Microsofti küberkaitse raport: üle poole rünnakutest Baltimaades on seotud väljapressimise ja lunavaraga

6 kuud tagasi - 18.10.2025 Autor: AM

Renate Strazdina, Microsofti Põhja-Euroopa klastri tehnoloogiajuht.

Microsoft on värskelt kergitanud katet digitaalse kuritegevuse tegelikult palgelt ning pilt, mis avaneb, ei räägi niivõrd spionaažist, kuivõrd külmast, kalkuleerivast rahahimust.

Rahamasin nimega lunavara

Microsofti värske digitaalkaitse raport (*Microsoft Digital Defense Report*) lööb lauale kainestavad faktid. Kui vaadata teadaoleva motiiviga küberründeid, siis lausa üle 52% neist on seotud väljapressimise ja lunavaraga: kurjategijad tungivad süsteemi, krüpteerivad (lukustavad) seal elutähtsad failid ning nõuavad nende vabastamise eest kopsakat lunaraha.

Võrdluseks, klassikaline luuretegevus moodustab teadaolevatest rünnetest vaid närused 4%. Tänased küberhundid on valdavalt finantskasu jahtivad kriminaalid, mitte riikide poolt toetatud salaagendid.

Ja see puudutab absoluutselt kõiki. Raporti kohaselt on 80% juhtudest ründe eesmärgiks andmete vargus. Isikuandmed, kliendiandmebaasid, ärisaladused – see kõik on mustal turul kuum kaup.

Selle rünnakutelaviini ulatus on hoomamatu. Microsoft töötleb iga päev üle 100 triljoni signaali. See on kosmiline number, mille toel tõrjutakse umbes 4,5 miljonit uut pahavara levitamise katset, analüüsitakse 38 miljonit identiteediriski ja kontrollitakse 5 miljardit e-kirja.

Ründajate töö on nüüd muutunud õõvastavalt lihtsaks. Automatiseerimine ja kergesti kättesaadavad küberkuritegevuse tööriistad tähendavad, et rünnata saab mastaapsemalt kui kunagi varem ja ilma eriliste oskusteta.

Lisaks on mängu tulnud tehisintellekt, mis aitab meisterdada üha usutavamaid õngitsuskirju ja keerukamat ründekoodi, mis pääseb traditsioonilistest

kaitsemeetmetest mööda.

Raport saadab ettevõtete juhtkondadele karmi, kuid selge sõnumi: küber-turvalisus pole enam ammu pelgalt IT-osakonna peavalu, vaid strateegiline juhtimisprioriteet. Turvalisus tuleb lõimida iga digitaalse muutuse ja äriprotsessi südamesse.

Balti riigid: rahulik pind, sügav sisu

Kus asub selles globaalses tormis Eesti? 2025. aasta esimese poole andmetel paigutus Eesti küberkuritegevusest mõjutatud riikide seas 63. kohale. Meie naabrid Läti ja Leedu olid vastavalt 64. ja 53. kohal.

“On julgustav näha, et ükski kolmest Balti riigist ei kuulu enim mõjutatud riikide hulka. Samas, ründajad ei puhka – nad kasutavad kiiresti ära uusimaid tehnoloogiaid, sealhulgas tehisintellekti,“ sõnas **Renate Strazdina**, Microsofti Põhja-Euroopa klastri tehnoloogiajuht.

Strazdina juhib tähelepanu murettekitavale trendile: “Näeme muutust, kus üha enam on sihikul lisaks valitsustele, ka väiksed ja keskmised ettevõtted, seda sageli isegi riiklike ründajate poolt. See areng tähendab, et peame kõik jätkuvalt panustama küberjulgeolekusse. Ühise koostöö ja valvsuse abil saavad Balti riigid jääda vastupidavaks ja olla eeskujuks kogu piirkonnale.“

Haavatavad sihtmärgid: haiglad ja koolid

Küberründajad teavad, kust hammustada. Üha sagedamini satuvad rünnaku alla just elutähtsad teenused – haiglad, koolid ja kohalikud omavalitsused. Nende käes on äärmiselt tundlikke andmeid, kuid asutuste küberkaitse võimekus on sageli piiratud.

Tagajärjed on kohutavad: viibiv arstiabi, häiritud haridussüsteem või seisakud transpordis. Lunavararündajad teavad, et need sektorid on süsteemide taastamise eest valmis maksma kiiresti, sest kaalul on inimeste heaolu ja turvalisus.

Riiklikud varjud tegutsevad edasi

Kuigi enamik rünnakuid on rahalise motiiviga, ei ole riiklikult toetatud ründajad kuhugi kadunud. Nemad sihivad endiselt võtmesektoreid, peamiselt luureandmete või majandusliku kasu eesmärgil, kirjutab Microsofti raport.

- **Hiina** laiendab varjatult ründeid erinevate tööstuste ja MTÜ-de vastu, kasutades varjatud ligipääsuks sageli nõrgalt kaitstud võrguseadmeid.
- **Iraan** ründab Euroopa ja Pärsia lahe logistikaettevõtteid, tõenäoliselt eesmärgiga häirida kaubaliiklust.
- **Venemaa** on laiendanud ründeid Ukrainast kaugemale, võttes sihikule eriti just väikeste NATO-riikide ettevõtteid, kasutades neid väravatena suuremate organisatsioonide süsteemidesse pääsemiseks.
- **Põhja-Korea** keskendub rahalisele kasule ja luurele, saates oma IT-töötajaid välismaale tööle, et nende teenistus režiimi toetuseks suunata.

Mida teha? Üks lahendus on peaaegu lollikindel

Vananenud turvameetmetest enam ei piisa, kuid üks lahendus on tavakasutaja jaoks ülitõhus.

Microsofti raport kinnitab, et üle 99% identiteedirünnakutest saab ennetada mitmetasemelise autentimise (MFA) abil.

MFA on lihtsustatult nagu kaheastmeline lukk digitaalsel uksel. Lisaks paroolile (mida on lihtne varastada) vajatakse sisselogimiseks ka teist tõendit – näiteks koodi oma telefonirakendusest või sõrmejälge. See lihtne lisasamm muudab konto kaaperdamise ründaja jaoks eksponentsiaalselt keerulisemaks. Eriti tõhus on just andmepüügi-kindel MFA.

Küberjulgeolek on tehisintellekti ajastul muutunud kahe teraga mõõgaks: ründajad kasutavad AI-d rünnakute lihvimiseks, kaitsjad aga ohtude kiiremaks avastamiseks. See on pidev võidujooks, kus osalevad kõik.

- Uudised

- Tarkvara
- Turvalisus

Pilt