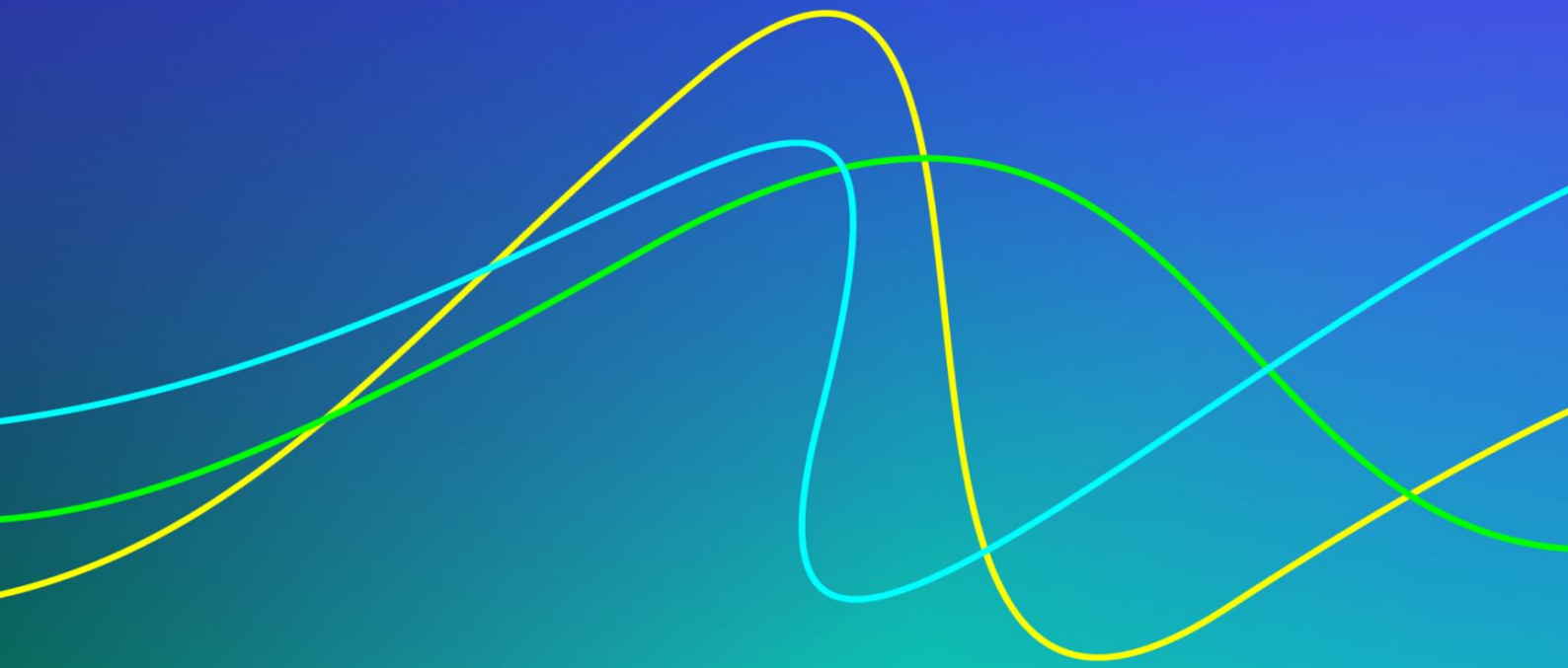
RIIGI INFOSÜSTEEMI AMET

Näidisteekaart



Kaasrahastanud Euroopa Liit

ECCC

Sisukord

Sissejuhatus ja lühikokkuvõte

Sissejuhatuses tuleb kirjeldada, miks infoturbe hindamine ette võeti, millal see läbi viidi, kelle poolt ja kelle toel. Lühikokkuvõte peaks andma edasi põhilised soovitused, mis aitaksid kõige enam tõsta ettevõtte küberturvalisuse taset.

Ettevõttes viidi läbi infoturbe alane hindamine, kasutades RIA poolt välja töötatud küberpöörde teekaardi metoodikat. Hindamise eesmärk on toetada ettevõtteid infoturbe taseme tõstmisel ning seeläbi vähendada tõenäosust, et ettevõtte langeb küberrünnaku ohvriks ning kannatab seeläbi rahalist kahju.

Teekaardiks vajaliku kaardistuse viis läbi (***Teekaardi koostaja ettevõtte nimetus*** + ***eksperdi/ekspertide nimed)***. Projektiga alustati 01.11.2022 ja lõpetati 15.11.2022.

Kaardistuse tulemusena soovitame ***Tellijal (ettevõtte X nimetus)*** juurutada arvutivõrgu segmentideks jaotamist, võttes aluseks serverites ja tööjaamades asuvate andmete kaitsevajadus ning seada sisse võrgusegmentide vaheline läbipääsukontroll. See vähendab oluliselt riski langeda lunavararünnaku ohvriks, kus ründaja võib takistada ettevõtte tootmist olulisel määral.

Samuti soovitame juurutada turvanõrkuste automatiseeritud paigaldamist vastavalt ärikriitilistele süsteemidele.

Teostatud tööde skoop

Siia tuleks kirjutada teekaardi skoobist lähtuvad tegevused. Samuti on see koht, kuhu lisada lisandunud tegevused, kui neid tehti teekaardile lisaks

Ettevõtte teekaardi jaoks tehti kaardistus kõigepealt kaugelt OÜ Tootmisettevõtte tegevuse hindamiseks ning seejärel ettevõtte 4 füüsilises asukohas. Kaardistuse skoop oli järgmine:

1. Avalikust internetist potentsiaalsete rünnete sooritamiseks kasuliku informatsiooni kogumine ja tehniliste nõrkuste leidmine
2. Välisperimeeter ja avalikud veebilehed
3. Tulemüüri kasutus ja tulemüürireeglite ülevaatus
4. Kontorite võrgud (4 asukohta): tööjaamad ja serverid. Kontorite Wifi võrgud ja nende seadmed
5. Kaugligipääsud – VPN, IPSEC tunnelid jne
6. Serverite võrgud ja haldusvõrgud
7. Valvesüsteemid ja nende võrgud – läbipääsusüsteemid, videovalve
8. Automaatikavõrgud – UPS-id, hooneautomaatika (4 asukohta)
9. Serveri- ja seadmeruumide füüsilise turbe vaatus
10. Riskianalüüsi ja taasteplaanide olemasolu ja ülevaatus

Metoodika

Metoodika peatükis tuleb anda ülevaade metoodikast ning põhjendada, miks selline metoodika valiti.

Infoturbealane hindamine viidi läbi nn halli kasti meetodil ehk ettevõtte (IT) töötajad olid hindamisest teadlikud ning aitasid hindamist võimalikult efektiivselt ellu viia. Selline meetod võimaldab hindajatel riskipõhiselt valida valdkonnad, millele rohkem keskenduda, jäädes samas ettenähtud ajaraami. Hindamisel kasutati info kogumiseks ning testide planeerimiseks nii intervjuusid, paikvaatlusi, olemasoleva dokumentatsiooni läbivaatamist, manuaalseid ja automatiseeritud teste ja skannereid. Hindamise käigus vaadati võimalikult laialt ettevõtte küberturvalisust, et tagada ettevõtte toimepidevus ning vähendada küberründe võimalust.

Peamised tuvastatud probleemid, järeldused ja ettepanekud

Kõige tähtsam peatükk. Siin tuleb välja tuua kokkuvõte leidudest ja nende juurpõhjused. Tavaliselt on nendeks mingi poliitika/protsessi puudumine või need on ebapiisavad või neid ei järgita. Samuti võib olla juurpõhjuseks ebapiisav ressurss (liiga vähe IT/infoturbe töötajaid võrreldes hallatava lahendusega) või puuduvad töövahendid (või valed töövahendid – näiteks puudub keskhaldus).

1. **Ettevõttes ei ole selgelt määratud IT ja küberturvalisuse teemade eest vastutaja juhtkonna tasemel.**
   Ettepanek: Määrata formaalselt juhtkonna liige, kes vastutab IT ja küberturvalisuse eest
2. **Ettevõttes puudub infoturbe teemade eest vastutaja. Puudub äripoole sisend vajalikule turbetasemele.**
   Ettepanek: Välja kujunenud praktika kohaselt otsustab infoturbe küsimusi IT partner, kes teeb otsuseid oma parima äranägemise järgi, mis ei pruugi olla kooskõlas äriliste vajadustega. Ettepanek on regulaarselt IT-partneriga läbi arutada infoturbe küsimused, lähtudes ärivajadustest.
3. **Puudub süstemaatiline IT turvalisuse tagamine.**
   Ettepanek: Võtta kasutusele sobiv IT turvalisuse raamistik – CIS 18, E-ITS, ISO27001 vms.
4. **Puuduvad IT juhtimise ja planeerimise poliitikad**
   Ettepanek: Töötada välja poliitikad segmenteeritud võrguarhitektuur IT ja automaatikasüsteemide jaoks;

Eduka rünnaku toimepanemiseks vajalikud ressursid

See on hinnang ettevõtte juhtkonnale ja vastab küsimusele, kas eduka rünnakuga saavad hakkama automaatne skript, 2 tundi Youtube-i vaadanud koolipoiss/pahur endine töötaja või on vaja pikema aja jooksul märkimisväärsete oskustega spetsialiste rakendada.

Eduka rünnaku, mis häiriks tugevalt ettevõtte tööd, toimepanemiseks vajaminevad teadmised ja ressursid on madalad. Ettevõte on eriti haavatav enda ja oma lepingupartnerite endiste töötajate poolt ning internetti avatud haldamata teenuste tõttu.

Järeldused ja ettepanekud

Turvalisuse hindaja eksperthinnang. Arvesse peab võtma ettevõtte profiili – „tavalist“ 50 arvutitöökohaga tootmisettevõtet ei ole mõtet võrrelda 5000 töötajaga e-pangandusele spetsialiseerinud pangaga.

Ettevõtte üldine IT turvalisuse tase on madal. Selleks, et vähendada eduka rünnaku riski ja äriteenuse katkemist, soovitame AS Tootmisettevõttel juurutada arvutivõrgu segmentideks jaotamist, võttes aluseks serverites ja tööjaamades asuvate andmete kaitsevajadus ning seada sisse võrgusegmentide vaheline läbipääsukontroll. See vähendab oluliselt riski langeda lunavararünnaku ohvriks, kus ründaja võib takistada ettevõtte tootmist olulisel määral.

Samuti soovitame juurutada turvanõrkuste automatiseeritud paigaldamist vastavalt ärikriitilistele süsteemidele.

Tehniline osa:

Läbiviidud tegevused

Testimise läbiviimiseks kasutatud tark- ja riistvara nimetused koos kirjeldustega, kasutatud metoodikate, standardite ja parimate praktikate kirjeldused

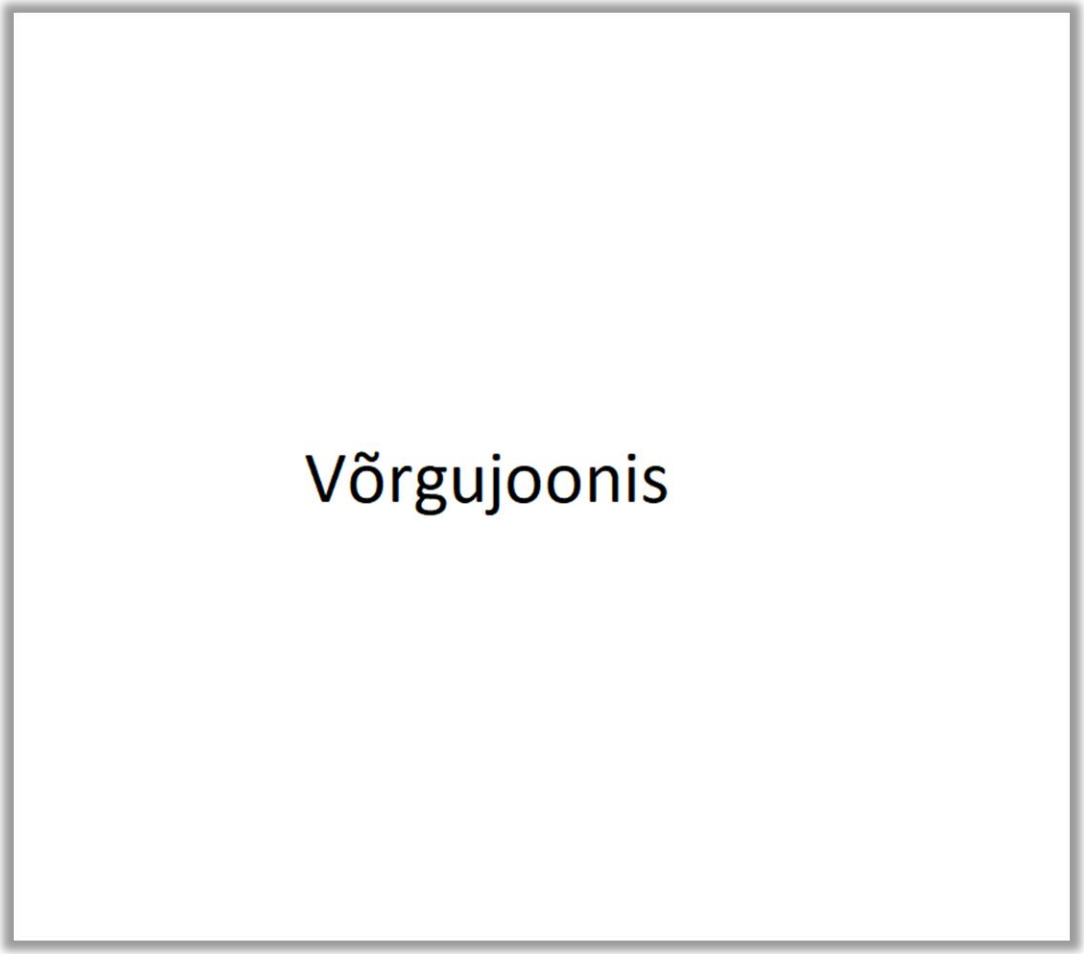
Peatükk peab andma võimalikult lihtsas keeles ülevaate, mida projekti jooksul tehti. Samuti tuleb siin ära kirjeldada, mida ei tehtud.

Kohapealne hindamine viidi läbi kahe eksperdi poolt 08. – 10. novembril 2022. Kohapealsele hindamisele eelnes testide läbiviimine üle interneti ning dokumentatsiooniga tutvumine. Kaardistus hõlmas järgmisi tegevusi:

1. Kõikide portide skaneering ettevõtte välistel IP aadressidel;
2. Avaliku veebilehe https://www.ria.ee turvalisuse hindamine;
3. Tulemüürireeglite ülevaatus keskses tulemüüris;
4. Sisevõrgu skaneering tööriistaga Nessus;
5. WiFi võrkude turvalisuse hindamine Narnia kontoris, Tuuleaugu tehases ja Kaevuääre logistikakeskuses;
6. Kaugligipääsude turvalisuse hindamine (nii töötajate kui ka site-2-site);
7. Pisteline serverite turvalisuse hindamine;
8. Videovalvesüsteemi turvalisuse hindamine;
9. Tööstusseadmete, SCADA ja juhtarvutite võrgu turvalisuse hindamine;
10. Serveri- ja seadmeruumide füüsilise turbe ülevaatus Narnias, Tuuleaugul ja Kaevuäärel.

Ettevõtte IT keskkonna kirjeldus

Ettevõtte ja selle IT keskkonna üldine kirjeldus ja võrgujoonis. Võrgu joonise detailsusaste on mõistlik valida nii, et see ei vananeks liiga kiiresti ja ettevõte oleks võimeline seda edaspidi uuendama.



AS Tootmisettevõte põhitegevus on ping-pongi pallide tootmine. Ettevõttes töötab 350 töötajat kolmes asukohas. Peakontor asub Narnia külas, kus on 25 arvutitöökohta ja serveriruum 3 füüsilise serveri ning kettakastiga. Tuuleaugu külas asub tehas, kus on 20 arvutitöökohta ning 5 tehase operaatori töökohta. Samuti on tehases teine serveriruum 3 serveri ning kettakastiga. Kaevuääre logistikakeskuses on 3 arvutitöökohta. Kõikides asukohtades on läbipääsusüsteem, videovalvesüsteem ja kaks WiFi võrku – töötajate võrk „Ping“ ja külaliste võrk „Pong“. Erinevate asukohtade vahel on PPTP VPN tunnelid.

Tähtsamad leiud
Leidudest tulenevad riskid ja nende parandamise keerukus on jagatud kolme kategooriasse, mida eristatakse järgmiselt:

Riskide klassifitseerimine	
Madal	Madala riski realiseerumise korral on organisatsiooni tööprotsessid vähesel määral häiritud.
Keskmine	Keskmise riski korral on osad organisatsiooni tööprotsessid tõsiselt häiritud.
Kõrge	Kõrge riski korral on kogu organisatsiooni tööprotsessid tõsiselt häiritud.

Puuduste kõrvaldamise keerukus	
Madal	Puuduse kõrvaldamisele kulub vähem kui üks tööpäev. Tööprotsessides ei ole vaja teha muudatusi.
Keskmine	Puuduse kõrvaldamiseks kulub rohkem kui tööpäev kuni kaks töönädalat. Tööprotsessides või süsteemides tuleb teha olulisi muudatusi.
Kõrge	Puuduse kõrvaldamiseks kulub kuid kuni aasta. Tööprotsessides või süsteemides tuleb teha kas kardinaalseid muudatusi või tuleb need uuesti ülesse ehitada.

Iga tuvastatud nõrkus peab omama unikaalset numbrit, pealkirja, nõrkust omava seadme/protsessi identifikaatorit (nt IP aadress, hostinimi, vms) nõrkuse kirjeldust, soovitavat lahendust või viidet juhendile, kuidas lahendust teha. Kui võimalik, peab leiu juures olema välja toodud CVSS v3 või v3.1 Base Score. Nõrkusi võib grupeerida, siis tuleb märkida riskitase vastavalt kõige kõrgema riskiga nõrkuse järgi ning parandamise keerukus kõige aeganõudvama nõrkuse parandamise järgi. Nõrkused peavad olema sorteeritud nii, et eespool on kõrgeima riski ja madalaima parandamise keerukusega nõrkused.

L1. Nõrk võrgu planeerimine

RISK: Kõrge CVSS: 9,2	Parandamise keerukus: Keskmine

Tähelepanek:
- Serverid ja tööjaamad asuvad kontorivõrgus (192.168.1.0/24), lisaks on kontorivõrgust täielik ligipääs tööstusautomaatika serveritele (192.168.2.0/24).
- Kontorivõrgule on ligipääs töötajatele mõeldud WiFi tugijaama (192.168.1.200) kaudu.
- Sisevõrkude vahelised tulemüürireeglid on seadme, mitte teenuse põhised, mis võimaldab ühenduda kõikide sihtseadme teenuste/portide poole.
- Kõikidest sisevõrkudest on piiramatu ligipääs internetile.
- Puudub seadmete haldusvõrk.
- Tulemüüri reeglid on dokumenteerimata.
- Site-to-Site VPN tunnelid kasutavad paroolipõhist autentimist, parool on kõikidel tunnelitel sama.
- VPN kasutab vananenud ja ebaturvalisi algoritme SHA-1 ja 3DES, võtmevahetuseks IKEv1.

Segmenteerimata võrgu või võrgu puhul, mille segmentide vahelist liiklust ei filtreerita, ei ole võimalik piirata ega tuvastada tööjaamade, serverite vahelist liiklust. Tulemüürist lubatud piiramatu ligipääs tööstusautomaatika võrgus asuvatele serveritele/teenustele loob riski, et iga kontorivõrgu seadme kompromiteerumise korral on võimalik ründajal või pahavaral takistuseta tööstusautomaatika seadmeid kompromiteerida.

Serveritel ja tööjaamadel ei ole seadistatud lokaalseid tulemüüre, mis aitaksid piirata pahaloomulist tegevust ja mis on osa mitmekihilise kaitse (*defence-in-depth*) filosoofiast.
Selline olukord võimaldab pahavaral takistamatult sisevõrgus levida kuna töötajate ja ka avalikke teenuseid pakkuvad serverid asuvad samas võrgus sh on ligipääs tööstusautomaatika serveritele/teenustele.

WiFi võrgule ligipääsu korral on ründajal võimalik koheselt saada ligipääs ka olulistele teenustele SCADA segmendis ning muudele sisemistele teenustele.

Soovitused:
Soovitame tungivalt juurutada arvutivõrgu segmentideks jaotamist, võttes aluseks serverites ja tööjaamades asuvate andmete kaitsevajadus ning seada sisse võrgusegmentide vaheline läbipääsukontroll.

Arvutivõrk tuleb segmenteerida erinevateks turvadomeenideks, segmentide vaheline liiklus peab olema kontrollitud tulemüüridega ning järgida tuleb minimaalõiguste printsiipi (*least privilege principle*). Alustada tuleb kriitilisemate (tööstusautomaatika, serverid) võrkude eraldamisest, kus tuleb lubada interneti suunalist liiklust ainult vajaduse põhiselt.

WiFi põhine ligipääs sisevõrgule ilma VPN ühendust kasutamata ei ole meie hinnangul piisavalt turvaline lahendus. See tõttu soovitame eraldada WiFi tugijaama täielikult sisevõrgu taristust ning WiFi ühenduse korral järgida samu reegleid, mis kaugtöö puhul.

Serverite, IP telefonide ja muude seadmete jaoks on mõistlik luua eraldi haldusliideste segment (*management network*), mida kasutatakse ainult seadmete administreerimiseks.

Arvestades võrgu suurust ning keerukust ei ole tegemist liialt keerulise ja aega nõudva ülesandega. Meie hinnangul ei tohiks peakontori võrgu segmenteerimiseks kuluda olemasolevate vahenditega rohkem kui üks kuu, kasutada saab olemasolevaid võrguseadmeid. Küll aga nõuab see tööprotsesside muutmist, mille tingivad eelkõige muudatused tööstusautomaatika halduses/monitooringus.

Tulemüüri reeglid peavad olema dokumenteeritud koos selgituste ja põhjendustega, et tagada järjepidev tulemüüri haldus.

Täiendavad soovitused tööstusautomaatika võrgusegmenteerimise osas on käesoleva dokumendi Lisas 1.

Site-to-site VPN tunnelite puhul soovitame vältida paroolipõhist autentimist, kui see ei ole võimalik, peab igal tunnelil olema oma turvaline parool, mida tuleb mõistliku aja tagant vahetada (IT töötajate vahetumine, parooli leke, poliitikas täpsustatud aeg). Paroolide asemel soovitame kasutada sertifikaadipõhist autentimist.

L2. Turvapaigad on paigaldamata kriitilistes segmentides

RISK: Kõrge CVSS: 8,5	Parandamise keerukus: Keskmine

Tähelepanek:
- 2. serveri ja 14 tööjaama operatsioonisüsteem on uuendamata ning kasutatakse tuntud turvanõrkustega versiooni
- Kuna serverite ja tööjaamade kontorivõrgust ligipääs tööstusautomaatika serveritele, on võimalik turvanõrkuse CVE-2018-23222 ja teiste abil ründajal ligi pääseda tööstussseadmetele.

Tööjaamade ja serverite kaudu on võimalik tuntud ja kõrge CVSS skooriga turvanõrkuste abil ründajal saada kas automatiseeritud skriptide, skännimise või siis õngitsuskirjade kaudu ligipääs kogu ettevõtte informatsioonile ning ka tööstusseadmetele.

Soovitused:
Soovitame juurutada inventuuripoliitikat ja turvapaigaldamise poliitikat, mis tekitaks keskselt teadlikkuse sellest, millised seadmed on uuendatud ja millistel võib olla puuduseid. Seadmed, millel pole võimalik ärikriitilisuse tõttu turvapaikasid õigeaegselt paigaldada, tuleks eraldada segmenteerimise käigus teise tsooni ning lubada internetisuunalist liiklust vaid vajaduspõhiselt.

Ilmnenud probleemide koondtabel

Probleem	Risk	Parandamise keerukus:	Prioriteetsus
Nõrk võrgu planeerimine	Kõrge	Keskmine	1
Turvapaigad on puudu	Kõrge	Keskmine	2

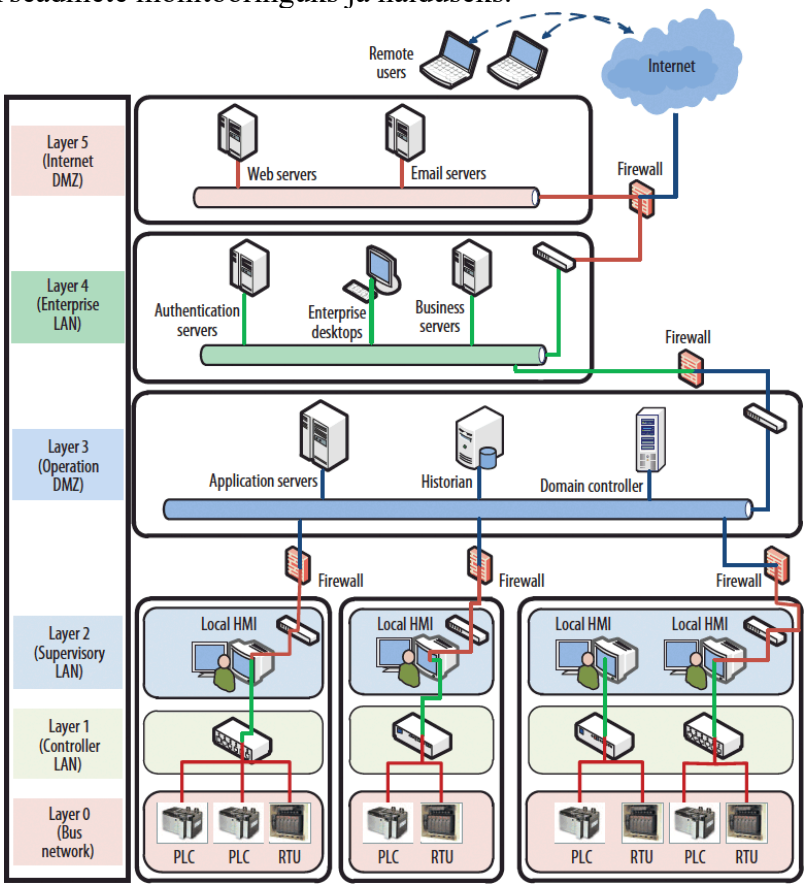
1 aasta soovituslik tegevuskava

Lähtudes eelpool väljatoodud nõrkustest soovitame järgnevaid samme ettevõtte turvalisuse tõstmiseks järgmise 12 kuu jooksul.

1. Turvapaigaldamise ja inventeerimise poliitika väljatöötamine, tehnoloogia soetamine ja juurutamine
    a. Inventuuri tellimine teenusena ja/või vastava tehnoloogia juurutamine ettevõtte infosüsteemides, et olukorrapilti parandada
    b. Turvapaikade paigaldamine
    c. (Vajadusel) uute litsentside soetamine
    d. Turvapaigaldamise ja inventeerimise poliitika ja protsesside kirjeldamine dokumentatsioonis, sealhulgas turvapoliitika väljatöötamine seadmete jaoks, millel pole võimalik ärikriitilisuse tõttu turvapaikasid õigeaegselt paigaldada.
2. Võrgu segmenteerimise planeerimine ja elluviimine
    a. Protsesside kaardistamine
    b. Võrgu segmenteerimise plaani koostamine
    c. Ärikriitiliste seadmete testimine eraldatud võrkudes
    d. Vajalike seadmete soetamine ja testimine
    e. Migratsioon
3. Ettevalmistavad tegevused infoturbepoliitika raamistiku (E-ITS, ISO, CIS18, vms) rakendamiseks
    a. Vastutava töötaja värbamine/määramine
    b. Tööprotsesside kaardistamine ja skoobi ettevalmistamine

LISA 1 – Tööstusautomaatika võrkude segmenteerimise põhimõtted
Võrkude segmenterimisel soovitame lähtuda allolevast joonisest ja planeerida vähemalt järgmised turvadomeenid

- DMZ (Internet DMZ) - teenuste jaoks, mis peavad olema avalikult kättesaadavad.
- Külaliste/WiFi võrk - külaliste juurdepääs Interneti.
- Kontori võrk (Enterprize LAN)- tavakasutajate tööjaamad.
- IT süsteemide administraatorite tööjaamad.
- SCADA DMZ (Operation DMZ) – Teenuste jaoks mis peavad olema saadaval SCADA seadmete monitooringuks ja halduseks.



https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/IoT_Security_Lab/IEC62443_WP.html

Näiteid juurdepääsu põhimõtetest:

- DMZ'sse paigutatud masinatest sisevõrku ühenduste algatamine on üldjuhul keelatud.
- Serverite segmendist on Internetti ligipääs lubatud ainult uuenduste ja paikade allalaadimiseks (Windows updates, Linux'i repositooriumid). Tavaline Internetis surfamine serveritest peab olema keelatud.
- Serverite administreerimisliidestele pääseb ligi ainult administraatorite segmendist. Soovitatav on sinna paigutada eraldi n.ö. “jump box”, kuhu on ligipääs ainult administraatoritele üle RDP/SSH.
- Kui segmendis sees olevad masinad omavahel suhtlema ei pea, siis soovitame tööjaamade ja serverite puhul kasutada ka seadmepõhist tulemüüri, mis piirab samas segmendis omavaheliste ühenduste tegemist. Võimalusel tuleks rakendada ka Private VLAN funktsionaalsust. Private VLANi kuuluvatel masinad näevad L2 tasemel ainult gateway liidest.

- Eriti olulised on eelnevad meetmed tööjaamade puhul. Tüüpiliselt võetakse kõigepealt üle tavakasutaja arvuti client-side ründega ja sealt liigutakse edasi teistesse süsteemidesse. Seadmepõhised tulemüürid ja või private VLAN aitavad uute tööjaamade ülevõtmist vältida või vähemalt aeglustada.
- SCADA süsteemide administraatorid ei tohi juurdepääsuks "istuda" samas Layer2 alamvõrgus juhtimisüsteemide liidestega. Häda korral võib üleminekuperioodiks kasutusele võtta JumpPointi SCADA DMZ võrgus.
- Tootjapoolne tugi sh. SCADA süsteemide administreerimisega seotud tegevused peavad käima "Supervisory LAN" kaudu, kohapeal, kohalike administraatorite juuresolekul.
- SCADA süsteemide administraatorite tööjaamad ei tohi asuda samas Layer 2 alamvõrgus juhtimisüsteemide liidestega. Olemasoleva lahenduse puhul soovitame SCADA halduseks kasutada terminal serveri põhist nö "jump box" lahendust, mis võimaldab isikupõhist autentimist ning serveris peab sisalduma kogu halduseks vajaminev tarkvarakomplekt. Kasutaja poolne andmete (failide) edastamine terminal serverisse peab olema keelatud.

Muud põhimõtted:

- SCADA süsteemide administreerimiseks soovitame kasutada täiesti eraldi arvuteid, kust tavapärase kontoritööga seotud tegevusi ei sooritada. Nendel arvutitel tuleb keelata igasugune väline meedia (USB pulgad).
- Hoonetes füüsilised võrgupesad, mida ei kasutata tuleb võrgukommutaatoritest (switch) lahti ühendada või pesad väljalülitatud asendisse seadistada.
- Mitme võrguliidesega ja korraga mitmesse segmenti ühendatud masinate (multi-homed) arv tuleb minimeerida. Juurdepääs ühest segmendist teise peab toimuma ainult läbi tulemüüri.
- SCADA Layer 2 võrgust peab olema keelatud kogu väljuv võrguliiklus ning sisenev liiklus peale halduseks ettenähtud ühenduste.
- SCADA Layer 3 võrgust peab olema keelatud kogu väljuv võrguliiklus peale SCADA monitooringu info edastamise Layer 2 võrku ning sisenev liiklus peale halduseks ettenähtud ühenduste Layer 2 võrgust.