**„Microsoft“ skaitmeninės gynybos ataskaita 2025: daugiau nei pusė kibernetinių atakų susijusios su išpirkos reikalavimais ir šantažu**

*Kibernetinio nusikalstamumo apimtys. Kodėl Baltijos šalys turi išlikti žingsniu priekyje*

**2025 m. spalio 17 d., Vilnius** – „Microsoft“ pristatė naujausią skaitmeninės gynybos ataskaitą ([Microsoft Digital Defense Report 2025](https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025?msockid=3043950b234760192cb984bd274766c4)), kurioje atskleidžiama, jog daugiau nei 52 proc. kibernetinių atakų, kurių motyvai buvo nustatyti, yra susijusios su šantažu ir išpirkos reikalavimais (angl. *extortion and ransomware*), o šnipinėjimas sudaro tik 4 proc. Šiuo metu išpuolius dažniausiai vykdo finansinės naudos siekiantys nusikaltėliai, o ne valstybių remiami veikėjai. 80 proc. atvejų kibernetinių atakų tikslas buvo duomenų vagystė – tai rodo, kad grėsmė yra universali.

**Kibernetinio nusikalstamumo apimtys: grėsmių skaičius**

Kiekvieną dieną „Microsoft“ apdoroja daugiau nei 100 trilijonų signalų, blokuoja apie 4,5 mln. naujų kenkėjiškų programų atakų, analizuoja maždaug 38 mln. įtartinos tapatybės atvejų ir nuskenuoja apie 5 mlrd. el. laiškų, ieškodama kenkėjiškų priedų ir sukčiavimo grėsmių. Procesų automatizavimas ir lengvai prieinami kibernetinio nusikalstamumo įrankiai leidžia nusikaltėliams vykdyti masines, globalias operacijas, o dirbtinis intelektas (DI) spartina sudėtingo ir įtikinamo turinio, naudojamo šios operacijose, kūrimą.

Ataskaitoje pabrėžiama, kad kibernetinis saugumas yra strateginis prioritetas, o ne vien informacinių technologijų (IT) srities rūpestis. Verslo vadovai turi užtikrinti, kad saugumas būtų integruotas į kiekvieną skaitmeninės transformacijos etapą.

**Užpuolikai nesnaudžia**

Pačios kompanijos duomenys rodo, kad pirmoje šių metų pusėje Lietuva pagal nusikalstamo kibernetinio aktyvumo dažnumą ir poveikį „Microsoft“ klientams užėmė 53-ią vietą pasaulyje, Estija – 63-ią, o Latvija – 64-ą.

„Džiugina, kad nė viena iš trijų Baltijos šalių nepatenka tarp labiausiai kibernetinio aktyvumo paveiktų valstybių. Tačiau užpuolikai nesnaudžia – jie sparčiai įsisavina naujausias technologijas, įskaitant dirbtinį intelektą, kad tobulintų savo metodus“, – sako Renate Strazdina, „Microsoft“ Šiaurės Europos šalių regiono technologijų skyriaus vadovė.

Pasak jos, taikiniais vis dažniau tampa ne tik vyriausybinės institucijos, bet ir mažos bei vidutinės įmonės.

„Be finansinės naudos siekiančių nusikaltėlių, vis dažniau tokias atakas vykdo ir priešiškai nusiteikusių valstybių remiami veikėjai. Besikeičianti grėsmių aplinka reiškia, kad kibernetinis saugumas ir investicijos į jį turi išlikti mūsų visų prioritetu. Bendradarbiaudamos ir išlaikydamos budrumą, Baltijos šalys ne tik gali pačios atsispirti šioms grėsmėms, bet ir tapti pavyzdžiu visam regionui“, – kalba R. Strazdina.

**Atakų taikiklyje – kritinės svarbos paslaugos**

Ligoninės, mokyklos ir savivaldos institucijos vis dažniau tampa taikiniais dėl jautrių duomenų ir ribotų saugumo išteklių. Tokių atakų pasekmės gali būti vėluojanti medicininė pagalba, sutrikęs švietimo procesas ar net paralyžiuotas susisiekimas. Nusikaltėliai išnaudoja šiuos pažeidžiamumus, nes minėtų sektorių atstovai dažniau linkę operatyviai sumokėti išpirką, kad atnaujintų gyvybiškai svarbią veiklą.

„Microsoft“ skaitmeninės gynybos ataskaitoje taip pat pabrėžiama, kad pasenusios saugumo priemonės nebeatitinka šiuolaikinių grėsmių. Efektyvi gynyba nuo kibernetinių atakų reikalauja modernizavimo ir glaudaus bendradarbiavimo tarp valdžios institucijų ir verslo organizacijų. Individualiems vartotojams rekomenduojama naudoti daugiapakopį tapatybės patvirtinimą (angl. *multi-factor authentication, MFA*), kuris gali užkirsti kelią daugiau nei 99 proc. netikros tapatybės pagrindu (angl. *phishing*) vykdomų atakų.

**Išlieka ir priešiškų valstybių remiamos grėsmės**   
Nors didžiąją dalį kibernetinių nusikaltimų vykdo finansinės naudos siekiantys nusikaltėliai, priešiškai nusiteikusių valstybių remiami veikėjai taip pat taikosi į svarbiausius šalių sektorius ir regionus – daugiausia ekonominio šnipinėjimo, rečiau – finansinės naudos tikslais:

* **Kinija** plečia atakas prieš įvairius verslo sektorius ir nevyriausybines organizacijas (NVO), pasinaudodama pažeidžiamais įrenginiais.
* **Iranas** atakuoja logistikos bendroves Europoje ir Persijos įlankoje, tikėtina, siekdamas trikdyti komercinį transportą.
* **Rusija** atakuoja ne tik Ukrainą, bet ir įmones NATO šalyse – ypač mažesnes, pasinaudodama jomis kaip „vartais“ į didesnes organizacijas ir struktūras.
* **Šiaurės Korėja** Pagrindinį dėmesį skiria finansinei naudai ir šnipinėjimui, įskaitant ir užsienyje dirbančius IT specialistus, kurie režimą remia ir savo uždirbtais pinigais.

**Dirbtinis intelektas – ir grėsmė, ir privalumas**

Tiek nusikaltėliai, tiek kibernetinių atakų gynybos specialistai vis dažniau pasitelkia ir dirbtinį intelektą. Pirmieji jį naudoja masinėms, automatizuotoms sukčiavimo kampanijoms ir netikros informacijos ar turinio kūrimui, o antrieji – saugumo spragų aptikimui ir vartotojų apsaugai.

**Kibernetinis saugumas – bendra atsakomybė**

Grėsmėms sudėtingėjant, organizacijos turi nuolat atnaujinti savo gynybos priemones ir dalintis žvalgybine informacija. Šalių vyriausybės turi sukurti aiškias atsakomybės sistemas, kurios užtikrintų realias pasekmes už kenkėjišką veiklą ir skatintų skaidrumą. „Microsoft“ savo ruožtu saugumą stiprina per „Saugios ateities iniciatyvą“ ([Secure Future Initiative](https://www.microsoft.com/en-us/trust-center/security/secure-future-initiative?msockid=3043950b234760192cb984bd274766c4)) ir pasaulinį bendradarbiavimą.

Skaitmeninei transformacijai spartėjant – ypač dėl DI plėtros – kibernetinės grėsmės vis labiau veikia ekonominį stabilumą, visuomenės pasitikėjimą ir asmeninį kiekvieno iš mūsų saugumą. Šių iššūkių sprendimui reikia ne tik technologinių inovacijų, bet ir bendrų, koordinuotų visuomenės pastangų.

\*\*\*

Kontaktas žiniasklaidai:

Beatričė Mikšytė

+370 635 37 649

beatrice@ideaprima.lt