**Kova su sukčiais – bankų kasdienybė: ko nemato klientai?**

**Apie sukčius, iš gyventojų išviliojančius įvairias pinigų sumas, pranešama kone kasdien. Viešojoje erdvėje galima rasti daugybę įspėjimų ir patarimų žmonėms, kaip nuo šių aferų apsisaugoti. Vis tik, skaičiuojant statistiškai, tiesiogiai su sukčiais susiduria palyginti nedidelė visuomenės dalis. Bet yra viena žmonių grupė, su šiomis grėsmėmis kovojanti kasdien, kiekvieną darbo minutę. Tai – bankų bei kitų finansinių įstaigų pinigų plovimo, sukčiavimo prevencijos ir IT specialistai.**

Ekspertų vertinimu, kasmet sukčių aukomis visame pasaulyje tampa virš 600 milijonų žmonių. Bendra iš jų išviliota suma pastaruosius dvejus metus viršijo po trilijoną JAV dolerių kasmet. Kibernetinių grėsmių nuolat daugėja, jos tampa rafinuotesnės, o nusikaltėliai randa vis naujų būdų pasiekti aukas.

„Pagrindinės kibernetinių atakų ir finansinių sukčiavimų schemos mūsų šalyje žengia koja kojon su pasaulinėmis tendencijomis. Naudojamos tokios socialinės inžinerijos formos kaip „phishing“ (suklastoti el. laiškai), „smishing“ (suklastotos SMS žinutės), „vishing“ (skambučiai apsimetant institucijų atstovais), o pastaruoju metu daugėja ir „quishing“ atvejų – tai QR kodais pagrįstas sukčiavimas“, – pagrindines grėsmes vardija „Urbo“ banko Pinigų plovimo ir sukčiavimo prevencijos departamento direktorius Petras Gotautas.

Pasak jo, sukčiavimo schemose vis dažniau naudojamas ir dirbtinis intelektas (DI), kuris sparčiai mokosi generuoti itin kokybišką, taisyklingą tekstą, todėl nyksta kalbiniai sukčiavimo ženklai, kurie anksčiau padėdavo gana lengvai identifikuoti grėsmes.

**DI – ne tik priešininkas, bet ir pagalbininkas**

Sukčiams nuolat stengiantis įsisavinti naujausias technologijas, kitoje barikadų pusėje esančios finansų institucijos daro tą patį.

„Saugant žmonių pinigus, DI padeda greitai išanalizuoti milijardus skirtingų duomenų bei pastebėti net ir pačius subtiliausius nukrypimus nuo įprastų konkretaus kliento veiksmų. Pavyzdžiui – prisijungimo prie elektroninės bankininkystės vietos, įrenginio tipo, IP adreso, biometrinių duomenų, mokėjimo įpročių ir t. t. Kitaip tariant, realiuoju laiku taikomas dirbtinis intelektas leidžia operatyviai atpažinti įtartinus mokėjimus, reikalaujančius papildomos peržiūros“, – pasakoja P. Gotautas.

Jis priduria, jog sukčiavimo prevencijos sistemos su integruotu DI veikia ne tik pagal iš anksto nustatytus scenarijus, bet ir nuolat mokosi bei prisitaiko prie naujų aplinkybių. Ši jo savybė, pasak specialisto, leidžia greitai identifikuoti ne tik jau žinomus, bet ir visiškai naujus rizikingus elgsenos modelius.

**Vien robotai saugumo neužtikrins**

Nepaisant spartaus technologijų vystymosi, esminį vaidmenį kovoje su finansiniais nusikaltimais ir toliau atlieka žmonės.

„Kibernetinių atakų ir sukčiavimo pavojų stebėsena banke nenutrūksta nė minutei. Žinoma, ne darbo valandomis šią užduotį atlieka ir prevenciją užtikrina automatinės IT sistemų užkardos, tačiau užfiksavus grėsmę, į procesą bet kuriuo paros metu įsijungia atsakingi darbuotojai“, – sako P. Gotautas.

Pasak jo, ekspertų įvertinimui nukreipiamas kiekvienas rimtesnis automatinių sistemų įspėjimas. Tuomet jau žmonės atlieka išsamius tyrimus, nustato konkrečią sukčiavimo schemą, surenka duomenis apie nusikaltėlių veikimo būdus ir visą informaciją perduoda teisėsaugos institucijoms.

P. Gotautas pabrėžia, jog svarbus sukčiavimo prevencijos įrankis yra ir aktyvus klientų įsitraukimas.

„Mes be išimčių patikriname ir įvertiname kiekvieną atvejį, apie kurį praneša klientas – net jei jis iš pirmo žvilgsnio atrodo nereikšmingas. Būtent iš realios žmonių patirties operatyviai sužinome apie naujus sukčiavimo metodus ir galime patobulinti savo algoritmus, kad jie greičiau ir tiksliau atpažintų tokius atvejus ateityje“, – aiškina ekspertas.

**Iššūkių netrūksta**

Nepaisant daugybės kasdienių pergalių užkardant nusikalstamas veiklas, bankai vis dar susiduria ir su reikšmingais iššūkiais. Vienas jų – nepakankamas keitimasis duomenimis apie sukčius ir jų veiklą tarp skirtingų finansų įstaigų. Pasak P. Gotauto, bendra duomenų bazė bendroje Europos mokėjimų eurais erdvėje (angl. Single Euro Payments Area – SEPA) galėtų ženkliai prisidėti prie greitesnės prevencijos ir sukčiavimo atvejų aptikimo.

„Kol tokio sprendimo nėra, Lietuvos finansų institucijos glaudžiai bendradarbiauja per Pinigų plovimo prevencijos kompetencijų centrą, dalijasi informacija apie visas grėsmes bei rizikas“, – sako P. Gotautas.

Norint apsisaugoti nuo klaidų ar atrasti saugumo spragas, banke periodiškai atliekami saugumo sistemų testai, įskaitant ir vadinamuosius „simuliacinius išpuolius“.

„Tai – tarsi virtualios grėsmės, kuriomis siekiama išbandyti, kaip sistema reaguoja į potencialų sukčiavimą, ar sugeba jį laiku identifikuoti ir ar negeneruoja per daug klaidingų įspėjimų. Tokie testai ne tik padeda tobulinti algoritmus, bet ir atskleidžia konkrečius sistemos pažeidžiamumus“, – pasakoja „Urbo“ ekspertas.

Pasak jo, sistemos efektyvumas vertinamas ne rečiau kaip kartą per metus, tačiau bet kokie veikimo trūkumai ar nepakankamas tikslumas koreguojami nedelsiant, vos juos pastebėjus.

**Kasdienis, niekada nesibaigiantis darbas**

Dar vienas svarbus aspektas, pasak specialisto, yra banko darbuotojų saugumo kultūra.

„Dirbantieji su jautriais klientų duomenimis privalo laikytis griežtų vidinių protokolų, reguliariai dalyvauti mokymuose ir išlaikyti žinių patikrinimus. Tai padeda sumažinti žmogiškųjų klaidų, galinčių tapti potencialiu įsilaužimo tašku, riziką“, – sako P. Gotautas.

Ne paskutinėje vietoje, pasak eksperto, ir ilgalaikės strategijos svarba.

„Kibernetinis saugumas nėra ir negali būti statiškas – tai nuolat besikeičianti aplinka. Tad ir mūsų tikslas nėra pasiekti kažkokį galutinį tašką, o nuolat tobulinti technologijas, organizacinius procesus ir specialistų kompetencijas. Tai – kasdienis, nesibaigiantis darbas“, – apibendrina P. Gotautas.

**Daugiau informacijos:**Beatričė Mikšytė  
+370 635 37 649  
[beatrice@ideaprima.lt](mailto:beatrice@ideaprima.lt)