Tallinna Ülikool
Informaatika instituut

Jüri Schkiperov

JUHTIMISSÜSTEEMIDE IT TURVARAAMISTIKU LOOMINE AS EESTI RAUDTEE NÄITEL

Magistritöö

Juhendaja: Andro Kull, PhD

Autor: ..... „.....“ 2012

Juhendaja: ..... „.....“ 2012

Instituudi direktor: ..... „.....“ 2012

Tallinn 2012

Autorideklaratsioon

Deklareerin, et käesolev magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....
(kuupäev) (autor)

Sisukord

Sissejuhatus

Tänapäevases maailmas puutume me pidevalt kokku erinevate IT lahendustega. Olgu see riistvaraline tahvel-, süle- või lauaarvuti, mobiiltelefon, pangaautomaat või tarkvaraline operatsioonisüsteem, kontoritarkvara või internetirakendus infoportaali, sotsiaalmeedia kogukond, vajavad need kõik lihtsalt ja turvalist keskkonda. Paljud IT lahendused toimetavad taustal, on meile praktiliselt märkamatud kuna neid kasutatakse erinevate tehnoloogiliste lahenduste juhtimisel nt. laevade, lennukite ja rongide juhtimine; mobiilside juhtimine; tehaste tehnoloogia juhtimine; tuumaelektrijaama seadmete juhtimine; jne.

Tavakodaniku maailmapildis räägitakse temale oluliste süsteemide nt. e-mail, sotsiaalmeedia, jne. turvalisusest, kuid suures pildis on raske eirata taustalahenduste turvalisust. Mida arvutiseeritusmaks muutuvad erinevad lahendused, seda suuremaks lähevad ka probleemid ja esile kerkivad juhtimissüsteemide tehniliste lahenduste turvamehhanismide väljatöötamine. Probleeme on tekitanud keeruline Stuxnet worm, mis põhjustas probleeme Siemens juhtimissüsteemides (Geer 2011: 13, 24), erinevad võrgurünnakud kriitiliste infrastruktuuride pihta (Stiennon 2010), katkestused EMT ja Elioni sidevõrgus, Swedbanki soov viia oma serverite infrastruktuuri väljapoole Eestit.

Lahendusi, mis kontrollivad ja juhivad erinevaid infrastruktuuri ja tööstuse tehnilisi lahendusi jagatakse suures plaanis kaheks: järelvalve ja andmete kogumise süsteemid (SCADA) ja hajutatud juhtimissüsteemid (DCS). Antud lahendused oleksid näiteks elektri- ja veevarustus, kommunikatsioonisüsteemid, transpordi juhtimine, jne. Ilma selliste süsteemideta ei suudaks me tänapäevases ühiskonnas toimida. Turvalisus antud süsteemides on võtmeküsimus meie elustandardi hoidmisel ja kaitsmisel. Loodud on erinevaid standardeid ja raamistike erinevatele lahendustele, kuid ühtset ja universaalset ei ole veel välja töötatud ja arvatavalt ei olegi seda võimalik mõistlikult teha. Järgides erinevaid spetsiifilisi nüansse erinevatel valdkondadel on loodud mitmeid üldisi turbe standardeid, mis põhinevad erinevate ettevõtete parimate turbe praktikatel ja on kooskõlas üldise turvalisuse reeglitega.

Magistritöö eesmärk on luua raudtee juhtimissüsteemide IT infrastruktuuri üldine turvaraamistik AS Eesti Raudtee näitel. Töös soovitakse leida võimalikult optimaalne lahendus, kasutades ära levinuimaid standardeid, soovitusi ja parimaid praktikaid.

Töös käsitletakse järgmisi uurimisküsimusi:

- Milliseid IT standardeid, soovitusi, parimaid praktikaid, jne. kasutatakse juhtimissüsteemides?
- Missugused oleksid raudteele sobilikud põhilised IT juhtimissüsteemide alased standardeid, soovitusi, parimaid praktikaid, jne. mille alusel luuakse raudtee juhtimissüsteemide turvaraamistik?
- Millised oleksid konkreetsed juhendid ja turvameetmed?
- Mida peaks tulevikus veel ette võtma, et suurendada süsteemi IT alast turvalisust?

Autorile teadaolevalt ei ole Eestis sellist valdkonda varem vaadeldud. Raudtee kui kriitilise infrastruktuuri pakkuja ja suure ohu allikas, peab omama kindlapiirilist juhtimissüsteemide IT turvalist käitlemisel (EN 2008). Kuna erinevad SCADA ja DCS lahendused on paljudes turvakäsitlustes ühtlustunud, siis käsitletakse neid töös juhtimissüsteemide nime all. Raamistiku väljatöötamiseks on palju erinevaid lahendusi ja kindlasti ei saa ükski neist olla üks ja ainuõige. Magistritöö on keskendunud küll konkreetse ettevõtte lahenduse raamistikule, kuid kindlasti on võimalik seda edasi arendada, üle võtta ka teistel raudtee transpordisektori ja kriitilise infrastruktuuriettevõtetel.

1. Infoturve

1.1. Infoturbe mõiste

Infoturve on info ja infosüsteemi kaitsmine loata ligipääsu, kasutamise, publitseerimise, muutmise ja hävitamise eest. Ettevõttele on oluline vähendada infovarade kasutamisest tulenevaid ohte ja viia riskid minimaalse lubatud tasemeni.

IT turve koosneb kolmest põhilisest väärtusest (RIA 2009):

1. **Käideldavus** - eelnevalt kokkulepitud vajalikul/nõutaval tööajal kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus (st vajalikul/nõutaval ajahetkel ja vajaliku/nõutava aja jooksul) selleks volitatud tarbijaile (isikutele või tehnilistele vahenditele);
2. **Terviklus** - andmete õigsuse/täielikkuse/ajakohasuse tagatus ning päritolu autentsus ja volitamatute muutuste puudumine.
3. **Konfidentsiaalsus** - andmete kättesaadavus ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele andmetele peavad ligi pääsema ainult volitatud kasutajad.

Üha enam ähvardab organisatsioone ja nende infosüsteeme erinevad ohud nt. arvutipõhised pettused, vandalism, üleujutused, jne. Paljud infosüsteemid ei ole kavandatud ülimalt turvaliseks. Tehnilise turvalisuse vahendite kõrvale on vaja erinevaid sobivad haldusi, protseduure ja meetmeid. (EVS 2008:7)

Infoturbe esimeseks sammuks (EVS 2008:8) on turvanõuete väljaselgitamine:

1. üks allikas tuleneb organisatsiooni seest riskide kaalutlemisest. Riskide kaalutlemiseks on erinevad riskide meetodid. Riskidega tuleb kogu aeg ja korrapäraselt tegutseda;
2. teine allikas on õigusaktid, eeskirjad jne. nõuded mida peavad organisatsiooni enda kõrval täitma ka kõik kolmandad osapooled;
3. kolmas allikas on konkreetse infotöötluse printsiipide, eesmärkide ja talitusnõuete kogum, mille on organisatsioon välja töötanud tegevuse toetuseks.

Järgnevaks sammuks (EVS 2008: 9) on turvameetmete valimine. Valik luuakse konkreetse ettevõtte vajadustest lähtuvalt.

Võib kasutada mingit konkreetset standardit ja teha kõik tegevused ainult antud standardi järgi. Reaalsuses on seda raske ellu viia, kuna iga ettevõte on omamoodi eriline ja võimalik on kasutada erinevaid standardeid, soovitusi, parimaid praktikaid ja panna kõik erinevad sammud kokku ja luua ettevõtte spetsiifiliste suunistega sisemine turvastandard.

1.2. Infoturbe standardimine

Turbestandardeid võiks jagada kahte suuremasse rühma:

1. Konkreetsele andmeturbe metoodikale suunatud - standardis on kirjeldatud konkreetsed tegevused konkreetse lahendusele e. on loodud etalon, mille järgi tuleb joonduda. Sellesse rühma liigitub nt. ISKE (RIA 2011).
2. Kontrolli metoodikale suunatud - standardis vaadeldakse üldisi äriprotsesse ja IT süsteeme, määratletakse ohud/riskid ja kontrollitakse olemasolevaid rakendatud turvameetmeid. Standardid on välja töötatud peamiselt paremate praktikate järgi. Sellisesse rühma liigitub näiteks ISO ja IEC koostöös loodud standardite kogu ISO/IEC 27000.

Kindlasti on võimalik turbestandardeid liigitada veel mitut erinevat moodi. Tähele tuleb panna, et pole olemas ühest ja ainsamat IT turbestandardit, mis sobiks kõigisse ettevõtetesse ja asutustesse. Rahvusvaheliselt tunnustatud standardid on üldjuhul mahukad ja tavaliselt sobib suurematele ettevõttetele. Väiksematele ettevõtetel on loodud väiksemad parimate praktikate soovitused.

2. Juhtimissüsteemid

Esimese generatsiooni juhtimissüsteemid loodi kohalikule juhtimisele. Kõik süsteemid olid eraldi ja ei omanud omavahelisi ühendusi. Kogu süsteem oli üles ehitatud kindlate tarnijate toodangule ja kui olid loodud ühendused keskse süsteemiga, siis olid need väga algelised. Varusüsteem oli loodud selliselt, et kõik seadmed olid dubleeritud ja korraga töötas üks süsteem. (NCS 2004: 10)

Teise generatsiooni lahendused olid juba edasiarenenud ja kasutasid võrku omavaheliseks infovahetuseks. Paljud seadmed, tarkvara ja võrguprotokollid olid tootjakesksed ja seega ei ühildunud ühegi teise tarnijaga. Varusüsteemid olid juba täiustunud ja süsteemid olid pidevas töös. Enam ei pidanud süsteemid ootama kui varusüsteem ülesse tuli ja võttis üle põhisüsteemi töö, vaid kõik toimus koheselt ja automaatselt. (NCS 2004: 10)

Hetkel kasutatakse kolmanda generatsiooni seadmeid. Süsteemid on rohkem avatud ja universaalsemad, kuid siiski on päris palju tootjapõhiseid lahendusi. Rõhuasetus on kesksetel süsteemidel, võrgul ja töökindlusel. Kasutusele on võetud IP võrgud ja suurem vastupanu õnnetustele, mis lubab protsesse jaotada üle kogu võrgustiku ja ühe süsteemi hävinemine võimaldab jätkata tööd teises kohas. (NCS 2004: 12)

Algselt olid süsteemid loodud töötama järjestikahela võrgus, mis olid täiesti eraldatud teistest võrkudest. Järjestikahela võrgud olid loodud üks-ühele kommunikatsiooniks ja nende tehnoloogiad olid üpris piiratud ja mingit võrgu monitooringut ja turvalisust polnud vaja sellisesse lahendusse sisse programmeerida. Kuna kasutusel polnud hetkel juba laialt levinud TCP/IP võrke, siis polnud mingeid probleeme viiruste, häkkerite jne. Seoses IP võrkude levikuga juhtimissüsteemidesse on tekkinud suuremad ohud, sest juhtimissüsteemid viidi üle kaasaegsesse võrgumaailma, kuid kommunikatsioonilahenduste loogika jäi pahatihti järjestikahela aegsesse ajajärku.

Tabel 1. Tava IT ja juhtimissüsteemide lahenduste võrdlus (autor; DHS 2009: B-7; (Falco, Stouffer, Scarfone 2011:3-1 - 3-4; ENISA 2011:1.1.4)

Valdkond	**Tava IT**	**Juhtimissüsteemid**
Toodete eluiga	3..5 aastat	üle 20 aasta
Standardiseeritus ja ühilduvus	kõrge	madal
Riskid haldamine	suunatud andmete konfidentsiaalsusele ja täielikkusele tagamisele	protsessi kaitse ja inimeste turvalisus
Antiviirused ja muud turvalisusvahendid	tavaliselt ja laialt levinud	väheselt levinud ja raskesti rakendatavad
Operatsioonisüsteemid ja tarkvarad	kiires uuenemises, kiiresti võimalik kasutusele võtta	aeglaselt arendatavad, kasutuselevõtmine piiratud

Valdkond	**Tava IT**	**Juhtimissüsteemid**
Süsteemi paranduste väljalaskmine	kiire	aeglane
Süsteemi uuendused	kiire	aeglane, üleval hoitakse eelmiste põlvkondade tehnoloogiaid
Süsteemide ajakriitilisus	viivitused ja seiskud on aktsepteeritavad	kriitiline tähtsus ära hoida seisakuid
Kättesaadavus	viivitused ja seiskud on aktsepteeritavad	24 x 7 x 365
Turvateadlikus	üpris hea	vanast eraldatuse harjumusest vilets
Füüsiline ligipääsetavus ja turvalisus	lihtne ja kõrge	tihti eraldiseisvates kaugetes kõrvalistes kohtades ja väga kõrge

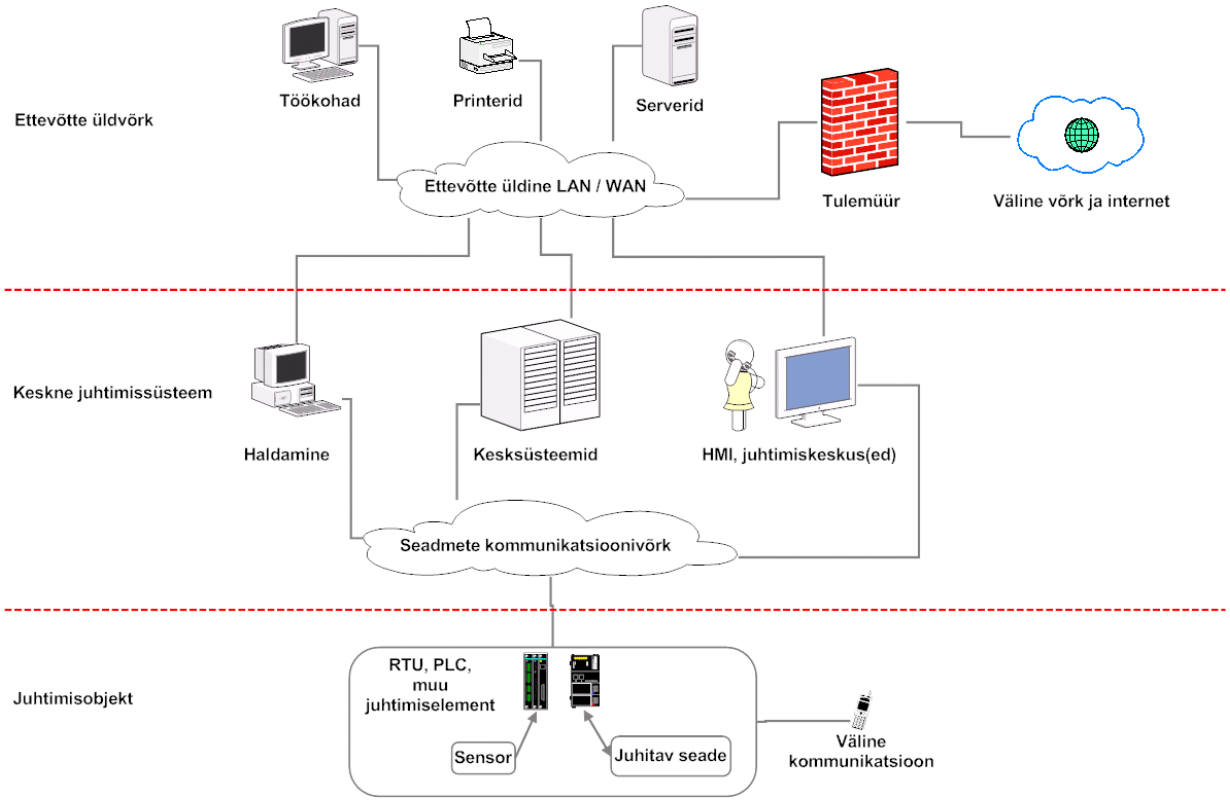
Lähtuvalt Tabel 1 näeme, et:

- Kui tava IT lahendused kestavad 3 kuni 5 aastat (tavaliselt on see nende maksimaalne garantiiperiood) ja on uuendustele kiirelt avatud, siis juhtimissüsteemide eluiga on üle 20 aasta ja üleval tuleb hoida mitut erinevat põlvkonda seadmeid.
- Kui tava IT süsteemid on suunatud andmete turvalisuse käitlemisele, siis juhtimissüsteemides on olulisel kohal protsessi jätkusuutlikus ja inimeste turvalisus.
- Tarkvaraliselt on tava IT töökohad kiiresti uuendatavad ja kiiresti kasutusele võetavad, samas kui juhtimissüsteemide tarkvara on aeglaselt arendatav ja üleval hoitakse vanu süsteeme, millel ei ole lihtsalt võimalik kasutada uuemaid tarkvarasid. Tarkvara uuendamisel tuleb juhtimissüsteemi tunduvalt kauem ja põhjalikult testida isoleeritud testkeskkonnas, enne kui on võimalik seda reaalsesse töösse rakendada.
- Tava IT lahendused on tihedasti omavahel integreeritud ja palju on avatud standarditega tooteid. Paljud erinevad lahendused toimivad üle kõikide platvormide ja versioonide. Juhtimissüsteemides on rohkem tootjakeskne lähenemine ja universaalsust on raske hetkeliste lahendustega saavutada.
- Süsteemide ajakriitilisus on juhtimissüsteemides tunduvalt tähtsamal kohal kui tava IT lahendustes.
- Juhtimissüsteemide peavad toimima praktiliselt igasugustes oludes ja vahetpidamata. Seisakute lubamine tähendab suuri probleeme.

- Juhtimissüsteemidel töötavate inimeste turvateadlikus on väiksem kuna enamasti on nad harjunud olema isoleeritud süsteemides, kus suurem osa turvalisusest on tagatud isoleeritusega.
- Füüsiliselt on juhtimissüsteemid hästi kaitstud, kuid nii mõnegi lahenduse puhul on süsteemid kaugel ja kõrvalistes kohtades, kus reaalne turvalisuse tagamine on komplitseeritud võrreldes tava IT lahendustega, kus kõik on ühes kohas koos või vähemalt on suuremal määral kohese füüsilise kontrolli all.

Süsteemide turvalisusele ja selle standardiseerimisele tuleb mõelda süsteemi loomisest peale. Juhtimissüsteemid, mis baseeruvad pahatihti reaalajalisele tööle ja pikaajaliste tehniliste süsteemide ümberehitamisele ja uute süsteemide sobitamisele vanasse on üldise turvalisuse ja sealt tuleneva IT turvalisuse mõistes problemaatilised. Näiteks vanemad süsteemid, mis on täiesti töökorras ei võimalda kindlasti krüpteeritud andmesidet, pahatihti on raskendatud lihtsamate IT maailmas tavapäraste turvameetmete kohene rakendamine.

Kindlasti on siin võimalik palju ära teha erinevate turvameetmetega nii loogilise kui füüsilise turvalisuse vallas. Erinevate turvameetmete rakendamine ei ole mõeldud üksnes väliste häkkerite vastu võitlemisena, vaid kogu süsteemi usaldusväärse ja töökindlana hoidmisena. Juhtimissüsteemid, mis on oma olemuselt reaalajasüsteemid peavad toimima igasugustes oludes. Väiksemad probleemid võivad viia edasi suurematele probleemidele ja lõppeda katastroofiliselt, mis halvimal juhul tähendab paljude inimeste hukkumist. Kõik süsteemid on pidevas arengus ja erandiks pole juhtimissüsteemid. Süsteemide arenemisega on samas tekkinud uue probleemid ja väljakutsed, mida on endaga kaasa toonud avatud süsteemid, IP teenused, juhtmevaba võrgu kasutamine, universaalsed lahendused, jne. Mida aeg edasi, seda rohkem sagenevad rünnakud juhtimissüsteemidele. DHS järgi tõusid raporteeritud turvalisuse intsidendid kriitilise infrastruktuuri objektidele 200% võrrelduna 2010 vs. 2011 (DHS 2012) . Ettevõtted soovivad avatust, ühest ja universaalset ligipääsu antud süsteemidele. See aga tähendab omakorda suuremaid nõudlusi turvalisusele kogu süsteemi vaatepildis.



Joonis 1. Tüüpiline juhtimissüsteem (autor)

Joonisel 1 on kujutatud tüüpilise juhtimissüsteemi skeem:

- Juhtimisobjektil on sensorid ja juhitavad seadmed, mida kontrollivad ja juhivad erinevad RTU, PLC ja muud juhtimiselemendid. Ühendused võivad erinevad lahendused ja süsteemi sisesed kui ka väliste kommunikatsiooniseadmetega (modemid, mobiilseadmed, jne.)
- Seadmed koonduvad kokku läbi ühise sisemise kommunikatsioonivõrgu.
- Keskuses on tavaliselt koos keskserverid ja toetavad lahendused. Keskselt hallatakse kogu süsteemi süsteemiadministraatorite töökohtadelt. Seadmeid juhivad juhtimiskeskus(t)e töötajad läbi erinevate HMI lahenduste.
- Kaasaegsed kesksed lahendused kasutavad erinevaid võrguteenuseid nt. internet, e-mail, juhtkonna aruandlus, jne.
- Üldisesse võrku on ühendatud ka kõik muud IT vahendid.
- Välistesse võrkudesse ja interneti pääseb tavaliselt läbi ettevõtte ühtse tulemüüri.

3. Ettevõte

3.1 Eesti Raudtee üldinfo

Eesti Raudtee on pika ajalooga ettevõtte. Tähtsamad sündmused oleksid järgnevad (EVR 2011):

- Esimene raudteeliin Eestis avati Tallinna ja Narva vahel 24. oktoobril 1870. See kuupäev tähistab Eesti Raudtee sündi.
- 15. novembril 1918 moodustati Eesti Vabariigi teedeministri käskkirjaga Eesti Vabariigi Raudtee.
- 1940. aastal liideti Eesti Vabariigi Raudtee Nõukogude Liidu raudteevõrku.
- 1991. aastal Eesti Vabariigi iseseisvuse taastamise järel omandas varem sõjaväestatud organisatsioon majandusliku transiidikanali funktsioonid.
- 1992. aasta jaanuaris moodustati riigiettevõte Eesti Raudtee, mis 1997. aasta augustis kujundati ümber aktsiaseltsiks.
- 2000. aasta aprillis kuulutas Eesti Erastamisagentuur välja AS Eesti Raudtee 66 protsendi aktsiate erastamiskonkursi.
- 30. aprillil 2001 sõlmis Eesti Erastamisagentuur konkursi võitnud Baltic Rail Services OÜ-ga erastamislepingu ja 31. augustil 2011 omandas enamusosaluse.
- 9. jaanuaril 2007 ostis Eesti Vabariik tagasi 66 protsenti aktsiaid 2,35 miljardi krooni eest, saades uuesti ettevõtte ainuomanikuks.
- 2008. aasta suvel kolis Eesti Raudtee uude peahoonesse Tallinnas Toompuiestee 35.
- 14. jaanuaril 2009 kanti äriregistrisse AS Eesti Raudtee jagunemine eraldumise teel, mille käigus asutati kaks tütarettevõtet: infrastruktuuri haldamise ja korrashoiuga tegelev AS EVR Infra ning kaubaveondusega tegelev AS EVR Cargo.

Tähtsamad arvnäitajad seisuga 31.12.2010 (EVR 2011):

- Müügitulu - 1 684,6 miljonit krooni (~107,6 miljonit €)
- Puhaskasum - 328,7 miljonit krooni (~21,0 miljonit €)
- Investeeringud - 617,7 miljonit krooni (~39,5 miljonit €)
- Töötajate arv - 1 737
- Keskmine kuupalk - 14 866 krooni (~950 €)
- Veetud kaupu - 13,31 miljonit tonni
- Vedureid - 77
- Kaubavaguneid - 3090

- Raudtee liinide pikkus - 1217 km s.h. elektrifitseeritud 132 km
- Rööpa vahe - 1520/1524 mm
- Jaamasid - 63

3.2. Eesti Raudtee juhtimissüsteemid

Põhilised juhtimissüsteemid EVRis:

- Jaamateede juhtimine - süsteem juhib ja monitoorib konkreetse jaama jaamateid, juhtimine toimub kohaliku jaamakorraldaja või keskuse raudtee dispetšeri poolt;
- Peateede juhtimine - süsteem juhib ja monitoorib pikkade lõikude teid;
- Hotbox - süsteem monitoorib veeremi erinevate osade temperatuuri ja annab teada kui temperatuur on üle mingi lubatud normi;
- Elektrivarustus - süsteem juhib ja monitoorib elektrivõrgustikku;
- Pöörangute soojendus - süsteem soojendab külmal perioodil pööranguid ja monitoorib olukorda;
- Telekommunikatsioon - telekommunikatsioonivõrgu juhtimine ja monitoorimine;
- Raadioside - raadioside võrgu juhtimine ja monitoorimine.

Juhtimissüsteemide haldamisel kasutatakse erinevaid tarkvarasid, mis on välja töötatud väljaspool või oma töötajate poolt.

Eesti Raudtee, kui kriitilise infrastruktuuri omanik, juhindub alati ühe osana oma igapäevatöös turvalisusest ja ohutusest tema valduses oleval infrastruktuuril. Hetkel on kasutusel mitmed erinevad IT süsteemide turvalahendused. Äriinfosüsteemide turvalisuse tagamine toimub peamiselt läbi ISKE juhendite ja meetmete.

Ettevõtte on otsustanud välja töötada ühtsed IT turvastandardi. Käesolev töö on üldise tervikliku turvalahenduse väljatöötamise, kus on koos kõik ettevõtte erinevate valdkondade IT turvalahendused, üks oluline osa. Kõik osad kokkupanduna moodustavad tulevikus ühe tervikliku IT valdkonna sisemise turvastandardi.

4. Üldised nõuded raudteele ja juhtimissüsteemide turvalisusele.

4.1. Eesti Vabariigi raudteealane üldine seadusandlus

Toimimiseks raudteel peab ettevõte järgima paljusid spetsiifilisi seaduseid, eeskirju, norme, jne. Eesti Vabariigis on raudtee järelvalve teostajaks Tehnilise Järelvalve Ameti raudteeteenistus.

Põhilised raudtee ja infrastruktuuri toimimises järgitavad alusdokumentideks oleksid:

- Raudteeseadus (RT 2012, Raudteeseadus) - peamine seadusandlus raudteel opereerimiseks. Rakendusaktidena on antud seadusega kooskõlas seadust täpsustavad ja lahti mõtestavad õigusaktid nt. Raudtee tehnokasutuseeskiri, Raudtee-ettevõtja avalikku reisijateveoteenust osutavaks raudtee-ettevõtjaks määramise kord, Tava- ja kiirraudteesüsteemi koostalitluse tehniliste kirjelduste kohaldamise kord, jne. Olles Euroopa liidu õigusruumis, siis on meil kohustus järgida direktiive nt. "NÕUKOGU DIREKTIIV (91/440/EMÜ) 29. juuli 1991 ühenduse raudteede arendamise kohta", "EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV 2001/16/EÜ, 19. märts 2001, üleeuroopalise tavaraudteevõrgustiku koostalitlusvõime kohta". Antud õigusaktides puuduvad otsesed viited IT info- ja juhtimissüsteemidele ja vajalikud detailsed normid.
- Raudteeseaduse kõrval on veel spetsiifilisemaid seadusi, mida raudtee peab järgima nt. Tehnilise normi ja standardi seadus, Teeseadus, Ehitusseadus, jne.
- Hädaolukorra seadus (RT 2012, Hädaolukorra seadus) - elutähtsa infrastruktuuri toimimise tagamise seadus. Eesti Raudtee, kui avaliku raudtee infrastruktuuri valdaja, on seaduse järgi kriitilise infrastruktuuri omanik, mille toimimise peab ta tagama. Euroopa üldises kontekstis on kriitilise infrastruktuuri valdkonna oluline direktiiv "NÕUKOGU DIREKTIIV 2008/114/EÜ, 8. detsember 2008, Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta". Eestis tegeleb kriitilise informatsiooni infrastruktuuri (RIA 2012. Kriitilise informatsiooni infrastruktuuri kaitse) operatiivtasemel kaitsega RIA allosakond CERT.

4.2. Raudtee spetsiifilised standardid

Raudtee kasutatakse erinevaid valdkonnaspetsiifilisi standardeid. Mõned standardid on üle võetud Eesti Standardikeskuse poolt ja need on eestistatud. Suurem osa standarditest on hetkel veel ingliskeelsed.

Tähtsamate eestindatud standarditena võiks välja tuua järgnevad:

- EVS-EN 50125 sari:
    - 1:2006 Raudteealased rakendused. Keskkonnatingimused seadmetele. Osa 1: Veeremil asetsevad seadmed
    - 2:2003 Raudteealased rakendused. Keskkonnatingimused seadmetele. Osa 2: Paiksed elektripaigaldised
    - 3:2006 Raudteealased rakendused. Keskkonnatingimused seadmetele. Osa 3: Signalisatsiooni- ja telekommunikatsiooniseadmed
- EVS-EN 50126-1:2005 Raudteealased rakendused. Töökindluse, kasutatavuse, hooldatavuse ja ohutuse (TKHO) määratlemine ning esitlemine. Osa 1: Põhinõuded ja üldprotseduur
- EVS-EN 50155:2007 Raudteealased rakendused. Raudteeveeremil kasutatavad elektroonikaseadmed
- EVS-EN 50128:2011 Raudteealased rakendused. Side-, signalisatsiooni- ja andmetöötlussüsteemid. Raudtee juhtimis- ja turvangusüsteemide tarkvara
- EVS-EN 50129:2005 Raudteealased rakendused. Side-, signalisatsiooni- ja andmetöötlussüsteemid. Ohutust tagavad elektroonikasüsteemid signalisatsiooniks
- EVS-EN 50159:2010 Raudteealased rakendused. Side-, signalisatsiooni- ja andmetöötluse süsteemid. Ohutusega seotud teabeedastus ülekandesüsteemides
- EVS-EN 50155:2007/AC:2010 Raudteealased rakendused. Veeremil kasutatavad elektroonikaseadmed

3.3. Juhtimissüsteemide turvastandardid ja parimad praktikad

Erinevate osapoolte poolt on välja töötatud erinevaid standardeid ja parimaid praktikaid, samas mõned neist keskenduvad pigem riist- ja tarkvarale, jättes üldise turvapoliitika tahaplaanile. Kuna turvalisus on rohkem kui ainult riist- ja tarkvara, siis tuleks keskenduda ühtsele ja terviklikule turvapoliitikale.

Tuntumaid standardite loojaid antud valdkonnas on International Society of Automation ja tema allüksus turvalisus standardi loojana ISA99. Tema poolt on loodud järgnevad standardid:

- ISA99 Security Guidelines and User Resources for Industrial Automation and Control Systems, 3rd Edition
- ANSI/ISA-99.00.01-2007 - Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models
- ANSI/ISA-99.02.01-2009 - Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ANSI/ISA-99.02.01-2009 - Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program
- ANSI/ISA-TR99.00.01-2007 - Security Technologies for Industrial Automation and Control Systems

Eraldi võiks välja tuua riigid ja nende ametid, kus suurte infrastruktuuride kaitsmiseks luuakse eraldi standardeid ja soovitusi. Magistritöö loomisel on tutvutud teiste seas järgnevate organisatsiooni materjalidega:

- European Network and Information Security Agency, Euroopa Liit - Euroopa liidu poolt loodud informatsiooni turvalisuse eest vastutav organisatsioon. Kodulehe (ENISA 2012) kaudu saab erinevat informatsiooni. Omab kriitilise infrastruktuuri kaitsmise üksust, mille ülesandeks on aidata kaasa Euroopa Liidu siseselt arendada, välja töötada, mõõta, jne. kriitilise infrastruktuuri turvalisust.
- U.S. Department of Commerce agency National Institute of Standards and Technology, Ameerika Ühendriigid - tehniliste standardite väljatöötaja. On välja töötanud juhendi juhtimissüsteemide turvalisuse vallas (Falco, Stouffer, Scarfone 2011). Antud juhendmaterjali valdkonna üks peamisi materjale, millele viitavad paljud teised valdkonna turvalisusega tegelejad.
- U.S. Department of Homeland Security, Ameerika Ühendriigid - tagab Ameerika Ühendrikkides sisemist turvalisust. Veebilehelt (DHS koduleht 2012) saab informatsiooni kõikide valdkondade kohta;
- DHS osa US-CERT, Ameerika Ühendriigid - ühe tähtsa IT turvalisuse valdkonna osana DHS alluvuses opereerib US-CERT ja hoiab üleval CSSP programmi. Antud programmi veebilehel (US-CERT juhtimissüsteemide koduleht 2012) on võimalik saada hea ülevaade võimalikest juhtimissüsteemide ohtudest ja soovitused ohtude

vähendamiseks ja hoidumiseks. Omab palju erinevaid soovitusi ja parimaid praktikaid infrastruktuuride turvalisuse valdkonnas.

- Australian Government's Critical Infrastructure Resilience, Austraalia - Austraalia kriitilise infrastruktuuri turvalisuse eest vastutav amet. Loodud on ühtne võrgukeskkond (TISN koduleht 2012), kus hoitakse informatsiooni kriitilise infrastruktuuri turvalisuse tagamisest. Kasutajad on riigiasutused ja eraettevõtted.
- Centre for the Protection of National Infrastructure, Suurbritannia - riiklik organisatsioon, mis aitab kaasa Suurbritannia infrastruktuuri turvalisuse tõstmisele. Veebilehe (CPNI koduleht 2012) vahendusel on võimalik ligi pääseda juhtimissüsteemide turvalisuse soovitustele (PA Consulting Group for CPNI 2005-2011).

4.4. EVS-ISO/IEC 27002

Eesti Standardikeskuse poolt üle võetud ISO ja IEC standard IT infoturbe halduse tegevusjuhiste kohta. Rahvusvaheline standard rajab suunised ja üldpõhimõtted infoturbe halduse algatamiseks, evitamiseks, käigushoiuks ja täiustamiseks organisatsioonis. Standardis visandatud eesmärgid annavad üldisi suuniseid infoturbe halduse üldtunnustatud sihtide kohta. Vaadeldakse erinevaid IT valdkondasi ja antakse üldisi juhtnööre. (EVS 2008)

Täpsemate infosüsteemide turvalisuse tagamiseks võib olla vaja rakendada lisameetmeid. Eesti mõistes oleks kasulik kasutada ISKE meetmeid. Kuna tegemist on levinud standardiga, siis omab antud standard ka kokkupuutepunkte nt. COBITi ja ITILiga.

4.5. ISKE

ISKE on kehtestatud Vabariigi Valitsuse määrusega (Riigi Teataja 2009. Infosüsteemide turvameetmete süsteem). Määrus on kohustuslik kõikidele riigiasutustele ja kohalikele omavalitsustele, samas võivad kõik vabatahtlikult rakendada ISKE meetmeid. ISKE baseerub Saksamaal välja töötatud BSI infoturbe standardile.

ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. ISKE rakendusjuhendi esimene versioon valmis 2003. aasta oktoobrikuus. ISKEs on kirjeldatud kolm turbe taset – madal (L), keskmine (M) ja kõrge (H). Vastav turbetase määratakse andmetele turvaklasside (turvaosaklasside) määramise kaudu. Turvaklasside määramisel lähtutakse teabe konfidentsiaalsusest, teabe terviklikkusest,

aegkriitilise teabe käideldavusest, teabe hilinemise tagajärgede lubatavast kaalukusest. ISKE rakendamine asutuses ei ole ühekordne projekt. See on pidev protsess, sest muutuvad nii IT keskkond, turvaohud ja -meetmed kui ka rakendusjuhend. ISKE rakendusjuhend ilmub täiendatud kujul uue versioonina kord aastas, sõltuvalt allikmaterjali uute versioonide avaldamisest. (RIA 2011)

5. Raudtee juhtimissüsteemi IT turvaraamistiku loomine

Raamistiku loomine on esimene samm juhtimissüsteemi turvastandardi väljatöötamisel.

Raamistiku loomisel on põhilisteks märksõnadeks:

- juhtimissüsteemide standard peab tulevikus olema üks osa ettevõtte üldisest turvapoliitikast.
- luua sobilik alusmaterjal tulevase EVR sisese juhtimissüsteemide standardi väljatöötamiseks ja pöörata juba hetkel tähelepanu probleemsetele momentidele, mida on võimalik juba hetkelises staadiumis parandada;
- raamistik peab olema üldine ja minema detailidesse ainult siis, kui meede on kriitilise tähtsusega alusturvalisusele, lihtsalt ja probleemivabalt rakendatav juhtimissüsteemidesse;
- kasutada teadmisi olemasoleva äriinfosüsteemide turvaeeskirjast, mis on loodud ISKE alusel.

Standardite ja parimate praktikate valikute tegemisel on põhilisteks märksõnadeks:

- ei tohi olla keerukas ja komplitseeritud;
- kiirelt ja probleemideta rakendatavad olemasolevatesse süsteemidesse;
- üleüldine kättesaadavus;
- võimalikult vähese rahalise väljaminekuga hankimine, võimalusel tasuta, vabalt saadaval ja vabalt rakendatav ettevõttes.

Lähtuvalt eeltoodust, otsustas autor kasutada järgnevaid materjale:

- ISO/IEC27002 (EVS 2008) - antud standardist on võetud jaotis kuna see katab mõistlikul viisil kõiki IT turbe valdkondasi. Lisaks on standardist võetud aluspõhimõtted, mida autor on oluliseks pidanud üldise raamistiku loomisel juhtimissüsteemide kontekstis;

- DHS soovitused standardite väljatöötajale (DHS 2011) - vaadeldakse konkreetseid täiendavaid soovitusi juhtimissüsteemide IT standardi väljatöötajatele;
- ISKE (RIA 2011) - lisana ISO/IEC27002 materjalidele laiendatakse vajadusel täiendavalt ISKE meetmetega, mis annavad turvalisusele lisaväärtust juhtimissüsteemidele;
- vajadusel ülejäänud olulised seadused, standardid ja parimad praktikad - nt. HOS, Raudteeseadus, raudtee spetsiifilised standardid, CPNI, ENSIA, NIST, jne.

Töö loomise käigus vaadeldi juhtimissüsteemide uuringuid, kus toodi väljas sarnased kriitilise infrastruktuuri turvalisuse probleemid. Eraldi võiks välja tuua Tabel 2 olevad üldised nõrkused. Tabel 2 alamjaotused on tehtud ISO/IEC27002 (EVS 2008) alusel.

Tabel 2. Infoturbe nõrkused (DHS 2011. Common Cybersecurity Vulnerablebilities in ICS; ENISA 2011)

Tähis	**Nõrkuse lühikirjeldus**
	Turvapoliitika:
N1	Infoturbe formaalne puudumine
	Infoturbe korraldus:
N2	Vähe formaalseid eeskirju, juhendeid, jne.
N3	Juhtkonna vähene osalemine
N4	Küberturvalisusega tegeleva meeskonna puudulik komplekteeritus
	Side ja käituse haldus:
N5	Nõrk testkeskkond
N6	Vilets uuenduste haldus
N7	Nõrk varunduse haldus
N8	Puudulik dokumentatsioon
N9	Vaikeparoolide kasutamine
N10	Puudulik võrguseadmete ja tulemüüride konfigureerimine
N11	Erinevate väliste meediate kasutuse kontrolli puudumine
N12	Logimise puudumine või vilets logimine
	Pääsu reguleerimine:

Tähis	Nõrkuse lühikirjeldus
N13	Kaugligipääsu reeglite puudumine
N14	Vale pääsuõiguste kontroll
N15	Ebaturvaliste teenuste kasutamine
N16	Tulemüüride puudumine
N17	Võrkude segmenteerimise puudumine
	Infosüsteemide hankimine, väljatöötamine ja hooldus:
N18	Nõrk uuenduste testimine
N19	Paroolide programmeerimine süsteemi koodi
N20	Informatsiooni lekked testsüsteemidest
	Infoturbeintsidentide haldus:
N21	Intsidentidest mitte teatamine
N22	Teatatud intsidentidest mitte õppimine
	Jätkusuutlikkuse haldus:
N23	Puudulikud õnnetuse järgsed taastamise juhised
N24	Puudulik arusaam õnnetuse järgsete taastamiste tehnoloogiatest
	Vastavus:
N25	Puudulik auditeerimine ja kontroll

Võib eeldada, et tabelis 2 välja toodud nõrkused ei ole ainult Ameerika Ühendriikide ja Euroopa Liidu kriitilise infrastruktuuri probleemid, vaid need puudutavad valdkonda laiemalt. Paljude nõrkused on lihtsasti lahendatavad ja ei nõua eriti rahalisi ressursse. Samas teised nõuavad aega, palju inimtööd ja teadmisi, suuri rahalisi ressursse, jne.

Raamistiku loomisel pööratakse peamiselt tähelepanu jämeda riskianalüüsiga ja uuringus leitud nõrkuste lahendamisele. Raamistiku arenemisel sisemiseks standardiks tegeletakse juba laiemalt antud valdkonna probleemidega.

5.1. Riskide kaalutlemine ja käsitlus

Risk on tõenäoline sündmus, mis võib põhjustada mingit kahju. Riski mõõdetakse tõenäosuse ja mõjuga, mis riski realiseerumisel tekiks. Analüüsi käigus vaadeldakse erinevaid riskimomente ettevõttele.

5.1.1. Valdkonna lühikokkuvõte ja nõuded

HOS (RT 2012, Hädaolukorra seadus):

- HOS1.1 - Kõikidel kriitiliste infrastruktuuri omanikel tuleb läbi viia üldine riskianalüüs.

ISO/IEC27002 (EVS 2008: p 4):

- ISO1.1 - Nõue tuua välja konkreetselt riskid.
- ISO1.2 - Luua pidev riskihalduse süsteem.
- ISO1.3 - Ükski meetmestik ei saa lõplikult välistada riske. Läbi pideva seire, hindamise ja edasiarenduste suudetakse saavutada mõistlik lahendus.

DHS (DHS 2011: p 2.18):

- DHS1.1 - Välja tuleb töötada süsteem riskide halduseks ja hindamiseks.
- DHS1.2 - Juhtimissüsteemide riskihaldus võib olla osa ettevõtte riskihaldusest, kuid erilise vajaduse korral võib olla täiesti eraldi.
- DHS1.3 - Juhtimissüsteemide, kui osa kriitilisest infrastruktuurist, riskihaldus peab olema pideva jälgimise all. Mõistlik oleks tellida sõltumatu väline meeskond, kelle osaks oleks pidev IT turvakontroll, perioodiline etteteatamata sissetungimise testid, valmisoleku kontroll, jne.

5.1.2. Raamistiku olulised meetmed ja tegevused

IT turvaraamistiku loomiseks oluline IT juhtimissüsteemi riskianalüüs viiakse läbi jämeda metoodikaga, kus kasutatakse Hädaolukorra riskianalüüsi juhendi materjale (RT 2011. Hädaolukorra riskianalüüsi koostamise juhend) järgnevaid samme:

- Loetletakse ülesse võimalikud jämedad elulised riskimomendid (Tabel 7);
- Riskile antakse esinemise tõenäosus, mis jaguneb astmeteks T1 kuni T5 (Tabel 3);
- Riskile antakse raskusaste, mis jaguneb astmeteks R1 kuni R5 (Tabel 4);
- Riskile antakse vastavalt riskitabelist raskusaste, kus “riski raskusaste” = “tõenäosus” x “mõju” (Joonis 2);

- Riski raskusastmed jagunevad astmesse 1 kuni 4 (Tabel 5);
- Riskile antakse hinnang olemasolevate kontrolli tõhususest K1 kuni K4 (Tabel 6).

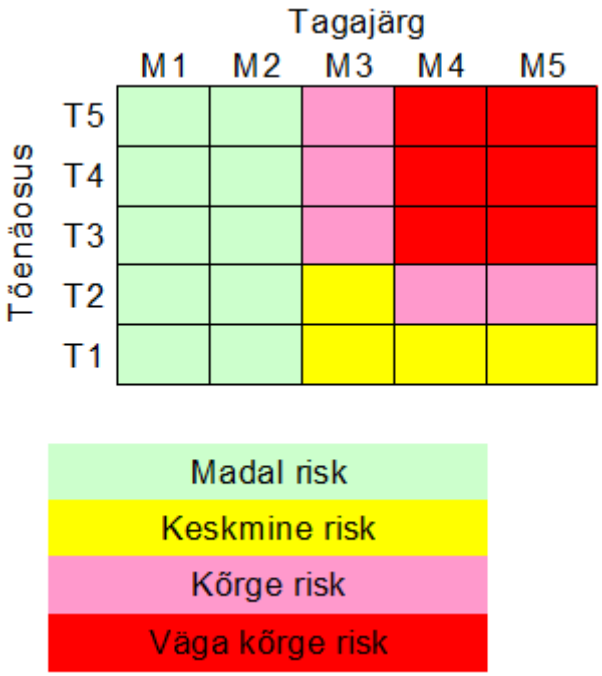
Tabel 3. Riskide tõenäosuse astmed (RT 2011. Hädaolukorra riskianalüüsi koostamise juhend. Lisa 1. Hädaolukordade esinemise tõenäosuse hindamise tabel)

Tõenäosus-aste	Tõenäosus	Tõenäosus 1 aasta jooksul	Selgitus
T1	Väga väike	<0.005% kuni 0.05%	1 võimalus 20 000-st kuni 1 võimalus 2000-st. et hädaolukord leiab aset 5 aasta jooksul
			1 võimalus 100 000-st kuni 1 võimalus 10 000-st. et hädaolukord leiab aset 1 aasta jooksul
T2	Väike	>0.05% kuni 0.5%	1 võimalus 2 000-st kuni 1 võimalus 200-st. et hädaolukord leiab aset 5 aasta jooksul
			1 võimalus 10 000-st kuni 1 võimalus 1000-st. et hädaolukord leiab aset 1 aasta jooksul
T3	Keskmine	>0.5% kuni 5%	1 võimalus 200-st kuni 1 võimalus 20-st. et hädaolukord leiab aset 5 aasta jooksul
			1 võimalus 1000-st kuni 1 võimalus 100-st. et hädaolukord leiab aset 1 aasta jooksul
T4	Suur	>5% kuni 50%	1 võimalus 20-st kuni 1 võimalus 2-st. et hädaolukord leiab aset 5 aasta jooksul
			1 võimalus 100-st kuni 1 võimalus 10-st. et hädaolukord leiab aset 1 aasta jooksul
T5	Väga suur	>50%	suurem kui 1 võimalus 2-st. et hädaolukord leiab aset 5 aasta jooksul
			suurem kui 1 võimalus 10-st. et hädaolukord leiab aset 1 aasta jooksul

Tabel 4. Riskide mõju astmed (autor, RT 2011. Hädaolukorra riskianalüüsi koostamise juhend. Lisa 2. Hädaolukordade tagajärgede hindamise raskusastmed)

Raskus-aste	Tagajärg	Tagajärje valdkond	Tagajärje kirjeldus kriteerium
M1 / A	Vähetähtis (Puudub)	Inimeste elu ja tervis	Üksikud raskelt ning kergelt kannatanud.
		Vara	Varalised kahjud puuduvad või on väga väikesed (0 - 575 204.84 eurot). [RT I. 25.11.2010. 3 - jõust. 01.01.20111

Raskus-aste	Tagajärg	Tagajärje valdkond	Tagajärje kirjeldus kriteerium
		Looduskeskkond	Sündmuskohal ei toimu mõõdetavat muutust ühegi populatsiooni arvukuses või ökosüsteemi talitlemises. See ei välista pärismaiste liikide arvukuses toimuvaid arvukuse looduslikke kõikumisi.
		Elutähtis teenus	Ajutised häired teenuse toimimises. Otsene kahju puudub.
M2 / B	Kerge	Inimeste elu ja teivis	Raskelt kannatanuid, kes vajavad kohest haiglaravi - kuni 30 kannatanut. Kannatanute arv ei ületa piirkondliku tervishoimessursi võimalusi.
		Vara	639 116.49-3 131 670.80 eurot. [RT I. 25.11.2010. 3 - jõust. 01.01.2011]
		Looduskeskkond	Sündmuskohal toimuvad muutused populatsiooni arvukuses või ökosüsteemi talitlemises. Eelnev olukord taastub ilma inimese sekkumiseta.
		Elutähtis teenus	Lühiajalised häired teenuse toimepidevuses.
M3 / C	Raske	Inimeste elu ja teivis	Üksikud hukkunud. Raskelt kannatanuid, kes vajavad kohest haiglaravi 31 - 170 kannatanut. Kannatanute arv ületab piirkondliku tervishoiuressiusi võimalused (va Tallinn), vajalik teiste piirkondade ressursi kaasamine.
		Vara	3 195 582.40 - 1 271 841.80 eurot. [RT I. 25.11.2010. 3 - jõust. 01.01.20111
		Looduskeskkond	Sündmuskohal toimuvad muutused ühe või mitme liigi isendite arvukuses ja ökosüsteemi talitlemises. Eelneva olukorra taastamine ei ole võimalik ilma inimese sekkumiseta.
		Elutähtis teenus	Rohkem kui ühe päevane häire teenuse toimepidevuses. Vajalik tagavara-süsteemide või alternatiivsete meetmete rakendamine.
M4 / D	Väga raske	Inimeste elu ja tervis	Kümned hukkunud. Raskelt kannatanuid, kes vajavad kohest haiglaravi 171-400 kannatanut. Kannatanute arv ületab regiooni tervislioiuressursi võimalused, vajalik kogu riigi tervishoiuressursi kaasamine.
		Vaia	1 278 233.00 - 5 106 540.70 eurot. [RT I. 25.11.2010. 3 - jõust. 01.01.20111
		Looduskeskkond	Sündmuskohal toimub suur muutus ühe või mitme liigi isendite arvukuses. Suure muutuse väärtus sõltub konkreetsest liigist. Kaitse all oleva ühe isendi hukkumine on suur muudatus. Hästi sigiva ning laia levikuga liigi üsna suure arvu isendite hukkumine võib olla vähese tähtsusega, eelkõige juhul, kui muutus mahub populatsiooni arvukuse loodusliku kõikumise piiridesse. Väga raske tagajärg on ka muutus ökosüsteemi talitlemises. sellise muutuse tekkimise eelset olukorda on tavaliselt väga raske taastada.
		Elutähtis teenus	Teenuse ajutine mittetoimimine vähendab oluliselt ühiskonna turvalisust.
M5 / E	Katastroofiline	Inimeste elu ja teivis	Mitmed kümned hukkunud. Üle 400 raskelt kannatanu. Kannatanute arv ületab kogu riigi tervislioiuressursi võimalused, vajalik rahvusvaheline abi.
		Vaia	Vajalik välisabi (kulud üle 0.5% SKP-st. üle 5 112 931.90 euro). [RT I. 25.11.2010. 3 - jõust. 01.01.2011]
		Looduskeskkond	Elukeskkonna hävimine sündmuskohal. Ökosüsteemi talitlemine on lakanud või pöördumatult kahjustatud. Muudatuse eelset olukorda võimatu taastada.
		Elutähtis teenus	Elutähtisa teenuse toimimine on täielikult lakanud.



Joonis 2. Riskimaatriks ja riskide raskusastmed (autor, RT 2011. Hädaolukorra riskianalüüsi koostamise juhend. Lisa 3. Riskimaatriks ja riskide määratlus.)

Tabel 5. Riskide raskusastmete selgitused (andmed Joonis 2. Autor, RT 2011. Hädaolukorra riskianalüüsi koostamise juhend. Lisa 3. Riskimaatriks ja riskide määratlus.)

Tähis	Nimetus	Selgitus
E	Väga kõrge risk	Need hädaolukorrad, mis langevad väga kõrge riskiklassi lahtrisse on esmased või kriitilised ning nendeks tuleb koheselt valmistuma hakata. Neil on küll keskmisest kõrgem tõenäosus, ent nendesse tuleb suhtuda kui kõrge prioriteediga hädaolukordadesse. Sellised hädaolukorrad vajavad mitte ainult ennetamise, vaid ka olulisi valmistumise meetmeid. Kohustuslikud on ametkondade vahelised õppused ja koolitused ning ressursiline planeerimine.
H	Kõrge risk	Need hädaolukorrad, mis langevad antud lahtritesse on käsitletavad kui olulised riskid. Nende tõenäosus on küll mõnevõrra madalam kui väga kõrgetel riskidel, kuid võttes arvesse nende potentsiaalseid tagajärgi, tuleks nendeks vajadusel valmistuda. Soovitav on korraldada ametkondade vahelisi õppusi ning planeerida ressursse hädaolukorra ennetamiseks ja tagajärgede leevendamiseks.
M	Keskmine risk	Väga väikese tõenäosusega hädaolukorrad, milleks on tarvis valmistuda vastavalt võimalustele. Hädaolukordadeks valmistumise ja leevendamise kohapealt kolmas prioriteet.
L	Madal risk	Asutuste igapäevased häired ja õnnetused, millega iga asutus peab hakkama saama ja valmistuma.

Tabel 6. Riskide olemasolev kontrollimehhanism (autor)

Tähis	Nimetus	Kontrollimehhanism
K1	Tugev	● Riskile on pööratud oluline tähelepanu; ● Ette on võetud kõik võimalikud efektiivsed mehhanismid; ● Toimub monitoorimine.
K2	Mõõdukas	● Riskile on pööratud mõõdukas tähelepanu; ● Ette on võetud mõned mehhanismid; ● Toimub mõnetine monitoorimine.
K3	Nõrk	● Riskile ei pöörata piisavat tähelepanu; ● Ette pole võetud mingeid tegevusi; ● Monitooringut ei toimu.
K4	Kontrollimatu	● Riski kontrollimine on väljaspool ettevõtet; ● Ettevõte on võimeline kontrollima tagajärgede likvideerimist.

Tabel 7. Riskide hindamine

Tähis	Selgitus	A*	B	C	D
R1	Toimub ettevõtte vastu suunatud väline häkkerlus, mille tagajärjel kaob oluline informatsioon ja rünnaku alla satub juhtimissüsteem	T2	M2	L	K1
R2	Ettevõtte sülearvuti varastatakse auto esiistmelt ja kaduma lähevad konfidentsiaalseid süsteemiandmeid ja delikaatseid isikuandmed	T2	M1	L	K1
R3	Ettevõtte sisevõrgus ründab oma töötaja koostöös välise partnerfirma töötajaga juhtimissüsteemi, et teha kahju tööandjale	T1	M2	L	K2
R4	Ise hangitud operatsioonisüsteemi vea tõttu seiskuvad mingid arvutid. Peale esimest süsteemi uuendamist tekib juurde veel probleeme. Peale operatsioonisüsteemi tootja poole pöördumist saadakse õiged uuendused	T1	M1	L	K1
R5	Väliselt partnerilt tellitud ja ise edasi arendatud tarkvara vea pärast toimub süsteemi seisak. Puuduliku dokumentatsiooni pärast ei suudeta viga kiirelt avastada	T1	M2	L	K2
R6	Viiruse pärast seiskub osa tööjaamasid ja kuna sisemiselt pole juhtimissüsteemi võrgus segmenteeritud, tekivad ülekoormused juhtimissüsteemis. Viirusest tekitud üldise jõudluse tõusu tagajärjel jooksevad umbe võrguseadmed ja üks võrguseade, mille jahutussüsteem oli katki läheb katki ja nõuab asendust, kuid seadet pole laos	T2	M2	L	K1

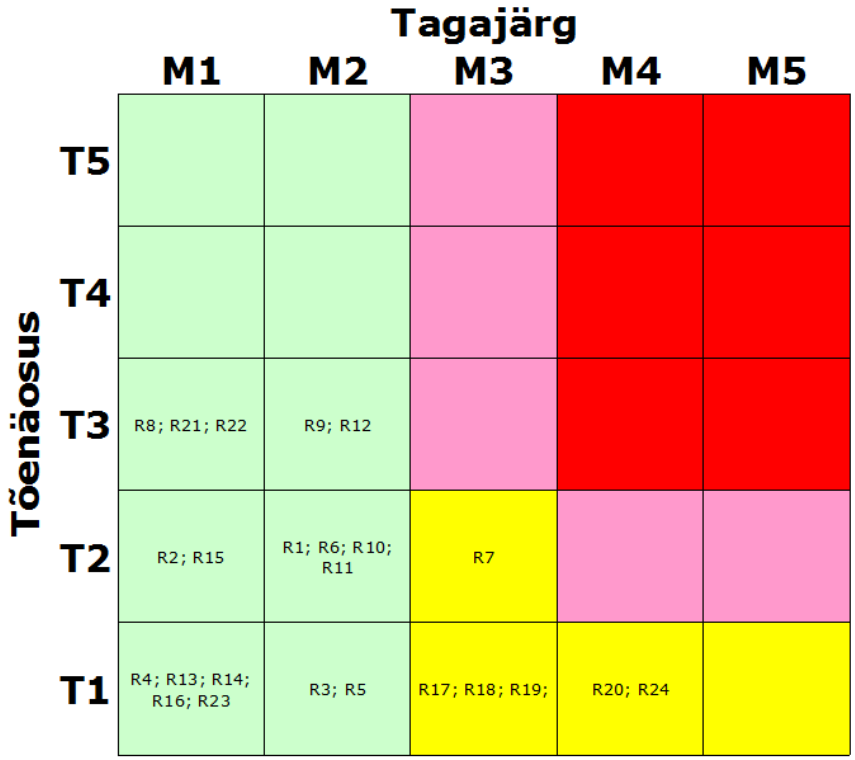
Tähis	Selgitus	A*	B	C	D
R7	Riistvara tõrke pärast seiskub mingi osa juhtimissüsteemist	T2	M3	M	K1
R8	Kasutaja usaldas pahaaimamatult parooli kaastöötajale, kes kasutades ära suuremat ligipääsu kopeeris delikaatseid isikuandmeid ja levitas neid kõigile	T3	M1	L	K2
R9	Tormi ajal lööb välk raadiomasti ja selle tulemusena hävivad kõik kohalikud võrguseadmed, mis olid ühendatud raadiolingiga. Välgu tagajärjel hävivad kõikide võrguprinterite võrgukaardid. Varuseadmed on keskuses ja nende kohale toimetamine on tormi tagajärjel raskendatud.	T3	M2	L	K1
R10	Elektrivoolu kõikumisest tekib ühel vanal hooldamata UPSil ülekoormus, mille tulemusena lähevad töökorrast välja sisemised UPSI elemendid ja ta seiskub. Töötajad ei oska UPSi käsitsi ümber lülitada ja tootja firma esindajaga pole sõlmitud hooldusleping ut ja kõik töötajad on puhkusel	T2	M2	L	K1
R11	Väline firma ühendus läbi VPN võrgu juhtimissüsteemiga ja uuendas süsteemi, kuid viletsa mobiilühenduse pärast katkes VPN ühendus ja vigase kontrollimata koodi tagajärjel kustutati osa sätetest ja andmetest jäädavalt	T2	M2	L	K1
R12	Peale andmete juhuslikku kustutamist üritatakse taastada eelmist süsteemi lindiseadmelt. Lindiseade on vigane ja pole suutnud korralikult ühtegi süsteemi varundada. Administraatorid on saanud teateid varundussüsteemilt, kuid on need kohe kustutanud ja monitooringu süsteemi pole varunduslahendust sisestatud	T3	M2	L	K1
R13	Kulleriks maskeerunud kurjategija lubati iseseisvalt turvatöötaja poolt hoonesse pakki viima, kuid tegelikult varastas isik mitu sülearvutit, milles oli unikaalsed juhtimissüsteemide andmed mida mujal polnud ja ta lahkus hoonest lahti unustatud tagaukse kaudu	T1	M1	L	K1
R14	Digitaalse infovahetuse raames saadetakse programmeerimise vea pärast liialt palju informatsiooni lepingupartnerile, kuid too ei teata probleemist vaid kasutab infot oma huvides	T1	M1	L	K1
R15	Ettevõtte töötaja laeb internetist alla pidevalt piraattarkvara. Töötaja vallandatakse, kuid töötaja kaebab otsuse töövaidluskomisjoni ja sealt nõutakse tõendeid, kuid puuduliku logimise pärast pole mingeid materjale olemas ja töötajale makstakse kompensatsiooni	T2	M1	L	K1
R16	Kohalikku arvutisse sisenetakse ühe kasutajaga ja universaalse parooliga. Ühest arvutist rünnatakse välismaist panka, ettevõte satub uurimise alla, kuid takkajärgi on	T1	M1	L	K1

Tähis	Selgitus	A*	B	C	D
	võimatu kindlaks teha, kes tol hetkel kasutas antud arvutit				
R17	Töötajaid ei ole piisavalt koolitatud uue programmiga ja õiguse süsteem pole veel paigas, kuid oskamatuse ja liiga suurte õiguste ja töötaja poolse katsetuse tagajärjel läheb juhtimissüsteemi osa rikki ja automaatne süsteem tekitab probleeme juhtimises	T1	M3	M	K1
R18	Serveriruumis lõhkeb radiaator mille tulemusena kahjustab vesi osa seadmeid. Seadmed on kindlustatud, kuid nende asendamine võtab aega.	T1	M3	M	K1
R19	Auto sõidab sisse juhtimissüsteemi seadmekapile, mille tulemusena tekivad probleemid lähipiirkonna seadmetes	T1	M3	M	K4
R20	Terrorismi eesmärkidel lõhatakse mingi juhtimiskonteiner seadmestikuga, mille tagajärjel katkeb pikaajaliselt juhtimine antud objektil	T1	M4	M	K4
R21	Kasutaja on teadlik, et arvutis toimub midagi kahtlast, kuid kuna teda ei kuulata kunagi IT inimeste poolt, siis ei räägi ta sellest kellelegi ja mingi aja pärast tekivad teistel probleemid	T3	M1	L	K1
R22	Tulenevalt seadme valest konfigureerimisest, pääsevad isikud, kelle pole luba, mingile infole ligi	T3	M1	L	K1
R23	Valesti seadistatud andmebaasis kustuvad kirjed	T1	M1	L	K1
R24	Seoses pommiähvardusega põhitöökohas mindi hädaolukorras üle varutöökohta, kuid varu IT süsteemid ei hakanud tööle	T1	M4	M	K1

* Veergude pealkirjad:
A - riski tõenäosus (tabel 3)
B - riski mõju (tabel 4)
C - riski raskusaste (tabel 5)
E - riski olemasolev kontrollimehhanism (tabel 6)

Võttes aluseks tabel 7 olevad andmed saame kokkuvõtte, kus jagades riskid erinevate tasemete vahel oleksid tulemused järgnevad:

- Väga kõrge risk - kokku 0
- Kõrge risk - kokku 0
- Keskmine risk - kokku 6
- Madal risk - kokku 18



Joonis 3. Riskide paiknemine riskimaatriksil (andmed Tabel 7.)

Lähtudes andmetest võib öelda, et IT alaseid riske on piisavalt ja nende keskmine aste on madal. Kuna tegemist on suure infrastruktuuri ettevõttega, siis on võimalikud probleemid, mis on põhjustatud välistest teguritest (R19 ja R20), kuid mille tagajärgedega peab ettevõte siiski ise hakkama saama. Nagu nähtub riskimaatriksile paigutatud riskidest (Joonis 3), paiknevad põhilised riskid maatriksis vasakul, mis tähendab riskide tõenäosus on madal ja nende tagajärjed on kergemad. Loetletud riskide osas ei ole ühtegi probleemi, millele juba hetkel tähelepanu ei pöörata.

Riskide hindamisel on näha, et riske on kõikides IT valdkondades. Kindlate ja selgete turvameetmetega on võimalik vähendada olemasolevaid riske.

Raamistiku tegevused riskide halduse valdkonnas oleksid järgnevad:

- MT1.1 - Läbi on viidud ettevõtte üldine riskianalüüs ja HOS tulenev üldine kriitilise infrastruktuuri analüüs. (HOS1.1)[1]
- MT1.2 - HOS tulevast üldisest riskianalüüsist tuleks minna edasi ja koheselt läbi viia ka detailne IT juhtimissüsteemide detailne riskianalüüs. (ISO1.1)

[1]Nüüd ja edaspidi: meetme/tegevuse (MT) taga sulgudes määratletakse viide eelnevale alajaotuse nõuetele, soovitustele ja parematele praktikatele, nõrkusele (Tabel 2) ja riskidele (Tabel 7).

- MT1.3 - Luua ettevõtte sisene riskide haldamise süsteem, mehitada see vastavate töötajatega ja tegeleda antud valdkonnaga pidevalt. (ISO1.2, ISO1.3, DHS1.1, DHS1.2)
- MT1.4 - Kaaluda lepingu sõlmimist sõltumatu meeskonnaga, kelle ülesandeks oleks auditite vahelisel perioodil testida süsteemi turvataset. (DHS1.3)

5.2. Turvapoliitika

Info turvapoliitika on eeskirjade, juhiste ja menetluste üldkogu, mis suunavad erinevate varade haldust, kaitset ja jaotamist organisatsiooni IT erinevates süsteemides. Turvapoliitika on juhtkonna poolne suunamine ja tugi vastavalt tegevusalastele nõuetele ning asjassepuutuvate õigusaktidele ja eeskirjadele. (EVS 2008: p.5)

5.2.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p. 5):

- ISO2.1 - Juhtkonnal tuleb anda suunamine ja tugi vastavalt tegevusalastele nõuetele ning asjassepuutuvatele õigusaktidele ja eeskirjadele. Juhtkond on turbepoliitika eesvedaja ja suunaja.
- ISO2.2 - Kõik dokumendid tuleb kinnitada juhtkonna poolt.
- ISO2.3 - Olulisematest osadest tuleb dokumendis tuleb ära määratleda: infoturbe määratlus, juhtkonna olulisus antud protsessis, raamstruktuur, vastavus teiste dokumentidega, nõuded koolitusele, jätkusuutlikuse haldus, infoturbepoliitika rikkumise tagajärjed.
- ISO2.4 - Infoturbepoliitika ei pea olema eraldiseisev dokument, vaid võib olla ettevõtte suurema ja üldisema poliitikadokumendi osa.
- ISO2.5 - Materjale tuleb pidevalt üle vaadata ja vajadusel kaasajastada.

DHS (DHS 2011: p. 2.1):

- DHS2.1 - Juhtimissüsteemid turvapoliitikad tuleks hoida ühe osana üldiste poliitikatega ja vajadusel korral lisada juhtimissüsteemide spetsiifilisi käsitlusi lisana.

5.2.2. Raamistiku olulised meetmed ja tegevused

- MT2.1 - Juhtimissüsteemide IT turvalisus tuleb võtta üldisesse jälgimisse. Juhatuse otsusega luua algne projektimeeskond ja anda konkreetsed suunised rollide jaotusest. (ISO2.1, ISO2.2,)
- MT2.2 - Välja tuleb töötada juhtimissüsteemide IT turvapoliitika punktid, mis täiendavad ettevõtte üldisi turvapoliitikaid. Kõik juhtimissüsteemide spetsiifilised punktid tuleb koondada ühtsesse alampunktidesse. (N1, ISO2.4, DHS2.1)
- MT2.2 - Algsest projektimeeskonnast peab välja kasvama EVR juhtimissüsteemide toimiv tuumik, kelle eestvedamisel arendatakse kogu valdkonna turvalisust. (ISO2.5)
- MT2.3 - Kõik materjalid tuleb alati kinnitada EVR juhatuse poolt. (ISO2.2)

5.3. Infoturbe korraldus

Infoturbe korraldus kujutab endast infoturbe valdkonna konkreetset korraldust s.h. juhtkonna poolset pidevat toetus, konkreetsete rollide määratlemist, suhtlemist erinevate osapooltega, sõltumatut auditeerimist, jne. (EVS 2008: p 6)

5.3.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 6):

- ISO3.1 - Juhtkond peaks selge suunamise, ilmutatava kohustumuse ning selgekujulise infoturbe kohustuste määramise ja tunnustamisega aktiivselt toetama turvalisust organisatsioonis.
- ISO3.2 - Juhtkonna põhilised ülesanded oleksid veel infoturbe selge piiritlemine, jälgima rakendamist, pidev toetus, ressursid, määrama töötajate rollid, tagama rakenduse kogu ettevõttes.
- ISO3.3 - Infotöötlusvahendite volitamise protsess.
- ISO3.4 - Luua kõigi väliste osapooltega konfidentsiaalsuslepped.
- ISO3.5 - Kontaktid ametivõimudega ja välise huvigruppidega.
- ISO3.6 - Infoturbe sõltumatu auditeerimine.
- ISO3.7 - Väljast tellitud teenuste haldamine ja väliste teenuste kasutamisriskide väljaselgitamine.

DHS (DHS 2011: p 2.2):

- DHS3.1 - Väljast tellitud teenuste lõpetamisel tuleb katkestada kõik ligipääsud süsteemidele. Eriti oluline on siin ligipääsud erinevatele tehnorajatiste juhtimissüsteemidele, mis ei pruugi olla ühendatud ühtsesse jälgimisse.
- DHS3.2 - Kuna juhtimissüsteemid kuuluvad kriitilise infrastruktuuri ühte ossa, siis tuleks luua kontaktid kohaliku CERT keskusega ja vajadusel kasutada nende abi.

5.3.2. Raamistiku olulised meetmed ja tegevused

- MT3.1 - Luua konkreetsed juhendid, eeskirjad, jne IT turvalisuse vallas tegutsemiseks ja teha need kõigile osapooltele kättesaadavaks. (N2, ISO3.1, ISO3.2)
- MT3.2 - Luua ettevõtte ülene turvanõukogu, kus oleksid esindatud nii juhatuse, tippjuhtkonna ja turbe eest vastutajad. Eesmärk oleks regulaarsel infovahetusel juhtidega olukorrast ettevõtte IT turbe vallas ja kaasata juhtkonna inimesi, et teadvustada antud valdkonna tähtsust ettevõtte töösse. (N3, ISO3.2)
- MT3.3 - Laiendada olemasoleva turvalisusega tegelevate inimeste töövaldkonda juhtimissüsteemidele ja vajadusel palgata juurde lisaks meeskonna liikmeid. (N4, ISO3.2)
- MT3.4 - Juhatus peab volitama inimesed, kes tegelevad infotöötlusvahendite reaalsesse töösse andmisega. (ISO3.3)
- MT3.5 - Korraldada esialgne üldine IT turvaaudit kõikidele süsteemidele. Viia sisse regulaarne IT auditite ja IT turvaaudit ajakava.(ISO3.6)
- MT3.6 - Koondada väljast tellitud teenused ühtsete üldiste nõuete alla ja vastavalt konkreetse valdkonna vajadustele lisada lisapunkte. Vaadelda konkreetseid riske iga teenuse kohta eraldi ja koos kõigi teiste teenustega. Väliste teenuste osutajad peavad aru saama oma osast ettevõtte sisemise IT turvalisuse kontekstis ja järgima kõike sisemisi reegleid ja vastutama oma tegevuse/tegevusetuse eest. Teenuste lepingu osana tuleb allkirjastada konfidentsiaalsuslepe. Väljast tellitud teenuse lõppemisel tuleb koheselt sulgeda kõik ligipääsud ja süsteemidele. Tagasi tuleb saada kõik varad, mis on usaldatud nende kätte. Välja tuleb töötada süsteem, kus oleksid kirjeldatud kõik jooksvad varad, kasutajaõigused, füüsilised pääsud, jne. mis tuleb tagastada või sulgeda enne teenuse lõpetamist. Vajadusel tuleb teenuse lõppedes vaadata üle olemasolev konfidentsiaalsusleping ja vajadusel seda uuendada. (R2, R11, R14, ISO3.4, ISO3.7, DHS3.1)

- MT3.7 - Luua kontakt erinevate turvavaldkonna organisatsioonidega. Kindlasti kaaluda mingi üldise koostöölepingu sõlmimist RIA infoturbeintsidentide käsitlemise osakonnaga, mis tegeleb CERT Eesti meeskonnana. (DHS3.2)

5.4. Varade haldus

Varade halduse eesmärgiks on kaitsta ettevõtte erinevaid varasid. (EVS 2008: p 6)

5.4.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 7):

- ISO4.1 - Saavutada varade asjakohane kaitse ja säilivus.
- ISO4.2 - Luua varade liigitus, märgistus ja inventeerida tähtsamad varad.
- ISO4.3 - Varad võivad olla erinevat liiki nt. andmebaasid, lepingud, arvutid, serverid, operatsioonisüsteemid, jne.
- ISO4.4 - Varadel peab olema omanik.
- ISO4.5 - Luua varade kasutamise reeglid.
- ISO4.6 - Anda varale turvaliigitus ja tagada sellel vastav kaitse.

ISKE (RIA :M2.226, M1.33, M2.309):

- ISKE4.1 - Ettevõtte väliste teenuste kasutamisel tuleb erilist hoolt kanda väliste isikute viibimisel turvapiirkondades, lepingu lõppemisel tagada ajutisse kasutusseusaldatud vara tagastamine.
- ISKE4.2 - Nõuded kaasas kantavatele seadmetele kui neid viiakse väljapoole ettevõtte territooriumit, eraldi välja tuua info kasutajatele.
- ISKE4.3 - Mobiilsete seadmete kasutuse poliitika ja eeskirjad s.h. andmete kaasas kandmine, õige seadme kasutamine, ligipääsemine erinevatele ressurssidele.

DHS (DHS 2011: p 2.4.16, p 2.4.18):

- DHS4.1 - Juhtimissüsteemides tuleks piirata väliseid andmekandjaid.
- DHS4.2 - Ettevõte peab keelama kasutada isiklikke andmekandjaid.
- DHS4.3 - Kui andmekandjal puudub selgelt identifitseeritav omanik, siis ei tohi seda kasutada juhtimissüsteemides.

- DHS4.4 - Eriline tähelepanu tuleb pöörata pääsupunktidele ja rakendada kõiki meetmeid, et kaitsta pääsupunkti taga olevat vara või identifitseerida, et pääsupunkti taga olev vara on kaitstud.

NIST (Falco, Stouffer, Scarfone 2011: p 6.2.2.2)

- NIST4.1 - Mobiilsed töövahendid, mis on mõeldud juhtimissüsteemide konfigureerimiseks (nt. PLC programmeerimiseks), ei tohiks lubada lahkuda turvaliselt tsoonist. Kõik antud seadmed peavad omama eriliselt tugevaid kaitsemehhanisme ja neid ei tohiks mingil juhul kasutada väljaspool juhtimissüsteemi võrku.

5.4.2. Raamistiku olulised meetmed ja tegevused

- MT4.1 - Luua korrektne juhtimissüsteemide IT varade nimekiri nii ettevõtte, kui objektipõhiselt. Rakendada ühtne ja ühene varade identifitseerimine, mis oleks kõigile arusaadav, kogu ettevõtte ulatuses. Objektipõhine seadmete detailsuse aste valida vastavalt vajadusele. (R6, ISO4.1, ISO4.2,)
- MT4.2 - Luua varuseadmete haldus ja paigutada varuseadmed õigetele kohtadele, mis tagaks varuseadme vahetuse olemasolu mõistliku aja jooksul kriitilistes sõlmpunktides. (R6, ISO4.1)
- MT4.3 - Igale varale määratletakse konkreetne omanik. Infosüsteemide erinevatele moodulitel võib olla erinevad omanikud. (ISO4.3, ISO4.4)
- MT4.4 - Luua konkreetsed kasutusreeglid juhtimissüsteemide IT süsteemidele. Materjal teha teatavaks allkirja vastu kõigile töötajatele. (ISO4.5)
- MT4.5 - Luua kaasas kantavate seadmete turvalise kasutamise reeglistik. Eraldi tähelepanu pöörata juhtimissüsteemi oluliste seadmete konfigureerimise seadmestiku kaasa kandmist ja ettevõtte territooriumilt välja viimist. (R2, ISKE4.2, ISKE4.3)
- MT4.6 - Luua kitsamad reeglid juhtimissüsteemide väliste andmekandjate kasutusele antud süsteemidel. Keelata tuleb kõikide tundmatute ja isiklike andmekandjate kasutamine juhtimissüsteemides. Lubatud peab olema ainult konkreetselt testitud tootjate seadmed. (N11, R2, DHS4.1, DHS4.2, DHS4.3)
- MT4.7 - Rakendada vajadusel nii kinniseid kui läbipaistvaid turvalisi uksi ja aknaid, et näha vara olukorda. Vajadusel tuleb kasutada videojälgimise lahendusi. (DHS4.4)
- MT4.8 - Väljapoole ettevõtet usaldatud varad nt. testseadmed, mobiilne aparatuur, jne. tuleb üle anda ainult aktidega ja lepingutega. (ISKE4.1)

- MT4.9 - Tuleks kaaluda eraldi mobiilseadmete hankimist juhtimissüsteemidele, mida ei kasutata kusagil mujal, kui ainult juhtimissüsteemide konfigureerimisel ja võrkudes. (NIST4.1)

5.5. Inimressursiturve

Inimressursiturve peamiseks eesmärgiks oleks hallata töösuhet enne, ajal ja pärast töölepingu sõlmimist. (EVS 2008: p 8)

5.5.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002(EVS 2008: p 8):

- ISO5.1 - Töötajad, alltöövõtjad ja kolmandad osapooled tunnevad oma kohustusi ja sobivad rollidesse, mis neile on antud;
- ISO5.2 - Personaliturve algab enne töötaja tööle võtmist ja lõpeb töötaja lahkumisega;
- ISO5.3 - Tuleb luua konkreetsed tööjuhised ja tutvustada turvalise käitumise eeskirju. Allkirjaga kinnitada turvaeeskirjaga tutvumist. Kohustust ja motiveeritud jälgida antud materjali.
- ISO5.4 - Koostöös personalitöötajaga peab välja töötama töölepingu osad turvaliseks käitumiseks töökohal ja pideva turvakoolituse protsess;
- ISO5.5 - Tööle võetava töötaja taustkontroll. Vajadusel korral tuleb kontrolli teostada kolmandate osapoolte välistele töötajatele.
- ISO5.6 - Kasutada kõiki vahendeid, et tõsta töötajate infoturbeteadlikust.
- ISO5.7 - Tuleb luua distsiplinaarprotsess turvalisust eiranud töötaja korralekutsumiseks.
- ISO5.8 - Välja töötada protsess, et töötaja lahkumisel oleks tagastatud kõik tema kasutuses olnud varad. Töötaja lahkumisel korral tuleb korrektselt ära võtta või sulgeda kõik ligipääsud nt. kasutajatunnused, võtmed, uksekaardid.

DHS (DHS 2011: p 2.3, 2.11):

- DHS5.1 - Töölepingu lõpetamisel soovitatakse läbi viia intervjuu milles tehakse selgeks töötajale tema õigused ja kohustused kui endise juhtimissüsteemi töötajana.
- DHS5.2 - Perioodiliselt tuleb läbi viia juhtimissüsteemide turvateadlikkuse tõstmise koolitust. Koolituse ajal tuleb üle vaadata vahepealsed dokumentide uuendused.
- DHS5.3 - Turvakoolitused tuleb planeerida vastavalt ametikohtade rollidele ja kohustustele.

- DHS5.4 - Perioodiliselt tuleb läbi viia praktilisi treeninguid, kus simuleeritakse reaalset turvaprobleemi ja vaadeldakse lahendusi.
- DHS5.5 - Koolituste ja treeningute kava ja selle täitmine tuleb pidevalt jälgida. Vajadusel tuleb teha sellesse korrektuure.

NIST (Falco, Stouffer, Scarfone 2011: p 6.2.1):

- NIST5.1 - Ametikoha loomisega tuleb määrata selle riskiaste ja nõuded. Juurdepääs süsteemile tuleb tagada alles pärast kõikide nõuete täitmist. Nõudeid tuleb pidevalt üle vaadata ja vajadusel uuendada.

5.5.2. Raamistiku olulised meetmed ja tegevused

- MT5.1 - Töötajad võetakse tööle läbi erinevate meetodite. Enne reaalsesse töökohta asumist kontrollitakse töötaja teadlikust ja sobilikust vastava ametikohaga. Olenevalt töökoha iseloomust, tuleb teha taustkontroll. (ISO5.1, ISO5.5, NIST5.1)
- MT5.2 - Kõikide materjalidega tutvumise kohta tuleb võtta allkiri. Kõik töötajad peavad vabalt ligi pääsema avalikele IT alastele juhistele ja materjalidele. Töötaja peab aru saama IT turvalisusest ja oma rollist selle tagamisel. Materjalide uuenemisel tuleb töötajatele sellest teada anda ja kontrollida nendega tutvumist. (ISO5.3, R2, R3, R8, R13, R15, R16, R17, R21)
- MT5.3 - Töötajaid peab erinevatel tasemetel pidevalt koolitama IT turvalisuse vallas. Vajadusel võib üldist turvamaterjali levitada läbi intraneti, siselehe, jne. (ISO5.6, R2, R3, R8, R13, R15, R16, R17, R21, DHS5.2, DHS5.3)
- MT5.4 - Koostöös erinevate osakondade ja teiste valdkonna oluliste asutustega tuleb läbi viia perioodilisi praktilisi treeninguid, mis aitavad kaasa reaalses olukorras toime tulemisel. Treeningute tulemused tuleb dokumenteerida ja luua ülevaade positiivsetest ja negatiivsetest tulemustest ja vajadusel võtta kasutusele meetmeid, et toimida kriisi situatsioonis paremini. (DHS5.4)
- MT5.5 - Turvakoolituste ja treeningute ajakava tuleb eelnevalt kooskõlastada mingi pikema perioodi ulatuses. Perioodi jooksul tuleb jälgida ajakava ja vastavalt reaalsele olukorrale korrigeerida. (DHS5.5)
- MT5.6 - Töösisekorra eeskirjadesse tuleb, kooskõlas kõikide seadustega, sisestada distsiplinaarkaristuse protsess. Töötaja peab olema teadlik oma kohustustest ja nende rikkumise tagajärgedest. (ISO5.7, R2, R3, R8, R13, R15, R16, R17, R21)

- MT5.7 - Töötaja ei pääse reaalsetele juhtimissüsteemidele ligi enne, kui on süsteemi selgeks õppinud testkeskkonnas ja saanud heakskiidu reaalsesse keskkonda tööle lubamiseks. (NIST5.1)
- MT5.8 - Välja tuleb töötada süsteem, kuhu oleks koondatud kõikide töötajate varad, kasutajaõigused, füüsilise pääsud, jne., mis tuleb tagastada või sulgeda enne töölepingu lõpetamist. Töölepingu lõppemisel tuleb töötajaga läbi viia vestlus, temale teada olevast informatsioonist. Vajadusel tuleb välja töötada konfidentsiaalsus leping ja kompensatsioonimehhanismid probleemide ennetamiseks. (ISO5.8, DHS5.1)

5.6. Füüsiline ja keskkonna turve

Füüsilise ja keskkonna turve peamine eesmärk on tagada üldine turvaline töökeskkond ja kaitsta seda erinevate ohtude eest. (EVR 2008: p 9)

5.6.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 9):

- ISO6.1 - Vältida lubamatut füüsilist juurdepääsu organisatsiooni territooriumile ja teabele, nende kahjustamist või häirimist.
- ISO6.2 - Tuleb luua selge turvaperimeeter ja kaitsta seda vajalike mehhanismidega.
- ISO6.3 - Luua konkreetsed sissepääsupunktid ja varustada need sobilike sissepääsu reguleerivate meetmetega.
- ISO6.4 - Kui on vajalik luua eriti turvalisi alasid, siis tuleb need vastavalt tähistada ja personalile teada anda nendes piirkondades kehtivatest erireeglitest.
- ISO6.5 - Seadmeid tuleb paigutada lähtuvalt riskidest ja volitamata ligipääs tuleb teha võimalikult keeruliseks.
- ISO6.6 - Jälgida tuleb tule- ja elektriohutust, oluline on maandus ja vajadusel tuleb tööstuskeskkondades kasutada erivahendeid.
- ISO6.7 - Välja tuleb töötada UPSide kasutamine ja elektrivarustuse kaitse.
- ISO6.8 - Kaabeldusi tuleb kaitsta väliste kahjustuste ja andmepüügi eest.
- ISO6.9 - Seadmete terviklikkuse ja käideldavuse tagamiseks tuleb neid hooldada.
- ISO6.10 - Kasutades seadmeid väljaspool ettevõtte territooriumit tuleb nendele erilist tähelepanu pöörata.
- ISO6.11 - Seadmeid tuleb turvaliselt kõrvaldada ja vajadusel taaskasutada

ISKE (RIA 2011: B 2.4)

- ISKE6.1 - Serveri- ja seadmeruumid tuleks eraldi projekteerida ja ehitada.

DHS (DHS 2011: p 2.4):

- DHS6.1 - Juhtimissüsteemidele ligipääs tuleb luua läbi kaheastmelise kontrolli.
- DHS6.2 - Iga juhtimissüsteemi ligipääsu pääsupunkt peab olema valve ja jälgimise all 24 tundi ja 7 päeva nädalas. Ettevõtte peab jälgima reaalaajaliselt kõiki pääsusündmusi ja iga võimaliku sissetungi kohta peab koheselt alustama vastutegevust.
- DHS6.3 - Ettevõtte töötaja peab saatma igal ajal väliseid külalisi ja välise teenuse pakkujaid.
- DHS6.4 - Ligipääsuks juhtimissüsteemidele peab olema väline inimene kaheastmeliselt tuvastatav.
- DHS6.5 - Perioodiliselt peab üle vaatama külaliste logi.
- DHS6.6 - Välja tuleb töötada tegevused üleujutuste ohtlikes piirkondades.
- DHS6.7 - Välja tuleb töötada süsteemide avarii väljalülitamised ja meetmed, et süsteemi ei kasutata pahatahtlikult/kogemata väljalülitamiseks.
- DHS6.8 - Välja tuleb töötada alternatiiv elektrivarustuse kaitse, et oleks tagatud pikema perioodi minimaalne elektrivarustus, kui põhi elektritarne kaabel ei tööta.
- DHS6.9 - Sisemist elektrivarustust (s.t. akudega) omavad süsteeme tuleb korrapäraselt hooldada, et oleks pidevalt tagatud nende töökindlus.
- DHS6.10 - Juhtimissüsteemidel peab olema alternatiivne töökoht. Antud kohta peab regulaarselt kontrollima, et oleks tagatud tema töökord põhitöökoha avariiolukorras.

NIST (Falco, Stouffer, Scarfone 2011: p 6.2.2.3):

- NIST6.1 - Eelistada tuleb fiiberoptilist kaabeldust, kuna see on vähem tundlikum keskkonnamõjudele ja rasekesti pealtkuulatav.

5.6.2. Raamistiku olulised meetmed ja tegevused

- MT6.1 - Koostöös EVR turvaosakonnaga kaardistada kõikide juhtimissüsteemide ligipääsupunktid ja võimaluse korral lülitada need kõik elektroonilise juhtimise alla. Vajadusel tuleb kasutada mitmeid erinevaid füüsilise turvalisuse meetmeid, et kaitsta perimeetrit. Luua konkreetne turvaperimeeter, märgistada see konkreetselt ja luua antud alal töötamise juhised. Eriline tähelepanu tuleks pöörata võtmete haldusele ja seda just

lõpetatud töölepinguid ja teenuseid silmas pidades. Mehitatud valve korral ja pidevalt väliseid külaliste käidavates kohtades tuleb välja töötada külastuse reeglid. (R13, ISO6.1, ISO6.2, ISO6.3, ISO6.4, DHS6.1, DHS6.2, DHS6.3)

- MT6.2 - Kõik juhtimisseadmed tuleb paigutada võimalikult turvaliselt, samas võimalikult mugavalt ligipääsetavasse kohta.(ISO6.5)
- MT6.3 - Väliste töötajate ja partnerite ligipääs juhtimissüsteemidele tuleks eraldi reglementeerida, täpselt kirja panna ja pidevalt täitmist kontrollida. (DHS6.2, DHS6.3, DHS6.4, DHS6.5)
- MT6.4 - Välja tuleb töötada hädaolukorra plaanid välgu ja tormi sagedastes piirkondades. (R9, ISO6.5, ISO6.7)
- MT6.5 - Üleujutuse ohtlikel aladel tuleb sellega projekteerimisel arvestada ja paigaldada õiged seadmed. Samas tuleb vajadusel välja töötada käitumisjuhendid hädaolukorras ja neid testida ja selgeks teha kõigile antud ala töötajatele. (DHS6.6, DHS6.7)
- MT6.6 - Juhtimissüsteemide objektidel tuleb konkreetselt tähistada tuleohutuse eest vastutajad ja kontaktisikud. regulaarselt tuleb teha ülevaatusi, et tuleoht oleks kontrolli all. Elektrivarustusega peavad tegelema ainult koolitatud ja sertifitseeritud töötajad. Koostöös päästeametiga tuleb läbi vaadata erinevad ohustsenaariumid konkreetsetel objektidel ja vajadusel teha korrektuurid olemasolevas keskkonnas. (ISO6.6)
- MT6.7 - Kriitiliste juhtimisseadmete stabiilse elektrivarustuse tagamiseks tuleb kasutada erinevaid meetmeid nt. mitu erinevatest alajaamadest tulevad sidendfiidrit, UPS, diiselgeneraator. UPSe tuleb pidevalt jälgida ja vastavalt tootja poolt soovitatud intervalli järel hooldada. (ISO6.7, ISO6.9, DHS6.7, DHS6.8, DHS6.9)
- MT6.7 - Pikkadel vahemaadel tuleb eelistada fiiberoptilise kaabli kasutamist, kuna selle pealtkuulamine on raske. Muud kaabelduse lahendused tuleb välja töötada vastavalt vajadusele, silmas pidades ligipääsetavust, ründaja ligipääsetavust, häireid, jne. (ISO6.8, NIST6.1)
- MT6.8 - Luua tuleb alternatiivne juhtimissüsteemi keskus ja töökohad, kus saab süsteemi juhtida avarii korral. Välja tuleb ehitada ja hankida kõik vajalikud seadmed. Varu juhtimissüsteemi tuleb korrapäraselt testida ja hooldada. Koolitada tuleb ka kasutajaid. (DHS6.10)
- MT6.9 - Juhtimissüsteemide serveri- ja seadmeruumid tuleb eraldi projekteerida ja ehitada. ISKE meetmestikust tuleb järgida L ja M taseme meetmeid, vajadusel rakendada H taseme meetmeid. Antud aladel peab kehtima eraldi reeglistikud, mida peavad kõik järgima. (R18, ISO6.5, ISKE6.1)

- MT6.10 - Juhtimissüsteemide avalikkusele ligipääsetavaid seadmeruume, konteinereid, jne. tuleb erilise tähelepanuga projekteerida ja ehitada. Ette tuleb näha suurem väliste ohtude kogum ja olla valmis võimalike tagajärgedega tegelema. (R19, R20, ISO6.1, ISKE6.1, DHS6.10)

5.7. Side ja käituse haldus

Side ja käituse haldus sisaldab endas erinevaid turvameetmeid s.h. konkreetse käitusprotseduurid ja -kohustused, kolmanda poole teenuste haldus, süsteemide planeerimine ja vastuvõtmine, kaitse erinevate kahjurkoodide eest, varundamishaldus, võrguturvalisust, infokandjate käitlus, infovahetust, seiret. (EVS 2008: p 10)

5.7.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 10):

- ISO7.1 - Käitusprotseduurid tuleks dokumenteerida ja teha kättesaadavaks, kes seda vajavad s.h. tuleks spetsifitseerima üksikasjalikud juhendid: varundamiseks, tehnilise toe kontaktandmed, süsteemi taaskäivituse ja taasteprotseduurid süsteemi tõrke puhuks;
- ISO7.2 - Infotöötlusvahendid ja -süsteemide muudatusi tuleks hallata s.h. tuleks luua muudatuste planeerimine ja testimine, muudatuste tegemise teavitus kõigile asjassepuutuvatele isikutele, edutu uuenduse tagasipööramine;
- ISO7.3 - Arendus-, testimis- ja töövahendid tuleb üksteisest eraldada, s.h. tuleb määratleda järgmised tegevused tarkvara üleviimine erinevate tasemete vahel, testimissüsteemi olemus ja haldus;
- ISO7.4 - Kolmandate poolte teenused ja nende haldus e. plaanimine, testimine, elluviimine, vastuvõtmine;
- ISO7.5 - Kahjurkoodi tõrjumine erinevate meetoditega s.h. antiviirused, elutähtsate teenuste kaitse;
- ISO7.6 - Võrguühenduse turve erinevate meetmetega s.h. seadmete võrku ühendamine, tulemüürid, reaalajaline monitoorimine;
- ISO7.7 - Infokandjate käitlemine, et vältida varade lubamatut avalikustamist, muutmist, kõrvaldamist ja hävitamist ning töötegevuse katkemist. Ird-infokandjaid (nt. mälupulgad, lindid, CD, välja trükitud materjalid) tuleb hoiustada turvalises keskkonnas, kriitilistest andmetest tuleb teha mitu erinevat koopiat, kõrvaldamine peab toimuma turvaliselt;

- ISO7.8 - Teabe kaitsmiseks lubamatu paljastamise või väärkasutamise eest tuleb kehtestada teabe käitluse ja talletuse protseduurid s.h. luua konkreetne õiguste süsteem ligipääsuks ja pidada registrit antud õiguste osas ja korrapäraselt kontrollida õiguste vajalikust;
- ISO7.9 - Andmeid tuleb levitada nii vähestele kui vajalik,
- ISO7.10 - Süsteemide dokumentatsioon tuleb hoiustada turvalisel, samas kergesti ligipääsetavas kohas kõigile volitatud töötajatele.
- ISO7.11 - Välja tuleb töötada infovahetuse protseduurid s.h. e-posti kasutamine, interneti ja muude välisvõrkude kasutamine, mobiilne informatsiooni vahetamine, krüptograafilised vahendid info kaitseks, paberväljastusseadmete kasutamise koolitused;
- ISO7.12 - Elektrooniline sõnumivahetuse kaitstus s.h. sõnumite kaitse volitamata juurdepääsule, teenuse töökindlus, tugevamad turvanõuded info edastamisel avaliku võrgu kaudu;
- ISO7.13 - Erinevate logimiste haldus s.h. kasutajate identifitseerimine, andmetele ligipääsemised või nurjunud katsed, IDS/IPS ja tulemüüri süsteemide logid, administraator- ja operaatorlogid;
- ISO7.14 - Kellade sünkroniseerimised, et tagada ühtne ja täpne aeg.

ISKE (RIA 2011: p 1.4)

- ISKE7.1 - Täpsustab erinevaid meetmeid andmevarunduse halduses.

DHS (DHS 2011: p 2.8):

- DHS7.1 - Juhtimissüsteemide konfigureerijate rollid tuleb täpselt kindlaks määrata ja perioodiliselt testida.
- DHS7.2 - Juhtimissüsteemide ja tava infosüsteemide konfigureerimise pordid tuleb hoida eraldatuna. Seda võib teha füüsilisel, võrgu, vms. tasemel. Kui see ei ole millegi pärast võimalik, tuleb teostada rohkem kontrollimist.
- DHS7.3 - Erinevad juhtimissüsteemid ja nende erinevad moodulid tuleb hoida eraldi.
- DHS7.4 - Juhtimissüsteemides tuleks vältida koostöö tarkvarasid nt. konverentskõned, videokõned, sõnumivahetusesüsteemid. Kui seda ei õnnestu teha, tuleb antud lahendused välja lülitada, kui nendega ei töötada.
- DHS7.5 - Juhtimissüsteemide võrkudes tuleb vältida reaalajaliste suuremahulise video (nt. videotelefonid) ja ajakriitilise audio (nt. VoIP telefonid) edastamine.

- DHS7.6 - Kasutades kaasaegseid virtualiseerimise lahendusi, peab silmas pidama, et kasutada tuleb erinevaid turvalahendusi keskse virtuaalplatvormi kaitsmisele kui ka kõigil eraldi virtuaalmasinatel antud platvormil.

ENISA (ENISA 2011: Annex I):

- ENISA7.1 - Juhtimissüsteemides võivad puududa viirustõrje rakendused. Viirustürjet tuleb teostada väliste meetmetega.

5.7.2. Raamistiku olulised meetmed ja tegevused

- MT7.1 - Esmajärjekorras tuleb välja töötada kirjalikud süsteemide käitlemise protseduurid. Erilist tähelepanu tuleks pöörata süsteemide konkreetsete rollide määratlemisele ja regulaarsele kontrollile, parooli haldusele, varundamisele ja süsteemide taastamisele (ellu viia meetmed L ja M, vajadusel kaaluda H meetmeid), tehnilise toe kontaktinformatsiooni asjakohasena hoidmine. (N7, N9, R12, ISO7.1, ISKE7.1, DHS7.1)
- MT7.2 - Kõik muudatused tuleb ette planeerida ja vajadusel testkeskkonnas läbi teha. Muudatuste halduses tuleb määratleda muudatuste sisse viimise kord, teavitamine, vigase muudatuse tagasipööramise protseduurid, jne. (N6, R4, ISO7.2)
- MT7.3 - Tuleb luua konkreetselt eraldatud arendus-, töö- ja testkeskkond, mis ei oleks omakorda seotud üldise äriinfosüsteemide keskkonnaga. Eraldi tuleb hoida erinevad juhtimissüsteemide ja nende moodulid. Eraldamiseks tuleb kasutada seadmete füüsilist seadmete ja võrkude eraldamist, tulemüüre, jne. Välja tuleb töötada reaalsete ja testandmete kasutamise, genereerimise, kustutamise kord. Rahalise kokkuhoiu eesmärgil, võiks kaaluda äriinfosüsteemide ja juhtimissüsteemide testkeskkonna ühildamist. Vajadusel korral tuleks kasutada virtuaal- ja füüsilisi süsteeme. (N5, ISO7.3, DHS7.2, DHS7.3)
- MT7.4 - Välja tuleb töötada ühtne kolmandate osapoolte kasutamise reeglistik ja seda järgida. Ühtne halduskeskkond aitab ära hoida eraldi keerutakte lepingute loomist ja vajadusel saab kasutada erinevate olemasolevate teenusepakkujate teenuseid erinevates alamüksustes. Süsteemis peavad olema sisestatud kõik volitatud kontaktisikud ja nende pääsuõigused, jooksvate teenuse kirjeldused, varad, jne. (ISO7.4)
- MT7.5 - Erinevate ohtlike viiruste, pahavara, jne. tuleb võidelda erinevate meetmetega. Kogu tehniline informatsioon tuleb kõigile asjaomastele töötajatele kättesaadavaks teha ja hoida jooksvalt korras. Erinevad võrgu segmendid tuleb erineval tasemel kaitsta. Eraldi

seisvad ja segmenteerivad turvaseadmed peaksid võimaldama tagada turvalisust mitmel tasemel nt. viirustõrje, tulemüür, jne. (ISO7.5, ENISA7.1)

- MT7.6 - Võrkude planeerimise, loomise ja haldamise loogika tuleb viia üleettevõtteliseks. Vajadusel luua infosüsteem kogu informatsiooni halduseks. Kuna võrgu sisemine turve puudutab palju erinevaid osapooli, tuleb luua võimalikult laiapõhjaline meeskond, kes antud teemaga tegelevad. (ISO7.6)
- MT7.7 - Luua kitsamad reeglid juhtimissüsteemide väliste andmekandjate kasutusele antud süsteemidel. Keelata tuleb kõikide tundmatute ja isiklike andmekandjate kasutamine juhtimissüsteemides. Lubatud peab olema ainult konkreetselt testitud tootjate seadmed. Kõiki väliseid infokandjaid tuleb hoiustada ainult nendele ette nähtud turvaliselt piiratud ligipääsuga kohtades. Kõik andmekandjad tuleb peale nende eluea lõppu turvaliselt hävitada. Vajadusel sõlmida lepingud väliste partneritega. (vt. MT4.6) (N11, ISO7.7)
- MT7.8 - Kõik tööd konfiguratsioonifailidega tuleb kirjalikult talletada ja muudatused korrektselt dokumenteerida. Konfigureerimistööd võib läbi viia ainult töötaja või väline partner, kes omab antud süsteemide peale koolitust või sertifikaati. Vajaduse korral tuleb konfigureerimistööd testkeskkonnas järgi uurida ja alles eduka testimise järel töösüsteemi lisada. Konfiguratsiooniandmetele, olgu nad digitaalsed või paberil, tuleb luua ligipääs ainult töötajatele, kes otseselt nende andmetega midagi teevad. Kõik õigused tuleb talletada õiguste süsteemi andmebaasis ja seda tuleb perioodiliselt kontrollida. Sama moodi tuleb teha ka paberil olevate informatsiooniga. Võimaluse korral tuleks paberandmed digitaliseerida ja talletada infosüsteemi, kus on võimalik tekitada paremaid ligipääsusüsteeme. Kogu informatsioon tuleb hoida ühtses kohas ja vajadusel ajakohastada. (N10, R22, ISO7.8, ISO7.9, ISO7.10)
- MT7.9 - Töötajate selgemaks ja turvalisemaks erinevate võrguteenuste kasutamisel tuleb luua eeskirjad. Kindlasti on vaja eeskirju: e-postile, internetile, sotsiaalmeedia võrgustikele. Eraldi tuleks koolitada töötajaid mobiilseadmetega töötamisel ja kindlasti õpetama kasutama efektiivsemalt multifunktsionaalseid kontorilahendusi. (ISO7.11)
- MT7.10 - Elektroonilisel teel sõnumeid vahetavate süsteemidele tuleb kehtestada eraldi reeglid. Enne infovahetuse algust tuleb välja töötada infovahetuse ja konfidentsiaalsuslepingud. Kogu infovahetus üle avalike võrkude tohib toimida ainult läbi turvakanalite. Erandina on infovahetus e-posti teel, kus suurem osa informatsioonist ei ole kriitilise tähtsusega. Konfidentsiaalse info edastamisel e-posti teel tuleb sõnumid krüpteerida. Võimalusel tuleb kasutada ID-kaardi erinevaid lahendusi. (R14, ISO7.12)

- MT7.11 - Juhtimissüsteemides tuleb selgelt piirata koostöö tarkvarade (nt. Skype, Windows Live Messenger), sotsiaalvõrgustike, reaalajalise video ja audio kasutamist, jne. Kõiki antud teenused tuleb kasutada, vastavalt ametikoha õigustele, tava IT arvutivõrgus ja arvutites. (DHS7.4, DHS7.5)
- MT7.12 - Juhtimissüsteemide virtuaallahenduste servereid tuleb eriti hoolega kaitsta erinevate rünnakute eest. Tähelepanu all peavad olema nii virtualiseerimise platvorm kui erinevad virtuaalsed masinad. Võimaluse korral peab kaitsmine olema teostatud mitmekihiliselt. (DHS7.6)
- MT7.13 - Kõikide süsteemide logimisandmed tuleb dubleerida. Võimalusel tuleb kasutada turvalist keskset logiserverit. Logisid tuleb jooksvalt jälgida, eriti oluline on erinevate nurjunud ligipääsude ja kasutajaõiguste väärkasutused. (N12, R6, ISO7.13)
- MT7.14 - Täpse aja tagamisel tuleb kasutada olemasolevat lokaalset või välisvõrgu ajaserverite teenuseid. Tähelepanelik tuleb olla erinevate kella keeramistega . (ISO7.14)

5.8 Pääsu reguleerimine

Pääsu reguleerimise peamine eesmärk oleks korrektselt hallata kasutajatunnuseid, pääse, paroole ja erinevaid võrguturvalisuse teenuseid. (EVS 2008: p 11)

5.8.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 11):

- ISO8.1 - Reguleerida pääsu teabe juurde. Pääsu reguleerimise reeglid peaksid arvestama levitamise ja volitamise poliitikat.
- ISO8.2 - Pääsuhalduse loomine, mille reegliks oleks: “kõik , mis ei ole selgesõnaliselt lubatud, on üldiselt keelatud”.
- ISO8.3 - Pääsule esitatavate talituslike ja turvanõuete põhjal tuleks kehtestada, dokumenteerida ja läbi vaadata pääsu reguleerimise poliitika s.h. ligipääs rakendustele, ligipääs võrgule, pääsuõiguste väljastamine ja äravõtmine, pääsuõiguste regulaarne ülevaatamine.
- ISO8.4 - Privileegide halduse loomine s.h. iga süsteemitootega ja iga rakendusega seotud privileegid ning need kasutajad, kellele nad tuleb anda, tuleb identifitseerida, süsteemihalduslike privileege tuleks anda eraldi kasutajaidentifikaatoritele, privileegide regulaarne ülevaatamine.

- ISO8.5 - Paroolide haldus s.h. paroolihalduse süsteemi väljatöötamine, konfidentsiaalsuse kohustus, vaikeparoolide kohene vahetamine, süsteemi poolne sund paroolide vahetamiseks.
- ISO8.6 - Kasutaja kohustused s.h. paroolide loomise reeglitest kinni pidamine ja õpetada, kuidas valida kvaliteetseid ja õigeid paroole, järelvalveta seadmete sulgemine pärast töö lõpetamist ja/või ajutise lahkumise korral, tundliku paber või digitaalinformatsiooni kaitsmine läbi "tühja laua ja tühja ekraani poliitika".
- ISO8.7 - Võrguteenuste kasutamine s.h. ligipääs erinevatele võrkudele, ligipääs väljast sisse, võrguseadmete kasutamine, kaugdiagnostika, erinevate lahenduste segmenteerimine;
- ISO8.8 - Ligipääs operatsioonisüsteemidesse s.h. jäädvustada sisse ja väljalogimised, jäädvustada nurjunud logimised, süsteemiutiliitide minimaliseerimine ja vajadusel kõrvaldamine;
- ISO8.9 - Rakenduste ja teabe pääsu reguleerimine, mille eesmärk on välistada volitamata juurdepääs rakendussüsteemides hoitavale teabele s.h. konkreetse infosüsteemi infole ligipääs ainult töökoha profiiliga tööks vajalikule osale;
- ISO8.10 - Mobiiltöötlus ja -side, mille eesmärk oleks selgelt reguleerida mobiilseadmetega töötamine ja turvalisuse tagamine, s.h. loogiline ja füüsiline kaitse, informatsiooni (nii tundliku kui ka avaliku) hoiustamine mobiilseadmes, varundus ja jätkusuutlikus.

ISKE (EVS 2008: p M 2.11):

- ISKE8.1 - Paroolide haldamiseks tuleb kasutada M 2.11 meetmeid.

DHS (DHS 2011: p 2.15):

- DHS8.1 - Avalik ligipääs tuleb kõikide võimalike turvavahendeid kasutades sulgeda. Sama moodi tuleb seda teha ka tava IT töökohtade poolsete ühendustega juhtimissüsteemide võrku.
- DHS8.2 - Kõik juhtimissüsteemide kasutajatunnused peavad olema loodud igale kasutajale eraldi. Grupi kasutajatunnuseid ei tohi kasutada. Kõik umbmäärased kasutajanimed (guest, anonymous, jne.) tuleb sulgeda. Teenuste käivitamise kasutajatunnused peavad olema selgelt eristatavad.
- DHS8.3 - Perioodiliselt tuleb kontrollida olemasolevate töötajate kõiki füüsilisi ja loogilisi pääsumehhanisme, et need toimiks temale vajalikus ulatuses.

- DHS8.4 - Perioodiliselt tuleb kontrollida lahkunud töötajate füüsilisi ja loogilisi pääsumehhanisme, et need ei toimiks enam.
- DHS8.5 - Õigused peavad tulema kasutaja rollidest. Üleliigseid õiguseid ei tohi avada.
- DHS8.6 - Vajadusel tuleb luua mitmetasandiline õiguste kontroll.
- DHS8.7 - Paroolide haldus peab vastama kõrgematele turvanõuetele.
- DHS8.8 - Nurjunud ligipääsu, vale kasutajanime, jne. süsteemi pääsemise katsed tuleb reaalajaliselt monitoorida ja koheselt teavitada süsteemihaldureid meetmete tarvitusele võtmiseks.
- DHS8.9 - Kõik töökohad mis ei asu turvalistel aladel ja mis ei nõua pidevat töö tegemist tuleb mingi aja tagant kui töö tegemist ei toimu automaatselt lukustada. Erinevad ühendused süsteemide vahel tuleb automaatselt üle vaadata ja pikemaajalised jõudeolekus olevad ühendused katkestada.
- DHS8.10 - Kõik ettevõtte välised ühendused juhtimissüsteemidesse, tuleks keelata. Kui tehnoloogiliselt on vajadus juhtmevabade seadmete järele, siis nende kasutamine tuleks eraldi reguleerida.
- DHS8.11 - Võimaluse korral tuleb eelistada mobiilseid seadmeid, mille kasutusalaks on ainult ja ainult juhtimissüsteemid.
- DHS8.12 - Kõik välised ja isiklikud mobiilsed seadmed, andmekandjad, jne. on juhtimissüsteemides keelatud.
- DHS8.13 - Ligipääs koostöötamise tarkvaradele tuleks juhtimissüsteemides keelata.

ENISA (ENISA 2011: Annex I):

- ENISA8.1 - Kasutada tuleks erinevaid autentimise vahendeid nt. ID kaart, ühekordsed paroolid, biomeetrilised turvalahendused, jne.
- ENISA8.2 - Tulemüürides tuleb kasutada kõrgema taseme lahendusi ja süva paketi kontrolli mehhanisme.

5.8.2. Raamistiku olulised meetmed ja tegevused

- MT8.1 - Välja tuleb töötada üldine pääsupoliitika, arvestades kõiki juhtimissüsteemide omapärasid. Vajadusel tuleb kasutada mitut erinevat turvatehnoloogiat piiramaks ligipääsu. Reeglina tuleb pääs avada ainult tööks vajalikule minimaalsele õigusele. Antud materjalid peavad olema ühe osana sisemisest turvaraamistikust. (N14, ISO8.1, ISO8.2, ISO8.3, ISO8.4, ISO8.9)

- MT8.2 - Luua tuleb kasutajatunnuste, pääsuõiguste ja paroolide halduse keskne süsteem. Antud süsteemis tuleb eraldi välja tuua kasutajatunnuste tellimine, loomine, sulgemine ja kontroll, erinevate rollide (nt. süsteemsed kasutajad, administraatorid, tavakasutajad, jne.) õigused, paroolide tugevus, muutmise nõue, piirangud, probleemidest teavitamine, jne. Juhtimissüsteemides ei tohi kasutaja anonüümseid kasutajatunnuseid. Kõik kasutajatunnused peavad olema seostatud konkreetse inimesega. (N14, R8, R16, R17, R22, ISKE8.1, ISO8.4, ISO8.5, ISO8.6, DHS8.2, DHS8.5, DHS8.7)
- MT8.3 - Mobiilsetele töökohtade kasutajaid tuleb õpetada turvaliselt käituma erinevates töökohtades. Võimaluse korral tuleb keelata seadmete ristkasutamist ja hankida eraldi mobiilsed konfigureerimisseadmed juhtimissüsteemidele. (ISO8.10, DHS8.11)
- MT8.4 - Regulaarselt tuleb üle vaadata ja jooksvalt kontrollida järgnevad tegevused kõik vaikeparoolid tuleb muuta; kasutajatunnuseid, mis ei ole leidnud kasutamist sulgeda; olemasolevad õigused ja kasutajatunnused; lahkunud töötajate kasutajatunnused; tähtis on paralleelselt vaadelda füüsilisi ja loogilisi ligipääse. (DHS8.3, DHS8.4)
- MT8.5 - Erinevate ressurssidele ligipääs tuleks juhtimissüsteemides tagada mitmetasemeliselt nt. kasutajatunnus, ID-kaart, konkreetne IP aadress, konkreetne kellaaeg, jne. Kõik ebaturvalised võrguteenused tuleb sulgeda. (N15, DHS8.6, ENISA8.1)
- MT8.6 - Võrgud tuleb segmenteerida. Kasutada tuleb tulemüüre, IPS/IDS seadmeid, ja muid turvalisust tõstvaid võrgumeetmeid. Erinevad juhtimissüsteemid tuleb hoida lahus üksteisest. Kõiki lahendusi tuleb keskselt monitoorida ja koheselt probleemidest teavitada õigeid töötajaid. Välistada tuleb tundmatute IT tavavõrgu klientide pääsu juhtimissüsteemidesse. Keelata tuleb kõik ettevõtte välised ühendused sisevõrku ja juhtimissüsteemidesse. Juhtmevabade ühenduste kasutamine tuleb lugeda mittesoovitavaks, kuid erilise vajaduse korral tuleb välja tööta eraldi reeglistik. (N13, N16, N17, R1, R3, R6, R11, ISO8.7, DHS8.1, DHS8.10, ENISA8.2)
- MT8.7 - Välja tuleb töötada erinevate süsteemide vahelised ühenduste reeglistik. Vajadusel rakendada mitmetasemelist turvakontrolli. Jõudeolekus olevad ühendused tuleb katkestada. (DHS8.9)
- MT8.8 - Töötajaid tuleb koolitada kasutajatunnuste ja paroolidega turvaliselt ümber käima, lahkudes töökohalt lukustama süsteemi ja töö lõppedes lülitama töökoha arvuti välja. Pikemaajaliselt jõude olekus arvutid tuleb automaatselt lukustada ja avada alles parooli sisestamise peal. (R8, ISO8.6, DHS8.9)

- MT8.9 - Jooksvalt tuleb monitoorida erinevaid süsteemseid ligipääse ja tulemüüri logisid. Probleemide korral tuleb kiirelt ja asjakohaselt reageerida. Vajaduse korral tuleb teavitada erinevaid töötajaid. (ISO8.8, DHS8.8)
- MT8.10 - Juhtimissüsteemides tuleb keelata isiklikud seadmed ja välised meediakandjad, ja võtta kastusele meetmed antud vallas. (DHS8.12)
- MT8.11 - Koostöötamise tarkvarade (nt Skype, Live Messenger, jne.) kasutamine tuleb juhtimissüsteemide keskkonnas keelata. (DHS8.13)

5.9. Infosüsteemide hankimine, väljatöötamine ja hooldus

Infosüsteemide hankimise, väljatöötamise ja hoolduse peamine eesmärk on turvaliselt hallata infosüsteemide eluea jooksul tehtavaid tegevusi. (EVS 2008: p 12)

5.9.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 12):

- ISO9.1 - Infosüsteemide turvanõuded, mille eesmärk on tagada, et turvalisus on infosüsteemide lahutamatu osa.
- ISO9.2 - Õige töötlus rakendustes, kus on eesmärk vältida rakendustes teabe vigu, kaotsiminekut, lubamatut muutmist või väärkasutust.
- ISO9.3 - Süsteemifailide turve, mis peab tagama süsteemifailide turve. Süsteeme tuleb turvata nii töö kui testfaasides.
- ISO9.4 - Turve arendus- ja tugiprotsessides, milles on oluline kõigi erinevate protsesside (muudatused süsteemis, muudatused operatsioonisüsteemis ja puutepunkt süsteemiga, väljast tellitud arendused, jne.) turvalisuse tagamine.
- ISO9.5 - Tehniliste nõrkuste haldus, mille eesmärk on vähendada riske, mis tulenevad avaldatud tehnilistest nõrkustest. Vaadelda tuleb kogu terviklahenduse erinevaid tehnilisi komponente.

DHS (DHS 2011: p 2.5, p 2.10):

- DHS9.1 - Ettevõtte peab välja töötama formaalse dokumendi, kus on määratud teiste seas infosüsteemide turvaline käitlus. Antud dokument peab kajastama infosüsteemi kõiki turvaspekte kogu tema eluea jooksul.

- DHS9.2 - Infosüsteemi loomisel, hankimisel ja töös hoidmisel peab järgima erinevaid litsentsitingimusi, olema kooskõlas erinevate õigusaktide, sisemiste eeskirjade, jne.
- DHS9.3 - Kõik infosüsteemide, mis on ostetud, tellitud või ise arendatud, peavad oma tervikliku dokumentatsiooni.
- DHS9.4 - Ettevõte peab omama ülevaadet kogu infosüsteemi tarneahelast. Vajadusel tuleb tutvuda tarnija ja temaga seotud kolmandate isikute sertifikaatide, litsentside, juhendite, jne.
- DHS9.5 - Infosüsteemi väljatöötamisel peavad kõik osalised hoidma ennast kursis turvalisus probleemidega oma valdkonnas.
- DHS9.6 - Juhtimissüsteemide kõiki infosüsteeme tuleb eelnevalt testida testkeskkonnas.
- DHS9.7 - Vajaduse korral tuleb välja töötada sisemised nõuded sisemiste infosüsteemide arendustööde väljatöötamiseks.
- DHS9.8 - Tähelepanelik tuleb olla vanade süsteemide töös hoidmisega ja võimaluse korral need välja vahetada nii pea kui saab.
- DHS9.9 - Süsteeme tuleb korrapäraselt hooldada. Süsteemide väliseks hoolduseks tuleb eelnevalt sõlmida leping, mis tagaks juhtimissüsteemide turvalise hooldusteenuse saamise.

5.9.2. Raamistiku olulised meetmed ja tegevused

- MT9.1 - Tuleb luua formaalne dokument, milles oleksid kirjeldatud infosüsteemide hankimise, välja töötamise ja hoolduse nõuded. (ISO9.1, ISO9.2, DHS9.1)
- MT9.2 - Infosüsteemi erinevates elutsüklites tuleb tagada infosüsteemi enda turvalisuse kõrval süsteemi üldine turvalisus. (N20, ISO9.3, ISO9.4, ISO9.5)
- MT9.3 - Infosüsteemide erinevad arendustööde materjalid, dokumendid, litsentsid, tuleb talletada ühtsesse kohta ja uuendada neid. Kõik süsteemide peavad omama täielikku dokumentatsiooni. (R5, DHS9.2, DHS9.3)
- MT9.4 - Infosüsteemid tuleb hankida vastavalt vajadusele. Eelistada tuleks laiemalt levinud lahendusi. Tootjad ja arendajad peavad omama kõike vajalike sertifikaate, järgima seadusi ja standardeid. (N19, DHS9.4, DHS9.5)
- MT9.5 - Kõik juhtimissüsteemide infosüsteemid tuleb testida testkeskkonnas. Kogu testimise informatsioon tuleb dokumenteerida ja säilitada hilisemaks ülevaatuseks. (N18, R17, DHS9.6)

- MT9.6 - Enda arendatud juhtimissüsteemi infosüsteemid peavad vastama kõigile nõuetele. Sisemised töötajad peavad olema läbinud kõik koolitused ja omama vastavaid sertifikaate. (DHS9.7)
- MT9.7 - Eraldi juhendmaterjal tuleb koostada vanade süsteemide kasutamisel töökeskkonnas. Võimaluse korral tulevad need võimalikult kiiresti vahetada uute süsteemide vastu. Tähelepanelik tuleb olla erinevate turvaaspektide kohapealt kuna vanemad süsteemid ei pruugi omada häid turvameetmeid ja kasutusel tuleb hoida erinevaid lahendusi. (DHS9.8)
- MT9.10 - Süsteemide hooldusel tuleb sõlmida kõigi osapooltega hooldus- ja konfidentsiaalsuslepingud. Tähele tuleb panna piiranguid teistest turvalisuse valdkondadest vt. 5.6. Füüsilise ja keskkonna turve, 5.8 Pääsu reguleerimine. (DHS9.9)

5.10. Infoturbeintsidentide haldus

Infoturbeintsidentide halduse peamine eesmärk on infoturbeintsidentide kogumine, nendest õppimine ja nendeks ettevalmistumine. (EVS 2008: p 10)

5.10.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 10):

- ISO10.1 - Teatamine erinevatest intsidentidest (nt. inimvead, süsteemi ülekoormus, füüsilised turvalisus probleemid, ligipääsude rikkumised, jne.), mille eesmärk on tagada infosüsteemidega seotud turvasündmustest, et oleks võimalik õigeaegselt rakendada parandusmeetmeid. Teatamiskohustus tuleb panna kõigile osapooltele k.a. ettevõttega seotud kolmandatele osapooltele.
- ISO10.2 - Infoturbeintsidentide ja täiustuste haldus, mille eesmärgiks oleks tagada järjekindel ja toimiva metoodika rakendamine. Sisemiselt tuleb konkreetselt määratleda kohustused ja protseduurid .
- ISO10.3 - Intsidentidega võitlemisel tuleb kohe ka nendest õppida. Konkreetselt tuleks hinnata kõike intsidente ja määrata nende tüüpe, suurusi ja kasvõi umbkaudseid rahalisi kahjusid. Õppimine vanadest juhtumitest aitab kindlasti tulevikus paremini toime tulla.
- ISO10.4 - Infoturbe intsidentide tekkimisel tuleks mõelda kohe asitõendite kogumisele, kuna vajadusel on tulevikus vaja tõendeid sisemisteks distsiplinaarmenetlusteks või siis juba kohustus anda väljapoole edasi asjaomastele struktuuridele asjasse puutuvat informatsiooni.

DHS (DHS 2011: p 2.12):

- DHS10.1 - Ettevõte peab välja töötama intsidentide halduse. Välja peab töötama intsidenti halduse infosüsteemi. Süsteemis peab olema jälgitav kogu intsidendi eluea kõik etapid.
- DHS10.2 - Infosüsteemi alusel peab infoturve probleeme jälgima ja analüüsima.
- DHS10.3 - Infosüsteem peab automaatselt teavitama intsidentidest kõigi asjaosalisi. Vajadusel tuleb kaasata teisi vajalikke töötajaid probleemi lahendamises.
- DHS10.4 - Välja tuleb töötada üldiste intsidendi lahendamise standardsed plaanid. Plaane tuleb testida ja arendada, et tagada probleemi optimaalseim lahendamine.
- DHS10.5 - Igale intsidendile tuleb võimalikult optimaalselt läheneda. Regulaarselt tuleb jälgida intsidente ja nende lahendamist. Vajadusel tuleb korrigeerida intsidendi lahendamist ja vajadusel tuleb töötajaid probleemsetes valdkondades koolitada.

5.10.2. Raamistiku olulised meetmed ja tegevused

- MT10.1 - Välja tuleb töötada üleettevõtteline IT intsidentide haldus. Olemasoleva juhtimiskeskuse intsidendihalduse platvormile tuleb lisada IT valdkonna põhised juhtimissüsteemide klassifikaatorid, töötajad kes probleemidega tegelevad, koolitada juhtimiskeskuse töötajaid sisestama uusi probleeme, jne. (ISO10.1, ISO10.2, DHS10.1, DHS10.3,)
- MT10.2 - Perioodiliselt tuleb analüüsida intsidentide andmebaasi. Probleeme tuleb korrektselt klassifitseerida ja võimaluse korral välja töötada standard plaane erinevatele sagedasti esinevatele probleemidele. Intsidentide põhjal tuleb vajadusel koolitada nii IT kui ka tavatöötajaid turvalisemalt ja paremini kasutama IT vahendeid. Töötajatele peab meelde tuletama teavitamise kohustusest ja peab julgustama teavitama erinevatest probleemidest. (N21, N22, R21, ISO10.3, DHS10.2, DHS10.5)
- MT10.3 - Tõsisemate probleemide korral tuleb kohe alustada erinevate asitõendite korrektselt kogumist, dokumenteerimist ja süsteemi sisestamist. Koostöös erinevate osakondadega tuleb koolitada töötajaid antud valdkonnas. (ISO10.4)

5.11. Jätkusuutlikkuse haldus

Jätkusuutlikuse haldus on katkematu töö tagamise planeerimine, testimine, teostamine, hooldus ja ümberhindamine. (EVS 2008: p 14)

5.11.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 14):

- ISO11.1 - Jätkusuutlikuse tagamiseks kogu organisatsioonis tuleks välja töötada ja käigus hoida hallatav protsess, mis hoolitseb organisatsiooni jätkusuutlikkuseks vajalike infoturbenõuete eest s.h. riskid, elutähtsate tööprotsesside varad, infoturbeintsidentidest põhjustatud tegevuskatkestuste tõenäolise toime tundmine, kehtestatud plaanide ja protsesside regulaarne testimine ja ajakohastamine, jne.
- ISO11.2 - Välja tuleb selgitada talitusprotsessi katkestada võivad sündmused.
- ISO11.3 - Tuleks koostada ja viia ellu plaanid talituse säilimiseks või taastamiseks ning teabe käideldavuse tagamiseks nõutavalt tasemel ja nõutavate aegadega pärast elutähtsa põhiprotsessi katkestuse või tõrget. Tuleks silmas pidada, et kriisihalduse plaanid ja tegevused võivad erineda jätkusuutlikkuse halduse omadest s.t. võib esineda kriis, millega saab toime tulla tavalise haldusprotseduuridega.
- ISO11.4 - Jätkusuutlikkuse plaane tuleks nende ajakohasuse ja toimivuse tagamiseks regulaarselt testida ja ajakohastada s.h. stsenaariumite läbimängimine paberil, erinevad simuleeringud, taastamine alternatiivses asukohas, jne.

DHS (DHS 2011: p 2.12):

- DHS11.1 - Välja tuleb töötada jätkusuutlikkuse plaanid. Plaanis tuleb kirjeldada erinevate stsenaariumite järgi tegevused. Selgelt peab olema välja toodud erinevate töötajate rollid ja tegevused avarii korral.
- DHS11.2 - Tõsise avarii korral, kui käivitatakse jätkusuutlikkuse plaani, tuleb põhisüsteem korrektselt turvarežiimi tööle jätta. Tuleb teavitada kõigi osapooli. Probleemi lahenemisel tuleb tagasi minna algsele süsteemile ja jätkata igapäevatööd.
- DHS11.3 - Peale avarii lahendamist tuleb kõik tegevused läbi analüüsida ja vajadusel muuta, optimeerida ja õppida neist.
- DHS11.4 - Regulaarselt tuleb läbi viia treeninguid, et jätkusuutlikus oleks tagatud tõsiste avariide korral. Treeningute osana tuleb jälgida reageerimisaega. Treeningu läbides tuleb analüüsida kõike tegevusi ja vajadusel muuta plaani.

- DHS11.5 - Luua tuleb alternatiivne asukoht, kus on olemas kõik telekommunikatsioonid ja seadmed, et töötada võimalikult efektiivselt avarii olukordades. Alternatiivsele asukohale tuleb teha riskianalüüs ja vajadusel korrigeerida kõikide vahendite olemasolu.
- DHS11.6 - Alternatiivse asukoha süsteeme tuleb regulaarselt testida. Süsteeme tuleb regulaarselt varundada ja testida taastamist.

NIST (Falco, Stouffer, Scarfone 2011: p 6.2.3.2):

- NIST11.1 - Tuleb luua personali nimekiri, kes pääsevad ligi avarii korral erinevatele IT süsteemidele.
- NIST11.2 - Avarii olukorraks peab juhtimissüsteemide IT lahenduse kõrval olema olemas manuaalse juhtimise plaan juhuks, kui IT süsteemi ei ole võimalik töösse rakendada õigeaegselt.
- NIST11.3 - Luua konkreetsete töötajate nimekiri kelle vastutusalaks on alternatiives asukoha seadmestiku hooldus, varunduse tegemine ja taastamise testimine.

5.11.2. Raamistiku olulised meetmed ja tegevused

- MT11.1 - Välja tuleb töötada ettevõtte IT jätkusuutlikkuse plaan ja integreerida see olemasoleva jätkusuutlikkuse plaaniga. Välja tuleb selgitada kõik IT vahendeid kasutavad ärikriitilised protsessid. Erinevate intsidentide lahendamiseks tuleb luua omad plaanid. (ISO11.1, ISO11.2)
- MT11.2 - Plaanid tuleb välja töötada, koolitada kõike osapooli ja testida. Testimiseks võib kasutada mitmeid erinevaid meetodeid nt. reaalne testimine töökohal, paberil testimine, jne. Peale treeninguid tuleb tulemused dokumenteerida ja vajadusel teha korrektuurid plaanis. Tulemused tuleb läbi arutada kõigi osalejatega. Lõppraport tuleb kinnitada juhatuse poolt. (N23, N24, ISO11.3, ISO11.4)
- MT11.3 - Riskianalüüsist lähtuvalt tuleb leida alternatiivne asukoht, kus on võimalik jätkata tööd avarii ajal. Tuleb luua nimekiri IT töötajatest, kelle ülesandeks on osalemine avarii situatsiooni likvideerimisel ja kes tegelevad regulaarse alternatiiv asukoha seadmete hoolduse ja testimise, varunduse tegemise ja taastamise testimisega. Kõiki andmeid tuleb regulaarselt varundada ja testida nende taastamist. Vajadusel tuleb süsteeme kaasajastada. (N24, ISO11.4, NIST11.3)
- MT11.4 - Avarii korral, kui on otsustatud käivitatakse jätkusuutlikkuse plaani, tuleb põhisüsteem korrektselt turvarežiimi tööle jätta ja alustada paani järgimist. Valmis peab

olema manuaalseks juhtimiseks, kui IT süsteemid ei võimalda turvalist juhtimist. Probleemi lahendamisesesse peab kaasama ainult vajalikud IT töötajad. Avarii lahendamisel tuleb tagasi minna algsele süsteemile ja jätkata igapäevatööd. Kõik tegevused ja probleemid tuleb dokumenteerida ja lõppraport tuleb esitada juhatusele kinnitamiseks. (R19, R20, ISO11.4, NIST11.1, NIST11.2)

5.12 Vastavus

Vastavuse põhieesmärk on vältida õigusaktide, põhikirja, eeskirja nõuete, lepinguliste kohustuste ja turvanõuete rikkumist. (EVS 2008: p 15)

5.12.1. Valdkonna lühikokkuvõte ja nõuded

ISO/IEC27002 (EVS 2008: p 15):

- ISO12.1 - Kõik kohaldatavad õigusaktid, eeskirjad ja lepingute nõuded ning organisatsiooni meetod nende nõuete täitmiseks tuleks iga infosüsteemi ja kogu organisatsiooni kohta selgelt määratleda, dokumenteerida ja hoida ajakohasena.
- ISO12.2 - Kõik materjalid, mille suhtes võivad kellelgi olla intellektuaalse omandi õigused, ja omandlike tarkvaratoodete kasutamisel tuleks rakendada asjakohaseid protseduure, millega tagada vastavus õigusaktidele, eeskirjade ja lepingute nõuetele.
- ISO12.3 - Andmekaitse ja privaatsus tuleks tagada vastavalt kohaldavaile õigusaktide ja eeskirjade ning võimalike lepingusätete nõuetele.
- ISO12.4 - Kasutajaid tuleks tõrjuda kasutamast infotöötlusvahendeid lubamatuks otstarbeks.
- ISO12.5 - Tuleb tagada süsteemide vastavus organisatsiooni turvapoliitikatele ja -normidele.
- ISO12.6 - Süsteemide õige auditeerimine

DHS (DHS 2011: p 2.16,):

- DHS12.1 - Auditeerimise läbiviimisel tuleb vaadata, et antud toimingud ei tekitaks juhtimissüsteemides probleeme. Eelnevalt tuleb kooskõlastada kõik tegevused ja hinnata võimalike probleeme nende läbiviimisel.

5.12.2. Raamistiku olulised meetmed ja tegevused

- Kogu dokumentatsioon tuleb hoida ajakohasena. Määratleda tuleb vastutavad isikud ja regulaarselt kontrollida vastavust. (ISO12.1)
- Tava kasutajaid tuleb koolitada ja informeerida erinevatest õigusaktidest ja eeskirjades. Selgitada tuleb tavatöötaja tähtsus erinevates intellektuaalomandi probleemides ja võimalikest sanktsioonidest. Intellektuaalse omandi kaitse punktid tuleb selgelt välja tuua sisekorra eeskirjades ja töötaja peab andma allkirja tutvumise kohta. Füüsiliste ja loogiliste turvameetmetega tuleb võimalikult palju piirata võimalikke illegaalseid tegevusi nt. piraattarkvara allalaadimine, võrguteenuste häirimine, mittesobiliku sisuga materjalide hoiustamine ja levitamine, jne. Infotöötlusvahendeid tuleb kasutada peamiselt töö eesmärkidel. (R15, ISO12.2, ISO12.4, ISO12.5)
- Andmete töötlemisel tuleb jälgida erinevaid õigusakte. Eriti tähelepanelik tuleb olla delikaatsete andmete töötlemisel. Vajadusel tuleb konsulteerida Andmekaitse Inspektsiooniga. (R2, ISO12.3)
- IT auditeid tuleb läbi viia regulaarselt. Läbi tuleb viia nii sisemisi kui ka väliseid auditeid. Auditi plaan tuleb kõigiga kooskõlastada ja jälgida selle täpset täitmist. Auditi läbiviimisel tuleb tähelepanu pöörata, et ei segataks igapäevatööd nt. ressursimahukate võrgu turvatestide läbiviimine. (N25, ISO12.6, DHS12.1)

6. Tuleviku edasiarendused

Juhtimissüsteemide turvaraamistiku loomine on esimene suurem samm turvalisuse tõstmisel. Vaadeldes pikemat perspektiivi tuleks koheselt edasi tegeleda järgnevate valdkondadega:

- Riskide kaalutlemine ja käsitlus
    - Läbi viia detailne juhtimissüsteemide IT riskianalüüs.
- Turvapoliitika
    - Lähiajal ei ole näha, et välja töötatakse universaalne raudteel kasutatav juhtimissüsteemide IT turbe standard. Seega tuleb detailse riskianalüüsi tulemusena hakata edasi arendama raamistiku. Selle aluse tuleb välja töötada ühtne ettevõttesisene juhtimissüsteemide turvastandard;
    - Tuleb hoida kursis valdkonna standardite ja parimate praktikaga ja vajadusel muuta olemasolevat sisest standardit või vajadusel võtta kasutusele mõni sobilikum.
- Infoturbe korraldus
    - Luua juhtimissüsteemide IT turbe eest vastutaja ametikoht või ümber korraldada mõne olemasoleva töötaja töö, et antud valdkond oleks kaetud;
    - Luua koostöövõrgustik erinevate juhtimissüsteemide ettevõtete vahel vahetamaks kogemusi ja praktikaid IT turbe lahenduste vallas.
- Inimressursiturve
    - Luua iga-aastane stabiilne turvakoolituse eelarve. Kasutada kõiki võimalusi töötajate turvateadlikkuse tõstmiseks.
- Side ja käituse haldus
    - Luua juhtimiskeskuse IT lahenduste testkeskkond virtuaalplatvormile. Uurida erinevaid võimalusi juhtimissüsteemide IT lahenduste turvaliseks käitlemiseks virtuaalkeskkondades;
    - Luua juhtimiskeskusesse IT süsteemide monitooringu lahendus.
- Infosüsteemide hankimine, väljatöötamine ja hooldus
    - Turvaline juhtimissüsteemide arendamine on üks suuremaid väljakutseid kogu raudtee juhtimise valdkonnas. Olemasolev raamistik ei käsitle praktiliselt konkreetsete süsteemide arendustega seotud probleemistiku. Süsteemide arendamine ja programmeerimise jaoks on olemas eraldi standardid ja neid tuleks vaadelda järgmistes faasides eraldi.

- Infoturbeintsidentide haldus
    - Integreerida olemasolevasse juhtimiskeskuse intsidentide infosüsteemi IT alased intsidentide haldus.
- Jätkusuutlikkuse haldus
    - Kaasata jätkusuutlikkuse koolitusse ja treeningutesse rohkem IT töötajaid;
    - Alustada alternatiivse juhtimiskeskuse IT lahenduse projekteerimist.
- Vastavus
    - Läbi viia ettevõtte üldine IT infosüsteemide, IT turvasüsteemide ja juhtimissüsteemide IT audit.

Kokkuvõte

Turvalisuse tagamine juhtimissüsteemides on pidev protsess. Keskendudes välistele häkkeritele ja terrorismile, võime kiirelt kaotada fookuse, mis kokkuvõttes tähendab ühekülgset ja puuduliku turvaeeskirja ja mitteturvalist käitumist.

Esimeses peatükis vaadeldi üldiselt infoturvet ja selle standardiseerimist.

Teises peatükis tehti lühikokkuvõte juhtimissüsteemidest. Võrreldi juhtimissüsteeme ja tava IT lahendusi.

Kolmandas peatükis vaadeldi ettevõtet Eesti Raudtee ja tehti lühikokkuvõte ajaloost, üldistest numbritest ja peamiselt kasutatavatest juhtimissüsteemidest.

Neljandas peatükis pöörati tähelepanu üldistele nõuetele raudteel ja juhtimissüsteemide turvalisusele. Kirjeldati erinevaid õigusakte ja toodi välja erinevad juhtimissüsteemide turvalisuse standardid ja parimad praktikad. Kirjeldati lühidalt suurte riikide kriitilise infrastruktuuri turvalisuse haldajaid.

Viiendas peatükis toodi välja konkreetsed standardid, soovitused ja parimad praktikad, mille alusel luuakse raamistik. Tehti jäme riskianalüüs. Kõikide soovituste põhjal loodi üldine turvaraamistiku punktid, mida tuleks järgida ettevõtte sisese turvastandardi loomisel.

Kuuendas peatükis tehti ettepanekuid tuleviku arendusteks.

Nagu näha on IT turvalisususe tagamine juhtimissüsteemides mõnevõrra teistsuguse rõhuasetusega kui tavalise äri IT lahendustes, samas põhilised märksõnad on samad. Turvalisuse tagamine ei pea olema kallis ja raske. Tehes asju mõistlikul viisil, järgides suuniseid ja edasi arendades turvaraamistiku suudame me enda ümber tekitada turvalist maailma.

Kasutatud kirjandus

1. AS Eesti Raudtee 2011. Eesti Raudtee aastaaruanne 2010. http://www.evr.ee/failid/AASTARAAAMAT_2010.pdf (28.02.2012).
2. Centre for the Protection of National Infrastructure 2012. Koduleht. http://www.cpni.gov.uk/ (07.04.2012).
3. Eesti Standardikeskus 2008. EVS-ISO/IEC 27002:2008. INFOTEHNOLOOGIA: Turbemeetodid: Infoturbe halduse tegevusjuhis (ISO/IEC 27002:2005).
4. European Network and Information Security Agency 2012. Koduleht. http://www.nisa.europa.eu/ (28.02.2012).
5. European Network and Information Security Agency 2011. Protecting Industrial Control Systems. Recommendations for Europe and Member States. Annex I - VI. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems (28.02.2012).
6. Euroopa Nõukogu(EN) direktiiv 2008/114/EÜ 2008. Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta.
7. Falco, Joe; Scarfone, Karen; Stouffer, Keith 2011. Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-82 http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (03.04.2012).
8. Geers, Kenneth 2011. Strategic Cyber Security. ISBN 978-9949-9040-7-5. Tallinn.
9. ISA99 2011. ISA-62443.03.03 (99.03.03): Security for industrial automation and control systems: System security requirements and security assurance levels: Draft 3. http://www.isa.org/ (09.03.2012).
10. Kaska, Kadri; Tikk, Eneken, Vihul, Liis 2010. International Cyber Incidents: Legal Considerations. ISBN 978-9949-9040-0-6. Tallinn. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (28.02.2012).
11. National Communication System 2004. Supervisory Control and Data Acquisition (SCADA) Systems. http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf (28.02.2012).

12. PA Consulting Group for Centre for the Protection of National Infrastructure 2005-2011. Process control and SCADA security - good practice guidelines. http://www.cpni.gov.uk/advice/infosec/business-systems/scada/ (07.04.2012).
13. Riigi Infosüsteemide Arenduskeskus Juuli 2009. Infoturbe juhend. http://www.ria.ee/public/ISKE/Infoturbe_soovituste_juhend_v1.pdf (28.02.2012).
14. Riigi Infosüsteemi Amet 2011. Infosüsteemide Kolmeastmelise Etalonturbe süsteem ISKE http://www.ria.ee/iske (28.02.2012).
15. Riigi Infosüsteemi Amet 2012. Kriitilise informatsiooni infrastruktuuri kaitse. http://www.ria.ee/kiik/ (28.02.2012).
16. Riigi Teataja 2009. Vabariigi Valitsuse määrus: Infosüsteemide turvameetmete süsteem. https://www.riigiteataja.ee/akt/12901110?leiaKehtiv (28.02.2012).
17. Riigi Teataja 2011. Hädaolukorra riskianalüüsi koostamise juhend. https://www.riigiteataja.ee/akt/125112010010?leiaKehtiv (28.02.2012).
18. Riigi Teataja 2012. Hädaolukorra seadus. https://www.riigiteataja.ee/akt/130122011044?leiaKehtiv (28.03.2012).
19. Riigi Teataja 2012. Raudteeseadus. https://www.riigiteataja.ee/akt/120122011015?leiaKehtiv (28.02.2012).
20. Stiennon, Richard 2010. Surviving Cyberwar. ISBN 978-1-60590-675-1. USA.
21. The Trusted Information Sharing Network 2012. Koduleht. http://www.tisn.gov.au/Pages/default.aspx (07.04.2012).
22. US-CERT 2012. U.S. CERT juhtimissüsteemide koduleht. http://www.us-cert.gov/control_systems/ (07.04.2012).
23. U.S. Department of Homeland Security 2012. Koduleht. http://www.dhs.gov/index.shtm (07.04.2012).
24. U.S. Department of Homeland Security 2009. Strategy for Securing Control Systems. http://www.us-cert.gov/control_systems/pdf/Strategy%20for%20Securing%20Control%20Systems.pdf (28.02.2012).
25. U.S. Department of Homeland Security 2011. Catalog of Control Systems Security: Recommendations for Standards Developers. http://www.us-cert.gov/control_systems/pdf/CatalogofRecommendationsVer7.pdf (28.02.2012).

26. U.S. Department of Homeland Security 2011. Common Cybersecurity Vulnerabilities in Industrial Control Systems. http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf (28.02.2012).
27. U.S. Department of Homeland Security 2012. Control Systems Security Program and Industrial Control Systems Cyber Emergency Response Team: CSSP Year in Review: FY2011. http://www.us-cert.gov/control_systems/pdf/Year_in_Review_FY2011_Final.pdf (03.04.2012).

Summary

IT Security Framework for Control Systems. The Case of Estonian Railways Ltd

In the modern world we constantly come into contact with various IT-solutions. Whether hardware solutions for tablets, laptops or PCs, mobile phones, ATMs or software operating systems, office software or internet applications for information portal, social media communities, they all need a simple and safe environment. Many IT-solutions operate in the background. We practically do not notice them as they are utilised to control different technological solutions, e.g. the control of ships, airplanes and trains; the management of mobile communications; the control of technology in factories; the management of equipment of a nuclear power station, etc.

The solutions that control and manage various infrastructure solutions and technical solutions for factories are in general divided into two: supervisory control and data acquisition (SCADA) and distributed control system (DCS). Various standards and frameworks have been created for different solutions, but there is no common and universal one as probably it is not reasonably possible. Taking into account the various specific features of different fields, many general security standards have been established based on various companies' best security practices and in conformity with the general safety rules.

The aim of the present master's thesis is to establish a general security framework for the IT infrastructure of railway control systems based on the example of AS Eesti Raudtee. The objective is to find an optimal solution employing the most common standards, recommendations and best practices.

The first chapter gives an overview of information security and the standardisation thereof.

The second chapter gives a short overview of control systems. A comparison of control systems and ordinary IT-solutions is provided.

The third chapter concentrates on AS Eesti Raudtee and describes the history of the company, gives an overview of general indicators and the main control systems used by the company.

The fourth chapter highlights the general requirements applicable on railways and the requirements established for the security of control systems. Different legislation is described and the standards and best practices of control system security are highlighted. A short overview is given of the administrators of IT security of critical infrastructure in major countries, also of their standards, instruction materials and best practices.

The fifth chapter analyses various standards, best practices and recommendations for the administration of security. The main resources used are the following:

- Information technology Security techniques. Code of practice for information security management (ISO/IEC 27002:2005) – a section of this standard is used as it reasonably covers all IT-security related domains. In addition, the fundamental principles that the author of the present master's thesis considered important in creating an overall framework in the context of control systems have also been taken from this standard;
- ISKE (three-level IT baseline security system) – as an addition, the materials of ISO/IEC27002 are, if necessary, complemented by ISKE measures that provide an additional value to control system security;
- U.S. Department of Homeland Security 2011. Catalog of Control Systems Security: Recommendations for Standards Developers. – the specific additional recommendations for the developers of a control system standard are discussed;
- European Network and Information Security Agency 2011. Protecting Industrial Control Systems. Recommendations for Europe and Member States. – the specific recommendations as regards the improvement of control system security are discussed;
- Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC): Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-82 – the specific additional recommendations as regards the establishment of control system security are discussed.
- PA Consulting Group for Centre for the Protection of National Infrastructure 2005-2011. Process control and SCADA security - good practice guidelines – the specific best practices for control systems are discussed.

- If necessary, other important acts, standards and best practices, e.g. HOS (emergency response systems), Railways Act, railway-specific standards.

An overall risk analysis is provided. Based on all of the recommendations a general security framework is provided that should be followed in developing an IT security standard for an internal control system.

The sixth chapter concentrates on future developments.

The guaranteeing of security of control systems is an on-going process. Concentrating on external hackers and terrorism we may soon lose focus which may result in a one-sided and faulty security protocol and unsafe behaviour. The guaranteeing of IT-security in control systems has a somewhat different emphasis than in the case of ordinary business IT-solutions. However, the main keywords are the same. The ensuring of safety does not have to be expensive and difficult. When doing things reasonably, following guidelines and developing the security framework further we are able to create a secure world around us.

Lühendid

IT	infotehnoloogia
SCADA	supervisory control and data acquisition
DCS	distributed control system
EVR	AS Eesti Raudtee
HOS	Hädaolukorra seadus
DHS	U.S. Department of Homeland Security
RIA	Riigi Infosüsteemi Amet
ISKE	infosüsteemide kolmeastmeline etalonturbe süsteem
BSI	Bundesamt für Sicherheit in der Informationstechnik
ISO	International Standard Organisation
IEC	International Electrotechnical Commission
EVS	Eesti Standardikeskus
NCS	National Communication System
CPNI	Centre for the Protection of National Infrastructure
NIST	National Institute of Standards and Technology
CSSP	Control Systems Security Program
TISN	The Trusted Information Sharing Network
ENISA	European Network and Information Security Agency
RT	Riigi Teataja
IP	internet protocol
TCP	transmission control protocol
VOIP	voice over internet protocol
VPN	virtual private network
RTU	remote terminal unit
PLC	programmable logic controller
IED	intelligent electronic device
HMI	human-machine interface
ICS	industrial control systems
LAN	local area network
WAN	wide area network
ISA	International Society of Automation

COBIT	control objectives for information and related technology
ISACA	Information Systems Audit and Control Association
CERT	Computer Emergency Response Team
UPS	uninterruptible power supply
IDS	intrusion detection system
IPS	intrusion prevention system