

INFOTEHNOLOOGIA

Turbemeetodid

Infotehnoloogiavõrkude turve

Osa 3: Võrkudevahelise side turve

turvalüüside abil

(ISO/IEC 18028-3:2005)

Information technology

Security techniques

IT network security

Part 3: Securing communications between

networks using security gateways

(ISO/IEC 18028-3:2005)

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard on 2005. aastal ilmunud rahvusvahelise standardi ISO/IEC 18028-3 "Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways" tõlge eesti keelde.

Standard EVS-ISO/IEC 18028-3 on koostatud Majandus- ja Kommunikatsiooniministeeriumi tellimusel. Standardi tõlkis Cybernetica AS ja tõlke kiitis heaks EVS/TK 4 "Infotehnoloogia".

Rahvusvahelise standardi ISO/IEC 18028-3:2005 tekst on avaldatud Eesti standardina EVS-ISO/IEC 18028-3:2007, mis on kinnitatud Eesti Standardikeskuse 07.12.2007 käskkirjaga nr 201 ning jõustub selle kohta EVS Teataja 2008. aasta jaanuarikuu numbris teate avaldamisega.

This standard is the Estonian [et] version of the International standard ISO/IEC 18028-3:2005 "Information technology – Security techniques – IT network security – Part 3: Securing communications between networks using security gateways". It has the same status as the official version.

In case of interpretation disputes the English text applies.

Standardite reprodutseerimis- ja levitamiseõigus kuulub Eesti Standardikeskusele

SISUKORD

EESSÕNA.....	4
SISSEJUHATUS	5
1 KÄSITLUSALA	7
2 NORMATIIVVIITED	7
3 TERMINID JA MÄÄRATLUSED	7
4 LÜHENDID.....	10
5 TURVANÕUDED.....	11
6 TURVALÜÜSIDES KASUTATAVAD MEETODID	12
6.1 Pakettide filtreerimine.....	12
6.2 Pakettide oleku kontroll	12
6.3 Rakendusproksi.....	13
6.4 Võrguaadresside transleerimine (NAT).....	13
6.5 Sisu analüüsimine ja filtreerimine	13
7 TURVALÜÜSI KOMPONENDID	14
7.1 Kommutaatorid	14
7.2 Marsruuterid.....	15
7.3 Rakendustaseme lüüs	15
7.4 Turvaseadmed	15
8 TURVALÜÜSI ARHITEKTUUR.....	16
8.1 Struktuurmeetod.....	16
8.1.1 Paketifilter-tulemüür	16
8.1.2 Kahepoolse hostiga lüüs	17
8.1.3 Varjestatud hostiga arhitektuur	18
8.1.4 Varjestatud alamvõrguga arhitektuur.....	19
8.2 Astmemeetod	21
9 VALIMISE JA KONFIGUREERIMISE JUHISEID	24
9.1 Turvalüüsi arhitektuuri ja sobivate komponentide valimine	25
9.2 Riistvara- ja tarkvaraplatvorm	25
9.3 Konfigureerimine	25
9.4 Turvafunktsioonid ja -sätted	26
9.5 Administreerimine	27
9.6 Logimine	27
9.7 Dokumentatsioon	28
9.8 Revisjon	28
9.9 Koolitus.....	28
9.10 Mitmesugust.....	28
Kasutatud kirjandus	30

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud 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 IECga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse rahvuslikele kogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75 protsendilt hääletanud rahvuslikelt kogudelt.

Tuleb pöörata tähelepanu võimalusele, et mõned selle rahvusvahelise standardi elemendid võivad olla patendiõiguse objektiks. ISO ega IEC ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

Standardi ISO/IEC 18028-3 koostas ISO/IEC ühendatud tehniline komitee JTC 1 "Infotehnoloogia" alamkomitee SC 27, "Infoturbemeetodid".

ISO/IEC 18028, üldpealkirjaga "Infotehnoloogia. Turbemeetodid. Infotehnoloogia-võrkude turve", koosneb järgmistest osadest.

- Osa 1: Võrguturbe haldus
- Osa 2: Võrguturbe arhitektuur
- Osa 3: Võrkudevahelise side turve turvalüüside abil
- Osa 4: Kaugpöörduse turve
- Osa 5: Võrkudevahelise side turve virtuaalsete privaativõrkude abil.

SISSEJUHATUS

Side ja infotehnoloogia valdkonnad otsivad kõikehõlmavaid ökonoomseid turbelahendusi. Turvaline võrk peaks olema kaitstud rünnete eest, olgu need pahatahtlikud või ettekavatsematud, ning peaks vastama tööalastele nõuetele, mis puudutavad teabe ja teenuste konfidentsiaalsust, terviklust, käideldavust, salgamise vääramist, jälitatavust, autentsust ja stabiilsust. Võrgu turve on oluline ka arveldus- või kasutamisteabe õigsuse seisukohalt. Kogu võrgu (sealhulgas rakenduste ja teenuste) üldise turvalisuse saavutamiseks on olulised toodete turbevõimed. Kuna terviklahenduste saamiseks ühendatakse üha suurem arv tooteid, otsustab lahenduse õnnestumise nende koostalitlusvõime või selle puudumine. Turbele tuleb mitte ainult pöörata tähelepanu iga toote ja teenuse puhul, vaid teda tuleb arendada nii, et edendataks turbevõimete põimumist täieulatuslikus turbelahenduses tervikuna. Seetõttu on ISO/IEC 18028 eesmärk anda detailseid juhiseid infosüsteemide võrkude ja nende vaheliste ühenduste halduse, käigushoiu ja kasutamise turbeaspektide kohta. Need, kes organisatsioonis vastutavad üldise infoturbe eest ja eriti võrguturbe eest, peaksid suutma sobitada selles standardis olevat materjali oma konkreetsete vajadustega. Standardi peaeesmärgid on järgmised.

- ISO/IEC 18028-1: määratleda ja kirjeldada võrguturbega seotud mõisted ja anda juhiseid võrguturbe halduse kohta, sealhulgas selle kohta, kuidas piiritleda ja analüüsida sidega seotud tegureid, mida tuleb arvestada võrguturbe nõuete väljaselgitamiseks, ning tutvustada võimalikke turbealasid ja spetsiifilisi tehnilisi alasid (mida käsitlevad ISO/IEC 18028 järgmised osad);
- ISO/IEC 18028-2: määratleda standardne turbearhitektuur, mis kirjeldab üht kooskõlalist raamstruktuuri võrguturbe plaanimise, projekteerimise ja teostamise abistamiseks;
- ISO/IEC 18028-3: määratleda meetodid võrkudevaheliste infovoogude kaitsmiseks turvalüüside abil;
- ISO/IEC 18028-4: määratleda kaugpöörduse turbe meetodid;
- ISO/IEC 18028-5: määratleda meetodid võrkude vahel loodavate ühenduste kaitsmiseks virtuaalsete privaatvõrkude (VPNide) abil.

ISO/IEC 18028-1 puudutab kõiki, kes on seotud võrgu omamise, käituse või kasutamiseega. See hõlmab juhte ja haldureid, kellel on spetsiifilised kohustused infoturbe ja/või võrguturbe ja võrkude käituse alal või kes vastutavad organisatsiooni üldise turbekava ja turvapoliitika väljatöötamise eest, lisaks neile ka kõrgemaid juhte ja muid mittetehnilisi juhte või kasutajaid.

ISO/IEC 18028-2 puudutab kõiki neid töötajaid, kes osalevad võrguturbe arhitektuuriaspektide plaanides, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-3 puudutab kõiki neid töötajaid, kes osalevad turvalüüside detailses plaanides, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-4 puudutab kõiki neid töötajaid, kes osalevad kaugpöörduse turbe detailses plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-5 puudutab kõiki neid töötajaid, kes osalevad VPNi turbe detailses plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

INFOTEHNOLOOGIA

Turbemeetodid. Infotehnoloogiavõrkude turve

Osa 3: Võrkudevahelise side turve turvalüüside abil

Information technology

Security techniques. IT network security

Part 3: Securing communications between networks using security gateways

1 KÄSITLUSALA

ISO/IEC 18028 see osa annab ülevaate mitmesugustest turvalüüsidest kasutatavaist meetoditest ja komponentidest ning turvalüüside arhitektuuri eri tüüpidest. Ta annab ka juhiseid turvalüüside valimiseks ja konfigureerimiseks.

Samasuguseid meetodeid kasutavad ka personaalsed tulemüürid, kuid nad jäävad ISO/IEC 18028 käsitusala väljast, sest nad ei kujuta endast turvalüüsi.

ISO/IEC 18028 selle osa eeldatav lugejaskond on tehnilised ja haldustöötajad, näiteks IT-juhid, süsteemiadministraatorid, võrguadministraatorid ja infoturbepersonal. Ta annab juhiseid, mis aitavad kasutajal valida turvalüüsi jaoks õiget tüüpi arhitektuuri, mis kõige paremini vastab kasutaja turvanõuetele.

2 NORMATIIVVIITED

Alljärgnevas viidatud dokumendid on käesoleva dokumendi rakendamiseks mõõdapärasmatud. Dateeritud viidete puhul kehtib ainult siin viidatud redaktsioon. Dateerimata viidete puhul kehtib viidatud dokumendi uusim redaktsioon (koos võimalike muudatustega).

ISO/IEC 18028-4:2005 Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 4: Kaugpöörduse turve

3 TERMINID JA MÄÄRATLUSED

Käesoleva dokumendi otstarbeks kehtivad järgmised terminid ja määratlused.

3.1**alarm**

"viivitamatu" märguanne selle kohta, et infosüsteemi ja võrgu vastu võib olla suunatud rünne või et nad võivad olla õnnetusjuhtumi, tõrke või inimvea tõttu ohus