KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2017/2288

2017 m. gruodžio 11 d.

dėl IRT techninių specifikacijų, kuriomis remiamasi vykdant viešuosius pirkimus, nustatymo

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2012 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 1025/2012 dėl Europos standartizacijos, kuriuo iš dalies keičiamos Tarybos direktyvos 89/686/EEB ir 93/15/EEB ir Europos Parlamento ir Tarybos direktyvos 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB ir 2009/105/EB ir panaikinamas Tarybos sprendimas 87/95/EEB ir Europos Parlamento ir Tarybos sprendimas Nr. 1673/2006/EB ([1]), ypač į jo 13 straipsnio 1 dalį,

pasikonsultavusi su IRT standartizacijos srities Europos įvairių suinteresuotųjų šalių platforma ir su šio sektoriaus ekspertais,

kadangi:

(1) standartizacija turi didelę reikšmę įgyvendinant strategiją „Europa 2020“ ([2]). Keliose strategijos „Europa 2020“ pavyzdinėse iniciatyvose pabrėžta savanoriškos standartizacijos svarba produktų ar paslaugų rinkose, kad būtų užtikrintas produktų ir paslaugų suderinamumas bei sąveikumas, skatinama technologinė plėtra ir remiamos inovacijos;

(2) standartai yra labai svarbūs Europos konkurencingumui ir nepaprastai reikalingi inovacijoms ir pažangai. Komisijos komunikatai dėl bendrosios rinkos ([3]) ir dėl bendrosios skaitmeninės rinkos ([4]) patvirtina bendrų standartų svarbą siekiant užtikrinti Europos skaitmeninės ekonomikos tinklų ir sistemų sąveikumą. Ši svarba padidinama priėmus komunikatą dėl IRT standartizacijos prioritetų ([5]), kuriame Komisija nurodo prioritetines IRT technologijas, kurių standartizacija yra itin svarbi bendrajai skaitmeninei rinkai sukurti;

(3) Komisijos komunikate „Strateginė Europos standartų vizija. Tolesni tvaraus Europos ekonomikos augimo iki 2020 m. skatinimo ir spartinimo veiksmai“ ([6]) pripažintas informacinių ir ryšių technologijų (IRT) srities standartizacijos savitumas, nes sprendimai, taikomosios programos ir paslaugos dažnai būna parengti pasaulinių IRT forumų ir konsorciumų, šiuo metu pirmaujančių IRT standartus rengiančių organizacijų;

(4) Reglamentu (ES) Nr. 1025/2012 dėl Europos standartizacijos nustatyta sistema, pagal kurią Komisija gali nuspręsti identifikuoti svarbiausias ir plačiausiai pripažintas IRT technines specifikacijas, parengtas ne Europos, tarptautinių ar nacionalinių standartizacijos organizacijų, kuriomis galima remtis, visų pirma siekiant užtikrinti viešųjų pirkimų sąveikumą. Suteikus galimybę perkant aparatinę bei programinę įrangą ir informacinių technologijų paslaugas naudoti įvairiausias IRT technines specifikacijas, bus įmanoma užtikrinti prietaisų, paslaugų ir taikomųjų programų sąveikumą, viešojo administravimo institucijoms bus lengviau išvengti susisaistymo, kuomet, baigus galioti viešųjų pirkimų sutarčiai, perkantysis subjektas negali keisti tiekėjo, nes naudoja IRT nuosavybinius sprendimus, ir bus skatinama konkurencija sąveikių IRT sprendimų pasiūlos srityje;

(5) kad IRT technines specifikacijas būtų galima nurodyti vykdant viešuosius pirkimus, jos turi atitikti Reglamento (ES) Nr. 1025/2012 II priede nustatytus reikalavimus. Atitiktis tiems reikalavimams valdžios institucijoms reiškia garantiją, kad IRT techninės specifikacijos yra parengtos vadovaujantis Pasaulio prekybos organizacijos standartizacijos srityje pripažintais atvirumo, skaidrumo, nešališkumo ir sutarimo principais;

([1]) OL L 316, 2012 11 14, p. 12.
([2]) Komisijos komunikatas „2020 m. Europa. Pažangaus, tvaraus ir integracinio augimo strategija“. COM(2010) 2020 galutinis, 2010 m. kovo 3 d.
([3]) Komisijos komunikatas „Bendrosios rinkos tobulinimas. daugiau galimybių piliečiams ir įmonėms“. (COM(2015) 550 *final*, 2015 m. spalio 28 d.).
([4]) Komunikatas „Europos bendrosios skaitmeninės rinkos strategija“. COM(2015) 192 *final*, 2015 m. gegužės 6 d.
([5]) COM(2016) 176 *final*, 2016 m. balandžio 19 d.
([6]) COM(2011) 311 *final*, 2011 m. birželio 1 d.

(6) sprendimas dėl IRT specifikacijos identifikavimo turi būti priimtas pasikonsultavus su IRT standartizacijos srities Europos įvairių suinteresuotųjų šalių platforma, sukurta Komisijos sprendimu 2011/C 349/04 ([1]), ir kitaip pasitarus su šio sektoriaus ekspertais;

(7) IRT standartizacijos srities Europos įvairių suinteresuotųjų šalių platforma įvertino šias technines specifikacijas, kuriomis remiamasi vykdant viešuosius pirkimus, ir pateikė palankias rekomendacijas dėl jų identifikavimo: Siuntėjo politikos strategiją leisti naudoti domeno vardus e. pašto adrese (angl. *SPF-Sender Policy Framework for Authorizing Use of Domains in Email*, SPF), STARTTLS-SMTP paslaugos išplėtimą saugiam SMTP protokolui taikant transporto lygmens saugumo protokolą (angl. *STARTTLS-SMTP Service Extension for Secure SMTP over Transport Layer Security*, STARTTLS-SMTP) ir Interneto inžinerijos darbo grupės (angl. *Internet Engineering Task Force*, IETF) sukurtą DANE-SMTP apsaugą taikant oportunistinę DNS pagrįstą nurodytų subjektų transporto lygmens apsaugą (angl. *DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security*, DANE-SMTP); Struktūrinę grėsmės informacijos išraišką (angl. *Structured Threat Information Expression*, STIX 1.2) ir Struktūrinės informacijos standartų tobulinimo organizacijos (angl. *Organization for the Advancement of Structured Information Standards*, OASIS) sukurtą Patikimą automatizuotą keitimąsi indikatorių informacija (angl. *Trusted Automated Exchange of Indicator Information*, TAXII 1.1). Vėliau dėl platformos įvertinimo ir rekomendacijų konsultuotasi su sektoriaus ekspertais ir jie patvirtino palankias rekomendacijas dėl specifikacijų identifikavimo;

(8) IETF sukurta SPF techninė specifikacija yra atvirasis standartas, kuriame nurodomas techninis metodas suklastotam siuntėjo adresui aptikti. SPF sudaro galimybę patikrinti, ar žinutė išsiųsta iš serverio, kuriam suteiktas toks leidimas. Tai yra paprasta e. pašto patvirtinimo sistema, sukurta e. pašto falsifikavimui nustatyti; taikant šią sistemą gaunantieji e. pašto mainų serveriai gali patikrinti, ar su domeno vardu gautas e. laiškas siunčiamas iš to domeno administratorių autorizuoto prieglobos serverio. SPF tikslas – užkirsti kelią brukalo siuntėjams siųsti žinutes, kurių siuntėjo langelyje („From“) nurodytame adrese naudojamas suklastotas konkretaus domeno vardas. Gavėjai gali pasitikrinti SPF įrašą ir nustatyti, ar žinutė, kurioje teigiama, kad ji išsiųsta iš to domeno, yra išsiųsta iš autorizuoto e. pašto serverio;

(9) IETF sukurta STARTTLS-SMTP yra priemonė, kurią taikant esamas nesaugus ryšys patobulinamas iki saugaus ryšio. STARTTLS yra paprastojo elektroninio pašto persiuntimo protokolo (angl. *Simple Mail Transfer Protocol*, SMTP) paslaugos plėtinys, kurį taikant SMTP serveris ir klientas gali naudoti transporto lygmens saugumo protokolą (angl. *Transport Layer Security*, TLS) ir naudotis privačiais, autorizuotais ryšiais internete. Ypač nesaugūs ryšiai e. paštu yra svarbus išpuolių būdas, taikomas siekiant patekti į valstybinius tinklus. Jei naudotojas išsiunčia e. laišką, naudotojo e. pašto tiekėjo serveris išsiunčia šį e. laišką gavėjo e. pašto serveriui. Taikant TLS šių e. pašto serverių ryšys gali būti iš anksto apsaugotas. STARTTLS siūlo galimybę nekoduotą (paprasto teksto) ryšį pakeisti koduotu TLS ryšiu;

(10) IETF sukurta DANE-SMTP yra protokolų rinkinys, skirtas interneto saugumui sustiprinti domeno vardų sistemoje (DNS) įvedant raktus ir juos apsaugant DNSSEC (angl. *DNS Security*). Norint sukurti saugų ryšį su nežinoma šalimi pageidautina atlikti siunčiančiosios šalies autentiškumo ir paskirties patikrinimą internete. Tai galima atlikti taikant sertifikavimo įstaigų išduotus sertifikatus viešojo rakto infrastruktūroje (PKI) arba paties pasirašytus sertifikatus. Taikant DANE domeno turėtojas (registruotojas) per DNSSEC apsaugotą DNS įrašą gali pateikti papildomos informacijos, papildančios internetinius sertifikatus. Todėl DANE yra itin svarbi kovojant su aktyviais išpuolių vykdytojais;

(11) OASIS sukurta STIX 1.2 yra kalba, skirta kibernetinės grėsmės informacijai aprašyti standartiniu ir struktūrizuotu būdu. Ji apima pagrindines temas, susijusias su kibernetinės grėsmės duomenimis, ir skirta išpuolių analizei ir keitimuisi informacija apie juos palengvinti. Ji apibūdina visapusišką kibernetinės grėsmės informaciją, įskaitant priešiškos veiklos rodiklius, kaip antai IP adresų ir rinkmenų sumaišymą, ir kontekstinę informaciją apie grėsmes, įskaitant priešišką taktiką, technologijas ir procedūras (TTP); išnaudojimo taikinius; kampanijas ir veiksmų kryptis (COA). Visa ši informacija visapusiškai apibūdina priešiškos kibernetinės veiklos motyvus, galimybes ir veiklos rūšis ir tokiu būdu padeda apsisaugoti nuo atakų;

(12) OASIS sukurta TAXII v1.1 techninė specifikacija standartizuoja patikimus, automatinius informacijos apie kibernetinę grėsmę mainus. TAXII apibūdina paslaugas ir keitimąsi informacija dėl dalijimosi taikytina kibernetinės grėsmės informacija, susijusia su organizacija, produktu arba paslauga, siekiant nustatyti kibernetinę grėsmę, jos išvengti arba ją sumažinti. Taikant TAXII organizacijoms suteikiama galimybė geriau būti informuotoms apie padėtį, susijusią su atsirandančiomis grėsmėmis, ir sudaroma galimybė lengvai keistis informacija su partneriais, tuo pačiu pasinaudojant esamais ryšiais ir sistemomis,

([1]) 2011 m. lapkričio 28 d. Komisijos sprendimas 2011/C 349/04, kuriuo sukuriama įvairių suinteresuotųjų Europos šalių platforma informacinių technologijų ir telekomunikacijų standartizacijos srityje (OL C 349, 2011 11 30, p. 4).

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Vykdant viešuosius pirkimus yra tinkamos nurodyti priede išvardytos techninės specifikacijos.

2 straipsnis

Šis sprendimas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Priimta Briuselyje 2017 m. gruodžio 11 d.

Komisijos vardu
Pirmininkas
Jean-Claude JUNCKER

PRIEDAS

Interneto inžinerijos grupė (IETF)

Nr.	IRT techninės specifikacijos pavadinimas
1	SPF-Siuntėjo politikos strategija (angl. *Sender Policy Framework*)
2	STARTTLS-SMTP Paslaugos išplėtimas saugiam SMTP protokolui taikant transporto lygmens saugumo protokolą (angl. *Service Extension for Secure SMTP over Transport Layer Security*)
3	DANE-SMTP Apsauga taikant oportunistinę DNS pagrįstą nurodytų subjektų transporto lygmens apsaugą (TLS) (angl. *Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (TLS)*)

Struktūrinės informacijos standartų tobulinimo organizacija (OASIS)

Nr.	IRT techninės specifikacijos pavadinimas
1	STIX 1.2 Struktūrinė grėsmės informacijos išraiška (angl. *Structured Threat Information Expression*)
2	TAXII 1.1 Patikimas automatizuotas keitimasis indikatorių informacija (angl. *Trusted Automated Exchange of Indicator Information*)