Avaldatud eesti keeles: märts 2011
Jõustunud Eesti standardina: märts 2011

See dokument on EVS-i poolt loodud eelvaade

INFOTEHNOLOOGIA
Turbemeetodid
Infoturbe hindamise kriteeriumid
Osa 1: Sissejuhatus ja üldmudel

Information technology
Security techniques
Evaluation criteria for IT security
Part 1: Introduction and general model

(ISO/IEC 15408:2009)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard:

– on rahvusvahelise standardi ISO/IEC 15408-1:2009 „Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model“ ingliskeelse teksti identne tõlge eesti keelde ning tõlgendamise erimeelsuste korral tuleb lähtuda ametlikus keeles avaldatud tekstist,

– on kinnitatud Eesti Standardikeskuse 10.02.2011 käskkirjaga nr 29;

– on jõustunud sellekohase teate avaldamisel EVS Teataja 2011. aasta märtsikuu numbris.

Standardi tõlkis Cybernetica AS, standardi tõlke on heaks kiitnud EVS/TK 4 „Infotehnoloogia“.

Standardi tõlke koostamisettepaneku esitas EVS/TK 4, standardi tõlkimist korraldas Eesti Standardikeskus ning rahastas Majandus- ja Kommunikatsiooniministeerium.

See dokument on EVS-i poolt loodud eelvaade

ICS 35.040 Märgistikud ja informatsiooni kodeerimine
Võtmesõnad: infotehnoloogia, arvutivõrk, infoturve, infoturbe haldus
Hinnagrupp V

Standardite reprodutseerimis- ja levitamisõigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonilisse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:
Aru 10, 10317 Tallinn, Eesti; www.evs.ee; telefon: 605 5050; e-post: info@evs.ee

SISUKORD

EESSÕNA IV
SISSEJUHATUS V
1 KÄSITLUSALA 1
2 NORMIVIITED 1
3 TERMINID JA MÄÄRATLUSED 1
3.1 ISO/IEC 15408 üldised terminid ja määratlused 1
3.2 Klassiga ADV seotud terminid ja määratlused 9
3.3 Klassiga AGD seotud terminid ja määratlused 12
3.4 Klassiga ALC seotud terminid ja määratlused 13
3.5 Klassiga AVA seotud terminid ja määratlused 16
3.6 Klassiga ACO seotud terminid ja määratlused 17
4 TERMINILÜHENDID 17
5 ÜLEVAADE 18
5.1 Üldist 18
5.2 Hindamisobjekt (TOE) 18
5.3 ISO/IEC 15408 sihtgrupp 20
5.4 ISO/IEC 15408 osad 21
5.5 Hindamise kontekst 21
6 ÜLDMUDEL 22
6.1 Üldmudeli sissejuhatuseks 22
6.2 Varad ja vastumeetmed 22
6.3 Hindamine 26
7 TURVANÕUETE KOHANDAMINE 26
7.1 Operatsioonid 26
7.2 Komponentide vahelised sõltuvused 29
7.3 Laiendkomponendid 29
8 KAITSEPROFIILID JA PAKETID 30
8.1 Sissejuhatus 30
8.2 Paketid 30
8.3 Kaitseprofiilid 30
8.4 Kaitseprofiilide ja pakettide kasutamine 33
8.5 Liitprofiilide kasutamine 33
9 HINDAMISE TULEMUSED 33
9.1 Sissejuhatus 33
9.2 Kaitseprofiilide hindamise tulemused 34
9.3 Turvasihtide ja hindamisobjektide hindamise tulemused 34
9.4 Vastavusdeklaratsioon 34
9.5 Turvasihtide ja hindamisobjektide hindamise tulemuste kasutamine 36
Lisa A (teatmelisa) Turvasihtide spetsifikatsioon 37
Lisa B (teatmelisa) Kaitseprofiilide spetsifikatsioon 53
Lisa C (teatmelisa) Juhised operatsioonide kohta 59
Lisa D (teatmelisa) Kaitseprofiili vastavus 62
Kasutatud kirjandus 64

See dokument on EVS-i poolt loodud eelvaade

EESSÕNA

ISO (Rahvusvaheline Standardimisorganisatsioon) ja IEC (Rahvusvaheline Elektrotehnika Komisjon) moodustavad spetsialiseeritud ülemaailmse standardimise süsteemi. ISO või IEC eri maade liikmeskogud osalevad rahvusvaheliste standardite väljatöötamises tehniliste komiteede kaudu, mis on nendes organisatsioonides rajatud, et käsitleda 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 mitteriiklikud organisatsioonid. Infotehnoloogia valdkonnas on ISO ja IEC rajanud ühise tehnilise komitee ISO/IEC JTC 1.

Rahvusvahelised standardid kavandatakse vastavalt ISO/IEC direktiivide 2. osas esitatud reeglitele.

Ühise tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Ühises tehnilises komitees heakskiidetud rahvusvahelised standardikavandid saadetakse maade liikmeskogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab vähemalt 75% hääletanud liikmeskogude heakskiitu.

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõned osad võivad olla patendiõiguse subjektiks. ISOt ega IEC-d ei saa pidada vastutavaks mõne või kõigi selliste patendiõiguste väljaselgitamise osas.

Standardi ISO/IEC 15408-1 on koostanud ühise tehnilise komitee ISO/IEC JTC 1 (infotehnoloogia) alamkomitee SC 27 (turbemeetodid). ISO/IEC 15408 omaga identse teksti on Ühiskriteeriumide projekti sponsor-organisatsioonid avaldanud pealkirjaga „Infoturbe hindamise ühiskriteeriumid“. Mõlema publikatsiooni ühine XML-kuju asub aadressil http://www.oc.ccn.cni.es/xml.

Käesolev kolmas redaktsioon tühistab ja asendab teise redaktsiooni (ISO/IEC 15408-1:2005), mis on tehniliselt redigeeritud.

ISO/IEC 15408 üldpealkirjaga „Infotehnoloogia. Turbemeetodid. Infoturbe hindamise kriteeriumid“ koosneb järgmistest osadest:

— *Osa 1. Sissejuhatus ja üldmudel*

— *Osa 2. Funktsionaalsed turvakomponendid*

— *Osa 3. Tagatislikud turvakomponendid*

See dokument on EVS-i poolt loodud eelvaade

SISSEJUHATUS

ISO/IEC 15408 teeb võimalikuks sõltumatute turbe hindamiste tulemite võrreldavuse. Selleks annab see ühe üldise nõudestiku IT-toodete turvafunktsioonistiku kohta ning turbe tagamise meetmed, mida neile IT-toodetele rakendatakse turbe hindamise käigus. Need IT-tooted võivad olla rakendatud riistvaras, püsivaras või tarkvaras.

Hindamisprotsess selgitab välja teatava usaldusmäära selle kohta, kas niisuguste IT-toodete turvafunktsioonistik ja neile rakendatavad kindlusmeetmed vastavad neile nõuetele. Hindamistulemused võivad aidata tarbijail otsustada, kas hinnatavad IT-tooted rahuldavad nende turvavajadusi.

ISO/IEC 15408 on kasulik juhend turvafunktsioonidega IT-toodete väljatöötamiseks, hindamiseks ja/või soetamiseks.

ISO/IEC 15408 on kavandatud paindlikuna ning võimaldab rakendada tervet rida hindamismeetodeid terve rea IT-toodete tervele reale turvaomadustele. Standardi kasutajad peaksid olema ettevaatlikud, et standardi paindlikkust mitte kuritarvitada. Näiteks võib ISO/IEC 15408 kasutamine ebasobivate hindamismeetodite, asjakohatute turvaomaduste või ebasobivate IT-toodete puhul viia tarbetute hindamistulemusteni.

Sellel, et mingit IT-toodet on hinnatud, on tähendus ainult hinnatud turvaomaduste ja kasutatud hindamismeetodite kontekstis. Otsustamiseks, kas hindamine annab mõttekaid tulemusi, on hindamisorganeil soovitatav hoolikalt kontrollida tooteid, omadusi ja meetodeid. Seda konteksti on soovitatav arvestada ka hinnatud toodete soetajail, et otsustada, kas toode on kasulik ja rakendatav konkreetsele olukorrale ja vajadustele.

ISO/IEC 15408 käsitleb varade kaitset lubamatu avalikustamise, muutmise või kasutuskõlbmatuse eest. Üldiselt nimetatakse turvalisuse rikkumise nende kolme tüübiga seotud kaitse kategooriaid vastavalt konfidentsiaalsuseks, terviklikkuseks ja käideldavuseks. ISO/IEC 15408 võib peale nende kolme olla rakendatav ka infoturbe muudele aspektidele. ISO/IEC 15408 on rakendatav riskidele, mida tekitavad nii (pahatahtlikud või muud) inimtegevused kui ka muud tegevused. Standard ISO/IEC 15408 ei taotle rakendatavust teistel IT aladel peale infoturbe, kuid seda võidakse nendes rakendada.

Teatud teemad loetakse väljaspool ISO/IEC 15408 käsitlusala olevaiks nendega kaasnevate erimeetodite või mõningase perifeersuse tõttu infoturbe suhtes. Mõned neist on loetletud järgnevalt.

a) ISO/IEC 15408 ei sisalda turbe hindamise kriteeriume, mis puudutavad IT turvafunktsioonidega otseselt mitteseotud halduslikke turvameetmeid. On aga arvestatud sellega, et sageli võidakse olulist turvet saavutada või toetada halduslike, näiteks korralduslike, personalialaste, füüsiliste ja protseduuriliste meetmetega.

b) Infoturbe mõningate füüsiliste tehniliste aspektide (näiteks elektromagnetilise kiirguse ohje) hindamist ei ole konkreetselt hõlmatud, kuid selles valdkonnas saab rakendada paljusid käsitletud mõisteid.

c) ISO/IEC 15408 ei käsitle hindamismetoodikat, millega tuleks nimetatud kriteeriume rakendada. Selle metoodika annab ISO/IEC 18045.

d) ISO/IEC 15408 ei käsitle halduslikku ega õiguslikku raamstruktuuri, mille tingimustes võivad hindamisorganid rakendada nimetatud kriteeriume. Eeldatakse aga, et standardit ISO/IEC 15408 kasutatakse hindamise eesmärkidel mingi sellise raamstruktuuri kontekstis.

e) Protseduurid hindamistulemite kasutamiseks akrediteerimisel jäävad ISO/IEC 15408 käsitlusalast välja. Akrediteerimine on halduslik protsess, millega antakse õigus käitada IT-toodet (või toodete kogumit) selle täielikus käituskeskkonnas, sisaldades ka kõiki IT-väliseid osi. Hindamisprotsessi tulemid sisestatakse akrediteerimise protsessi. Et aga IT-väliste omaduste ning nende ja IT turvaosade vahelise seose hindamiseks on sobivamaid meetodeid, peaksid akrediteerijad seadma neile aspektidele eraldi tingimusi.

f) ISO/IEC 15408 ei hõlma krüptograafiliste algoritmide olemuslike omaduste hindamise kriteeriume. Kui peaks olema vajadus krüptograafia matemaatilisi omadusi sõltumatult hinnata, peaks sellise hindamise tingimused seadma see hindamisskeem, mille raames rakendatakse standardit ISO/IEC 15408.

Eeldokument on EVS-i poolt koostatud eelvaade

Kogu dokumendi ulatuses kasutatud ISO terminoloogia, nagu „saab“, „teatmeline“, „võib“, „normatiivne“, „peab, tuleb“ ja „peaks, tuleks“, on määratletud ISO/IEC direktiivide 2. osas. Tuleb silmas pidada, et terminil „peaks, tuleks“ on lisatähendus, mis on rakendatav käesoleva standardi kasutamisel (vt märkus allpool). Termini „peaks, tuleks“ kasutamiseks standardis ISO/IEC 15408 kehtib järgnev määratlus:

peaks, tuleks (*should*)

normatiivses tekstis näitab „peaks, tuleks“, et „mitme võimaluse hulgast on üks eriti sobiv, nimetamata või välistamata muid, või et teatav teguviis on eelistatud, kuid mitte tingimata nõutav.“ (ISO/IEC direktiivid, 2. osa).

MÄRKUS ISO/IEC 15408 tõlgendab fraasi „mitte tingimata nõutav“ tähendust nii: muu võimaluse valimine nõuab põhjendust selle kohta, miks ei valitud eelistatavat võimalust.

See dokument on EVS-i poolt loodud eelvaade

1 KÄSITLUSALA

ISO/IEC 15408 selles osas kehtestatakse infoturbe hindamise üldmõisted ja põhimõtted ning määratakse kindlaks hindamise üldmudel, mis on esitatud standardi eri osades ning mis on tervikuna mõeldud kasutamiseks IT-toodete turvaomaduste hindamise alusena.

Standardi ISO/IEC 15408 esimeses osas kirjeldatakse standardi kõiki osi, määratletakse terminid ja lühendid, mida kasutatakse kõigis osades, kehtestatakse hindamisobjekti (*Target of Evaluation* - TOE) tuummõiste, määratakse hindamise kontekst ja kirjeldatakse lugejaskonda, kellele on hindamise kriteeriumid suunatud. Sissejuhatavalt kirjeldatakse põhilisi turvamõisteid, mis on vajalikud IT-toodete hindamiseks.

Standard määratleb mitmesugused operatsioonid, millega saab lubatavate operatsioonide kasutamise teel kohandada funktsionaalseid ja tagatislikke komponente, mis on esitatud standardi osades ISO/IEC 15408-2 ja ISO/IEC 15408-3.

Esitatud on kaitseprofiilide (PP) tuummõisted, turvanõuete paketid ja vastavuse teema ning kirjeldatud on hindamise tagajärgi ja tulemeid. ISO/IEC 15408 käesolev, esimeses osas antakse suunised turvasihtide (ST) spetsifitseerimiseks ja kirjeldatakse komponentide korraldust kogu mudeli ulatuses. Hindamismetoodika üldteave ja hindamisskeemide käsitlusala on standardis ISO/IEC 18045.

2 NORMIVIITED

Järgmised dokumendid on vajalikud ISO/IEC 15408 käesoleva osa rakendamiseks. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse järgmisi termineid ja määratlusi.

MÄRKUS See jaotis sisaldab ainult neid termineid, mida kasutatakse eritähenduses kogu standardis ISO/IEC 15408. Mõnesid selles standardis kasutatud üldiseid terminikombinatsioone ei ole selles jaotises määratletud, kuid selguse mõttes on need kasutuskontekstis selgitatud.

3.1 ISO/IEC 15408 üldised terminid ja määratlused

3.1.1
kahjulikud toimingud (*adverse actions*)
toimingud, mida ohuagent sooritab mingi vara suhtes

3.1.2
varad (*assets*)
olemid, mis hindamisobjekti omanikule on eeldatavalt väärtuslikud

3.1.3
kinnistamine (*assignment*)
(ISO/IEC 15408) komponendis või nõudes tuvastatud parameetri spetsifitseerimine

3.1.4
tagatis (*assurance*)
alus veendumiseks, et hindamisobjekt vastab funktsionaalsetele turvanõuetele

See dokument on EVS poolt loodud eelvaade