VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2017/2288

z 11. decembra 2017

o určení technických špecifikácií IKT, na ktoré sa môže odkazovať pri verejnom obstarávaní

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 z 25. októbra 2012 o európskej normalizácii, ktorým sa menia a dopĺňajú smernice Rady 89/686/EHS a 93/15/EHS a smernice Európskeho 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 ktorým sa zrušuje rozhodnutie Rady 87/95/EHS a rozhodnutie Európskeho parlamentu a Rady č. 1673/2006/ES ([1]), a najmä na jeho článok 13 ods. 1,

po konzultácii s Európskou multilaterálnou platformou pre normalizáciu v oblasti IKT a odborníkmi z tohto odvetvia,

keďže:

(1) Normalizácia zohráva významnú úlohu pri podporovaní stratégie Európa 2020 ([2]). Viaceré z hlavných iniciatív stratégie Európa 2020 zdôrazňujú význam dobrovoľnej normalizácie na trhoch s výrobkami alebo službami z hľadiska zabezpečenia kompatibility a interoperability medzi výrobkami a službami, posilnenia technologického vývoja a podpory inovácií.

(2) Normy majú zásadný význam pre konkurencieschopnosť Európy a sú kľúčové z hľadiska inovácie a pokroku. V oznámeniach Komisie o jednotnom trhu ([3]) a o jednotnom digitálnom trhu ([4]) sa potvrdzuje relevantnosť spoločných noriem pre zabezpečenie potrebnej interoperability sietí a systémov v rámci európskeho digitálneho hospodárstva. To sa zdôraznilo prijatím oznámenia o prioritách v oblasti normalizácie IKT ([5]), v ktorom Komisia určila prioritné informačné a komunikačné technológie, ktorých normalizácia má podľa nej zásadný význam pre dobudovanie jednotného digitálneho trhu.

(3) Komisia vo svojom oznámení s názvom „Strategická vízia pre európske normy: smerom k posilneniu a urýchleniu udržateľného rastu európskeho hospodárstva do roku 2020“ ([6]) uznáva osobitný charakter normalizácie v oblasti informačných a komunikačných technológií, v ktorej sa riešenia, aplikácie a služby často vyvíjajú v rámci celosvetových fór a konzorcií IKT, ktoré dnes majú vedúcu pozíciu v organizáciách pre vývoj noriem pre IKT.

(4) Nariadením (EÚ) č. 1025/2012 o európskej normalizácii bol vytvorený systém, na základe ktorého sa môže Komisia rozhodnúť určiť najrelevantnejšie a všeobecne najviac akceptované technické špecifikácie IKT vydané organizáciami, ktoré nie sú európskymi, medzinárodnými ani vnútroštátnymi normalizačnými organizáciami, na ktoré sa potom môže odkazovať, predovšetkým v záujme zaistenia interoperability verejného obstarávania. Možnosť používať pri obstarávaní hardvéru, softvéru a služieb informačných technológií celú škálu technických špecifikácií IKT umožní interoperabilitu medzi zariadeniami, službami a aplikáciami, pomôže orgánom verejnej správy vyhnúť sa situáciám, ktoré nastávajú, keď verejný obstarávateľ nemôže po skončení zmluvy o obstarávaní zmeniť dodávateľa, pretože využíva riešenia v oblasti IKT chránené autorským právom, a podporí hospodársku súťaž v oblasti poskytovania interoperabilných riešení IKT.

(5) Nato, aby sa na technické špecifikácie IKT mohlo odkazovať pri verejnom obstarávaní, musia byť tieto špecifikácie v súlade s požiadavkami stanovenými v prílohe II k nariadeniu (EÚ) č. 1025/2012. Súlad s uvedenými požiadavkami subjektom verejného sektora zaručuje, že technické špecifikácie IKT sú stanovené v súlade so zásadami otvorenosti, transparentnosti, nestrannosti a konsenzu, ktoré v oblasti normalizácie uznáva Svetová obchodná organizácia.

([1]) Ú. v. EÚ L 316, 14.11.2012, s. 12.
([2]) Oznámenie Komisie „Európa 2020: Stratégia na zabezpečenie inteligentného, udržateľného a inkluzívneho rastu“. KOM(2010) 2020 v konečnom znení, 3. marca 2010.
([3]) Oznámenie Komisie s názvom „Zlepšovanie jednotného trhu: viac príležitostí pre ľudí a podniky“. COM(2015) 550 final z 28. októbra 2015.
([4]) Oznámenie o stratégii pre jednotný digitálny trh v Európe COM(2015) 192 final zo 6. mája 2015.
([5]) COM(2016) 176 final z 19. apríla 2016.
([6]) KOM(2011) 311 v konečnom znení z 1. júna 2011.

(6) Rozhodnutie o určení špecifikácie IKT sa má prijať po konzultácii s Európskou multilaterálnou platformou pre normalizáciu v oblasti IKT zriadenou rozhodnutím Komisie 2011/C 349/04 ([1]) doplnenej o ďalšie formy konzultácií s odborníkmi z príslušného odvetvia.

(7) Európska multilaterálna platforma pre normalizáciu v oblasti IKT hodnotila a vydala kladné odporúčanie, pokiaľ ide o určenie týchto technických špecifikácií, na ktoré sa môže odkazovať pri verejnom obstarávaní: „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), ktoré vyvinula Osobitná skupina pre internetovú techniku [Internet Engineering Task Force (IETF)]; „Structured Threat Information Expression“ (STIX 1.2) a „Trusted Automated Exchange of Indicator Information“ (TAXII 1.1), ktoré vyvinula Organizácia pre rozvoj štruktúrovaných informačných štandardov [Organization for the Advancement of Structured Information Standards (OASIS)]. Toto hodnotenie a odporúčanie platformy bolo následne predložené na konzultáciu s odborníkmi z odvetvia, ktorí potvrdili kladné stanovisko k určeniu týchto špecifikácií.

(8) „SPF“ je technická špecifikácia, ktorú vyvinula skupina IETF ako otvorenú normu, v ktorej sa špecifikuje technický postup na odhalenie falšovania adresy odosielateľa. SPF ponúka možnosť skontrolovať, či bola správa odoslaná zo servera, ktorý je na to oprávnený. Ide o jednoduchý systém validácie emailov, navrhnutý na odhaľovanie spoofingu emailov prostredníctvom mechanizmu, ktorý prijímajúcim emailovým serverom umožňuje skontrolovať, či email prichádzajúci z určitej domény pochádza od hostiteľského servera autorizovaného administrátormi domény. Účelom SPF je zabrániť spamerom, aby odosielali emaily so sfalšovanými adresami odosielateľa (From-addresses) z konkrétnej domény. Príjemcovia môžu skontrolovať záznam SPF, aby overili, či bol email, ktorý údajne pochádza z danej domény, skutočne odoslaný z autorizovaného emailového servera.

(9) „STARTTLS-SMTP“, vyvinutá skupinou IETF, je spôsobom, ako z existujúceho nezabezpečeného pripojenia vytvoriť zabezpečené pripojenie. STARTTLS je rozšírením služby Simple Mail Transfer Protocol („SMTP“), ktoré umožňuje SMTP serveru a klientovi využiť zabezpečenie Transport Layer Security („TLS“) na súkromnú, overenú komunikáciu cez internet. Najmä nezabezpečená emailová komunikácia predstavuje jedno z hlavných miest, ktorými sa útočníci dostanú do vládnych sietí. Ak používateľ odošle email, emailový server jeho poskytovateľa emailových služieb odošle tento email na emailový server prijímateľa. Spojenie medzi týmito emailovými servermi môže byť vopred zabezpečené pomocou TLS. Špecifikácia STARTTLS ponúka spôsob ako zvýšiť zabezpečenie nešifrovaného (plain-text) spojenia na úroveň zašifrovaného spojenia TLS.

(10) Špecifikácia „DANE-SMTP“ vyvinutá skupinou IETF je súborom protokolov na posilnenie bezpečnosti internetu tým, že umožňuje vkladanie kľúčov do systému názvov domén (Domain Name System – DNS) a ich zabezpečenie prostredníctvom DNSSEC (DNS Security). Pri vytváraní zabezpečeného spojenia s neznámym účastníkom je žiaduce overiť online pravosť odosielajúcej strany a miesta určenia. To je možné na základe certifikátov vydaných certifikačnými orgánmi v rámci systému PKI alebo autocertifikátov. Špecifikácia DANE umožňuje držiteľovi domény („registrujúci subjekt“) poskytovať dodatočné informácie nad rámec online certifikátov prostredníctvom DNS záznamu zabezpečeného DNSSEC. Špecifikácia DANE je preto obzvlášť dôležitá pri boji proti aktívnym útočníkom.

(11) Špecifikácia „STIX 1.2“ vyvinutá organizáciou OASIS predstavuje jazyk na opis informácií o kybernetických hrozbách štandardizovaným a štruktúrovaným spôsobom. Pokrýva hlavné témy, pokiaľ ide o informácie o kybernetických hrozbách, čím uľahčuje analýzu a výmenu informácií o útokoch. Charakterizuje rozsiahly súbor informácií o kybernetických hrozbách vrátane ukazovateľov aktivite útočníka, ako sú napríklad IP adresy, hašované súbory a kontextové informácie o hrozbách, ako sú napríklad taktiky, techniky a postupy (TTP) útočníka, ciele útoku, kampane a postupy protiopatrení (COA). Tieto informácie spolu plne charakterizujú motívy, schopnosti a aktivity kybernetického útočníka a pomáhajú tak pri ochrane pred útokmi.

(12) Technická špecifikácia „TAXII v1.1“, ktorú takisto vyvinula organizácia OASIS, normalizuje overenú a automatizovanú výmenu informácií o kybernetických hrozbách. Špecifikácia TAXII definuje služby a výmeny správ na zdieľanie využiteľných informácií o kybernetických hrozbách medzi organizáciami, produktmi alebo službami s ohľadom na odhaľovanie, prevenciu a zmierňovanie kybernetických hrozieb. Špecifikácia TAXII pomáha organizáciám získať lepšie situačné povedomie o vznikajúcich hrozbách a umožňuje im jednoducho zdieľať informácie s partnermi, pričom môžu využívať existujúce vzťahy a systémy,

([1]) Rozhodnutie Komisie 2011/C 349/04 z 28. novembra 2011, ktorým sa zriaďuje Európska multilaterálna platforma pre normalizáciu v oblasti IKT (Ú. v. EÚ C 349, 30.11.2011, s. 4).

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Technické špecifikácie uvedené v prílohe spĺňajú podmienky na to, aby sa na ne mohlo odkazovať pri verejnom obstarávaní.

Článok 2

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Bruseli 11. decembra 2017

Za Komisiu
predseda
Jean-Claude JUNCKER

PRÍLOHA

Osobitná skupina pre internetovú techniku (Internet Engineering Task Force, IETF)

č.	Názov technickej špecifikácie 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)

Organizácia pre rozvoj štruktúrovaných informačných štandardov (Organisation for the Advancement of Structured Information Standards, OASIS)

č.	Názov technickej špecifikácie IKT
1.	STIX 1.2 Structured Threat Information Expression
2.	TAXII 1.1 Trusted Automated Exchange of Indicator Information