Съвет на
Европейския съюз

Брюксел, 20 март 2019 г.
(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	

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	19 март 2019 г.
До:	Делегациите
№ предх. док.:	6866/19
Относно:	Заключения на Съвета относно капацитета за киберсигурност и изграждането на способности в ЕС

Приложено се изпращат на делегациите заключенията на Съвета относно капацитета за киберсигурност и изграждането на способности в ЕС, приети на заседанието на Съвета по общи въпроси на 19 март 2019 г.

ПРИЛОЖЕНИЕ

Заключения на Съвета относно капацитета за киберсигурност и изграждането на способности в ЕС

Съветът на Европейския съюз,

1. КАТО ПРИПОМНЯ заключенията си „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“[1];

2. КАТО ПРИПОМНЯ заключенията си относно координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността[2];

3. КАТО ПРИПОМНЯ заключенията си относно изграждане на външен киберкапацитет на ЕС[3];

4. КАТО ИЗТЪКВА ОТНОВО, че високо равнище на мрежова и информационна сигурност може да се постигне чрез укрепване на капацитета и способностите в областта на киберсигурността на държавите членки и на институциите, агенциите и органите на ЕС и последващо засилване на тяхната киберустойчивост;

5. КАТО ПРИВЕТСТВА напредъка, постигнат от държавите членки в укрепването на екипите за реагиране при инциденти с компютърната сигурност (CSIRT);

6. КАТО ПРИВЕТСТВА създаването от държавите членки на мрежата на CSIRT с активната подкрепа на Комисията и ENISA, както и засиленото сътрудничество на стратегическо равнище чрез групата за сътрудничество за МИС, съставена от държавите членки, Комисията и ENISA;

---

1 14435/17 (Заключения на Съвета относно Съвместното съобщение до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ от 20 ноември 2017 г.)

2 10086/18 (Заключения относно координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността от 26 юни 2018 г.)

3 10496/18 (Заключения на Съвета относно насоки за изграждането на външен киберкапацитет на ЕС от 26 юни 2018 г.)

7. КАТО ИЗТЪКВА ключовата роля на групата за сътрудничество за МИС за предоставянето на необходимите насоки за уеднаквяване в най-голяма степен на подхода за транспонирането на директивата за МИС[4] в целия ЕС, както и за разрешаване на свързани с киберсигурността въпроси;

8. КАТО ОТЧИТА съществуващата подкрепа, предоставяна от Комисията на държавите членки за изграждането на капацитет на CSIRT чрез Механизма за свързване на Европа;

9. КАТО ОТЧИТА подкрепата, предоставена на правоприлагащите органи за изграждане на капацитет в борбата с киберпрестъпността чрез фонд „Вътрешна сигурност“ и CEPOL;

10. КАТО ПРИВЕТСТВА актуализирането на политическата рамка на ЕС за кибернетична отбрана с цел допълнително подпомагане на развитието на способностите за кибернетична отбрана на държавите членки;

11. КАТО ПРИВЕТСТВА напредъка, постигнат от държавите членки при изпълнението на директивата за МИС;

12. КАТО ОТБЕЛЯЗВА, че киберсигурността е сложна, взаимозависима и постоянно променяща се област, което налага адаптирането на политическата и правната рамка към нови технологични тенденции и нововъзникващи технологии като изкуствения интелект, блоковата верига и квантовата изчислителна технология;

---

[4] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г.).

13. КАТО ИЗТЪКВА, че програмите за образование и обучение в областта на киберсигурността, както и информирането и повишаването на осведомеността относно заплахите за сигурността на крайните потребители са от ключово значение за намаляването на рисковете за киберсигурността;

14. КАТО ПОДЧЕРТАВА, че киберученията са ефективен инструмент за оценяването и допълнителното подобряване на равнището на подготвеност на ЕС и неговите държави членки за борба с мащабните инциденти и кризи в областта на киберсигурността;

15. КАТО ИЗТЪКВА ОТНОВО, че киберпространството няма граници, което означава, че трансграничните и междусекторните перспективи и сътрудничество са основен принцип на дейностите и инициативите за изграждане на капацитет за киберсигурност;

16. КАТО ИЗТЪКВА важността на сътрудничеството между публичния сектор, частния сектор и академичните среди, по-специално посредством съвместни проекти;

17. КАТО ИЗТЪКВА значението на гражданско-военното сътрудничество, работата по отношение на общите цели в кибернетичната област с цел гарантиране на последователен и ефективен отговор на киберзаплахите;

18. ОТБЕЛЯЗВА напредъка, постигнат от група държави членки при разработването на екипи за бързо реагиране при кибератаки с цел задълбочаване на доброволното сътрудничество в кибернетичната област посредством взаимопомощ;

19. ПРИВЕТСТВА текущите обсъждания в Съвета относно предложението на Комисията за регламент на Европейския парламент и на Съвета за създаване на Европейски център за промишлена, технологична и изследователска компетентност в областта на киберсигурността и мрежа от национални координационни центрове;

20. НАСЪРЧАВА активното участие в текущата работа на групата за сътрудничество за МИС, по-специално по отношение на изграждането на киберкапацитет;

21. НАСЪРЧАВА текущата работа на групата за сътрудничество за МИС относно координирания отговор на ЕС при мащабни инциденти и кризи в областта на киберсигурността;

22. ПРИКАНВА държавите членки да надградят собствените си национални стратегии в областта на киберсигурността и да интегрират киберсигурността в други области, като отчитат специфичните за сектора изисквания;

23. ПРИКАНВА държавите членки да извършват непрекъснато наблюдение, проучване/оценка на въздействието на мерките, предприети за укрепване на киберустойчивостта и на капацитета и способностите в кибернетичната област на национално равнище;

24. ПРИКАНВА държавите членки да интегрират киберсигурността и цифровата грамотност в учебните програми на всички равнища на образование (основно, средно, висше и учене през целия живот) при целесъобразност въз основа на установени и бъдещи длъжностни характеристики;

25. ПРИКАНВА държавите членки да осъществяват инициативи за осведоменост в областта на киберсигурността и киберхигиената за обществеността и крайните потребители, насочени към служителите в публичния сектор;

26. НАСЪРЧАВА държавите членки да провеждат учения в областта на киберсигурността на национално равнище, както и да провеждат и/или участват в учения в областта на киберсигурността на равнище ЕС с цел изпитване и обучение на стратегическите и технологичните аспекти и ефективно разработване на необходимите умения на практическо равнище;

27. ПРИКАНВА държавите членки да продължат да разработват техническите и оперативните способности в областта на киберсигурността на екипите си за реагиране при инциденти с компютърната сигурност в областта на предотвратяването на инциденти, смекчаването на последствията от тях и отговора на инциденти;

28. ПРИЗОВАВА Комисията и ENISA да продължат с подкрепата си за разработване на капацитета и способността на мрежата на CSIRT от страна на държавите членки за по-добро сътрудничество, обмен на информация относно инциденти и ефективен отговор при мащабни трансгранични инциденти;

29. ПРИКАНВА държавите членки да продължат да подпомагат правоприлагащите органи да разработват специфични компетентности в сътрудничество с компетентните европейски органи с оглед на ефективната борба с киберпрестъпността на равнище ЕС;

30. ПРИКАНВА държавите членки да увеличат инвестициите в изграждането на киберкапацитет;

31. ПРИЗОВАВА Комисията и ENISA да изпълняват програми и да провеждат обучения за повишаване на осведомеността по въпросите на киберсигурността, насочени към служители на институциите, агенциите и органите на ЕС;

32. ПРИЗОВАВА ЕС и държавите членки да обменят информация и най-добри практики на доброволна основа с оглед да допринасят за определянето и задоволяването на основните потребности при изграждането на киберкапацитет на национално равнище и на равнище ЕС;

33. ПРИКАНВА ЕС и неговите държави членки да подкрепят научните изследвания в областта на киберсигурността и да насърчават разглеждането на киберсигурността в други области на обучение, като обединяват различни клонове на свързаната с киберсигурността научноизследователска и развойна дейност в едно цяло, както и да насърчават върховите постижения при научните изследвания в областта на киберсигурността;

34. ПРИКАНВА ЕС и неговите държави членки да разработват научни изследвания в областта на киберсигурността, които да отразяват обществените потребности и да интегрират резултатите от научните изследвания на пазара;

35. ПРИЗОВАВА ЕС и неговите държави членки да вземат предвид киберсигурността при изготвянето на обществените поръчки за ИКТ, когато е уместно.