Eesti Energeetika Veteranide Ühenduse koosoleku memo nr 8/2017

Tallinn, Eesti Energia, Lelle 22

07.12.2017

Koosolekust võttis osa 30 Ühenduse liiget.

Päevakorras:

1. Küberkaitsest elektrivõrkudes.
2. Informatsioonilised teated.

Koosoleku juhataja Rein Talumaa teavitab koosolijaid energeetikaveteranide auväärsetest sünnipäevadest:
Tiiu Tiigimägi sai 20. novembril 81-aastaseks,
Väino Kõppo sai 27. novembril 83-aastaseks ja
Mati Valdma sai 28. novembril 81-aastaseks.

1.1 Catapult Labs OÜ juhatuse liige Heikki Kolk teeb ettekande teemal „Küberkaitsest Euroopa energeetikaettevõtetes“. Ettekandja töötas tänavuse aasta alguseni Eesti Energias ja Elektrilevi OÜs 10 aastat, viimati võrgutehnoloogia osakonna juhtivspetsialistina. Ta alustas SCADAst ja osales edaspidi kõigis suuremais juhtimisalastes projektides.

Miks üldse räägitakse energeetikaettevõtete turvalisusest nii palju? Varem olid alajaamade ja energeetikaobjektide vahel privaatsed teistele ligipääsmatud vaskkaablid. Arvati, et ettevõttest väljaspool ei saa nagunii keegi aru, kuidas seadmed on seotud ning töötavad. 2007. a tõestas üks USA uurimislaboritest projekti AURORA raames, et said SCADA kaudu üle võtta generaatori juhtimise ja kõigutasid generaatori pöördeid üles-alla. Paari minutiga suudeti generaatori koodid välja peilida ning oleks võidud minna generaatori lõhkumiseni. 2010. a murdis pahavara Stuxnet sisse Taani tuumaettevõttesse, põhjustades 2000 tsentrifuugi purunemise ning väljavahetamise. 2012. a viidi Saudi Araabia naftatööstuses kõik juhtimissüsteemid rivist välja ja 17 päeva jooksul ei läinud töötlejatelt välja ühtki liitrit naftat, sest arveldussüsteemid ei töötanud ning ei suudetud arvet pidada, kes kui palju kütust sai. Saudid otsustasid riigi majanduse käigushoidmiseks kütust tasuta välja jagama hakata. Põhimõtteliselt midagi katki ei tehtud ega ära ei rikutud, kahjustati ainult raamatupidamistarkvara.

Eestis on küberturvalisuse tagamise alusdokumentideks hädaolukorra seadus ja rahvusvahelised standardid[1], milliste nõuetele toetudes peab elektrisüsteem olema üles ehitatud. Eestis on kehtiv ka infosüsteemide kolmeastmeline turvameetmete süsteem ISKE, mille väljatöötamisel ja arendamisel on aluseks võetud vastav Saksamaa infoturbe standard. ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. ISKE rakendusjuhendi esimene versioon valmis 2003. aasta oktoobrikuus.

---

[1] EVS-ISO/IEC 27001:2014 „Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded“ ning EVS-ISO/IEC 27002:2014 „Infotehnoloogia. Turbemeetodid. Infoturbemeetodite tavakoodeks“

1.2 Vahepliigina kirjeldab Elektrilevi käiduosakonna peaspetsialist Üllar Viitkar küberrünnakut USA elektrivõrgus. Läbi Interneti suudeti arvutivõrku meiliga sisse sööta Exceli tabel, mille avamisel suunati see peaarvutisse. Pahavara oli arvutis ligi 8 kuud ja kogus andmeid. Paar päeva enne jõule aktiveeriti juhtmevaba liin ja hakati sellega toimetama. Hiire töö alajaamade juhtimisel oli salvestatud ja hakati tegelema alajaamade väljalülitamisega. Kui kohalik dispetšer seda märkas, siis logis ta enda välja, kuid sisse logida ta enam ei saanud, sest paroolid olid ära vahetatud ning hiir toimetas ja lülitas alajaamad välja. Rünnak kestis ainult mõned minutid.

1.3 Eesti Energia infoturbejuht Olev Sepp esineb teemal „Küberturbe väljakutsed ja lahendused Eesti Energias“. Maailma üldiste kübertrendidena jätkuvad paha- ja lunavararünnakud, rünnakud mobiilseadmetele, infosüsteemide rünnakud läbi Interneti ja suurte ettevõtete andmelekked. Olukord Eestis on rahulikum, lunavara mõju on väike, kuid jätkuvaks teemaks on õngitsemine[2]. Eesti Energia info on suuline, paberkandjal ja digitaalne ning ohuks on info lekked, volitamata ligipääs infole ja infosüsteemide tõrked. Igal töötajal on Eesti Energia infoturbe tagamisel oluline roll läbi oma teadmiste, teadlikkuse ja tegevuse mõjude ning tagajärgede hindamise. Energeetikas töötajate arenguks viiakse läbi infosüsteemide kasutajakoolitusi, riskiteadlikkuse tõstmise koolitusi ja inimeste teadmiste ning oskuste tõstmist läbi kriisiharjutuste.

1.4 Elektrilevi infoturbejuht Indrek Künnapuu teeb ettekande teemal „Küberturvalisus Elektrilevis“. Elektrilevil on hallata ja hooldada 61 000 km elektriliine, 22 000 alajaama, 475 000 klienti, 650 000 kaugloetavat arvestit ja 6000 IPseadet. Seadmete turvalise töö tagamiseks hoitakse SCADA Internetist eemal, seadmeid kontrollitakse pidevalt, andmete ja käskude liiklus alajaamade ning SCADA vahel on krüpteeritud, tehakse pidevat 24/7 monitooringut ja perioodilisi turvateste. Uuenduste tegemise juures säilitatakse ka vanade andmete koopiad, et neile vajadusel tagasi minna. Praegustes alajaamades on probleemiks sealse automaatika eeldatav 20aastane eluiga, piiratud monitooring, puuduv kaughaldus ja liigesus ning kohalik turvalisus on tagatud seintega. Traadita sidevõrgu eluiga on samuti lühike – 450 MHz võrk suleti 2016. a, WiMax suleti 2017. a, 3G side, millist praegu kasutab umbes 100 000 seadepunkti, suletakse 2020. aastal ja järgneb 4G ning 5G ajajärk. Kaugloetavatele arvestitele ülemineku järel on esinenud erinevaid füüsilisi rünnakuid, elektriskeemide muutmisi ja ka kauglugerite kadumisi. Kaugarvesti kõrvale on asetatud tugev magnet, mis lülitab arvesti välja. Selline vargus tavatarbimise vähenemisega tuleb aga kiiresti avalikuks. Tulevikuprobleemide lahendamiseks loodi koos TTÜ vastava ala spetsialistidega jaotussüsteemi arengulabor Elektrilevi MEKTORY.

2. Koosoleku juhataja teatab, et järgmine koosolek on 16. jaanuaril 2018 ja kuulame Mati Valdma plaanikohast ettekannet. Seoses veebruarikuusse jääva Eesti riigi 100. sünniaastapäeva tähistamisega teeb ta aga ettepaneku viia veebruarisse plaanitud Hugo Pikandit meenutav koosolek üle märtsikuusse ja kuulata veebruaris Tiit Metusala ettekannet Elekter 100 Eestis elektri tootmise ja varustamise ajaloost. Kohalolijad nõustusid ettepanekuga.

Koosolekut juhatas Rein Talumaa

Memo koostas Rein Tivas

---

[2] (õngitsemine (inglise keeles phishing) on rünnaku tüüp, kus pahalane üritab varastada kasutaja isikuandmeid nagu parool)