Riigi Infosüsteemi Amet

Euroopa Liit
Euroopa
Regionaalarengu Fond

Eesti
tuleviku heaks

IT-riskianalüüsi näidis ETOdele

11. detsember 2015

1 Näidisettevõtte kirjeldus

AS Soojus on energiasektori ettevõte, kes Morna linnaga sõlmitud operaatorlepingu kohaselt on kohustatud tagama Morna linna territooriumil paiknevate ettevõtete ja elanike sooja tarbevee ja kaugküttega varustamise.

Ettevõtte eesmärk on toota keskkonda säästvat ja taastuvtoorainel põhinevat elektrit ja soojust ning tagada kõigi oma klientide lepinguliste vajaduste katmine.

Ettevõttel on üks modernne ja kõrge automatiseerituse astmega multifunktsionaalne katlamaja, mis asub väljaspool linna piire. Ettevõte toodab elektrit ja soojust peamiselt taastuvtoorainest ja olmejäätmetest, kuid on ümber seadistatav ka gaasiküttele. Toodetud elekter müüakse üldisesse elektrivõrku, toodetavad elektrikogused ei mõjuta oluliselt riigi elektritootmist.

Toimepidevuse kindlustamiseks kuuluvad ettevõttele linnas kaks vana, õliküttel töötavat katlamaja, mis pärast uue energiajaama valmimist suleti. Vanades katlamajades on olemas nädala kütusevarud ja testitulemused kohaselt on nad 48 tunni jooksul võimelised ajutiselt üle võtma linna küttega varustamise. Reservkatlamajad suudavad talveperioodil tagada linna varustamise soojusega minimaalsel tasemel.

Ettevõtte administratiivhoone asub linnas, katlamaja territooriumist väljaspool. Ettevõtte tehnilisel personalil on kontoriruumid katlamaja territooriumil asuvas haldushoones. Samas hoones asuvad ka tööstusautomaatika operaatorite tööruumid.

Ettevõttes töötab 70 töötajat. Ettevõttel on lepingud veetorustike haldamiseks ja veevarustuse tagamiseks AS-iga Morna Vesi ja mitmeid lepinguid tarnijatega tooraine tarnimiseks. Ettevõtte ei korralda ise transporti, vaid on laojääkide jälgimise ja logistika ostnud sisse välistelt partneritelt. Partneritel on kaugligipääs AS Soojus infosüsteemi vajalike laovarude, arvestusliku toorainevajaduse ja tarnete kohaletoimetamise jälgimiseks.

Ettevõtte IT osakonnas töötab kokku kolm töötajat: IT juht, võrguadministraator ja kasutajatoe spetsialist. Lisaks on IT süsteemidega kursis finantsosakonna analüütik, kes tegeleb andmelao arendmise ja jooksva aruandluse koostamisega.

Ettevõtte IT infrastruktuur on suures osas viimase kolme aasta jooksul uuendatud või välja vahetatud. Seoses uue katlamaja kasutusele võtuga võeti kasutusele ka moodsad tööstusautomaatika seadmed, mis võimaldavad katelde töö juhtimist üle arvutivõrgu. Eelmisel aastal viidi lõpule võrkude segmenteerimine, mille käigus eraldati kontorivõrk ja tööstusautomaatika võrgud. Ettevõte ei tegele tarkvara arendusega, valdavalt kasutatakse turul tuntud tarkvarasüsteeme. Spetsiaaltarkvara arenduseks ja halduseks on sõlmitud arenduslepingud tootjatega. Olemasolevad infosüsteemid on kaardistatud, olulistemal süsteemidel on olemas ka varundus- ja taasteplaanid.

Vastavalt hädaolukorra seadusele käsitletakse kaugküttesüsteemi ja –võrgu toimimist elutähtsa teenusena. AS Soojus on koostanud ka toimepidevuse riskianalüüsi. Ettevõte on sätestanud kriitiliste tegevustena peakatlamaja toimimisega seotud tegevused. Ettevõte hindas, et peakatlamaja toimimise jaoks on kriitiliselt tähtis IT-süsteemide, eriti Tootmisinfosüsteemi toimimine.

2 Sisendid IT-riskianalüüsi läbiviimiseks

2.1.1 Infosüsteemide kaardistus

Infosüsteemide kaardistus on läbi viidud AS Soojuse IT osakonna ja infovara omanike koostöös enne riskianalüüsi teostamist. IT osakonna vastutab infovarade registri regulaarse ülevaatamise ja vajadusel selle uuendamise eest.

AS Soojus on oma infosüsteemide kaardistamisel lähtunud ISKE etalonturbe metoodikast ning eelnevalt määranud oma infovaradele ISKE turvaklassid. Turvaklasside määramisel lähtuti järgmistest näitajatest:

Käideldavus (K) –õigeaegne ja hõlbus andmete kättesaadavus volitatud tarbijale.

K0 – töökindlus madal, lubatud summaarne tööseisak on üle 1 ööpäeva nädalas;

K1 – lubatud summaarne seisak nädalas kuni 1 ööpäev;

K2 – lubatud summaarne seisak nädalas kuni 2 tundi;

K3 – lubatud summaarne seisak nädalas kuni 10 minutit

Terviklus (T) - andmete õigsuse tagatus, päritolu autentsus ja volitamatute muutuste puudumine.

T0 – info allikas, info muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontrollid pole vajalikud;

T1 – info allikas, info muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse ja ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele;

T2 – info allikas, info muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalik info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;

T3 – info allikal, info muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

Konfidentsiaalsus (S) – andmete kättesaadavus ainult selleks volitatud tarbijaile ning kättesaamatus kõigile ülejäänutele.

S0 – avalik info: juurdepääsu teabele ei piirata, st lugemisõigus kõigil huvitatutel, muutmise õigus määratletud tervikluse nõuetega;

S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatud juurdepääsu taotleva isiku õigustatud huvi korral;

S2 – salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;

S3 – ülisalajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Antud näite lähteandmete põhjal koostatud töötabelid on esitatud eraldiseisvas Exceli failis (vt **Naidisettevotte_riskide_kaalutlemine.xls).**

Infosüsteemide kaardistuse tulem on esitatud järgmises tabelis:

Infosüsteem	Omanik	Turvaklass
Finantsarvestuse tarkvara	Pearaamatupidaja	K2T2S2
Personalitarkvara	Personalijuht	K1T2S2
Klienditarkvara	Müügijuht	K1T1S1
Andmeladu	Finantsdirektor	K1T1S1
MS Office kontoritarkvara	IT juht	pole määratud
MS Exchange grupitöötarkvara	IT juht	K3T1S2
Dokumendihaldussüsteem	IT juht	K1T1S1
Varundustarkvara	IT juht	K2T1S2
Viirustõrjetarkvara	IT juht	K2T1S1
Intranet	IT juht	K0T1S1
Veebileht	Turundusjuht	K3T1S0
Videovalvesüsteem	Haldusjuht	K1T2S2
Uksekaardisüsteem	Haldusjuht	K3T2S2
Soojusarvestuse tarkvara	Automaatikaosakonna juhataja	K3T1S1
Kaaluprogramm	Tootmisjuht	K3T1S1
Tootmisinfosüsteem	Tootmisjuht	K3T1S2
Tööstusautomaatika SCADA	Automaatikaosakonna juhataja	K3T1S2
Võrgu Monitooringusüsteemid	Tootmisjuht	K2T1S1
Tehnohoolde infosüsteem	Automaatikaosakonna juhataja	K2T1S1

Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Infosüsteemid

Väljavõte ettevõtte IT inventari kataloogist:

Inv.nr.	Infovara	Spetsifikatsioon	Soetamisaeg	Vastutaja
xxx	Domeenikontroller	xxx	xxx	xxx
xxx	Windows server	xxx	xxx	xxx
xxx	Linux server	xxx	xxx	xxx
xxx	Windows 7 töökohad	xxx	xxx	xxx
xxx	Windows XP töökohad	xxx	xxx	xxx
xxx	Sülearvutid	xxx	xxx	xxx
xxx	VMWARE virtuaalserverid	xxx	xxx	xxx
xxx	Võrguseade XXX1	xxx	xxx	xxx
xxx	Andmebaasiserver	xxx	xxx	xxx
xxx	Võrguseade XXX2	xxx	xxx	xxx
xxx	Väline tulemüür	xxx	xxx	xxx
xxx	Sisene tulemüür	xxx	xxx	xxx
xxx	Kontori WiFi seadmed	xxx	xxx	xxx
xxx	Külaliste WiFi seadmed	xxx	xxx	xxx
xxx	Tsentraalne UPS	xxx	xxx	xxx
xxx	SAN kesksalvestusseadmed	xxx	xxx	xxx
xxx	Arvutivõrk	xxx	xxx	xxx
xxx	Printerid	xxx	xxx	xxx

Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Infovarad

2.1.2 Kriitiliste protsesside ja kriitiliste tegevuste määramine

AS Soojus on teostanud eelmistel aastatel toimepidevuse riskianalüüsi, milles on määratletud kriitilise protsessina soojusenergia tootmise. Ettevõtte teist põhiprotsessi, elektrienergia tootmist, ei loeta elutähtsaks teenuseks, sest selle teenuse osutamine AS Soojus poolt ei oma otsest mõju teenuse tarbijatele aga tekita neile teenuse katkemist.

Soojuseenergia tootmiseks on kriitilise tähtsusega paekatlamaja häireteta töö. Seega määras elutähtsa teenuse osutaja kriitilise tegevusena peakatlamaja toimimise.

2.1.3 Ärimõjude analüüs

AS Soojus juhatuse poolt kinnitatud analüüsi kohaselt algavad tõsised probleemid siis, kui katlamaja katkestus talveperioodil kestab kauem kui üks ööpäev (MTD = 24h). Paraku ei suudeta varukatlamajasid (alternatiivne võimalus) tööle saada enne kui kahe ööpäeva möödudes. Järelikult tuleb kaardistada riskid ja kasutusele võtta meetmed, mis vähendaksid peakatlamaja toimimisega seotud infosüsteemide katkestuste võimalikud tekkepõhjused. Infosüsteemide taastamiseks on püstitatud eesmärk saada need uuesti tööle hiljemalt 8 tunni jooksul pärast katkestuse algust (RTO=8h). See jätaks piisavalt aega vajalikeks muudeks tegevusteks, et kogu teenus tööle saada maksimaalselt 24 tunni jooksul.

2.1.4 Aktsepteeritava turvataseme määramine

AS Soojus juhatus hindas, et tulenevalt piiratud ressurssidest ning lähtudes olulisuse printsiibist, aktsepteeritakse vaikimisi kõik väga madalad ja madalad riskid. Täiendavaid investeeringuid kaalutakse alates riskitasemest R3 – Kõrge risk (vt. „IT riskianalüüsi koostamise juhend ETOdele“, tabel 4 Riskiklasside kirjeldused) .

3 IT riskianalüüs ja riskide hindamine

3.1.1 Kriitiliste tegevuste toimimise jaoks vajalike infosüsteemide määratlemine

Järgmises tabelis on esitatud toimepidevuse riskianalüüsist ja muudest juhtkonna poolt tehtud riskijuhtimisotsustest saadud sisend kriitiliste infovarade määratlemiseks. Järgnevalt teostatud analüüsi käigus tuvastati, et peakatlamaja toimimisega on seotud neli erinevat infosüsteemi. Kõik need süsteemid ei ole tingimata vajalikud tööle saada, sest katlamaja võib toimida ka mittetäieliku IT funktsionaalsusega, tootmisandmete statistika olemasolu ei ole kriitiline funktsionaalsus ja arvete genereerimiseks vajaliku info saab hiljem sisestada ka käsitsi.

Igale infosüsteemil on määratud infosüsteemi omanik. Infosüsteemi omanik on ettevõtte töötaja, kes vastutab selle protsessi toimimise eest, millega antud infosüsteem kõige rohkem seotud on. Infosüsteemi omanik on üldjuhul äripoolelt. Infosüsteemi omanik võib delegeerida infosüsteemiga seotud infovaradega tehtavad toimingud kas vastava äriüksuse töötajale või IT töötajale, kuid vastutus infosüsteemi toimimise eest jääb endiselt infosüsteemi omanikule.

Antud näite korral olid infosüsteemide omanikud määratud riskianalüüsile eelneva IT varade kaardistuse käigus (Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Infosüsteemd). Riskianalüüsi käigus kontrolliti üle, kas omanikud on oma kohustustest teadlikud.

Kriitilise tegevuse sõltuvus infosüsteemist määrati kasutades järgnevat skaalat :

1 – sõltuvus ei ole eriti oluline

2- sõltuvus on oluline, aga on olemas alternatiivne lahendus

3 – sõltuvus on kriitiline

Kriitiline tegevus	Kriitilise tegevuse toimimiseks vajalik infosüsteem	Infosüsteemi kirjeldus	MTD	RTO	Teenuse pakkuja/ asukoht	Kasutajad/ omanik	Kriitilise tegevuse sõltuvus infosüsteemist/ IKT teenusest
Peakatlamaja toimimine	Tootmis-infosüsteem	Põhisüsteem katlamaja töö juhtimiseks	24 h	8 h	Põhiasukoht	Tootmisjuht	3
Peakatlamaja toimimine	Uksekaardi-süsteem	Pääsukaardil põhinev juurdepääsusüsteem	24 h	8 h	Põhiasukoht	Haldusjuht	1
Peakatlamaja toimimine	Soojus-arvestuse tarkvara	Tarkvara, mis kogub tootmisandmeid andmelao jaoks	24 h	8 h	Põhiasukoht	Tootmisjuht	2
Peakatlamaja toimimine	Kaalu-programm	Katla sisendi koguste reguleerimine ja kontroll	24 h	8 h	Põhiasukoht	Tootmisjuht	2
Peakatlamaja toimimine	Tööstus-automaatika SCADA	Automaatikaseadme andurite töö juhtimine ja tulemuste edastamine tootmisinfosüsteemi	24 h	8 h	Põhiasukoht	Automaatika osakonna juhataja	3

Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Kriitilised süsteemid

Tabel on kirjeldatud IT riskianalüüsi koostamise juhendi lisas 1 Elutähtsa teenusetoimepidevust mõjutavad infosüsteemid.

3.1.2 Infosüsteemidega seotud infovarade leidmine

Järgnevas näites teostatakse ainult IT riskianalüüsi esimene iteratsioon, lähtudes ainult tuvastatud peakatlamaja toimimisega kriitilises sõltuvuses olevaid infosüsteemidest, milleks on Tootmisinfosüsteem ning tööstusautomaatika SCADA süsteem.

Riskianalüüsi tuleks praktikas korrata ka nende infosüsteemidega, millest kriitiline tegevus otseselt ei sõltu ja mis ei põhjusta otseselt teenuse pikaajalist katkemist, kuid võivad sisaldada olulisi kahjusid seoses konfidentsiaalsuse ja tervikluse kaoga. Antud näite puhul on selleks Soojusarvestuse tarkvara, mis sisaldab klientide andmeid ning mille alusel arvutatakse välja klientidele esitatavad arved.

Lähtudes infovarade kaardistusest, IT osakonna halduses olevast infosüsteemide dokumentatsioonist ja intervjuudest IT töötajatega, täideti ära tabel, mille aluseks on IT riskianalüüsi koostamise juhendi lisa2 Infosüsteemidega seotud infovarad.

Kriitiline tegevus	Kriitilise tegevuse toimimiseks vajalik infosüsteem	Infosüsteemi toimimiseks vajalik infovara	Infovara kirjeldus	MTD	RTO	Teenuse pakkuja/ asukoht	Kasutajad/ omanik
Peakatlamaja toimimine	Tootmisinfosüsteem	Linux server	Server, millele on paigaldatud tootja poolt tootmistarkvara	24 h	8 h	Korpus I Serveriruum	Võrguadministraator
Peakatlamaja toimimine	Tootmisinfosüsteem	Tootmistarkvara	Spetsiaaltarkvara	24 h	8 h	Korpus I Serveriruum	Tootmisjuht
Peakatlamaja toimimine	Tootmisinfosüsteem	Arvutivõrk	Katlamaja arvutivõrk	24 h	6 h	Korpus I	Võrguadministraator
Peakatlamaja toimimine	Tootmisinfosüsteem	Windows 7 tööjaam	Operaatori tööjaam süsteemi halduseks	24 h	8 h	Operaatoriruum	Operaator/IT
Peakatlamaja toimimine	Tootmisinfosüsteem	Sisemine tulemüür	Tootmisvõrgu ja kontorivõrgu vahel	24 h	8 h	Korpus I Serveriruum	Võrguadministraator
Peakatlamaja toimimine	Tootmisinfosüsteem	Võrguseadmed	Katlamaja arvutivõrgu võrguseadmed	24 h	8 h	Serveriruum	Võrguadministraator
Peakatlamaja toimimine	Tööstusautomaatika SCADA	Automaatikaseadmed	Katlamaja opereerimiseks kasutatavad tööstusseadmed	24 h	6 h	Korpus I	Peaautomaatik
Peakatlamaja toimimine	Tööstusautomaatika SCADA	Kontrollerite tarkvara	Tööstusseadmete programmid ja põhivara	24 h	6 h	Korpus I	Peaautomaatik
Peakatlamaja toimimine	Tööstusautomaatika SCADA	Arvutivõrk	Katlamaja arvutivõrk	24 h	6 h	Korpus I	Võrguadministraator
Peakatlamaja toimimine	Tööstusautomaatika SCADA	Võrguseadmed	SCADA võrguseadmed	24 h	6 h	Korpus I seadmekapp	Võrguadministraator

Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Kriitilised infovarad.

Infosüsteemi toimimiseks vajalike infovarade määramisel võib sarnased infovarad, mille mõju infosüsteemile on sarnane ja millel on ühine omanik, grupeerida kokku ühise nimetaja alla.
Niimoodi tekitati tabelisse kirje „Võrguseadmed“, kuigi infovarade inventuuris on kirjeldatud iga võrguseade omaette reana.
Infovara omanik on ettevõtte töötaja, kellele on määratud vastutus infovara turvalisuse ja hoolduse eest. Infovara omanik võib, aga ei pruugi olla sama isik, kes on infosüsteemi omanik. Antud näite puhul IT infrastruktuuri eest vastutus delegeeritud IT osakonda.
Üks infovara võib olla oluline komponent mitme infosüsteemi jaoks (antud näite puhul on selleks „Arvutivõrk“), sellisel juhul määrab infovara MTD ja RTO väärtused kõige väiksemate lubatud parameetritega infosüsteem (antud näite puhul „Tööstusautomaatika SCADA“ .

3.1.3 Ohtude tuvastamine

Ohtude tuvastamisel otsustati antud näite korral tugineda järgmisele kompaktsele ohtude registrile ja analüüsida süstemaatiliselt ükshaaval läbi kõik eelnevald kaardistatud kriitilised infovarad.

- füüsiline kahjustus
- loodussündmus

- elektrikatkestus
- võrgukatkestus
- tarkvara viga
- riistvara viga
- seadme rike
- küberrünne
- füüsiline rünne
- kasutaja viga
- administreerimisviga
- välise teenusepakkuja viga

Juhul, kui infovarasid on palju või ohtude register on liiga mahukas, kasvab võimalike kombinatsioonide arv kiiresti liiga suureks ja nende formaalne kirjeldamine ja analüüsimine tabeli kujul muutub liiga töömahukaks. Sellisel juhul on otstarbekas tabelisse kanda ainult eelneva ajurünnaku käigus reaalsete ohustsenaariumitena tunduvad infovara ja ohtude kombinatsioonid.

Tulemused kanti järgmisse tabelisse, mille aluseks on IT riskianalüüsi koostamise juhendi lisa 5 Elutähtsa teenuse osutaja infosüsteemidega seotud riskid (täidetakse veerud „Oht“ ja „Mõjutatud infosüsteemid ja infovarad“).

					Tagajärgede hinnang				
Oht (sündmus või asjaolu, mis võib põhjustada katkestust)	Mõjutatud infosüsteemid ja infovarad	Nõrkused	Raskeim tagajärg	Tõenäosus	K	T	S	Tj	Riski-klass
füüsiline kahjustus	Linux server			2	Ja	Ei	Ei	B	R1
loodussündmus	Linux server			2	Ja	Ei	Ei	B	R1
elektrikatkestus	Linux server			3	Ja	Ei	Ei	B	R2
võrgukatkestus	Linux server			2	Ja	Ei	Ei	B	R1
tarkvara viga	Linux server			3	Ja	Ja	Ja	B	R2
riistvara viga	Linux server			3	Ja	Ei	Ei	A	R1
seadme rike	Linux server			1	Ja	Ei	Ei	A	R1
küberrünne	Linux server	uuendamata tarkvarakomponendid	Kätte saadud administraatoriõiguste pahatahtlik ärakasutamine	2	Ja	Ei	Ja	D	R3
füüsiline rünne	Linux server			2	Ja	Ei	Ei	B	R1
kasutaja viga	Linux server			1	Ja	Ja	Ei	A	R1
administreerimisviga	Linux server			3	Ja	Ja	Ei	B	R2
välise teenusepakkuja viga	Linux server			1	Ja	Ei	Ei	B	R1
füüsiline kahjustus	Tootmistarkvara			0					
loodussündmus	Tootmistarkvara			0					
elektrikatkestus	Tootmistarkvara			3	Ja	Ei	Ei	B	R2
võrgukatkestus	Tootmistarkvara			3	Ja	Ei	Ei	B	R2
tarkvara viga	Tootmistarkvara	testimata uuendused	Valed käsud automaatika juhtimisel põhjustavad süsteemide hävimise	2	Ja	Ja	Ja	D	R3
riistvara viga	Tootmistarkvara			0					
seadme rike	Tootmistarkvara			0					
küberrünne	Tootmistarkvara	uuendamata tarkvarakomponendid	Süsteemi konfiguratsiooni ja andmetega manipuleerimine põhjustab süsteemide hävimise	1	Ja	Ja	Ei	D	R3
füüsiline rünne	Tootmistarkvara			0					
kasutaja viga	Tootmistarkvara			3	Ja	Ei	Ei	B	R2
administreerimisviga	Tootmistarkvara			3	Ja	Ei	Ei	B	R2
välise teenusepakkuja viga	Tootmistarkvara	inimliku eksimuse võimalikkus	Tänu andmete ja konfiguratsiooni tahtmatule kustutamisele tekib pikaajline katkestus	3	Ja	Ja	Ei	C	R3
füüsiline kahjustus	Arvutivõrk			3	Ja	Ei	Ei	B	R2
loodussündmus	Arvutivõrk			2	Ja	Ei	Ei	B	R1
elektrikatkestus	Arvutivõrk			0					
võrgukatkestus	Arvutivõrk			3	Ja	Ei	Ei	B	R2
tarkvara viga	Arvutivõrk			0					
riistvara viga	Arvutivõrk			3	Ja	Ja	Ei	B	R2
seadme rike	Arvutivõrk			3	Ja	Ei	Ei	B	R2
küberrünne	Arvutivõrk			2	Ja	Ei	Ei	C	R2
füüsiline rünne	Arvutivõrk			3	Ja	Ei	Ei	B	R2
kasutaja viga	Arvutivõrk			0					
administreerimisviga	Arvutivõrk			3	Ja	Ei	Ei	B	R2
välise teenusepakkuja viga	Arvutivõrk			2	Ja	Ei	Ei	B	R1
füüsiline kahjustus	Windows 7 tööjaam			4	Ei	Ei	Ei	A	R2
loodussündmus	Windows 7 tööjaam			3	Ei	Ei	Ei	A	R1
elektrikatkestus	Windows 7 tööjaam			4	Ei	Ei	Ei	A	R2
võrgukatkestus	Windows 7 tööjaam			3	Ei	Ei	Ei	A	R1
tarkvara viga	Windows 7 tööjaam			4	Ei	Ei	Ei	A	R2
riistvara viga	Windows 7 tööjaam			4	Ei	Ei	Ei	A	R2
seadme rike	Windows 7 tööjaam			3	Ei	Ei	Ei	A	R1
küberrünne	Windows 7 tööjaam	kasutaja ettevaatamatus, uuendamata tarkvarakomponendid	Tööjaama kasutamine hüppelauana kriitilistesse süsteemidesse tungimiseks	4	Ei	Ei	Ja	C	R3
füüsiline rünne	Windows 7 tööjaam			4	Ei	Ei	Ei	A	R2
kasutaja viga	Windows 7 tööjaam			4	Ei	Ei	Ja	A	R2
administreerimisviga	Windows 7 tööjaam			3	Ei	Ei	Ja	A	R1
välise teenusepakkuja viga	Windows 7 tööjaam			0					
füüsiline kahjustus	Sisemine tulemüür			2	Ja	Ei	Ei	B	R1
loodussündmus	Sisemine tulemüür			2	Ja	Ei	Ei	B	R1
elektrikatkestus	Sisemine tulemüür			3	Ja	Ei	Ei	B	R2
võrgukatkestus	Sisemine tulemüür			2	Ja	Ei	Ei	B	R1
tarkvara viga	Sisemine tulemüür			3	Ja	Ei	Ja	B	R2
riistvara viga	Sisemine tulemüür			3	Ja	Ei	Ei	B	R2
seadme rike	Sisemine tulemüür			3	Ja	Ei	Ei	B	R2
küberrünne	Sisemine tulemüür			2	Ja	Ei	Ja	C	R2
füüsiline rünne	Sisemine tulemüür			2	Ja	Ei	Ei	B	R1
kasutaja viga	Sisemine tulemüür			0					
administreerimisviga	Sisemine tulemüür			3	Ja	Ei	Ja	B	R2
välise teenusepakkuja viga	Sisemine tulemüür			0					
füüsiline kahjustus	Võrguseadmed			3	Ja	Ei	Ei	A	R1
loodussündmus	Võrguseadmed			3	Ja	Ei	Ei	A	R1
elektrikatkestus	Võrguseadmed			3	Ja	Ei	Ei	A	R1
võrgukatkestus	Võrguseadmed			2	Ja	Ei	Ei	A	R1
tarkvara viga	Võrguseadmed			2	Ja	Ei	Ei	A	R1
riistvara viga	Võrguseadmed			3	Ja	Ei	Ei	A	R1

Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Riskitabel

3.1.4 Nõrkuste tuvastamine ja tõenäosuse hindamine

Töötades eelnevalt koostatud riskitabeliga edasi, analüüsiti iga konkreetse infovara ja ohutüübi kombinatsiooni korral infovara võimalikke nõrkusi selle ohu vastu ning selle tulemusena täideti ära Riskitabeli veerg „Tõenäosus“ vastavalt juhendi tabelile 2 Ohu realiseerumise tõenäosuse kriteeriumid.

3.1.5 Tagajärgede hindamine

Kasutades endiselt sama riskitabelit, elimineeriti sealt read, mille riskistsenaariumi tõenäosust peeti olematuks. Ülejäänud riskistsenaariumite korral hinnati intsidendi tagajärgedest tulenevaid kahjusid vastavalt juhendi tabelile 2 Ohu realiseerumise tagajärgede kriteeriumid. Tagajärgede hindamisel arvestati ka ohu mõjudega infovara käideldavusele, terviklusele ja konfidentsiaalsusele.

Täideti riskitabeli tagajärgede hinnangu veerud K, T, S ja Tj .

3.1.6 Riskitaseme mõõtmine

Tagajärje ja Tõenäosuse kombinatsioonina leiti riskistsenaariumile riskiklass (R1 – R5) . Kõrgema riskireitingu saanud riskistsenaariumite omavaheliseks võrdluseks ja täiendavaks analüüsiks dokumenteeriti tabelis infovaraga seotud nõrkused antud ohu vastu ja lisati detailne mõju kirjeldus, mis võib intsidendi puhul juhtuda. On loomulik, et täiendava analüüsi käigus võivad kas tõenäosuse või tagajärgede reiting ning seeläbi ka riskiklass muutuda. Vastavad muudatused kanti ka riskitabelisse.

4 Riskikäsitlus

Riskikäsitlusplaani koostamise aluseks võeti Riskitabelis tuvastatud riskistsenaariumid, mille riskiklass ületas aktsepteeritavate riskide lävendi (antud näite puhul riskiklassid R3, R4 ja R5).

Riskikäsitlusplaan vormistati vastavalt juhendi lisale 7 Riskide loetelu koos turvameetmete rakendamise kavaga.

Risk	Riskiklass	Meede	Meetme maksumus	Meetme rakendamise eest vastutaja	Tähtaeg
Küberrünne Linux serveri vastu	R3	Linux tarkvarakomponetide update, serveri s tehtavate muudatuste monitooringu sisseseadmine	5 000	IT juht	ASAP
Tootmistarkvara tarkvara viga	R3	Kõik live-süsteemi muudatused peavad läbima muudatuste halduse protsessi, tekitada testkeskkond	50 000	IT juht	1.07.2016
Küberrünne tootmistarkvara vastu	R3	Tootmistarkvara versiooniuuendus, mis sisaldab ka teadaolevaid turvaparandusi	130 000	IT juht	Teostataks e täiendav analüüs
Välise teenusepakkuja viga tootmistarkvara konfigureerimisel	R3	Kõik live-süsteemi muudatused peavad läbima muudatuste halduse protsessi, piirata välise teenusepakkuja juurdepääs tootmiskeskkonnale	50 000	IT juht	1.07.2016
Küberrünne administreerimiseks kasutatava tööjaama vastu	R3	Piirata administreerimiseks kasutatava tööjaama pääs internetti, tarkvarakomponentide uuendamine,	1000	IT juht	ASAP
Automaatikaseadmete füüsiline kahjustumine	R3	Võtta kasutusele meetmed seadmete paremaks märgistamiseks ja kaitseks kuumuse ning niiskuse eest	1 000	Automaatika osakonna juhataja	ASAP
Küberrünne SCADA kontrollertarkvara vastu	R3	Kontrollerite tarkvara uuendus, piirata juurdepääs seadmetele	20 000	Automaatika osakonna juhataja	1.03.2016

Tabel: Naidisettevotte_riskide_kaalutlemine.xls - Riskikäsitlusplaan

Riskikäsitlusplaani täiendati konkreetselt sõnastatud riskikäsitlusmeetmega, samuti anti hinnang meetme eeldatavale maksumusele. AS Soojus juhtkond kinnitas riskikäsitlusplaani, misjärel määratati igale meetmele selle rakendamise tähtaeg ja vastutaja ning eraldati selleks vajalikud ressursid. Sõltuvalt meetme maksumusest võidakse ka valida mõni muu riskikäsitlusmeetod, antud juhul otsustati läbi viia täiendav analüüs tootmistarkvara versiooniuuenduse otstarbekuse kohta. Kõik tehtud riskikäsitlusotsused dokumenteeriti riskikäsitlusplaanis ja kinnitati juhatuses