PROVÁDĚCÍ ROZHODNUTÍ KOMISE (EU) 2017/2288

ze dne 11. prosince 2017

o určení technických specifikací IKT, na něž se odkazuje při zadávání veřejných zakázek

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES ([1]), a zejména na čl. 13 odst. 1 uvedeného nařízení,

po konzultaci s Evropskou platformou pro normalizaci v oblasti IKT složenou z mnoha zúčastněných stran a s odborníky z příslušného odvětví,

vzhledem k těmto důvodům:

(1) Normalizace sehrává důležitou úlohu v podpoře strategie Evropa 2020 ([2]). Několik stěžejních iniciativ strategie Evropa 2020 zdůraznilo význam dobrovolné normalizace na trzích výrobků nebo služeb, aby byla zajištěna slučitelnost a interoperabilita výrobků a služeb a podpořen technologický rozvoj a inovace.

(2) Normy mají zásadní význam pro konkurenceschopnost Evropy a pro inovace a pokrok. Sdělení Komise o jednotném trhu ([3]) a jednotném digitálním trhu ([4]) potvrzují význam společných norem pro zajištění nezbytné interoperability sítí a systémů v evropské digitální ekonomice. Toto je zdůrazněno přijetím sdělení o prioritách pro normalizaci IKT ([5]), v němž Komise označuje prioritní technologie IKT, u kterých se má za to, že normalizace má zásadní význam pro dokončení jednotného digitálního trhu.

(3) Sdělení Komise s názvem „Strategická vize pro evropské normy – další pokroky v posílení a urychlení udržitelného růstu evropského hospodářství do roku 2020“ ([6]) uznává zvláštní povahu normalizace v oblasti informačních a komunikačních technologií (IKT), v níž se řešení, aplikace a služby často vytvářejí v rámci globálních fór a konsorcií IKT, která jsou dnes vedoucími organizacemi v oblasti tvorby norem IKT.

(4) Nařízením (EU) č. 1025/2012 o evropské normalizaci byl zaveden systém, s jehož pomocí může Komise rozhodnout o určení nejvýznamnějších a nejšířeji přijímaných technických specifikací IKT vydávaných jinými organizacemi, než jsou evropské, mezinárodní nebo vnitrostátní normalizační organizace, přičemž na tyto specifikace lze následně odkazovat, a to především s cílem dosáhnout interoperability při zadávání veřejných zakázek. Možnost využívat veškeré technické specifikace IKT při pořizování hardwaru, softwaru a služeb IT umožní interoperabilitu mezi zařízeními, službami a aplikacemi, pomůže orgánům veřejné správy vyhnout se patovým situacím, které nastávají, když veřejný zadavatel nemůže změnit poskytovatele po uplynutí doby platnosti smlouvy na veřejnou zakázku, jelikož využívá řešení chráněná vlastnickými právy, a podpoří hospodářskou soutěž mezi dodavateli interoperabilních řešení IKT.

(5) Aby byly technické specifikace IKT způsobilé pro odkazování při zadávání veřejných zakázek, musí splňovat požadavky stanovené v příloze II nařízení (EU) č. 1025/2012. Soulad s těmito požadavky zaručuje veřejným orgánům, že technické specifikace IKT jsou vytvořeny v souladu se zásadami otevřenosti, transparentnosti, nestrannosti a konsensu uznávanými Světovou obchodní organizací v oblasti normalizace.

([1]) Úř. věst. L 316, 14.11.2012, s. 12.
([2]) Sdělení Komise s názvem „Evropa 2020. strategie pro inteligentní a udržitelný růst podporující začlenění“. KOM(2010) 2020 v konečném znění, 3.3.2010.
([3]) Sdělení Komise s názvem „Zlepšování jednotného trhu: více příležitostí pro lidi a podniky“. COM(2015) 550 final ze dne 28. října 2015.
([4]) Sdělení o strategii pro jednotný digitální trh v Evropě. COM(2015) 192 final ze dne 6. května 2015.
([5]) COM(2016) 176 final ze dne 19. dubna 2016.
([6]) KOM(2011) 311 v konečném znění ze dne 1. června 2011.

(6) Rozhodnutí o určení specifikace IKT se přijímá po konzultaci s Evropskou platformou pro normalizaci v oblasti IKT složenou z mnoha zúčastněných stran (zřízenou rozhodnutím Komise 2011/C 349/04 ([1])), která je doplněna dalšími formami konzultací s odborníky z příslušného odvětví.

(7) Evropská platforma pro normalizaci v oblasti IKT složená z mnoha zúčastněných stran posoudila a vydala kladné doporučení týkající se určení následujících technických specifikací pro účely odkazování při zadávání veřejných zakázek: „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)“ a „DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security (DANE- SMTP)“, které byly vyvinuty Komisí pro technickou stránku internetu (Internet Engineering Task Force (IETF)); „Structured Threat Information Expression (STIX 1.2)“ a „Trusted Automated Exchange of Indicator Information (TAXII 1.1)“, které byly vyvinuty Organizací pro rozvoj strukturovaných informačních standardů (Organization for the Advancement of Structured Information Standards (OASIS)). Toto posouzení a doporučení vydané platformou bylo následně postoupeno ke konzultaci odborníkům z příslušného odvětví, kteří potvrdili toto kladné doporučení týkající se určení.

(8) Technické specifikace SPF vyvinuté Komisí pro technickou stránku internetu jsou otevřeným standardem, který specifikuje technickou metodu k odhalení zfalšované adresy odesílatele. SPF umožňuje ověřovat, zda je zpráva odeslána ze serveru, který má k tomu oprávnění. Jde o jednoduchý systém validace e-mailů vytvořený za účelem odhalování fingované identity u e-mailů, který příjemci e-mailu nabízí mechanismus umožňující ověřit, že e-mail přicházející z domény pochází od hostingového subjektu, jenž byl autorizován správcem této domény. Účelem SPF je bránit spammerům v zasílání zpráv s falšovanou adresou odesílatele v konkrétní doméně. Příjemci zpráv mohou nahlédnout do záznamů SPF, aby si ověřili, zda zpráva, která se tváří, že pochází z konkrétní domény, přichází z autorizovaného e-mailového serveru.

(9) „STARTTLS-SMTP“ vyvinutý Komisí pro technickou stránku internetu je způsob, jak z existujícího nezabezpečeného připojení vytvořit zabezpečené připojení. STARTTLS je rozšířením služby protokolu Simple Mail Transfer Protocol (SMTP), která umožňuje, aby server SMTP a klient používali zabezpečení Transport Layer Security (TLS) k poskytování soukromé, ověřené komunikace přes internet. Je to právě nezabezpečená elektronická komunikace, která je nejčastěji zneužívána k prolomení vládních sítí. Pokud uživatel posílá e-mail, odešle jej e-mailový server jeho poskytovatele e-mailových služeb e-mailovému serveru příjemce. Spojení mezi těmito dvěma e-mailovými servery lze dopředu zabezpečit pomocí TLS. STARTTLS nabízí způsob, jak zvýšit zabezpečení nešifrovaného (plain-text) připojení na úroveň zašifrovaného připojení TLS.

(10) „DANE-SMTP“ vyvinutý Komisí pro technickou stránku internetu je souborem protokolů posilujících bezpečnost internetu tím, že umožňují vložit klíče do systému Domain Name System (DNS) a zabezpečit jej pomocí DNSSEC (DNS Security). Při navazování bezpečného připojení s neznámou třetí stranou je žádoucí ověřovat online pravost odesílatele a místo určení. Lze to dělat pomocí certifikátů vydaných certifikačními orgány (CA) v rámci systému PKI nebo samopodepsanými certifikáty. DANE umožňuje držiteli domény (registrantovi), aby poskytoval další informace nad rámec online certifikátů prostřednictvím záznamů DNS zabezpečených pomocí DNSSEC. DANE je tudíž důležitý zejména pro boj proti aktivním útočníkům.

(11) „STIX 1.2“ vyvinutý Organizací pro rozvoj strukturovaných informačních standardů, je jazyk popisující informace o kybernetických hrozbách standardizovaným a strukturovaným způsobem. Pokrývá hlavní témata, pokud jde o kybernetické hrozby týkající se údajů, usnadňuje analýzu útoků a výměnu informací o nich. Charakterizuje rozsáhlý soubor informací o kybernetických hrozbách, včetně indikátorů nepřátelských aktivit, jako jsou IP adresy a hashe souborů, a kontextových informací ohledně hrozeb, jsou nepřátelské taktiky, techniky a postupy (Tactics, Techniques and Procedures – TTP); využívání cílů; opatření Campaigns and Courses of Action (COA). Na základě souboru všech těchto informací lze kompletně charakterizovat motivaci kyberútočníků, jejich schopnosti a aktivity, což usnadňuje obranu proti útokům.

(12) Technické specifikace „TAXII v1.1“ rovněž vyvinuté Organizací pro rozvoj strukturovaných informačních standardů standardizují důvěryhodnou automatickou výměnu informací o kybernetických hrozbách. TAXII definuje služby a výměny zpráv pro sdílení upotřebitelných informací o kybernetických hrozbách mimo rámec dané organizace, daného produktu nebo dané služby za účelem odhalení, prevence a zmírňování kybernetických hrozeb. TAXII poskytuje organizacím nástroje, kterými mohou dosáhnout zlepšení situačního povědomí o vznikajících hrozbách, a umožňuje jim snadno sdílet informace s partnery, a přitom staví na stávajících vztazích a systémech,

([1]) Rozhodnutí Komise 2011/C 349/04 ze dne 28. listopadu 2011, kterým se zřizuje Evropská platforma pro normalizaci v oblasti IKT složená z mnoha zúčastněných stran (Úř. věst. C 349, 30.11.2011, s. 4).

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Technické specifikace uvedené v příloze jsou způsobilé pro odkazování při zadávání veřejných zakázek.

Článek 2

Toto rozhodnutí vstupuje v platnost dvacátým dnem po zveřejnění v *Úředním věstníku Evropské unie*.

V Bruselu dne 11. prosince 2017.

Za Komisi
předseda
Jean-Claude JUNCKER

PŘÍLOHA

Komise pro technickou stránku internetu (Internet Engineering Task Force, IETF)

č.	Název technické specifikace IKT
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)

Organizace pro rozvoj strukturovaných informačních standardů (Organization for the Advancement of Structured Information Standards)

č.	Název technické specifikace IKT
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information