Riigiasutused seisavad silmitsi enneolematute küberohtudega: parimaks kaitsjaks saab tehisintellekt

1 aasta tagasi - 28.01.2025 Autor: AM

Riigiasutustest on nüüd saanud kogu maailmas riiklikult mahitatud ohustajate tähtsuselt kolmas sihtmärk, kirjutab Microsoft oma turvaülevaates. Küberturvalisus on muutunud esmatähtsaks.

Kui küberkuritegevus oleks majandusharu, oleks see maailmas suuruselt kolmas ja prognoosi kohaselt kerkib selle aastakulu 2025. aastal 9,5 triljoni dollarini. Küsimus on selles, kas riigiasutused on järgmiseks ründelaineks valmis. Lunavara, identiteediründed ja muud küberohud seavad ohtu riigi julgeoleku, üldsuse usalduse ning elutähtsa taristu. Nende ohtude vastu võitlemiseks peavad riigiasutused kiiresti tegutsema, et tugevdada oma turbeseisundit ning võtta kasutusele tehisintellekt ja rajada selle abil vastupidavad kaitseliinid arenevate küberohtude vastu, kaitsmaks kodanikke ja elutähtsaid andmeid.

Laienev ohumaastik

Eelmisel aastal tuvastas ainuüksi Microsoft iga päev üle 600 miljoni küberründe, mille sihtmärgiks olid kliendid, sealhulgas riigiasutused ja elutähtis taristu.

Hiljutises Microsofti digikaitse aruandes juhitakse tähelepanu küberrünnete keerukuse märkimisväärsele suurenemisele, eriti riigiasutuste ning elutähtsate sektorite, näiteks tervishoiu, energeetika ja rahanduse vastu. Kui geopoliitilised pinged kasvavad, arenevad ka küberründe meetodid ja sellega kaasneb suurem oht riigiasutustele. Näiteks on ainuüksi paroolirünnete arv kerkinud kõigest kolme aastaga 572-lt sekundis rohkem kui 7000-le sekundis.

IDC prognoosi kohaselt on 2027. aastaks 95% riikidest kogenud ulatuslikku küberrünnet, mille on põhjustanud küberohustajad, kes kasutavad genereerivat tehisintellekti. Sama aruande järgi on ainult 30% riikidest piisavalt kerksed, et hoida ära suuremaid katkestusi ja turbemurdeid.

Kuidas tehisintellekt küberturvet muudab

Samal ajal kui küberturvariskid suurenevad, kasvab ka tehisintellekti võime neid ohte leevendada.

Näiteks Ukrainas on tehisintellektipõhistel avaliku pilve tehnoloogiatel olnud käimasoleva sõja ajal tähtis osa valitsuse süsteemide küberrünnete eest kaitsmisel. Tehisintellektipõhised tööriistad on võimaldanud Ukraina ametiasutustel tuvastada kiiresti ohud ja neile reageerida, tagades, et elutähtsad teenused toimivad endiselt ka jõuliste rünnete ajal. Just sellise ohu reaalajas tuvastamise ja kiire reageerimise tõttu ongi tehisintellekt küberturbe seisukohast nii oluline.

Samamoodi toimus Albaanias suur elutähtsate riiklike süsteemide vastu suunatud küberrünne, mida toetasid Iraani häkkerid. Microsofti, Ameerika Ühendriikide FBI ja Albaania küberturbe ekspertide koostöös kaitses riik edukalt oma taristut ning asus kaitset tugevdama. Selline valitsuste ja eraettevõtete viljakas partnerlus näitab, et küberturbe probleemide lahendamisel on koostöö äärmiselt vajalik.

Tehisintellekti roll turvalisuse suurendamisel

Avalikus sektoris on tehisintellekti roll suurem kui lihtsalt ohu tuvastamine. See muudab küberturbe käsitlemise viisi. Tehisintellektipõhised süsteemid suudavad töödelda tohutuid andmehulki reaalajas ning tuvastada kõrvalekaldeid ja nõrkusi, mida oleks käsitsi raske avastada. Automatiseerimine võimaldab intsidente prioriseerida, andes küberturbe spetsialistidele vaba aega keerukamatele probleemidele keskendumiseks.

Üks märkimisväärne näide pärineb Serbia IT- ja e-riigi ametist, kus võeti kasutusele tehisintellektipõhine tööriist Copilot for Security, mille ülesanne on aidata meeskondadel ohte tõhusamalt tuvastada ning nendega tulemuslikumalt tegeleda. Lisaks aitab tehisintellekt turbemeeskondadel kiiresti võimalikke riske märgata ja lühendab aega, mis kulub tekkivatele ohtudele reageerimiseks.

Peale tõhususe suurendamise aitab tehisintellekt leevendada oskustöötajate kriitilist nappust küberturbe valdkonnas. Terves maailmas nähakse avalikus sektoris vaeva, et leida piisavalt palju väljaõppinud küberturbe spetsialiste, kes tuleksid toime küberohtude kasvava mahu ja keerukusega. Tehisintellekt aitab välja, automatiseerides rutiinsed ülesanded ja võimaldades väiksemal meeskonnal tõhusalt tegevust laiendada, ilma et peaks palkama lisatöötajaid.

Küberrünnete kulu kasvab

Küberrünnete kulu kasvab kiiresti. 2024. aastal teatas lunavara ohvriks langemisest 34% riigi- ja kohaliku omavalitsuse organisatsioonidest – see on 2023. aasta 69%-ga võrreldes märkimisväärne langus. Taastekulud on aga kahekordistunud, need olid keskmiselt 2,83 miljonit dollarit ühe ründe kohta. Riigiasutuste vastu suunatud küberrünnetega ei kaasne ainult rahaline kaotus, vaid need võivad mõjuda katastroofiliselt riigi julgeolekule, kodanike usaldusele ja elutähtsale taristule. Kui ohtu satuvad kodanike peamised digisüsteemid, võib see kaasa tuua suured teenusekatkestused, mis mõjutavad igapäevaelu.

Ratko Mutavdzic.

Microsofti Euroopa, Lähis-Ida ja Aafrika riigiasutuste sektori direktor Ratko Mutavdzic kommenteeris olukorda järgmiselt: „Digiriigi teenuste turvamise tee on selge – igas küberturvastrateegias peab kesksel kohal olema tehisintellekt. Riigiasutused peavad seadma esikohale investeeringud tehisintellektipõhistesse küberturbelahendustesse, et ühelt poolt kaitsta end rünnete vastu ning teisalt reageerida nendele reaalajas ja tagada kerksus. Seda käsitlusviisi on rõhutatud veelgi Euroopa Liidu NIS2-direktiivis, milles kehtestatakse rangemad küberturvalisuse normid, nõudes täiustatud intsidendiaruandeid, rangemat tarneahela järelevalvet ja juhatuse suuremat vastutust. Tehisintellekti

integratsiooni ja õigusnormidele vastavuse kombinatsioon lisab digiriigi teenustele kerksust, võimaldades neil küberohtudele vastu seista ning neist kiiresti taastuda.“

Avaliku sektori juhtide peamised õppetunnid on järgmised.

1. **Koostöö on ülitähtis**. Küberohtude mastaap tähendab, et ükski riik ei saa end nende vastu üksinda kaitsta. Selleks, et jagada vajalikku teavet ja rajada tugevam kaitse, peavad riigiasutused ning eraettevõtted tegema rahvusvahelist koostööd.
2. **Tehisintellektipõhiste lahenduste kasutuselevõtmine.** Avaliku sektori turvaraamistikesse tuleb lõimida tehisintellektipõhine tehnoloogia, et suurendada ohtude avastamise ning neile reageerimise kiirust ja täpsust. See ei tähenda ainult uute töövahendite ostmist, vaid ka paradigma muutust tehisintellekti kui turbestrateegia vundamendi kasutamise suunas.
3. **Oskuste arendamine.** Tehisintellekt suudab küll paljud küberturbetööd automatiseerida, aga oskuslikest küberturbe spetsialistidest on ikkagi puudus. Avalik sektor peab edendama oma töötajaskonna kutsealast täiendusõpet, et areneval ohumaastikul püsti püsida.
4. **Paratamatuseks valmistumine.** Riigiasutused peavad küberrünneteks ennetavalt valmistuma, mitte lihtsalt nende toimumisele reageerima. See tähendab korrapäraseid ohuhindamisi, koolitusi ja erandolukorra plaanimist. Tehisintellektipõhised seire- ja ohutuvastusvahendid võivad seda tööd toetada, tagades, et riigiasutused on valmis kõigeks, mis võib juhtuda.
5. **Avalike teenuste turvalise ja tehisintellektipõhise tuleviku tagamine.** Samal ajal kui valitsused digipöördega edasi liiguvad, on kindla küberturvalisuse vajadus pakilisem kui kunagi varem. Tehisintellekt pole enam lihtsalt valikuline tööriist, vaid tervikliku turvastrateegia oluline osa. Tehisintellektipõhiste küberturbelahenduste kasutuselevõtmine, koostöö teiste riigiasutuste ja erasektori partneritega ning töötajaskonna väljaõpe võimaldavad riigiasutustel kaitsta oma digitaristut ning tagada, et avalikud teenused jäävad turvaliseks, tõhusaks ja kõigile kättesaadavaks.

- Tegijad
- Uudised
- Lahendused

- Tehisintellekt
- Turvalisus

Pilt