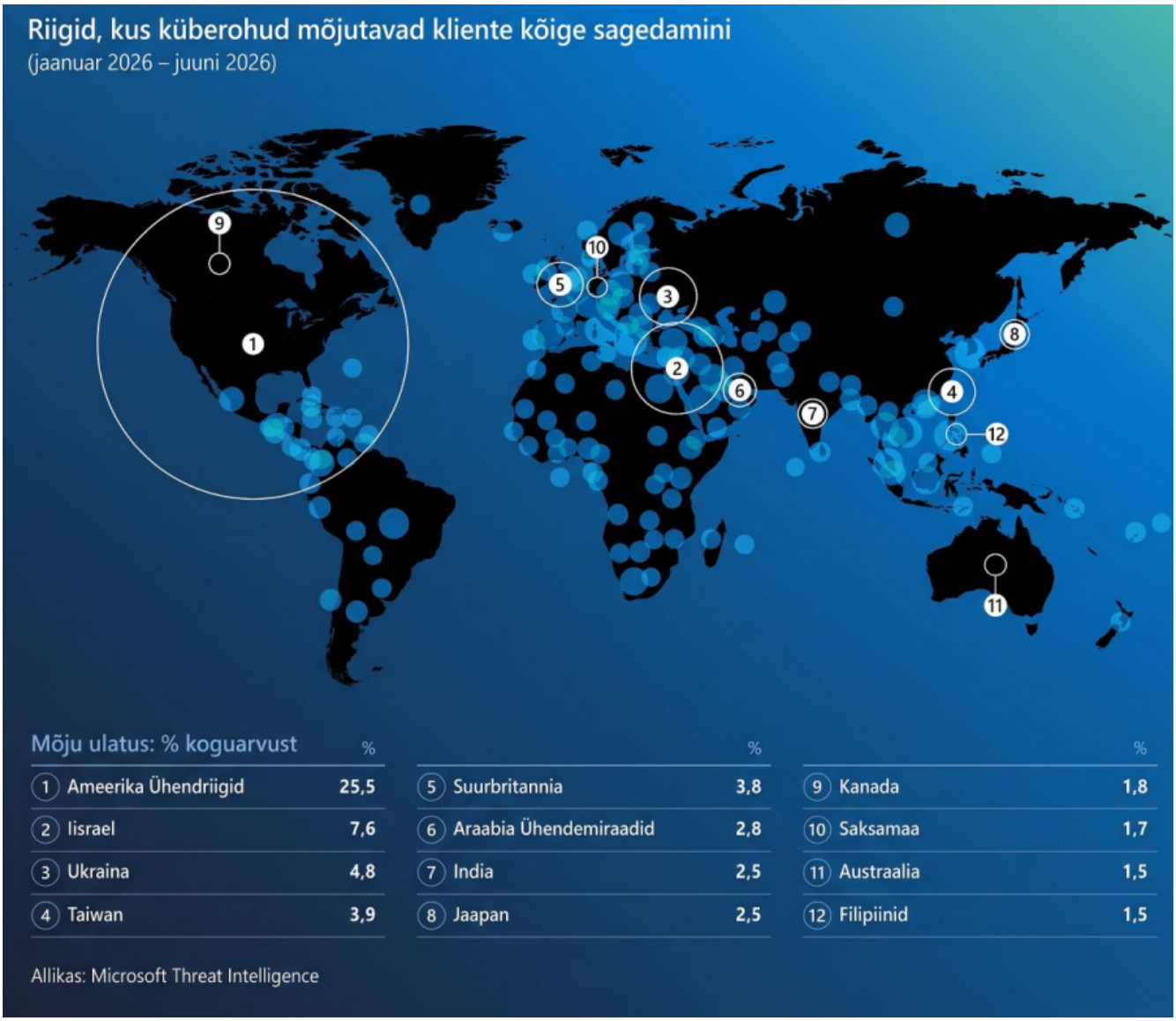
Microsofti raport: valitsussektor on küberohtudest kõige enam mõjutatud

1 kuu tagasi - 11.10.2026 Autor: AM

Microsofti värske digitaalkaitse raport näitab, et valitsussektor ja avalikud teenused olid 2026. aastal küberohtudest enim mõjutatud sektor, kus ohutegevuse osakaal tõusis 17 protsendilt 27 protsendini.

Raporti järgi on valitsusasutused ka riikliku taustaga kübertegevuse kõige sagedamini sihitud sektor. Põhjuseks tuuakse tundlik teave, oluliste teenuste toimimine ning tihe seotus alltöövõtjate, tehnoloogiaettevõtete ja kriitilise taristu haldajatega.

Ühe organisatsiooni kaudu võib rünnak jõuda ka teiste süsteemideni. Microsofti hinnangul muudavad tehisintellekt ja omavahel seotud digisüsteemid küberohud kiiremaks ja keerukamaks.



Tehisintellekt kasvatab riske

Microsofti turbe müügi- ja insenerivaldkonna juht **Nataliia Burlakova** kirjeldas tehisintellekti mõju kahel moel. Burlakova sõnul kasutavad küberründajad tehisintellekti juba praegu, samal ajal kui paljud organisatsioonid alles kaaluvad selle rakendamist küberturvalisuses.

Burlakova hinnangul loob tehisintellekti kontrollimatu kasutamine uue ründepinna, sest paljud tehisintellekti agendid tegutsevad kasutaja nimel ja kasutavad tema ligipääsuõigusi. Kompromiteeritud agent ühendab masinliku tegutsemiskiiruse ja -mahuga kasutajale antud õigused.

Seetõttu peavad tehisintellekti kasutamise reeglid, kasutajakontode kaitse, võimalikult piiratud ligipääsuõigused ja tehisintellektil põhinevate rakenduste tegevuse jälgimine olema turvastrateegia osa.

Andmepüük ja konto ülevõtmine sagenevad

Raportist selgub, et andmepüük moodustas 2026. aastal 23% täheldatud küberrünnakutest, võrreldes 7%-ga 2025. aastal. Varastatud kasutajakontod ja sisselogimisandmed on ründajate jaoks jätkuvalt oluline pääsetee organisatsioonide süsteemidesse.

52,2% rünnakutest, mille puhul kasutati kehtivat kasutajakontot, viisid ka täiendavate sisselogimisandmete varguseni. Esialgne konto kompromiteerimine võib kasvada lunavararünnakuks, spionaažiks, andmevarguseks või oluliste teenuste häirimiseks.

Tehisintellekt kiirendab ründeid ka ajaliselt. Ajavahemik haavatavuse avastamisest kuni küberrünnakuni võib olla lühem kui 24 tundi ning avalikult registreeritud tarkvarahaavatavuste arv ehk CVE-de arv võib 2026. aastal jõuda rekordilise 72 000ni.

Samal ajal pikenes aeg, mis jääb ründaja süsteemile ligipääsu saamise ja tegevuse avastamise või peatamise vahele. Ründajad kasutavad üha rohkem võtteid, mis muudavad nende tegevuse tavapärase kasutajategevusega sarnaseks.

Raport soovitab viit sammu

Raportis tuuakse välja viis sammu, mis aitavad valitsustel küberrünnakuteks paremini valmistuda ja oluliste teenuste toimimist tagada. Rõhutatakse ka avaliku ja erasektori koostöö tähtsust kriitilise taristu kaitsmisel ning uute tehnoloogiate kasutamise reeglite kujundamisel.

Olulised rollid ja koostööreeglid tuleks kokku leppida enne kriisi, et rünnaku korral saaks infot koguda, otsuseid teha ja avalikkust teavitada. Samuti soovitatakse käsitleda tehisintellekti turvalisust riigi toimepidevuse ja kriitilise taristu kaitse osana.

Lisaks tuleb arvestada, et üks rünnak võib kiiresti levida ning kriisiplaanid peavad hõlmama ka tarnijaid, partnereid ja teenusepakkujaid. Infovahetus avaliku ja erasektori vahel peab olema kiire, usaldusväärne ja kahepoolne.

Viimase sammuna rõhutatakse, et oluliste teenuste toimimine peab olema tagatud ka häirete ajal. Selleks soovitatakse korraldada regulaarseid õppusi, milles osalevad poliitikakujundajad, ametnikud, õiguskaitseasutused, kriitilise taristu haldajad ja erasektori partnerid.

Microsofti 5 sammu, mis aitavad küberrünnakuteks paremini valmistuda

1. Valmistu kiiremini arenemateks küberohtudeks

Olulised rollid, vastutusalad ja koostööreeglid tuleb kokku leppida juba enne kriisi. Nii saab rünnaku korral kiiremini infot koguda ja hinnata, otsuseid teha, eri asutuste ja ettevõtete tegevust koordineerida ning avalikkust teavitada.

2. Turvalisus peab olema tehisintellekti ökosüsteemi osa

Tehisintellekti turvalisust tuleb käsitleda riigi toimepidevuse ja kriitilise taristu kaitse osana, mitte ainult tehnilise probleemina. Tehisintellekti süsteemid sõltuvad omavahel seotud taristust, andmetest, mudelitest, rakendustest, tarnijatest ja juhtimisprotsessidest. Seetõttu tuleb turvalisusega arvestada juba tehnoloogia loomisel, süsteeme regulaarselt testida, tugevdada tarneahelate kaitset ning tagada läbipaistvus ja selged vastutusalad. Oluline on ka rahvusvaheline koostöö tehisintellektiga seotud riskide vähendamisel.

3. Tuleb arvestada, et üks rünnak võib kiiresti levida

Valitsusasutus ei pruugi rünnaku alguses teada, kas tegemist on kuritegeliku tegevuse, riikliku taustaga rünnaku või millegi muuga. Kuigi ründajate eesmärgid võivad erineda, kasutavad nad sageli samu viise süsteemidesse pääsemiseks – näiteks varastatud kasutajakontosid, avalikult kättesaadavaid rakendusi, inimeste eksitamist või tavapäraseid süsteemihaldusvahendeid. Seetõttu peavad kriisiplaanid hõlmama ka tarnijaid, partnereid ja teenusepakkujaid, kellele olulised teenused toetuvad. Rünnakud võivad levida üle organisatsioonide, sektorite ja riigipiiride, mistõttu on vajalik ka rahvusvaheline koostöö.

4. Avalik ja erasektor peavad infot küberohtude kohta omavahel kiiresti jagama

Ühes organisatsioonis avastatud rünnak võib anda varase hoiatuse laiemast ohust. Info, mis eraldi vaadates ei pruugi tunduda oluline, võib koos teiste organisatsioonide ja riikide andmetega näidata, et tegemist on koordineeritud rünnakuga.

Infovahetus peab olema kiire, usaldusväärne ja kahepoolne. See ei tohiks tähendada ainult seda, et ettevõtted edastavad ohuteavet riigile. Ka riigiasutused peaksid jagama ettevõtetega praktilist infot, juhiseid ja hoiatusi, mis aitavad neil oma süsteeme ja teenuseid kaitsta. Selleks on vaja usaldusväärseid infovahetuskanaleid, selgeid reegleid ja kaitset neile, kes jagavad infot heas usus. Samuti tuleb investeerida ühisesse ohuteabe kogumisse ja rünnakute tuvastamise võimekusse.

5. Oluliste teenuste toimimine tuleb tagada ka häirete ajal

Valitsused peavad teadma, millised teenused on ühiskonna toimimiseks kõige olulisemad ja millistest süsteemidest, kasutajakontodest, tarnijatest ja taristust need sõltuvad. Ainult kriisiplaanidest ei piisa. Valitsused peaksid regulaarselt korraldama õppusi, kus osalevad poliitikakujundajad, ametnikud, õiguskaitseasutused, kriitilise taristu haldajad ja erasektori partnerid. Nii saab enne päris kriisi välja selgitada, kus võivad tekkida probleemid otsustamisel, info jagamisel, avalikkuse teavitamisel või eri sektorite koostöös.

- Uudised
- Lahendused

- Turvalisus
- Tarkvara

Pilt

