RIIGI INFOSÜSTEEMI AMET

OHUHINNANG Oktoober 2026

Internetile avatud tööstusseadmed ja nende riskid

Olukord

Erineva suurusega ettevõtted kasutavad mitmesuguseid tööstusautomaatika *(ingl k Operational Technology ehk OT)* seadmeid, mis jälgivad ja / või juhivad füüsilisi protsesse, seadmeid või tööstuslikke süsteeme. Need koguvad füüsilistelt protsessidelt andmeid ning mõjutavad neid mõõtmise, juhtimise või automaatika kaudu. Näiteks basseini veekvaliteedi kontroller, ruumi ventilatsiooniseadmete juhtpaneel, kaitselülitite kaugjuhtimissüsteem alajaamas ja nii edasi.

Levinud praktika Eestis ja ka teistes riikides on võimaldada tööstusseadmete kaughaldust interneti kaudu. See tähendab, et seade ise või nende kontrollimiseks mõeldud juhtpaneel on ühendatud internetti ja seadistatud interneti kaudu ligipääsetavaks ehk teisisõnu, tehnik või haldur saab sellesse veebi kaudu sisse logida, kontrollida seadme tegevust ja näite ja neid vajadusel muuta.

Riskid

Küberturvalisuse vaatest on **internetile avatud tööstusseadmed väga kõrge riskiga**, sest neid on spetsiaalsete tööriistadega väga lihtne internetis tuvastada ka potentsiaalsetel ründajatel. Lisaks on sellised seadmed sageli **pärandseadmed, aegunud või turvanõrkustega tarkvaraga ja ebapiisavate turvaseadistustega,** mis teeb nende ründamise eriti lihtsaks. Sihtmärgiks ei ole sageli mitte individuaalsed seadmed, vaid näiteks mingi konkreetse tootja konkreetse seeria seadmed, millel on teada ja tuvastatavaid turvanõrkusi. Ründed internetile avatud OT-seadmete vastu on viimasel paaril aastal muutunud tavalisemaks - tegemist on suhteliselt lihtsa ründepinnaga, mida erinevad ohustajad järjest rohkem ära kasutavad.

Rünnete tagajärjed võivad olla mõõdukatest (näiteks piiratud arvu väheoluliste seadmete lokaalne kompromiteerimine) keskmiste (näiteks seadmete kontrollitavate näitude manipuleerimine ilma väga tõsiste tagajärgedeta) **kuni väga tõsisteni** (näiteks suure osa seadmete muutmine kasutuskõlbmatuks, seadmete kontrollitavate elutähtsate teenuste takistamine ja seeläbi inimeste elu ohustamine, seadmete kompromiteerimise kaudu SCADA süsteemidesse sisse pääsemine, nende kasutuskõlbmatuks muutmine või nende kaudu suure kahju põhjustamine).

Riigi Infosüsteemi Amet
Pärnu maantee 139a, 15169 Tallinn
+372 663 0200
ria@ria.ee

ria.ee

Eesti tuntuim näide internetile avatud tööstusautomaatika rünnetest on 2023 detsembris toimunud rünnak mitmete katlamajade Unitronics juhtpaneelide vastu. Globaalselt tuntuim näide on hetkel 2026 oktoobris Prantsusmaal aset leidnud rünne Danfoss külmseadmete juhtpaneelide vastu, mille tõttu hävines supermarketites miljonite eurode eest kaupa.

RIA juhised internetile avatud OT-seadmete omanikele

1. Piira seadmetele ligipääs internetist, kui see on vähegi võimalik
2. Kui ligipääs internetist on hädavajalik, rakenda turvameetmed: tugev parool ja mitmikautentimine, range pääsupoliitika, VPN-i kasutamine.
3. Uuenda regulaarselt kõigi IT-, automaatika ja tehnosüsteemide tarkvara. Kui tarkvarauuendused ei ole võimalikud, eemalda seade internetist.
4. Eralda OT-seadmete võrk kontorivõrgust. Võimalusel segmenteeri OT-seadmete võrgu erinevad osad selliselt, et kriitilise tähtsusega seadmetele ei oleks ligipääs võimalik ka siis, kui mõni madalama kriitilisusega seade on kompromiteeritud.
5. Kui saad CERT-EE-lt hoiatuse, et sinu seade on haavatavustega ja / või internetile avatud, suhtu sellesse tõsiselt ja tegele probleemiga kiiresti. Määra oma ettevõttes inimene, kelle ülesanne see on.
6. Hooldustööde tegijatele ava ligipääs ainult hooldustööde ajaks.
7. Kontrolli regulaarselt, kellel on seadmetele ligipääs, sh kaugligipääs.
8. Tee plaan olukorraks, kui seadmed enam ei tööta või on need vaja ajutiselt tööst eemaldada (näiteks minna üle käsitsi juhtimisele).

Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond koostöös RIA kriitilise informatsiooni infrastruktuuri kaitse osakonnaga.

Kui vajad lisainfot või abi, võta ühendust RIA kriitilise informatsiooni infrastruktuuri kaitse osakonnaga kikk@ria.ee

Riigi Infosüsteemi Amet
Pärnu maantee 139a, 15169 Tallinn
+372 663 0200
ria@ria.ee

ria.ee