EESTI STANDARD EVS-ISO/IEC 27032:2024

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

KÜBERTURVE
Juhised Interneti turbeks

Cybersecurity
Guidelines for Internet security
(ISO/IEC 27032:2023, identical)

EVS • EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO/IEC 27032:2023 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 mais 2024;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2024. aasta maikuu 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 Cybernetica AS, standardi on heaks kiitnud EVS/TK 04.

See standard on rahvusvahelise standardi ISO/IEC 27032:2023 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 27032:2023. 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) ja IEC (International Electrotechnical Commission) moodustavad ülemaailmse standardimise kohandatud süsteemi. Rahvuslikud organisatsioonid, kes on ISO või IEC liikmed, osalevad rahvusvaheliste standardite väljatöötamisel asjakohase organisatsiooni loodud tehniliste komiteede kaudu, mille eesmärk on tegeleda konkreetsete tehniliste valdkondadega. ISO ja IEC tehnilised komiteed teevad koostööd mõlemale organisatsioonile huvi pakkuvates valdkondades. Selles töös osalevad ka muud ISO-ga ja IEC-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused.

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

ISO ja IEC pööravad tähelepanu võimalusele, et selle dokumendi rakendamine võib olla seotud patendi (patentide) kasutamisega. ISO ega IEC ei võta seisukohta mis tahes esitatud patendiõiguste tõendamise, kehtivuse ega rakendatavuse eest. Selle dokumendi avaldamise kuupäeva seisuga ei ole ISO ega IEC saanud teateid patendi (patentide) kohta, mida võib vaja minna selle dokumendi rakendamiseks. Dokumendi kasutajaid on siiski hoiatatud, et siin esitatu ei pruugi olla uusim teave, mis võib olla saadud patendiandmebaasist (kättesaadav veebilehtedelt www.iso.org/patents ja https://patents.iec.ch). ISO ega IEC ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

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

Selgitused standardite vabatahtliku kasutuse kohta 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. IEC korral vt www.iec.ch/understanding-standards.

Selle dokumendi on koostanud ühendatud 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 27032:2012), mis on tehniliselt üle vaadatud.

Peamised muudatused on järgmised:

— pealkiri on muudetud;

— dokumendi struktuuri on muudetud;

— riski kaalutlemise ja riskikäsitluse lähenemisviisi on muudetud, Interneti turvariskide tuvastuseks ja halduseks on lisatud sisu ohtude, nõrkuste ja ründevektorite kohta;

— lisasse A on lisatud jaotises 9.2 esitatud Interneti turvameetmete ja standardis ISO/IEC 27002 esitatud turvameetmete vaheline vastendus.

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

SISSEJUHATUS

See dokument keskendub Interneti turvaküsimuste käsitlemisele ja annab juhiseid selliste tavaliste Interneti turvaohtude käsitlemiseks, nagu on

— ründed suhtluskunstiga;

— nullpäevaründed;

— privaatsuse ründed;

— häkkimine ning

— kahjuliku tarkvara (kahjurvara), nuhkvara ja muu nugivara levik.

Juhised selles dokumendis esitavad Interneti turvariskide käsitluseks tehnilisi ja muid turvameetmeid, hõlmates meetmeid, millega

— valmistuda rünneteks;

— ründeid vältida;

— ründeid avastada ja seirata;

— rünnetele reageerida.

Juhised keskenduvad ala headele tavadele ning laialdasele tarbijate ja töötajate õpetamisele, aitamaks huvipooltel täita aktiivset rolli Interneti turvaprobleemide käsitlemisel. Dokument keskendub ka Interneti kaudu kulgeva teabe konfidentsiaalsuse, tervikluse ja käideldavuse ning muude lisanduda võivate omaduste, näiteks autentsuse, jälitatavuse, salgamatuse ja usaldatavuse säilitamisele.

See hõlmab Interneti turvajuhiseid

— rollide,

— poliitikate,

— meetodite,

— protsesside ja

— rakendatavate tehniliste turvameetmete kohta.

Selle dokumendi käsitlusala arvestades on esitatud turvameetmed paratamatult üldjoonelised. Igale alale kohaldatavaile detailse tehnilise spetsifitseerimise standarditele ja juhistele on edasiseks juhendamiseks viidatud selle dokumendi sees. Lisa A esitab vastavuse selles dokumendis nimetatud meetmete ja standardi ISO/IEC 27002 omade vahel.

See dokument ei käsitle eraldi neid meetmeid, mida organisatsioon võib vajada elutähtsa taristu või riigi julgeoleku toetuseks. Sellistes süsteemides aga saab rakendada enamikku selles dokumendis mainitud meetmeist.

See dokument kasutab seniseid standardis ISO/IEC 27002, ISO/IEC 27033 sarjas, tehnilises spetsifikatsioonis ISO/IEC TS 27100 ja standardis ISO/IEC 27701 esitatud kontseptsioone illustreerimaks

— seoseid Interneti turbe, veebiturbe, võrguturbe ja küberturbe vahel;

— detailjuhiseid jaotises 9.2 nimetatud Interneti turvameetmete kohta, käsitledes Internetile avatud süsteemide küberturbevalmidust.

Tehnilises spetsifikatsioonis ISO/IEC TS 27100 mainituna on Internet ülemaailmne võrk, mida organisatsioonid kasutavad kogu oma sideks, nii digitaalseks kui ka kõnesideks. Võttes arvesse, et mõned kasutajad suunavad nende võrkude vastu ründeid, on oluline hoolitseda asjasse puutuvate turvariskide eest.

1 KÄSITLUSALA

See dokument esitab

— Interneti turbe, veebiturbe, võrguturbe ja küberturbe vaheliste seoste seletuse;

— ülevaate Interneti turbest;

— huvipoolte piiritluse ja kirjelduse nende rollidest Interneti turbes;

— üldjoonelised juhised tavaliste Interneti turvaküsimuste käsitluseks.

See dokument on mõeldud Internetti kasutavatele organisatsioonidele.

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.

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

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 veebipõhine lugemisplatvorm: kättesaadav veebilehelt https://www.iso.org/obp;

— IEC Electropedia: kättesaadav veebilehelt https://www.electropedia.org/.

3.1
ründevektor (*attack vector*)
tee või vahend ründaja juurdepääsuks arvutile või võrguserverile pahatahtliku tagajärje tekitamiseks

NÄIDE 1 Esemevõrgu seadmed.

NÄIDE 2 Nutitelefonid.

3.2
ründaja (*attacker*)
isik, kes sihilikult kasutab ära tehniliste ja muude turvameetmete nõrkusi varguseks infosüsteemides ja -võrkudes või nende rikkumiseks või infosüsteemi- ja võrguressursside lubatava kasutamise käideldavuse rikkumiseks

[ALLIKAS: ISO/IEC 27033-1:2015, 3.3]

3.3
segarünne (*blended attack*)
rünne, mis mitut ründevektorit (3.1) kombineerides püüab maksimeerida kahjustuse tõsidust ja laostamise kiirust

