Avaldatud eesti keeles: jaanuar 2012
Jõustunud Eesti standardina: jaanuar 2012

INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 1: Ülevaade ja mõisted

Information technology
Security techniques
Network security
Part 1: Overview and concepts
(ISO/IEC 27033-1:2009)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27033-1:2009 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisel EVS Teataja 2012. aasta jaanuarikuu numbris.

Standardi on tõlkinud AS Cybernetica, standardi tõlke on heaks kiitnud EVS/TK 4 „Infotehnoloogia“.

Standardi tõlkimise ettepaneku on esitanud EVS/TK 4, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

See standard on rahvusvahelise standardi ISO/IEC 27033-1:2009 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardikeskus ja sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO/IEC 27033-1:2009. It has been translated by the Estonian Centre for Standardisation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: arvutivõrk, infotehnoloogia, infoturbe haldus, infoturve
Hinnagrupp W

SISUKORD

EESSÕNA IV
SISSEJUHATUS V
1 KÄSITLUSALA 1
2 NORMIVIITED 1
3 TERMINID JA MÄÄRATLUSED 2
4 LÜHENDID 6
5 STRUKTUUR 8
6 ÜLEVAADE 10
6.1 Taust 10
6.2 Võrguturbe plaanimine ja haldus 12
7 RISKIDE TUVASTAMINE JA ETTEVALMISTUSED TURVAMEETMETE PIIRITLEMISEKS 14
7.1 Sissejuhatus 14
7.2 Teave praeguste ja/või plaanitavate võrkude kohta 14
7.3 Infoturvariskid ja võimalikud reguleerimisalad 18
8 TUGIMEETMED 20
8.1 Sissejuhatus 20
8.2 Võrguturbe haldus 21
8.3 Tehniliste nõrkuste haldus 24
8.4 Identifitseerimine ja autentimine 24
8.5 Võrgu revisjonilogimine ja seire 25
8.6 Sissetungi avastamine ja tõrje 26
8.7 Kaitse kahjurkoodi eest 27
8.8 Krüptograafiapõhised teenused 28
8.9 Jätkusuutlikkuse haldus 29
9 VÕRGUTURBE KAVANDAMISE JA TEOSTAMISE JUHISED 29
9.1 Taust 29
9.2 Võrgu tehnilise turbe arhitektuur ja lahendus 29
10 TÜÜPSED VÕRGUSTSENAARIUMID. RISKID, KAVANDAMISMEETODID JA REGULEERIMISKÜSIMUSED 31
10.1 Sissejuhatus 31
10.2 Internetti pääsu teenused töötajaile 32
10.3 Tõhusa koostöö teenused 32
10.4 Partnerteenused (B2B) 32
10.5 Tarbeteenused (B2C) 32
10.6 Ostuteenused 33
10.7 Võrgu segmentimine 33
10.8 Mobiilside 33
10.9 Rändkasutajate võrgutugi 33
10.10 Kodu- ja väikekontorite võrgutugi 34
11 TEHNILINE KÜLG. RISKID, KAVANDAMISMEETODID JA REGULEERIMISKÜSIMUSED 34
12 TURBELAHENDUSTE VÄLJATÖÖTAMINE JA TESTIMINE 34
13 TURBELAHENDUSE KÄITUS 35
14 LAHENDUSE TEOSTUSE SEIRE JA LÄBIVAATUS 35
Lisa A (teatmelisa) Tehniline külg. Riskid, kavandamismeetodid ja reguleerimisküsimused 36
Lisa B (teatmelisa) ISO/IEC 27001 ja ISO/IEC 27002 võrguturbealaste meetmete ning ISO/IEC 27033 selle osa jaotiste vahelised viited 58
Lisa C (teatmelisa) Turbeprotseduuride dokumendi näidismall 63
Kirjandus 66

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmesorganisatsioonid osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud käsitlema tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvi pakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IEC-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühendatud tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Ühendatud tehnilise komitee põhiülesanne on rahvusvaheliste standardite koostamine. Tehnilistes komiteedes vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks rahvuslikele liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletusel osalenud rahvuslikest liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO-t ega IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27033-1 on koostanud ISO/IEC ühendatud tehnilise komitee JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Turbemeetodid“.

See dokument asendab standardit ISO/IEC 18028-1:2006.

ISO/IEC 27033 üldpealkirjaga „Infotehnoloogia. Turbemeetodid. Võrguturve“ koosneb järgmistest osadest.

— Osa 1: Võrguturbe juhised.

Koostamisel on

— Osa 2: Võrguturbe kavandamise ja teostamise juhised; ja

— Osa 3: Tüüpsed võrgustsenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused.

Tulevaste osade teema moodustavad riskid, kavandamismeetodid ja reguleerimisküsimused järgmistel aladel:

— võrkudevahelise side turve turvalüüside abil,

— virtuaalsete privaatvõrkude turve,

— IP-konvergents,

— traadita võrgud.

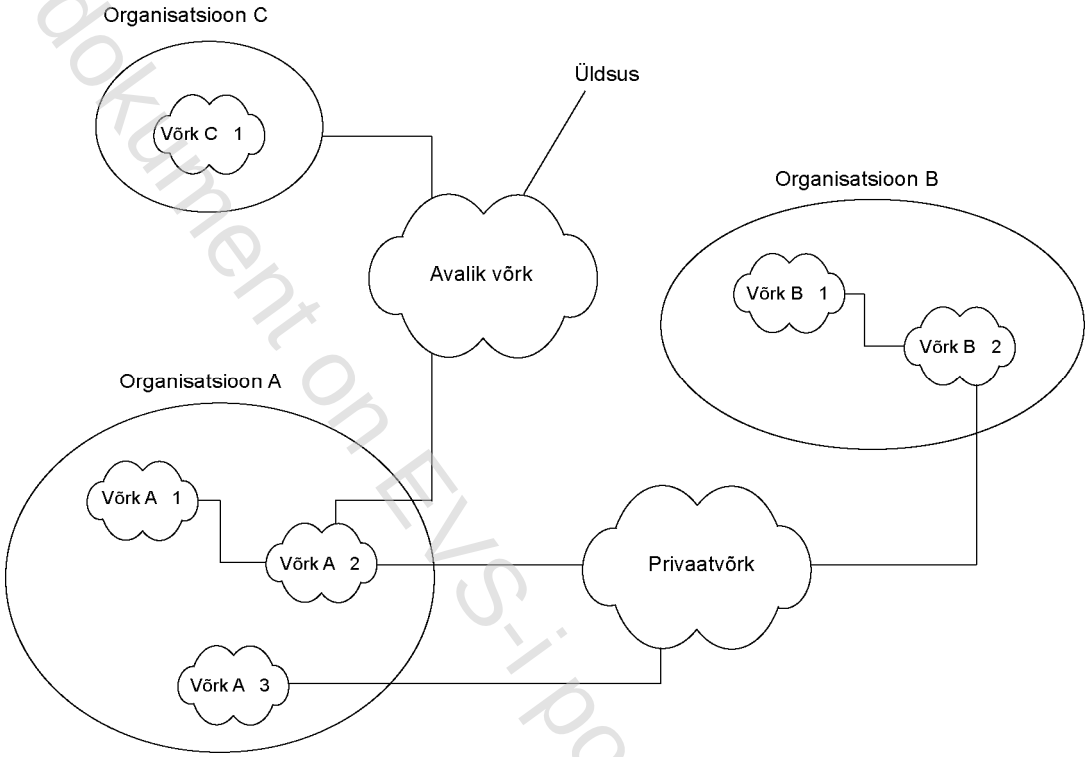
SISSEJUHATUS

Tänapäeval on enamiku ettevõtete ja riigiasutuste infosüsteemid ühendatud võrkudega (vt joonis 1), kusjuures võrguühendused on tüübilt vähemalt üks järgnevaist:

— organisatsioonisisesed,

— organisatsioonidevahelised,

— organisatsiooni ja üldsuse vahelised.



Joonis 1 — Üldised võrguühenduste tüübid

Peale selle pakub avalike võrkude (eriti Interneti) tehnoloogia kiire areng märkimisväärseid soodsaid äritegevuse võimalusi ning organisatsioonid rakendavad elektroonilist äritegevust üha enam ülemaailmses ulatuses ning pakuvad avalikke võrguteenuseid. Nimetatud võimaluste hulka kuuluvad odavam andmeside, Interneti kasutamine lihtsalt ülemaailmse ühendusmeediumina ja seejärel arenenumad teenused, mida annavad Interneti teenuste tarnijad. See võib tähendada suhteliselt odavate kohalike ühenduspunktide kasutamist ahela mõlemas otsas, aga ka täieulatuslikke võrgustatud elektroonilise kaubanduse ja teeninduse süsteeme veebipõhiste rakenduste ja teenuste abil. Uus tehnoloogia (sh andmete, kõne ja video integratsioon) suurendab ka soodsaid kaugtöö võimalusi, nii et töötajad saavad küllaltki pikkadel perioodidel tegutseda oma kodustes töökohtades. Nad saavad olla ühenduses kaugvahendite abil, millega pääseda organisatsiooni ja kogukonna võrkudesse ning tööalast tegevust toetava nendega seotud teabe ja teenuste juurde.

See keskkond soodustab oluliste ärialaste hüvede saamist, kuid sisaldab uusi turvariske, mida tuleb hallata. Kuna organisatsioonide tegutsemine sõltub tugevalt teabe ja sellega seotud võrkude kasutamisest, võib teabe ja teenuste konfidentsiaalsuse, tervikluse ja käideldavuse kadu avaldada organisatsiooni tegevusele olulist kahjulikku mõju. Seega on üks peamisi nõudeid võrkude ning nendega seotud infosüsteemide ja teabe korralik kaitstus. Teisisõnu, sobiva võrguturbe teostamine ja säilitamine on organisatsiooni tegevuse eduks elutähtis.

Selles kontekstis otsitakse side- ja infotehnoloogia valdkondades kuluefektiivseid terviklikke turbelahendusi, mis on suunatud võrkude kaitsele pahatahtlike rünnete ja tahtmatute väärtoimingute eest ning tegevusalaste teabe ja teenuste konfidentsiaalsus-, terviklus- ja käideldavusnõuete täitmisele. Võrgu turve on oluline ka võimaliku arveldus- või kasutamisteabe täpsuse säilitamiseks. Kogu võrgu (sh rakenduste ja teenuste) turvalisuse seisukohalt on toodete turvaomadused väga olulised. Paljude toodete kombineerimisel terviklahenduste saamiseks määrab aga lahenduse edu nende koostalitlusvõime või viimase puudumine. Turve peab olema mitte ainult üks iga toote ja teenuse puhul arvestatav tahk, vaid seda tuleb arendada nii, et see soodustaks turvaomaduste põimimist üldisesse turbelahendusse.

ISO/IEC 27033 eesmärk on anda üksikasjalikke juhiseid infosüsteemide võrkude ja nendevaheliste ühenduste halduse, käituse ja kasutamise turbeaspektide kohta. Need, kes organisatsioonis vastutavad infoturbe, eriti aga võrguturbe eest, peaksid suutma sobitada selles standardis olevat materjali oma erinõuetega. Standardi peamised eesmärgid on järgmised.

— ISO/IEC 27033-1. Ülevaade ja mõisted: määratleda ja kirjeldada võrguturbega seotud mõisted ja anda võrguturbe halduse juhiseid. See hõlmab ülevaadet võrguturbest ja sellega seotud määratlusi ning ka juhiseid selle kohta, kuidas tuvastada ja analüüsida võrgu turvariske ja seejärel määratleda võrguturbe nõuded. Sissejuhatavalt käsitletakse kvaliteetsete tehnilise turbe arhitektuuride loomist ning riski, kavandamise ja reguleerimise aspekte, mis on seotud tüüpiliste võrgustsenaariumite ja võrgutehnoloogia aladega (üksikasjalikumalt käsitletakse neid ISO/IEC 27033 järgmistes osades).

— ISO/IEC 27033-2. Võrguturbe kavandamise ja teostamise juhised: määratleda, kuidas organisatsioonid peaksid jõudma konkreetsetele ärikeskkondadele sobivat võrguturvet tagavate kvaliteetsete tehnilise turbe arhitektuuride, lahenduste ja teostusteni, kasutades järjekindlat asjakohast lähenemisviisi võrguturbe plaanimisele, kavandamisele ja teostamisele mudelite või karkasside abil (selles kontekstis kirjeldatakse mudeli või karkassi abil üldjoontes esitust või kirjeldust, mis näitab tehnilise turbe arhitektuuri mingi arhitektuuri- või kavanditüübi struktuuri ja üldist toimimisviisi); puudutab kõiki töötajaid, kes osalevad võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke).

— ISO/IEC 27033-3. Riskid, kavandamismeetodid ja reguleerimisküsimused tüüpsete võrgustsenaariumite puhul: määratleda tüüpiliste võrgustsenaariumitega seotud spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused. Puudutab kõiki töötajaid, kes osalevad võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises (nt võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbeametnikke).

Ootuste kohaselt käsitlevad ISO/IEC 27033 tulevased osad alljärgnevaid teemasid.

— ISO/IEC 27033-4. Riskid, kavandamismeetodid ja reguleerimisküsimused turvalüüse kasutava võrkudevahelise side turbe puhul: määratleda spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused võrkudevaheliste teabevoogude turvamisel turvalüüsidega. Puudutab kõiki töötajaid, kes osalevad turvalüüside detailses plaanimises, kavandamises ja teostamises (nt võrguarhitektid ja -projekteerijad, võrguhaldurid ja võrguturbeametnikud).

— ISO/IEC 27033-5. Riskid, kavandamismeetodid ja reguleerimisküsimused virtuaalsete privaatvõrkude turbe puhul: määrata kindlaks spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused virtuaalsete privaatvõrkudega (VPN) loodud ühenduste turbe puhul. Puudutab kõiki töötajaid, kes osalevad VPN turbe detailses plaanimises, kavandamises ja teostamises (nt võrguarhitektid ja -projekteerijad, võrguhaldurid ja võrguturbeametnikud).

— ISO/IEC 27033-6. IP-konvergents: määrata kindlaks spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused IP-konvergentsvõrkude (s.t andmete, kõne ja video konvergentsiga võrkude) turbe puhul. Puudutab kõiki töötajaid, kes osalevad IP-konvergentsvõrkude turbe detailses plaanimises, kavandamises ja teostamises (nt võrguarhitektid ja -projekteerijad, võrguhaldurid ja võrguturbeametnikud).

— ISO/IEC 27033-7. Traadita võrgud: määrata kindlaks spetsiifilised riskid, kavandamismeetodid ja reguleerimisküsimused traadita võrkude, sh raadiovõrkude turbe puhul. Puudutab kõiki töötajaid, kes osalevad traadita võrkude ja raadiovõrkude turbe detailses plaanimises, kavandamises ja teostamises (nt võrguarhitektid ja -projekteerijad, võrguhaldurid ja võrguturbeametnikud).

Tuleb rõhutada, et ISO/IEC 27033 annab üksikasjalikke teostuse lisajuhiseid nende võrguturbe meetmete kohta, mida standardi põhitasemel kirjeldab ISO/IEC 27002.

Kui edaspidi ilmub uusi osi, puudutavad need kõiki töötajaid, kes osalevad nende osadega kaetud võrguaspektide detailses plaanimises, kavandamises ja teostamises (nt võrguarhitektid ja -projekteerijad, võrguhaldurid ja võrguturbeametnikud).

Tuleks silmas pidada, et see standard ei ole etalon- ega normdokument regulatiivsete või õigusaktidest tulenevate turvanõuete küsimustes. Standard rõhutab küll nende mõjurite tähtsust, kuid ei saa neid konkreetselt esitada, sest need sõltuvad konkreetsest riigist, ettevõtte tüübist jne.

Kui pole öeldud teisiti, on ISO/IEC 27033 kogu selles osas esitatud juhised kohaldatavad praegustele ja/või plaanilistele võrkudele, mida edaspidi nimetatakse lihtsalt võrkudeks või võrguks.

1 KÄSITLUSALA

ISO/IEC 27033 see osa annab ülevaate võrguturbest ja seotud määratlustest. Standard määratleb ja kirjeldab mõisteid, mis on seotud võrguturbega ja annab võrguturbe halduse juhiseid. (Lisaks sidelülide kaudu edastatava teabe turbele puudutab võrguturve seadmete turvet, nende seadmetega seotud haldustegevuste turvet, rakendusi ja teenuseid ning lõppkasutajaid.)

Standard puudutab kõiki, kes on seotud mingi võrgu omamise, käituse või kasutamisega. Lisaks juhtidele ja ülematele, kellel on erikohustused infoturbe ja/või võrguturbe ja võrgu käituse alal või kes vastutavad organisatsiooni üldise turbekava ja turvapoliitika väljatöötamise eest, kuuluvad nende hulka kõrgemad juhid ja muud kasutajate mittetehnilised juhid. See puudutab ka kõiki võrguturbe arhitektuuri aspektide plaanimises, kavandamises ja teostamises osalejaid.

Lisaks annab ISO/IEC 27033 see osa

— juhiseid selle kohta, kuidas tuvastada ja analüüsida võrgu turvariske ning määrata selle analüüsi põhjal võrgu turvanõuded;

— ülevaate meetmetest, mis toetavad võrgu tehnilise turbe arhitektuure ja nendega seotud tehnilisi meetmeid ning ka neid mittetehnilisi ja tehnilisi meetmeid, mis on rakendatavad mitte ainult võrkudele;

— sissejuhatava kirjelduse kvaliteetsete võrgu tehnilise turbe arhitektuuride saavutamise ning tüüpiliste võrgustsenaariumite ja võrgu tehnoloogiliste aladega seotud riski-, kavandamis- ja reguleerimisaspektide kohta (üksikasjalikumalt käsitlevad neid ISO/IEC 27033 järgmised osad);

— lühida küsimuste käsitluse, mis on seotud võrguturbe meetmete teostamise ja käitusega ning nende teostuse pideva seire ja läbivaatusega.

Kokkuvõttes annab standard ülevaate standardisarjast ISO/IEC 27033 ning sissejuhatuse teistesse osadesse.

2 NORMIVIITED

Alljärgnevalt nimetatud dokumendid on vajalikud selle standardi rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 7498 (kõik osad). Information technology — Open systems interconnection — Basic reference model

ISO/IEC 27000:2009. Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2005. Information technology — Security techniques — Code of practice for information security management

ISO/IEC 27005:2008. Information technology — Security techniques — Information security risk management

EE MÄRKUS Ülalnimetatud standarditest on eesti keeles avaldatud järgnevad:

EVS-ISO/IEC 27000:2010. Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Ülevaade ja sõnavara

EVS-ISO/IEC 27001:2006. Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded

EVS-ISO/IEC 27002:2008. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis

EVS-ISO/IEC 27005:2009. Infotehnoloogia. Turbemeetodid. Infoturvariski haldus