KOMISJONI RAKENDUSOTSUS (EL) 2017/2288,

11. detsember 2017,

mis käsitleb selliste IKT tehniliste kirjelduste kindlaksmääramist, millele riigihangetes viidata

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrust (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ, ([1]) eriti selle artikli 13 lõiget 1,

pärast IKT standardimist käsitleva Euroopa sidusrühmade platvormi ja valdkondlike ekspertidega konsulteerimist

ning arvestades järgmist:

(1) Standardimisel on strateegia „Euroopa 2020“ eesmärkide saavutamisel täita oluline roll ([2]). Mitmes strateegia „Euroopa 2020“ juhtalgatuses rõhutatakse toote- ja teenusteturgudel toimuva vabatahtliku standardimise olulisust, et tagada toodete ja teenuste vaheline kokkusobivus ja koostalitlusvõime ning edendada tehnika arengut ja toetada innovatsiooni.

(2) Standardid on Euroopa konkurentsivõime, innovatsiooni ja arengu seisukohast ülimalt olulised. Komisjoni teatised, mis käsitlevad ühtset turgu ([3]) ja digitaalset ühtset turgu, ([4]) kinnitavad ühiste standardite olulisust, et tagada Euroopa digitaalses majanduses võrkude ja süsteemide vajalik koostalitlusvõime. Seda toetati teatise vastuvõtmisega IKT standardimise prioriteetide kohta, ([5]) milles komisjon määras kindlaks digitaalse ühtse turu väljakujundamiseks esmatähtsad info- ja kommunikatsioonitehnoloogiad, mille puhul peetakse standardimist väga oluliseks.

(3) Komisjoni teatises „Euroopa standardeid käsitlev strateegiline visioon: Euroopa majanduse jätkusuutliku kasvu edendamine ja kiirendamine 2020. aastaks“ ([6]) tunnistatakse info- ja kommunikatsioonitehnoloogia (edaspidi „IKT“) valdkonna standardimise eripära: selles valdkonnas tegelevad lahenduste, rakenduste ja teenuste väljatöötamisega sageli üleilmsed IKT foorumid ja konsortsiumid, mis on praegu juhtivad IKT standardiorganisatsioonid.

(4) Määrusega (EL) nr 1025/2012, mis käsitleb Euroopa standardimist, on loodud süsteem, mille kohaselt võib komisjon valida välja kõige sobivamad ja laialdasemalt heakskiidetud IKT tehnilised kirjeldused, mille on väljastanud organisatsioonid, mis ei kuulu Euroopa, rahvusvaheliste või riiklike standardimisorganisatsioonide hulka; selle võib võtta aluseks, et tagada koostalitlusvõime riigihangete puhul. Võimalus kasutada riistvara, tarkvara ja infotehnoloogiateenuste hangetes võimalikult paljusid IKT tehnilisi kirjeldusi võimaldab tagada seadmete, teenuste ja rakenduste koostalitlusvõime, aitab ametiasutustel vältida seotust, mis tekib, kui avaliku sektori hankija ei saa pärast hankelepingu tähtaja lõppemist muuta toote või teenuse pakkujat firmaomaste IKT-lahenduste kasutamise tõttu, ning see soodustab konkurentsi koostalitlusvõimeliste IKT-lahenduste pakkumisel.

(5) Selleks et IKT tehnilistele kirjeldustele saaks riigihangetes viidata, peavad need vastama määruse (EL) nr 1025/2012 II lisas sätestatud nõuetele. Nende nõuete täitmine on ametiasutustele tagatiseks, et IKT tehnilised kirjeldused on kehtestatud kooskõlas Maailma Kaubandusorganisatsiooni poolt standardimise valdkonnas tunnustatud avatuse, läbipaistvuse, erapooletuse ja üksmeele põhimõtetega.

([1]) ELT L 316, 14.11.2012, lk 12.
([2]) Komisjoni teatis pealkirjaga „Euroopa 2020. aastal: Aruka, jätkusuutliku ja kaasava majanduskasvu strateegia“. COM(2010) 2020 (final), 3. märts 2010.
([3]) Komisjoni teatis „Ühtse turu täiustamine: rohkem võimalusi inimestele ja ettevõtetele“. COM(2015) 550 (final), 28. oktoober 2015.
([4]) Teatis Euroopa digitaalse ühtse turu strateegia kohta. COM(2015) 192 (final), 6. mai 2015.
([5]) COM(2016) 176 (final), 19. aprill 2016.
([6]) COM (2011) 311 (final), 1 juuni 2011.

(6) Otsus IKT kirjelduste kindlaksmääramise kohta võetakse vastu pärast komisjoni otsusega 2011/C 349/04 ([1]) loodud IKT standardimist käsitleva Euroopa sidusrühmade platvormiga konsulteerimist, millele lisaks on peetud täiendavaid konsultatsioone valdkonna ekspertidega.

(7) IKT standardimist käsitlev Euroopa sidusrühmade platvorm hindas järgmisi tehnilisi kirjeldusi ja esitas pooldava arvamuse selle kohta, et võtta need riigihangetes aluseks: „SPF-Sender Policy Framework for Authorizing Use of Domains in Email“ („SPF“, „STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security („STARTTLS-SMTP“)“ ja „DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security („DANE- SMTP“)“, mille on välja töötanud Interneti Tehniline Operatiivkogu (IETF); „Structured Threat Information Expression („STIX 1.2“) ja „Trusted Automated Exchange of Indicator Information („TAXII 1.1“)“, mille on välja töötanud struktureeritud teabe standardite edendamise organisatsioon (OASIS). Seejärel esitati platvormi hinnang ja soovitused konsulteerimiseks valdkondlikele ekspertidele, kes kinnitasid pooldavat arvamust nende väljavalimise kohta.

(8) IETFi välja töötatud tehniline kirjeldus „SPF“ on avatud standard, mis kirjeldab võltsitud saatja aadressi avastamise tehnilist meetodit. SPF pakub võimalust kontrollida, kas sõnum on saadetud selleks autoriseeritud serverilt. See on lihtne e-posti aadressi valideerimise süsteem, mis on ette nähtud e-kirjade võltsimise avastamiseks mehhanismi abil, mis võimaldab e-kirja saajal kontrollida, kas domeenilt saabunud e-kiri pärineb hostinime alt, mille on autoriseerinud selle domeeni administraatorid. SPFi eesmärk on takistada rämpspostisaatjatel saata sõnumeid konkreetse domeeni võltsitud saatja aadressiga. E-kirja saaja saab kasutada SPFi kirjet, et teha kindlaks, kas sõnum, mis väidab, et saabub sellelt domeenilt, on pärit autoriseeritud meiliserverilt.

(9) IETFi väljatöötatud STARTTLS-SMTP on meetod, et muuta olemasolev ebaturvaline ühendus turvaliseks ühenduseks. STARTTLS on lihtsa meiliedastusprotokolli (SMTP) teenuse laiendus, mis võimaldab SMTP serveril ja kliendil kasutada transpordikihi turbeprotokolli (TLS), et tagada internetis privaatne autenditud teabevahetus. Eelkõige e-posti teel toimuv ebaturvaline suhtlus on peamine ründevektor valitsusasutuste võrkudesse sissemurdmisel. Kui kasutaja saadab e-kirja, saadab kasutaja meiliteenuse pakkuja meiliserver selle e-kirja saaja meiliserverile. Nende meiliserverite vahelise ühenduse saab eelnevalt TLSiga turvaliseks muuta. STARTTLS pakub võimalust muuta krüpteerimata (lihtteksti kujul) ühendus krüpteeritud TLS-ühenduseks.

(10) IETFi väljatöötatud DANE-SMTP on interneti turvalisuse parandamise protokollistik, mis võimaldab paigutada domeeninimede süsteemi võtmeid ja neid DNSSECi abil (DNSi turvalaiendid) abil turvata. Tundmatu isikuga turvalise ühenduse loomiseks on soovitav saatja ja sihtkoha autentsuse veebipõhine kontrollimine. Seda saab teha sertifikaatide abil, mille sertifitseerimisasutused on PKI-süsteemi raames välja andnud, või iseallkirjastatud sertifikaatide abil. DANE võimaldab domeeninime valdajal (registreerijal) anda DNSSECiga turvatud DNS-kirje kaudu täiendavat teavet lisaks internetisertifikaatidele. DANE on seepärast eriti oluline võitluses aktiivsete ründajate vastu.

(11) OASISe väljatöötatud STIX 1.2 on küberohte käsitlevat teavet standarditud ja struktureeritud viisil kirjeldav keel. See hõlmab küberohu andmetega seotud peamisi küsimusi ja lihtsustab analüüsi ja rünnakutega seotud teabevahetust. Sellega kirjeldatakse põhjalikult küberohuga seotud teavet, kaasa arvatud ründetegevuse indikaatoreid, nagu rünnetega seotud IP-aadressid ja failide räsiväärtused ning taustainfo, näiteks ründetaktika, -tehnika ja -toimingud; nõrkuste ärakasutamise sihtmärgid; kampaaniad ja tegevuse käik (ingl k Campaigns and Courses of Action ehk COA). Kogu see teave iseloomustab täielikult küberünnakute motivatsioone, võimekust ja tegevust ning aitab seega kaitsta rünnakute vastu.

(12) TAXII v1.1 on samuti OASISe väljatöötatud tehniline kirjeldus, millega standarditakse küberohu teabe usaldusväärne ja automaatne vahetamine. TAXII määrab kindlaks teenused ja sõnumite vahetamise küberohuga seotud kasutuskõlbliku teabe jagamiseks organisatsioonide, toodete või teenuste üleselt, et avastada, vältida ja leevendada küberohte. TAXII võimaldab organisatsioonidel saavutada tekkimisjärgus ohtude osas parema olukorrateadlikkuse ja annab neile võimaluse teavet kergesti oma partneritega jagada, kasutades samas olemasolevaid suhteid ja süsteeme,

([1]) Komisjoni 28. novembri 2011. aasta otsus 2011/C 349/04, millega luuakse IKT standardimist käsitlev Euroopa sidusrühmade platvorm (ELT C 349, 30.11.2011, lk 4).

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Riigihangetes võib viidata lisas loetletud tehnilistele kirjeldustele.

Artikkel 2

Käesolev otsus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Brüssel, 11. detsember 2017

Komisjoni nimel
president
Jean-Claude JUNCKER

LISA

Interneti Tehniline Operatiivkogu (IETF)

Nr	IKT tehnilise kirjelduse nimetus
1	SPF-Sender Policy Framework
2	STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security
3	DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (TLS)

Struktureeritud teabe standardite edendamise organisatsioon (OASIS)

Nr	IKT tehnilise kirjelduse nimetus
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information