US-CCU küberturbe kontroll-küsimustik

Autorid

John Bumgarner ja Scott Borg

Tõlgitud Riigi Infosüsteemide Arenduskeskuse tellimusel.

LÕPPVERSIOON

2007

Käesolev küberturbe kontroll-küsimustik on avalikustatud tasuta, kuid on siiski autoriõigusega kaitstud ning seda ei või müüa ega edasi müüa üheski muus vormis ilma kasumit mittetaotleva uurimisinstituudi U.S. Cyber Consequences Uniti sõnaselge loata.

Selle dokumendi kasutajad peaksid meeles pidama, et ükski küberturbe kontroll-küsimustik ei ole täiuslik ning selles loetletud turvameetmetest on põhimõtteliselt võimalik mööda minna. U.S. Cyber Consequences Unit ei võta vastutust selle kontroll-küsimustiku rakendamise tagajärgede ega ka selles sisalduda võivate vigade eest.

U.S. Cyber Consequences Unit kavatseb seda loendit igal aastal uuendada. Teretulnud on soovitused paranduste tegemiseks ning need tuleks saata aadressil checklist_comments@usccu.us.

Autorid on väga tänulikud kõigile neile, kes jagasid oma soovitusi pärast varasema kavandi lugemist.

US-CCU KÜBERTURBE KONTROLL-KÜSIMUSTIK

AUTORID JOHN BUMGARNER JA SCOTT BORG

Selles kontroll-küsimustikus on toodud põhjalik ülevaade meetmetest, mida ettevõtted ja teised organisatsioonid peaksid rakendama, et vähendada oma haavatavust küberrünnete suhtes. Loendi koostajad John Bumgarner, U.S. Cyber Consequences Uniti turbetehnoloogia teadusdirektor, ja Scott Borg, U.S. Cyber Consequences Uniti direktor, on selle loomisel lähtunud arvukatest reaalsetest küberturbe nõrkustest, mille nad on oma töö käigus avastanud. Kui loendi pikkus hakkas lähenema selle praegusele pikkusele, otsustasid koostajad heita pilgu ka varasematele küberturbe kontroll-küsimustikele, veendumaks, et uues loendis käsitletakse ka kõiki varasemates loendites kajastuvaid olulisemaid teemasid. Seejärel saadeti uue kontroll-küsimustiku kavand paljudele küberturbe ekspertidele, kes andsid selle kohta sadu kommentaare. Autorid lisasid kõik praktilisemat laadi ettepanekud ühte kõikehõlmavasse dokumenti ja püüdsid selle varal luua võimalikult tervikliku ülevaate kõigist olemasolevatest küberründekanalitest ja nende kaitsmiseks vajalikest meetmetest.

Selleks, et muuta kontroll-küsimustiku ülesehitus võimalikult selgeks ja mõistetavaks, on nõrkused ja meetmed jagatud kuue infosüsteemi komponendi järgi rühmadesse:
1) riistvara, 2) tarkvara, 3) võrgud, 4) automatiseerimine, 5) inimesed ja 6) tarnijad.

Nende rühmade selgitamiseks tuleks täpsustada veel paari aspekti. Tarkvara nõrkused on õigupoolest tarkvara nõrgad kohad sellesse *pääsu* mõttes, sest turvaohu tekkimiseks peab keegi püüdma tarkvarale pärast selle valmistamist, verifitseerimist ja paigaldamist ligi pääsema. Tarkvara tarne nõrkust tuleb käsitleda ühena infosüsteemi nõrkadest kohtadest, kuna tarkvara tarnijad suhtlevad infosüsteemidega regulaarselt veel tükk aega pärast tarkvara müümist või litsentseerimist. Muud tüüpi tarnijaid ei ole üldjuhul vaja pidada infosüsteemi nõrkuseks, kuna nad ei osale hiljem infosüsteemis toimuvates operatsioonides. Automatiseerimisega seotud nõrkade kohtade hulka ei kuulu mitte ainult füüsilisi ja infoprotsesse vahendavad süsteemid, vaid ka *mis tahes* automaatsed protsessid, mille tulemiks on tegelikud tooted. Kuna peaaegu iga infosüsteemi töö tulemusel tekib vähemalt üks tegelik toode, iseenda varundusmeedium, on automatiseerimisega seotud nõrkused olulised mitte ainult tööstuste, vaid ka kõigi infosüsteemide seisukohalt.

Iga peamine valdkond, milles võivad toimuda küberründed, on jaotatud omakorda kaheks või enamaks ründekanaliks. Need kitsamad ründekanalid on rühmitatud tegevuste

järgi, mida on vaja teha või jälgida infosüsteemi vastavate komponentide turvalisuse säilitamiseks. Kokkuvõttes määratleti kuusteist ründekanalit, mis on toodud alljärgnevas tabelis.

ÜLEVAADE PEAMISTEST KÜBERRÜNDE KANALITEST
Esimene valdkond: riistvara nõrkused
1. kanal. Füüsilised seadmed
2. kanal. Füüsiline keskkond
3. kanal. Füüsilised kaassaadused
Teine valdkond: tarkvara ligipääsu nõrkused
4. kanal. Identsuse autentimine
5. kanal. Rakenduse privileegid
6. kanal. Sisendandmete õigsuse kontroll
7. kanal. Sobivad käitumismustrid
Kolmas valdkond: võrgu nõrkused
8. kanal. Püsivõrguühendused
9. kanal. Katkestatavad võrguühendused
10. kanal. Võrgu hooldus
Neljas valdkond: automatiseerimisega seotud nõrkused
11. kanal. Kaugseireandurid ja juhtimissüsteemid
12. kanal. Varundusprotseduurid
Viies valdkond: inimkasutaja nõrkused
13. kanal. Turvaprotseduuride täitmine inimeste poolt
14. kanal. Turvalisust ohustavad tahtlikud teod
Kuues valdkond: tarkvara tarnija nõrkused
15. kanal. Tarkvaraarenduse sisepoliitikad
16. kanal. Ettevõtteväliste tarnijatega suhtlemise poliitika

Eeltoodud kuueteistkümne kanali juurde on toodud pealkirjad, mille alla on rühmitatud vastavate ründekanalite kaitsmiseks rakendatavad vastumeetmed. Kõiki kontroll-küsimustikus käsitletavaid eri nõrkusi kirjeldatakse nende kõrvaldamiseks või minimeerimiseks vajalike vastumeetmete kaudu. Loend on koostatud küsimuste vormis, kuna jah-vastus võimaldab loendi järgi kontrollijal kiiresti kindlaks teha, et on rakendatud asjakohaseid meetmeid. Mõned küsimused võivad sisaldada ebamäärasena tunduvaid sõnu nagu 'range', 'täpne, 'küllaldane', 'piisav', kuid tegelikult on neil konkreetses kontekstides üsna täpne tähendus. Enamikel juhtudel on nende mõistete täpseks tõlgendamiseks lihtsalt vaja küsida „Mis on selle meetme eesmärk?“ ja siis teha kindlaks, kas sellest meetmest piisab selle eesmärgi saavutamiseks.

Autorid on püüdnud igati vältida moesõnade ja eriala žargooni kasutamist. Selle asemel on püütud kogu teave edasi anda võimalikult lihtsalt, selgelt ja sisutihedalt. Kõik hetkel moesõnade järgi tuntud küberturbe teemad on siin olemas, kuid moesõnu endid siit ei leia.

Kontroll-küsimustikust on teadlikult välja jäetud paljud ettevõttepoliitika ja verifitseerimisega seotud küsimused, kuna nende aspektidega tegelemine peaks tavaliselt olema iseenesest mõistetav. *Iga* kontroll-küsimustikus toodud turvameede peaks kajastuma poliitikas. *Iga* kontroll-küsimustikus toodud turvameedet tuleb mingil viisil verifitseerida. Eesmärk on tagada kontroll-küsimustikus toodud turvameetmete tegelik rakendamine. Poliitikad ja verifitseerimine on vaid nende rakendamist toetavad vahendid. Kui kontroll-küsimustikus on sõnaselgelt kasutatud termineid 'ettevõttepoliitika' ja 'verifitseerimine', tuleb selles valdkonnas võtta tarvitusele erimeetmed. Üldjuhul aga kätkevad hea juhtimise põhimõtted juba iseenesest vajalikke poliitikaid ja verifitseerimist.

Kontroll-küsimustikust on enamjaolt välja jäetud ka tõhusa küberturbe kindlustamiseks vajalikud organisatsioonilised ja haldussüsteemid, kuna nende süsteemide varal määratletakse rollide, vastutuse ja ergutuste efektiivne jaotus ja käsuliinid, mis kõik kuuluvad mitte küberturbe, vaid üldjuhtimise valdkonda. Mõned küberturbe poliitikate haldusega seotud põhimõtted ja juhised on toodud teistes U.S. Cyber Consequences Uniti koostatud dokumentides. Kuid tegelikult saab samu küberturbe meetmeid rakendada paljude erinevate haldussüsteemide varal.

Dokumendis küll kasutatakse korduvalt termineid 'ettevõtted' ja 'äritegevus', kuid neid tuleb vaadelda väga laias tähenduses. Küberturbe mõistes võib ettevõtteks pidada iga organisatsiooni, millel on oma eelarve ja infosüsteemid ning mis püüab tegeleda praktiliste tegevustega. Nende hulka kuuluvad ministeeriumid ja riigiasutused, mittetulundusühingud ja ka enamik vabaühendusi. Äritegevus, millega need organisatsioonid tegelevad, võib olla mis tahes tegevus, millega luuakse või edastatakse

mingit väärtust, olenemata sellest, kas seda väärtust hinnatakse või kirjeldatakse rahas. Valik termini 'ettevõtted' kasuks langes lihtsalt seetõttu, et enamike riigi infosüsteemide omanikeks on ja neid haldavad ettevõtted.

Paljud ettevõtted kindlasti avastavad, et mitte kõik kontroll-küsimustikus sisalduvad küsimused ei käi nende infosüsteemide kohta. Näiteks, mõned ettevõtted ei hakka kasutama selliseid kaugseireandureid ja juhtimissüsteeme, millele keskendutakse 11. kanali alla koondatud küsimustes. Mõned ettevõtted võivad jällegi leida, et neil ei ole praktiline pidada füüsiliselt eraldi paiknevaid andmekeskusi, mida on paljudes küsimustes mainitud. Nii mõnedki ettevõtted avastavad, et neil ei ole nii väga kriitilisi süsteeme, mis õigustaksid kontroll-küsimustikus kirjeldatud kõige keerukamate turvameetmete kasutamist. Enne mingi küsimuse rakendamatuks kuulutamist peaks ettevõte siiski veenduma, et see ei osutaks märkamata jäänud nõrgale kohale. Infosüsteemi omadused, mis ei ole konkreetses tegevusharus ilmselged, võivad siiski osutada selles valdkonnas esinevale suurele turvanõrkusele.

Tärniga (*) tähistatud vastumeetmeid on praegu koos tavatarnijatelt saadavate toodete ja tehnikaga väga keeruline või kallis rakendada. See tähendab, et vähemalt hetkel on nende rakendamiseks vaja eraldi lahendust, alates olemasolevast riistvarast ja lõpetades eritellimusprogrammidega. Turvalahenduste tarnijad, riigiasutused ja institutsioonid, mis rahastavad turvauuringuid ja -arendust peaksid eriti tähelepanu pöörama tärniga tähistatud küsimustele. Need on kõik valdkonnad, kus infoturbe parandamiseks on vaja kiiresti uusi tooteomadusi või teenuseid.

Nendel juhtudel, kui seda US-CCU kontroll-küsimustikku kasutatakse infoturbe vastavuse kontrollimise standardina, tuleb tärniga tähistatud küsimusi käsitleda valikulisena. Tulevaste kuude ja aastate jooksul, kui hakatakse pakkuma uut tehnikat, uusi tooteid ja teenuseid ning kontroll-küsimustikku uuendatakse perioodiliselt, kaovad kahtlemata paljud neist tärnidest ning praegu valikulised nõuded muutuvad ajapikku turvalahenduste standardiks. Vahepeal ei ole mõttekas eeldada, et ettevõtted tegeleksid turbeküsimustega, millele ei pakuta tavapäraseid standardlahendusi, kuigi need küsimused võivad olla väga olulised.

Võib tunduda, et mõnda tärniga *tähistamata* kontroll-küsimustiku küsimust on keeruline või kallis rakendada, kuid enamikel juhtudel see ainult tundub nii. On tõsi, et nende nõrkade kohtade kaitsmiseks on olemas mõned väga kallid meetodid ning pakutakse mõnda väga kallist toodet. Kuid peagu kõikide tärniga tähistamata küsimuste puhul on olemas suhteliselt odavad viisid, kuidas neid turvanõudeid täita.

Kui küberturvet käsitleda riskikolmnurgana, mille kolm nurka on ohud, tagajärjed ja nõrkused, siis see kontroll-küsimustik käsitleb ainult nõrkusi. Kontroll-küsimustiku tõhusaks kasutamiseks on vaja arvesse võtta ka riskikolmnurga *ülejäänud* nurgad. See

tähendab ohtude piisavalt head tundmist, et teada, milliseid ründeid võib mingil hetkel oodata. Kuid mis veelgi olulisem, see tähendab ka tagajärgede piisavalt head tundmist, et otsustada, kui kriitilised on mitmesugused tarkvararakendused, kui salajane on eri liiki teave ning millised kulutused turbele on nende kaitsmiseks õigustatud. Kuigi need teemad jäävad küberturbe kontroll-küsimustikust välja, selgitatakse neid Scott Borgi tulevases raamatupikkuses aruandes "*Küberrünnakud. Käsiraamat majanduslike ja strateegiliste riskide mõistmiseks" ("Cyber-Attacks: A Handbook for Understanding the Economic and Strategic Risks")*.

See US-CCU küberturbe kontroll-küsimustik *ei ole* mõeldud asendama kõiki varasemaid nõrkuste kontroll-küsimustikke ning see ei muuda teisi loendeid ebavajalikeks. Tegelikult on hoopis nii, et selle üldloendi kasutamiseks on tavaliselt vaja rakendada lisaloendeid, eriloendeid, mis sisaldavad palju täpsustusi spetsiifiliste turbeprobleemide, uusimate tehniliste arenduste ja konkreetsete tegevusharude erinõuete kohta. Loodetavasti aitab käesolev US-CCU loend juhtida siiski tähelepanu paljudele nõrkadele kohtadele, mis muidu võiksid jääda märkamata.

Esimene valdkond. Riistvara nõrkused

1. kanal. Füüsilised seadmed

Füüsiliste seadmete jälgimine

1.01. Kas ettevõte peab igas ruumis ja igas konkreetses füüsilises asukohas asuvate elektroonikaseadmete varaloendit ja täpset arvestust nende üle?

1.02. Kas seda varaloendit saab kiiresti ja kergesti uuendada, kui seadme eest vastutav töötaja lubab selle teise kohta viia?

1.03. Kas igal elektroonikaseadmel on vöötkoodiga silt või mõni muu identifikaator selle lihtsaks tuvastamiseks?

1.04. Kui infoseade on piisavalt salajane, kas see on siis varustatud raadioidentimise (RFID) kiipidega, et seadme liikumist saaks jälgida peaaegu reaalajas? *

1.05. Kas on kehtestatud üksikasjalik poliitika selle kohta, milliseid seadmeid võib ettevõtte territooriumilt välja viia ja milliseid lubasid on vaja seadme ümberpaigutamiseks?

1.06. Kui elektroonikaseadet on vaja ettevõtte territooriumilt välja viia, kas on olemas tõhus viis selle seadme liikumise jälgimiseks?

1.07. Kas korraldatakse ettehoiatamata kontrollkäike, et veenduda elektroonikaseadmete olemasolus seadmete loendis registreeritud asukohtades?

Füüsiliste seadmete kaitsmine

1.08. Kas eriti olulised elektroonikaseadmed on koondatud andmekeskustesse nende lihtsamaks kaitsmiseks?

1.09. Kas rakendatakse füüsilisi turvatõkkeid elektroonikaseadmete kaitsmiseks varguse või pahatahtliku rikkumise eest?

1.10. Kui välised kõvakettad ja muud välised andmekandjad, mida on lihtne kaasa võtta, sisaldavad salajast teavet, kas need on siis lisameetmena ankurdatud? *

1.11. Kas juhtmekapid on kogu aeg kindlalt lukustatud?

1.12. Kas andmekeskus ja juhtmekapid on varustatud sissetungivastase alarmiga?

1.13. Kas andmekeskuse ja juhtmekappide sissetungivastast alarmi jälgitakse väljapoolt asukohta?

1.14. Kas ainult volitatud kasutajad pääsevad füüsiliselt ligi turvaseadmete konsooli liidestele, nagu näiteks nendele, millega hallatakse tulemüüre ja sissetungi tuvastamise süsteeme?

1.15. Kas andmekeskuste ja muude alade, milles on kriitilisi andmeid sisaldavad seadmed, ripplaed ja tõstetud põrandad on turvatud selliselt, et sinna ei pääseks kõrvalasuvatelt aladelt ja ventilatsioonisüsteemidest?

Elektroonsete pääsuportide kaitsmine

1.16. Kas kasutamata võrgupordid on füüsiliselt blokeeritud võrgukommutaatorite või füüsiliste turvatõketega, mis hoiavad ära volitamata juurdepääsu?

1.17. Kui võrgupordid ei ole tegelikult blokeeritud, kas on kehtestatud protseduurid nendele portidele volitamata juurdepääsu jälgimiseks?

1.18. Kas on olemas füüsilised turvatõkked nagu lukustatud katted või pistikud, mis on paigaldatud selleks, et kaitsta kõiki süsteemi meediumite pääsupunkte (nt USB-pordid, CD-draivid jne)? *

1.19. Kui meediumipordid ei ole tegelikult blokeeritud, kas on kehtestatud protseduurid nende volitamata juurdepääsu jälgimiseks? *

1.20. Kas füüsiline pääs kõigi võrgukommutaatorite kasutamata portide, eriti SPAN *(Switched Port Analyzer)* -porti, on blokeeritud?

1.21. Kas on takistatud füüsiline pääs kõigi ruuterite konsooli ja lisaportide juurde?

Sideliinide kaitsmine

1.22. Kas on paigaldatud füüsilised turvatõkked, et kaitsta süsteemi sisenevaid ja sealt väljuvaid võrgukaableid, et neid ei oleks lihtne katkestada ega vigastada?

1.23. Kas kriitilised sidekaablid ja kaablikimbud on ettevõtte ruumides paigaldatud nii, et nende juurde on edastuse pealtkuulamiseks füüsiliselt raske pääseda?
1.24. Kas koht, kus telefoni- ja andmekaablid sisenevad ehitisse, on füüsiliselt kaitstud?
1.25. Kas ettevõtte uurib, milliseid füüsilisi turvameetmeid internetiteenuse pakkujad ja muud sideettevõtted rakendavad, enne kui ta otsustab, millisest ettevõttest teenust osta?

Seadmete juurde füüsilise pääsu reguleerimine

1.26. Kas andmekeskus on kogu aeg kindlalt lukustatud ning uksed sissepääsukohtades suletud?
1.27. Kas andmekeskuse ustel on silt “Sisenemine keelatud”?
1.28. Kas sissepääsu andmekeskusesse reguleeritakse meetoditega nagu skännitavad töötõendid, kiipkaardid, lähitoimekaardid, biomeetrilised andmed või lukud, mis avanevad personaalse kombinatsiooni sisestamisel?
1.29. Kas pääsu reguleerimise seadmete logisid (nt ligipääsukaartide ja videojälgimise logisid) vaadatakse korrapäraselt läbi?
1.30. Kas sellise läbivaatamise käigus analüüsitakse ka ebaõnnestunud füüsilise sissepääsu katseid?
1.31. Kas andmekeskuste ja muude infotöötlusseadmetega varustatud alade sissepääsude jälgimiseks kasutatakse videojälgimist?
1.32. Kui andmekeskustes kasutatakse videojälgimist, kas siis jälgimine toimub väljapool asukohta?
1.33. Kui andmekeskustes kasutatakse videojälgimist, kas video salvestatakse püsikandjale, mida ei saa võltsimise eesmärgil muuta?
1.34. Kui andmekeskustes kasutatakse videojälgimist, kas videosalvestisi hoitakse alles piisavalt kaua, et oleks võimalik tagantjärele uurida turvanõuete rikkumist, mida ei avastatud mitme kuu jooksul?
1.35. Kui jälgimiseks kasutatakse turvakaameraid, eriti juhtmeta kaameraid, kas need on kaitstud häirimise, volitamata läbivaatamise ja kujutiste võltsimise eest? *
1.36. Kas ainult volitatud kasutajad pääsevad turvakomponentide nagu tulemüüride ja IDS-i juhtimispultide juurde?
1.37. Kas reguleeritakse ja jälgitakse füüsilist juurdepääsu kõigi juhtmeta ja infrapuna üleslinkide juurde?
1.38. Kas faksimasinad, mis võtavad vastu ja millega prinditakse salajast teavet, on kaitstud volitamata juurdepääsu eest?

Töötajate füüsilise juurdepääsu reguleerimine

1.39. Kas on olemas vahendid, millega kontrollitakse, kes siseneb ruumi ja väljub ruumist, kus infosüsteemid füüsiliselt asuvad?

1.40. Kas on kehtestatud selged piirangud, kes töötajatest võivad siseneda andmekeskusesse, ning kas neid piiranguid rakendatakse täpselt?

1.41. Kas on kehtestatud selged eeskirjad juhtmekappidele juurdepääsu kohta ning kas neid kontrollitakse rangelt?

1.42. Kas töötaja rolli muutumisel kontrollitakse rangelt seda, et ka tema füüsilise juurdepääsu õigusi muudetaks?

1.43. Kas füüsilise juurdepääsu õigused ja vahendid nagu töötõendid deaktiveeritakse kohe, kui töötaja vabastatakse töölt või ta lahkub töölt või läheb pensionile?

1.44. Kas tarnijate pääsu andmekeskusesse kontrollitakse rangelt nii, et sinna lubatakse ainult nõuetekohaselt volitatud tarnija töötajaid?

1.45. Kas võõrad isikud peavad andmekeskusesse sisenemisel ennast registreerima keelualale sisenemise loa saamiseks?

1.46. Kas tarnijatele antud füüsilise juurdepääsu õigusi ja vahendeid vaadatakse sageli läbi ning need deaktiveeritakse kohe, kui tarnija töötajad vahetuvad?

1.47. Kas on kehtestatud ranged poliitikad, milles sisalduvad protseduurid selle kohta, kuidas töötajad, näiteks valvurid, peavad sisenema andmekeskusesse pärast tööaega?

1.48. Kas ettevõtte turvapoliitikates on ette nähtud, kuidas tuleb siseneda andmekeskusesse avarii korral?

2. kanal. Füüsiline keskkond

Keskkonnatingimuste reguleerimine

2.01. Kas on olemas ruumide keskkonnatingimuste reguleerimise seadmed, näiteks kütte- ja jahutussüsteemid, mis suudavad hoida elektroonikaseadmete töötamise tagamiseks püsivat temperatuuri?

2.02. Kas elektroonikaseadmed on kaitstud niiskuse või liigniiskuse eest?

2.03. Kui ruumi keskkonnatingimuste reguleerimise seadmed on kaugjuhitavad, kas siis need juhtseadmed on piisavalt kaitstud volitamata juurdepääsu eest?

2.04. Kas on olemas ruumi keskkonnatingimusi reguleerivad seadmed, mis suudavad kaitsta süsteemi peale temperatuuri ja niiskuse ka muude tegurite nagu suits, tolm ja kemikaaliaurud eest?

2.05. Kas andmekeskuses ja juhtmestikukappides on olemas keskkonnatingimuste mõõtmise andurid, eriti temperatuuri-, suitsu- ja niiskusandurid?

2.06. Kas ruumid, kus hoitakse elektroonikaseadmeid, on varustatud tulekahju tõrjesüsteemiga, mida sobib kasutada elektriseadmete korral?
2.07. Kas elektroonikaseadmeid täis ruumide kõrval asuvatel aladel on tulekahju tekkimist ärahoidvad tulekahju tõrjesüsteemid?

Elektrivarustus

2.08. Kas elektrisüsteemi avariilülititel on selgelt nähtavad sildid, nende kontrollimiseks kasutatakse videojälgimist ja neid kaitsevad kaitsekilbid, et ei saaks tekkida ebasobivat elektrivarustuse katkestust?
2.09. Kas on olemas füüsilised turvatõkked, et kaitsta andmekeskuse lähedal paiknevaid ühenduskaableid nii, et neid ei saaks lihtsalt katki teha ega vigastada?
2.10. Kas on rakendatud meetmeid selleks, et andmekeskusest kaugemal asuvad ühenduskaablid ei läbiks kergesti tuvastatavalt ebaturvalisi kohti?
2.11. Kas elektrivarustussüsteemi komponendid nagu elektripaneelid ja kaitselülitikarbid on kaitstud volitamata juurdepääsu eest?
2.12. Kui kasutatakse puhvertoiteallikaid (UPS-e), siis kas need on kaitstud volitatud kaugligipääsu eest?
2.13. Kui süsteemid on piisavalt kriitilised, siis kas need on ühendatud elektrivarustussüsteemi kahte eri ühenduse marsruuti pidi?
2.14. Kas reservgeneraatorid on kaitstud kaitsevahenditega nagu lukud, alarmid ja okastraataiad?
2.15. Kas on tagatud piisav reservelektrivarustus ja seda eriti igale ettevõtte üldiseks edasiseks püsimiseks vajalikule kriitilisele süsteemile?
2.16. Kas reservelektrivarustuse süsteemi jaoks on olemas piisav kütusetagavara ka juhuks, kui kütusetarneahel ei toimi suhteliselt pikka aega?
2.17. Kas reservelektrivarustuse süsteemi katsetatakse korrapäraselt täiskoormusel ning lastakse sellel töötada piisavalt pikka aega, et kontrollida kõigi selle osade töökorras olekut?
2.18. Kas reservelektrivarustuse süsteem asub kohas, kus ei teki kergesti üleujutust?
2.19. Kas on olemas kaitse tugevate elektrilöökide vastu, mida võib tekitada välk või mille võib ka kunstlikult esile kutsuda?

Füüsiline kaitse

2.20. Kas kriitilised arvuti- ja sideseadmete ruumid on piisavalt kaugel kohtadest, kus võivad eriti kergesti tekkida ohtlikud tulekahjud, plahvatused ja ohtlike ainete lekked?

2.21. Kas kriitilised arvuti- ja sideseadmete ruumid asuvad piisavalt kaugel avalikest parkimiskohtadest, tänavatest ja muudest kohtadest, kus saab kergesti pommi detoneerima panna?
2.22. Kas kriitilised arvuti- ja sideseadmed asuvad eemal tavalistest akendest, kust võidakse sisse visata või heita pomme, tulistada relvadest ja mikrolainerelvadest?
2.23. Kas reservgeneraatorid asuvad piisavalt kaugel avalikest parkimiskohtadest, tänavatest ja muudest kohtadest, kus saab kergesti pommi detoneerima panna?
2.24. Kui elektroonsed süsteemid on piisavalt kriitilised ning piisavalt tähtsad sihtmärgid, kas nende ümber on mingi metallkaitse, mis aitaks kaitsta mittetuuma elektromagnetimpulss-rünnete eest? *
2.25. Kas on olemas turvaline tarnimis- ja laadimisala, mis paikneb füüsiliselt eraldi andmekeskusest nii, et seadmete lisamisel või asendamisel ei tekiks võimalust volitamata juurdepääsuks ega lõhkeseadeldiste paigaldamiseks?
2.26. Kas elektroonikaseadmed ja muud vahendid kontrollitakse füüsiliselt üle enne nende viimist andmekeskusesse veendumaks, et nendega ei ole manipuleeritud?

3. kanal. Füüsilised kaassaadused

3.01. Kas salajast teavet sisaldavate dokumentide printimine on takistatud, kui neid dokumente ei ole vaja töö tegemiseks printida? *
3.02. Kas on kehtestatud piisavalt täpsed protseduurid, et piirata volitamata pääsu salajase teabega paberväljatrükkide juurde?
3.03. Kas ettevõtte turvapoliitikad määratlevad hoiustamisvahendite tüübi, mida võib kasutada salajase teabega paberväljatrükkide hoidmiseks?
3.04. Kas on kehtestatud piisavalt täpsed protseduurid paberväljatrükkide turvaliseks hävitamiseks?
3.05. Kas on piisavalt hoolitsetud selle eest, et korduskasutamise ja ringlussevõtu programmid ei ohustaks paberväljatrükkide turvalist käsitsemist?
3.06. Kas on kehtestatud piisavalt täpsed poliitikad ja protseduurid, mis reguleerivad kaasaskantavate magnetkandjate nagu näiteks universaalse jadasiiniseadme (USB-seadme) kasutamist?
3.07. Kas on kehtestatud piisavalt täpsed protseduurid, mis piiravad volitamata pääsu varundusmeediumite juurde?
3.08. Kas on olemas piisavalt täpsed protseduurid salajast teavet sisaldavate CD-ROM-ide ja kaasaskantavate magnetkandjate korralikuks inventeerimiseks?
3.09. Kas on olemas protseduurid andmekandjate loendist esemete eemaldamise registreerimiseks, mille kohaselt vastutavad töötajad kõigepealt kinnitavad, et

meediumid on äraviskamiseks eemaldatud, teiseks seda, et need on korralikult hävitatud või puhastatud ning kolmandaks, et füüsilised jäänused on ära visatud?

3.10. Kas on kehtestatud piisavalt ranged protseduurid iga sellise kaasaskantava andmekandja nõuetekohaseks transportimiseks, mida on vaja viia väljapoole asukohta?

3.11. Kas on olemas rutiinsed protseduurid, millega tagatakse, et salvestite nagu kõvakettad, lindid, välkmälu- ja *zip*-kettad on täielikult üle kirjutatud enne nende muuks otstarbeks kasutada andmist?

3.12. Kas on kehtestatud piisavalt täpsed protseduurid salvestite nagu kõvakettad, lindid, välkmälu- ja *zip*-kettad hävitamiseks või puhastamiseks, kui neid enam äritegevuse jaoks ei kasutata?

3.13. Kas on kehtestatud piisavalt täpsed protseduurid salvestite puhastamise kohta, mis saadetakse garantiiajal tagasi asendamiseks, mida müüakse avalikult või mis annetatakse heategevuseks?

3.14. Kas salajast teavet sisaldavad kasutatud CD-ROM-id hävitatakse nõuetekohaselt (mitte lihtsalt ei tehta katki) enne nende äraviskamist?

Teine valdkond. Tarkvara ligipääsu nõrkused

4. kanal. Identsuse autentimine

Autentimispoliitikad

4.01. Kas infosüsteeme kaitstakse tavapäraste autentimismehhanismidega nagu näiteks kasutajanimi ja parool?

4.02. Kas iga kasutaja juurdepääs süsteemi rakendustele piirdub ainult nende rakendustega, mis on sellele kasutajale vajalikud ja mis on talle omistatud?

4.03. Kui rakendus võimaldab juurdepääsu salajasele teabele, kas siis selle pääsu saamiseks peab kasutaja ennast veel kord autentima?

4.04. Kui rakendus on piisavalt kriitilise tähtsusega või teave piisavalt salajane, kas siis süsteem kasutab täiuslikemaid autentimismehhanisme nagu biomeetria, kahefaktorilisi lubakaarte *(two-factor tokens)* või väljakutsesuhtlust (*challenge exchange*)?

4.05. Kas terminalid ja tarkvarasüsteemid on seatud kasutajat välja logima ja uut sisselogimist nõudma mingi passiivse perioodi järel või kui mingi muu seade näitab, et töötaja on terminali juurest lahkunud?

4.06. Kui kriitilisele süsteemile pääseb ligi kaugelt ühe või rohkem kui ühe mainitud autentimismehhanismiga, siis kas ühendus ise on püsiühendus või krüpteeritud?

4.07. Kui pääsumehhanismina kasutatakse täiuslikumat autentimist, kas seda kasutatakse järjekindlalt ja tõhusalt kogu ettevõttes?
4.08. Kas on olemas protseduur kaheastmeliste lubakaartide ja kiipkaartide privileegide tühistamiseks, kui nende turvalisus on ohtu seatud?
4.09. Kas on olemas häiremehhanism, mis saadab signaali, kui tehakse katse kasutada kaheastmelist lubakaarti või kiipkaarti pärast selle tühistamist? *
4.10. Kui kasutatakse biomeetrilisi andmeid, kas siis identiteedi tõendamiseks on vaja ka PIN-i?
4.11. Kui kasutatakse biomeetrilisi andmeid, kas siis rakendatakse reaalajas skaneerimist või kasutatakse muid meetmeid, millega kinnitatakse andmete saamist elavalt inimeselt? *
4.12. Kas vajaduse korral on ettevõttel viis, kuidas pääseda ligi andmetele ja rakendustele, mida tavaliselt kaitstakse personaalse kaheastmelise autentimismehhanismiga nagu näiteks biomeetriline autentimine? *

Pääsu ja pääsukatsete jälgimine

4.13. Kas ettevõtte eeskirjad näevad ette, et kõik pääsukatsed tuleb logida, hoolimata sellest, kas need õnnestusid või mitte, eriti selliste rakenduste korral, mis täidavad kriitilisi funktsioone või säilitavad salajast teavet?
4.14. Kas kõiki süsteemiadministraatori poolt paroolidesse tehtud muudatusi logitakse ja kontrollitakse?
4.15. Kas kõiki pääsuprivileegide laiendamisi logitakse ja kontrollitakse?
4.16. Kas on olemas häiremehhanism, mis hoiataks, kui kasutatakse üldist juur- või administraatoritasandi (nt domeeniadministraatori) kontot?
4.17. Kas kõik pääsulogid kirjutatakse ülekirjutamiskaitsega kettale või muule püsikandjale, kus ka süsteemiadministraator ei saa neid muuta? *
4.18. Kas õnnestunud autentimisi kontrollitakse veendumaks, et antud pääs oli õige ja asjakohane?
4.19. Kas on tehtud jõupingutusi selleks, et välja selgitada ja uurida õnnestunud pääsukatseid, mis on toimunud ebaharilikul ajal päeval või öösel?
4.20. Kas mitmeid rakendusse pääsemise ebaõnnestunud katseid kontrollitakse kiiresti?
4.21. Kas on kavandatud automaatsed alarmid ja kaitsemeetmed kaitseks jõurünnete *(brute force attacks)* eest, mis on suunatud sisselogimismehhanismide vastu ja mille käivitavad mitmekordsed sisselogimiskatsed, isegi kui need on toimunud pikema aja jooksul või mitmete kasutaja-ID-dega?

Paroolide ja biomeetriliste andmete haldamine

4.22. Kas ettevõtte poliitikates on ette nähtud turvalised paroolide väljastamise protseduurid?

4.23. Kas ettevõtte poliitikates on määratletud nõutav parooli lühim pikkus, võttes arvesse kasutaja rolli ning seda, millise pikkusega paroole kõnealused süsteemid toetavad?

4.24. Kas ettevõttes arendatavaid rakendusi kaitstakse paroolidega, millele on ette nähtud vähim ja suurim märkide arv?

4.25. Kas ettevõtte poliitikates on kehtestatud keeruka parooli valimise nõuded, millega nähakse ette erinevate märkide või selliste märkide kasutamist, mis on valitud suurest hulgast märkidest?

4.26. Kas on hoolt kantud selle eest, et paroole ei saadetaks edasi tekstina e-meili ega vahetu sõnumside teel?

4.27. Kas töötajad on kohustatud kehtiva ettevõtte poliitika järgi vahetama oma paroole korrapäraselt?

4.28. Kas töötajatel takistatakse paroolivahetuse korral eelmiste paroolide kasutamine?

4.29. Kas ettevõtte poliitikates on kehtestatud piisavad paroolinõuded võrguseadmete nagu ruuterite ja kommutaatorite kasutamisel?

4.30. Kas on rakendatud meetmeid välistamaks olukordi, kus keegi saab enda kätte paroolid, kui ta varastab krüpteeritud või krüpteerimata faili, kus neid hoitakse?

4.31. Kas on olemas häiremehhanism, mis hoiataks paroole sisaldava faili vargusest? *

4.32. Kas on kehtestatud protseduur paroolide kiireks ja turvaliseks vahetamiseks, kui on põhjust arvata, et nende turvalisus on ohtu seatud?

4.33. Kas ettevõtte turvapoliitikates on ette nähtud paroolide kohene deaktiveerimise, kui töötaja töösuhe lõpeb, ta lahkub töölt või läheb pensionile?

4.34. Kas serverite ja tööjaamade rakendusi auditeeritakse korrapäraselt, et välja selgitada kasutamata või endistele töötajatele määratud kontod ning tagada, et need kontod on eemaldatud või neile määratakse uued paroolid?

4.35. Kas on olemas range biomeetriliste identifikaatorite väljaselgitamise protsess, mis annab kindluse, et nii kogutud andmed pärinevad õigelt isikult?

4.36. Kui kasutaja biomeetrilised andmed on kogutud, kas neid hoitakse siis turvalises kohas, kus neid ei saa manipuleerida ega varastada?

4.37. Kas ettevõttel ja selle tarnijatel on olemas kava biomeetriliste andmete asendamiseks alternatiivsetega, kui nende andmete turvalisus on ohustatud? *

4.38. Kas ettevõtte poliitikates on kehtestatud protseduurid biomeetriliste andmete hävitamiseks, kui neid ei ole enam vaja?

Krüpteerimisvõtmete ja digisertifikaatide haldamine

4.39. Kas krüpteerimisvõtmed luuakse turvaliselt, kasutades selleks heakskiidetud meetodeid?

4.40 Kas dekrüpteerimise protseduurid aktiveeritakse eraldi sisselogimisest ning kas nõutakse selleks erinevaid paroole?

4.41. Kas krüpteerimisvõtmete genereerimist logitakse võltsimiskindlasse faili, mis registreerib töötaja genereeritava identiteedi ja aja?

4.42. Kas krüpteerimisvõtmeid ja digisertifikaate jagatakse turvalisel moel, mis välistab varguse?

4.43. Kas krüpteerimisvõtmeid hoitakse turvaliselt, kasutades tunnustatud meetodeid?

4.44. Kas krüpteerimisvõtmed hävitatakse turvalisel moel, kasutades tunnustatud meetodeid?

4.45. Kas on kehtestatud kiire ja tõhus protseduur, kuidas toimida kompromiteeritud krüpteerimisvõtmete korral?

4.46. Kas kehtivad rutiinsed ja usaldusväärsed protseduurid privaatvõtmete ja individuaalsete kasutajatega seotud pääsufraaside arhiveerimiseks?

4.47. Kui privaatvõtmeid hoitakse alles, kas need arhiveeritakse parooliga kaitstud ja krüpteeritud alal, et vältida nende manipuleerimist või vargust?

4.48. Kas privaatvõtmeid ja seotud pääsufraaside võtmeid hoitakse alles pärast seda, kui nad ei ole enam aktiivselt kasutuses, et vajaduse korral saaks varasemaid krüpteeritud faile taastada?

4.49. Kas ettevõtte poliitikates on kehtestatud protseduurid digisertifikaatidel põhinevate autentimismehhanismide juurutamiseks?

4.50. Kas digisertifikaatide privaatvõtmete koopiaid hoitakse parooliga kaitstud ja krüpteeritud alal, mis võimaldab nende taastamist ja kaitseb varguse eest?

4.51. Kas süsteemidel, millele on installitud sertifikaadid, rakendatakse piisavaid turvameetmeid, et ära hoida nende sertifikaatide privaatvõtmete vargust?

4.52. Kas on kehtestatud protseduur, mis võimaldab kiiresti tühistada kompromiteeritud digisertifikaatide privaatvõtmeid?

4.53. Kas krüpteerimisvõtmetel ja digisertifikaatidel on kehtivusaeg?

Dokumentide autentsuse haldamine

4.54. Kas dokumendid, kus kajastatakse ettevõtte tööd või positsioone, on konverteeritud raskesti muudetavasse vormingusse enne, kui neid hakatakse väljapool ettevõtet elektrooniliselt levitama?

4.55. Kas dokumendid digiallkirjastatakse, kui neid konverteeritakse vormingutesse, mis ei võimalda neid lihtsalt muuta?

4.56. Kas oluliste dokumentide digiallkirju kontrollitakse korrapäraselt veendumaks, et need dokumendid on ka tegelikult loonud isik, kes näib nende autorina?

4.57. Kas tähtsad e-kirjad saadetakse kasutades rakendust, mis teeb nende sisust räsi ja lisab digiallkirja nii, et e-kirjade sisu ja nende saatja identiteeti ei ole kerge võltsida?

4.58. Kas oluliste e-kirjade kättesaamise kohta kogutakse ja hoitakse alles andmeid, et oleksid olemas tõendid selle kohta, et need meilid jõudsid adressaatideni?

5. kanal. Rakenduse privileegid

Privileegide kohandamine

5.01. Kas tarkvara ja riistvara vaikimisi turvasätteid muudetakse enne nende kasutama hakkamist?

5.02. Kas ettevõte on ametlikult määranud oma olulisemate või laiemalt kasutatavate tarkvararakenduste turvaklassid?

5.03. Kas ettevõttes pääsevad ainult need kasutajad olulistesse rakendustesse, kellel on neid ka tegelikult vaja kasutada?

5.04. Kas ettevõte on ametlikult määranud oma infofailide salastatuse klassid?

5.05. Kas ettevõttes pääsevad salastatud andmete juurde ainult need kasutajad, kes neid andmeid ka tegelikult kasutama peavad?

5.06. Kas ainult neil töötajatel, kellel on oma tavapärase töö käigus vaja muuta dokumentides või andmebaasides andmeid või neid sinna sisestada, on luba seda teha?

5.07. Kas kasutaja saab moodustada salajase teabe väljundeid nagu näiteks väljaprinte ja e-kirja manuseid ainult selles ulatuses, mida tema töö ja kohustused nõuavad?

5.08. Kas juur- ja administraatoritasandi privileegid on antud ainult neile, kes neid tõesti vajavad?

5.09. Kas juur- ja administraatoritasandi privileegid on reguleeritud ja auditeeritud?

5.10. Kas kehtib dokumenteeritud heakskiidu andmise protseduur inimestele virtuaalsetesse privaatvõrkudesse pääsu võimaldamise kohta?

5.11. Kas kehtib dokumenteeritud heakskiidu andmise protseduur inimestele modemite kaugpöörduse õiguse andmise kohta?

5.12. Kas on olemas protseduur, mille kohaselt dokumenteeritakse ja jälgitakse missugused privileegid on iga töötaja jaoks aktiivsed?
5.13. Kas iga töötaja tarkvararakenduse privileegid vaadatakse uuesti üle ja korrigeeritakse, kui tema tööülesannetes on toimunud olulisi muudatusi?
5.14. Kas on olemas protseduur, mille kohaselt võetakse privileege ära ja kinnitatakse nende äravõtmine, kui neid ei ole enam vaja?

Privileegide üldine reguleerimine

5.15. Kas töötajatel takistatakse salajase teabe salvestamist kaasaskantavatele salvestitele nagu flopid, CD-ROM-id või USB-kettad, välja arvatud juhul, kui seda on äritegevuse pärast vaja? *
5.16. Kas jälgitakse rakendusi, et välja selgitada, kas salajast teavet on prinditud, salvestatud või alla laaditud ilma põhjendatud vajaduseta? *
5.17. Kas kohalikult säilitatavaid kriitiliste andmete faile hoitakse tavaliselt krüpteeritud vormis, kui neid ei kasutata? *
5.18. Kas volitatud kasutaja saab salajasi andmefaile lubamatul viisil üles või alla laadida süsteemist teise süsteemi?
5.19. Kas kõiki üleslaaditud salajasi andmefaile jälgitakse ja logitakse?
5.20. Kas kõiki üleslaaditud krüpteeritud andmefaile jälgitakse ja logitakse?
5.21. Kas on olemas meetmed, millega hoitakse ära volitatud kasutajate poolt täitmisfailide (.exe) allalaadimine oma süsteemi ilma neid faile enne pahavara suhtes skaneerimata?
5.22. Kui töötajad saavad salvestada salajast teavet kohalikule kettale, kas siis seda tegevust jälgitakse ja logitakse? *
5.23. Kas volitatud kasutaja pääseb pääsupiiranguga ressursside juurde teistes süsteemides lisaparoolideta ja/või IP-aadressi õigsust kontrollimata?
5.24. Kui rakendusteenust tuleb konkurentsi pärast kaitsta, kas siis see tehakse kättesaadavaks veebis ainult usaldusväärsetele töötajatele, mitte avalikkusele?

6. kanal. Sisendandmete õigsuse kontroll

6.01. Kas paroolivälјale sisestatavad märgid on maskeeritud nii, et kõrvalseisja ei saaks neid lugeda?
6.02. Kas on olemas programm, mis kontrollib paroole nende loomisel, et need vastaksid ettevõtte turvapoliitikates paroolidele ettenähtud nõuetele?
6.03. Kas kõigile rakenduse sisestusväljadele on seatud teatavate märkide ja avalduste piirangud? (nt isikukoodi numbriväli ei tohiks lubada sisestada midagi peale numbrite)

6.04. Kas kõik rakenduse sisestusväljad on piiratud asjakohase vähima ja suurima pikkusega? (nt isikukoodi numbriväli ei tohiks lubada sisestada rohkem kui üksteist numbrit)
6.05. Kas sisestusväljadele seatud piirangud on piisavad, et need ei aktsepteeriks täitmiskäske?
6.06. Kas andmebaasi andmeväljadele on seatud piirangud, mis vastavad kasutajaliidese väljade piirangutele, et ei oleks võimalik ebaõigeid andmeid ja täitmiskäske otse andmebaasi sisestada?
6.07. Kas andmeväljadele, mida on harva vaja muuta, seatakse kohe kirjutuskaitse, kui andmesisestus on verifitseeritud korrektsena?
6.08. Pärast seda, kui andmeväljale on seatud kirjutuskaitse, kas on olemas asjakohane protseduur, kuidas saaks välja eritingimustel parandada ja parandust verifitseerida?
6.09. Kas veateated on korralikult koostatud nii, et nad ei avaldaks infot tarkvara sisemise disaini ja konfiguratsiooni kohta?
6.10. Kas silumisfunktsioon on blokeeritud, et ei tekiks kanalit info hankimiseks tarkvara sisemise disaini ja konfiguratsiooni kohta?
6.11. Kas kriitiliste rakenduste teenuspordid on konfigureeritud filtreerima andmeid, mis ei vasta nende rakenduste ettenähtud talitlusparameetritele? *****
6.12. Kas kriitilistel rakendustel kasutatavatele teenusportidele on tehtud koormusteste tagamaks, et neil ei tekiks kergesti teenuspordi tasandil puhvri ületäitumist?
6.13. Kas kriitilisi protsesse juhtivatele sisenditele on eelnevalt määratud parameetrid, et nendele parameetritele mittevastavate sisestuste katsed kas blokeeritakse või nõutakse kinnitust teisest allikast? *****

7. kanal. Sobivad käitumismustrid

7.01. Kas on olemas häiremehhanism, mis hoiataks, kui töötajad sisestavad andmeid kogustes või jaotusega, mis ei ole kooskõlas töötajate tavapärase töömahuga? *****
7.02. Kas on olemas häiremehhanism, mis hoiataks, kui faile avatakse ebaharilikes kogustes või järjekorras, mis ei ole kooskõlas tavapärase tööga? *****
7.03. Kas on olemas häiremehhanism, mis hoiataks, kui internetis tehtavad äritehingud hõlmavad ebaharilikku kombinatsiooni kliendi identiteetidest ning arve- ja tarneaadressidest? *****
7.04. Kas on olemas rutiinsed protseduurid, kuidas kontrollida juhtimissüsteemide reguleerimisi ja muudatusi veendumaks, et muudatused, mis peaksid korreleeruma, ka korreleeruksid? *****

7.05. Kas on võetud samme, et välja selgitada ja uurida õnnestunud pääsukatseid, mis on toimunud ebaharilikul ajal päeval või öösel, kui arvutid võivad märkamatult teostada volitamata operatsioone? *
7.06. Kas on olemas mingeid meetmeid, et tuvastada valeandmete või -käskude sisestamise juhtumeid ilma avastamata sissetungita? *
7.07. Kas andmebaas on nii projekteeritud, et salajast teavet ei saa üle kirjutada ilma, et järgnevaid ajatempliga parandusi ei arhiveeritaks turvaliselt? *
7.08. Kas on olemas mehhanism kriitilistes andmebaasides kõigi muudatuste jälgimiseks ja logimiseks?
7.09. Kas kriitilistesse andmebaasidesse tehtavate muudatuste logi analüüsitakse korrapäraselt, et avastada ebatavalisi, sealhulgas ebatavalistel aegadel ja sagedusega tehtavaid pääsukatseid? *
7.10. Kui andmete muudatused logitakse, kas siis seda logi analüüsitakse korrapäraselt andmebaasides toimunud ebatavaliste muudatusmustrite suhtes? *
7.11. Kas süsteemi- ja turvalogisid hoitakse alles viisil, mis välistab nende muutmise või kustutamise pärast nende talletamist?
7.12. Kas süsteemis on nn. "meepotid" (*honey token*-id), mis koosnevad võltsdokumentidest või -kontodest ning nende jälgimismehhanismidest, et kindlaks teha kas ja millal nendele ligi pääseti? *
7.13. Kas on olemas automaatne protsess, mis otsiks süsteemides märke valeinfo sisestamise kohta? *
7.14. Kas on olemas automaatne mehhanism, mis paneb valeinfoga kompromiteeritud süsteemid karantiini ilma neid sulgemata? *

Kolmas valdkond. Võrgu nõrkused

8. kanal. Püsivõrguühendused

Võrguühenduse terviklus

8.01. Kas ka võrk ise on kaitstud autentimisprotseduuridega lisaks võrgus olevate süsteemide kaitsmisele?
8.02. Kas on rakendatud meetmeid, et ära hoida volitamata süsteemide lihtsat võrku ühendamist?
8.03. Kas võrguliiklust jälgitakse korrapäraselt, et välja selgitada tavapärane kasutus?
8.04. Kas võrguliiklust jälgitakse korrapäraselt varjatud kanalite avastamiseks?
8.05. Kas võrguseadmed on konfigureeritud nii, et need annaksid olulisemale liiklusele nagu protsessi juhtimise käskudele eesõiguse vähemtähtsa liikluse nagu e-kirjad ees?

8.06. Kas kriitilistel süsteemidel on varusideühendusi?
8.07. Kas väga kriitilistes võrkudes on varu võrgu kommuteerimisel (*switching fabric*)?
8.08. Kui salajast teavet edastatakse üle võrgu, võrku või võrgust välja, siis kas andmed on krüpteeritud kaitsmaks neid pealtkuulamise või muutmise eest?
8.09. Kas ettevõtte poliitikates on määratletud, millist liiki andmesidet tuleks krüpteerida ja milliseid krüpteerimistehnoloogiaid tuleks kasutada?
8.10. Kas partnervõrkudega turvalise side tagamiseks kasutatakse virtuaalseid privaatvõrgu ühendusi?
8.11. Kas väliste partnervõrkudega krüpteerimata võrguühendustele on kehtestatud turvanõuded?
8.12. Kas väga salajase sisuga juhtmega või juhtmeta IP-kõnede (VoIP) korral on edastus krüpteeritud?

Võrgukomponendi terviklus

8.13. Kas iga ruuter, kommutaator, server, tööjaam või mõni muu infoseade peab vastama minimaalsetele turvastandarditele enne selle võrku lülitamist?
8.14. Kas käivitamisel kontrollitakse automaatselt võrgutarkvara komponente turvakonfiguratsioonide muudatuste suhtes, mida on tehtud pärast süsteemi viimast käivitamist, ning kui leitakse tehtud muudatusi, kas siis süsteemiadministraatorit teavitatakse sellest automaatselt? *
8.15. Kas süsteeme, mis ei vaja laivõrguühendust, ei ühendata laivõrku?
8.16. Kas võrku kontrollitakse regulaarselt volitamata süsteemide suhtes?
8.17. Kui tarkvarapõhiseid IP-telefone kasutatakse salajaste andmete edastamiseks, kas need on turvalised kõne pealtkuulamisvahendite (*voice loggers*) eest? *
8.18. Kas on tehtud teste veendumaks, et kriitilisi süsteeme ei ole võimalik liiga kergesti rivist välja viia suurte andmehulkade või suure liikluse tõttu, mida võidakse kasutada näiteks teenuse tõkestamise ründe korral?
8.19. Kas on olemas mehhanism, millega automaatselt taaskäivitada kriitilisi komponente nagu näiteks veebiserveri rakendusi, kui teised rakendused ei suuda nendega korduvalt ühendust luua, ning teavitada süsteemioperaatorit, et seda tehti?
8.20. Kas kriitilised süsteemid kasutavad varu DNS servereid vähendamaks selle teenuse katkemise mõju, kui see pärineb ainult ühest allikast?
8.21. Kas rakendatakse meetmeid jälgimaks DNS servereid rünnete suhtes, mis suunavad päringuid ümber volitamata asukohtadesse?

8.22. Kas kriitilistele süsteemidele tehakse nõrkuste kontrolli *(vulnerability scans)* või läbistusteste *(penetration tests)* enne süsteemide ühendamist ettevõtte võrkudega?
8.23. Kas ettevõtte võrkudes tehakse kriitiliste süsteemide nõrkuste kontrolli *(vulnerability scans)* või läbistusteste *(penetration tests)* regulaarselt?
8.24. Kas nõrkuste kontrolli *(vulnerability scans)* või läbistusteste *(penetration tests)* tehakse kõikidele internetti ühendatavatesse või kliendi kasutatavates süsteemides ja rakendustest enne nende võrku ühendamist?
8.25. Kas tehakse regulaarselt nõrkuste kontrolli *(vulnerability scans)* või läbistusteste *(penetration tests)* internetti ühendatud või kliendi kasutatavates süsteemides ja rakendustest?

Traadita ühendused ja modemid

8.26. Kas kehtivad selged ja rangelt kehtestatud reeglid traadita ühenduste loomise ja kasutamise kohta sisevõrkudes?
8.27. Kas traadita side analüsaatorit kasutatakse regulaarselt, et välja selgitada kõik volitamata traadita seadmed, mis võivad olla võrku ühendatud?
8.28. Kas printeritel on blokeeritud traadita, infrapuna- ja Bluetooth-lingid, kui neid äritegevuse seisukohalt ei ole vaja?
8.29. Kui salajase teabe edastamiseks kasutatakse traadita tehnoloogiaid nagu näiteks traadita kohtvõrku (LAN), Bluetoothi või traadita USB-d, kas need ühendused kasutavad heatasemelisi krüpteerimismeetodeid?
8.30. Kas Bluetooth-seadmete vaike-PIN-id *(default PIN's)* muudetakse enne nende kasutama hakkamist?
8.31. Kas salajases võrgus traadita tehnoloogia kasutamisel on blokeeritud plinkimine *(beaconing)*, mis teavitab võrgu olemasolust?
8.32. Kas traadita võrgu tehnoloogia kasutamisel roteeritakse jagatud krüpteerimisvõtmeid regulaarselt?
8.33. Kas traadita võrgu tehnoloogia kasutamisel pääsevad ainult volitatud seadmed traadita võrku?
8.34. Kas ettevõtte poliitikates on kehtestatud protseduurid modemite paigaldamiseks ettevõtte infrastruktuuri?
8.35. Kas volitatud modemite kasutamisel rakendatakse turvameetmeid nagu tagasihelistuse ja kõneedastuse tuvastamine?
8.36. Kas ettevõttes korraldatakse regulaarselt nn. sõjavalimise (*war-dialing*) kampaaniaid, et avastada volitamata modemeid, mida saab kätte sissehelistades?

8.37. Kas ettevõtte telefonikeskjaamu kontrollitakse regulaarselt, et avastada väljapoolt tulevaid katseid leida sõjavalimise kampaaniatega volitamata modemeid?

Tulemüürid ja sissetungi tuvastuse ja tõrjumise süsteemid

8.38. Kas ettevõte on koostanud loendid nii sisse- kui ka väljapoole suunatud liikluse sihtkohtadest ja liiklusetüübist, mida ta soovib lubada läbi oma tulemüüride?

8.39. Kas ettevõte on konfigureerinud oma tulemüürid nii, et lubatakse ainult ettevõtte heakskiidetud loendites ettenähtud liiklust?

8.40. Kas ettevõttes kehtib kooskõlastamise protseduur, kui tahetakse muuta reeglistikku, mis määratleb läbi tulemüüride lubatava liikluse?

8.41. Kas ettevõttes on ette nähtud tulemüüridest läbi lubatava liikluse loendite korraline läbivaatamine nii, et loendites oleks arvesse võetud ettevõtte liikluse vajadustes toimunud muutusi?

8.42. Kas ettevõttes on ette nähtud korraline tulemüüride kontrollimine veendumaks, et reeglistikku on korralikult rakendatud ilma *ad hoc*-muudatusi tegemata?

8.43. Kas tulemüüride turvalogisid hoitakse alles viisil, mis välistab nende muutmise või kustutamise?

8.44. Kas tulemüüride turvalogisid vaadatakse korrapäraselt läbi volitamata liikluse tuvastamiseks?

8.45. Kas on juurutatud tulemüüre selleks, et kaitsta kriitilisi süsteeme volitamata pääsu eest ettevõtte oma töötajate poolt?

8.46. Kas ettevõtte säilitab oma ruuterite täielikke pääsuloendeid, sealhulgas kasutatud IP aadresse ja portide numbreid?

8.47. Kas ettevõttes on ette nähtud oma ruuterite regulaarne kontrollimine veendumaks, et pääsuloendeid on õigesti rakendatud?

8.48. Kas ettevõttes on ette nähtud ruuterite pääsuloendite regulaarne läbivaatamine, et saaks võtta arvesse ettevõtte liikluse vajaduste muutusi?

8.49. Kas võrgus kasutatakse sissetungi tuvastamise ja/või tõrjumise süsteeme?

8.50. Kas jälgitakse pidevalt sissetungi tuvastamise süsteemide turvahoiatusi?

8.51. Kas sissetungi tuvastamise ja tõrjumise süsteemis uuendatakse pidevalt signatuure?

8.52. Kas sissetungi tuvastamise ja tõrjumise süsteemi turvalogisid vaadatakse korrapäraselt läbi ebahariliku tegevuse avastamiseks?

8.53. Kas sissetungi tuvastamise ja tõrjumise süsteemi turvalogisid hoitakse alles selliselt, mis välistab nende muutmise või kustutamise?

Filtreerimine

8.54. Kas kasutatakse veebifiltreid, et piirata konfidentsiaalse teabe üleslaadimist veebipõhistesse e-posti rakendustesse? *

8.55. Kas kasutatakse veebifiltreid, et piirata salajase teabe üleslaadimist andmeportaalidesse *(storage portals)* ja kontaktkataloogide portaalidesse? *

8.56. Kas kasutatakse veebifiltreid, et piirata salajase teabe edastamist elektroonsete õnnitluskaartide portaalide kaudu? *

8.57. Kas ettevõte filtreerib töötajate internetist allalaaditut nende töörollide põhjal? *

8.58. Kas ettevõte filtreerib sisu, et tõrjuda vaenulikku Active X-i, JavaScripti ja Java Appletsi?

8.59. Kas ettevõte filtreerib sisu kõigi e-postiga saadetud manuste korral, et blokeerida või jälitada salajase teabe edastamist? *

8.60. Kas ettevõte filtreerib kõiki täidetavaid *(executable)* e-kirja manuseid?

8.61. Kas konfidentsiaalse teabe edastamise piiramiseks ettevõttevälistele isikutele kasutatakse e-posti filtreid, välja arvatud juhul, kui see on lubatud ja krüpteeritud? *

8.62. Kas ettevõte filtreerib sisu, et kontrollida kiirsuhtluse sõnumite *(instant messages)* saatmist, mis võivad sisaldada salajast teavet? *

8.63. Kas ettevõtte märgistab salajased dokumendid digivesimärkidega nii, et sisufiltrid suudaksid neid paremini tuvastada? *

8.64. Kas ettevõte filtreerib sisu väljuva failiedastusprotokolli (FTP) või triviaalse failiedastusprotokolli (TFTP) edastustel nii, et igasuguse salajase teabe edastus blokeeritakse või seda jälitatakse?

8.65. Kas ettevõte piirab võrguhaldusprotokolli SNMP päringud interneti lüüsis?

8.66. Kas ettevõte piirab sisemised SNMP-päringud volitamata süsteemidelt kriitilistele serveritele ja võrguseadmetele?

8.67. Kas ettevõte kasutab siseneva ja väljuva liikluse filtreerimist oma interneti lüüsides?

8.68. Kas ettevõte kasutab perimeetri ruuteritel siseneva ja väljuva liikluse filtreerimist, et ära hoida IP-aadresside võltsimist?

8.69. Kas ettevõte kasutab siseneva ja väljuva liikluse filtreerimist partnervõrkude vahel?

8.70. Kas tulemüüri või ruuteri reeglid takistavad volitamata väljuvaid ühendusi avalikest süsteemidest nagu veebiserverid?

9. kanal. Katkestatavad võrguühendused

Telekommunikatsiooni probleemid

9.01. Kas kodus töötavad töötajad kasutavad arvuteid, millesse on installeeritud tulemüürid, viirustõrje, turvapaigad, virtuaalse privaatvõrgu tarkvara ning millel on kasutatud muid turvameetmeid, mida ettevõte peab vajalikuks?

9.02. Kas reisivatele töötajatele antakse standarditud arvutiseadmed, milles rakendatakse turvameetmeid salajaste andmete kaitsmiseks arvuti kaotamise või varguse korral lisaks sellele, et seadmed vastavad muudele ettevõtte turvanõuetele?

9.03. Kas ettevõtte poliitikates on kehtestatud turvanõuded ettevõtte võrku sissehelistamise või virtuaalse privaatvõrgu ühendustele?

9.04. Kas ettevõtte poliitikates on kehtestatud turvanõuded väljapool asutust asuvate traadita modemite ja traadita lairibaühenduste kohta?

9.05. Kas kaugtöötegijad kasutavad ettevõtte võrku pääsemiseks kahefaktorilist autentimist?

9.06. Kas kaugtöötegijad peavad ettevõtte võrku pääsemiseks kasutama virtuaalseid privaatvõrguühendusi?

9.07. Kui kasutatakse veebipõhist virtuaalselt privaatvõrku, kas siis see kõrvaldab turvaliselt teabe sessiooni kohta sessiooni algatanud arvutist?

9.08. Kas kaugühenduste kaudu tehtavaid tegevusi monitooritakse täiendavalt, et kompenseerida asjaolu, et neid jälgitakse vähem teistest aspektidest?

Töötajate ja partnerite ebakorrapärased ühendused

9.09. Kas hoolduseks perioodiliselt võrku ühendatavaid sülearvuteid, andmekandjaid või muid seadmeid kontrollitakse rangelt?

9.10. Kas tarkvara uuendamiseks perioodiliselt võrku ühendatavaid sülearvuteid, andmekandjaid või muid seadmeid kontrollitakse rangelt?

9.11. Kas sülearvutite ja pihuarvutite traadita, infrapuna- ja Bluetooth-lingid on blokeeritud, kui neid ei ole äritegevuse seisukohalt vaja kasutada?

9.12. Kas sülearvutitesse sisseehitatud mikrofonid ja kaamerad on blokeeritud salastatud aladel viibimise ajal?

9.13. Kui salajast teavet on vaja talletada sülearvutites, kas see teave on siis krüpteeritud?

9.14. Kas ettevõte skaneerib kõiki sülearvuteid, mille on ajutiselt ettevõtte võrku ühendanud ettevõtte tarnijad ja lepingulised isikud veendumaks, et seal ei ole viiruseid, usse ja muud pahavara?

9.15. Kas ettevõtte võrku ajutiselt ühendatud ettevõtte tarnijate ja lepinguliste isikute sülearvutite tegevust jälgitakse?
9.16. Kas ettevõtte poliitikates on kehtestatud turvanõuded pihuarvutite, nutitelefonide, USB-ketaste, iPodide, digikaamerate ja muude seadmete kohta, mida saab ettevõtte võrku ühendada?
9.17. Kui on lubatud kasutada eemaldatavaid infoseadmeid, kas siis ettevõte jälgib nende kasutamist? *
9.18. Kui on lubatud kasutada pihuarvuteid ja nutitelefone, kas siis ettevõte piirab salajase teabe allalaadimist nendele seadmetele?
9.19. Kui salajast teavet on vaja ajutiselt hoida pihuarvutites või nutitelefonides, kas siis see teave on krüpteeritud?
9.20. Kui on lubatud kasutada pihuarvuteid või nutitelefone, kas siis nendele seadmetele on installitud viirustõrje?
9.21. Kui pihuarvutites või nutitelefonides kasutatakse viirustõrjetarkvara, kas siis definitsioonifaile uuendatakse korrapäraselt?

E-äri ühendused

9.22. Kui äritehinguid tehakse interneti kaudu, kas siis kliendilt ja kliendi arvutist kogutakse andmeid, mis aitavad tehingut autentida?
9.23. Kas on olemas mehhanism, mis võimaldab klientidel kontrollida, et nad on selle ettevõtte tegelikul veebisaidil, kellega nad kavatsevad äritehingut sooritada? *
9.24. Kas kliendi verifitseerimine e-äritehingute jaoks on kaitstud automatiseeritud rünnete eest pildi kuvamise või audio taasesitamisega, mida ainult inimene saab ära tunda? *
9.25. Kui interneti kaudu tehakse rahaliselt suuri äritehinguid, kas siis need tehingud autenditakse digisertifikaatidega, kahefaktoriliste loakaartide või täiendavate autentimismehhanismidega?
9.26. Kui e-äritehingute tegemiseks kasutatakse digisertifikaate, kas siis need sertifikaadid on väljastanud tunnustatud sertifitseerimisorgan?
9.27. Kui e-äritehingute tegemiseks kasutatakse digisertifikaate, kas on olemas verifitseerimise mehhanism selleks, et tõendada äritehingu tegelik sooritamine süsteemist, mille kohta sertifikaat on väljastatud? *
9.28. Kas on kehtestatud mehhanismid, et ära hoida internetis tehtavate tellimuste või äritehingute käskude muutmist?
9.29. Kas on olemas mehhanism, mis automaatselt lõpetab e-äritehingu sessiooni pärast mingit passiivset perioodi?

9.30. Kas salajasi kliendiandmeid nagu krediitkaardinumbreid ja isiku identifikaatoreid töötlevad eraldi süsteemid, millega töödeldakse veebitehinguid?
9.31. Kas kliendi veebisaidid on varustatud manipuleerimisvastase tarkvaraga, mis automaatselt taastaks iga saidi selle õigesse seisundisse, kui tehakse katse seda näotustada (*deface*)?
9.32. Kas e-äritehingute veebiportaale kontrollitakse sagedamini turvaprobleemide suhtes kui muid ettevõtte infosüsteeme?

10. kanal. Võrgu hooldus

Võrgu dokumendid

10.01. Kas ettevõtte võrgu kohta on olemas detailsed võrgu topoloogia skeemid, et oleks võimalik jälitada kõiki marsruute?
10.02. Kui need võrgu topoloogia skeemid on olemas, kas neis on loetletud kasutatavad teenuse liikumisteed ja protokollid?
10.03. Kas on kontrollitud, et võrgu topoloogia skeemil olev teave oleks korrektne, hõlmates kõiki võrgu komponente ja ühendusi?
10.04. Kas korruste plaan või geograafiline kaart näitavad täpselt, kuhu on pandud võrgukaablid?
10.05. Kas kõik võrgu topoloogiat ja füüsilist korruste plaani sisaldavad dokumendid on korralikult kaitstud volitamata juurdepääsu eest?
10.06. Kas kõik kaablid ja seadmed, mis asuvad juhtmestikukappides ja muudes kohtades, kus neid võib olla vaja ümber konfigureerida, on füüsiliselt märgistatud?
10.07. Kas seadme korpusel on ees ja taga sildid, mis vähendavad seadme valesti ümber konfigureerimise ohtu?

Turvasuunised ja standardid

10.08. Kas on olemas süsteem tarkvaraparanduste ja -uuenduste jälgimiseks, mis logib teadaandeid, et parandused ja uuendused on vajalikud, teatatud väljalaskekuupäevi ja kuupäevi ning millal need tegelikult saadakse?
10.09. Kas ettevõtte asjaomastele isikutele antakse teada kõigist uutest nõrkadest kohtadest, et nad saaksid rakendada kompenseerivaid ja kaitsvaid meetmeid selles ajavahemikuks, mis jääb avastatud nõrkade kohtade ja asjaomase paranduse või uuenduse installimise vahele?
10.10. Kas on olemas protseduurid tarkvaraparanduste ja -uuenduste installeerimiseks viisil, mis minimeerib tõrgete tekkimise ohu varasema katsetamise, hoolikalt

valitud installimise aegade ja avariiolukorra protseduuride täitmisega, et kiiresti taastada viimati teadaolev veatu seisund?

10.11 Kas turvaseadeid ja konfiguratsioone kontrollitakse uuesti pärast paranduste ja uuenduste installimist tagamaks, et neid ei ole tahtmatult ümber seadistatud vähem turvalistele sätetele või vaikesätetele?

10.12. Kas on olemas korraline protseduur kinnitamaks, et leitud tarkvaraparandused ja -uuendused on tõesti installitud õigel ajal ja ettenähtud viisil?

10.13. Kas tarnija vaikelisi turvasätteid muudetakse süsteemis enne, kui need süsteemid võrku ühendatakse?

10.14. Kas on olemas poliitikad, mis piiravad ja jälgivad nende kaughaldusvahendite kasutamist, mis võimaldavad juhtida süsteeme väljastpoolt ettevõtte võrku?

10.15. Kas ettevõttel on tarnijatega kokkulepped, milles nad garanteerivad võrgu töökindluse ja teenuse täpse taseme?

10.16. Kas on olemas protseduurid liikluse mahu piiramiseks, et võrku ei saaks muuta töövõimetuks erinevate teenuste üleliigse koormuse tõttu?

10.17. Kas on olemas protseduurid lisaserverite lisamiseks ja liikluse ümbersuunamiseks, et vältida oluliste võrgukomponentide töökorrast väljaviimist erinevate teenuste liigse koormuse tõttu?

10.18. Kas ettevõtte poliitikad keelavad kasutada süsteemi haldamiseks krüpteerimata protokolle nagu Telnet, FTP ja SNMP, välja arvatud, kui süsteem vajab neid protokolle?

10.19. Kui süsteemide haldamiseks on vaja krüpteerimata protokolle, kas vastavad ühendused suletakse pärast teatava ajavahemiku möödumist?

10.20. Kas kõik serveri- ja tööjaamad on konfigureeritud kindla turvastandardi kohaselt?

10.21. Kas kõik võrgukomponendid nagu ruuterid ja kommutaatorid on konfigureeritud kindla turvastandardi kohaselt?

10.22. Kas kõik tulemüürid ja sissetungi tuvastamise süsteemid on konfigureeritud kindla turvastandardi kohaselt?

10.23. Kas ruuterite, kommutaatorite ja muud võrgukomponentide kaughaldus on piiratud ainult volitatud IP aadressidega?

10.24. Kas loogiline pääs turvakomponentide haldamise liidestele (nt tulemüür, IDS jne) on piiratud ainult volitatud süsteemidele või IP aadressidele?

Süsteemi- ja turvalogimine

10.25. Kas kõikide kriitiliste serverite konfiguratsioonimuudatused logitakse?

10.26. Kas ruuterite ja kommutaatorite konfiguratsioonimuudatused logitakse?

10.27. Kas tulemüüride ja sissetungi tuvastamise süsteemide konfiguratsioonimuudatused logitakse?
10.28. Kas kriitilistel serveritel on süsteemilogi *(syslog)* lubatud ja andmed logitakse kaugsüsteemi?
10.29. Kas ruuteritel ja kommutaatoritel on süsteemilogi *(syslog)* lubatud ning andmed logitakse kaugsüsteemi?
10.30. Kas traadita pääsupunktides on süsteemilogi *(syslog)* lubatud ning andmed logitakse kaugsüsteemi?

Neljas valdkond. Automatiseerimisega seotud nõrkused

11. kanal. Kaugseireandurid ja juhtimissüsteemid

11.01. Kas on olemas plaanid, kus on täpselt näidatud kõik ühendusteed, mille kaudu juhtimissüsteemid on ühendatud?
11.02. Kas kõik dokumendid, milles on kaardistatud loogilise pääsu marsruudid juhtimissüsteemidesse, on hästi kaitstud volitamata juurdepääsu eest?
11.03. Kas kõik juhtimissüsteemid, mida ei ole vaja internetti ühendada, on internetist isoleeritud?
11.04. Kas kõiki ühendusi juhtimissüsteemide ja interneti vahel hinnatakse korrapäraselt selleks, et kindlaks teha, kas neid on tegelikult vaja?
11.05. Kas kõik juhtimissüsteemid on ettevõtte võrgust isoleeritud, kui ei ole mingit vajadust neid sellesse ühendada?
11.06. Kui juhtimissüsteemi ei ole võimalik ettevõtte võrgust isoleerida, kas siis seda süsteemi kaitstakse väga piiravate tulemüüride ja ründetuvastamise süsteemidega?
11.07. Kas on kantud hoolt selle eest, et sissetungijatele ei oleks tehtud kättesaadavaks selgeid skemaatilisi jooniseid füüsiliste protsesside ja nende haldamise süsteemide kohta?
11.08. Kas juhtimissüsteemi komponentide, nagu kaugjuhitavad lülitid ja klapid, aadressid ja käsukoodid on määratud või uuesti määratud nii, et neid ei ole kerge ära arvata või tuletada? *
11.09. Kas on olemas meetmed nagu kaugalarmid, mis hoiataksid, et kaugseireandureid manipuleeritakse füüsiliselt selleks, et nad esitaksid valenäitusid?
11.10. Kas kaugseireandurid on planeeritud või modifitseeritud nii, et ükskõik kellel oleks neid füüsiliselt manipuleerides raske panna valeandmeid edastama? *
11.11. Kas väga kriitiliste juhtimisseadmete juurde pääseb teise juhtimiskanali kaudu, tagades nii juurdepääsu ka siis, kui esimeses kanalis on tõrge?

11.12. Kas on olemas teine komplekt andureid, mis mõõdavad kriitilisi protsesse teistsuguse meetodiga, et esimeselt andurikomplektilt saadavaid valeandmeid oleks võimalik kiiresti avastada? *
11.13. Kui kaugseireandurid suhtlevad traadita, mobiili- või satelliitside kaudu, kas siis on rakendatud meetmeid, et ära hoida andmeedastuste võltsimine? *
11.14. Kas on olemas plaanid ja protseduurid, kuidas tegutseda kriitiliste traadita ühenduste võimaliku segamise korral?
11.15. Kui kaugterminali seadmetel on võime rakendada paroole või krüpteerimist ning talitlemise kiirusnõuded seda lubavad, kas siis rakendatakse neid turvameetmeid?
11.16. Kas kõikidel võrku installitud uutel kaugterminali seadmetel ja muudel juhtimisseadmetel on vahetatavad paroolid või muud ümberprogrammeeritavad autentimismehhanismid?
11.17. Kas kõik kriitiliste juhtimisandmete perioodilised automatiseeritud edastused, kus kiirus ei ole takistuseks, on kaitstud krüpteerimisega?
11.18. Kas kriitilised süsteemi komponendi on nii konfigureeritud, et nad uuendaksid regulaarselt oma kellaaega turvalisest ajaallikast?
11.19. Kas kõik võrgukomponendid on sünkroniseeritud kasutama sama kellaaega, ajavööndit ja kuupäeva?
11.20. Kas eriti kriitilised süsteemikomponendid uuendavad korrapäraselt oma aega erinevastest ajaallikatest, et oleks võimalik avastada ühe ajaallika ühenduste võltsimist või korruptsiooni? *
11.21. Kas on olemas piisavalt alarme, mis hoiatavad kasutajaid, kui kriitilised protsessid on väljumas ohutu töötamise tavaparameetrite piiridest? *
11.22. Kas kaugterminali seadmete operatsioonisüsteemide uuendused saadetakse turvaliselt turvalisest allikast?
11.23. Kas kaugterminali seadmete seisundipäringud saadetakse turvaliselt turvalisest allikast?

12. kanal. Varundusprotseduurid

Varundusstrateegia

12.01. Kas varundatakse operatsioonisüsteeme, programme, talitlemisandmeid ja ka andmeid ennast?
12.02. Kas andmeid varundatakse nii tihti kui see on vajalik, lähtudes nende majanduslikust väärtusest ja muutmise sagedusest?

12.03. Kas varundatud andmeid hoitakse piisavalt kaua, et oleks alles rikkumata koopia, kui andmeid on pikka aega järk-järgult rikutud viisil, mida on raske avastada?
12.04. Kas kõiki turvalisuse tagamise seisukohalt olulisi tegevuslogisid varundatakse sageli ja hoitakse vormingus, mis välistab nende manipulatsiooni?
12.05. Kas kommutaatorite ja ruuterite konfiguratsioone varundatakse korrapäraselt?
12.06. Kas rakenduspääsu logifaile varundatakse korrapäraselt turvalisse kohta?
12.07. Kas rakenduspääsu logifaile hoitakse alles piisavalt pikka aega, et oleks võimalik jälitada igasugust pikemat aega toimunud volitamata andme muutmise allikat?
12.08. Kas on olemas mitu varundust nii, et kui üks neist kaob või muudetakse volitamata, siis on võimalik süsteemi ikkagi taastada?
12.09. Kas varundusi kontrollitakse korrapäraselt, et nad oleksid loetavad ja volitamata muutmata?
12.10. Kas on olemas protseduurid varundatud andmete volitamata muutmise korral tegutsemise kohta, eriti kriisiolukorras? *
12.11. Kas varundus edastatakse korrapäraselt võrgust isoleeritud salvestile?
12.12. Kas varundus edastatakse korrapäraselt füüsiliselt kaugemal paiknevasse kohta?
12.13. Kas kriitilised varundused, mida ei ole veel kaugemal paiknevasse kohta edastatud, on salvestatud ja märgistatud niisugusel moel, et neid on lihtne kaasa võtta, kui on vaja füüsiliselt evakueeruda?
12.14. Kui varundatud info kadumine ohustaks ettevõtet, kas siis varundusi hoitakse rohkem kui ühes kaugemal paiknevas kohas?

Varunduse turve

12.15. Kas on olemas protseduurid selle kohta, kuidas tegutseda selliste krüpteerimata varundatud lintide kaotuse või varguse korral, milles sisaldub ettevõttele omane või salajane teave?
12.16. Kas varundusprotseduur hõlmab andmete kontrollimist vaenulike koodide nagu viiruste ja Trooja hobuste suhtes enne nende varundamist? *
12.17. Kui varundatav teave on oma iseloomult salajane või ettevõttele omane, kas see siis krüpteeritakse varundusprotsessis nii, et seda saaks säilitada krüpteeritud kujul? *
12.18. Kas varundamisel kasutatakse krüpteerimisvõtmeid, mida hoitakse turvalises kohas ja roteeritakse selleks, et üks kompromiteeritud võti ei võimaldaks paljastada kõiki andmeid? *

12.19. Kas varunduste krüpteerimisvõtmeid hoiustatakse turvalisel kujul teises kohas koos kavaga, millal ja kus neid kasutatakse? *

12.20. Kui varundatud koopiaid viiakse füüsiliselt teise kaugemasse kohta, kas need koopiad pannakse siis sekkumiskindlatesse anumatesse, mida veetakse turvalises transpordivahendis ja jälgitakse vedamise ajal? *

12.21. Kas kõiki varundusmeediumeid kaitstakse hoidmise ajal füüsilise varguse eest, hoitagu neid siis kohapeal või kaugemal?

12.22. Kui varundusmeediumeid ei ole enam varunduse eesmärgil vaja, kas siis on olemas turvalised protseduurid nende hävitamiseks või korduskasutusse võtmiseks, hoitagu neid siis kohapeal või kaugemal?

12.23. Kui varundatud koopia saadetakse elektroonselt kaugsüsteemi, kas siis see teave edastatakse sellesse asukohta krüpteeritult või ettenähtud turvalise püsiühendusvõrgu kaudu?

Viies valdkond. Inimkasutaja nõrkused

13. kanal. Turvaprotseduuride täitmine inimeste poolt

Turvakoolitus

13.01. Kas kõik töötajad osalevad korrapäraselt ettevõttele oluliste turvapoliitikate koolitustel ning kas neile jagatakse piisavalt selgitusi selle kohta, miks need poliitikad on olulised?

13.02. Kas töötajaid koolitatakse jälgima oma sülearvuteid ja muid kaasaskantavaid infoseadmeid või hoidma neid turvalistes kohtades, kui nad kannavad või kasutavad neid väljapool töökohta?

13.03. Kas töötajaid on koolitatud mitte valima paroole, mis on moodustatud selliste isiklike biograafiliste andmete alusel, mis võivad olla avalikult kättesaadavad?

13.04. Kas töötajatele on selgitatud paroolide ebaturvalistes kohtades, nagu näiteks töökohal olevatel märkmepaberitel, hoidmise ohtusid?

13.05. Kas töötajatele selgitatakse, milliseid ettevõttes töödeldavaid andmeid tuleb pidada salajaseks?

13.06. Kas töötajaid õpetatakse olema ettevaatlik e-postiga saadetava tarkvara suhtes, isegi kui tundub, et selle pakke on valmistanud ja saatnud usaldusväärsed tarnijad?

13.07. Kas töötajaid on õpetatud mitte langema sotsiaalse manipulatsiooni ohvriks telefonis või internetis nii, et nad avaldaks privaatset infot või tipiksid või valiksid konkreetses järjestuses numbreid või märke?

13.08. Kas töötajatele tuletatakse korrapäraselt meelde, et nad ei laadiks alla sellist tüüpi faile, mis võivad sisaldada täitmiskoode, et nad ei avaks kahtlasi e-kirju ning installiks isiklikku tarkvara ettevõtte süsteemidesse?
13.09. Kas töötajatele selgitatakse turvariske, kui nad talletavad isiklikku teavet, eriti personaalset identimisinfot oma mobiiltelefonides?
13.10. Kas töötajatele on selgitatud seda, et masstoodanguna valmistatud ja levitatav tarkvara võib siiski sisaldada pahavara?
13.11. Kas töötajatele on selgitatud, kui ohtlik on klikkida võrgu linkidel, mida turvatöötajad ei ole dokumenteerinud ja millele nad ei ole luba andnud, isegi kui nende installimist võivad paluda kõrgema juhtkonna liikmed?
13.12. Kas kõikide töötajate teadmisi turvaprotseduuride, sealhulgas uute tekkivate ohtude kohta kontrollitakse korrapäraselt?

Vastutus turvalisuse eest

13.13. Kas ettevõtte turvalisuse tagamise kohustus on lisatud töötaja ametijuhendisse?
13.14. Kas kõik töötajad peavad allkirjastama kokkulepped konfidentsiaalsuse ja intellektuaalomandi kohta?
13.15. Kas kõiki ettevõtte lepingulisi isikuid, hoonete haldajaid, vedajaid ja hooldusettevõtteid teavitatakse sõnaselgelt ettevõtte turvapoliitikatest ja -standarditest, mis kehtivad nende tegevuse kohta?
13.16. Kas kõiki ettevõtte lepingulisi isikuid, hoonete haldajaid, vedajaid ja hooldusettevõtteid on lepinguga kohustatud tagama selliste turvapoliitikate ja -standardite rakendamine, mis on vähemalt sama ranged kui ettevõtte enda poolt rakendatavad?
13.17. Kas sisselogimis- ja autentimiskuvadele on postitatud õigus-märkused, millega hoiatatakse, et volitamata pääsu või kasutamist peetakse ebaseaduslikuks sissetungiks?
13.18. Kas töötajatel on keelatud installida isiklikku, meelelahutuslikku või lihtsalt volitamata tarkvara ettevõtte seadmetele?
13.19. Kas ettevõtte poliitikates on kehtestatud, kuidas töötajad peavad kasutama e-posti, internetti ja kiirsõnumsidet *(instant messaging)*?
13.20. Kas töötajatel on keelatud lubada teistel töötajatel kasutada oma personaalarvutit?
13.21. Kas töötajatel on keelatud jagada paroole?
13.22. Kas töötajatel on keelatud kasutada isikutuvastamise vahendeid nagu töötõendid ja lähitoimekaardid, et võimaldada teistele töötajatele juurdepääs IT ruumidesse ja infosüsteemidesse?

13.23. Kas iga ettevõttele kuuluva või liisitud infoseadme eest on määratud vastutama üks töötaja?
13.24. Kas konkreetse infoseadme eest vastutavalt töötajalt nõutakse seda, et ta jälgiks selle seadme üldist turvalisust?
13.25. Kas infoseadmel on märgistus või mõned muud identifitseerivad märgid, mis aitavad selgitada, kelle vastutada on konkreetne infoseade?
13.26. Kas on olemas piisavad ergutused, et töötajad teataksid turvanõuete rikkumisest ja ebasoovitavast käitumisest, tagades neile samas, et neid ei süüdistata ega karistata sellise teatamise eest?
13.27. Kas töötajad võetakse korralikult vastutusele igasuguse tegevuse eest ettevõtte infosüsteemis, millega rikutakse ettevõtte turvapoliitikaid?

Turvalisuse ülevaatused

13.28. Kas ettevõtte infoturbepoliitikaid ja nende rakendamist vaatab igal aastal läbi lisaks audiitorile ka ekspert?
13.29. Kas ettevõtte infoturbepoliitikate ja nende rakendamise iga-aastane läbivaatus on piisavalt ulatuslik, et avastada nõrkusi füüsilistes seadmetes ja töötajate käitumises?
13.30. Kas ettevõtte infoturbepoliitikaid ja nende rakendamist kontrollitakse hoolikalt veendumaks, et ettevõte vastab tegevusharu eeskirjadele ja tunnustatud standarditele?
13.31. Kas auditite ja läbivaatuste käigus analüüsitakse ettevõtte infoturbesüsteemi, et välja selgitada valdkonnad, kus on vaja rakendada erinevaid või lisavastumeetmeid?
13.32. Kas on olemas usaldusväärne süsteem kõikide töötajate märgatud, auditite käigus avastatud, tarnijate teatatud või massimeedias kajastatud nõrkusi puudutavate probleemide loetellu lisamiseks ja väljaselgitamiseks, et turvatöötajad saaksid kiiresti ja korrapäraselt kasutada uuendatud loetelu, kus on näidatud, millised nõrgad kohad on juba parandatud ja mida on veel vaja parandada?
13.33. Kas parandusmeetmeid rakendatakse õigeaegselt, kui on vaja tegeleda veelgi olulisemate avastamata või teatamata nõrkustega?
13.34. Kas hiljuti avastatud nõrkade kohtade parandamiseks mõeldud parandusprogramme jälgitakse igakuiselt, et uurida, kas nendes valdkondades toimub kiire ja stabiilne edenemine?

13.35. Kas ettevõtte infoturbesüsteemi üksteisele järgnevaid auditeid ja ülevaatusi võrreldakse omavahel, et kõrgem juhtkond saaks veenduda, et ettevõtte infoturbe tase paraneb, mitte ei halvene?

Juhtumite lahendamine ja neile reageerimine

13.36. Kas töötajatele selgitatakse mitmesuguseid küberründe strateegiaid piisavalt üksikasjalikult ja esitatakse need mitmetes variantides, et töötajad suudaksid ära tunda selliste rünnete varased märgid ja neist kohe teatada?

13.37. Kas töötajad teavad, kellele nad peaksid teatama nii ettevõttes kui ka väljapool seda toimuvast ründest?

13.38. Kas töötajatele, kellel on pääs väga kriitilistesse süsteemidesse või ruumidesse, on antud eraldi pääsukoodid, mille kasutamine osutaks, et neid sunnitakse teataval viisil tegutsema? *

13.39. Kas on olemas automatiseeritud tuvastamise süsteemid, mis käivitaksid hääletu kaugalarmi, kui kasutatakse koode, mis viitavad sunniviisilisele tegutsemisele? *

13.40. Kas on olemas teisi sidekanaleid, mida saaks kasutada, kui tavapärased kanalid on rikutud?

13.41. Kas töötajad teavad, kuidas rikutud süsteeme isoleerida neid võrgust eemaldades?

13.42. Kas on olemas plaanid selliste süsteemide käsitsi karantiini panemiseks ja jälgimiseks, mida on valeinfoga rikutud, ilma neid sulgemata?

13.43. Kas on olemas protseduur karantiiniliinide muutmiseks, kui saadakse paremat infot võimaliku rikkumise kohta?

13.44. Kas töötajad teavad, kuidas toimida rikutud infosüsteemide taastamisel nende viimati teadaolevasse veatusse seisundisse?

13.45. Kas on olemas mehhanism viimati teadaoleva veatu seisundi taastamiseks, kui see seisund esines suhteliselt kaua aega tagasi?

13.46. Kui on olemas muud süsteemid, mis võiksid asendada suletud või ründe tõttu mittetöökindlaks muutunud süsteeme, kas siis töötajad teavad, kuidas neile üle minna?

13.47. Kas töötajad teavad, kuhu nad peaksid pöörduma lisateabe ja juhiste saamiseks, kui ründed jätkuvad?

13.48. Kui ettevõte osutab püsiklientidele kiiresti vajatavaid teenuseid, kas siis on olemas nimekiri klientidest, kellele tuleb esmajärjekorras teenuste osutamine taastada?

13.49. Kas ründele reageerivad võtmetöötajad teavad, kuidas koguda ja hoida alles tõendeid korraliku juurdlusanalüüsi tegemiseks ja süüdistuse esitamiseks?

13.50. Kas korraldatakse korrapäraselt õppusi, mille ajal võtmetöötajad sooritavad neid tegevusi, mida nad sooritaksid siis, kui peaksid reageerima küberründele mõistlikul ja realistlikul viisil?
13.51. Kas töötajatele õpetatakse, kuidas toimida turvaliselt andmekandjate ja kaasnevate materjalidega eriolukorras, mis on tekkinud õnnetuse tagajärjel?
13.52. Kas võtmetöötajatele on antud võimalus harjutada avariiolukorras reageerimist tegeliku matkeharjutuse käigus? *
13.53. Kas tegelike juhtumite ja õppuste järel toimub arutelu, mille ülesandeks on välja selgitada, mida õpiti?

14. kanal. Turvalisust ohustavad tahtlikud teod

Taustauuringud

14.01. Kas uuritakse nende töötajate tausta, kellel on kõrgemal tasemel ligipääs infole, isegi kui nende palk ja ametikoha nimetus ei pruugi osutada nende pääsutasemele?
14.02. Kui töötaja edutatakse tunduvalt kõrgemale vastutuse ja pääsutasemele, kas siis korraldatakse uus taustauuring?
14.03. Kas taustauuring korraldatakse ka ehitise hoolduspersonalile näiteks nagu majahoidjad?
14.04. Kui sellise töötaja, kellel on pääs kriitilistesse süsteemidesse, isiklikus või finantskäitumises on toimunud märgatav muutus, kas siis on olemas protseduur uue taustauuringu märkamatuks korraldamiseks, mis hõlmab selliseid asju nagu lühikese aja jooksul muutunud krediidireitingud või seletamatu rikkuse märgid? *
14.05. Kas püütakse jälgida nende endiste töötajate asukohta, kes tundsid väga põhjalikult kriitilisi süsteeme ja protseduure?

Käitumise kontrollimine

14.06. Kas ettevõttes levitatakse üldiselt infot ainult vajaduse korral, pidades siiski meeles seda, et valdkondade vahel on vaja infot jagada ning et infot on ka vaja selleks, et töötajad saaksid aru, kui oluline on mõista põhjuseid, miks nad midagi teevad?
14.07. Kui konkreetne sisendkategooria on piisavalt kriitiline, kas siis ettevõttes on ette nähtud, et selle sisendkategooria peab kinnitama teine töötaja enne selle töötlemist?
14.08. Kas vastutusalad on jagatud töötajate vahel sellisel moel, et üks töötaja ei saa sooritada kriitilist operatsiooni ilma teiste töötajate teadmata?
14.09. Kas ettevõte piirab töötajate pääsu kriitilistesse süsteemidesse kontrollimata kohtadest ja aegadel, mil ei saa teha järelevalvet?

14.10. Kas ehitise hoolduspersonalil nagu majahoidjad on takistatud sisenemine väga salastatud aladele, välja arvatud siis, kui seda kontrollivad vahetult turvatöötajad?
14.11. Kas ehitise hoolduspersonali nagu majahoidjad jälgitakse videojälgimissüsteemi kaudu ka aladel, mis on ainult mõõdukalt salajased?
14.12. Kas töötaja füüsilisi ja elektroonseid pääsulogisid vaadatakse korrapäraselt läbi, et välja selgitada pääsukatsed, mis ei tulene tavapärastest töökohustustest?
14.13. Kas ettevõte kontrollib süstemaatiliselt oma töötajate mitmeid ebaõnnestunud sisselogimiskatseid?
14.14. Kas töötajaid takistatakse pääsemast failide juurde, millest selguks, et nende käitumist on jälgitud ning ka see, kas nende käitumine on esile kutsunud erilise tähelepanu?
14.15. Kas töötajatelt nõutakse korralise puhkuse võtmist, mis võimaldaks nende ajutistel asendajatel märgata tegevusi, mis jääksid muidu ehk avastamata?
14.16. Kas on olemas meetmed, mis takistaksid töötajatel lahkumast territooriumilt salajast teavet sisaldavate flopide või USB-seadmetega? *

Suhted töötajatega

14.17. Kas ettevõte on seadnud esikohale töötajate õiglase ja heas usus kohtlemise selle asemel, et kasutada igat võimalus lühiajalise konkurentsieelise saavutamiseks?
14.18. Kas ettevõttes on olemas piisavad mehhanismid, mis võimaldavad töötajatel esitada oma kaebusi karistuseta ja nii, et nad näevad, et nende kaebust lahendatakse tõsiselt?
14.19. Kas ettevõte koondab inimesi viisil, mis ei tekita endistes töötajates vaenulikkust?
14.20. Kas ettevõttel on olemas protseduur, mis võimaldaks töötajatel teatada väljastpoolt tehtavatest katsetest välja pressida nende koostöö alusel turvasüsteemist mööda hiilides nii, et väljapressimise alust ei oleks vaja laialdaselt avaldada ega teha alalist märget selle kohta töötaja andmetesse?
14.21. Kui töötaja kogeb isiklikus elus raskusi, kas on olemas poliitika, mille kohaselt saaks ajutiselt leevendada töötaja vastutuse määra kriitilistes süsteemides ja kriitilistesse süsteemidesse pääsul?

Kuues valdkond. Tarkvara tarnija nõrkused

15. kanal. Tarkvaraarenduse sisepoliitika

Uue tarkvara arendamise turvaprotseduurid

15.01. Kas ettevõttel on kirjalik poliitika, kus on esitatud tarkvara ettevõttes arendamise sammud ja protseduurid?

15.02. Kas tarkvara arendamise tsükkel järgib suuniseid, mis põhinevad tegevusharu turbe heal taval?

15.03. Kas ettevõtte turvapoliitikad näevad ette, et kõik tarnijad ja lepingupoole töötajad, kes tegelevad tarkvara arendamisega, peavad vastama minimaalsetele turvanõuetele?

15.04. Kas turbespetsialistid hindavad kavandatavat tarkvara disaini infoturbe seisukohalt enne alfaversioonide loomist?

15.05. Kas ettevõttel on selline jälgimise süsteem, millega saab välja selgitada töötaja või ettevõttevälise isiku, kes kirjutas ettevõttes loodava tarkvara iga koodirea?

15.06. Kas kõigile programmeerijatele, kes töötavad tarkvara rakendusega, antakse teada, et peetakse täpset arvestust kõikide koodiridade kirjutajate kohta?

15.07. Kas ettevõttel on protseduurid tarkvara kirjutamise ajal koodi sisestamiseks nii, et mitte keegi peale programmeerija, kes on registreeritud selle eest vastutajaks, ei saa seda koodirida muuta? *

15.08. Kas kontrollitakse ja jälgitakse muudatusi lähtekoodi teegis nii, et administraatori õigustega isik ei saaks mööda minna allika kontrollimoodulist? *

15.09. Kas iga osakoodi kirjutamise ajal hoitakse alles kommentaarid selle kohta, et teised arendajad ja turvaspetsialistid saaksid kiiresti aru, mida antud osa on kavandatud tegema?

15.10. Kas ettevõttel on eelnevalt heakskiidetud koodimoodulid, mida saab sisestada uude tarkvarasse, et saada standardsed turvafunktsioonid, nagu näiteks autentimine ja krüpteerimine?

15.11. Kas ettevõte annab arendajatele fiktiivsed andmed, et arendatavaid rakendusi ei pea proovima eraviisilisel, salajasel ega ettevõtte andmetel?

15.12. Kas arendatavaid rakendusi proovitakse testimissüsteemides, mis on täiesti isoleeritud tegelikust tootmise keskkonnast?

Turvaomadused, mida tuleb lisada uude tarkvarasse

15.13. Kas arendatav rakendus on projekteeritud krüpteerima salajast teavet, mida see talletab failis või andmebaasis?

15.14. Kas arendatav rakendus on projekteeritud krüpteerima salajast teavet, mida see kirjutab kohaliku süsteemi registrisse?

15.15. Kas arendatav rakendus on projekteeritud krüpteerima salajast teavet, mida see kirjutab hävimälusse *(volatile memory)*?

15.16. Kas arendatav rakendus on projekteeritud krüpteerima salajast teavet, mida see edastab teise süsteemi?

15.17. Kas arendatav rakendus on projekteeritud krüpteerima salajast teavet, mida see kirjutab küpsistesse?

15.18. Kas arendatav rakendus on projekteeritud ära hoidma laialdaselt ennustatavaid autentimis- ja krüpteerimiskoode?

15.19. Kas arendatav rakendus on projekteeritud kasutama käskude täitmisel vähima privileegi põhimõtet?

15.20. Kas koodikomponentide tähendus on arendatavates rakendustes, mis on projekteeritud tegema kriitilisi operatsioone, võimaluse korral maskeeritud (*masked*) või varjatud (*obfuscated*)?

15.21. Kas kriitilised arendatavad rakendused on projekteeritud autentima allkomponente, nagu näiteks dünaamiliselt lingitavad teegid, tagamaks nende autentsust enne kasutamist? *

Uue tarkvara turvalisuse katsetamine

15.22. Kas ettevõtte arendatava tarkvara suhtes on korraldatud koodi läbivaatamine turvalisuse seisukohalt, sellest hoolimata, kas tarkvara telliti mujalt või loodi ettevõttes enne lõppversiooni ettevalmistamist juurutamiseks? *

15.23 Kas tarkvara katsetamiseks kasutatavad kasutajakontod eemaldatakse süstemaatiliselt enne, kui tarkvara tegelikult kasutama hakatakse?

15.24. Kui lähtekoodis on arendajate kommentaarid, mis on arendamisprotsessis alles jäänud, kas need eemaldatakse käsitsi enne programmi juurutamist?

15.25. Kas ettevõte laseb infoturbeasjatundjatel korraldada arendatud tarkvara nõrkade kohtade testimisi, sellest hoolimata, kas tarkvara on mujalt tellitud või ettevõttes loodud?

15.26. Kas ettevõte laseb infoturbespetsialistidel korraldada regulaarseid nõrkade kohtade testimisi juba juurutatud rakendustel?

16. kanal. Ettevõtteväliste tarnijatega suhtlemise poliitika

Suhted tarijatega

16.01. Kas ettevõttel on kirjalik poliitika, milles on täpsustatud tarkvara tarnijate ja ettevõtteväliste arendajatega suhtlemise sammud ja protseduurid?

16.02. Kas tulevasteks tarnijateks ja ettevõttevälisteks arendajateks on ainult need isikud, kelle puhul saab tõendada, et nad vastavad tegevusharu infoturbe standarditele?

16.03. Kas tarnijatelt või lepingulistelt töötajatelt nõutakse, et nad osaleksid kliendi ettevõtte infominutitel või turbepoliitikate koolitusel?

16.04. Kas tarnijatelt või lepingulistelt töötajatelt nõutakse lepinguga, et nad peavad järgima kliendi ettevõtte turvapoliitikaid?

16.05. Kas ettevõtte poliitikad näevad ette, et tarnija töötajad peavad allkirjastama saladuste mitteavaldamise kokkulepped *(non-disclosure agreements)*?

16.06. Kas teeninduslepingutes nähakse ette, et tarnijad peavad uurima oma töötajate tausta enne, kui nad määratakse tegelema ettevõtte tellimusega?

16.07. Kui rakendus tehti kolmandast isikust tarnija poolt, kas siis tarnija suudab tõendada seda, et rakendas ettevaatusabinõusid selleks, et rakendusel ei oleks tagauksi, mis võimaldaks kolmandale poolele sissepääsu?

16.08. Kas tarkvaratarnijatelt nõutakse kinnitust, et nende koodi on üksikasjalikult ja põhjalikult uuritud turvalisuse suhtes enne, kui see juurutamiseks tarnitakse?

16.09. Kas tarkvaratarnijatelt nõutakse deponeerimise korraldamist, et hoiustada ja kaitsta ostetavates või litsentsitavates rakendustes kasutatavat lähtekoodi?

Tarnijasuhete pidev haldamine

16.10. Kas on olemas usaldusväärsed kanalid iga tarkvaratarnija käest uuenduste saamiseks?

16.11. Kas on olemas korraline protseduur interneti või telefoni teel kinnituse saamiseks selle kohta, et tarnija füüsiline saadetis on autentne?

16.12. Kas tarnijad saadavad füüsilisi saadetisi sellistes pakendites ja siltidega, mida on raske võltsida või manipuleerida?

16.13. Kui on vaja rakendada tarkvarauuendusi, kas siis on olemas garantii, et neid uuendusi katsetati piisavalt asjakohases tarkvarakeskkonnas enne installimist?

16.14. Kas tarnijate pääsuõigustele, mida neil on vaja tarkvara ja uuenduste installimiseks, kehtivad asjakohased piirangud ja lõppemistähtaeg?

16.15. Kas on olemas protseduur, mida rakendatakse korrapäraselt, et tagada varasemate tarnijate ja lepinguliste isikute pääsuõiguste tegelik tühistamine kohe, kui need ei ole enam vajalikud?

16.16. Kas on olemas meetmed, millega tagatakse süsteemi toimimine uuenduste paigaldamise ajal ning mille abil on võimalik taastada süsteem selle viimases teadaolevas veatus seisundis, kui uuenduste paigaldamine peaks ebaõnnestuma?

16.17. Kas ettevõttel on kehtestatud protsessid, mis piiraks, kontrolliks ja jälgiks tarnijate või lepinguliste isikute pääsu siseteabe juurde? *

16.18. Kas ettevõttel on kehtestatud protsessid, mis selgitaks välja ja lõpetaks tarnija, lepingulise isiku ja muude väljasttellitud teenuste osutajate juurdepääsu, kui seda enam vaja ei ole?

16.19. Kas tarnijate saabumised ja lahkumised on logitud ja jälgitud elektroonselt või füüsiliselt?

16.20. Kas on olemas protseduurid, mille kohaselt toimub ettevõttele kuuluva teabe koopiate hävitamise tõendamine pärast seda, kui tarnijad on tellitud tarkvara üle andnud?

16.21. Kas jälgitakse nende endiste tarnijate või lepinguliste isikute tegevust, kes tegelesid kriitilise teabe või kriitiliste süsteemidega, selles suhtes, kas nad rikuvad saladuse mitteavaldamise kokkuleppeid?

Luba kasutada US-CCU küberturbe kontroll-küsimustikku

US-CCU küberturbe kontroll-küsimustik, mille autoriõigus kuulub US-CCU-le, võib lisada teise dokumenti, viia teise formaati ja tarkvarasse tasuta, kuid ainult siis, kui on täidetud järgmised tingimused:

1) US-CCU-le esitatakse kavandatava publikatsiooni näidis ning US-CCU kinnitab kirjalikult, et see on kooskõlas käesolevate US-CCU suunistega.

2) Käesolev teade esitatakse hästi märgatavas kohas publikatsiooni lisatavas sissejuhatuses, organisatsiooni andmetes või selgitavas materjalis.

3) Kui publikatsiooni lisatakse muid küberturbe küsimusi, siis US-CCU küberturbe kontroll-küsimustikus sisalduvad küsimused tuleb esitada paksus kirjas, kaldkirjas või mõnes muus kirjalaadis, mis neid selgelt eristab ülejäänud materjalist.

4) Publikatsioonis tuleb esitada kõik US-CCU küberturbe kontroll-küsimustiku küsimused ühtegi välja jätmata.

5) US-CCU küberturbe küsimuste originaalsõnastust ei tohi muuta.

6) Publikatsiooni tiitellehel ja kaanel tunnustatakse US-CCU autoriõigust ning US-CCU küberturbe kontroll-küsimustiku küsimuste autorsust, mis kuulub selgelt John Bumgarnerile ja Scott Borgile.

7) Kasutatud US-CCU küberturbe kontroll-küsimustiku konkreetse väljaande kuupäev tuleb selgelt märkida publikatsiooni tiitellehele ja kaanele.

8) Publikatsiooni kasutajatele antakse käesolevaga teada, et US-CCU küberturbe kontroll-küsimustik on otse US-CCU-lt avalikkusele tasuta kättesaadav.