

Bruselj, 20. marec 2019
(OR. en)

7737/19

CYBER 101	RELEX 287
COPEN 118	TELECOM 141
COPS 92	DAPIX 109
COSI 52	CATS 43
DATAPROTECT 98	CSC 111
IND 102	CSCI 47
JAI 313	IA 106
JAIEX 44	EJUSTICE 44
POLMIL 31	

IZID POSVETOVANJA

Pošiljatelj:	generalni sekretariat Sveta
Datum:	19. marec 2019
Prejemnik:	delegacije
Št. predh. dok.:	6866/19
Zadeva:	Sklepi Sveta o krepitvi zmogljivosti in zmožnosti na področju kibernetске varnosti v EU

V prilogi vam pošiljamo sklepe Sveta o krepitvi zmogljivosti in zmožnosti na področju kibernetске varnosti v EU, ki jih je Svet za splošne zadeve sprejel 19. marca 2019.

Sklepi Sveta o krepitvi zmogljivosti in zmožnosti na področju kibernetске varnosti v EU

Svet Evropske unije –

1. OB OPOZARJANJU na sklepe z naslovom „Odpornost, odvracanje in obramba: okrepitev kibernetске varnosti za EU“¹;
2. OB OPOZARJANJU na sklepe o usklajenem odzivu EU na velike kibernetске incidente in krize²;
3. OB OPOZARJANJU na sklepe o krepitvi zunanjih kibernetских zmogljivosti³;
4. OB VNOVIČNEM POUDARJANJU, da je visoko raven varnosti omrežij in informacijskih sistemov mogoče zagotoviti s povečanjem zmogljivosti in zmožnosti držav članic ter institucij, agencij in organov EU na področju kibernetске varnosti in z nadaljnjo krepitvijo njihove kibernetске odpornosti;
5. OB POZDRAVLJANJU napredka, ki so ga dosegle države članice pri krepitvi skupin za odzivanje na incidente na področju računalniške varnosti (skupine CSIRT);
6. OB IZRAŽANJU PRIZNANJA državam članicam za ustanovitev mreže skupin CSIRT z dejavno podporo Komisije in ENISA ter za okrepljeno sodelovanje na strateški ravni v okviru skupine za sodelovanje na področju varnosti omrežij in informacij, ki jo sestavljajo države članice, Komisija in ENISA;

¹ Dok. 14435/17 (Sklepi Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: „Odpornost, odvracanje in obramba: okrepitev kibernetске varnosti za EU“ z dne 20. novembra 2017).

² Dok. 10086/18 (Sklepi o usklajenem odzivu EU na velike kibernetске incidente in krize z dne 26. junija 2018).

³ Dok. 10496/18 (Sklepi Sveta o smernicah za krepitev zunanjih kibernetских zmogljivosti EU).

7. OB POUDARJANJU ključne vloge, ki jo ima skupina za sodelovanje na področju varnosti omrežij in informacij pri zagotavljanju potrebnih smernic za čim večjo uskladitev pristopa pri prenosu direktive o varnosti omrežij in informacij⁴ po vsej EU ter pri reševanju pomembnih vprašanj kibernetске varnosti;
8. OB PRIZNAVANJU obstoječe podpore, ki jo Komisija nudi državam članicam za krepitev zmogljivosti skupin CSIRT prek instrumenta za povezovanje Evrope;
9. OB PRIZNAVANJU podpore organom kazenskega pregona za krepitev zmogljivosti v boju proti kibernetškemu kriminalu prek Sklada za notranjo varnost in CEPOL;
10. OB POZDRAVLJANJU posodobitve okvira politike EU za kibernetško obrambo s ciljem nadaljnje podpore razvoju zmogljivosti držav članic za kibernetško obrambo;
11. OB IZRAŽANJU ZADOVOLJSTVA nad napredkom, ki so ga države članice dosegle pri izvajanju direktive o varnosti omrežij in informacij;
12. OB UGOTAVLJANJU, da je kibernetška varnost kompleksno, soodvisno in stalno spreminjajoče se področje, ki zahteva prilagajanje političnega in pravnega okvira novim tehnološkim trendom in tehnologijam v vzponu, kot so umetna inteligenca, veriga podatkovnih blokov in kvantno računalništvo;

⁴ Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016).

13. OB POUDARJANJU, da so programi izobraževanja in usposabljanja, povezani s kibernetško varnostjo, ter obveščanje in ozaveščanje o varnostnih grožnjah za končne uporabnike ključni za zmanjševanje tveganj za kibernetško varnost;
14. OB POUDARJANJU, da so vaje za kibernetško varnost učinkovito orodje za ocenjevanje in nadaljnje izboljševanje ravni pripravljenosti EU in njenih držav članic za preprečevanje velikih kibernetških incidentov in kriz;
15. OB VNOVIČNEM POUDARJANJU, da je kibernetški prostor brez meja, kar pomeni, da so čezmejni in medsektorski vidik ter sodelovanje ključna podlaga dejavnosti in pobud za krepitev kibernetških zmogljivosti.
16. OB IZPOSTAVLJANJU pomena sodelovanja med javnim sektorjem, zasebnim sektorjem in akademskimi krogi, zlasti prek skupnih projektov;
17. OB IZPOSTAVLJANJU pomena civilno-vojaškega sodelovanja ob prizadevanjih za uresničitev skupnih ciljev na kibernetškem področju ter zagotovitev usklajenega in učinkovitega odzivanja na kibernetške grožnje –
18. OPOZARJA na napredek, ki ga je dosegla skupina držav članic pri razvoju enot za hitro odzivanje na kibernetške grožnje s ciljem poglobitve prostovoljnega sodelovanja na kibernetškem področju prek medsebojne pomoči;

19. POZDRAVLJA razprave v Svetu o predlogu Komisije za uredbo Evropskega parlamenta in Sveta o ustanovitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetno varnost ter mreže nacionalnih koordinacijskih centrov;
20. SPODBUJA dejavno udeležbo pri delu, ki poteka v okviru skupine za sodelovanje na področju varnosti omrežij in informacij, zlasti v zvezi s krepitvijo kibernetnih zmogljivosti;
21. SPODBUJA skupino za sodelovanje na področju varnosti omrežij in informacij pri delu v zvezi z usklajenim odzivom EU na velike kibernetne incidente in krize;
22. POZIVA države članice, naj nadgradijo nacionalne strategije za kibernetno varnost, slednji pa ob upoštevanju posebnih zahtev za posamezne sektorje namenijo posebno pozornost;
23. POZIVA države članice, naj stalno spremljajo in ocenjujejo učinke ukrepov, sprejetih za krepitev kibernetne odpornosti, ter povečajo kibernetne zmogljivosti in zmožnosti na nacionalni ravni;
24. POZIVA države članice, naj kibernetno varnost in digitalno pismenost vključijo v učne načrte na vseh ravneh izobraževanja (v osnovnošolsko, srednješolsko in terciarno izobraževanje ter v vseživljenjsko učenje) in, kjer je to ustrezno, v uveljavljene poklicne profile in poklicne profile prihodnosti;
25. POZIVA države članice, naj izvedejo pobude za ozaveščanje o kibernetni varnosti in za kibernetno higieno, namenjene javnosti in končnim uporabnikom, še posebej pa zaposlenim v javnem sektorju;
26. SPODBUJA države članice, naj izvedejo vaje iz kibernetne varnosti na nacionalni ravni, izvedejo pa naj jih tudi na ravni EU in/ali v njih sodelujejo, da bi tako preskusili in se usposobili za strateške in tehnološke vidike ter učinkovito in na praktični ravni razvili potrebna znanja in spretnosti;

27. POZIVA države članice, naj nadaljujejo razvoj tehničnih in operativnih zmogljivosti svojih skupin CSIRT na področju kibernetске varnosti pri preprečevanju in blaženju incidentov ter odzivanju nanje;
28. POZIVA Komisijo in ENISA, naj še naprej podpirata razvoj zmogljivosti in zmožnosti mreže skupin CSIRT po državah članicah s ciljem boljšega sodelovanja, izmenjave informacij o incidentih in učinkovitega odzivanja na velike čezmejne incidente;
29. POZIVA države članice, naj še naprej pomagajo organom pregona pri razvoju posebnih kompetenc v sodelovanju s pristojnimi evropskimi organi za učinkovit boj proti kibernetски kriminaliteti na ravni EU;
30. POZIVA države članice, naj povečajo naložbe v krepitev kibernetских zmogljivosti;
31. POZIVA Komisijo in ENISA, naj izvedeta programe ozaveščanja in usposabljanja zaposlenih v institucijah, agencijah in organih EU o kibernetски varnosti;
32. POZIVA EU in njene države članice, naj prostovoljno izmenjujejo informacije in dobre prakse, da bi prispevale k opredelitvi in uresničitvi glavnih potreb po krepitvi kibernetских zmogljivosti na nacionalni ravni in ravni EU;
33. POZIVA EU in njene države članice, naj podprejo raziskave v zvezi s kibernetско varnostjo in slednjo promovirajo kot problematiko na drugih študijskih področjih ter tako različna področja raziskav in razvoja, povezana s kibernetско varnostjo, povežejo v celoto, hkrati pa spodbujajo odličnost na področju raziskav v zvezi s kibernetско varnostjo;
34. POZIVA EU in njene države članice, naj razvijejo raziskave v zvezi s kibernetско varnostjo, ki bodo upoštevale družbene potrebe in rezultate raziskav vključevale na trg;
35. POZIVA EU in njene države članice, naj kibernetско varnost, če je to primerno, upoštevajo v javnih naročilih na področju IKT.