Avaldatud eesti keeles: august 2024
Jõustunud Eesti standardina: august 2024

INFOTEHNOLOOGIA
Infoturvaintsidentide haldus
Osa 1: Põhimõtted ja protsess

Information technology
Information security incident management
Part 1: Principles and process
(ISO/IEC 27035-1:2023, identical)

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27035-1:2023 ingliskeelse teksti sisu poolest identne tõlge eesti keelde [ja sellel on sama staatus mis ümbertrüki meetodil vastu võetud originaalversioonil]. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles augustis 2024;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta augustikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 04 „Infotehnoloogia“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Standardi on tõlkinud Teabering OÜ, standardi on heaks kiitnud EVS/TK 04.

Standardi mõnedele sätetele on lisatud Eesti olusid arvestavaid märkusi, selgitusi ja täiendusi, mis on tähistatud Eesti maatähisega EE.

See standard on rahvusvahelise standardi ISO/IEC 27035-1:2023 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO/IEC 27035-1:2023. It was translated by the Estonian Centre for Standardisation and Accreditation. 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 (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad ka ISO-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (vt www.iso.org/directives või www.iec.ch/members_experts/refdocs).

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. ISO ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest. Dokumendi väljatöötamise jooksul väljaselgitatud või selgunud patendiõiguste üksikasjad on esitatud peatükis „Sissejuhatus“ ja/või ISO-le saadetud patentide deklaratsioonide loetelus (vt www.iso.org/patents) või IEC-le saadetud patentide deklaratsioonide loetelus (vt https://patents.iec.ch).

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused standardite vabatahtliku kasutuse ja vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil www.iso.org/iso/foreword.html ja IEC-s aadressil www.iec.ch/understanding-standards.

Selle dokumendi eest vastustab tehnilise komitee ISO/IEC JTC 1 „Information technology“ alamkomitee SC 27 „Information security, cybersecurity and privacy protection“.

Teine väljaanne tühistab ja asendab esimest väljaannet (ISO/IEC 27035-1:2016), mis on tehniliselt üle vaadatud.

Peamised muudatused on järgnevad:

— pealkiri on muudetud;

— uued terminid „intsidendi haldusrühm“ ja „intsidendi koordinaator“ on määratletud peatükis 3;

— uued jaotised 4.5, 4.6 ja 4.7 on lisatud peatükki 4;

— peatüki 5 uus pealkiri on “Protsess”;

— Lisa C on uuendatud;

— uus Lisa D on lisatud;

— teksti on toimetatud.

Standardisarja ISO/IEC 27035 kõikide osade loetelu on leitav ISO ja IEC veebilehtedelt.

Igasugune tagasiside või küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav veebilehelt www.iso.org/members.html ja www.iec.ch/national-committees.

SISSEJUHATUS

Standardisari ISO/IEC 27035 annab täiendavaid juhiseid intsidendihalduse meetmete kohta standardis ISO/IEC 27002. Neid meetmeid tuleks rakendada lähtuvalt infoturvariskidest, millega organisatsioon silmitsi seisab.

Infoturvapoliitika või -meetmed üksi ei taga teabe, infosüsteemide, teenuste või võrkude täielikku kaitset. Pärast meetmete rakendamist jäävad tõenäoliselt alles nõrkused, mis võivad vähendada infoturbe tõhusust ja hõlbustada infoturvaintsidentide esinemist. Sellel võivad olla otsesed ja kaudsed negatiivsed tagajärjed organisatsiooni äritegevusele. Lisaks on vältimatu, et uued, varem tuvastamata ohtude juhtumid põhjustavad intsidente. Organisatsiooni ebapiisav ettevalmistus selliste intsidentidega tegelemiseks muudab reageerimise vähem tõhusaks ja suurendab potentsiaalsete negatiivsete tagajärgede ulatust äritegevusele. Seetõttu on oluline, et iga organisatsioonil, mis soovib tugevat infoturbekava, oleks struktureeritud ja kavandatud lähenemisviis järgmistele küsimustele:

— infoturvaintsidentide haldamise kavandamine ja ettevalmistus, sealhulgas poliitika, korraldus, plaan, tehniline tugi, teadlikkuse ja oskuste koolitus jne;

— infoturvaintsidentide ja intsidendiga seotud nõrkuste avastamine, nendest teatamine ja hindamine;

— infoturbeintsidentidele reageerimise viis, sealhulgas asjakohaste meetmete aktiveerimine

— mõju ennetamiseks, vähendamiseks ja sellest taastumiseks;

— asjakohaselt teatatud intsidendiga seotud infoturvanõrkuste käsitlemine;

— infoturvaintsidentidest ja intsidendiga seotud nõrkustest õppimine, ennetavate meetmete rakendamine ning infoturvaintsidentide haldamisele üldise lähenemisviisi täiustamine.

ISO/IEC 27035 sari on mõeldud täiendama teisi standardeid ja dokumente, mis annavad juhiseid infotuvaeintsidentide uurimise ja nende uurimise ettevalmistamise kohta. ISO/IEC 27035 sari ei ole kõikehõlmav juhend, vaid viide teatud aluspõhimõtetele ja määratletud protsessile, mille eesmärk on tagada, et tööriistu, tehnikaid ja meetodeid saab sobivalt valida ning vajaduse korral näidata, et need sobivad infotuvaeintsidentide uurimise otstarbeks.

Kuigi ISO/IEC 27035 sari hõlmab infoturvaintsidentide haldamist, hõlmab see ka mõningaid infoturbe nõrkuste aspekte. Juhised nõrkuste avalikustamise ja nõrkuste käsitlemise kohta tarnijate poolt on esitatud ka vastavalt standardites ISO/IEC 29147 ja ISO/IEC 30111.

ISO/IEC 27035 sari eesmärk on anda teadmisi otsustajatele neile esitatud digitaalsete tõendite usaldusväärsuse kindlaksmääramisel. See on rakendatav organisatsioonidele, kes peavad kaitsma, analüüsima ja esitama potentsiaalseid digitaalseid tõendeid. See on oluline poliitikakujundajate jaoks, kes loovad ja hindavad digitaalsete tõenditega, mis on sageli osa suuremast tõendusmaterjalist, seotud protseduure.

Lisateavet uurimisstandardite kohta leiate lisast A.

Taotluslikult tühjaks jäetud

1 KÄSITLUSALA

See dokument on ISO/IEC 27035 sarja standardite alusdokument. Selles esitatakse infoturvaintsidentide haldamise põhitegevuste kontseptsioonid, põhimõtted ja protsessid, mis pakuvad struktureeritud lähenemisviisi, kuidas valmistuda intsidentide avastamiseks, aruandluseks, hindamiseks ja neile reageerimiseks ning saadud kogemuste rakendamiseks.

Selles dokumendis antud infoturvaintsidentide haldusprotsessi ja selle põhitegevuste juhendid on üldised ja mõeldud kohaldamiseks kõikidele organisatsioonidele, olenemata nende tüübist, suurusest või olemusest. Organisatsioonid saavad kohandada juhiseid vastavalt oma tüübile, suurusele ja äritegevuse iseloomule seoses infoturvariskidega. See dokument kehtib ka infoturvaintsidentide haldusteenuseid pakkuvate väliste organisatsioonide kohta.

2 NORMIVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

EVS-EN ISO/IEC 27000:2020. Infotehnoloogia — Turbemeetodid — Infoturbe halduse süsteemid — Ülevaade ja sõnavara.

3 TERMINID JA MÄÄRATLUSED

Dokumendi rakendamisel kasutatakse standardis ISO/IEC 27000 ning allpool esitatud termineid ja määratlusi.

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogiaandmebaase järgmistel aadressidel:

— ISO Online browsing platform: veebiaadressil https://www.iso.org/obp

— IEC Electropedia: veebiaadressil https://www .electropedia .org/

EE MÄRKUS Eestikeelsete terminite aluseks on Andmekaitse ja infoturbe leksikon https://akit.cyber.ee/.

3.1 Mõisted, määratlused ja lühendid

3.1.1
intsidendi haldusrühm (*incident management team* IMT)
meeskond, mis koosneb asjakohaselt kvalifitseeritud ja usaldusväärsetest organisatsiooni liikmetest, kes vastutavad kõigi infoturvaintsidentide haldamise tegevuste eest kooskõlastatult teiste osapooltega nii sise- kui ka väliste intsidentide elutsükli jooksul.

MÄRKUS Selle meeskonna juhti võib nimetada intsidendihalduriks, kelle tippjuhtkond on määranud asjakohaselt reageerima igat tüüpi intsidentidele.

3.1.2
intsidendi reageerimisrühm (*incident response team* IRT)
sobivalt kvalifitseeritud ja usaldusväärsetest liikmetest koosnev meeskond, kes reageerib intsidentidele ja lahendab neid koordineeritult.

MÄRKUS 1 IRT-sid võib olla mitu, üks intsidendi iga aspekti jaoks.

