Európai Bizottság

AZ UNIÓ HELYZETE 2018

Erős kiberbiztonság kialakítása Európában

#SOTEU

2018. szeptember 12.

„A kibertámadásokat nem állítják meg a határok, de reagálási képességünk országról országra igen nagy mértékben különbözik. Így biztonsági rések keletkeznek, melyek gyenge pontjaikkal még jobban vonzzák a támadásokat. Az EU-nak szilárdabb és hatékonyabb struktúrákra van szüksége a kibertámadásokkal szembeni erős ellenálló képesség és az informatikai támadásokkal szembeni fellépés érdekében. Nem kívánunk e globális fenyegetés leggyengébb láncszeme lenni.”

Jean-Claude Juncker, tallinni digitális csúcstalálkozó, 2017. szeptember 29.

Annak érdekében, hogy Európa megfelelő eszközökkel rendelkezzen a folyamatosan változó jellegű kibertámadásokkal szembeni fellépéshez, az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselője 2017-ben az erős unióbeli kiberbiztonság kiépítését célzó, széles körű intézkedéscsomagot terjesztett elő. Ezeket az erőfeszítéseket most olyan javaslat egészíti ki, amely elősegíti, hogy az EU egyesítse a rendelkezésre álló kutatási és innovációs forrásokat és szakértelmet, és a következő generációs kiberbiztonsági és digitális technológiák területén vezető szerepre tegyen szert.

Napjaink kiberfenyegetései

2016-ban naponta több mint 4000 zsarolóprogram-támadás történt

Tavaly **az európai vállalatok 80%**-a tapasztalt legalább egy kiberbiztonsági eseményt

Az összes iparágat vizsgálva a **biztonsági incidensek** száma 2015-ben **38%**-kal nőtt – az elmúlt 12 évben a legnagyobb mértékben

Egyes tagállamokban az elkövetett bűncselekmények **50%-a a kiberbűnözéshez köthető**

A 2017. májusi WannaCry támadás **több mint 150 országot és világszerte, számos ágazatra kiterjedően több mint 230 000 rendszert** érintett, számottevő hatást gyakorolva az internethez kapcsolódó alapvető szolgáltatásokra, például a kórházi és mentőszolgálatokra

A kibertámadásokkal szembeni ellenálló képesség erősítése

A Bizottság jelenleg is támogatást nyújt az EU kibertámadásokkal szembeni ellenálló képességének és reagálási képességének erősítéséhez és az e támadásokkal szembeni elrettentés fokozásához, többek között következő eszközökkel:

Az első uniós kiberbiztonsági jogszabály (a hálózati és információs rendszerek biztonságáról szóló irányelv) hatékony végrehajtásának támogatása a következők révén:

JOBB KIBERBIZTONSÁGI KÉPESSÉGEK

A tagállamoknak javítaniuk kell kiberbiztonsági képességeiket

EGYÜTTMŰKÖDÉS

Fokozott uniós szintű együttműködés

KOCKÁZATMEGELŐZÉS

A kulcsfontosságú ágazatok (például energia, közlekedés, egészségügy) szereplői kötelesek intézkedéseket hozni a veszélyek megelőzése és a kiberbiztonsági események kezelése érdekében

Együttműködés a tagállamokkal a következők terén:

EURÓPAI UNIÓS KIBERBIZTONSÁGI ÜGYNÖKSÉG

Az Európai Uniós Kiberbiztonsági Ügynökség megerősítése, hogy megfelelőbben támogathassa a tagállamokat

UNIÓS TANÚSÍTÁSI KERETRENDSZER

uniós tanúsítási keretrendszer a termékek és szolgáltatások kiberbiztonságának garantálására

ÖSSZEHANGOLT REAGÁLÁS

Gyors és összehangolt válasz biztosítása a nagyléptékű kibertámadásokra

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) támogatást nyújt a tagállamok kiberbiztonsági hatóságainak az EU kibertámadásokkal szembeni védelmének erősítése érdekében.

Az erőforrások és a szakértelem egyesítése a kiberbiztonsági technológiák terén

A már létező uniós kiberbiztonsági kezdeményezéseken túlmenően a Bizottság ma javaslatot tesz arra, hogy – a folyamatosan változó fenyegetéssel lépést tartó eszközök és technológiák kifejlesztésének és bevezetésének érdekében – ezeknek az erőfeszítéseknek a kiegészítésére jöjjön létre egy kompetenciaközpont-hálózat, valamint az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont.

Az Európai Központ feladata lesz, hogy a következő hosszú távú uniós költségvetés keretében a kiberbiztonsággal kapcsolatban előirányzott forrásokat a tagállamokkal együtt a lehető legcélzottabb módon koordinálja. Ez elősegíti új európai kiberképességek kialakítását.

Európában jelenleg is széles körű szakértelem áll rendelkezésre – **Európa-szerte több mint 660 kiberbiztonsági kompetenciaközpont** működik. A szakértelem hatékony kiaknázása és alkalmazása érdekében a Bizottság mechanizmust javasol a következők érdekében:

a meglévő szakértelem összegyűjtése, megosztása és az ahhoz való hozzáférés biztosítása

az uniós kiberbiztonsági termékek és megoldások bevezetésének elősegítése

hosszú távú stratégiai együttműködés biztosítása az iparágak, a kutatóközösségek és a kormányok között

költséges infrastruktúrák esetében közös beruházások és az ilyen infrastruktúrák megosztása

Európai kompetenciaközpont:

Koordinálja a 2021–2027-as időszakra szóló következő hosszú távú uniós költségvetés keretében a Digitális Európa és a Horizont Európa programok égisze alatt a kiberbiztonság céljára előirányzott pénzeszközöket. A központ a **kiberbiztonsági** kutatás és innováció előmozdítása érdekében támogatást nyújt a hálózatnak és a Közösségnek. Emellett **közös beruházásokat** szervez az EU, a tagállamok és az ipar számára. Például a Digitális Európai program keretében **2 milliárd eurót** fordítanak az EU digitális gazdaságának, társadalmának és demokráciájának védelmére az EU kiberbiztonsági ágazatának fellendítése, valamint a legkorszerűbb kiberbiztonsági berendezések és infrastruktúra finanszírozása révén.

A nemzeti koordinációs központok hálózata:

Minden tagállam kijelöl egy-egy nemzeti koordinációs központot a hálózat élére, amely szerepet vállal az új kiberbiztonsági képességek fejlesztésében és a szélesebb körű kompetenciaépítésben. A hálózat segít azonosítani a tagállamokban megvalósuló, leginkább releváns kiberbiztonsági projekteket, és támogatást nyújt számukra.

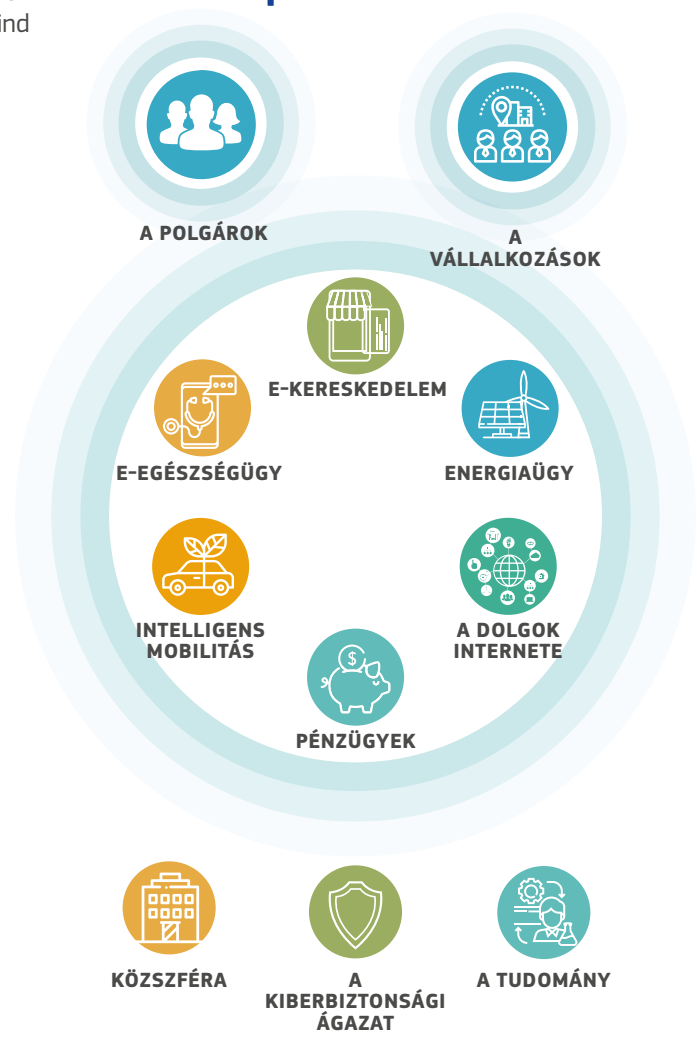
Kompetenciaközösség:

a kutatás, a magán- és a közszféra kiberbiztonsági érdekelt feleinek nagy, nyitott és sokszínű csoportja, ideértve mind a polgári, mind a védelmi hatóságokat.

Mi fog javulni?

- a munka megfelelőbb koordinálása;
- a szakértelemhez való hozzáférés;
- a tesztelési és kísérleti létesítményekhez való hozzáférés;
- a termékek kiberbiztonságának értékelése;
- az innovatív kiberbiztonsági termékekhez és megoldásokhoz való hozzáférés;
- a termékek és szolgáltatások piaci bevezetésének támogatása;
- fokozott láthatóság a potenciális befektetők és üzleti partnerek irányában;
- költségmegtakarítás más tagállamokkal való társbefektetés révén;
- az Európai Unió arra irányuló kapacitása, hogy önállóan biztosítsa gazdasága és demokráciája védelmét;
- az EU mint új globális vezető a kiberbiztonság terén.

Ki profitál ebből?



Kiadóhivatal

Print ISBN 978-92-79-92458-3 doi:10.2775/15938 NA-04-18-693-HU-C
PDF ISBN 978-92-79-92495-8 doi:10.2775/89417 NA-04-18-693-HU-N