RIIGI INFOSÜSTEEMI AMET

OHUHINNANG[1] 13. detsember 2023

Ründelaine tööstusautomaatika juhtseadmete vastu

Olukord

Iisraeli-vastased häktivistid on asunud ründama Unitronics tööstusautomaatika juhtseadmeid (PLC), mida **kasutavad ka mitmed Eesti tööstusettevõtted**. Ohustatud on kõik nimetatud tootja seadmeid kasutavad ettevõtted ning kui seade on internetile avatud ja / või muul moel nõrgalt kaitstud, **on tõenäosus ründe ohvriks langeda suur.** Ehkki käimasolev laine sihib just antud tootja seadmeid, võib olla tavapärasest suurem oht ka teistele tööstusautomaatika seadmetele.

30.11 tabas küberrünnak vähemalt kolme Eesti ettevõtte tööstusautomaatika juhtseadmeid. Ühel juhul seiskus kaheksa katlamaja kaugjuhtimisseadme töö. Mõjutatud katlamajad viidi üle käsijuhtimisele ja soojatootmine ei katkenud.
Teise rünnakuga sai pihta ühe valla vee-ettevõte ning selle tulemusena seiskusid üheksa reovee ja ühe joogivee pumbajaama kaugjuhtimisseadmed, kuid pumbajaamade töö siiski jätkus. Kolmas samalaadne rünnak tabas ehitusmaterjalide tootjat.

12.12 tabas rünnak veel ühte Eesti väiksemat katlamaja, mille töö seiskus ning hetkel sõltub asula soojatootmine varukatlamajast.

Rünnete iseloomustus ja mõju

Ründeks kasutatakse pahavara, mis kirjutab üle seadmete tarkvara ja muudab need kasutuskõlbmatuks. Eesti juhtumite puhul on rünnet võimaldanud peamiselt asjaolu, et PLC seadmed on olnud internetist kergesti ligi pääsetavad.

Seadmete taastamine ründe järgselt ei ole vähemalt osade juhtumite puhul võimalik ja need tuleb välja vahetada. Sõltuvalt konkreetse tööstusettevõtte automaatika ülesehitusest ja vastastikustest sõltuvustest võib rünnaku mõju olla väga suur, mõjutades näiteks kütte- või veevarustust.

Ründelaine on globaalne ja näiteid edukatest rünnetest on teada mitmetest riikidest. Detsembri esimesel nädalal oli näiteks ühe Iiri asula 180 majapidamist 1-2 päeva veeta, kuna kohalik pumbajaam oli langenud ründe ohvriks.

RIA soovitused tööstuslikke juhtimisseadmeid (eriti Unitronics tootja omi) kasutavatele ettevõtetele:

1. Veendu, et need seadmed ei ole internetist ligi pääsetavad. Kui kaughaldus on vajalik, tõsta seadmed tulemüüri taha ning kasuta VPN-ühendust või mõne side-ettevõtte pakutavat privaat-APN lahendust. Kus võimalik, rakenda mitmikautentimist.

[1] 1 1 KüTS'i paragrahv 12: (3) Riigi Infosüsteemi Amet edastab isikutele küberintsidendi ennetamiseks ja lahendamiseks ohuteateid, mis võimaldavad rakendada küberintsidendi mõju vältivaid või vähendavaid abinõusid.

2. Veendu, et seadmetel on vahetatud ära tehaseparool ning kasuta tugevat parooli.
3. Rakenda võrkude segmenteerimist: tööstuslikud seadmed peavad olema eraldatud võrgus ning sellele ligipääs ainult neil töötajatel, kelle jaoks see on vajalik.
4. Mõtle läbi kriisiplaan ja vastastikused sõltuvused, juhuks kui sinu tööstusautomaatika satub küberründe ohvriks.
5. CERT-EE seirab oma tööriistadega Eesti küberruumi ning saadab internetiteenusepakkujatele (ISP) hoiatusi nende võrgus aktiivselt ärakasutatavate turvanõrkuste kohta. Kui saad ISP kaudu CERT-EE teavitusi, võta neid tõsiselt!

Kui soovid olla kursis Eesti küberruumis toimuvaga, jälgi RIA kuukokkuvõtteid.

Ohuhinnangu koostas RIA analüüsi- ja ennetusosakond koostöös CERT-EE-ga.