ЕВРОПЕЙСКА СМЕТНА ПАЛАТА

BG

Съобщение за пресата

Люксембург, 29 март 2022 г.

Органите на ЕС трябва да повишат подготвеността си в областта на киберсигурността

Броят на кибератаките срещу институциите на ЕС се увеличава рязко. Нивото на подготвеност по отношение на киберсигурността в тези институции е различно и като цяло не съответства на растящата заплаха. Тъй като органите на ЕС са тясно свързани, слабостите в един от тях могат да изложат останалите на заплахи за сигурността. Такива са заключенията на специалния доклад на Европейската сметна палата, който разглежда доколко управляващите органи на ЕС са подготвени да реагират на киберзаплахи. Одиторите препоръчват да се въведат обвързващи правила за киберсигурност и да се увеличат ресурсите, предоставени на Екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU). Одиторите посочват още, че Европейската комисия следва също да насърчава по-близкото сътрудничество между органите на ЕС, а CERT-EU и Агенцията на Европейския съюз за киберсигурност следва да се фокусират повече върху институциите на ЕС с по-малко опит в управлението на киберсигурността.

Броят на сериозните киберинциденти в органите на ЕС се е увеличил над десет пъти в периода между 2018 г. и 2021 г. Работата от разстояние предоставя значително по-голям брой потенциални точки за достъп за извършителите на такива атаки. Сериозните инциденти често се причиняват от сложни кибератаки, които обикновено са свързани с използването на нови методи и технологии, а разследването им и възстановяването след тях могат да отнемат седмици или месеци. Пример за това е кибератаката срещу Европейската агенция по лекарствата, която причини изтичане и манипулиране на чувствителни данни по начин, целящ да подкопае доверието във ваксините.

„Институциите, органите и агенциите на ЕС са привлекателни цели за потенциални извършители на атаки, особено групи, които са способни да провеждат много сложни незабележими атаки с цел кибершпионаж или други злонамерени цели“, заяви Бетина Якобсен, членът на ЕСП, който ръководи одита. *„Подобни атаки могат да имат значителни политически последици, да нанесат вреда върху цялостната репутация на ЕС и да подкопаят доверието в неговите институции. ЕС трябва да увеличи усилията си за защита на своите органи и институции.“*

Настоящото съобщение за пресата има за цел да представи основните послания на специалния доклад, приет от Европейската сметна палата. Пълният текст на доклада е публикуван на eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

Основната констатация на одиторите е, че институциите, органите и агенциите на ЕС невинаги са добре защитени срещу киберзаплахи. Те нямат единен подход в областта на киберсигурността, невинаги прилагат основни механизми за контрол и ключови добри практики в областта на киберсигурността, нито предоставят систематично обучения по киберсигурност. Размерът на отделените за киберсигурност ресурси варира значително, като някои органи на ЕС са имали много по-ниски разходи в сравнение с други подобни организации. Въпреки че разликите в нивото на киберсигурност теоретично могат да бъдат обосновани с различните рискови профили на всяка организация и степента на чувствителност на обработваната информация, одиторите подчертават, че слабостите в киберсигурността в един орган на ЕС могат да изложат няколко други организации на заплахи за киберсигурността (органите на ЕС са свързани помежду си, а често и с публични или частни организации в държавите членки).

Екипът за незабавно реагиране при компютърни инциденти (CERT-EU) и Агенцията на Европейския съюз за киберсигурност (ENISA) са двете основни организации, на които е възложена задачата да предоставят подкрепа в областта на киберсигурността. Поради ограничени ресурси или отдаване на приоритет на други области те не са в състояние да предоставят на органите на ЕС цялата необходима подкрепа. Одиторите посочват, че несподелянето на информация също представлява недостатък — например, не всички органи на ЕС докладват навреме относно съществуващите уязвимости или сериозните киберинциденти, които са ги засегнали и могат да засегнат и други институции.

Обща информация

Понастоящем не съществува правна рамка за информационна сигурност и киберсигурност в институциите, агенциите и органите на ЕС. Те не са обект на най-широкообхватното законодателство на ЕС в областта на киберсигурността — Директивата от 2016 г. относно сигурността на мрежите и информационните системи (Директива за МИС), както и на предложеното ѝ изменение — Директива МИС2. Не съществува и изчерпателна информация относно размера на средствата, изразходвани от органите на ЕС за киберсигурност. Общите правила за информационна сигурност и киберсигурност за всички органи на ЕС са включени в съобщението относно Стратегията на ЕС за Съюза на сигурност за периода 2020—2025 г., публикувано от Комисията през юли 2020 г. В Стратегията на Европейския съюз за киберсигурност за цифровото десетилетие, публикувана през декември 2020 г., Комисията поема ангажимент да предложи регламент относно общи правила за киберсигурност за всички органи на ЕС. Предложено е и установяването на нова правна уредба за CERT-EU, която да укрепи неговия мандат и да увеличи финансирането му.

Специален доклад 05/2022 *„Киберсигурност в институциите, органите и агенциите на ЕС — нивото на подготвеност като цяло не съответства на заплахите“* е публикуван на уебсайта на ЕСП. ЕСП вече разгледа предизвикателствата пред ефективното прилагане на политиката на ЕС за киберсигурност в преглед, публикуван през 2019 г.

Контакт с пресслужбата

Пресслужба на ЕСП: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu — Моб. тел. (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu — Моб. тел. (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu — Моб. тел. (+352) 621 552 224