



Брюксел, 10 юни 2022 г.
(OR. fr, en)

9716/22

LIMITE

CYBER 198
TELECOM 255
CSC 228
CSCI 74
FIN 590

БЕЛЕЖКА ПО ТОЧКИ I/A

От:	Генералния секретариат на Съвета
До:	Комитета на постоянните представители/Съвета
№ предх. док.:	9317/2/22 REV 2
Относно:	Проект за заключения на Съвета относно Специален доклад № 05/2022 на Европейската сметна палата, озаглавен „Киберсигурност в институциите, органите и агенциите на ЕС — нивото на подготвеност като цяло не съответства на заплахите“ - Одобряване

1. На 30 март 2022 г. Европейската сметна палата публикува своя Специален доклад № 05/2022, озаглавен „Киберсигурност в институциите, органите и агенциите на ЕС — нивото на подготвеност като цяло не съответства на заплахите“¹.
2. На заседанието си от 13 април 2022 г. Комитетът на постоянните представители възложи специалния доклад на Хоризонталната работна група по въпроси на кибернетичното пространство².

¹ 8040/22.

² 8041/22.

3. На 3 май 2022 г. представители на Сметната палата представиха специалния доклад на Хоризонталната работна група по въпроси на кибернетичното пространство. След обсъждането на доклада на същото заседание на работната група председателството изготви проект за заключения на Съвета, който беше обсъден от работната група на заседанието ѝ от 24 май 2022 г.
4. На 10 юни 2022 г. Хоризонталната работна група по въпроси на кибернетичното пространство постигна съгласие по текста, изложен в приложението.
5. Комитетът на постоянните представители се приканва да одобри този проект за заключения и да предложи на Съвета да ги приеме на някое от следващите си заседания.

ПРОЕКТ ЗА ЗАКЛЮЧЕНИЯ НА СЪВЕТА

относно Специален доклад № 05/2022 на Европейската сметна палата, озаглавен „Киберсигурност в институциите, органите и агенциите на ЕС — нивото на подготвеност като цяло не съответства на заплахите“

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

КАТО ПРИПОМНЯ заключенията си относно подобряване на разглеждането на специалните доклади, изготвяни от Сметната палата в рамките на процедурата по освобождаване от отговорност³;

1. ВЗЕМА ПОД ВНИМАНИЕ Специален доклад № 05/2022 на Европейската сметна палата, озаглавен „Киберсигурност в институциите, органите и агенциите на ЕС — нивото на подготвеност като цяло не съответства на заплахите“⁴.
2. ПОДЧЕРТАВА колко важно и спешно е да се повиши нивото на киберсигурност в институциите, органите и агенциите на ЕС, като се имат предвид неотдавнашното ускоряване на цифровия преход в рамките на институциите, чувствителността на информацията, която те обработват, все по-големият брой и сериозност на атаките срещу институциите, органите и агенциите на ЕС и нивото на заплахи, които ги застрашават.

³ 7515/00 + COR 1.

⁴ 8040/22.

3. ПРИПОМНЯ заключенията на Европейския съвет от 20 юни 2019 г.⁵, в които Европейският съвет прикани институциите на ЕС, заедно с държавите членки, да работят по мерки за укрепване на устойчивостта и за подобряване на културата на ЕС по отношение на сигурността спрямо кибернетични и хибридни заплахи от източници извън ЕС, и за да се защитят по-добре информационните и комуникационните мрежи на ЕС, както и процесите му на вземане на решения, от всякакъв вид злонамерени действия.
4. ПРИПОМНЯ заключенията си от 10 декември 2019 г. относно допълнителните усилия за укрепване на устойчивостта на хибридни заплахи и за борба с тях⁶, в които призова институциите, органите и агенциите на ЕС, с подкрепата на държавите членки, да гарантират капацитета на Съюза да защитава своя интегритет и да повишат сигурността на информационните и комуникационните мрежи и на процесите на вземане на решения на ЕС спрямо всякакви видове злонамерени действия въз основа на цялостна оценка на заплахите. За тази цел, в цитираните заключения, институциите, органите и агенциите на ЕС, с подкрепата на държавите членки, следва да разработят и приложат цялостен набор от мерки за гарантиране на своята сигурност, в съответствие с мандата, предоставен от Европейския съвет през юни 2019 г.⁷
5. ПРИПОМНЯ заключенията си от 22 март 2021 г. относно стратегията на ЕС за киберсигурност за цифровото десетилетие⁸, в които подчерта, че киберсигурността е изключително важна за функционирането на публичната администрация и институции и на национално равнище, и на равнище ЕС, както и за нашето общество и икономика като цяло.

⁵ EUCO 9/19.

⁶ 14972/19.

⁷ EUCO 9/19.

⁸ 6722/21.

6. ПРИПОМНЯ заключенията си от 23 май 2022 г. относно установяването на позицията на Европейския съюз в киберпространството⁹, в които институциите, органите и агенциите на ЕС бяха насърчени да участват в картографирането на съществуващите инструменти за сигурна комуникация в киберпространството, за да бъдат те обсъдени в съответните органи на Съвета и със съответните групи за сътрудничество, като мрежата на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) и мрежата за връзка на организациите при кибернетични кризи (EU CyCLONe).
7. ПОДЧЕРТАВА необходимостта от справяне със системния риск, който съществува във взаимосвързаността между институциите, органите и агенциите на ЕС, както и между тях и институциите на държавите членки, въпреки тяхната институционална независимост и административна автономност.
8. ВЗЕМА ПОД ВНИМАНИЕ констатациите в специалния доклад, а именно, че институциите, органите и агенциите на ЕС не са постигнали ниво на киберподготвеност, което да съответства на заплахите, и имат различни нива на зрялост на киберсигурността. ОТЧИТА, че нивото на подготвеност на институциите, органите и агенциите на ЕС в областта на киберсигурността, както и полезните взаимодействия между тях, следва да бъдат подобрени.
9. Във връзка с това настоятелно НАСЪРЧАВА институциите, органите и агенциите на ЕС да продължат да прилагат мерки за управление на риска в киберпространството, които гарантират съизмеримо ниво на киберсигурност, както е предвидено в предложената директива относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148, за да се подобри нивото им на подготвеност.
10. ПРИКАНВА институциите, органите и агенциите на ЕС да увеличат усилията си за защита срещу киберзаплахите и да засилят сътрудничеството си за установяване на съгласувани стандарти и спецификации, по-специално за обществените поръчки, проектите и услугите, свързани с киберсигурността, и да подобрят оперативната съвместимост на своите информационни системи, включително с цел да се гарантира сигурната комуникация на неklasифицирано съдържание.

⁹ 9364/22.

11. ПРИКАНВА Агенцията на Европейския съюз за киберсигурност (ENISA) и екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU), в рамките на съответните си правомощия, да засилят сътрудничеството си в подкрепа на институциите, органите и агенциите на ЕС по отношение на усилията им в областта на киберсигурността, по-специално по отношение на изграждането на капацитет за онези институции, органи и агенции на ЕС, които са с по-ниско ниво на зрялост на киберсигурността.
12. ВЗЕМА ПОД ВНИМАНИЕ заключенията и препоръките в специалния доклад и ОТЧИТА, че нивото на подготвеност на институциите, органите и агенциите на ЕС в областта на киберсигурността, както и полезните взаимодействия между тях, следва да бъдат съществено подобрени. Институциите, органите и агенциите на ЕС следва да разполагат с цялостна рамка за управление на риска в областта на киберсигурността, да извършват редовни оценки на риска и одити въз основа на обща или добре позната методика и международните стандарти и да систематизират програмите за повишаване на осведомеността и за обучение на персонала в областта на киберсигурността.
3. ИЗТЪКВА също така, че институциите, органите и агенциите на ЕС следва да заделят достатъчно средства в своите бюджети, за да се гарантира изпълнението на мерките за защита срещу киберзаплахи, като същевременно се спазва многогодишната финансова рамка, и ВЗЕМА ПОД ВНИМАНИЕ препоръката в специалния доклад да бъде назначен орган, който да представлява всички институции, органи и агенции на ЕС, и да му бъдат предоставени подходящ мандат и средства за мониторинг на спазването на общите правила за киберсигурност.
14. ОТЧИТА, че CERT-EU следва да бъде информиран незабавно за значителните киберинциденти в рамките на институциите, органите и агенциите на ЕС и за тази цел следва да разполага с подходящи ресурси, които са предвидими и адаптирани към настоящото ниво на заплаха и към нуждите на институциите, органите и агенциите на ЕС, по-специално откъм персонал, техническо оборудване и инфраструктура.

15. ОТБЕЛЯЗВА, че сътрудничеството и обменът на информация относно киберсигурността, както и оперативната съвместимост на сигурните канали за комуникация между институциите, органите и агенциите на ЕС следва да бъдат засилени и систематизирани. ПРИЗОВАВА в това сътрудничество и обмен на информация да бъдат включени и публичните органи, отговарящи за киберсигурността в държавите членки.
16. ВЗЕМА ПОД ВНИМАНИЕ отговорите на Комисията, CERT-EU и ENISA, придружаващи специалния доклад.
17. ПРИКАНВА Комисията да вземе предвид препоръките в специалния доклад и да демонстрира амбиция при разработването на политиките в областта на киберсигурността на институциите, органите и агенциите на ЕС, както и да се застъпва за повече полезни взаимодействия между тях.
