



## **Iraani taustaga rühmitus asus riiki tabanud rünnakute eest kätte maksma küberruumis, ohus võivad olla ka Eesti ettevõtted ja asutused**

### **Taust**

11. märtsil tabas maailma üht suurimat meditsiiniseadmete tootjat, 61 riigis tegutsevat USA ettevõtet Stryker küberrünnak, mille tagajärjel on ettevõtte töö tugevalt häiritud. Teenusekatkestused algasid USA idaranniku aja järgi pärast keskööd, mil paljud ettevõtte seadmed lõpetasid töö.

Rünnaku eest on avalikult vastutuse võtnud Iraani taustaga rühmitus Handala, mille peamisteks sihtmärkideks on seni olnud Iisraeli ettevõtted ja asutused.

Ehkki konkreetne rünnak tabas USA meditsiiniettevõtet, on kasutatud ründevektori tõttu potentsiaalselt ohus ka teised riigid ja sektorid. Sarnaseid kättemaksu-ründeid oleme näinud varemgi: 2023. aasta novembris, loetud nädalad pärast Iisraeli ja Gaza vahel lahvatanud konflikti algust, tabas ka mõnesid Eesti katlamaju ja pumbajaamasid küberrünnak, mille omistas endale üks teine Iraani rühmitus. Toona rünnati Iisraeli tootja Unitronics tööstusautomaatika kontrollereid.

### **Rünnaku sisu**

Esialgse info kohaselt said ründajad ligipääsu Strykeri Microsoft 365 (M365) Globaalse Administraatori õigustes kontole, mis annab piiramatu ligipääsu ja õiguse muuta seadistusi, lähtestada paroole ja hallata kasutajakontosid. Seejärel andsid ründajad lõppseadmete haldusteenuse Microsoft Intune kaudu käsu kustutada sellega liidestatud seadmete sisu. Lisaks rikuti Strykeri Microsoft Entra (identiteedi- ja juurdepääsulahendus) teenuseid.

Väidetavalt suudeti kahjustada suurusjärgus 200 000 seadet, sh töötajate süle- ja tahvelarvuteid ning telefone. Samuti kiitles rühmitus 50 terabaidi andmete vargusega.

### **Soovitused**

Vältimaks sarnase rünnaku ohvriks langemist, peaksid ettevõtted ja asutused, kes kasutavad Microsoft 365 teenuseid:

1. Kontrollima üle kõik oma M365 administraatorikontod:
  - sulgema mittevajalikud,
  - jätma ülejäänutele minimaalsed vajalikud õigused,
  - kaitsma kontosid mitmeastmelise autentimisega (eelistatult riistvaraliste turvavõtmetega).

<sup>1</sup> KÜTSi paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.



2. Piirama ligipääsu administraatorikontode (kindlatele seadmetele, IP-dele, vms) kasutades selleks Microsoft Entra Conditional Access-i (<https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview>)
3. Mitte kasutama administraatori õigustes kasutajakontot jooksvalt igapäevasteks toiminguteks.
4. Veenduma, et M365 logisid ja teavitusi jälgitakse aktiivselt ning vähimagi ohu või kahtluse korral reageeritakse koheselt. Erilist tähelepanu tuleks pöörata administraatoriõiguste loomisele ja muutmisele ning sisenemistele ebatavalistest asukohtadest või seadmetest.
5. Võtma kasutusele Microsoft Entra Privileged Identity Management (<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure>)

*Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond.*