RAHANDUSTEENUSED
Infoturbe suunised

Financial services
Information security guidelines

EESTI STANDARDIKESKUS

EESTI STANDARDI EESSÕNA

Käesolev Eesti standard sisaldab rahvusvahelise standardiorganisatsiooni ISO tehnilise aruande ISO/TR 13569:2005 “Financial services – Information security guidelines” identse tõlke eesti keelde.

Standardi tõlkis Cybernetica AS.

Standardi kavandi on heaks kiitnud infotehnoloogia standardimise tehniline komitee EVS/TK 4.

Rahvusvaheline tehniline aruanne ISO/TR 13569:2005 on avaldatud Eesti standardina EVS-ISO/TR 13569:2006, mis on kinnitatud Eesti Standardikeskuse 15.12.2006 käskkirjaga nr 179.

Standard jõustub selle kohta EVS Teataja 2007. aasta jaanuarikuu numbris teate avaldamisega.

This standard contains an identical Estonian translation of the English text of the International Technical Report ISO/TR 13569:2005 “Financial services – Information security guidelines”.
The International Technical Report ISO/TR 13569:2005 has the status of an Estonian National Standard.

SISUKORD

EESSÕNA

ISO (Rahvusvaheline Standardiorganisatsioon) on ülemaailmne eri maade standardiorganite (ISO liikmeskogude) föderatsioon. Töö rahvusvaheliste standardite koostamiseks sooritatakse tavaliselt ISO tehniliste komiteede kaudu. Igal liikmeskogul, mis on huvitatud mingist valdkonnast, mille tarbeks on rajatud tehniline komitee, on õigus olla esindatud selles komitees. Selles töös osalevad käsikäes ISO-ga ka muud rahvusvahelised, riiklikud ja mitteriiklikud organisatsioonid. Kõigis elektrotehnilise standardimise küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

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

Tehnilise komitee peamine ülesanne on koostada rahvusvahelisi standardeid. Tehnilises komitees vastuvõetud rahvusvahelised standardikavandid saadetakse rahvuslikele liikmeskogudele hääletamiseks. Avaldamine rahvusvahelise standardina nõuab heakskiitu vähemalt 75% hääletanud rahvuslikelt liikmeskogudelt.

Erandasjaoludel, kui tehniline komitee on kogunud andmeid, mis laadilt erinevad harilikult rahvusvahelise standardina avaldatavaist (näiteks senise tehnikataseme andmeid), võib ta oma osavõtvate liikmete liht-häälteenamusega otsustada avaldada tehnilise aruande. Tehniline aruanne on oma loomult täielikult teatmeline ega kuulu läbivaatusele enne temas sisalduvate andmete tunnistamist kehtetuiks või kasutuiks.

Tuleb pöörata tähelepanu võimalusele, et mõned selle dokumendi elemendid võivad olla patendiõiguse objektiks. ISO ei ole kohustatud mingeid või kõiki selliseid patendiõigusi välja selgitama.

ISO/TR 13569 koostas tehniline komitee ISO/TC 68 “Rahandusteenused” alamkomitee SC 2 “Turbehaldus ja üldine pangandustegevus”.

Käesolev kolmas redaktsioon tühistab ja asendab teise redaktsiooni (ISO/TR 13569:1997), olles selle uustöötlus. Selle koosseisu kuulub ka ISO/TR 13569:1997/Amd. 1:1998.

SISSEJUHATUS

Koos arvuti- ja võrgupõhise tehnoloogia kasutuselevõtuga on muutunud rahandusala tavad. Kasvanud sõltuvus elektroonilistest tehingutest on suurendanud vajadust hallata info- ja sidetehnoloogia turvalisust. Äripoliitikatel põhinevate turvatavadega reguleeritavate elektroonilise side mehhanismide kaudu kantakse iga päev üle tohutuid summasid rahas ja väärtpaberitena.

Selliste tehingute suur väärtus ja juba ainuüksi maht üha ulatuslikumalt ühendatud avatud keskkonnas avab rahandusala võimalikele ränkadele tagajärgedele. Kokkuühendatud võrgud ning pahatahtlike vastaste üha suurem arv ja arukus raskendavad seda riski pankadele ja nende klientidele toimimise võimalusega. Kui aga rahandustehingud süstemaatiliselt hõlmavad tähtsaid maksesüsteeme, võivad sellised tagajärjed negatiivselt mõjutada sisemaiseid ja ülemaailmseid rahandusturge.

Vajadus laiendada äritegevust nendesse keskkondadesse ja tulla toime riskiga nõuab tugevat ja toimivat ettevõtte infoturbekava. Rahandusasutused peavad haldama selliseid kavasid igakülgselt, nii nagu nad haldavad riski väljakujunenud äritavade ja lepetega, ülesannete täitmise hoolika väljasttellimisega, kindlustusega ja sobivate turvameetmete kasutamisega. Peale selle tuleb neil oma turvakavasid kujundada nii, et need arvestaksid muutuvaid riske ja nõudeid, mis tulenevad laienevast riiklikust ja rahvusvahelisest õiguslikust ja regulatiivsest keskkonnast.

Baseli leping hoiatab meid, et tegevusalased, õiguslikud ja regulatiivsed riskid võivad põhjustada või suurendada krediidi- ja likviidsusriske. Nende riskide haldamine on tõusnud rahandusasutuse infoturbekavas keskse kohale. Iga asutus peab oma riskidele avatuse tundmiseks tõlgendama neid riske omaenda äritegevuse seisukohalt. Hoolikalt tuleb arvestada tegevusriske, sealhulgas kelmust ja kuritegevust, loodusõnnetusi ja terroriakte. Väikese tõenäosusega sündmused, näiteks Aasiat 2004. aasta detsembris vapustanud tsunami ja terroristide ründed New York City rahandusasutustele üheteistkümnendal septembril 2001. aastal, juhtuvad kindlasti ja nende puhuks tuleb plaanida.

Käesolev tehniline aruanne on mõeldud kasutamiseks igasuguse suurusega ja igat tüüpi rahandusasutustele, kellel on vaja rakendada ettenägelikku ja majanduslikult mõistlikku infoturbe halduse kava. Ta annab kasulikke juhiseid ka rahandusasutuste teenusetarnijaile ning võib olla allikdokumendiks rahandusala teenindavatele õppejõududele ja kirjastajatele.
Selle tehnilise aruande eesmärgid on

- määratleda infoturbe halduse kava;
- esitada selle kava poliitika, organisatsioon ja vajalikud struktuurikomponendid;
- pakkuda turvameetmete valimise kohta juhiseid, mis esindavad aktsepteeritud ettenägelikke äritavasid rahandusrakendustes;
- teavitada rahandusasutuste juhtkonda vajadusest süstemaatiliselt käsitleda oma infoturbe halduse kavas õiguslikke ja regulatoorseid riske.

Käesolev tehniline aruanne pole mõeldud andma kõigile rahandusteenuste asutustele mingit ainsat üldist lahendust. Iga organisatsioon peab sooritama riskianalüüsi ja valima sobivad meetmed. See tehniline aruanne annab selle protsessi läbiviimiseks suuniseid, mitte konkreetseid lahendusi.

Taotluslikult tühjaks jäetud

EESTI STANDARD EVS-ISO/TR 13569:2006

RAHANDUSTEENUSED
Infoturbe suunised

Financial services
Information security guidelines

1 KÄSITLUSALA

Käesolev tehniline aruanne annab rahandusasutustele suuniseid infoturbekava väljatöötamiseks. Ta sisaldab sellise kava poliitikate, organisatsiooni ning struktuuriliste, õiguslike ja regulatiivsete komponentide käsitluse. Vaadeldakse turvameetmete ning nüüdisaegses rahandusasutuses infoturberiski halduseks vajalike elementide valimise ja teostuse kaalutlusi. Antakse soovitusi, mis põhinevad asutuse ärikeskkonna, tavade ja protseduuride arvestamisel. Nendes juhistes käsitletakse ka õiguslikele ja regulatiivsetele nõuetele vastavuse küsimusi, mida tuleks arvestada kava koostamisel ja elluviimisel.

2 NORMATIIVVIITED

Käesoleva dokumendi rakendamisel on vältimatud järgnevad viidatud dokumendid. Dateeritud viidete puhul on kohaldatav ainult viidatud versioon. Dateerimata viidete puhul kehtib viidatud normdokumendi uusim redaktsioon (koos võimalike muudatustega).

ISO 9564 (kõik osad). Pangandus. Personaalsete identifitseerimisnumbrite (PIN) haldus ja turve

ISO 10202 (kõik osad). Rahandustehingukaardid. Integraallülituskaarte kasutavate rahandustehingusüsteemide turvaarhitektuur

ISO 11568 (kõik osad). Pangandus. Võtmehaldus (jaepanganduses)

ISO/IEC 11770 (kõik osad). Infotehnoloogia. Turbemeetodid. Võtmehaldus

ISO 15782 (kõik osad). Sertifikaatide haldus rahandusteenustes

ISO 16609:2004. Pangandus. Nõuded sümmeetrilisi meetodeid kasutavale sõnumite autentimisele

ISO/IEC 17799. Infotehnoloogia. Turbemeetodid. Infoturbe halduse tegevusjuhis

ISO/IEC 18028 (kõik osad). Infotehnoloogia. Turbemeetodid. Infotehnoloogia võrgturve

ISO/IEC 18033 (kõik osad). Infotehnoloogia. Turbemeetodid. Krüpteerimisalgoritmid

ISO 21188. Avaliku võtme infrastruktuur rahandusteenustes. Tavad ja poliitika raamstruktuur.

3 TERMINID JA MÄÄRATLUSED

3.1
a) pääsu reguleerimine; (*access control*)
b) pääsuregulaator
funktsioonid, mis piiravad juurdepääsu teabele või infotöötlusvahenditele ja võimaldavad saada juurdepääsu ainult selleks volitatud isikutel või rakendustel, sealhulgas füüsilised pääsuregulaatorid, mis põhinevad füüsiliste tõkete paigutamisel volitamata isikute ja kaitstava inforessursi vahele, ja loogilised pääsuregulaatorid, mis rakendavad muid vahendeid

3.2
jälitatavus (*accountability*)
omadus, mis tagab, et mingi olemi toiminguid saab üheselt jälitada selle olemini
[ISO 7498-2; ISO/IEC 13335-1:2004, määratlus 2.1]

3.3
alarm (*alarm*)
viivitamatut tähelepanu nõuda võiva turvarikke või ebahariliku või ohtliku olukorra indikatsioon

3.4
vara (*asset*)
miski, millel on organisatsiooni jaoks väärtus
[ISO/IEC 13335-1:2004, määratlus 2.2]

3.5
a) audit; (*audit*)
b) revisjon
funktsioon, mis püüab kontrollida turvameetmete olemasolu ja otstarbekust ning teatab puudustest asjakohasele haldustasemele

3.6
revisjonipäevik (*audit journal*)
süsteemi tegevuste kronoloogiline jäädvustis, mis on piisav, et võimaldada rekonstrueerida, läbi vaadata ja uurida keskkondade ja toimingute jada, mis ümbritseb iga sündmust tehingu teel ta algatamisest kuni lõpptulemuste väljastuseni või mis viib selle sündmuseni
[ISO 15782-1:2003, määratlus 3.3]