Az Európai Unió
Tanácsa

Brüsszel, 2017. december 12.
(OR. en)

15748/17

CYBER 215
TELECOM 362
ENFOPOL 618
JAI 1206
MI 959
COSI 333
JAIEX 117
RELEX 1122
IND 377
CSDP/PSDC 720
COPS 400
POLMIL 167

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2017. december 12.
Címzett:	a delegációk
Előző dok. sz.:	14435/17 + COR 1
Tárgy:	Cselekvési terv az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről szóló tanácsi következtetések végrehajtására – Cselekvési terv (2017. december 12.)

Mellékelten továbbítjuk a delegációknak az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről szóló tanácsi következtetések végrehajtására irányuló cselekvési tervet, amelyet az Általános Ügyek Tanácsa 2017. december 12-én elfogadott.

MELLÉKLET

Az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről szóló tanácsi következtetések végrehajtására irányuló ezen cselekvési terv stratégiai szintű dokumentum, amely az Európai Tanácstól 2017. október 19-én és a Tanácstól 2017. október 24-én kapott megbízás nyomán készült. Amint a 2017. november 20-i tanácsi következtetések is előrevetítették, a cselekvési terv élő dokumentum lesz, így azt a Tanács rendszeresen felülvizsgálja és naprakésszé teszi. Célja, hogy a tanácsi következtetések és a lentebb részletezett fellépések végrehajtása horizontális felügyeletének és stratégiai nyomon követésének eszközéül szolgáljon.

Fellépés[1]	**Vezető/elsődlegesen felelős**	**Érdekelt felek és/vagy egyéb érintett felek**	**Határidő**	**Elért eredmények**	**Megjegyzések/észrevételek**
A kiberbiztonsági irányelv teljes körű és hatékony átültetésének és végrehajtásának biztosítása					
A kiberbiztonsági irányelv átültetése és végrehajtása	Tagállamok; Európai Bizottság		2018. május	A Bizottság összegzi az elért eredményeket, majd azokat az együttműködési csoport megvitatja	
A tagállamok közötti hatékony stratégiai együttműködés biztosítása az együttműködési csoporton belül	Tagállamok / a Tanács elnöksége	Európai Bizottság, ENISA		Az elért eredményeket az együttműködési csoport a rendszeres jelentése keretében összegzi	Az együttműködési csoport munkájának részletesebb kidolgozása a csoport kétéves munkaprogramjában történik

[1] A fellépések végrehajtására adott esetben a többéves pénzügyi kereten belüli források figyelembevételével kerül sor.

a CSIRT-hálózat teljes körű operatív képességének elérése	Tagállamok / a Tanács elnöksége	ENISA, Európai Bizottság		Az elért eredményeket a hálózat a rendszeres jelentése keretében összegzi az együttműködési csoportnak	
A nagy léptékű kiberbiztonsági események elhárítását célzó uniós szintű intézkedések fokozása rendszeres páneurópai kiberbiztonsági gyakorlatok végzése révén					
Kiberdiplomáciai gyakorlatok végzése a rosszindulatú kibertevékenységekkel szembeni küzdelem közös diplomáciai keretének alkalmazásáról	EKSZ	Tagállamok, Európai Bizottság és ENISA		A Tanács egymást követő elnökségei, a keret alkalmazásáról folytatott megbeszélések az EE elnökség alatt kezdődtek	
Rendszeres „CYBER EUROPE” gyakorlatok végzése	Az elnökség a tagállamokkal közösen	Tagállamok, ideértve a CSIRT-hálózatot, ENISA, EKSZ, Európai Bizottság			A gyakoriságot az ENISA megbízásának keretében történő feladatmeghatározáskor és az ENISA igazgatótanácsában folytatott megbeszélések során állapítják meg

Rendszeres stratégiai kiberbiztonsági gyakorlatok végzése a különböző tanácsi formációkban	Elnökség	Az EKSZ és/vagy az Európai Bizottság támogatás a mellett		„EU CYBRID 2017” gyakorlat végzése az EE elnökség alatt a Külügyek Tanácsa/Védelem számára	A rendszerességet a Tanács keretében ülésező tagállamok állapítják meg
Az Európai Uniós Kiberbiztonsági Ügynökségről, az 526/2013/EU rendelet hatályon kívül helyezéséről, valamint az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról szóló európai parlamenti és tanácsi rendelet (a „kiberbiztonsági jogszabály”)[2] társjogalkotók általi elfogadása					
A kiberkérdésekkel foglalkozó horizontális munkacsoport részletes megbeszélést folytat a jogalkotási javaslatról, előkészítve az általános megközelítést	BG elnökség		2018. június	A javaslat vizsgálatát az EE elnökség vezeti	
A társjogalkotók közötti tárgyalások véglegesítése	AT elnökség		2018. december		Indikatív határidő

[2] A végrehajtás nem sérti az Európai Parlament hatásköreit.

A kiberbiztonsági kompetenciaközpontok hálózatának és ahhoz kapcsolódóan egy európai kiberbiztonsági kutatási és kompetenciaközpontnak a létrehozása					
A kiberbiztonsági kompetenciaközpontok hálózatának és ahhoz kapcsolódó európai kiberbiztonsági kutatási és kompetenciaközpontnak a létrehozására vonatkozó hatásvizsgálat, költségvetési előrejelzés és releváns jogi eszközök kidolgozása	Európai Bizottság	Tagállamok, EKSZ, EDA	2018. június		A kidolgozott eszközökkel kapcsolatos további lépésekről a Tanács keretében ülésező tagállamok döntenek
Kísérleti fázis megkezdése a „Horizont 2020” keretprogramon belül	Európai Bizottság	Tagállamok, kiberbiztonsági együttműködési csoport	2018 vége/2019 eleje		

Európai kapacitás kidolgozása a polgárok, vállalkozások és kormányok számára a digitális egységes piacon rendelkezésre álló termékekben és szolgáltatásokban használt kriptográfiai eszközök erősségének értékelésére	Tagállamok		2019		
Elegendő finanszírozás biztosítása a kiberreziliencia kialakításának, valamint a kiberbiztonsággal kapcsolatos kutatás-fejlesztésre Unió-szerte irányuló erőfeszítéseknek a támogatására					
A kiberbiztonság területére fordított elegendő finanszírozás biztosítása, a rendelkezésre álló forrásokra figyelemmel	Tagállamok; Európai Bizottság		2020		

A kiberreziliencia kialakításához, valamint a kiberbiztonsággal kapcsolatos kutatás-fejlesztésre Unió-szerte irányuló erőfeszítéseihez nyújtott közszektorbeli hozzájárulások fokozása	Tagállamok		2020		
A kiberreziliencia kialakításához, valamint a kiberbiztonsággal kapcsolatos kutatás-fejlesztésre Unió-szerte irányuló erőfeszítéseihez nyújtott magánszektorbeli hozzájárulások ösztönzése	Európai Bizottság	Európai Kiberbiztonsági Szervezet (ECSO) támogatásával	2018		
Az új technológiák kiberbiztonsági alkalmazásaiba való beruházások növelése	Európai Bizottság, tagállamok	Európai Kiberbiztonsági Szervezet (ECSO) támogatásával	2020		

Egy Kiberbiztonsági Vészhelyzet-elhárítási Alap létrehozására irányuló esetleges javaslat vizsgálata	Tanács[3]				Ennek vizsgálatára kizárólag abban az esetben kerül sor, ha az Európai Bizottság javaslatot nyújt be
Elegendő finanszírozási forrás megtartása kiberbiztonsági célokra a meglévő eszközök és elfogadott programok keretében	Tagállamok, Európai Bizottság	EBB	2020		

[3] Az Európai Parlament hatáskörének sérelme nélkül, amennyiben alkalmazandó.

Hiteles, megbízható és összehangolt kiberbiztonsági szolgáltatások nyújtása és azok irányítása az uniós intézmények számára					
Az uniós intézmények, szervek és hivatalok kiberbiztonsági irányításának tisztázása és harmonizálása	Tanács, Európai Bizottság és EKSZ	Uniós intézmények, szervek és hivatalok	2020	Az irányításról és az annak terén elért eredményekről jelentést kell benyújtani a kiberkérdésekkel foglalkozó horizontális munkacsoporthoz	
Megfelelő erőforrások és támogatás biztosítása a CERT-EU fejlesztéséhez	Uniós intézmények, szervek és hivatalok		2020	A CERT-EU rendszeresen jelentést tesz a munkacsoportnak a hatáskörébe tartozó intézményeket ért kiberfenyegetésekről. A CERT-EU számára biztosítandó erőforrások kérdése szerepelhet a munkacsoport napirendjén	
A kibertudatosság, a digitális készségek, az oktatás és a képzés hangsúlyosabbá tétele					
Hatékonyabb kibertudatossági kampányok a tagállamokban	Tagállamok	ENISA	2020		

A kiberbiztonság témájának fokozott bevonása a felsőoktatási, oktatási és szakképzési programok tantervébe	Tagállamok	Európai Bizottság, ECSO	2020	Az eredményeket a tagállamok és az Európai Bizottság követi nyomon	
Oktatási kapcsolattartók hálózatának létrehozása	Tagállamok	ENISA	2020		
Kiberbiztonsági gyakornoki programok általánossá tétele és fokozása	Tagállamok	Európai Bizottság, ECSO	2020		
A kiberbiztonsággal kapcsolatos tájékozottság kialakítása a kritikus társadalmi és gazdasági tevékenységekben részt vevő közigazgatási szervek körében	Tagállamok		2020	A hat tagállam, az EKSZ és az EDA által 2015 májusában aláírt kiberhigiéniai kötelezettségvállalás	

Az EU kapacitásának növelése a rosszindulatú kibertevékenységek megelőzésére, megakadályozására, felderítésére és elhárítására					
A kiberbiztonság szempontjának általános érvényesítése a már meglévő uniós szintű válságkezelési mechanizmusokban	Európai Bizottság, Tanács	EKSZ, uniós ügynökségek	2018		
A kiberbiztonsági eseményekre adandó válasz megfelelő kezelése a nemzeti válságkezelési mechanizmusokban, valamint a szükséges eljárások létrehozása az uniós szintű együttműködéshez	Tagállamok		2018		
az uniós kibervédelmi szakpolitikai keret naprakésszé tétele	Tagállamok, EKSZ, EDA, Európai Bizottság		2018		
A kiberbiztonsági eseményekre való reagálásért felelős polgári és katonai közösségek közötti együttműködés ösztönzése	Tagállamok				

Kibervédelmi képzési és oktatási fórum létrehozása	Európai Bizottság	EKSZ, EDA, EBVF	2018 vége		
A javasolt védelmi kezdeményezések teljes körű kiaknázása az EU kibervédelmi képességei fejlesztésének felgyorsítása érdekében	Tagállamok	EKSZ, EDA, Európai Bizottság			A kibervédelmi projektek kidolgozására sor kerülhet a PESCO keretében, amennyiben a PESCO-ban részt vevő tagállamok azt szükségesnek ítélik. Az Európai Védelmi Alap finanszírozhat kibervédelmi projekteket, amennyiben azok szerepelnek a munkaprogramokban

A bűnözés elleni küzdelem erősítése a kibertérben, valamint a kibertérben való hatékony büntető igazságszolgáltatás előtt álló akadályok felszámolása					
A sötét világhálón (Dark Web) folytatott, terjedő bűnözés elleni küzdelemre vonatkozó ütemterv kidolgozása	Europol	Tagállamok	2018 eleje	Az ütemterv jóváhagyása és végrehajtásának nyomon követése a COSI feladata	
A Bizottság által javasolt gyakorlati intézkedések végrehajtása a titkosítással kapcsolatban a büntetőeljárások keretében felmerülő kihívások leküzdésére, az emberi jogok és az alapvető szabadságok tiszteletben tartása mellett.	Európai Bizottság	Tagállamok, Europol	folyamatban	Eredmények nyomon követése: CATS	

A bűnüldöző és igazságügyi hatóságoknak a bűncselekmények nyomozására és az elkövetők büntetőeljárás alá vonására való képességeinek javítása	Tagállamok	Európai Bizottság		Az eredmények nyomon követése a CATS által, javaslat önkéntes magatartási kódexek kidolgozására az internethozzáférés-szolgáltatók számára az egyes IPv4-címek mögött álló előfizetők számának korlátozása érdekében, a szolgáltatói szintű hálózati címfordítást (CGN) felváltó alternatív technológiák alkalmazásával (tagállamok). Az Európai Bizottságnak az uniós internetfórumon fel kell vetnie a forrásportok számsora naplózásának kérdését az internetes tartalomszolgáltatóknál.	A kiberbűnözés elleni küzdelemről készített kölcsönös értékelések hetedik fordulójáról szóló GENVAL-zárójelentés ajánlásainak figyelembevétele

Ösztönzők nyújtása a magánszektor részére az IPv6 bevezetésére, például a vonatkozó követelményeknek a közbeszerzésekben való esetleges előírásával	Tagállamok	Európai Bizottság	folyamatban	Az eredmények nyomon követése a Tanács érintett előkészítő szervei által (a kiberkérdésekkel foglalkozó horizontális munkacsoport, COSI)	
Vészhelyzet-elhárítási protokoll kidolgozása és jóváhagyása a nagy léptékű kiberesemények re való koordinált uniós bűnüldözési válaszra vonatkozóan.	Europol	Tagállamok, Európai Bizottság, EKSZ, Tanács	2018 eleje	A protokoll jóváhagyása és végrehajtásának nyomon követése a COSI feladata	
A bűnüldöző hatóságok elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférésének elősegítéséről szóló jogalkotási javaslat benyújtása	Európai Bizottság	Tanács, Európai Parlament	2018 eleje	Eredmények nyomon követése: CATS	

Az elektronikus bizonyítékokhoz való, határokon átnyúló hozzáférés javítását szolgáló gyakorlati intézkedések végrehajtásában elért eredményekről szóló jelentés benyújtása (kitérve a bűnüldöző hatóságok és a magánszektor közötti együttműködésre is)	Európai Bizottság	Tagállamok	2017 vége	Eredmények nyomon követése: CATS	
Teljes mértékben működőképes platform létrehozása a tagállamok számára az európai nyomozási határozatok online formanyomtatványainak és az elektronikus bizonyítékoknak a biztonságos cseréjére.	Európai Bizottság	Tagállamok	2019 közepe	Eredmények nyomon követése: CATS	

A nemzetközi együttműködés erősítése a nyitott, szabad, békés és biztonságos globális kibertér érdekében					
A párbeszéd folytatása a nemzetközi partnerekkel a nyitott, szabad, békés és biztonságos globális kibertér iránti globális támogatás elérése érdekében	EKSZ, Tanács, Európai Bizottság	Tagállamok	2019 közepe	Eredmények nyomon követése: a kiberkérdésekkel foglalkozó horizontális munkacsoport	
Uniós kiberkapacitás-építési hálózat létrehozása és uniós kiberkapacitás-építési iránymutatások kidolgozása	EKSZ, Európai Bizottság, a tagállamok támogatásával				Lehetséges együttműködés a számítástechnikai szakértők világfórumával (GFCE)
EU–NATO együttműködés kialakítása az oktatás és képzés területén	EKSZ, Tanács, EDA	Tagállamok			
Az EU–NATO együttműködés folytatása a kibervédelmi gyakorlatok területén, valamint a bevált válságkezelési gyakorlatok megosztása	EKSZ, Tanács	Tagállamok, EDA, Európai Bizottság			

Az új technológiák kritikus kiberbiztonsági alkalmazásainak kezelése az érintett nemzetközi exportellenőrzési rendszerek keretében	Tagállamok, Európai Bizottság				
Egységes uniós álláspont kialakítása és kommunikálása a globális internetirányításról szóló megbeszélésekhez.	Tanács, Európai Bizottság, EKSZ	Tagállamok	2018, és folyamatban	A COSI-nak elő kell segítenie egy közös uniós álláspont elfogadását az általános adatvédelmi rendelet előírásainak megfelelő olyan WHOIS rendszerre vonatkozóan, amely gyors és időszerű hozzáférést biztosít a domain-nevek és az IP-címek tulajdonosaira vonatkozó pontos nyilvántartási adatokhoz (WHOIS-adatok) jogszerű célokból, így például bűnüldözési, fogyasztóvédelmi, valamint a szellemitulajdon-jogok védelmével vagy kiberbiztonsági tevékenységekkel kapcsolatos célokból.	