PROVEDBENA ODLUKA KOMISIJE (EU) 2017/2288

od 11. prosinca 2017.

o utvrđivanju tehničkih specifikacija IKT-a za pozivanja u javnoj nabavi

(Tekst značajan za EGP)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Uredbu (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća ([1]), a posebno njezin članak 13. stavak 1.,

nakon savjetovanja s europskom platformom za više interesnih skupina o normizaciji IKT-a i sa stručnjacima iz sektora,

budući da:

(1) Normizacija ima važnu ulogu u podupiranju strategije Europa 2020. ([2]). U nekoliko vodećih inicijativa strategije Europa 2020. naglašava se važnost dobrovoljne normizacije na tržištima proizvoda ili usluga radi osiguravanja usklađenosti i interoperabilnosti među proizvodima i uslugama, poticanja tehnološkog razvoja i podupiranja inovativnosti.

(2) Norme su temelj europske konkurentnosti i ključ za inovativnost i napredak. Komunikacije Komisije o jedinstvenom tržištu ([3]) i jedinstvenom digitalnom tržištu ([4]) potvrđuju važnost zajedničkih normi za osiguranje nužne interoperabilnosti mreža i sustava u europskom digitalnom gospodarstvu. To je ojačano donošenjem Komunikacije o prioritetima normizacije IKT-a ([5]) u kojoj Komisija utvrđuje prioritetne tehnologije IKT-a u kojima se normizacija smatra neophodnom za dovršenje jedinstvenog digitalnog tržišta.

(3) U Komunikaciji Komisije pod naslovom „Strateška vizija za europske norme: kretanje naprijed kako bi se poboljšao i ubrzao održivi rast europskoga gospodarstva do 2020.” ([6]) prepoznaje se specifičnost normizacije informacijskih i komunikacijskih tehnologija (IKT) jer se razvoj rješenja, aplikacija i usluga IKT-a često odvija u okviru globalnih foruma i konzorcija IKT-a koji su danas vodeće organizacije za razvoj normi u sektoru IKT-a.

(4) Uredbom (EU) br. 1025/2012 o europskoj normizaciji uspostavljen je sustav u okviru kojega Komisija može odlučiti o utvrđivanju najrelevantnijih i najšire prihvaćenih tehničkih specifikacija IKT-a koje su izdale neeuropske, međunarodne ili nacionalne organizacije za normizaciju, a na koje se može pozivati ponajprije kako bi se osigurala interoperabilnost u javnoj nabavi. Mogućnost uporabe cijelog raspona tehničkih specifikacija IKT-a pri nabavi hardvera, softvera i usluga iz područja informacijske tehnologije omogućit će interoperabilnost među uređajima, uslugama i aplikacijama, pomoći će javnim upravama da izbjegnu ovisnost o određenoj tehnologiji do koje dolazi kad javni nabavljač nakon isteka ugovora o javnoj nabavi zbog uporabe zaštićenih vlasničkih rješenja IKT-a ne može promijeniti pružatelja usluga te će potaknuti tržišno natjecanje u ponudi interoperabilnih rješenja IKT-a.

(5) Kako bi tehničke specifikacije IKT-a bile prihvatljive za pozivanja u javnoj nabavi, moraju biti u skladu sa zahtjevima navedenima u Prilogu II. Uredbi (EU) br. 1025/2012. Usklađenost s tim zahtjevima jamči javnim tijelima da su tehničke specifikacije IKT-a utvrđene u skladu s načelima otvorenosti, transparentnosti, nepristranosti i konsenzusa koja Svjetska trgovinska organizacija (WTO) priznaje u području normizacije.

([1]) SL L 316, 14.11.2012., str. 12.
([2]) Komunikacija Komisije „Europa 2020.: Strategija za pametan, održiv i uključiv rast”. COM(2010) 2020 final od 3. ožujka 2010.
([3]) Komunikacija Komisije „Poboljšanje jedinstvenog tržišta: više prilika za ljude i poduzeća”. COM(2015) 550 final od 28. listopada 2015.
([4]) Komunikacija o strategiji jedinstvenog digitalnog tržišta za Europu. COM(2015) 192 final od 6. svibnja 2015.
([5]) COM(2016) 176 final od 19. travnja 2016.
([6]) COM(2011) 311 final od 1. lipnja 2011.

(6) Odluku o utvrđivanju specifikacija IKT-a treba donijeti nakon savjetovanja s europskom platformom za više interesnih skupina o normizaciji IKT-a, osnovanom Odlukom Komisije 2011/C 349/04 ([1]), te drugih savjetovanja sa stručnjacima iz sektora.

(7) Europska platforma za više interesnih skupina o normizaciji IKT-a ocijenila je i dala pozitivno mišljenje o utvrđivanju sljedećih tehničkih specifikacija za pozivanja u javnoj nabavi: „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) i „DANE-SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security" (DANE-SMTP), koje je razvila Radna skupina za razvoj interneta (Internet Engineering Task Force – IETF); „Structured Threat Information Expression" (STIX 1.2) i „Trusted Automated Exchange of Indicator Information" (TAXII 1.1), koje je razvila Organizacija za unaprjeđivanje strukturiranih informacijskih normi (OASIS). Ocjena i mišljenje o platformi dostavljeni su potom na savjetovanje sa stručnjacima iz sektora koji su također dali pozitivno mišljenje o tom utvrđivanju.

(8) Tehnička specifikacija SPF, koju je razvio IETF, otvorena je norma kojom se utvrđuje tehnička metoda za otkrivanje krivotvorene adrese pošiljatelja. SPF nudi mogućnost provjere je li poruka poslana s poslužitelja s kojeg smije biti poslana. To je jednostavan sustav provjere e-pošte namijenjen otkrivanju krivotvorene e-pošte s pomoću mehanizma koji omogućuje primatelju e-pošte da provjeri je li dolazna pošta s neke domene poslana s glavnog poslužitelja koji su odobrili administratori te domene. Svrha je SPF-a spriječiti pošiljatelje neželjene pošte da šalju poruke s krivotvorenom adresom pošiljatelja na određenoj domeni. Primatelji mogu pogledati zapis SPF-a kako bi utvrdili dolazi li poruka za koju se čini da je s određene domene zaista s ovlaštenog poslužitelja e-pošte.

(9) STARTTLS-SMTP, koji je razvio IETF, metoda je za pretvaranje postojeće nesigurne veze u sigurnu. STARTTLS je proširenje usluge SMTP (Simple Mail Transfer Protocol) koja omogućuje SMTP poslužitelju i klijentu da koriste protokol TLS (Transport Layer Security) za omogućivanje privatne, autenticirane komunikacije putem interneta. Posebno nezaštićena komunikacija e-poštom velik je vektor napada u proboju vladinih mreža. Ako korisnik pošalje e-poštu, poslužitelj e-pošte korisnikova davatelja usluga poslat će tu e-poštu na poslužitelj e-pošte primatelja. Veza između tih poslužitelja e-pošte može biti unaprijed zaštićena s pomoću TLS-a. STARTTLS nudi mogućnost pretvaranja nešifrirane veze (s običnim tekstom) u šifriranu TLS vezu.

(10) DANE-SMTP, koji je razvio IETF, paket je protokola za poboljšanje internetske sigurnosti omogućivanjem da se u DNS (Domain Name System) postave ključevi i da se zaštite s pomoću DNSSEC-a (DNS Security). Pri uspostavi sigurne veze s nepoznatom stranom poželjna je internetska provjera autentičnosti pošiljatelja i odredišta. To se može postići s pomoću certifikata koje izdaju certifikacijska tijela u sustavu PKI ili samopotpisanih certifikata. DANE omogućuje nositelju domene (registriranoj osobi) da pruži dodatne informacije uz internetske certifikate putem DNS zapisa zaštićenog s pomoću DNSSEC-a. DANE je stoga posebno važan za borbu protiv aktivnih napadača.

(11) STIX 1.2, koji je razvio OASIS, jezik je za standardizirano i strukturirano opisivanje informacija o kiberprijetnjama. U pogledu podataka o kiberprijetnjama obuhvaća glavne teme te olakšava analizu i razmjenu podataka o napadima. Može opisati širok spektar informacija o kiberprijetnjama, uključujući pokazatelje aktivnosti napadača poput IP adresa i raspršivanja datoteka te kontekstualne informacije o prijetnjama kao što su protivničke taktike, tehnike i postupci (Tactics, Techniques and Procedures – TTP); mete iskorištavanja; kampanje i tijek aktivnosti (Campaigns and Courses of Action – COA). Te informacije zajedno u potpunosti opisuju motivaciju, sposobnosti i aktivnosti protivnika te tako pomažu u obrani od napada.

(12) Tehničkom specifikacijom TAXII v.1.1, koju je isto tako razvio OASIS, standardizira se pouzdana, automatizirana razmjena informacija o kiberprijetnjama. TAXII definira usluge i poruke za razmjenu konkretnih informacija o kiberprijetnjama izvan okvira organizacija, proizvoda ili usluga kako bi se kiberprijetnje mogle otkriti, spriječiti ili ublažiti. TAXII omogućuje organizacijama da postanu svjesnije novih prijetnji te da lako razmjenjuju informacije s partnerima i iskoriste postojeće odnose i sustave,

([1]) Odluka Komisije 2011/C 349/04 od 28. studenoga 2011. o osnivanju europske platforme za više interesnih skupina o normizaciji IKT-a (SL C 349, 30.11.2011., str. 4.).

DONIJELA JE OVU ODLUKU:

Članak 1.

Tehničke specifikacije navedene u Prilogu prihvatljive su za pozivanja u javnoj nabavi.

Članak 2.

Ova Odluka stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 11. prosinca 2017.

Za Komisiju
Predsjednik
Jean-Claude JUNCKER

PRILOG

Radna skupina za razvoj interneta (IETF)

Br.	Naslov tehničke specifikacije IKT-a
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)

Organizacija za unaprjeđivanje strukturiranih informacijskih normi (OASIS)

Br.	Naslov tehničke specifikacije IKT-a
1.	STIX 1.2 Structured Threat Information Expression
2.	TAXII 1.1 Trusted Automated Exchange of Indicator Information