INFOTEHNOLOOGIA
Turbemeetodid
Infotehnoloogiavõrkude turve
Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkude abil (ISO/IEC 18028-5:2006)

Information technology
Security techniques
IT network security
Part 5: Securing communications across networks using virtual private networks (ISO/IEC 18028-5:2006)

EESTI STANDARDIKESKUS

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard on 2006. aastal ilmunud rahvusvahelise standardi ISO/IEC 18028-5 "Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks" tõlge eesti keelde.

Standard EVS-ISO/IEC 18028-5 on koostatud Majandus- ja Kommunikatsiooniministeeriumi tellimusel. Standardi tõlkis Cybernetica AS ja tõlke kiitis heaks EVS/TK 4 "Infotehnoloogia".

Rahvusvahelise standardi ISO/IEC 18028-5:2006 tekst on avaldatud Eesti standardina EVS-ISO/IEC 18028-5:2007, mis on kinnitatud Eesti Standardikeskuse 07.12.2007 käskkirjaga nr 203 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 18028-5:2006 "Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks". It has the same status as the official version.

In case of interpretation disputes the English text applies.

SISUKORD

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.

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

ISO/IEC 18028, üldpealkirjaga "Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude 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 privaatvõrkude 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 nendevaheliste 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 kasutamisega. 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 plaanimises, projekteerimises ja teostamises (näiteks võrguhaldureid, administraatoreid, insenere ja võrguturbe ametnikke).

ISO/IEC 18028-3 puudutab kõiki neid töötajaid, kes osalevad turvalüüside detailses plaanimises, 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).

EESTI STANDARD EVS-ISO/IEC 18028-5:2007

INFOTEHNOLOOGIA
Turbemeetodid. Infotehnoloogiavõrkude turve
Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkude abil

Information technology
Security techniques. IT network security
Part 5: Securing communications across networks using virtual private networks

1 KÄSITLUSALA

ISO/IEC 18028 see osa annab detailseid juhiseid turvaaspektide kohta VPN-ühenduste kasutamisel võrkude kokkuühendamiseks või kaugkasutajate ühendamiseks võrkudega. Ta on rajatud võrguhalduse juhistele, mida annab ISO/IEC 18028-1.

Ta on suunatud neile, kes vastutavad selliste tehniliste meetmete valimise ja teostamise eest, mis on vajalikud võrguturbe tagamiseks VPN-ühenduste kasutamisel, ja VPNi turbe sellele järgneva võrguseire eest.

ISO/IEC 18028 see osa annab ülevaate virtuaalsetest privaatvõrkudest, esitab VPNi turvaeesmärgid ja teeb kokkuvõtte VPNi turvanõuetest. Ta annab juhiseid turvaliste VPNide valimise ja rakendamise kohta ning VPNi turbe võrguseire kohta. Ta annab ka teavet tüüpiliste VPNides kasutatavate tehnoloogiate ja protokollide kohta.

2 NORMATIIVVIITED

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

ISO/IEC 7498 (kõik osad) Infotehnoloogia. Avatud süsteemide ühendamine. Etalonmudel. Alusmudel

ISO/IEC 13335-1:2004 Infotehnoloogia. Turbemeetodid. Info- ja sideturbe haldus. Osa 1: Info- ja sideturbe halduse mõisted ja mudelid

ISO/IEC 17799:2005 Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis

ISO/IEC 18028-1:2006 Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 1: Võrguturbe haldus

ISO/IEC 18028-2:2006 Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 2: Võrguturbe arhitektuur

ISO/IEC 18028-3:2006 Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 3: Võrkudevahelise side turve turvalüüside abil

ISO/IEC 18028-4:2006 Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 4: Kaugpöörduse turve.

3 TERMINID JA MÄÄRATLUSED

3.1 Terminid, mis on määratletud teistes rahvusvahelistes standardites

Käesoleva dokumendi otstarbeks kehtivad ISO/IEC 7498 (kõigi osade) terminid ja määratlused ning järgmised standardis ISO/IEC 13335-1 määratletud terminid: jälitatavus, vara, autentsus, käideldavus, etalonmeetmed, konfidentsiaalsus, andme-terviklus, toime, terviklus, turvapoliitika, salgamise vääramine, usaldatavus, risk, riskianalüüs, riskihaldus, (turva)meede, oht ja nõrkus.

3.2 Terminid, mis on määratletud ISO/IEC 18028 selles osas

Käesoleva dokumendi otstarbeks kehtivad järgmised terminid ja määratlused.

3.2.1
kihi 2 kommuteerimine
tehnoloogia, mis ühenduste loomiseks ja ohjeks kihi 2 protokolle kasutavate seadmete vahel kasutab sisemisi kommuteerimismehhanisme

> Märkus. Tavaliselt kasutatakse seda kohtvõrgukeskkonna simuleerimiseks kõrgemate kihtide protokollidele.

3.2.2
kihi 2 VPN
virtuaalne privaatvõrk, mida kasutatakse simuleeritud kohtvõrgukeskkonna loomiseks võrgu infrastruktuuril

> Märkus. Kihi 2 VPNiga kokkuühendatud saidid võivad töötada nii, nagu asuksid nad ühes ja samas kohtvõrgus.

3.2.3
kihi 3 kommuteerimine
tehnoloogia, mis kasutab võrkudevaheliste ühenduste loomiseks ja ohjeks sisemisi kommuteerimise mehhanisme koos tavaliste marsruutimismehhanismidega või rakendab selleks multiprotokoll-märgendkommuteerimise (MPLS) meetodeid

3.2.4
kihi 3 VPN
virtuaalne privaatvõrk, mida kasutatakse simuleeritud laivõrgukeskkonna loomiseks võrgu infrastruktuuril

> Märkus. Kihi 3 VPNiga kokkuühendatud saidid võivad töötada nii, nagu asuksid nad privaatses laivõrgus.

3.2.5
privaatne, privaat-
ainult mingi volitatud grupi liikmeile määratud: VPNide kontekstis iseloomustab VPN-ühenduse kaudu kulgevat liiklust