**Pranešimas žiniasklaidai**

**2023 m. rugsėjo 21 d.**

**Kokiu laikotarpiu galima tikėtis kibernetinių atakų aktyvumo?**

**Tarptautiniai bendrovės „Astra Security“ duomenys rodo, kad per dieną įvykdoma daugiau nei 2 tūkst. kibernetinių įsilaužimų, kurie pasikartoja kas 39 sekundes. Prasidėjus sėslesniam rudens sezonui daugelis dėl darbų ir mokslų aktyviau naršo internete, o tai atveria platesnes galimybes kibernetiniams nusikaltėliams. Ekspertų teigimu, sukčių aktyvumas kinta ne tik keičiantis sezonams, bet ir reikšmingų įvykių metu.**

**Įtaką daro visuomenėje svarbūs įvykiai**

Kibernetinio saugumo ekspertų asociacijos vadovė ir „Women4Cyber Lietuva“ bendruomenės narė Renata Karpavičė sako, kad nors sukčių aktyvumas dažnai siejamas su prasidedančiu šventiniu sezonu, dažniausiai kibernetinių atakų pagausėjimą galima išvysti visuomenėje vykstant svarbiems įvykiams.

Kibernetinių nusikaltimų kiekiai padidėja ne tik rudenį, kai potencialiu taikiniu tampa studentai ir moksleiviai, bet ir kalėdiniu ar pajamų deklaravimo metu. Tokiais laikotarpiais fiktyvių pranešimų srautas būna didžiausias. Dažniausiai tai būna pranešimai, susiję su netikromis internetinėmis parduotuvėmis, siuntomis, netikromis finansų institucijų svetainėmis siekiant išvilioti el. bankininkystės duomenis. Taip pat fiktyvūs pranešimai gali ateiti ir valstybinių institucijų ar labdaros tikslais sukurtų organizacijų vardu.

„Pavyzdžiui, policijos vardu gaunami pranešimai daugiausia būna apie nesumokėtas baudas. Jei policija ar kita valstybinė institucija sukuria naują elektroninę paslaugą, sukčiai dažnai ieško būdų, kaip tuo pasinaudoti ir išvilioti asmeninius duomenis iš gyventojų. Tai buvo nutikę ir karo fone, siekiant pasinaudoti žmonių gerumu, kai buvo sukurta daugiausia netikrų labdaros fondų“, – pasakoja R. Karpavičė.

**Prarastus pinigus susigrąžinti įmanoma**

Nors kibernetinėms atakoms rengti pasitelkiami skirtingi metodai, visų jų tikslas išlieka tas pats – pasisavinti asmeninius arba mokėjimo duomenis. Romas Čereška, „Citadele“ banko Baltijos šalių lėšų valdymo ir prekybos finansavimo tarnybos vadovas, sako, kad internetiniai nusikaltėliai tiesiogiai įsilaužti į banko sistemas kol kas nebando.

„Dažniausiai sukčiai kuria svetaines, kurios labai panašios į bankų ar kitų institucijų, tačiau jose veikia tik nuorodos, kurias nuspaudus kyla rizika atskleisti asmeninius duomenis. Visos kitos nuorodos dažnai neveikia“, – paaiškina R. Čereška.

Anot jo, reikia atkreipti dėmesį į atidaromo puslapio adresą, jei kyla įtarimas, rekomenduojama jungtis prie savo banko sau įprastais būdais – per programėlę ar interneto naršyklę. Taip pat sukčius galima atpažinti iš skubinimo atlikti veiksmą.

Jeigu kibernetinė ataka vis dėlto įvyko ir apsisaugoti iš anksto nepavyko, reikėtų kreiptis į savo banką ir tuomet apie incidentą informuoti e. policiją. Kartu apie įvykusią ataką galima pranešti ir Nacionaliniam kibernetinio saugumo centrui, kur panaši informacija renkama, siekiant matyti bendrą kibernetinių incidentų aktyvumą.

„Jei suvedus asmeninius duomenis supratote, kad tai buvo sukčių pranešimas, pirmiausia reikia kreiptis i banką ir keisti banko prisijungimus, slaptažodžius, blokuoti turimas korteles. Bankai gali padėti susigrąžinti prarastus pinigus, jei buvo mokėta kortele arba kai kuriais atvejais tarpininkauti su kitais bankais, siekiant žmogui sugrąžinti pervedimo metu prarastą sumą“, – pataria „Citadele“ banko atstovas.

**Sukčiai manipuliuoja jausmais**

Kadangi tobulėja kibernetinių nusikaltimų aptikimo ir gynybos techniniai sprendimai, kibernetiniai nusikaltėliai ypač aktyviai savo atakoms ir sukčiavimo schemoms pasitelkia socialinę inžineriją (angl. social engineering). Tai būdas, kuriuo sukčiai atakų metu manipuliuoja žmonėmis.

R. Karpavičė priduria, kad tokioms atakoms sukčiai ruošiasi labai kompleksiškai. Pavyzdžiui, prie atakų, kuriomis siekiama sutrikdyti tam tikrų paslaugų tiekimą (angl. DDoS attack), kai kuriais atvejais prisideda ir visiškai nesusiję pašaliniai asmenys. Sukčiai, manipuliuodami ideologiniais įsitikinimais, gali kviesti prisidėti prie atakų asmeniui leidžiant panaudoti jo kompiuterį masinėje atakoje. Viena duomenų nutekinimo ataka gali lengvai materializuotis į investicinio sukčiavimo scenarijus.

**Papildoma informacija:**

Aurelija Grikinaitė-Čepėnienė

Korporatyvinės komunikacijos vadovė Lietuvoje

„Citadele“ bankas

[aurelija.grikinaite-cepeniene@citadele.lt](mailto:aurelija.grikinaite-cepeniene@citadele.lt)

[www.citadele.lt](http://www.citadele.lt)