EESTI STANDARD **EVS-ISO/IEC 27033-4:2015**

Avaldatud eesti keeles: veebruar 2015
Jõustunud Eesti standardina: veebruar 2015

INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 4: Võrkudevahelise side turve turvalüüside abil

Information technology
Security techniques
Network security
Part 4: Securing communications between networks using security gateways
(ISO/IEC 27033-4:2014)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27033-4:2014 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2015. aasta veebruarikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 4 „Infotehnoloogia", standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

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

See standard on rahvusvahelise standardi ISO/IEC 27033-4:2014 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 27033-4:2014. It was 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

SISUKORD

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnikakomisjon) moodustavad ülemaailmse standardimise spetsialiseeritud süsteemi. ISO või IEC rahvuslikud liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendesse organisatsioonidesse loodud käsitlemaks tehnilise tegevuse eri valdkondi. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale huvipakkuvatel aladel. Selles töös osalevad käsikäes ISO ja IEC-ga ka muud rahvusvahelised riiklikud ja mitteriiklikud organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühise tehnilise komitee ISO/IEC JTC 1.

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

Ühise tehnilise komitee põhiülesanne on rahvusvaheliste standardite koostamine. Ühises tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks rahvuslikele kogudele. Avaldamine rahvusvahelise standardina nõuab, et hääletusel osalenud rahvuslikest kogudest kiidaks selle heaks vähemalt 75 %.

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

Standardi ISO/IEC 27033-4 on koostanud ühise tehniline komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbe meetodid“.

See standardi ISO/IEC 27033-4 esimene redaktsioon tühistab ja asendab standardi ISO/IEC 18028-3:2005, olles selle tehniline uustöötlus.

ISO/IEC 27033 koosneb järgmistest osadest üldpealkirjaga „Infotehnoloogia. Turbemeetodid. Võrguturve“ („Information technology — Security techniques — Network security“):

— Osa 1: Ülevaade ja mõisted (Part 1: Overview and concepts);

— Osa 2: Võrguturbe kavandamise ja teostamise juhised (Part 2: Guidelines for the design and implementation of network security);

— Osa 3: Tüüpsed võrgustsenaariumid. Riskid, kavandamismeetodid ja reguleerimisküsimused (Part 3: Reference networking scenarios – Threats, design techniques and control issues);

— Osa 4: Võrkudevahelise side turve turvalüüside abil (Part 4: Securing communications between networks using security gateways);

— Osa 5: Võrkudevahelise side turve virtuaalsete privaatvõrkudega (VPN) (Part 5: Securing communications across networks using Virtual Private Networks (VPNs));

— Osa 6: Traadita IP-võrku pääsu turve (Part 6: Securing wireless IP network access).

(Tuleb pidada silmas, et võib järgneda veel muid osi. Nende osadega kaetavate võimalike teemade hulka kuuluvad näiteks kohtvõrgud, laivõrgud, lairibavõrgud, veebimajutus, Interneti e-post ja marsruuditav juurdepääs kolmandatele organisatsioonidele. Kõigi niisuguste osade põhijaotised peaksid olema „Riskid“, „Kavandamismeetodid“ ja „Reguleerimisküsimused“.)

SISSEJUHATUS

Enamiku äriettevõtete ja riigiasutuste infosüsteemid on ühendatud võrkudega, kusjuures võrguühendus on üks või mitu järgmistest:

— organisatsiooni sees;

— eri organisatsioonide vahel;

— organisatsiooni ja üldsuse vahel.

Üldkasutatava võrgutehnoloogia (eriti Interneti) kiire arengu tõttu, mis pakub olulisi soodsaid ärivõimalusi, arendavad organisatsioonid pealegi üha enam elektroonilist äritegevust ülemaailmses mastaabis ja annavad võrgu kaudu avalikke teenuseid. Soodsate võimaluste hulka kuuluvad andmeside madalam maksumus, Interneti kasutamine lihtsalt ülemaailmse ühendusvahendina ja arenenumad teenused, mida annavad Interneti-teenuste tarnijad (ISP). See võib tähendada suhteliselt odavaid liitumispunkte kanali mõlemas otsas, aga ka täieulatuslikke elektronkaubanduse ja teenusetarne süsteeme, mis kasutavad veebipõhiseid rakendusi ja teenuseid. Peale selle lisab uus tehnoloogia (sealhulgas andmete, kõne ja video integratsioon) kaugtöö (kaugkodutöö) võimalusi. Kaugtöötajad saavad kaugvahendite abil hoida kontakti organisatsiooni ja kogukonna võrkude poole pöördumisel ning nendega seotud tööalase teabe ja teenuste saamisel.

See keskkond soodustab küll kindlasti olulisi ärilisi hüvesid, kuid käsitlemist nõuavad ka uued turvaohud. Kuna organisatsioonide äritegevus sõltub tugevalt teabe ja sellega seotud võrkude kasutamisest, võib teabe ja teenuste konfidentsiaalsuse, tervikluse ja käideldavuse kadu avaldada äritegevusele olulist kahjulikku toimet. Niisiis, on olemas tugev vajadus kaitsta võrke ning nendega seotud infosüsteeme ja teavet. Teisiti öeldes, adekvaatse võrguturbe evitus ja käigushoid on iga organisatsiooni äritegevuse eduks elutähtis.

Selles kontekstis otsivad side ja infotehnoloogia valdkonnad kuluefektiivseid kõikehõlmavaid turvalahendusi, mis on suunatud võrkude kaitsele kuritahtlike rünnete ja tahtmatute väärtoimingute eest, rahuldades seega äritegevuse nõudeid teabe ja teenuste konfidentsiaalsusele, terviklusele ja käideldavusele. Mingi võrgu turve on oluline ka selle võrgu kasutamise õige arvelduse saavutamiseks. Võrgu üldise (sealhulgas rakenduste ja teenuste) turbe seisukohalt on otsustav osa toodete turvaomadustel. Kui aga terviklahenduste saamiseks ühendatakse mitmeid tooteid, määrab lahenduse edu koostalitlusvõime või selle puudumine. Turve peab olema mitte ainult üks iga toote või teenuse hooleaine, vaid seda tuleb arendada nii, et see soodustaks turbevõimete põimumist turbe terviklahenduses.

ISO/IEC 27033-4 „Võrkudevahelise side turve turvalüüside abil“ eesmärk on anda juhiseid selle kohta, kuidas tuvastada ja analüüsida võrgu turvaohte, mis on seotud turvalüüsidega, määratleda ohtude analüüsi põhjal võrguturbe nõuded turvalüüsidele, tutvustada kavandamismeetodeid võrgu tehnilise turbe sellise arhitektuuri saamiseks, mis hoolitseks tüüpiliste võrgustsenaariumidega seotud ohtude ja meetmeaspektide eest ning lahendaks turvalüüside probleemid, mis on seotud võrguturbe meetmete evitamise, käigushoiu, seire ja läbivaatusega.

ISO/IEC 27033-4 puudutab kõiki neid töötajaid, kes osalevad turvalüüside detailses plaanimises, kavandamises ja teostamises (näiteks võrguarhitekte ja -projekteerijaid, võrguhaldureid ja võrguturbe ametnikke).

Taotluslikult tühjaks jäetud

1 KÄSITLUSALA

ISO/IEC 27033 see osa annab juhiseid võrkudevahelise side turbeks turvalüüside (tulemüüride, rakenduste tulemüüride, sissetungi tuvastuse süsteemi vm) abil vastavalt turvalüüside dokumenteeritud infoturvapoliitikale, sealhulgas selle kohta, kuidas

a) tuvastada ja analüüsida võrgu turvaohte, mis on seotud turvalüüsidega;

b) ohtude analüüsi põhjal määratleda võrguturbe nõudeid turvalüüsidele;

c) kasutada kavandamis- ja teostamismeetodeid tüüpiliste võrgustsenaariumidega seotud ohtude ja meetmeaspektide käsitlemiseks;

d) käsitleda probleeme, mis on seotud võrgu turvalüüsi turvameetmete evitamise, käigushoiu, seire ja läbivaatusega.

2 NORMVIITED

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 27033 1. Information technology – Security techniques – Network security – Part 1: Overview and concepts

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardis ISO/IEC 27033-1 ning alljärgnevalt esitatud termineid ja määratlusi.

3.1
bastion (*bastion host*)
tugevdatud operatsioonisüsteemiga eriarvuti, mida kasutatakse sisenevate ja väljuvate pakettide püügiks mingis võrgus ning süsteemis, millega harilikult tuleb igal väljaspoolsel ühenduda mingi teenuse saamiseks, või süsteemis, mis asub organisatsiooni tulemüüris

specific host with hardened operation system that is used to intercept packets entering or leaving a network and the system that any outsider must normally connect with to access a service or a system that lies within an organization's firewall

3.2
tarkvarapõhine lõpptulemüür (*end-point software-based firewall*)
ühelainsal arvutil töötav tarkvararakendus, mis kaitseb selle arvuti sisenevat ja väljuvat võrguliiklust, lubades ja keelates sidet lõppkasutaja määratletud turvapoliitika põhjal

software application running on a single machine, protecting network traffic into and out of that machine to permit or deny communications based on an end user-defined security policy

3.3
tugevdatud operatsioonisüsteem (*hardened operating system*)
operatsioonisüsteem, mis on konfigureeritud või kavandatud spetsiaalselt minimeerima rikkumise või ründe võimalust

MÄRKUS Operatsioonisüsteem võib olla sellise keskkonna jaoks konfigureeritud üldotstarbeline (näiteks Linux) või individualiseeritum lahendus.