ODPOVEDE EURÓPSKEJ KOMISIE

NA OSOBITNÚ SPRÁVU DVORA AUDÍTOROV

Kybernetická bezpečnosť inštitúcií, orgánov a agentúr EÚ: úroveň pripravenosti nezodpovedá hrozbám

SK

SK

Obsah

V tomto dokumente sa predkladajú odpovede Európskej komisie na pripomienky k osobitnej správe Európskeho dvora audítorov v súlade s článkom 259 nariadenia o rozpočtových pravidlách, ktoré budú uverejnené spoločne s osobitnou správou.

I. STRUČNÉ ODPOVEDE KOMISIE

a) Všeobecný úvod

Kybernetická bezpečnosť sa stala najvyššou politickou a prevádzkovou prioritou Európskej komisie. Kríza spôsobená pandémiou COVID-19 zvýšila našu závislosť od digitálnych služieb (cloud computing, mobilné zariadenia, umelá inteligencia). V posledných dvoch rokoch sme boli svedkami masívneho prechodu na prácu z domu. Znamená to, že počítačová kriminalita, ako aj kybernetická špionáž, ktoré sú dvomi hlavnými hrozbami, ktorým čelia inštitúcie, orgány a agentúry EÚ, sa v skutočnosti takisto vo veľkom prejavili v online priestore. Komisia tento trend uznáva. Preukázala stabilné a rozhodné vedúce postavenie v oblasti kybernetickej bezpečnosti. Akt o kybernetickej bezpečnosti nadobudol účinnosť v roku 2019 a okrem iného sa ním rozšíril mandát agentúry ENISA, čím sa upevnila jej pozícia. Týmto aktom sa takisto nadviazala formálna spolupráca medzi agentúrou ENISA a tímom CERT-EU (tím reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach). Komisia v roku 2020 navrhla posilniť smernicu o kybernetickej bezpečnosti, pričom zákonodarca EÚ sa blíži k dohode o tomto návrhu.

Súčasťou stratégie kybernetickej bezpečnosti z roku 2020 boli takisto tri opatrenia, ktoré majú vplyv na kybernetickú bezpečnosť inštitúcií, orgánov a agentúr EÚ. Oznámilo sa v nej nariadenie o informačnej bezpečnosti v inštitúciách, orgánoch a agentúrach EÚ a nariadenie o spoločných pravidlách kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry EÚ a zámer poskytnúť nový právny základ pre tím CERT-EU na posilnenie mandátu a financovania, aby sa zabezpečili primerané zdroje vzhľadom na rastúce hrozby, riziká a incidenty.

Práca na príprave týchto návrhov pokročila. Hoci ešte nie sú prijaté kolégiom, ich prijatie sa očakáva v prvom štvrťroku 2022. Dôležité otázky, o ktorých sa diskutovalo medzi inštitúciami v tejto prípravnej fáze, sa týkajú právneho základu návrhu, ako aj fiškálnej kapacity všetkých inštitúcií, orgánov a agentúr EÚ s cieľom splniť požiadavky v súvislosti s financovaním ich vlastných potrieb v oblasti kybernetickej bezpečnosti, ako aj nájsť potrebné zdroje na podporu tímu CERT-EU, rozpočtu a predovšetkým pracovných miest.

Pripravenosť inštitúcií, orgánov a agentúr EÚ na kybernetickú bezpečnosť dosahuje rôzne úrovne vyspelosti. Niekoľko inštitúcií, orgánov a agentúr EÚ má dobrú výkonnosť, pokiaľ ide o pripravenosť na kybernetickú bezpečnosť, a naďalej by mali ísť príkladom, pričom by stimulovali a podnecovali pokrok a ďalšie zlepšenia v celom prostredí kybernetickej bezpečnosti. Aby sa dosiahol merateľný pokrok, je dôležité vziať do úvahy rôzne úrovne vyspelosti medzi inštitúciami, orgánmi a agentúrami EÚ a stanoviť priority zameraním opatrení na zlepšenie, a to v prvom rade na tie inštitúcie, orgány a agentúry EÚ, pri ktorých identifikované nedostatky vedú k najvyššej expozícii.

b) Stanovisko Komisie ku kľúčovým pripomienkam a odporúčaniam EDA

Komisia víta správu EDA o kybernetickej bezpečnosti inštitúcií, orgánov a agentúr EÚ. Berie na vedomie, že v správe sa zdôrazňuje význam spoločných právnych rámcov pre všetky inštitúcie, orgány a agentúry EÚ, pokiaľ ide o bezpečnosť informácií a kybernetickú bezpečnosť, a to s cieľom zvýšiť celkovú úroveň kybernetickej bezpečnosti vo všetkých oblastiach. Komisia poznamenáva, že hlavné pripomienky a odporúčania EDA nie sú zamerané na vlastnú prevádzkovú kybernetickú

bezpečnosť Komisie ako takú, ale na úlohu Komisie v oblasti politiky pri navrhovaní legislatívy s cieľom zvýšiť kybernetickú vyspelosť inštitúcií, orgánov a agentúr EÚ.

V budúcich nariadeniach o „informačnej bezpečnosti v inštitúciách, orgánoch a agentúrach EÚ“ a o „spoločných pravidlách kybernetickej bezpečnosti pre inštitúcie, orgány a agentúry EÚ“ sa stanovia spoločné pravidlá v záujme dosiahnutia vysokých úrovní bezpečnosti informácií a kybernetickej bezpečnosti, ale ich vykonávanie v rámci organizačného a prevádzkového kontextu všetkých inštitúcií, orgánov a agentúr EÚ (najmä pokiaľ ide o ich profil v oblasti hrozieb a rizikový profil) zostáva samostatnou zodpovednosťou inštitúcií, orgánov a agentúr EÚ. Navrhované nariadenie o kybernetickej bezpečnosti bude obsahovať mechanizmy na zabezpečenie súladu, ktoré sú vhodné a primerané cieľu a rozsahu pôsobnosti nových pravidiel bez toho, aby bola dotknutá samostatnosť inštitúcií, orgánov a agentúr.

Komisia v súčasnosti predsedá podskupine pre kybernetickú bezpečnosť Medziinštitucionálneho výboru pre digitálnu transformáciu (ICDT), pričom ide o funkciu na báze striedania sa (na obdobie až dvoch rokov). Uvádza sa, že na prácu podskupiny nie sú pridelené žiadne osobitné zdroje: všetky opatrenia vychádzajú z maximálneho úsilia dobrovoľných účastníkov.

Komisia súhlasí so všeobecnou myšlienkou, že treba posilniť zdroje a mandát tímu CERT-EU.

Na základe týchto skutočností Komisia podporuje kľúčové pripomienky a odporúčania obsiahnuté v správe. Naše podrobné stanovisko je vysvetlené v doplňujúcich poznámkach v oddiele III. Pokiaľ ide o odporúčania, Komisia prijíma odporúčanie 1 písm. a), b), c), d), e), f), g) a odporúčanie 2 písm. a), b), c).

c) Najnovší relevantný vývoj a ďalšie kroky

Ukončila sa formálna konzultácia na úrovni generálnych riaditeľov inštitúcií, orgánov a agentúr EÚ o konsolidovaných návrhoch týchto dvoch nariadení (bezpečnosť informácií, kybernetická bezpečnosť) a prebieha posúdenie prijatej spätnej väzby, a to pred dokončením balíka a jeho prijatím kolégiom v prvom štvrťroku 2022.

II. ODPOVEDE KOMISIE NA HLAVNÉ PRIPOMIENKY EDA

1. Úrovne vyspelosti kybernetickej bezpečnosti inštitúcií, orgánov a agentúr EÚ

Komisia súhlasí, že pri sledovaní úrovne výdavkov inštitúcií, orgánov a agentúr EÚ vynaložených na kybernetickú bezpečnosť je dôležité zohľadniť hrozby a riziká.

Pokiaľ ide o aspekt ľudských zdrojov, stabilita personálneho obsadenia inštitúcií, orgánov a agentúr EÚ je podobne ovplyvnená viacerými faktormi. Trh s prijímaním špecializovaných odborníkov na kybernetickú bezpečnosť je čoraz zložitejší. V mnohých prípadoch nie sú pravidlá v oblasti ľudských zdrojov prispôsobené špecializovaným profilom (prijímanie zamestnancov, kariérny rast, odborná príprava). Okrem toho všeobecný tlak rozpočtového orgánu na personálne obsadenie v inštitúciách, orgánoch a agentúrach EÚ znamená, že v nových oblastiach s vysokou prioritou, ako je kybernetická bezpečnosť,

nie je stále zabezpečený dostatok pracovných miest, a to najmä v rámci interných prevádzkových služieb.

V odkaze na pokrok v oblasti správy a riadenia rizík by sa mala zohľadniť skutočnosť, že monitorovanie súladu v súčasnosti postupuje od pilotného projektu k úplnému zavádzaniu. Preto je pochopiteľné, že pokrytie je zatiaľ pomerne nízke. Tento projekt v oblasti súladu je ďalšou fázou procesu dlhodobého zlepšovania kybernetickej vyspelosti, ktorý sa začal vymedzením spoločnej metodiky v oblasti rizík, vybudovaním spoločného nástroja, zavedením riadenia zraniteľnosti a monitorovaním, testovaním a osvedčením inventarizácie aktív. Na tejto dlhej ceste sa dosiahol pokrok aj napriek zložitosti základne aktív Komisie s viac ako 1 000 informačnými systémami prevádzkovanými viac ako 50 generálnymi riaditeľstvami a výkonnými agentúrami.

2. Mechanizmy spolupráce inštitúcií, orgánov a agentúr EÚ

Tím CERT-EU je pozoruhodným úspechom v oblasti podpory spolupráce nielen medzi inštitúciami, orgánmi a agentúrami EÚ, ale aj na európskej úrovni, a to prostredníctvom svojej účasti ako riadneho člena siete CSIRT, ktorá bola zriadená smernicou NIS. Týmto spôsobom je tím CERT-EU ukážkovým príkladom toho, ako možno posilniť spoluprácu a služby v oblasti kybernetickej bezpečnosti. Pripomienky EDA k tímu CERT-EU veľmi jasne poukazujú na vynikajúcu prácu, ktorú tím CERT-EU vykonáva v čoraz agresívnejšom prostredí kybernetických hrozieb, a to napriek neustálemu nedostatku zdrojov.

Podľa súčasnej medziinštitucionálnej dohody (IIA) sú decentralizované agentúry a spoločné podniky EÚ oficiálne zastúpené v riadiacej rade tímu CERT-EU agentúrou ENISA. Okrem toho ich stanoviská na zasadnutiach riadiacej rady vyjadruje zástupca Poradného výboru pre informačné a komunikačné technológie (ICTAC), ktorý sa na nich môže zúčastňovať s cieľom pomôcť agentúre ENISA pri jej úlohe zastupovania agentúr, nemá však formálne kreslo ani hlas. Otázka primeraného zastúpenia agentúr v riadiacej rade tímu CERT-EU sa bude riešiť v navrhovanom nariadení doplnením zloženia riadiacej rady najviac o troch zástupcov určených Sieťou agentúr EÚ (EUAN), a to na návrh jej Poradného výboru pre IKT.

Účasť v podskupine pre kybernetickú bezpečnosť výboru ICDT sa zakladá na maximálnom úsilí, pričom o úrovni angažovanosti rozhodujú jednotlivé inštitúcie, orgány a agentúry EÚ. Pri príprave novej rámcovej zmluvy o kybernetickej bezpečnosti sa riešia zlepšenia v oblasti výmeny informácií o obstarávaní, ktoré je dôležitou témou v rámci pracovnej skupiny 2 podskupiny pre kybernetickú bezpečnosť.

Pokiaľ ide o spoločné nástroje pre služby, akými sú e-maily a videokonferencie, existuje už možnosť používať systém SECEM-2, ktorý Komisia zaviedla pre všetky inštitúcie, orgány a agentúry EÚ, pričom zašifrované e-maily závisia od účinného spravovania šifrovacích kľúčov a certifikátov. Okrem toho sa vyvíja nástroj SECABC umožňujúci šifrovanie e-mailov medzi inštitúciami s cieľom poskytnúť od roku 2022 všetkým zainteresovaným inštitúciám, orgánom a agentúram EÚ prístup k nemu. Podarilo sa už zaviesť bezpečné videokonferencie prostredníctvom služieb bezpečnej sieťovej komunikácie a môžu sa *ad hoc* rozšíriť aj na iné inštitúcie, orgány a agentúry EÚ tým, že sa bude spravovať totožnosť účastníkov stretnutia. Výmena citlivých informácií sa bude riešiť aj v navrhovanom nariadení o informačnej bezpečnosti (t. j. prostredníctvom spoločnej klasifikácie a spoločného označovania).

3. Výmena informácií o závažných incidentoch alebo zraniteľných miestach

Skutočnosť, že nie všetky inštitúcie, orgány a agentúry EÚ oznamujú tímu CERT-EU závažné incidenty alebo zraniteľné miesta, sa rieši v návrhu nariadenia o kybernetickej bezpečnosti v súlade s návrhom Komisie uvedeným v smernici NIS 2[1]. Úroveň vykonávania bude závisieť od dodatočných zdrojov, ktoré na tento účel vyčlenia samostatné inštitúcie, orgány a agentúry EÚ. Vzhľadom na inštitucionálnu samostatnosť inštitúcií, orgánov a agentúr zostáva rozsah presadzovania takýchto oznámení obmedzený, a to aj podľa navrhovaného nariadenia v súčasnej plánovanej podobe. Navrhované nariadenie o kybernetickej bezpečnosti bude obsahovať mechanizmy na zabezpečenie súladu, ktoré sú vhodné a primerané cieľu a rozsahu pôsobnosti nových pravidiel bez toho, aby bola dotknutá samostatnosť inštitúcií, orgánov a agentúr.

III. ODPOVEDE KOMISIE NA ZÁVERY A ODPORÚČANIA EDA

Odporúčanie 1 – Zlepšiť kybernetickú pripravenosť inštitúcií, orgánov a agentúr EÚ prostredníctvom spoločných záväzných pravidiel a zvýšeného objemu zdrojov pre tím CERT-EU

Navrhované znenie nariadenia bude obsahovať osobitné opatrenia určené na ďalšie zvýšenie spoločnej úrovne kybernetickej bezpečnosti. Uvedené opatrenia sa premietnu do plánov kybernetickej bezpečnosti, ktoré sa vymedzia a vykonajú na úrovni inštitúcií, orgánov a agentúr EÚ v rámci ich vlastného rámca pre správu kybernetickej bezpečnosti.

Komisia toto odporúčanie prijíma. Pokiaľ ide o konkrétne čiastkové odporúčania, Komisia poznamenáva, že:

a) Komisia prijíma odporúčanie 1 písm. a). Návrh nariadenia bude obsahovať ustanovenia o rámcoch pre správu a kontrolu, ktoré budú zriadené na najvyššej úrovni výkonného riadenia jednotlivých inštitúcií, orgánov a agentúr EÚ, a to s cieľom zabezpečiť účinné a obozretné riadenie všetkých rizík kybernetickej bezpečnosti.
b) Komisia prijíma odporúčanie 1 písm. b). V návrhu nariadenia sa zdôrazní zmienka o prístupe k riadeniu kybernetickej bezpečnosti založenom na riziku, pričom sa jasne uvedie, že opatrenia, plány bezpečnosti informačných technológií a skutočné vykonávanie základných kontrol by malo nasledovať po hodnoteniach.
c) Komisia prijíma odporúčanie 1 písm. c). Vzdelávacie programy, programy na zvyšovanie povedomia a programy odbornej prípravy v oblasti kybernetickej bezpečnosti sa v návrhu nariadenia uvedú ako súčasť základného scenára týkajúceho sa kybernetickej bezpečnosti.
d) Komisia prijíma odporúčanie 1 písm. d). Z našich skúseností vyplýva, že hoci sú pravidelné audity a testy nevyhnutné, nepostačujú na zabezpečenie pokroku. Preto je potrebné

[1] Návrh smernice Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii a o zrušení smernice (EÚ) 2016/1148, COM(2020) 823 final.

pravidelné podávanie správ a transparentnosť ako súčasť rámca pre správu kybernetickej bezpečnosti v súlade s odporúčaním 1 písm. a).

e) Komisia prijíma odporúčanie 1 písm. e). Návrh nariadenia bude obsahovať ustanovenia týkajúce sa oznamovania závažných kybernetických hrozieb, zraniteľných miest a incidentov inštitúciami, orgánmi a agentúrami EÚ tímu CERT-EU.

f) Komisia prijíma odporúčanie 1 písm. f). Komisia podporuje potrebu posilniť zdroje tímu CERT-EU. Ustanovenia týkajúce sa personálneho obsadenia a finančných príspevkov od inštitúcií, orgánov a agentúr EÚ sa zahrnú do znenia návrhu nariadenia.

g) Komisia prijíma odporúčanie 1 písm. g). Navrhované nariadenie bude obsahovať mechanizmy na zabezpečenie súladu, ktoré sú vhodné a primerané cieľu a rozsahu pôsobnosti ustanovení, pokiaľ ide o inštitucionálnu samostatnosť inštitúcií, orgánov a agentúr EÚ. Obsah budúceho nariadenia závisí od výsledku legislatívneho postupu a je dôsledkom rozhodnutia zákonodarcu EÚ v súvislosti s návrhom Komisie.

Odporúčanie 2 – Podporiť ďalšie synergie medzi inštitúciami, orgánmi a agentúrami EÚ vo vybraných oblastiach

Komisia v súčasnosti predsedá podskupine pre kybernetickú bezpečnosť Medziinštitucionálneho výboru pre digitálnu transformáciu (ICDT) a súhlasí s odporúčaniami na podporu riešení pre konzistentnú a bezpečnú výmenu citlivých informácií, systematickú výmenu informácií o projektoch kybernetickej bezpečnosti a spoločných rámcoch obstarávania a o zmluvách na služby v oblasti kybernetickej bezpečnosti.

Komisia toto odporúčanie prijíma. Pokiaľ ide o konkrétne čiastkové odporúčania, Komisia poznamenáva, že:

a) Komisia prijíma odporúčanie 2 písm. a). Komisia predkladá podskupine pre kybernetickú bezpečnosť výboru ICDT technické iniciatívy a služby s cieľom presadzovať a podporovať spoločné nástroje na výmenu citlivých informácií umožňujúce služby, ako sú e-maily a videokonferencie. Takisto poznamenávame, že v navrhovanom nariadení o informačnej bezpečnosti sa budú riešiť spoločné označenia a spoločné pravidlá o spracovaní citlivých neutajených informácií.

b) Komisia prijíma odporúčanie 2 písm. b). Existujúce pracovné skupiny v rámci podskupiny pre kybernetickú bezpečnosť výboru ICDT sa týmto bodom zaoberajú a budú ho ďalej rozvíjať. Zlepšenia v oblasti výmeny informácií o obstarávaní sa riešia pri príprave novej rámcovej zmluvy o kybernetickej bezpečnosti.

c) Komisia prijíma odporúčanie 2 písm. c). Inštitúcie, orgány a agentúry EÚ už majú prístup k medziinštitucionálnym rámcovým zmluvám v oblasti IKT, ktoré spravuje Komisia. Príprava novej rámcovej zmluvy o kybernetickej bezpečnosti sa bude koordinovať s podskupinou pre kybernetickú bezpečnosť výboru ICDT.

Odporúčanie 3 – Zvýšiť zameranie tímu CERT EU a agentúry ENISA na menej vyspelé inštitúcie, orgány a agentúry EÚ

Toto odporúčanie je určené tímu CERT-EU a agentúre ENISA.