ОТГОВОРИ НА ЕВРОПЕЙСКАТА КОМИСИЯ

ПО СПЕЦИАЛНИЯ ДОКЛАД НА ЕВРОПЕЙСКАТА СМЕТНА ПАЛАТА

Киберсигурността в институциите, органите и агенциите на ЕС — нивото на подготвеност не съответства на заплахите

BG

BG

Съдържание

В настоящия документ са представени отговорите на Европейската комисия на констатациите и оценките, които се съдържат в специален доклад на Европейската сметна палата в съответствие с член 259 от Финансовия регламент и които трябва да бъдат публикувани заедно със специалния доклад.

I. ОТГОВОРИ НА КОМИСИЯТА НАКРАТКО

а) Общо въведение

Киберсигурността се превърна в основен политически и оперативен приоритет на Европейската комисия. Кризата, свързана с COVID, засили зависимостта ни от цифровите услуги (изчисления в облак, преносими устройства, изкуствен интелект). През последните две години наблюдаваме значително преминаване към работа от дома. Това означава, че както киберпрестъпността, така и кибершпионажът — двете основни заплахи, пред които са изправени институциите, органите и агенциите на ЕС (EUIBA), на практика също започнаха да се извършват онлайн в големи мащаби. Комисията признава тази тенденция. Тя демонстрира последователно и решително лидерство в областта на киберсигурността. Актът за киберсигурността влезе в сила през 2019 г., като наред с другото разшири мандата на ENISA и я превърна в постоянно действаща агенция. С този акт също така беше установено официално сътрудничество между ENISA и CERT-EU (екипа за незабавно реагиране при компютърни инциденти, който оказва подкрепа на всички EUIBA). През 2020 г. Комисията предложи да се засили Директивата за мрежова и информационна сигурност, като законодателните органи са много близо до постигане на съгласие.

Стратегията за киберсигурността от 2020 г. също съдържа три действия, свързани с киберсигурността на EUIBA. В нея бяха обявени Регламент относно информационната сигурност в институциите, органите и агенциите на ЕС, Регламент относно общите правила за киберсигурност в институциите, органите и агенциите на ЕС и намерението на Комисията да се осигури ново правно основание за CERT-EU, даващо възможност за по-силен мандат и увеличено финансиране, така че екипът да разполага с достатъчно ресурси в ситуация на нарастващи заплахи, рискове и инциденти.

Работата по изготвянето на тези предложения напредна. Въпреки че те все още не са приети от колегиума, се очаква да бъдат приети през първото тримесечие на 2022 г. Важни въпроси, обсъждани между институциите на този подготвителен етап, са свързани с правното основание на предложението, както и с бюджетния капацитет на всички EUIBA да отговорят на изискванията както по отношение на финансирането на собствените си нужди от киберсигурност, така и за намирането на необходимите ресурси за подкрепа на CERT-EU, за бюджета и по-специално за длъжностите.

Нивото на подготвеност на институциите, органите и агенциите на ЕС в областта на киберсигурността е на различни равнища на зрялост. Няколко EUIBA са постигнали добри резултати по отношение на подготвеността във връзка с киберсигурността и следва да продължат да служат като лидери, като насърчават и вдъхновяват напредъка и по-нататъшните подобрения в областта на киберсигурността като цяло. За да се постигне измерим напредък, е важно да се признаят различните равнища на зрялост сред EUIBA и да се определят приоритети, като действията за подобряване се насочат на първо място към онези EUIBA, в които установените пропуски водят до най-висока изложеност на риск.

б) Позицията на Комисията относно ключовите констатации, оценки и препоръки на ЕСП

Комисията приветства доклада на ЕСП относно киберсигурността в институциите, органите и агенциите на ЕС. Тя взема под внимание факта, че в доклада се подчертава значението на общите за всички EUIBA правни рамки по отношение на информационната сигурност и киберсигурността за повишаване на общото ниво на киберсигурност във всички области. Комисията отбелязва, че основните констатации, оценки и препоръки на ЕСП не са насочени към оперативната киберсигурност на самата Комисия, а към ролята на Комисията от гледна точка на политиката при предлагането на законодателство за повишаване на зрелостта в областта на киберсигурността на EUIBA.

С бъдещите регламенти относно „информационната сигурност в институциите, органите и агенциите на ЕС“ и „общите правила за киберсигурност в институциите, органите и агенциите на ЕС“ ще се определи общата уредба за постигане на високи равнища на информационна сигурност и киберсигурност, но автономна отговорност за тяхното прилагане в рамките на организационния и оперативния контекст на всяка EUIBA (по-специално характерните за тях заплахи и рискове) ще носят EUIBA. В предложения регламент относно киберсигурността ще бъдат включени механизми за осигуряване на съответствие, които са подходящи и съизмерими с целта и обхвата на новите правила, без да се засяга автономността на институциите, органите и агенциите.

Понастоящем Комисията председателства подгрупата за киберсигурност на Междуинституционалния комитет за цифрова трансформация (ICDT) на ротационен принцип (за период до 2 години). Отбелязва се, че за работата на подгрупата не са предоставени специални ресурси: всички действия се основават на полагането на максимални усилия от страна на участниците на доброволна основа.

Комисията е съгласна с общата идея за укрепване на ресурсите и мандата на CERT-EU.

Предвид това Комисията подкрепя основните констатации, оценки и препоръки, съдържащи се в доклада. Нашата подробна позиция е изложена в допълнителните коментари в раздел III. По отношение на препоръките, Комисията приема препоръка 1, букви а), б), в), г), д), е) и ж) и препоръка 2, букви а), б) и в).

в) Последни събития от значение и следващи стъпки

Формалният процес на консултации на равнището на генералните директори на EUIBA относно консолидираните проекти на двата регламента (информационна сигурност, киберсигурност) приключи и в момента се извършва оценка на получената обратна информация, преди пакетът да бъде завършен и приет от колегиума през първото тримесечие на 2022 г.

II. ОТГОВОРИ НА КОМИСИЯТА НА ОСНОВНИТЕ КОНСТАТАЦИИ И ОЦЕНКИ НА ЕСП

1. Равнища на зрялост на EUIBA в областта на киберсигурността

Комисията е съгласна, че когато се наблюдава нивото на разходите на EUIBA за киберсигурност, е важно да се вземат предвид заплахите и рисковете.

Също така, по отношение на човешките ресурси, стабилността на числеността на персонала на EUIBA се влияе от редица фактори. Пазарът за набиране на специализирани експерти по киберсигурност става все по-сложен. В много случаи правилата в областта на човешките ресурси не са приспособени към специализираните профили (набиране, кариерно развитие, обучение). Освен това общият натиск от страна на бюджетния орган върху числеността на персонала в EUIBA означава, че нововъзникващите области с висок приоритет, като например киберсигурността, остават без достатъчен брой длъжности, особено във вътрешните оперативни служби.

При отбелязването на напредъка в управлението и управлението на риска следва да се вземе предвид фактът, че мониторингът на съответствието вече преминава от пилотен етап към пълно внедряване. Поради това е нормално обхватът засега да е доста нисък. Този проект за осигуряване на съответствие е следващият етап от дългосрочен процес на подобряване на зрелостта в областта на киберсигурността, който започна с определянето на обща методология за риска, създаването на общи инструменти, въвеждането на управление на уязвимостите и на наблюдение, тестване и валидиране на инвентаризацията на активите. Беше постигнат напредък по този дълъг път въпреки сложността на базата от активи на Комисията, в която са включени над 1000 информационни системи, управлявани от над 50 генерални дирекции и изпълнителни агенции.

2. Механизми за сътрудничество на EUIBA

CERT-EU постигна удивителен успех в насърчаването на сътрудничеството не само между EUIBA, но и на европейско равнище, чрез участието му като пълноправен член на мрежата на CSIRT, създадена съгласно Директивата за МИС. По този начин CERT-EU е пример за това как сътрудничеството и услугите в областта на киберсигурността могат да бъдат подобрени. Констатациите и оценките на ЕСП във връзка със CERT-EU показват много ясно изключителната работа, извършвана от CERT-EU в условията на все по-враждебна среда на киберзаплахи и с хроничен недостиг на ресурси.

Съгласно настоящото Междуинституционално споразумение (IIA) ENISA представлява официално децентрализираните агенции и съвместните предприятия на ЕС в управителния съвет на CERT-EU. Освен това техните мнения се изразяват на заседанията на управителния съвет от представител на Консултативния комитет по ИКТ (ICTAC), който може да присъства, за да съдейства на ENISA в нейната задача да представлява агенциите, но няма официално място или право на глас. Въпросът за адекватното представителство на агенциите в управителния съвет на CERT-EU ще бъде разгледан в предложения регламент чрез допълване

на състава на управителния съвет с до трима представители, определени от Мрежата на агенциите на Съюза (EUAN), по предложение на нейния Консултативен комитет по ИКТ.

Участието в подгрупата за киберсигурност на ICDT се основава на полагането на максимални усилия на нивото на ангажираност, определено от всяка EUIBA. При подготовката на новия рамков договор в областта на киберсигурността, като важна тема в рамките на оперативна група 2 на подгрупата по киберсигурност, се разглеждат подобрения в обмена на информация относно обществените поръчки.

По отношение на общите инструменти за услуги като електронна поща и видеоконференция вече има възможност да се използва системата SECEM-2, внедрена от Комисията за всички EUIBA, за криптирана електронна поща, като тя зависи от ефективното управление на ключовете и сертификатите за криптиране. В допълнение към това в процес на разработка е SECABC — инструмент, с който се осигурява възможност за криптиране на електронната поща между институциите, като намерението е да се предложи достъп до него на всяка заинтересована EUIBA от 2022 г. нататък. Вече са постигнати сигурни видеоконферентни връзки за услуги, свързани с чувствителна некласифицирана информация, и те могат да бъдат разширени, така че да обхванат и други EUIBA на ad hoc основа чрез управление на самоличността на участниците в срещата. Споделянето на чувствителна информация ще бъде разгледано и в предложения регламент относно информационната сигурност (например чрез общо етикетиране и общи обозначения).

3. Споделяне на информация за значителни инциденти или уязвимости

На факта, че не всички EUIBA уведомяват CERT-EU за значителни инциденти или уязвимости, е обърнато внимание в проекта на регламент относно киберсигурността в съответствие с предложението на Комисията за Директива за МИС-2[1]. Степента на изпълнение ще зависи от допълнителните ресурси, отделени за това от автономните EUIBA. Възможностите за налагане на такива уведомления остават ограничени, включително съгласно предложения регламент в планирания му в момента текст, поради институционалната автономност на EUIBA. В предложения регламент относно киберсигурността ще бъдат включени механизми за осигуряване на съответствие, които са подходящи и съизмерими с целта и обхвата на новите правила, без да се засяга автономността на институциите, органите и агенциите.

[1] Предложение за Директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148, COM/2020/823

III. ОТГОВОРИ НА КОМИСИЯТА НА ЗАКЛЮЧЕНИЯТА И ПРЕПОРЪКИТЕ НА ЕСП

Препоръка 1 — Подобряване на подготвеността на всички EUIBA в областта на киберсигурността чрез общи обвързващи правила и увеличаване на ресурсите за CERT-EU

В предложения текст на регламента ще бъдат включени конкретни мерки, чиято цел е да се повиши допълнително общото ниво на киберсигурност. Споменатите мерки ще бъдат превърнати в планове за киберсигурност, които ще се определят и прилагат на равнището на EUIBA в рамките на тяхната собствена рамка за управление на киберсигурността.

Комисията приема тази препоръка. По отношение на конкретните подпрепоръки Комисията отбелязва следното:

а) Комисията приема препоръка 1а. В проекта на регламент ще бъдат включени разпоредби относно рамки за управление и контрол, създадени на най-високото равнище на изпълнително управление на всяка EUIBA, за да се гарантира ефективно и разумно управление на всички рискове, свързани с киберсигурността.

б) Комисията приема препоръка 1б. В проекта на регламент ще се засили споменаването на основания на риска подход за управление на киберсигурността, като се изясни, че действията, плановете за сигурност на ИТ и действителното прилагане на основните механизми за контрол следва да следват оценките.

в) Комисията приема препоръка 1в. Програмите за образование, повишаване на осведомеността и обучение в областта на киберсигурността ще бъдат включени като част от основния сценарий за киберсигурност в проекта на регламент.

г) Комисията приема препоръка 1г. Опитът ни показва, че въпреки че редовните одити и проверки са от съществено значение, те не са достатъчни, за да се гарантира постигането на напредък. Следователно са необходими редовно отчитане и прозрачност като част от рамката за управление на киберсигурността по буква а).

д) Комисията приема препоръка 1д. В проекта на регламент ще бъдат включени разпоредби, свързани с уведомяването на CERT-EU от EUIBA за значителни киберзаплахи, уязвимости и инциденти.

е) Комисията приема препоръка 1е. Комисията подкрепя необходимостта от укрепване на ресурсите на CERT-EU. Разпоредби, свързани с персонала и финансовите вноски от EUIBA, ще бъдат включени в текста на проекта на регламент.

ж) Комисията приема препоръка 1ж. В предложения регламент ще бъдат включени механизми за осигуряване на съответствие, които са съизмерими с и пропорционални на целта и обхвата на разпоредбите, при зачитане на институционалната автономност на EUIBA. Съдържанието на бъдещия регламент зависи от резултата от законодателната процедура и е резултат от решение, взето от законодателния орган на ЕС във връзка с направеното от Комисията предложение.

Препоръка 2 — Насърчаване на допълнителни полезни взаимодействия между EUIBA в избрани области

Комисията, която понастоящем е председател на подгрупата за киберсигурност на Междуинституционалния комитет за цифрова трансформация, е съгласна с препоръките във връзка с насърчаването на решенията за последователен и сигурен обмен на чувствителна информация, систематичен обмен на информация относно проекти, свързани с киберсигурността, и общи рамки за обществени поръчки и договори за услуги в областта на киберсигурността.

Комисията приема тази препоръка. По отношение на конкретните подпрепоръки Комисията отбелязва следното:

а) Комисията приема препоръка 2а. Комисията представя в подгрупата за киберсигурност на ICDT технически инициативи и услуги за насърчаване и подкрепа на общи инструменти за обмен на чувствителна информация, с които се осигуряват възможности за услугите, като електронна поща и видеоконференции. Ние също така отбелязваме, че общите обозначения и общите правила за обработка за чувствителна некласифицирана информация ще бъдат разгледани в предложения регламент относно информационната сигурност.

б) Комисията приема препоръка 2б. Съществуващите работни групи в рамките на подгрупата за киберсигурност на ICDT разглеждат този въпрос и той ще бъде доразвит. При подготовката на новото рамково споразумение в областта на киберсигурността се разглеждат подобрения в обмена на информация относно обществените поръчки.

в) Комисията приема препоръка 2в. EUIBA вече имат достъп до междуинституционални рамкови споразумения в областта на ИКТ, управлявани от Комисията. Подготовката на новото рамково споразумение в областта на киберсигурността ще бъде координирана с подгрупата по киберсигурност на ICDT.

Препоръка 3 — Засилване на фокуса на CERT-EU и ENISA върху EUIBA с по-ниски равнища на зрялост

Адресати на тази препоръка са CERT-EU и ENISA.