekto (DI) pažanga sparčiai prisideda prie inovatyvių verslo sprendimų. Tačiau nepaisant technologinio tobulėjimo, 2023 metais finansinių sukčių aktyvumas augo trečdaliu, rodo Pinigų plovimo prevencijos kompetencijų centro duomenys. Ekspertai pasidalino, kokiais būdais sukčiai apgavystėms pasitelkia DI, ir atskleidė, kaip galima jiems sutrukdyti.**

**Klonuoja balsą, žino, kur apsipirkinėjote**

Nors, anot Citadele“ banko Baltijos šalių lėšų valdymo ir prekybos finansavimo tarnybos vadovo Romo Čereškos, bankinio sukčiavimo atvejų lygis Baltijos šalyse, palyginti su kitomis valstybėmis, yra labai žemas, pastaruoju metu vyksta sukčiavimo transformacija iš analoginio į skaitmeninį. Anksčiau sukčiai skambindavo apsimesdami giminaičiais ar parduotuvės atstovais ir prašydavo pervesti pinigų į banko sąskaitą. Dabar dažniau bandoma pasisavinti asmens duomenis, siekiant turėti pilną prieigą prie žmogaus banko paskyros, kad jo vardu būtų galima vykdyti mokėjimus.

„Tobulėjant DI, ateityje atskirti sukčių atsiųstą žinutę ar laišką gali tapti vis sunkiau. Nėra taip, jog sukčiai individualiai rašo kiekvieną el. laišką. Jie taip pat turi susikūrę įvairių savo sistemų, kurios padeda kurti bei valdyti informaciją, kad ji atrodytų kuo tikroviškesnė“, – sako R. Čereška.

Lietuvos dirbtinio intelekto asociacijos valdybos narys dr. Paulius Pakutinskas taip pat antrina, kad **metodų sukčiams pasitelkti DI yra labai daug. Jis gali būti naudojamas, pavyzdžiui, balso klonavimui, skambinant ir žinomo žmogaus balsu pasakant, kad kažką laimėjote.**

**„Dauguma atvejų sukčiai yra ne lietuviai, tad jiems reikia savo žinutes išversti į lietuvių kalbą, taigi net gerai tekstą išverčiančios vertimo programėlės gali būti sukčių nusikaltimo grandinės dalimi. Jie gali adaptuoti žinutes pagal šalį, pasveikinti su vykstančia nacionaline švente ir pakviesti pasijungti kažkur ir ką nors tariamai laimėti. Arba pagal tam tikrą tikimybę gali apskaičiuoti, kad greičiausiai apsipirkinėjote tam tikrame prekybos tinkle ir atitinkamai suformuluoti žinutę: „Sveikiname apsipirkus pas mus, jūs laimėjote X, spauskite nuorodą ir atsiimkite prizą“,** – **sukčių metodais dalinasi P. Pakutinskas.**

Anot, siuntų pristatymo bendrovės „DPD“ IT saugumo vadovo Baltijos šalims Martyno Miškinio, kai DI tapo prieinamas praktiškai visiems fiziniams gyventojams, jo panaudojimo sritys ne tik suteikė daugiau supratimo visuomenei, kas tai yra, bet ir įgalino daugiau įrankių sukčiams. Pastarieji naudojasi gerai žinomais prekiniais ženklais ir imituoja jų komunikaciją, siekdami išvilioti pinigų.

„Su sukčiais tenka susidurti nuolat, tačiau lyginant su praeitais metais jų aktyvumas sumažėjęs. Tačiau tendencija kitą mėnesį jau gali būti kitokia. Pastebime, kad sukčių laiškai tobulėja, tiek dizaino tiek turinio prasme. Paskutiniai įdomesni bandymai – kenkėjiška nuoroda QR kode”, – teigia M. Miškinis.

**Pasprukti nuo sukčių – įmanoma**

Anot „Citadele“ banko atstovo,svarbu suprasti, kad dažniausiai sukčiavimo atvejai įvyksta ne dėl banko ar el. parduotuvės sistemos „nulaužimo“ ar sisteminių spragų, o dėl žmogaus patiklumo sukčiaus melagystėmis, kai atliekami prašomi veiksmai – mokėjimai, suteikiami prisijungimo duomenys. Tokiais atvejais atsiimti prarastas lėšas pavyksta ne visuomet.

„Kai klientas atsiskaito bankiniu pavedimu ar mokėjimų inicijavimu, pinigai pervedami iškart ir juos sunku susigrąžinti. Tačiau jei mokėjimas įvykdytas kortele, suvedant jos duomenis, pinigai nėra pervedami tą pačią minutę – dažniausiai gavėjas pinigus gauna per parą. Tai solidus laiko tarpas, per kurį galima suprasti, kad įvyko sukčiavimas, ir sustabdyti mokėjimą. Be to, galima pasinaudoti „VISA“ ar „Mastercard“ kortelių apsauga ir susigrąžinti prarastus pinigus“, – pasakoja R. Čereška.

Nors sukčių sėkmė didžiąją dalimi pačių vartotojų rankose, elektroninėms parduotuvėms paslaugas teikiantys bankai užtikrina mokėjimo dalies saugumą, diegia įvairias papildomą saugumą užtikrinančias schemas, pavyzdžiui, vadinamąją dviejų faktorių autentifikaciją. Šį apsaugos metodą galima naudoti keliais būdais: gaunant kodą SMS žinute, per specialias programėles ir panašiai.

„Turime automatizuotus procesus kurie, atpažinę įtartinus pervedimus, juos stabdo. Pavyzdžiui, jei ką tik atsiskaitėte Lietuvoje, o po penkių minučių – JAV, sistema fiksuoja, kad tai per trumpas laiko tarpas atsidurti kitame žemyne, ir mokėjimą sustabdo“, – pasakoja R. Čereška.

M. Miškinis taip pat teigia, kad verslas klientų duomenų saugumo užtikrinimui naudoja naujausias saugumo priemones, tinklo srautų analizes ir DI sprendimus, kurie analizuoja saugumo įvykius IT įrenginiuose.

 „Skelbiame viešus pranešimus internete, soc. tinkluose aiškiname vartotojams, kaip atpažinti sukčius. Techniškai juos identifikuojame, tačiau galimybių operatyviai blokuoti nuorodas neturime”, – pasakoja siuntų pristatymo bendrovės atstovas.

Lietuvos dirbtinio intelekto asociacijos valdybos narys teigia, kad **terpė naudoti DI, siekiant užkirsti kelią sukčiams yra labai didelė – DI gali analizuoti tam tikras anomalijas, kibernetinio saugumo specialistai gali stebėti neatitikimus.**

**„Mobiliojo ryšio operatorių galimybės ribojamos įstatymų, jie negali kištis į turinį, tačiau dabar yra visiškai šviežias reguliavimas, kuris leidžia operatoriams nepraleisti žinučių, turinčių atitinkamų požymių.** Reikia džiaugtis, kad šiuo metu Europos Sąjungoje yra priimta eilė norminių aktų. Vienas svarbesnių yra Tinklų ir informacinių sistemų direktyva (TIS 2), kuri kelia labai aukštus įpareigojimus valdyti kibernetines rizikas svarbiose veiklos srityse ir tai kelia bendrą kibernetinio saugumo lygį šalyse**“, – pasakoja ekspertas.**

**Pagrindinis ginklas – informacinis raštingumas**

Kartu su tobulėjančiu DI sukčių rengiamos atakos ateityje atrodys vis tikroviškiau, tad anot R. Čereškos, itin svarbu didinti žmonių informacinio raštingumo lygį.

„Net pati saugiausia saugumo sistema negali apsaugoti 100 proc., jei žmogus leidžiasi apgaunamas. Turime kritiškai vertinti informaciją. Paprasčiausias patarimas – jeigu nesate įsitikinę ar nuoroda yra tikra, nespauskite ant jos“, **–** pataria banko ekspertas.

P. Pakutinskas įvardija dar vieną taisyklę – netikėti per gerais pasiūlymais – jei jis atrodo per geras, tai greičiausiai yra netiesa.

„Sukčių metodikų yra labai sofistikuotų. Pavyzdžiui, jei užvaldė bei perėmė jūsų komunikaciją su partneriais ir iš jūsų labai skubiai reikalauja apmokėti sąskaitą, kai terminas, iš tikrųjų yra mėnesio pabaigoje, gal verta paimti telefoną ir paskambinti tos įmonės buhalterei ir paklausti kas čia įvyko, ar tikrai taip skubu? Taip pat, tokie dalykai, kaip atsiskaitomosios sąskaitos numerio pakeitimas versle turėtų kelti didelį šauktuką. Net jei sąskaita apmokėjimui gauta iš tinkamo adresato, bet yra atsiskaitomosios sąskaitos numerio pakeitimas ir tada raginama skubiai apmokėti ar įtarimą kelia kiti nebūdingi veiksmai verta patikrinti situaciją alternatyviais būdais, nebepasitikėkite tuo elektroninio pašto adresu iš kurio gavote sąskaitas“, **–** teigia P. Pakutinskas.