Avaldatud eesti keeles: veebruar 2018
Jõustunud Eesti standardina: veebruar 2018

INFOTEHNOLOOGIA
Turbemeetodid
Küberturbe juhised

Information technology
Security techniques
Guidelines for cybersecurity
(ISO/IEC 27032:2012, identical)

EESTI STANDARDIKESKUS EVS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27032:2012 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate avaldamisega EVS Teataja 2018. 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 AS Cybernetica, standardi on heaks kiitnud EVS/TK 4.

See standard on rahvusvahelise standardi ISO/IEC 27032:2012 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 27032:2012. 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 35.030

SISUKORD

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) 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 muud rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Infotehnoloogia alal on ISO ja IEC loonud ühendatud tehnilise komitee ISO/IEC JTC 1.

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

Ühise tehnilise komitee ISO/IEC JTC 1 põhiülesanne on rahvusvaheliste standardite koostamine. Ühises 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 objekt. ISO ega IEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

Standardi ISO/IEC 27032 on koostanud ISO/IEC ühise tehnilise komitee JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbe meetodid“.

SISSEJUHATUS

Küberruum on keerukas keskkond, mis tuleneb inimeste, tarkvara ja teenuste interaktsioonist Internetis, toetatuna ülemaailmsete hajusa info- ja sidetehnoloogia füüsiliste seadmetega ja ühendatud võrkudega. On aga turvaprobleeme, mida ei kata praegused infoturbe, Interneti-turbe, võrguturbe ning info- ja sidetehnoloogia turbe parimad tavad, sest nende alade vahel on lünki ning küberruumis puudub suhtlus organisatsioonide ja tarnijate vahel, sest küberruumi seni toetanud seadmetel ja ühendatud võrkudel on mitmeid omanikke, igal neist oma äri-, käitus- ja regulatsioonimured. Igal organisatsioonil ja tarnijal küberruumis on asjassepuutuvatel turvaaladel erinev huvipunkt, mis võtab vähe või ei võta üldse lähtematerjali teiselt organisatsioonilt või tarnijalt ning tulemuseks on küberruumi turbe killustatus.

Sellest lähtudes on selle standardi esmases huvipunktis küberruumi turvalisuse või küberturbe nende probleemide käsitlus, mis keskenduvad lünkade täitmisele küberruumi eri turvaalade vahel. Konkreetsemalt, see standard annab tehnilisi juhiseid tegelemaks üldiste küberturvariskidega, mille hulka kuuluvad

— inimestega manipuleerivad ründed,

— häkkimine,

— ründetarkvara (kahjurvara) vohamine,

— nuhkvara,

— muu potentsiaalselt soovimatu tarkvara (nugivara).

Tehnilised juhised pakuvad meetmeid nende riskide käsitluseks, sealhulgas meetmeid, millega:

— valmistuda rünneteks, mille tekitajad on näiteks kahjurvara või kuritegelikud isikud või organisatsioonid Internetis;

— avastada ja seirata ründeid;

— reageerida rünnetele.

Teine selle standardi huvipunkt on koostöö, sest on vaja riskiosaliste tõhusat ja toimivat teabejagamist, koordineerimist ja intsidendikäsitlust küberruumis. Seda koostööd tuleb teha turvaliselt ja usaldatavalt, nii et oleks kaitstud ka asjaosaliste privaatsus. Paljud neist riskiosalistest võivad paikneda eri asukohtades ja ajavööndites ning tõenäoliselt alluvad erinevatele regulatiivnõuetele. Riskiosaliste hulka kuuluvad

— tarbijad, kelleks võivad olla mitut liiki organisatsioonid või isikud;

— tarnijad, sealhulgas teenuseandjad.

Niisiis annab see standard ka ühe karkassi

— teabe jagamiseks,

— koordineerimiseks,

— intsidendikäsitluseks.

Sellesse karkassi kuuluvad

— kesksed usalduse loomise kaalutluste elemendid,

— koostööks ning teabevahetuseks ja -jagamiseks vajalikud protsessid,

— tehnilised nõuded süsteemide integreerimiseks ja koostalitluseks eri riskiosaliste vahel.

Standardi käsitlusala arvestades on pakutavad meetmed tingimata mingil üldisel tasemel. Täiendava juhatuse saamiseks on selles standardis viidatud igale alale kohaldatavatele detailsetele tehniliste spetsifikatsioonide standarditele ja juhistele.

1 KÄSITLUSALA

See standard annab juhiseid küberturvalisuse seisundi täiustamiseks, tuues esile selle tegevuse ainuomased tahud ning ta sõltuvused muudest turbealadest, sealhulgas

— infoturbest,

— võrguturbest,

— võrgustikuturbest,

— elutähtsa teabetaristu kaitsest (CIIP).

Standard hõlmab riskiosaliste etalonturbe tavasid küberruumis, andes

— ülevaate küberturbest,

— ühe seletuse küberturbe ja muude turbeliikide vahelise seose kohta,

— riskiosaliste määratluse ja nende küberruumirollide kirjelduse,

— juhiseid üldiste küberturvaküsimuste käsitluseks,

— ühe karkassi, millega võimaldada riskiosaliste koostööd küberturvaküsimuste lahendamisel.

2 KOHALDATAVUS

2.1 Lugejaskond

See standard on kohaldatav teenusetarnijaile küberruumis, lugejaskond aga hõlmab ka nende teenuste kasutajaist tarbijaid. Kui organisatsioonid annavad küberruumis teenuseid inimestele kodus kasutamiseks või teistele organisatsioonidele, võib neil olla vaja koostada sellel standardil põhinevaid juhiseid, mis sisaldaksid nende mõistmiseks ja nende järgi tegutsemiseks piisavaid lisaseletusi või näiteid lugejale.

2.2 Kitsendused

See standard ei käsitle

— küberohutust,

— küberkuritegevust,

— elutähtsa taristu kaitset,

— Interneti ohutust,

— Internetiga seotud kuritegevust.

On teada, et mainitud alade ja küberturbe vahel on seosed, kuid nende käsitlus ja nende aladega ühised meetmed jäävad selle standardi käsitlusalast välja.

Oluline on silmas pidada, et küberkuritegevuse mõistet on küll mainitud, kuid ei käsitleta. See standard ei anna juhiseid küberruumi õiguslike aspektide ega küberturbe reguleerimise kohta.

Juhised selles standardis piirduvad küberruumi realiseeringuga Internetis, otspunktid kaasa arvatud. Ei käsitleta aga küberruumi laienemist sidevahendite ja -platvormide kaudu muudele ruumesitustele ega nende füüsilise turbe aspektidele.

NÄIDE 1 Ei käsitleta küberruumi alustugedeks olevaid taristuelemente, näiteks sidekandjaid.

NÄIDE 2 Ei käsitleta küberruumiga infosisu allalaadimiseks ja/või manipuleerimiseks ühendatavate mobiiltelefonide füüsilist turvet.

NÄIDE 3 Ei käsitleta mobiiltelefonide tekstsõnumi- ja kõnekonverentsifunktsioone.

3 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

4 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse standardis ISO/IEC 27000 ning alljärgnevalt esitatud termineid ja määratlusi.

4.1
reklaamvara (*adware*)
rakendus, mis suunab kasutajaile reklaami ja/või kogub andmeid kasutajate võrgukäitumise kohta

MÄRKUS See rakendus võidakse installeerida kasutaja teadmisel või nõusolekul või selleta või olla sunnitud kasutajale peale muu tarkvara litsentsitingimuste kaudu.

application which pushes advertising to users and/or gathers user online behaviour

NOTE The application may or may not be installed with the user's knowledge or consent or forced onto the user via licensing terms for other software.

4.2
rakendus (*application*)
organisatsioonis mingi tegevusprotsessi või funktsiooni automatiseerimise teel kasutajaid teatud tööde sooritamisel või teatud tüüpi IT-probleemide käsitlemisel abistama kavandatud IT-lahendus, mis sisaldab rakendustarkvara, rakendusandmeid ja protseduure

IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

[ISO/IEC 27034-1:2011]

4.3
rakendusteenuse tarnija (*application service provider*)
operaator, kes annab mingit rakendusteenuseid pakkuvat majutatud tarkvaralahendust, mis sisaldab veebipõhiseid või klient-server-tüüpi väljastusmudeleid

NÄIDE Võrgustatud mängu operaator, kontorirakenduse andjad, võrgus talletuse tarnijad.

operator who provides a hosted software solution that provides application services which includes web based or client-server delivery models

EXAMPLE Online game operators, office application providers and online storage providers.

