Avaldatud eesti keeles: september 2012
Jõustunud Eesti standardina: september 2012

INFOTEHNOLOOGIA
Turbemeetodid
Infoturvaintsidentide haldus

Information technology
Security techniques
Information security incident management
(ISO/IEC 27035:2011)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27035:2011 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina sellekohase teate ilmumisega EVS Teataja 2012. aasta septembrikuu 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 27035:2011 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 27035:2011. 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: infoturvaintsidendid, infoturvaintsidentide haldus, infoturvaintsidentidele reageerimise rühm, infoturvanõrkused, turvakriminalistika
Hinnagrupp W

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 ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Ühise tehnilise komitee 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 subjekt. ISOt ega IEC-d ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

Standardi ISO/IEC 27035 on koostanud ühendatud tehnilise komitee ISO/IEC JTC 1 „Infotehnoloogia“ alamkomitee SC 27 „Infoturbemeetodid“.

See ISO/IEC 27035 esimene redaktsioon tühistab ja asendab ISO/IEC TR 18044:2004, olles selle tehniline uustöötlus.

SISSEJUHATUS

Üldiselt ei taga pelgalt infoturvapoliitikad või turvameetmed teabe, infosüsteemide, infoteenuste ega infovõrkude täielikku kaitstust. Pärast turvameetmete kasutuselevõttu jääb tõenäoliselt jääknõrkusi, mis võivad teha infoturbe toimetuks ja seega võimaldada infoturvaintsidentide toimumist. Sellel võib olla nii otseselt kui ka kaudselt kahjulik toime organisatsiooni äritegevusele. Lisaks hakkavad ilmnema seni tuvastamatud ohud. Kui organisatsioon ei ole selliste intsidentide käsitluseks piisavalt ette valmistunud, on igasugune reageerimine neile vähem mõjus ning suureneb võimalik kahjulik toime äritegevusele. Seega on oluline, et igal infoturvet tõsiselt võtval organisatsioonil oleks struktureeritud ja plaanitud metoodika, millega

- avastada infoturvaintsidente, neist teatada ja neid hinnata;
- reageerida infoturvaintsidentidele, sealhulgas rakendades sobivaid meetmeid kahjulike toimete vältimiseks ja vähendamiseks ning neist toibumiseks (nt kriisihalduse alade toeks);
- teatada infoturvanõrkustest, mida pole veel ära kasutatud infoturvasündmuste ja võib-olla ka infoturvaintsidentide põhjustamiseks, neid hinnata ja asjakohaselt käsitleda;
- õppida infoturvaintsidentidest ja nõrkustest, rajada preventiivseid meetmeid ning täiustada üldist infoturbehalduse metoodikat.

Standard annab infoturvaintsidentide halduse kohta juhiseid jaotistes 4 kuni 9. Need jaotised koosnevad mitmest alajaotisest, kus kirjeldatakse üksikasjalikult iga järku.

Termin „infoturvaintsidentide haldus“ hõlmab selles standardis mitte ainult infoturvaintsidentide, vaid ka infoturvanõrkuste haldust.

1 KÄSITLUSALA

See standard annab struktureeritud ja plaanitud metoodika, millega

a) avastada infoturvaintsidente, neist teatada ja neid hinnata;

b) reageerida infoturvaintsidentidele ja hallata neid;

c) avastada, hinnata ja hallata infoturvanõrkusi;

d) infoturvaintsidentide ja -nõrkuste haldamise tulemusena täiustada pidevalt infoturvaintsidentide ja -nõrkuste haldust.

See standard annab juhiseid suurtele ja keskmistele organisatsioonidele infoturvaintsidentide halduse kohta. Väiksemad organisatsioonid võivad kasutada selles standardis kirjeldatud dokumentide, protsesside ja rutiinide põhikomplekti vastavalt oma suurusele ja tegevusala tüübile sõltuvalt infoturvariskilisest olukorrast. Standard annab juhiseid ka välistele organisatsioonidele, kes osutavad infoturvaintsidentide halduse teenuseid.

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

3 TERMINID JA MÄÄRATLUSED

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

3.1
turvakriminalistika (*information security forensics*)
juurdluse ja analüüsi meetodite rakendamine infoturvaintsidentide tuvastuseks, jäädvustamiseks ja analüüsimiseks

application of investigation and analysis techniques to capture, record and analyse information security incidents

3.2
infoturvaintsidentidele reageerimise rühm (*information security incident response team*)
ISIRT
sobivate oskustega usaldatavate liikmete rühm organisatsioonist, mis käsitleb infoturvaintsidente nonde elutsükli jooksul

MÄRKUS Selles standardis kirjeldatud ISIRT on organisatsiooni talitus, mis katab infoturvaintsidentide protsessi ja keskendub peamiselt infotehnoloogiaga seotud intsidentidele. Muudel (sarnaste lühenditega) üldistel intsidendikäsitluse talitustel võib olla veidi teistsugune käsitlusala ja eesmärk. Järgmistel üldkasutatavail lühenditel on ISIRTi omaga sarnane, kuid mitte täpselt sama tähendus.

- CERT (Computer Emergency Response Team): arvutiavariide tõrje rühm; keskendub peamiselt info- ja sidetehnoloogia intsidentidele. Eri maades võib olla muid CERTi määratlusi.
- CSIRT (Computer Security Incident Response Team): arvutiturvaintsidentidele reageerimise rühm on teenindusorganisatsioon, kelle ülesanne on võtta vastu ja vaadata läbi arvutiturvaintsidentide teatisi ja vastavaid tegevusi ning neile reageerida. Neid teenuseid antakse tavaliselt mingile määratletud tarbijaskonnale, milleks võib olla mingi katusorganisatsioon (korporatsioon, riigiasutus, haridusasutus), piirkond või riik, teadusasutuste võrk, maksev klient.