Avaldatud eesti keeles: mai 2013
Jõustunud Eesti standardina: mai 2013

INFOTEHNOLOOGIA
Turbemeetodid
Võrguturve
Osa 3: Tüüpsed võrgustsenaariumid
Riskid, kavandamismeetodid ja reguleerimisküsimused

Information technology
Security techniques
Network security
Part 3: Reference networking scenarios
Threats, design techniques and control issues
(ISO/IEC 27033-3:2010)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27033-3:2010 inglisekeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2013. aasta maikuu 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 27033-3:2010 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 27033-3:2010. 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: andmesidevõrkude turve, turvaohud võrgus, võrguturbe meetodid
Hinnagrupp P

SISUKORD

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 vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Ühendatud tehnilise komitee põhiülesanne on rahvusvaheliste standardite koostamine. Ühendatud tehnilises komitees 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 ja IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27033-3 on koostanud ISO/IEC ühendatud tehnilise komitee JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Turbemeetodid“.

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

— Osa 1: Ülevaade ja mõisted

— Osa 2: Võrguturbe kavandamise ja teostamise juhised

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

Koostamisel on alljärgnevad osad:

— Osa 4: Võrkudevahelise side turve turvalüüside abil. Ohud, kavandamismeetodid ja reguleerimisküsimused

— Osa 5: Virtuaalsete privaatvõrkude turve. Ohud, kavandamismeetodid ja reguleerimisküsimused

Edaspidi võib lisanduda uusi osi, mis hõlmavad kohtvõrke, laivõrke, traadita ja raadiovõrke, lairibavõrke, kõnevõrke, IP-konvergentsvõrke (andmed, kõne, video), veebimajutuse arhitektuure, Interneti-meili arhitektuure (sh väljuvat siduspääsu Internetti ja sisenevat pääsu Internetist), marsruuditavat pääsu kolmanda osapoole organisatsioonidesse, ja muid sarnaseid teemasid.

1 KÄSITLUSALA

ISO/IEC 27033 selles osas on kirjeldatud tüüpsete võrgustsenaariumidega seotud ohte, kavandamismeetodeid ja reguleerimisküsimusi. Iga stsenaariumi tarbeks antakse juhiseid turvaohtude kohta ning nendega seotud riskide vähendamiseks vajalike turbe kavandamise meetodite ja turvameetmete kohta. Sobivates kohtades on viidatud standardiosadele ISO/IEC 27033-4, ISO/IEC 27033-5 ja ISO/IEC 27033-6 nende sisu dubleerimise vältimiseks.

ISO/IEC 27033 selles osas olevast teabest on kasu tehnilise turbe arhitektuuri ja/või lahenduse valikuvõimaluste läbivaatamisel ning tehnilise turbe eelisarhitektuuri või -lahenduse ja sellekohaste turvameetmete valimisel ja dokumenteerimisel ISO/IEC 27033-2 järgi. Millist teavet konkreetselt valida (koos teabega, mis valitakse osadest ISO/IEC 27033-4, -5 ja -6), sõltub läbivaadatava võrgukeskkonna karakteristikutest, s.t konkreetse(te)st võrgustsenaariumi(de)st ja tehnoloogiateema(de)st.

Üldiselt on ISO/IEC 27033 see osa oluliselt abiks turbe igakülgsel määratlemisel ja teostamisel igasuguse organisatsiooni võrgukeskkonnas.

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 27000. Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27033-1. Information technology — Security techniques — Network security — Part 1: Overview and concepts

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardites ISO/IEC 27000 ja ISO/IEC 27033-1 ning alljärgnevalt esitatud termineid ja määratlusi.

3.1
kahjurvara (*malware*, *malicious software*)
liik tarkvara, mis on kavandatud pahatahtliku kavatsusega ja sisaldab niisuguseid erijooni või võimeid, mis võivad põhjustada otseselt või kaudselt kahju kasutajale ja/või kasutaja arvutisüsteemile

MÄRKUS Vt ISO/IEC 27032.

category of software that is designed with a malicious intent, containing features or capabilities that could potentially cause harm directly or indirectly to the user and/or the user's computer system

NOTE See ISO/IEC 27032.

3.2
läbipaistmatus (*opacity*)
sellise teabe kaitstus, mida saaks tuletada võrgutoimingute vaatluse teel, näiteks tuletades VoIP-kõne ots-punktide aadresse

MÄRKUS Läbipaistmatus eeldab vajadust kaitsta lisaks teabele ka toiminguid.

protection of information that might be derived by observing network activities, such as deriving addresses of end-points in a voice-over-Internet-Protocol call

NOTE Opacity recognizes the need to protect actions in addition to information.