A BIZOTTSÁG (EU) 2017/2288 VÉGREHAJTÁSI HATÁROZATA

(2017. december 11.)

a közbeszerzésben hivatkozható IKT műszaki előírások azonosításáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről szóló, 2012. október 25-i 1025/2012/EU európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 13. cikke (1) bekezdésére,

az IKT-szabványosítással foglalkozó, több érdekelt felet tömörítő európai platformmal és az ágazati szakértőkkel folytatott konzultációt követően,

mivel:

(1) A szabványosítás fontos szerepet tölt be az Európa 2020 stratégia ([2]) előmozdításában. Az Európa 2020 stratégia számos kiemelt kezdeményezése hangsúlyozza a termék- és szolgáltatáspiacokon az önkéntes szabványosítás fontosságát a más termékekkel vagy szolgáltatásokkal való összeegyeztethetőség és interoperabilitás, valamint a technológiafejlesztés előmozdítása és az innováció támogatása szempontjából.

(2) A szabványok elengedhetetlenek az európai versenyképesség biztosításához, és kulcsszerepet játszanak az innovációban és a fejlődésben. Az egységes piacról ([3]) és a digitális egységes piacról ([4]) szóló bizottsági közlemények megerősítik a közös szabványok fontosságát európai digitális gazdaságon belül a hálózatok és rendszerek szükséges interoperabilitásának biztosítása terén. Ezt támasztja alá az IKT-szabványosítási prioritásokról szóló közlemény ([5]) elfogadása is, amelyben a Bizottság azonosítja azokat az elsőbbséget élvező információs és kommunikációs technológiákat, ahol a szabványosítás kulcsfontosságúnak tekinthető a digitális egységes piac megvalósításához.

(3) „Az európai szabványok stratégiai jövőképe: az európai gazdaság fenntartható növekedésének elősegítése és gyorsítása 2020-ig” című bizottsági közlemény ([6]) elismerte az információs és kommunikációs technológiák (IKT) terén zajló szabványosításnak azt a sajátosságát, hogy az IKT-megoldásokat, -alkalmazásokat és -szolgáltatásokat gyakran olyan globális IKT-fórumok és -konzorciumok fejlesztik, amelyek ma vezető IKT-szabványosítási szervezetek.

(4) A szabványosításról szóló 1025/2012/EU rendelet olyan rendszert alakított ki, amelyben a Bizottság dönthet annak megállapításáról, hogy a nem európai, nemzetközi vagy nemzeti szabványügyi szervezetek által elfogadott IKT műszaki előírások közül melyek a legrelevánsabbak és a legszélesebb körben elfogadottak, és amelyekre a közbeszerzésekben – elsősorban az átjárhatóság lehetővé tétele érdekében – hivatkozni lehet. Ha egy hardver, szoftver vagy információs technológiai szolgáltatás közbeszerzése során lehetőség van az IKT műszaki előírások teljes körének kihasználására, az lehetővé teszi az eszközök, szolgáltatások és alkalmazások közötti interoperabilitást, és segít elkerülni a közigazgatásban azt a csapdát, hogy a saját tulajdonú IKT-megoldások alkalmazása miatt a közbeszerző nem tud szolgáltatót váltani a beszerzési szerződés lejártával, továbbá ösztönzi a versenyt az interoperábilis IKT-megoldások szolgáltatásainak piacán.

(5) A közbeszerzési eljárásokban akkor lehet IKT műszaki előírásokra hivatkozni, ha azok megfelelnek az 1025/2012/EU rendelet II. mellékletében foglalt követelményeknek. Az említett követelményeknek való megfelelés garantálja a hatóságok számára, hogy az IKT műszaki előírások kidolgozása során érvényesüljenek a Kereskedelmi Világszervezet által a szabványosítás területén elismert következő elvek: a nyitottság, az átláthatóság, a pártatlanság és a konszenzus.

([1]) HL L 316., 2012.11.14., 12. o.
([2]) A Bizottság közleménye: „Európa 2020 – Az intelligens, fenntartható és inkluzív növekedés stratégiája”, COM(2010) 2020 végleges, 2010. március 3.
([3]) A Bizottság közleménye: „Az egységes piac továbbfejlesztése: a polgárok és vállalkozások lehetőségeinek bővítése”, COM(2015) 550 final, 2015. október 28.
([4]) A Bizottság közleménye: „Európai digitális egységes piaci stratégia”, COM(2015) 192 final, 2015. május 6.
([5]) COM(2016) 176 final, 2016. április 19.
([6]) COM(2011) 311 végleges, 2011. június 1.

(6) Az IKT-előírások kiválasztására vonatkozó határozatok elfogadása előtt a Bizottság konzultál a 2011/C 349/04 bizottsági határozattal ([1]) létrehozott, az IKT-szabványosítással foglalkozó, több érdekelt felet tömörítő európai platformmal, illetve más fórumokon az ágazati szakértőkkel.

(7) Az IKT-szabványosítással foglalkozó, több érdekelt felet tömörítő európai platform értékelte és a közbeszerzésben hivatkozhatóként történő elismerésre javasolta a következő műszaki előírásokat: az Internet Engineering Task Force (Internet-mérnöki Munkacsoport, IETF) által kidolgozott „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), valamint „DANE- SMTP Security via Opportunistic DNS-Based Authentication of Named Entities Transport Layer Security" (DANE- SMTP); az Organization for the Advancement of Structured Information Standards (OASIS) által kidolgozott „Structured Threat Information Expression" (STIX 1.2), valamint „Trusted Automated Exchange of Indicator Information" (TAXII 1.1). A platform által végzett értékelést és a megfogalmazott tanácsokat ezután megvitatták ágazati szakértőkkel, akik szintén az elismerés mellett foglaltak állást.

(8) Az IETF által kidolgozott „SPF" műszaki előírás egy nyílt szabvány, amely a feladó címének meghamisításának észlelésére szolgáló technikai módszert határoz meg. Az SPF lehetővé teszi annak ellenőrzését, hogy egy üzenetet arról a szerverről küldtek-e, amelyik erre jogosult. Ez egy egyszerű e-mail-validáló rendszer, amelyet arra terveztek, hogy azáltal észlelje az e-mailek meghamisítását, hogy az üzenetet fogadóknak lehetővé teszi annak ellenőrzését, hogy egy bizonyos domainből érkező üzenet egy olyan szervertől származik-e, amelyet a domain adminisztrátorai engedélyeztek. Az SPF célja, hogy a kéretlen elektronikus levelek küldőit megakadályozza valamely meghatározott domainbe tartozó hamisított feladói címmel történő üzenetek küldésében. A feladók egy SPF-bejegyzés alapján meghatározhatják, hogy egy állítólagosan abból a domainből érkező üzenet egy engedélyezett mailszerverről jön-e.

(9) Az IETF által kidolgozott „STARTTLS-SMTP" egy meglévő, nem biztosított összeköttetés biztosított összeköttetéssé történő átalakítására szolgáló módszer. A „STARTTLS" a „Simple Mail Transfer Protocol" (SMTP) szolgáltatás kiegészítése, amely egy SMTP szerver és kliens számára lehetővé teszi az interneten keresztül magánjellegű és hiteles kommunikációt lehetővé tevő „Transport Layer Security" (TLS) használatát. Különösen a biztosítás nélküli e-mail-kommunikáció jelentős támadási felületet nyújt a kormányzati hálózatok feltöréséhez. Ha egy felhasználó elküld egy e-mailt, a felhasználó mailszolgáltatójának mailszervere továbbítja ezt a levelet a fogadó mailszerverére. Az e szerverek közötti összeköttetés tehető előre biztonságossá a TLS-sel. A „STARTTLS" lehetőséget nyújt egy titkosítás nélküli (egyszerű szöveges) összeköttetés titkosított TLS-összeköttetéssé történő átalakítására.

(10) Az IETF által kidolgozott „DANE-SMTP" olyan protokollok eszköztára, amelyekkel azáltal javítható az internetes biztonság, hogy kulcsokat helyeznek el a domainnév-rendszerben (DNS), és azokat DNSSEC-kel („DNS Security") biztosítják. Amikor egy ismeretlen féllel létesítenek biztosított összeköttetést, kívánatos a feladó és a fogadó fél hitelességének online ellenőrzése. Ez megtehető a tanúsító hatóságok által a PKI-rendszerben kiadott vagy önállóan aláírt tanúsítványok által. A DANE lehetővé teszi a domain-név birtokosa (a regisztráló) számára, hogy az online tanúsítványokon túlmenően egy DNSSEC-kel biztosított DNS-bejegyzésben további információkat nyújtson. A DANE ezért különösen fontos az aktív támadók elhárításához.

(11) Az OASIS által kidolgozott „STIX 1.2" a kiberfenyegetésekre vonatkozó információk szabványos és strukturált módon történő leírására szolgáló nyelv. Lefedi a kiberfenyegetésekkel kapcsolatos főbb területeket, valamint megkönnyíti a támadások elemzését és megvitatását. Jellemzi a kiberfenyegetésekkel kapcsolatos információk széles körét, beleértve az ellenséges tevékenység mutatóit (mint például IP-címek és fájlok hash-kódjai), valamint a fenyegetésekre vonatkozó kontextuális információkat (mint például az ellenség taktikái, technikái és eljárásai: „Tactics, Techniques and Procedures" – TTP-k); a kihasznált célpontokat; kampányokat és fellépési mintákat (Courses of Action – COA). Ezen információk együtt teljes jellemzését adják a kiberellenség motivációinak, lehetőségeinek és tevékenységének, és ily módon segítenek a támadások elleni védekezésben.

(12) A szintén az OASIS által kidolgozott „TAXII v1.1" műszaki előírás szabványosítja a kiberfenyegetésekre vonatkozó információk megbízható és automatikus cseréjét. A TAXII szolgáltatásokat üzenetváltásokat határoz meg a kiberfenyegetésekre vonatkozó felhasználható információk szervezetek, termékek vagy szolgáltatások közötti határokon átnyúló cseréjére a kiberfenyegetések észlelése, megelőzése és hatásának mérséklése céljából. A TAXII lehetőséget ad a szervezeteknek, hogy javítsák helyzetismeretüket a kiberfenyegetések terén, és lehetővé teszi számukra, hogy könnyebben megosszák az információkat partnereikkel, mozgósítva a meglévő kapcsolatokat és rendszereket,

([1]) A Bizottság 2011/C 349/04 határozata (2011. november 28.) az IKT-szabványosítással foglalkozó, több érdekelt felet tömörítő európai platform létrehozásáról (HL C 349., 2011.11.30., 4. o.).

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A mellékletben felsorolt műszaki előírások hivatkozhatók közbeszerzési eljárásokban.

2. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Kelt Brüsszelben, 2017. december 11-én.

a Bizottság részéről
az elnök
Jean-Claude JUNCKER

MELLÉKLET

Internet Engineering Task Force, Internet-mérnöki Munkacsoport (IETF)

Szám	Az IKT műszaki előírás címe
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)

Organization for the Advancement of Structured Information Standards (OASIS)

Szám	Az IKT műszaki előírás címe
1	STIX 1.2 Structured Threat Information Expression
2	TAXII 1.1 Trusted Automated Exchange of Indicator Information