

Odhaľovanie kybernetických bezpečnostných incidentov a reakcia na ne

Rámec spolupráce EÚ napreduje, ale je len čiastočne účinný pre oneskorenia vo vykonávaní a obmedzenú výmenu informácií



EURÓPSKY
DVOR
AUDÍTOROV

Obsah

Body

01 – 23 | **Hlavné body**

01 – 07 | Prečo je táto oblasť dôležitá

08 – 23 | Čo sme zistili a čo odporúčame

24 – 01 | **Bližší pohľad na naše pripomienky**

24 – 74 | Hoci siete a mechanizmy kybernetickej bezpečnosti EÚ podporujú spoluprácu a reakciu, obmedzená výmena informácií a neúplné vykonávanie znižujú ich účinnosť

24 – 51 | Siete EÚ umožňujú spoluprácu členských štátov, ale obmedzená výmena informácií znižuje ich pridanú hodnotu

52 – 61 | Rezerva EÚ na účely kybernetickej bezpečnosti umožňuje rýchle nasadenie služieb reakcie na incidenty

62 – 74 | Cieľom európskeho systému varovania pred kybernetickobezpečnostnými hrozbami je zlepšiť kapacity na odhaľovanie hrozieb, ale tento systém nie je funkčný

75 – 01 | Projekty financované EÚ v rámci programu Digitálna Európa sú zamerané na posilnenie kybernetickej bezpečnosti, ale čelia výzvam pri vykonávaní a podávaní správ

75 – 81 | Oneskorenia pri zriaďovaní komunity pre kompetencie v oblasti kybernetickej bezpečnosti jej zabránili formovať program Digitálna Európa podľa jej potrieb

82 – 96 | Projekty financované EÚ sledujú príslušné ciele, ale mnohé z nich čelia operačným problémom

97 – 01 | Väčšina projektov financovaných EÚ nemá primerané výkonnostné rámce a údaje o výkonnosti programu Digitálna Európa týkajúce sa kybernetickej bezpečnosti nie sú presné

Prílohy

Príloha I – O tomto audite

Príloha II – Prostredie kybernetickej bezpečnosti v EÚ

Príloha III – Vybrané opatrenia v oblasti kybernetickej bezpečnosti

Príloha IV – Posúdenie projektov v oblasti kybernetickej bezpečnosti financovaných EÚ zo strany Európskeho dvora audítorov

Skratky

Glosár

Odpovede Komisie

Odpovede Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti (ECCC)

Odpovede Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA)

Harmonogram

Audítorský tím

01

Hlavné body

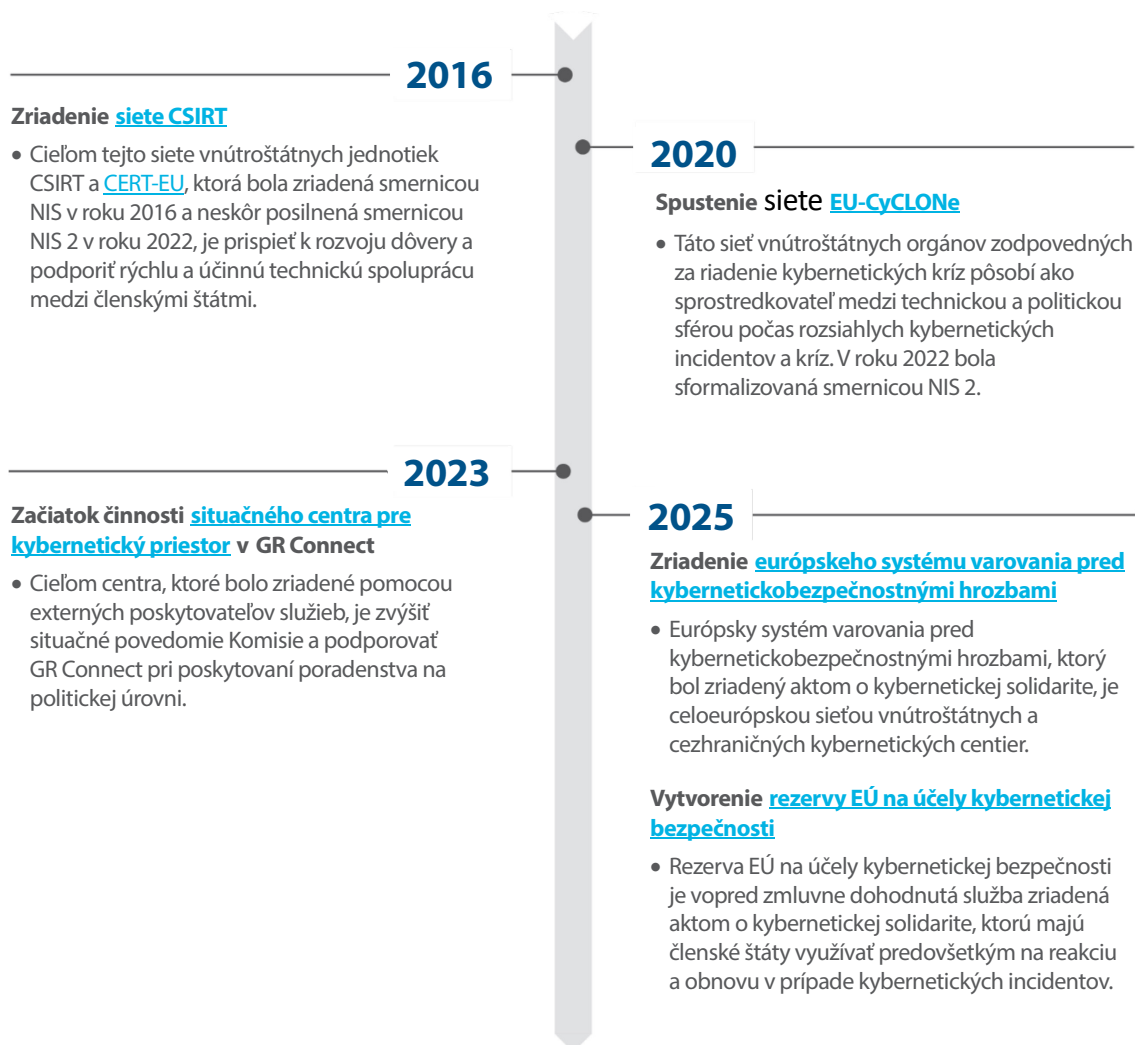
Prečo je táto oblasť dôležitá

- 01** Riziká kybernetických útokov sa zvyšujú, keďže naše hospodárstvo a náš každodenný život sú čoraz viac digitalizované. Kybernetická bezpečnosť sa vymedzuje ako „činnosti potrebné na ochranu sietí a informačných systémov, používateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami“¹. Kybernetická bezpečnosť si vyžaduje holistický prístup k predchádzaniu kybernetickým hrozbám, ich odhaľovaniu, reakcii na ne a zotaveniu sa z nich.
- 02** Do oblasti kybernetickej bezpečnosti EÚ sú zapojené mnohé verejné a súkromné subjekty na regionálnej a národnej úrovni, ako aj na úrovni EÚ v civilnej sfére. Kybernetická bezpečnosť je tiež kľúčovým prvkom národnej bezpečnosti a obrany.
- 03** Členské štáty nesú primárnu zodpovednosť za predchádzanie kybernetickým incidentom a krízam, ktoré ich postihujú, za prípravu a reakciu na ne. Keďže tieto incidenty môžu ovplyvniť hladké fungovanie vnútorného trhu, aj EÚ zohráva dôležitú úlohu v prípade významného incidentu alebo krízy. V posledných rokoch EÚ posilnila svoj vyvíjajúci sa regulačný rámec v oblasti kybernetickej bezpečnosti² a zriadila siete a mechanizmy uvedené na [ilustrácii 1](#) a v [prílohe II](#).

¹ Nariadenie (EÚ) 2019/881 ([akt o kybernetickej bezpečnosti](#)).

² Komisia napríklad v novembri 2025 navrhla [súhrnný balík opatrení v digitálnej oblasti](#) a v januári 2026 [revidovaný akt EÚ o kybernetickej bezpečnosti](#).

Ilustrácia 1 | Siete a mechanizmy kybernetickej bezpečnosti EÚ v rokoch 2016 – 2025



Jednotky CSIRT: jednotky pre riešenie počítačových bezpečnostných incidentov

GR CONNECT: Generálne riaditeľstvo pre komunikačné siete, obsah a technológie

EU-CyCLONe: Európska sieť styčných organizácií pre kybernetické krízy

Smernica NIS: Smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

Smernica NIS 2: Smernica (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii

Zdroj: EDA.

- 04** V súčasnom viacročnom finančnom rámci na roky 2021 – 2027 je hlavným zdrojom financovania kybernetickej bezpečnosti [program Digitálna Európa](#) (DIGITAL). Jeho celkový rozpočet je 8,1 mld. EUR, z čoho 1,4 mld. EUR je vyčlenených na posilnenie kybernetickej bezpečnosti.
- 05** Cieľom nášho auditu bolo posúdiť, či opatrenia EÚ pomáhajú pri odhaľovaní významných a rozsiahlych kybernetických bezpečnostných incidentov a reakcii na ne. Posúdili sme, či tomu tak bolo v prípade:
- sietí a mechanizmov na úrovni EÚ (t. j. siete jednotiek pre riešenie počítačových bezpečnostných incidentov (sieť CSIRT), Európskej siete styčných organizácií pre kybernetické krízy (EU-CyCLONe), Európskeho systému varovania pred kybernetickobezpečnostnými hrozbami, kybernetického situačného centra a rezervy EÚ na účely kybernetickej bezpečnosti),
 - opatrení financovaných v rámci programu Digitálna Európa.
- 06** Očakávame, že naše zistenia prispejú k posilneniu kybernetickej odolnosti EÚ zlepšením účinnosti a efektívnosti sietí a mechanizmov EÚ, ako aj zlepšením spôsobu výberu a monitorovania opatrení financovaných EÚ.
- 07** Audit sa týkal obdobia od roku 2022 do roku 2025. Vychádza z administratívnej kontroly a analýzy príslušných dokumentov, audítorských návštev v troch členských štátoch, Írsku, Grécku a Taliansku a písomných dotazníkov a rozhovorov s príslušnými zainteresovanými stranami. Ďalšie súvislosti a podrobnosti o rozsahu auditu a audítorskom prístupe uvádzame v [prílohe I](#).

Čo sme zistili a čo odporúčame

- 08** Celkovo sme dospeli k záveru, že opatrenia EÚ len čiastočne uľahčujú odhaľovanie významných a rozsiahlych kybernetických bezpečnostných incidentov a reakciu na ne. Hoci sa postupne zavádzal rámec spolupráce, stále sa pracuje na dosiahnutí jeho úplného využitia. Obmedzená výmena informácií, nedostatky v podávaní správ a značné oneskorenia vo vykonávaní bránia tomu, aby siete a mechanizmy EÚ dosiahli svoj plný potenciál. Projekty financované z programu Digitálna Európa sledujú príslušné ciele, ale viaceré z nich čelia operačným výzvam a oneskoreniam a v celkovom rámci monitorovania výkonnosti existujú nedostatky.

- 09** Súčasný rámec sietí a mechanizmov EÚ na uľahčenie odhaľovania významných kybernetických bezpečnostných incidentov a reakcie na ne bol vytvorený postupne. Rada v roku 2025 prijala [kybernetickú koncepciu](#), ktorou sa stanovuje rámec EÚ pre riadenie kybernetickobezpečnostných kríz. Zistili sme, že v kybernetickej koncepcii sa vo veľkej miere objasňujú úlohy a povinnosti, pokiaľ ide o riadenie kybernetických kríz v EÚ. Bez ohľadu na to sa však ešte musia formalizovať procesné opatrenia týkajúce sa spôsobu, akým by sieť jednotiek CSIRT (zriadená v roku 2016) a sieť EU-CyCLOne (sformalizovaná v roku 2023) mali spolupracovať (body [24 – 30](#)).
- 10** Zistili sme, že výmena informácií prostredníctvom týchto sietí je obmedzená. Je to spôsobené najmä oneskoreniami pri transpozícii [smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii](#) (smernica NIS 2), ťažkosťami pri určovaní, či má incident cezhraničný vplyv, a právnymi predpismi v oblasti národnej bezpečnosti, ktoré bránia výmene informácií. Pridaná hodnota sietí sa výrazne znižuje, ak členské štáty nie sú ochotné vymieňať si včasné a využiteľné informácie (body [31 – 44](#)).



Odporúčanie 1

Posilniť výmenu informácií medzi členskými štátmi

S cieľom zlepšiť odhaľovanie kybernetických bezpečnostných incidentov a reakciu na ne by Komisia s podporou Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) mala:

- a) navrhnuť skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti vykonať podrobnú analýzu obmedzení národnej bezpečnosti, ktoré limitujú výmenu informácií a ovplyvňujú kybernetickú odolnosť EÚ, a identifikovať právne a technické riešenia na zvýšenie výmeny informácií pri súčasnom rešpektovaní hraníc národnej bezpečnosti;
- b) bez toho, aby boli dotknuté rozhodnutia spoluzákonodarcov, v spolupráci s členskými štátmi zabezpečiť, aby jednotné kontaktné miesto na nahlasovanie incidentov navrhnuté v súhrnnom balíku opatrení v digitálnej oblasti dokázalo odhaliť potenciálne cezhraničné incidenty;
- c) pracovať na riešeníach, ktoré umožnia nahlasovanie incidentov agentúre ENISA v reálnom čase.

Cieľový dátum vykonania: písm. a) a písm. b) 2027, písm. c) 2028

- 11** V roku 2022 Komisia zriadila svoj sektor „kybernetického situačného centra“ s cieľom zvýšiť svoju situačnú informovanosť a podporiť tak svoju inštitucionálnu zodpovednosť za krízové riadenie. Fungovanie centra je vo veľkej miere podporované zmluvou s externými poskytovateľmi služieb. Zistili sme, že práca vykonaná externými poskytovateľmi služieb čiastočne duplikuje existujúcu kapacitu Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA), pokiaľ ide o situačnú informovanosť a monitorovanie hrozieb. Zastávame názor, že pri zriadení kybernetického situačného centra sa dostatočne nevyužil potenciál racionalizácie využitím informácií, ktoré už boli k dispozícii od Komisie a agentúry ENISA. Okrem toho chýbajúci ucelený a podrobný plán do budúcnosti po skončení platnosti zmluvy predstavuje riziko pre prevádzku kybernetického situačného centra po roku 2026 (body 45 – 51).



Odporúčanie 2

Racionalizovať spôsobilosti EÚ v oblasti situačnej informovanosti o kybernetickej bezpečnosti a optimalizovať šírenie informácií

V záujme zvýšenia efektívnosti by Komisia mala v spolupráci s agentúrou ENISA posúdiť uskutočniteľnosť spoločného získavania a analýzy informácií na účely situačnej informovanosti. Tieto informácie a súvisiace správy o kybernetických hrozbách by mala sprístupniť aj príslušným útvarom a agentúram EÚ.

Cieľový dátum vykonania: 2027

- 12** **Aktom o kybernetickej solidarite** z roku 2024 sa zriadila rezerva EÚ na účely kybernetickej bezpečnosti, ktorej cieľom je podporovať členské štáty pri reakcii na závažné kybernetické bezpečnostné incidenty a zotavovaní sa z nich. Pozostáva z vybraných poskytovateľov služieb pre každý členský štát, ktorí sú schopní reagovať na incidenty nepretržite. Hoci tento prístup pomáha riešiť špecifické požiadavky členských štátov a budovať dôveru, dostupný rozpočet je medzi ne rozdelený rovnomerne a nezohľadňuje osobitné potreby každého členského štátu (body 52 – 57).
- 13** Zastávame názor, že využívanie vopred zmluvne dohodnutých poskytovateľov umožňuje rýchle nasadenie služieb reakcie na incidenty. Hoci sa rezerva EÚ na účely kybernetickej bezpečnosti primárne zameriava na podporu reakcie a obnovy, ak sa nepoužíva na reakciu na incidenty, môže sa použiť na pripravenosť. Tento pružný prístup môže zabrániť tomu, aby sa nevyužili predplatené služby. Hrozí však, že sa rezerva v rozpore so zamýšľaným účelom využije prevažne na pripravenosť, a nie na reakciu (body 58 – 61).

- 14** Európsky systém varovania pred kybernetickobezpečnostnými hrozbami je sieť vnútroštátnych a cezhraničných kybernetických centier, ktorých cieľom je zlepšiť odhaľovanie kybernetických hrozieb, ich analýzu a reakciu na ne. Zistili sme, že v čase konania auditu neboli dve centrá (ATHENA a ENSOC) stále v prevádzke z dôvodu značných oneskorení pri obstarávaní nástrojov a služieb a že európsky systém varovania pred kybernetickobezpečnostnými hrozbami ešte nefungoval (body 62 – 70).
- 15** Jedným z kľúčových cieľov európskeho systému varovania pred kybernetickobezpečnostnými hrozbami je podporiť zmysluplnú výmenu informácií medzi zoskupeniami členských štátov. Hoci to má potenciál vyriešiť niektoré problémy týkajúce sa výmeny informácií, je takisto veľmi náročné integrovať kybernetické centrá do už aj tak zložitého prostredia kybernetickej bezpečnosti. Zistili sme, že požadované dohody o spolupráci, spoločná taxonómia a normy interoperability potrebné na úplné fungovanie európskeho systému varovania pred kybernetickobezpečnostnými hrozbami ešte neboli zavedené (body 71 – 74).



Odporúčanie 3

Integrovať európsky systém varovania pred kybernetickobezpečnostnými hrozbami do prostredia kybernetickej bezpečnosti EÚ

Komisia by mala spolu s agentúrou ENISA a členskými štátmi zabezpečiť zavedenie dohôd o spolupráci a noriem interoperability s cieľom uľahčiť výmenu informácií medzi cezhraničnými centrami, ktoré sú súčasťou európskeho systému varovania pred kybernetickobezpečnostnými hrozbami, sieťou jednotiek CSIRT a sieťou EU-CyCLONE.

Cieľový dátum vykonania: 2028

- 16** V roku 2018 Komisia navrhla vytvoriť Európske centrum kompetencií v oblasti kybernetickej bezpečnosti (ECCC) s cieľom riadiť kybernetickobezpečnostnú zložku programu Digitálna Európa od roku 2021. V [nariadení o ECCC](#) sa vyzýva na vytvorenie komunity pre kompetencie v oblasti kybernetickej bezpečnosti zloženej zo zástupcov priemyslu, akademických a výskumných organizácií. Vybraní členovia komunity pre kompetencie v oblasti kybernetickej bezpečnosti by následne vytvorili strategickú poradnú skupinu (body 75 – 76).

- 17** Zistili sme, že došlo k oneskoreniam pri získaní finančnej nezávislosti ECCC, komunity pre kompetencie v oblasti kybernetickej bezpečnosti a strategickej poradnej skupiny. To znamenalo, že komunita pre kompetencie v oblasti kybernetickej bezpečnosti a strategická poradná skupina nemohli prispieť k formovaniu pracovných programov programu Digitálna Európa. Zastávame názor, že to bola premárnená príležitosť (body 77 – 81).
- 18** Zistili sme, že všetky projekty, ktoré sme preskúmali, sledovali príslušné ciele, ktoré prispievajú k dosiahnutiu cieľov programu Digitálna Európa v oblasti kybernetickej bezpečnosti. Zistili sme však prípady, keď kvalita alebo dosiahnuté výsledky neboli uspokojivé, najmä z dôvodu oneskorení vo vykonávaní (body 82 – 87).
- 19** V [nariadení o programe Digitálna Európa](#) sa stanovuje, že z bezpečnostných dôvodov sa financovanie kybernetickej bezpečnosti môže obmedziť na subjekty usadené v členských štátoch a kontrolované členskými štátmi alebo občanmi členských štátov. Centrálna služba pre validáciu v [Európskej výkonnej agentúre pre výskum](#) vykonáva toto posúdenie vlastníctva a kontroly v mene ECCC (body 88 – 91).
- 20** V prípade finančnej podpory tretím stranám sú za posúdenie vlastníctva a kontroly zodpovední prijímatelia projektov na základe vlastného prístupu a metodiky. Zistili sme, že ECCC nepotvrdzuje ich metodiku ani nevykonáva kontroly s cieľom zabezpečiť, aby vybrané tretie strany boli vo vlastníctve a pod kontrolou EÚ. Zastávame názor, že existuje značné riziko, že prijímatelia nedokážu vykonávať tieto kontroly náležite. Toto riziko nebolo primerane zmiernené a mohlo by viesť k vystaveniu citlivej infraštruktúry, prevádzkových údajov a technológií kritických z hľadiska bezpečnosti (body 92 – 96).



Odporúčanie 4

Zabezpečiť dôkladné posúdenie vlastníctva a kontroly subjektov, ktoré dostávajú finančné prostriedky EÚ v rámci programu Digitálna Európa

Európske centrum kompetencií v oblasti kybernetickej bezpečnosti by malo:

- a) získať primerané uistenie, že prijímatelia zodpovední za poskytovanie finančnej podpory tretím stranám majú administratívne a technické kapacity potrebné na vykonávanie primeraných posúdení vlastníctva a kontroly na základe existujúcej metodiky, ktorú majú k dispozícii prijímatelia vykonávajúci finančnú podporu tretím stranám;
- b) na základe vzorky kontrolovať, či finančné prostriedky EÚ dostali len oprávnené subjekty.

Cieľový dátum vykonania: písm. a) 2026 pre písm. b) 2027

- 21** Prijímatelia, ktorí riadia projekty financované EÚ, musia centru ECCC podávať správy o svojom pokroku a výsledkoch, používajúc na to míľniky a výstupy. Tie sú kľúčové pre monitorovanie projektov a mali by sa náležite vymedziť. Zistili sme, že takmer ani jeden projekt v našej vzorke sa neriadil pokynmi, ako stanoviť míľniky a výstupy, a že mnohé z nich neboli užitočné na sledovanie pokroku (body 97 – 99).
- 22** Zistili sme, že mnohé ukazovatele výkonnosti, ktoré používajú prijímatelia, nie sú relevantné alebo merateľné a chýba im cieľová alebo východisková hodnota. Okrem toho vykazovanie týchto ukazovateľov bolo neprimerané, a preto nemôže slúžiť ako základ na posúdenie výkonnosti projektov (body 100 – 102).
- 23** Na monitorovanie výsledkov programu Digitálna Európa ako celku sa musia v rámci všetkých projektov vykazovať špecifické programové ukazovatele, ktoré Komisii slúžia ako podklad pre ročné [vyhlásenia o výkonnosti programu](#). ECCC je zodpovedné za zber a overovanie údajov poskytnutých pre tieto ukazovatele. Zistili sme niekoľko problémov týkajúcich sa spôsobu zberu údajov a ich celkovej kvality. Nenašli sme žiadne dôkazy o tom, že by ECCC overovalo presnosť vykázaných údajov. Na základe kontrol našej vzorky zastávame názor, že vykázané údaje presne neodrážajú dosiahnuté výsledky (body 103 – 106).



Odporúčanie 5

Posilniť rámec monitorovania výkonnosti zložky kybernetickej bezpečnosti programu Digitálna Európa

S cieľom umožniť primerané monitorovanie pokroku a výkonnosti by Európske centrum kompetencií v oblasti kybernetickej bezpečnosti malo:

- a) pred podpísaním grantov zabezpečiť, aby sa vo všetkých projektoch vymedzili míľniky, výstupy a ukazovatele výkonnosti, ktoré sú v súlade s pokynmi uvedenými vo formulári žiadosti;
- b) navrhnuť a zaviesť spoľahlivý systém zberu, vysledovateľnosti, overovania a agregácie údajov pre ukazovatele výkonnosti zložky kybernetickej bezpečnosti programu Digitálna Európa s cieľom zabezpečiť, aby ukazovatele presne odrážali dosiahnuté výsledky.

Cieľový dátum vykonania: 2027

Bližší pohľad na naše pripomienky

Hoci siete a mechanizmy kybernetickej bezpečnosti EÚ podporujú spoluprácu a reakciu, obmedzená výmena informácií a neúplné vykonávanie znižujú ich účinnosť

Siete EÚ umožňujú spoluprácu členských štátov, ale obmedzená výmena informácií znižuje ich pridanú hodnotu

- 24** Súčasný rámec EÚ pre siete a mechanizmy na uľahčenie odhaľovania významných kybernetických bezpečnostných incidentov a reakcie na ne bol vytvorený postupne, počnúc [smernicou o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii](#)³ (smernica NIS), ktorá nadobudla účinnosť v auguste 2016. Súčasnú prostredie kybernetickej bezpečnosti EÚ je znázornené v [prílohe II](#).

³ Smernica (EÚ) 2016/1148.

Siete EÚ umožňujú spoluprácu členských štátov na technickej a operačnej úrovni

- 25** Smernicou NIS sa zriadila [sieť jednotiek CSIRT](#), ktorá združuje tím [CERT-EU](#) (poskytovateľ služieb kybernetickej bezpečnosti pre inštitúcie, orgány, úrady a agentúry Únie) a jednotky CSIRT vymenované členskými štátmi. Cieľom tejto siete je budovať dôveru medzi vnútroštátnymi jednotkami CSIRT a podporovať rýchlu a účinnú operačnú spoluprácu medzi členskými štátmi.
- 26** Sieť [EU-CyCLONe](#) bola zriadená v roku 2020 ako neformálna sieť spolupráce pre vnútroštátne orgány zodpovedné za riadenie kybernetických kríz. Slúži ako most medzi technickou vrstvou, v ktorej pôsobí sieť jednotiek CSIRT, a politickou vrstvou Rady Európskej únie a jej [integrovanou politickou reakciou na krízu](#). Nadobudnutím účinnosti smernice NIS 2 v roku 2023 sa oficializovala úloha siete EU-CyCLONe a udelil sa jej jasný mandát.
- 27** Posúdili sme, či sú úlohy a povinnosti týchto sietí na úrovni EÚ dobre vymedzené a či umožňujú spoluprácu členských štátov.
- 28** Agentúra [ENISA](#) pôsobí ako sekretariát siete jednotiek CSIRT a siete EU-CyCLONe a poskytuje im zdroje, odborné znalosti, infraštruktúru a IT nástroje potrebné na spoluprácu a bezpečnú komunikáciu na účely výmeny informácií. Agentúra ENISA vo svojom prieskume spokojnosti⁴ zainteresovaných strán zo začiatku roka 2025 získala dobré hodnotenie za svoju výkonnosť ako sekretariát týchto sietí. Táto pozitívna spätná väzba sa potvrdila aj počas našich audítorských návštev, počas ktorých ju ocenili vnútroštátne orgány pre kybernetickú bezpečnosť.
- 29** Rada v roku 2025 prijala [kybernetickú koncepciu](#), v ktorej sa vymedzujú úlohy a povinnosti hlavných aktérov (vrátane siete jednotiek CSIRT a siete EU-CyCLONe) a mechanizmov zapojených do rozsiahlych kybernetických bezpečnostných incidentov alebo kybernetických kríz. Zistili sme, že v kybernetickej koncepcii sa vo veľkej miere objasňujú úlohy a povinnosti, pokiaľ ide o riadenie kybernetických kríz v EÚ, a zohľadňujú sa zmeny v prostredí od prvej koncepcie v roku 2017. Vymedzujú sa v nej tri úrovne spolupráce: technická, operačná a politická. Podrobne sa v nej opisujú nové siete a štruktúry zriadené od roku 2017, ako sú sieť EU-CyCLONe, tímy rýchlej reakcie EÚ na hybridné hrozby a európsky systém varovania pred kybernetickobezpečnostnými hrozbami, a rieši sa v nej, ako by sa riadenie kybernetických kríz malo začleniť do širšieho rámca reakcie EÚ na krízy.

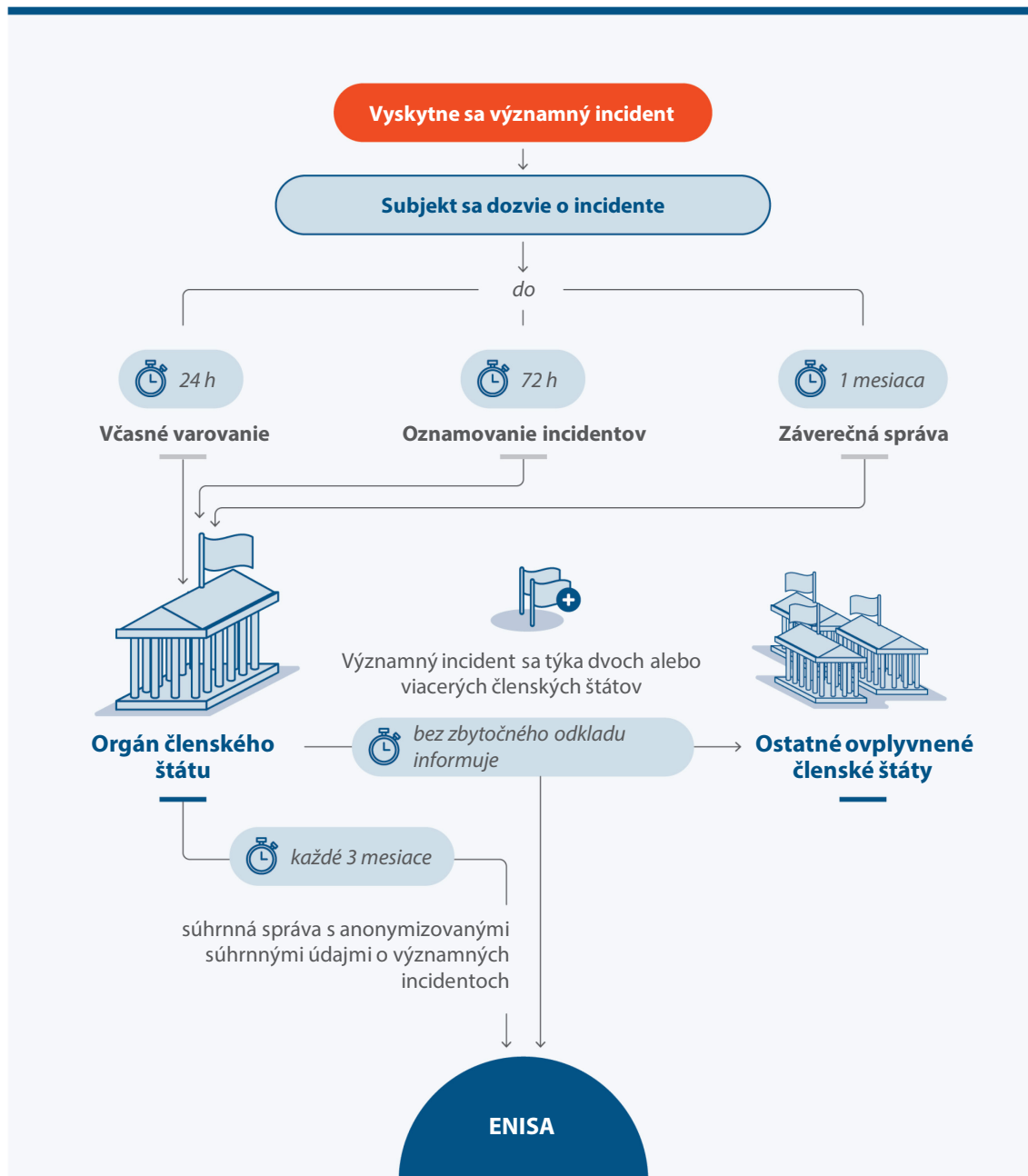
⁴ Konsolidovaná výročná správa o činnosti agentúry ENISA za rok 2024, s. 33 a 36.

- 30** Napriek oficiálnemu zriadeniu siete jednotiek CSIRT v roku 2016 a siete EU-CyCLONE v roku 2023 však tieto dve siete ešte musia oficiálne dohodnúť procesné opatrenia vzájomnej spolupráce. Nedohodli sa ani na kritériách pre sieť jednotiek CSIRT s cieľom informovať sieť EU-CyCLONE, že pozorovaný kybernetický bezpečnostný incident predstavuje potenciálny alebo prebiehajúci rozsiahly kybernetický bezpečnostný incident. Obe siete sa musia dohodnúť aj na spoločnej taxonómii úrovni závažnosti incidentov a kľúčových koncepcií, ako sú „hrozba“, „aktér hrozby“, „incident“ alebo „vplyv“, ktoré sú potrebné na umožnenie automatizovanej výmeny informácií. V súčasnosti existuje priestor na výklad toho, kedy sa incident kvalifikuje ako významný alebo rozsiahly. Orgány pre kybernetickú bezpečnosť všetkých troch kontrolovaných členských štátov spomenuli chýbajúcu spoločnú taxonómiu.

Obmedzená výmena informácií a podávanie správ výrazne znižujú pridanú hodnotu týchto sietí

- 31** Geografické hranice nebránia vzniku a šíreniu kybernetických bezpečnostných incidentov a kybernetických útokov. Výmena informácií medzi členskými štátmi, napríklad o taktikách a technikách používaných aktérmi hrozieb a o digitálnych znakoch, že došlo k porušeniu siete alebo informačného systému („ukazovatele narušenia“), môže významne prispieť k zvýšeniu kybernetickej bezpečnosti.
- 32** Zistili sme, že výmena informácií bola obmedzená, čo výrazne znižuje pridanú hodnotu týchto sietí. Obmedzenia, ktoré sme zaznamenali, sa týkajú najmä oneskorení pri transpozícii smernice NIS 2, problémov s určovaním, či má incident cezhraničný vplyv, právnych predpisov v oblasti národnej bezpečnosti, ktoré obmedzujú výmenu informácií, a nedostatočnej dôvery. Smernicou NIS 2 sa zavádza niekoľko požiadaviek na podávanie správ pre subjekty, ktoré patria do jej rozsahu pôsobnosti, a pre orgány členských štátov, ako je uvedené na [ilustrácii 2](#).

Ilustrácia 2 | Harmonogram oznamovania incidentov podľa smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v EÚ (NIS 2)



Zdroj: EDA na základe agentúry ENISA.

- 33** Členské štáty mali [smernicu NIS 2 transponovať](#) do vnútroštátneho práva do októbra 2024, ale len dva dodržali túto lehotu. Oneskorenia pri transpozícii majú významný vplyv na výmenu informácií, pretože subjekty, na ktoré sa vzťahuje smernica NIS 2, zatiaľ nie sú zo zákona povinné oznamovať incidenty. Komisia odhadla⁵, že sa smernica NIS vzťahuje na 15 500 subjektov, zatiaľ čo viac než 110 000 subjektov patrí do rozsahu pôsobnosti smernice NIS 2. Napríklad verejná správa, ktorá je podľa [správy agentúry ENISA o panoráme hrozieb](#) z roku 2025 najviac zacieleným sektorom EÚ, nemala povinnosť oznamovať incidenty podľa smernice NIS.
- 34** Oznamovanie údajov o incidentoch agentúre ENISA každé tri mesiace (t. j. dlho po možnom výskyte incidentu) obmedzuje ich pridanú hodnotu. Tieto údaje slúžia najmä na štatistické účely a vykazovanie historických trendov, nie na zlepšenie odhaľovania a reakcie. Agentúra ENISA poskytuje členským štátom [online nástroj](#) na predkladanie správ. Vzor na podávanie správ obsahuje minimálny súbor údajov, ktoré sa musia poskytnúť, ako je druh incidentu a príslušné odvetvie. Agentúra ENISA okrem toho navrhuje, aby členské štáty poskytli dodatočné informácie s cieľom umožniť podrobnejšiu analýzu údajov, napríklad prepojením incidentov s konkrétnymi zraniteľnosťami. Nie všetky členské štáty sa však rozhodli poskytovať tieto informácie, čím sa výrazne znížila kvalita a pridaná hodnota zozbieraných údajov.
- 35** Agentúra ENISA vo svojej [správe o stave kybernetickej bezpečnosti v EÚ za rok 2024](#) uviedla, že incidenty sú pravdepodobne nedostatočne nahlásované, keďže sa zdá, že počet nahlásených incidentov je nízky. V rokoch 2018 až 2021 členské štáty nahlásili agentúre ENISA 100 až 500 incidentov ročne. Tento počet sa postupne zvyšuje a v roku 2024 vzrástol na 1 276⁶.

⁵ Európska komisia, 2020, [správa o posúdení vplyvu](#).

⁶ Údaje [CIRAS](#) za rok 2024.

- 36** Agentúra ENISA vo svojej [správe o panoráme hrozieb za rok 2025](#), ktorá sa vzťahuje na obdobie od júna 2024 do júna 2025, identifikovala približne 4 800 kybernetických bezpečnostných incidentov⁷ prostredníctvom spravodajských informácií z otvorených zdrojov, ako sú spravodajské články. Tieto incidenty by podľa smernice NIS 2 nepodliehali oznamovacej povinnosti, keďže agentúra ENISA pri zbere údajov pokrýva širšie spektrum incidentov. Naopak, mnohé významné incidenty nie sú hlásené v spravodajských informáciách z otvorených zdrojov. Keďže údaje vykázané členskými štátmi sú anonymizované, agentúra ENISA nemôže korelovať incidenty, ktoré identifikuje, s incidentmi nahlásenými členskými štátmi. Preto nie je možné presne určiť rozsah nedostatočného nahlasovania incidentov, ale zastávame názor, že rozdiel medzi počtom incidentov nahlásených členskými štátmi a počtom incidentov v správe o panoráme hrozieb ukazuje, že nie všetky významné incidenty sú nahlásené.
- 37** Ďalším náznakom nedostatočného nahlasovania incidentov je počet oznámení ostatným ovplyvneným členským štátom a agentúre ENISA týkajúcich sa významných cezhraničných incidentov. Podobná požiadavka existovala aj v rámci smernice NIS, ale považovala sa za neúčinnú, keďže Komisia v roku 2020 dospela k záveru⁸, že oznámenia boli napriek tejto povinnosti zasielané len zriedka. Nesplnenie oznamovacej povinnosti pripísala chýbajúcim jasným spôsobom výmeny informácií a chýbajúcim spoločným cieľom, ktoré by motivovali k výmene informácií.
- 38** Povinnosť informovať ostatné členské štáty je zásadne dôležitá, aby sa zabránilo presahovaniu incidentov – ak sa tak nestane, negatívne to ovplyvní kybernetickú bezpečnosť EÚ. Sedem členských štátov nahlásilo v roku 2025 len 14 významných cezhraničných incidentov. Členské štáty predložili dve správy o incidentoch s možným cezhraničným vplyvom v roku 2024, ani jednu v roku 2023 a tri v roku 2022. Z toho vyplýva, že oznamovanie významných cezhraničných incidentov je veľmi nízke a neodráža skutočný rozsah takýchto útokov. S cieľom uviesť to do kontextu agentúra ENISA vo svojej [správe o panoráme hrozieb z roku 2024](#) identifikovala 322 incidentov, ktoré boli osobitne zamerané na dva alebo viaceré členské štáty. Incident v spoločnosti Collins Aerospace (pozri [rámcik 1](#)) je príkladom, keď členské štáty incident nenahlásili napriek tomu, že mal významný cezhraničný vplyv.

⁷ ENISA, [správa panoráme hrozieb z roku 2025](#).

⁸ Európska komisia, 2020, [správa o posúdení vplyvu](#).

Rámček 1

Kybernetický bezpečnostný incident narušil prevádzku letísk

V septembri 2025 bol Collins Aerospace, významný poskytovateľ technológií pre letecký priemysel, vystavený významnému ransomvérovému útoku, ktorý bol zameraný na jeho softvér na spracovanie cestujúcich. Útok prinútil veľké európske letiská, aby sa vrátili k manuálnej prevádzke, čo spôsobilo rozsiahle meškania a zrušenia letov. Narušenie bolo najvážnejšie na londýnskom letisku Heathrow, letisku v Bruseli, berlínskom letisku Brandenburg a letisku v Dubline.

Podľa smernice NIS 2 sa incident považuje za „významný“, ak okrem iného príslušnému subjektu spôsobí vážne prevádzkové narušenie služieb alebo finančnú stratu. Ani jeden členský štát však k tomuto incidentu nepristupoval ako k významnému alebo rozsiahlemu cezhraničnému incidentu. Ani jeden z ovplyvnených členských štátov preto incident oficiálne neoznámil agentúre ENISA ani iným členským štátom. Sieť jednotiek CSIRT neposkytovala sieti EU-CyCLONe poradenstvo, a preto nepodporila koordinované riadenie tohto incidentu.

Zdroj: Analýza EDA na základe rozhovorov s agentúrou ENISA.

- 39** Ďalším dôvodom obmedzeného oznamovania cezhraničných incidentov je skutočnosť, že je na každom orgáne členského štátu, aby určil, či má nahlásený incident cezhraničný vplyv, a aby identifikoval ostatné ovplyvnené členské štáty. Na základe informácií, ktoré majú k dispozícii, oznamujúci subjekt alebo orgán členského štátu nemusí vedieť o cezhraničnej povahe niektorých útokov. V súčasnosti neexistuje celoúnijná platforma, v ktorej by sa prijímali správy o incidentoch v reálnom čase od všetkých členských štátov a ktorá by mohla prepojiť informácie o odvetviach alebo ukazovateľoch ohrozenia s cieľom odhaliť cezhraničné incidenty. Existuje preto značné riziko, že niektoré cezhraničné incidenty nemusia byť identifikované a nahlásené.
- 40** Ani jeden členský štát nepovažoval od roku 2016 žiadny kybernetický bezpečnostný incident za „rozsiahly“. Toto vymedzenie sa v zásade vzťahuje na každý incident, ktorý má významný vplyv aspoň na dva členské štáty. Ani kybernetické bezpečnostné incidenty, ktoré spôsobili globálne výpadky a značné škody, ako sú incidenty uvedené na [ilustrácii 3](#), sa však nepovažovali za rozsiahle. V dôsledku toho eskalačný postup siete EU-CyCLONe nebol nikdy plne aktivovaný z dôvodu rozsiahleho kybernetického bezpečnostného incidentu.

Ilustrácia 3 | Príklady významných kybernetických bezpečnostných incidentov

WannaCry 2017 Celosvetový ransomvérový útok Infikovaných viac než 200 000 počítačov vo viac než 150 krajinách, čo ochromilo prevádzkovateľov kritickej infraštruktúry; šifrované údaje o infikovaných zariadeniach a požadovanom výkupnom na dešifrovanie 	NotPetya 2017 Deštruktívny malvér vydávaný za ransomvér Bol navrhnutý tak, aby natrvalo zmažal údaje, a zameral sa predovšetkým na Ukrajinu, pričom sa rýchlo šírila po celom svete, čo ochromilo nadnárodné spoločnosti a spôsobilo celosvetové škody 	Výpadok IT v súvislosti so systémom spoločnosti CrowdStrike júl 2024 Obrovský výpadok IT na celom svete Bol spôsobený chybnou aktualizáciou softvéru od kybernetickobezpečnostnej spoločnosti CrowdStrike, znefunkčnil milióny počítačov 
--	---	---

Zdroj: EDA, upravené podľa Cloudflare, ENISA, Europol, Wired, IBM, CrowdStrike.

- 41 Okrem oznamovacej povinnosti uloženej subjektom a členským štátom bola vytvorená sieť jednotiek CSIRT na uľahčenie výmeny informácií. Dôvera medzi členskými štátmi je jadrom siete jednotiek CSIRT, v rámci ktorej sa informácie vymieňajú na dobrovoľnom základe. Pridaná hodnota tejto siete sa výrazne znižuje, ak členské štáty nie sú ochotné vymieňať si včas informácie, na základe ktorých je možné konať.
- 42 Výmena informácií na úrovni EÚ je obmedzená vnútroštátnymi bezpečnostnými právnymi predpismi každého členského štátu. Ak sa členský štát domnieva, že informácie o kritickom subjekte súvisiace s kybernetickým útokom sú utajované alebo že oznámenie konkrétneho incidentu by poškodilo jeho národnú bezpečnosť, nie je povinný tieto informácie poskytnúť. Počas našich návštev v členských štátoch zástupcovia siete jednotiek CSIRT a siete EU-CyCLONe uviedli, že výmena informácií sa môže uskutočniť len v medziach právnych predpisov v oblasti národnej bezpečnosti. Na úrovni EÚ sa nevykonala analýza vnútroštátnych právnych rámcov členských štátov a ich vplyvu na výmenu informácií.

- 43** V roku 2016 sieť jednotiek CSIRT pozostávala z 28 národných jednotiek CSIRT s dvoma zástupcami za každý členský štát. Nedostatočná výmena informácií je pretrvávajúcim problémom a [Komisia v hodnotení](#) smernice NIS uznala, že „členské štáty si informácie medzi sebou nevymieňajú systematicky“, čo má vplyv najmä na účinnosť opatrení v oblasti kybernetickej bezpečnosti a úroveň spoločnej situačnej informovanosti na úrovni EÚ. Podľa smernice NIS 2 mnohé členské štáty okrem svojich národných jednotiek CSIRT vymenovali aj odvetvové jednotky CSIRT, takže sieť sa výrazne rozšírila. V čase konania auditu pozostávala zo 42 jednotiek CSIRT a viac než 700 jednotlivých účastníkov. Budovanie dôvery je preto ešte náročnejšie, keďže udržiavanie úzkych väzieb medzi všetkými členmi je zložité.
- 44** Sieť jednotiek CSIRT si je vedomá problému výmeny informácií a zvažuje rôzne opatrenia na zvýšenie dôvery v rastúcu sieť. Vytvorenie menších zoskupení členských štátov, ktoré tvoria cezhraničné centrá, ako sa podrobne uvádza v bodoch [62](#) – [74](#), je alternatívnym prístupom k celoeurópskej sieti, ktorý môže pomôcť riešiť túto výzvu.

Zmluvne dohodnuté služby kybernetického situačného centra čiastočne duplikuje existujúce kapacity a jeho budúce fungovanie nie je jasné

- 45** Podľa smernice NIS 2 v prípadoch, keď potenciálny alebo prebiehajúci rozsiahly kybernetický bezpečnostný incident má alebo pravdepodobne bude mať významný vplyv, sa Komisia stáva členom siete EU-CyCLONe⁹. Táto nová úloha a vývoj prostredia hrozieb viedli Komisiu k zriadeniu pracovnej skupiny pre kybernetickú koordináciu v rámci GR Connect v roku 2022. Táto pracovná skupina zahŕňa kybernetické situačné centrum, ktoré by malo Komisii pomôcť zvýšiť jej situačnú informovanosť s cieľom podporiť jej inštitucionálnu zodpovednosť za krízové riadenie. Mala by tiež pomôcť GR Connect poskytovať poradenstvo na politickej úrovni.
- 46** Pri zriaďovaní kybernetického situačného centra je Komisia vo veľkej miere podporovaná externými poskytovateľmi služieb, s ktorými bola v decembri 2022 uzavretá [zmluva](#) na takmer 18 mil. EUR na štyri roky. Posúdili sme zriadenie centra, jeho výstupy a plány Komisie na jeho budúce fungovanie.

⁹ Článok 16 ods. 2 [smernice NIS 2](#).

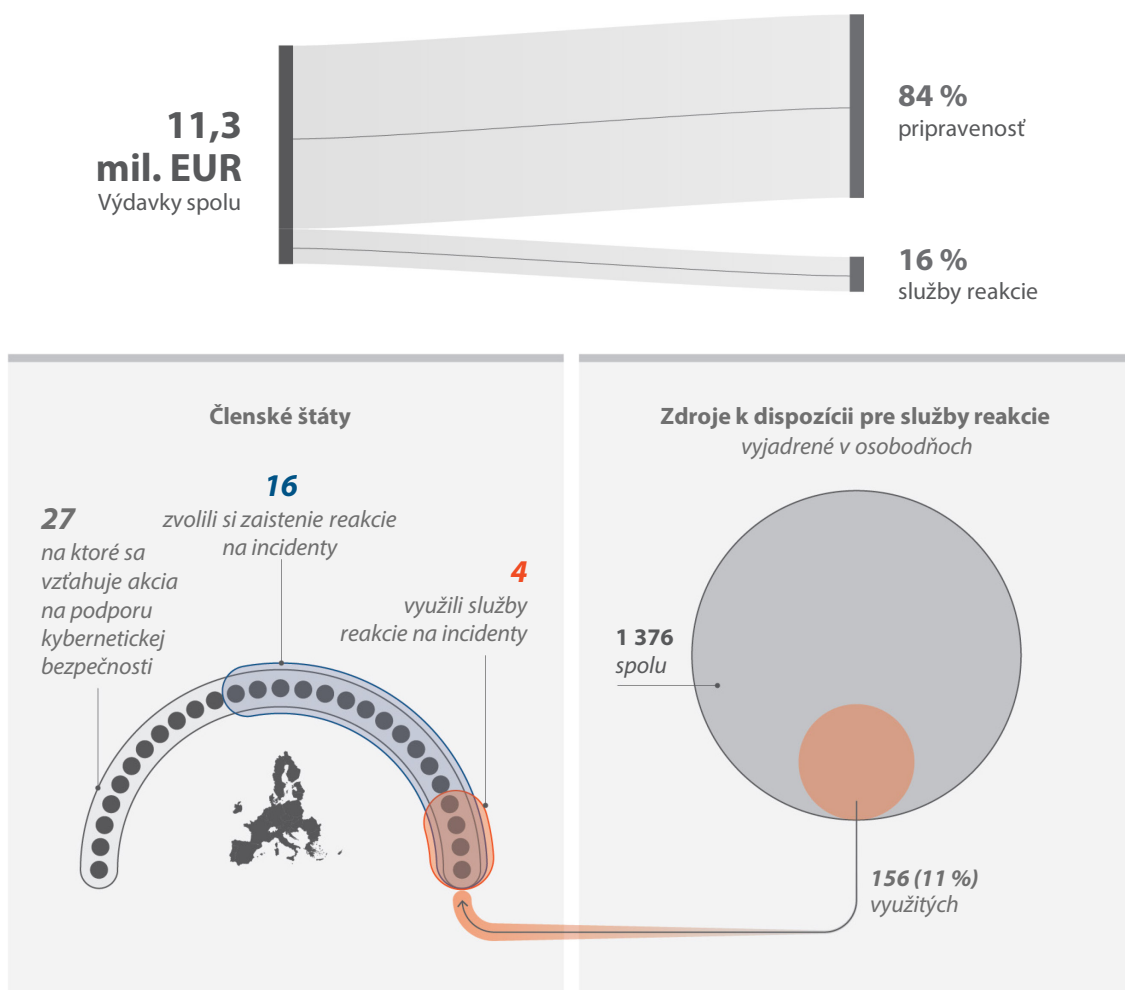
- 47** V rámci poskytovaných služieb dodávateľa vytvorili prehľad založený na komerčných spravodajských informáciách o kybernetických hrozbách s cieľom prezentovať a vymieňať si informácie o hrozbách. Vypracúvajú aj rôzne spravodajské správy o kybernetických hrozbách vrátane denných a týždenných správ a tematických správ o krajinách alebo odvetviach hospodárstva. Fyzické kybernetické situačné centrum, ktoré pozostáva z miestnosti vybavenej pracovnými stanicami diaľkovo pripojenými k ovládaciemu panelu spravovanému dodávateľmi, bolo zriadené v jednej z budov Komisie. V čase konania auditu kybernetické situačné centrum pozostávalo z malého počtu zamestnancov Komisie, ktorým pomáhali mnohí analytici zmluvných dodávateľov, ako aj odborníci z agentúry ENISA.
- 48** Zistili sme, že práca vykonaná externými poskytovateľmi služieb pre kybernetické situačné centrum čiastočne duplikuje existujúcu kapacitu agentúry ENISA. Agentúra ENISA má stálu kapacitu na situačnú informovanosť a monitorovanie hrozieb. Pravidelne uverejňuje správy o kybernetických hrozbách vrátane rýchlych správ o konkrétnych incidentoch a týždenných správ, ktoré poskytujú prehľad o hrozbách. Správy sú založené na spravodajských informáciách z otvorených zdrojov a sú podobné správam, ktoré vypracúvajú dodávateľa. Agentúra ENISA okrem toho vypracúva prehľady alebo sa podieľa na vypracovaní prehľadov na vysokej úrovni pre tvorcov politik v čase krízy, ktoré sú takisto porovnateľné s prehľadmi kybernetického situačného centra.
- 49** Okrem toho údaje, ktoré používa kybernetické situačné centrum na vypracovanie týchto správ, sú založené na komerčných spravodajských informáciách o kybernetických hrozbách a sú podobné údajom, ktoré používajú iné útvary Komisie, ako je Generálne riaditeľstvo pre digitálne služby a tím CERT-EU. Zastávame názor, že pri zriadení kybernetického situačného centra sa dostatočne nevyužil potenciál racionalizácie využitím informácií, ktoré už boli k dispozícii od Komisie a agentúry ENISA.
- 50** Platnosť zmluvy uplynie v decembri 2026. Potom dodávateľa už nebudú poskytovať služby kybernetickému situačnému centru. Tieto služby zahŕňajú poskytovanie údajov dostupných v prehľade, vypracúvanie správ o hrozbách a personálne obsadenie väčšiny centra. Prehľad sa odovzdá Komisii, ale ak sa nebude priebežne aktualizovať spravodajskými informáciami o kybernetických hrozbách, stratí svoju pridanú hodnotu.
- 51** V čase konania auditu Komisia nemala žiadne plány týkajúce sa podpory externými poskytovateľmi služieb na prevádzku kybernetického situačného centra po skončení platnosti zmluvy. Zastávame názor, že chýbajúci ucelený a podrobný plán do budúcnosti po skončení platnosti zmluvy predstavuje riziko pre prevádzku kybernetického situačného centra po roku 2026.

Rezerva EÚ na účely kybernetickej bezpečnosti umožňuje rýchle nasadenie služieb reakcie na incidenty

- 52** V roku 2022, bezprostredne po vojenskej agresii Ruska voči Ukrajine a uznávajúc, že rozsiahle kybernetické útoky sú čoraz rozšírenejšie, Komisia poskytla agentúre ENISA výnimočné finančné prostriedky vo výške 15 mil. EUR na pilotné vykonávanie [akcie na podporu kybernetickej bezpečnosti](#), ktorá sa začala v roku 2023. V roku 2023 Komisia poskytla dodatočné finančné prostriedky (približne 20 mil. EUR) na predĺženie programu do konca roka 2026.
- 53** Komisia takisto navrhla [akt o kybernetickej solidarite](#) – prijatý v decembri 2024 – s cieľom pripraviť sa na riešenie rozsiahlych kybernetických bezpečnostných incidentov. Aktom sa zriaďuje rezerva EÚ na účely kybernetickej bezpečnosti, ktorá zahŕňa služby reakcie na incidenty poskytované dôveryhodnými poskytovateľmi. Začala fungovať postupne v roku 2025 s rozpočtom 36 mil. EUR na obdobie 2025 – 2027.
- 54** Posúdili sme, ako bol organizovaný program akcie na podporu kybernetickej bezpečnosti, keďže tvorí základ rezervy EÚ na účely kybernetickej bezpečnosti. Skontrolovali sme aj to, či skúsenosti získané od roku 2022 prispeli k návrhu rezervy EÚ na účely kybernetickej bezpečnosti.
- 55** Agentúra ENISA navrhla akciu na podporu kybernetickej bezpečnosti ako mechanizmus na poskytovanie služieb na podporu pripravenosti a reakcie členských štátov na rozsiahle kybernetické bezpečnostné incidenty alebo krízy. Všetky služby sú vopred zmluvne dohodnuté agentúrou ENISA, čo znamená, že poskytovatelia služieb môžu začať pracovať hneď, ako to členské štáty vyžadujú. Je to aj vďaka štruktúre agentúry ENISA, ktorá zabezpečuje nepretržitú pohotovosť úradníka na vybavovanie žiadostí členských štátov.
- 56** Agentúra ENISA sa rozhodla rozdeliť dostupný rozpočet rovnomerne medzi členské štáty. V praxi agentúra vyhlásila verejnú súťaž rozdelenú na 27 častí, jednu za každý členský štát, s cieľom vybrať najviac troch súkromných poskytovateľov bezpečnostných služieb na poskytovanie služieb do konca roka 2026. Agentúra ENISA okrem toho vybrala niektorých poskytovateľov v rámci celoeurópskej časti na poskytovanie služieb oprávneným krajinám mimo EÚ, ako aj inštitúciám, orgánom a agentúram EÚ alebo na podporu reakcie na cezhraničné incidenty.

- 57** Tento prístup umožnil agentúre ENISA zohľadniť osobitné vnútroštátne požiadavky vrátane jazyka, národných bezpečnostných previerok alebo etablovanej prítomnosti v členských štátoch. Na druhej strane, keďže poskytovatelia neboli vybraní tak, aby boli schopní poskytovať služby v celej EÚ, hlavným nedostatkom tohto prístupu je, že ak členský štát nevyužíva vopred zmluvne dohodnuté služby, rozpočet viazaný na takéto služby pre konkrétny členský štát nemožno použiť na pomoc inému členskému štátu.
- 58** Pokiaľ ide o akciu na podporu kybernetickej bezpečnosti, členské štáty si môžu vybrať medzi službami pripravenosti alebo reakcie alebo ich kombináciou. Členské štáty sa v prvom rade rozhodli využiť dostupné finančné prostriedky na zlepšenie svojej pripravenosti (84 % výdavkov v roku 2023). Členské štáty, ktoré sa rozhodli pre zaistenie reakcie na incidenty (t. j. vopred stanovenú dohodu s poskytovateľom, ktorou sa zabezpečí, že členský štát bude mať prístup k službám poskytovateľa na požiadanie v záujme rýchlej reakcie na kybernetické bezpečnostné incidenty), ju využívali striedmo, ako je uvedené na [ilustrácii 4](#). V troch kontrolovaných členských štátoch orgány ocenili riadenie akcie na podporu kybernetickej bezpečnosti agentúrou ENISA.

Ilustrácia 4 | Opatrenia agentúry ENISA na podporu kybernetickej bezpečnosti do roku 2023



Zdroj: EDA na základe údajov agentúry ENISA.

- 59** V období 2024 – 2026 požiadalo o zaistenie reakcie na incidenty len deväť členských štátov. Naše rozhovory s agentúrou ENISA a orgánmi v troch členských štátoch potvrdili, že výrazne uprednostňujú činnosti v oblasti pripravenosti.

- 60** Hoci cieľom rezervy EÚ na účely kybernetickej bezpečnosti je v prvom rade podporiť reakciu a zotavenie, pokiaľ ide o závažné kybernetické bezpečnostné incidenty, vopred viazané služby z rezervy EÚ na účely kybernetickej bezpečnosti, ktoré sa nevyužívajú na reakciu na incidenty, možno zmeniť na služby pripravenosti. Tento pružný prístup môže zabrániť tomu, aby sa predplatené služby nevyužívali.
- 61** Zastávame názor, že model zvolený pre rezervu EÚ na účely kybernetickej bezpečnosti vychádza zo skúseností získaných z programu akcie na podporu kybernetickej bezpečnosti. Údaje o využívaní programu akcie na podporu kybernetickej bezpečnosti však poukazujú na riziko, že rezerva EÚ na účely kybernetickej bezpečnosti by sa mohla primárne použiť na pripravenosť, a nie na reakciu, čo je v rozpore s účelom stanoveným v akte o kybernetickej solidarite.

Cieľom európskeho systému varovania pred kybernetickobezpečnostnými hrozbami je zlepšiť kapacity na odhaľovanie hrozieb, ale tento systém nie je funkčný

- 62** Jedným z kľúčových cieľov európskeho systému varovania pred kybernetickobezpečnostnými hrozbami je podporiť zmysluplnú výmenu informácií s cieľom zlepšiť odhaľovanie kybernetických hrozieb, ich analýzu a reakciu na ne. Účasť v systéme varovania je dobrovoľná, ale členské štáty, ktoré sa rozhodnú pripojiť k cezhraničnému kybernetickému centru, sa musia zaviazat, že si budú vymieňať relevantné informácie s ostatnými členmi. Spoluprácou v zoskupeniach v dôveryhodnom a bezpečnom prostredí sa členské štáty môžu vyhnúť niektorým problémom týkajúcim sa výmeny informácií uvedeným v bodoch [31](#) – [44](#).
- 63** V čase konania auditu sa 13 členských štátov rozhodlo byť súčasťou európskeho systému varovania pred kybernetickobezpečnostnými hrozbami, čím sa zriadili dve cezhraničné centrá: ATHENA a ENSOC. Tretiemu cezhraničnému kybernetickému centru, NBCC, boli pridelené finančné prostriedky na jeho zriadenie v roku 2026, čím sa počet členov siete zvýšil na celkovo 20 krajín (18 členských štátov, ako aj Island a Nórsko¹⁰), ako je znázornené na [ilustrácii 5](#).

¹⁰ Pridružené krajiny mimo EÚ podľa článku 10 ods. 1 nariadenia (EÚ) 2021/694.

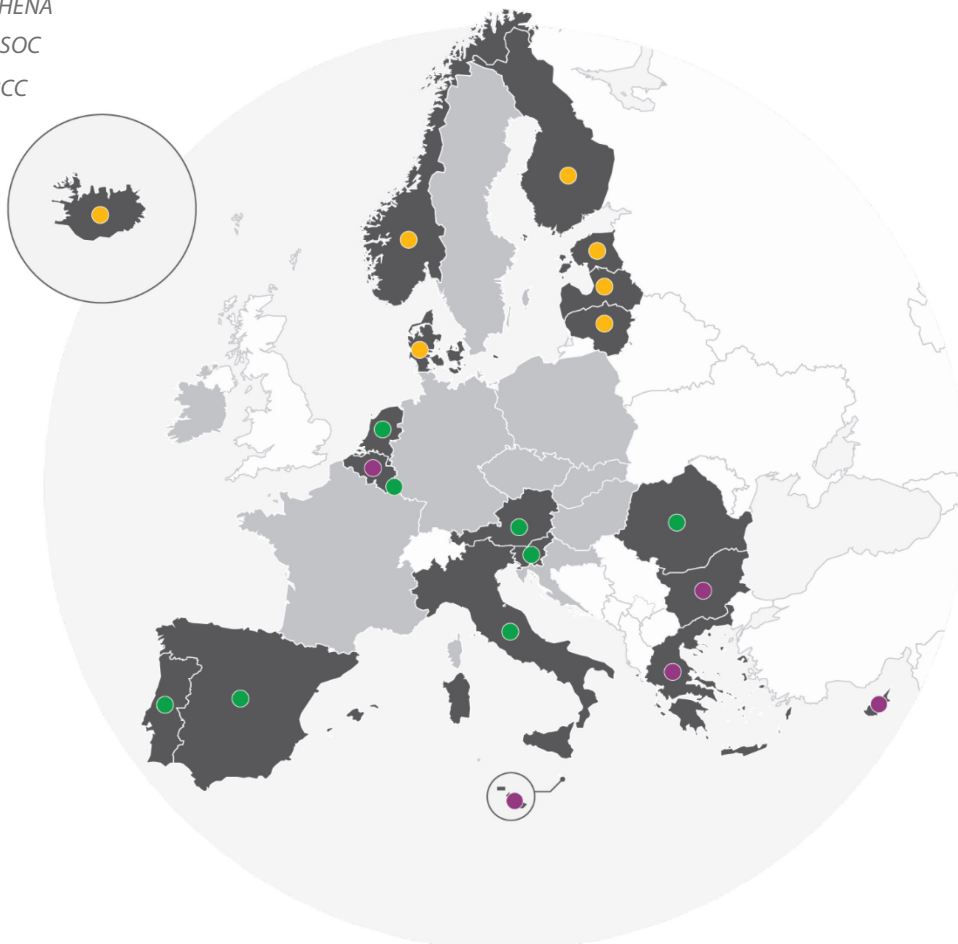
Ilustrácia 5 | Krajiny v európskom systéme varovania pred kybernetickobezpečnostnými hrozbami

■ Krajiny v európskom systéme varovania pred kybernetickobezpečnostnými hrozbami

● ATHENA

● ENSOC

● NBCC



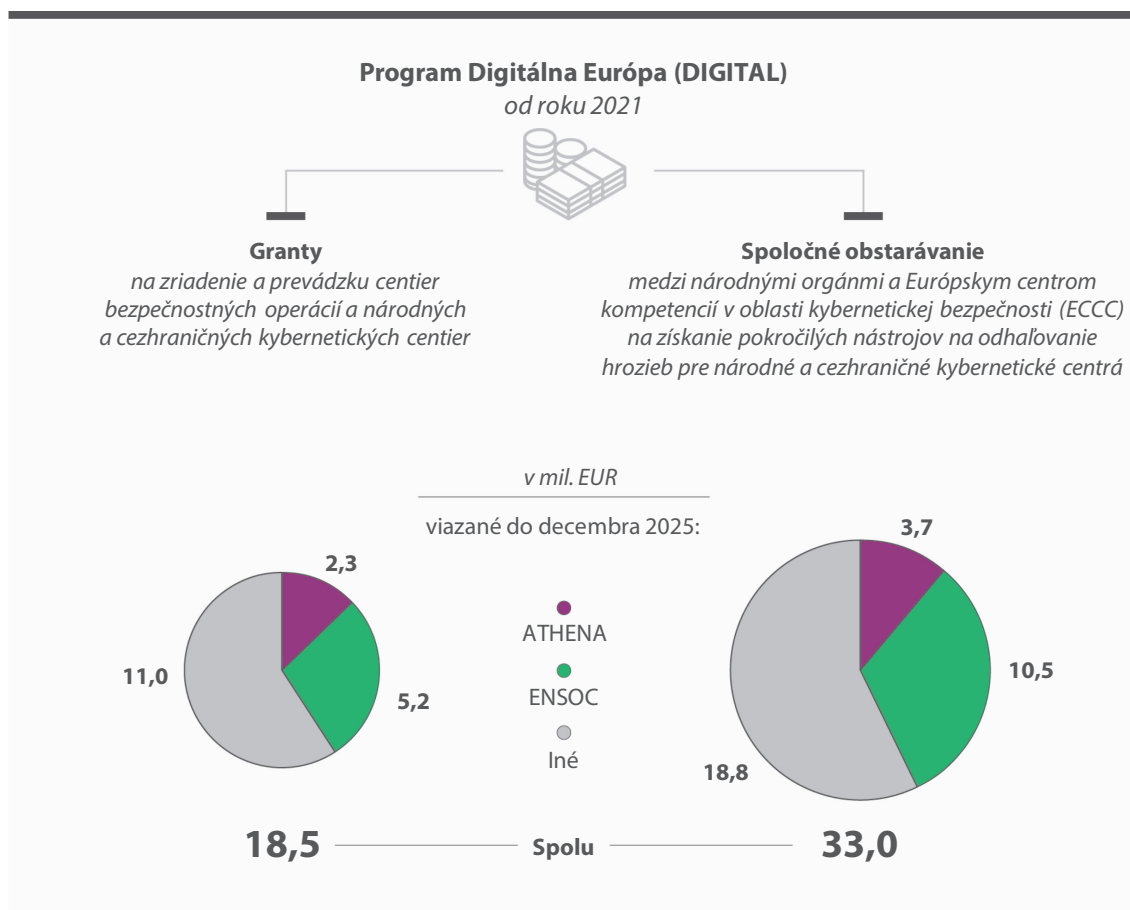
Zdroj: EDA.

- 64** Posúdili sme, ako boli zriadené prvé dve cezhraničné kybernetické centrá, ako aj ich pokrok pri dosahovaní cieľov európskeho systému varovania pred kybernetickobezpečnostnými hrozbami. Preskúmali sme aj to, ako zriadenie cezhraničných kybernetických centier zapadá do širšieho prostredia kybernetickej bezpečnosti a ako spolupracujú s existujúcimi sieťami a štruktúrami.

Zatiaľ sa nedosiahli konkrétne výsledky z dôvodu značných oneskorení vo verejnom obstarávaní

- 65** Finančné prostriedky na podporu zriaďovania národných a cezhraničných kybernetických centier sú k dispozícii prostredníctvom programu Digitálna Európa od roku 2021. Toto financovanie sa poskytuje prostredníctvom zložitého postupu s dvoma paralelnými tokmi: tradičné granty na podporu zriaďovania a prevádzky centier a spoločné obstarávanie na nákup pokročilých nástrojov na odhaľovanie hrozieb, ako je znázornené na [ilustrácii 6](#). Po výzve na predkladanie návrhov v novembri 2022 začali centrá ATHENA a ENSOC svoju činnosť v januári 2024.

Ilustrácia 6 | Financovanie kybernetických centier z programu Digitálna Európa



Zdroj: EDA na základe údajov ECCC.

- 66** Dvojfázové užšie postupy obstarávania¹¹ zorganizovali členovia centier ATHENA a ENSOC, ako aj GR Connect (prvá fáza) a novovytvorené centrum ECCC (druhá fáza). Cieľom dvojfázového prístupu je obmedziť obeh citlivých informácií poskytnutím podrobných technických špecifikácií len uchádzačom vybraným v prvej fáze.
- 67** Prvá fáza sa začala v máji 2024 v prípade centra ENSOC a v júli 2024 v prípade centra ATHENA. Spoločnosti, ktoré prejavili záujem, mali jeden mesiac na predloženie ponuky. Úspešní uchádzači však boli informovaní až v apríli 2025, takmer rok po začatí postupu.
- 68** Okrem toho postupy verejného obstarávania centra ENSOC ani centra ATHENA nemohli v tom čase prejsť do druhej fázy, keďže členovia centra a ECCC neboli schopní poskytnúť spoločnostiam zaradeným do užšieho výberu technické špecifikácie potrebné na predloženie ponuky, keďže stále pracovali na ich dokončení.
- 69** Druhá fáza postupov verejného obstarávania sa začala až v auguste 2025 v prípade niektorých častí centra ENSOC a bola naplánovaná na začiatok roka 2026 v prípade centra ATHENA. V čase konania auditu, 18 mesiacov po začatí postupu verejného obstarávania, nebola podpísaná žiadna zmluva ani na jednu časť. Zastávame názor, že nedostatočná príprava a zložitosť postupov verejného obstarávania mali nepriaznivý vplyv na ich včasné dokončenie.
- 70** Zistili sme, že cezhraničné centrá preto nie sú na dobrej ceste k dosiahnutiu svojich cieľov. Bez nástrojov na odhaľovanie hrozieb a výmenu informácií sú operačne pozastavené a európsky systém varovania pred kybernetickobezpečnostnými hrozbami ešte nefunguje, čo oddŕaľuje účinný rozvoj pokročilých spôsobilostí na odhaľovanie kybernetických hrozieb a incidentov a predchádzanie týmto hrozbám a incidentom. Boli podpísané zmeny s cieľom predĺžiť trvanie dohody o grante, aby sa zohľadnili doterajšie oneskorenia v postupoch verejného obstarávania (15 mesiacov v prípade centra ATHENA a 18 mesiacov v prípade ENSOC).

¹¹ Výzva centra ENSOC na predkladanie ponúk a výzva centra ATHENA na predkladanie ponúk.

Cezhraničné kybernetické centrá vytvárajú ďalšie komunikačné kanály, ktoré ešte viac zvyšujú zložitosť

- 71** Jednou z hlavných úloh cezhraničných kybernetických centier je výmena relevantných informácií s cieľom zlepšiť odhaľovanie hrozieb a reakciu na ne. Patria sem informácie o kybernetických hrozbách, zraniteľnostiach, ukazovateľoch ohrozenia a aktéroch hrozieb. Úlohy cezhraničných kybernetických centier sa čiastočne prekrývajú s úlohami národných jednotiek CSIRT a siete jednotiek CSIRT, najmä pokiaľ ide o výmenu informácií o kybernetických hrozbách a zraniteľnostiach. Úlohy cezhraničných kybernetických centier a jednotiek CSIRT nie sú jasne vymedzené. Podľa kybernetickej koncepcie z roku 2025 (bod 29) majú cezhraničné kybernetické centrá fungovať na technickej (ako národné jednotky CSIRT a sieť jednotiek CSIRT) aj operačnej úrovni (ako sieť EU-CyCLONe).
- 72** V akte o kybernetickej solidarite sa požaduje, aby cezhraničné kybernetické centrá medzi sebou podpisovali dohody o spolupráci s cieľom uľahčiť výmenu informácií. Agentúra ENISA mala do februára 2026 vydať usmernenia pre interoperabilitu medzi cezhraničnými kybernetickými centrami, ako sa to vyžaduje v akte o kybernetickej solidarite. Medzitým ECCC v decembri 2025 udelilo konzorciu (vrátane niektorých členov ENSOC a ATHENA) grant na vymedzenie technického rámca interoperability medzi cezhraničnými kybernetickými centrami. Usmernenia a rámec sa však dokončia až po uvedení cezhraničných kybernetických centier do prevádzky. Ako sme poukázali v našom stanovisku z roku 2023 k návrhu aktu o kybernetickej solidarite¹², existuje riziko, že bez rýchlej dohody by sa mohli vyvinúť systémy, ktoré budú navzájom nekompatibilné, čo by viedlo k zvýšeným nákladom.

¹² Stanovisko 02/2023 k návrhu nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú opatrenia na posilnenie solidarity a kapacít v Únii na odhaľovanie kybernetických hrozieb a incidentov, prípravu a reakciu na ne, bod 26.

- 73** Od cezhraničných kybernetických centier sa takisto vyžaduje, aby si bez zbytočného odkladu vymieňali relevantné informácie o rozsiahlych kybernetických bezpečnostných incidentoch so sieťou EU-CyCLONe a sieťou jednotiek CSIRT. Na úrovni členských štátov sa vytvorením národných kybernetických centier a účasťou v cezhraničných kybernetických centrách vytvárajú ďalšie úrovne komunikácie. Zložitosť zvyšuje aj koordinácia s členskými štátmi mimo EÚ¹³, ktoré nie sú členmi siete jednotiek CSIRT ani siete EU-CyCLONe.
- 74** Na dosiahnutie dohody o spoločnej taxonómii a spôsobe výmeny informácií a na zabezpečenie interoperability sú potrebné jasné dohody o spolupráci. Skúsenosti získané zo siete jednotiek CSIRT ukazujú, že ide o významnú výzvu. Zistili sme, že v čase konania auditu neboli dohodnuté žiadne procedurálne opatrenia o spolupráci a výmene informácií. Zastávame názor, že zriadenie národných a cezhraničných kybernetických centier by mohlo podporiť účinnejšiu výmenu informácií. Integrácia cezhraničných centier do už aj tak zložitého prostredia kybernetickej bezpečnosti však bude náročná a bude si vyžadovať dodatočné komunikačné kanály a dohody o spolupráci.

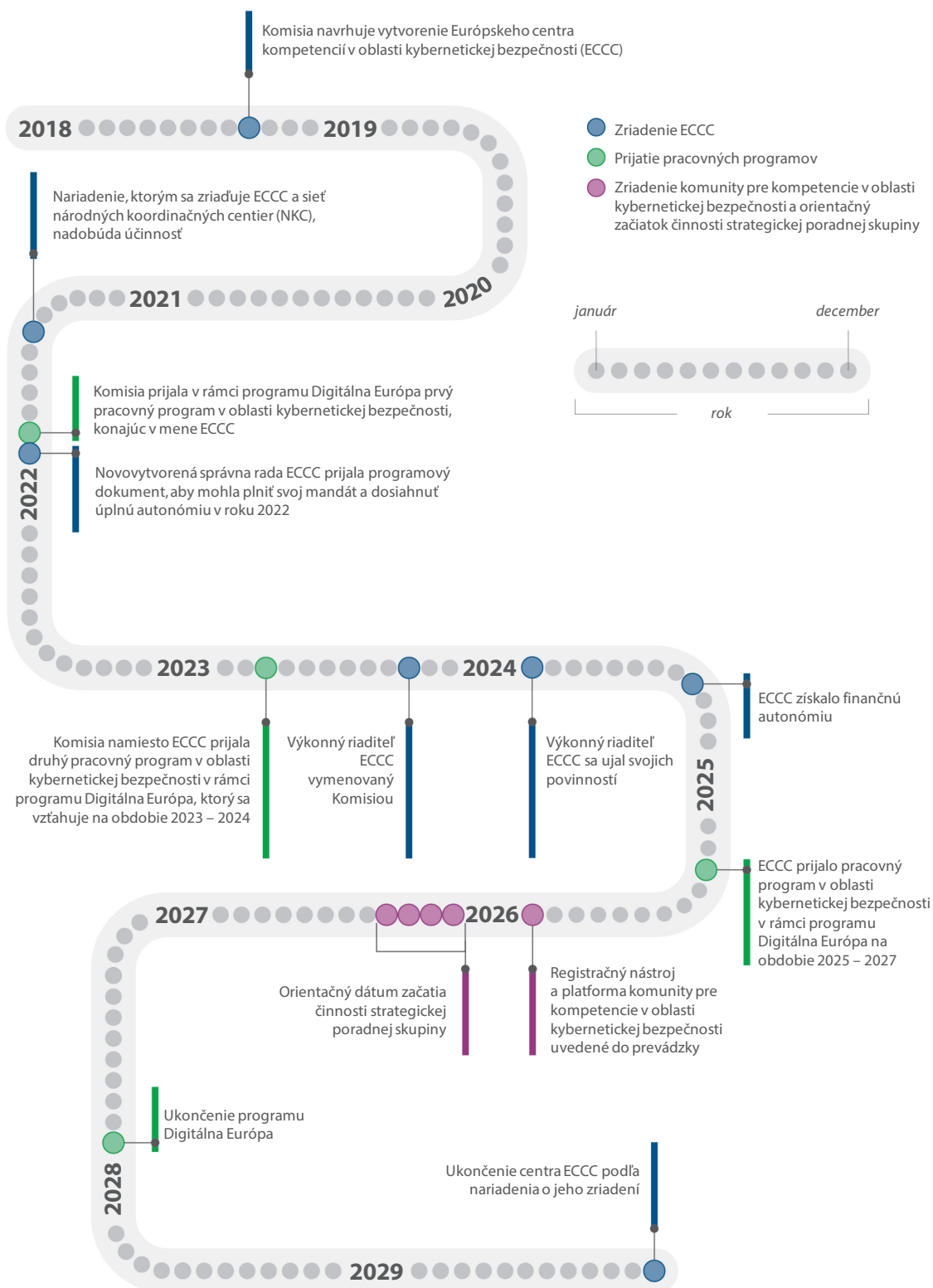
¹³ Island a Nórsko.

Projekty financované EÚ v rámci programu Digitálna Európa sú zamerané na posilnenie kybernetickej bezpečnosti, ale čelia výzvam pri vykonávaní a podávaní správ

Oneskorenia pri zriaďovaní komunity pre kompetencie v oblasti kybernetickej bezpečnosti jej zabránili formovať program Digitálna Európa podľa jej potrieb

- 75** S cieľom riadiť kybernetickobezpečnostnú zložku programu Digitálna Európa Komisia v roku 2018 navrhla vytvorenie Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti (ECCC). V nariadení o ECCC sa plánovalo, že ECCC bude podporované sieťou 29 národných koordinačných centier (NKC), jedným za každý členský štát, ako Island a Nórsko. Bola v ňom aj výzva na vytvorenie komunity pre kompetencie v oblasti kybernetickej bezpečnosti (ďalej len „komunita“) pozostávajúcej zo zástupcov priemyselných, akademických a výskumných organizácií, ako aj iných príslušných združení občianskej spoločnosti.
- 76** Do strategickej poradnej skupiny, ktorá je jednou z troch zložiek štruktúry ECCC, by sa vymenovalo najviac 20 členov komunity. Jednou z hlavných úloh strategickej poradnej skupiny je organizovať verejné konzultácie, ktoré budú podkladom pre program ECCC a pracovné programy programu Digitálna Európa.
- 77** Posudzovali sme, či program Digitálna Európa a jeho pracovné programy boli prijaté na základe dôkladnej analýzy potrieb, ako aj to, ako boli ECCC, sieť národných koordinačných centier, komunita a strategická poradná skupina schopné prispieť k pracovným programom. V praxi sa ECCC, sieť národných koordinačných centier, komunita a strategická poradná skupina zriaďovali postupne v priebehu niekoľkých rokov (pozri [ilustráciu 7](#)).

Ilustrácia 7 | Harmonogram zriadenia Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti, siete národných koordinačných centier, komunity a strategickej poradnej skupiny



Zdroj: EDA.

- 78** Keďže ECCC začalo plne fungovať až v septembri 2024, Komisia v mene ECCC prijala pracovné programy na obdobia 2021 – 2022 a 2023 – 2024. Dva pracovné programy prijaté Komisiou nemohli využiť prínos komunity.
- 79** Členské štáty medzitým začali zriaďovať svoje národné koordinačné centrá, ktoré pôsobia ako kontaktné miesta na vnútroštátnej úrovni pre komunitu. Ich zriadenie a prevádzka boli spolufinancované z programu Digitálna Európa, pričom v čase konania auditu bolo z finančných prostriedkov EÚ poskytnutých viac než 90 mil. EUR vrátane približne 44 mil. EUR, ktoré sa ďalej rozdelia prostredníctvom finančnej podpory tretím stranám. Na podporu národných koordinačných centier bolo do roku 2027 vyčlenených ďalších 38 mil. EUR.
- 80** Zistili sme, že v decembri 2025, štyri roky po zriadení ECCC a siete národných koordinačných centier, komunita ešte nebola zriadená a strategická poradná skupina ešte nebola vymenovaná. ECCC prijalo 14. marca 2025 najnovší pracovný program v oblasti kybernetickej bezpečnosti v rámci programu Digitálna Európa, ktorý sa vzťahuje na obdobie 2025 – 2027. Hoci ECCC vypracovalo a prijalo svoj pracovný program po rozsiahlych konzultáciách s členskými štátmi a sieťou národných koordinačných centier, nemohlo využiť vstup a poradenstvo komunity či strategickú poradnú skupinu. To je v rozpore s ustanoveniami jeho zakladajúceho nariadenia a považujeme to za premárnenú príležitosť.
- 81** Program Digitálna Európa bude ukončený v roku 2027 a ak sa jeho mandát nepredĺži, očakáva sa, že činnosť ECCC bude ukončená v roku 2029. Podpora siete národných koordinačných centier, komunity a strategickú poradnú skupinu by preto po ich zriadení mohla byť relevantná len počas krátkeho obdobia.

Projekty financované EÚ sledujú príslušné ciele, ale mnohé z nich čelia operačným problémom

82 Vybrali sme vzorku 11 projektov relevantných pre odhaľovanie kybernetických bezpečnostných incidentov a reakciu na ne, ktoré boli financované z programu Digitálna Európa v období 2022 – 2025 (pozri [ilustráciu 5](#) v [prílohe I](#) a [prílohu III](#)). Posúdili sme, či:

- ciele projektov boli v súlade s očakávanými výsledkami vyjadrenými vo výzvach na predkladanie návrhov a s celkovo s očakávanými výsledkami programu Digitálna Európa,
- projekty doteraz dosiahli plánované výstupy a výsledky,
- výstupy projektov boli dodané načas.

Výsledok nášho posúdenia uvádzame v [prílohe IV](#).

Niektoré projekty už dosahujú výsledky, ale mnohé čelia prevádzkovým výzvam a oneskoreniam

83 Zistili sme, že všetky projekty sledujú ciele, ktoré prispievajú k dosiahnutiu cieľov v oblasti kybernetickej bezpečnosti programu Digitálna Európa¹⁴, a že sa nimi rieši väčšina cieľov výziev na predkladanie návrhov¹⁵.

84 Z 11 projektov v našej vzorke boli dva projekty v počiatočnom štádiu realizácie, a preto sme nemohli dospieť k záveru o ich výkonnosti. Zvyšné štyri sme vyhodnotili ako uspokojivé, pokiaľ ide o dosahovanie plánovaných výstupov a výsledkov. Zastávame názor, že dva projekty vykazujú určité nedostatky, a tri sme vyhodnotili ako neuspokojivé (pozri [prílohu IV](#)).

85 Program Digitálna Európa sa výslovne zameriava na zvýšenie úrovne kybernetickej bezpečnosti malých a stredných podnikov (MSP). V tejto súvislosti niekoľko projektov ponúka konkrétne riešenia pre MSP (pozri [rámcik 2](#)).

¹⁴ Článok 6 [nariadenia \(EÚ\) 2021/694](#), ktorým sa zriaďuje program Digitálna Európa.

¹⁵ Výzvy: Budovanie kapacít centier bezpečnostných operácií; Zavedenie siete národných koordinačných centier v členských štátoch; Poskytovanie podpory pripravenosti a vzájomnej pomoci a Nové aplikácie umelej inteligencie a iné podporné technológie pre centrá bezpečnostných operácií.

Rámček 2

Príklady projektov, ktoré prinášajú hmatateľné výsledky pre MSP

Cieľom projektu **GR-SME-SOC** (projekt 6 v **prílohe III**) je poskytnúť nástroje a služby kybernetickej bezpečnosti MSP v Grécku zriadením centra bezpečnostných operácií prispôbeného ich potrebám. Projekt sa začal v januári 2024 a realizuje ho konzorcium piatich gréckych organizácií. Plánuje sa bezplatné poskytovanie služieb kybernetickej bezpečnosti 120 MSP počas jedného roka, potom budú tieto služby komerčne dostupné. V rámci projektu sa MSP ponúkajú pokročilé služby, ako je monitorovanie v reálnom čase, odhaľovanie hrozieb založené na umelej inteligencii a rýchla reakcia na incidenty.

V rámci projektu **NCC-IE** (projekt 3 v **prílohe III**) poskytol koordinátor projektu približne 1,8 mil. EUR vo forme grantov viac než 50 írskym MSP na zlepšenie ich kybernetickej bezpečnosti. Grantová schéma zvýhodnila spoločnosti s 2 až približne 200 zamestnancami vrátane rodinných podnikov, startupov a celosvetových vývozcov v rôznych odvetviach. Granty boli určené výlučne spoločnostiam, ktoré sa predtým podrobili preskúmaniu kybernetickej bezpečnosti, ktoré riadila štátna agentúra Enterprise Ireland. Grant pokrýval 80 % nákladov (do výšky 60 000 EUR) na vykonanie odporúčaní z preskúmania.

Zdroj: EDA.

- 86** Mnohé projekty v našej vzorke majú problémy s dodržaním termínov alebo čelia prevádzkovým výzvam (pozri **prílohu IV**). Zistili sme, že štyri projekty čelia značným oneskoreniam. Patria sem centrá ENSOC a ATHENA, ako je podrobne uvedené v bodoch **65 – 70**. Ďalšie príklady uvádzame v **rámčeku 3**.

Rámček 3

Príklady projektov, ktoré čelia prevádzkovým výzvam a oneskoreniam

V Írsku je jediným prijímateľom grantu na projekt **ILG-SOC** (projekt 8 v *prílohe III*) riadiaci orgán miestnej samosprávy (LGMA). Cieľom projektu je zriadiť centrálné bezpečnostné operačné centrum pre 31 miestnych orgánov, ktoré budú využívať pokročilé nástroje na odhaľovanie hrozieb a reakciu na ne. Projekt sa začal v októbri 2023 s trvaním tri roky. Preskúmanie v polovici trvania viedlo k zamietnutiu všetkých výstupov. Projekt zahŕňa niekoľko postupov verejného obstarávania, ktoré boli neúspešné alebo sa oneskorili. Trvanie projektu sa predĺži (bez dodatočného financovania), čo by mohlo poskytnúť dostatok času na úspešné ukončenie projektu.

V Grécku je cieľom projektu **EL-SOC** (projekt 5 v *prílohe III*) zriadiť konsolidované centrum bezpečnostných operácií na národnej úrovni, ktoré by zhromažďovalo informácie od odvetvových centier bezpečnostných operácií. To by poskytlo ucelený prehľad o situácii v oblasti kybernetickej bezpečnosti v reálnom čase. Projekt prebieha od januára 2024 do decembra 2026. Plánované obstarávanie hardvéru a služieb sa oneskorilo pre problémy s dokončením a uverejnením technických špecifikácií výzvy na predkladanie ponúk. Ako dôvody oneskorenia koordinátor projektu uviedol aj otázky týkajúce sa zabezpečenia vnútroštátneho spolufinancovania a obmedzenej dostupnosti zamestnancov na verejné obstarávanie.

Zdroj: EDA.

- 87** Ďalšie dva projekty v našej vzorke čelia miernym oneskoreniam. Tri projekty priniesli svoje výstupy včas. A napokon, dva projekty sú v počiatočnom štádiu realizácie, a preto o nich nemôžeme vyvodiť záver.

Bezpečnostné obmedzenia viedli k prevádzkovým výzvam a pri kontrolách vykonávaných prijímateľmi existujú značné riziká

- 88** V nariadení o programe Digitálna Európa sa stanovuje, že z bezpečnostných dôvodov sa financovanie kybernetickej bezpečnosti môže obmedziť na subjekty usadené v EÚ a kontrolované členskými štátmi alebo občanmi EÚ. Cieľom tohto obmedzenia je zmierniť riziko narušenia alebo vplyvu zo strany štátov mimo EÚ a zabrániť výmene citlivých bezpečnostných informácií s orgánmi mimo EÚ.

- 89** Povinnosť EÚ vlastniť a kontrolovať sa vzťahuje nielen na prijímateľov grantov, ale aj na ich subdodávateľov a všetkých príjemcov finančnej podpory tretím stranám (FSTP). S výnimkou druhej kategórie (pozri body [92](#) – [96](#)) vykonáva toto posúdenie centrálna služba pre validáciu [Európskej výkonnej agentúry pre výskum](#). Konečné rozhodnutie o oprávnenosti účasti na užších výzvach však stále prijíma orgán udeľujúci grant, t. j. GR Connect alebo centrum ECCC.
- 90** Počas našej auditorskej práce prijímatelia opakovane spomenuli praktické výzvy, ktoré predstavujú posúdenia vlastníctva a kontroly. Posúdenie vlastníctva a kontroly EÚ môže byť zložitý a zdĺhavý proces. Vyžaduje si analýzu úplnej vlastníckej štruktúry a kontrolného reťazca každej organizácie vrátane všetkých úrovní vlastníctva až po konečných vlastníkov. Centrálna služba pre validáciu požaduje, aby každý subjekt poskytol rozsiahle [listinné dôkazy](#) o svojej vlastníckej štruktúre a osobitných právach, správe a riadení spoločnosti a o všetkých obchodných, finančných alebo iných väzbách, na základe ktorých získava kontrolu.
- 91** V troch projektoch financovaných EÚ v našej vzorke bol neskôr vylúčený aspoň jeden prijímateľ konzorcia, pretože sa považoval za subjekt vo vlastníctve alebo pod kontrolou z krajiny mimo EÚ. Vylúčenie členov konzorcia poukazuje na to, že všetci účastníci programu Digitálna Európa úplne nerozumejú pojmu vlastníctvo a kontrola EÚ. Celkovo na základe údajov centrálnej služby pre validáciu vyplýva, že 7 % všetkých žiadateľov o grant alebo subdodávateľov v oblasti kybernetickej bezpečnosti v rámci programu Digitálna Európa v období 2022 – 2025 nevyhovelo posúdeniu. Predloženie žiadostí neoprávnenými účastníkmi v rámci výzvy na predkladanie návrhov spôsobuje oneskorenia, ako je uvedené v [rámčeku 4](#).

Rámček 4

Príklad prípadu, keď boli prijímatelia vylúčení po tom, ako neprešli bezpečnostnými kontrolami

Dvaja členovia konzorcia projektu [NG-SOC](#) (projekt 7 v [prílohe III](#)) neprešli posúdením vlastníctva a kontroly. Výsledok bol oznámený približne mesiac pred konečným termínom na podpísanie dohody o grante. Koordinátor projektu musel súhlasiť s prevzatím práce, ktorá bola pridelená dvom vylúčeným členom, keďže nebol čas nájsť nového partnera. Jeden z vylúčených členov pôsobil v špecifickom odvetví, v ktorom sa malo vyvinúť pilotné riešenie. Značná časť projektu, ktorá sa týkala testovania riešení v praxi, preto nemohla pokračovať tak, ako sa plánovalo. Táto situácia sa neskôr napravila zmenou dohody o grante tak, aby zahŕňal nových členov.

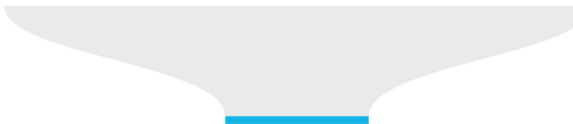
- 92** V rámci dvoch projektov, ktoré sme preskúmali (NCC-IE a CYberSynchrony), sa poskytuje finančná podpora tretím stranám. Tento mechanizmus financovania umožňuje prijímateľom grantov využívať časť grantu na financovanie iných subjektov prostredníctvom otvorených výziev. Finančná podpora tretím stranám môže uľahčiť prístup k finančným prostriedkom EÚ. V tomto prípade nesú prijímatelia výlučnú zodpovednosť za vykonanie posúdenia vlastníctva a kontroly a centrálna služba pre validáciu nie je doň zapojená.
- 93** V roku 2021 Komisia uverejnila všeobecné verejné usmernenia pre žiadateľov v prípade obmedzených výziev, ktoré boli aktualizované v roku 2026. Hoci je mechanizmus poskytovania finančnej podpory tretím stranám v prípade výziev programu Digitálna Európa zavedený od roku 2021, Komisia ani ECCC neposkytli prijímateľom podrobnú metodiku vykonávania posúdení vlastníctva a kontroly pri posudzovaní tretích strán, ktorým poskytujú finančnú podporu. V júli 2025 poskytlo ECCC nepovinné usmernenia, ktoré sieti národných koordinačných centier poskytli štruktúrovaný prístup k posúdeniam vlastníctva a kontroly. Toto usmernenie obsahuje všeobecné zásady a kroky, ktoré by sa mali prijať. V usmernení sa však nekonkretizuje, ako by sa mali kontroly vykonávať, pričom prijímatelia sú zodpovední za vypracovanie vlastného prístupu.
- 94** Zistili sme, že ECCC nepotvrdzuje metodiku prijatú prijímateľmi ani nevykonáva kontroly na základe vzorky s cieľom zabezpečiť, aby bola metodika dostatočne spoľahlivá a aby vybraní príjemcovia finančnej podpory boli skutočne vo vlastníctve a pod kontrolou EÚ.
- 95** Vo [výročnej správe za rok 2024](#) sme zistili, že od prijímateľov, ktorých Komisia poverila riadením finančnej podpory tretím stranám (v oblasti výskumu), sa nevyžadovalo, aby preukázali účinnosť svojich kontrol na zabezpečenie správnosti výdavkov EÚ. Podobne centrum ECCC neposudzuje administratívnu a technickú kapacitu prijímateľov na primerané riadenie posúdenia vlastníctva a kontroly. Ako sa podrobne uvádza v bode [90](#), toto posúdenie môže byť zložité a na úrovni EÚ ho vykonáva špecializovaný útvar so špecializovanými odbornými znalosťami.
- 96** V tejto súvislosti zastávame názor, že existuje značné riziko, že prijímatelia, ktorí sú zodpovední za vykonávanie kontrol posúdení vlastníctva a kontroly, ich nedokážu vykonávať primerane. Vzhľadom na povahu financovaných činností by tento nedostatok mohol odhaliť citlivú infraštruktúru, prevádzkové údaje a technológie kritické z hľadiska bezpečnosti.

Väčšina projektov financovaných EÚ nemá primerané výkonnostné rámce a údaje o výkonnosti programu Digitálna Európa týkajúce sa kybernetickej bezpečnosti nie sú presné

Väčšina projektov financovaných EÚ nemá primerané výkonnostné rámce

- 97** Prijímatelia, ktorí riadia projekty financované EÚ, musia ECCC podávať správy o ich pokroku a výsledkoch, používajúc na to míľniky, výstupy a ukazovatele, ako je uvedené na [ilustrácii 8](#). Posúdili sme, či míľniky a výstupy stanovené pre každý projekt primerane umožňujú monitorovať projekty. Posúdili sme tiež, či sú ich ukazovatele výkonnosti relevantné, merateľné a majú východiskovú a cieľovú hodnotu.

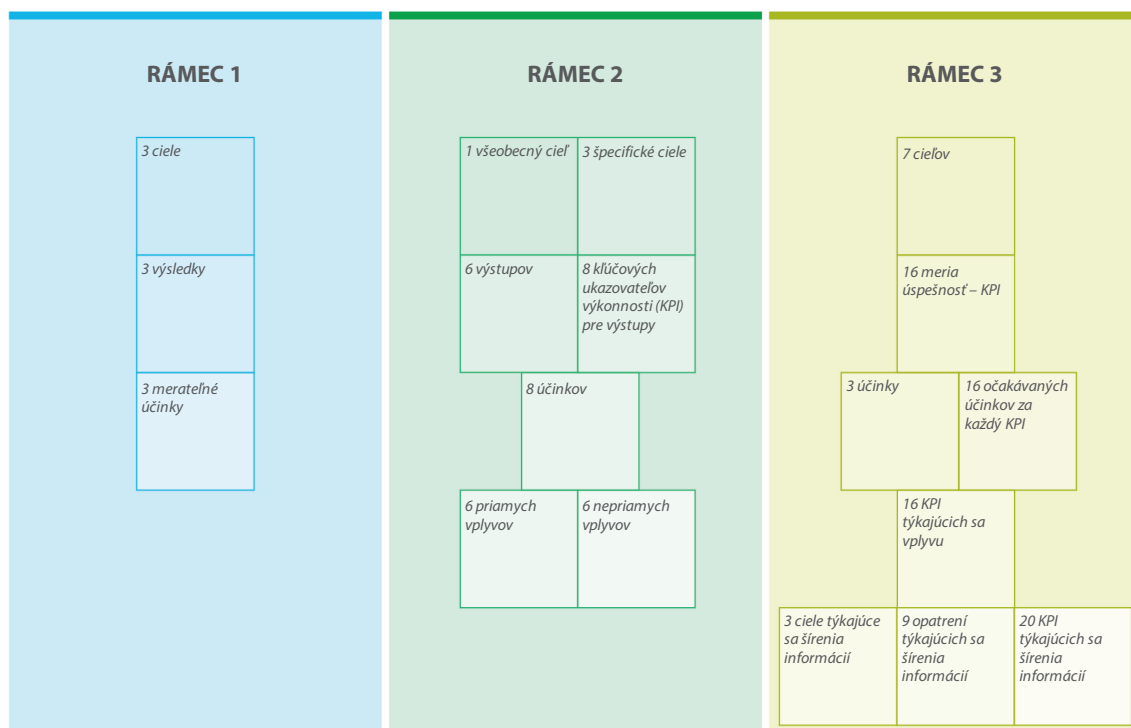
Ilustrácia 8 | Míľniky, výstupy a ukazovatele výkonnosti projektov programu Digitálna Európa

	 Míľniky	 Výstupy	 Ukazovatele výkonnosti
Čo sú	kontrolné body počas celého projektu, ktoré pomáhajú zmapovať pokrok	výstupy projektu predložené na preukázanie pokroku	používajú sa na meranie výstupov
Ako ich nastaviť	súvisia len s hlavnými výstupmi (obmedzené počtom)	len hlavné výstupy (10 až 15 max. na projekt)	konkrétne, merateľné, dosiahnuteľné, realistické a časovo ohrozené
Príklady	„spustenie pilotnej fázy platformy“	„príručka pre používateľov platformy“	„30 % skrátenie času reakcie na incidenty“
	 Štruktúrovaný prístup, súčasť online systému riadenia grantov		 Neštruktúrovaný prístup

Zdroj: EDA na základe [formulára žiadosti o grant](#).

- 98** Prijímatelia musia vo svojom návrhu projektu stanoviť súbor míľnikov a výstupov na základe štruktúrovaného prístupu uvedeného v pokynoch pre žiadateľov. Všetky míľniky a výstupy sú uvedené v online systéme riadenia grantov, aby sa uľahčila ich následná kontrola. Centrum ECCC zvyčajne preskúmava každý projekt dvakrát: raz v polovici trvania projektu a raz po jeho dokončení. Počas týchto preskúmaní externí odborníci overujú dosiahnutie míľnikov a výstupov a ECCC ich potvrdzuje. Míľniky a výstupy sú kľúčové pre monitorovanie projektov a mali by sa náležite stanoviť.
- 99** Zistili sme, že takmer ani jeden z projektov v našej vzorke sa neriadil pokynmi ohľadom počtu míľnikov a výstupov: počet míľnikov na projekt sa pohybuje od 8 do 39, zatiaľ čo počet výstupov od 8 do 45. Mnohé míľniky a výstupy nie sú v súlade s pokynmi, ako by sa mali vypracovať, a preto nie sú užitočné na sledovanie pokroku (napríklad „stretnutie s cieľom iniciovať vypracovanie výzvy na predkladanie návrhov v oblasti výskumu“ alebo „oficiálna zápisnica zo zasadnutia projektu“). V prípade troch projektov hodnotiaci výbor identifikoval tieto problémy pred podpísaním grantu. V dvoch prípadoch prijímatelia navrhli len menšie zmeny (napr. konečné termíny) bez toho, aby sa zaoberali hlavnými otázkami, zatiaľ čo v treťom prípade sa nevykonali žiadne zmeny. V prípade šiestich ďalších projektov v našej vzorke z našej analýzy vyplýva, že míľniky alebo výstupy nie sú v súlade s pokynmi a nie sú vždy primerané. Zastávame názor, že zle vymedzené výstupy či míľniky, alebo ak ich je príliš veľa, sťažujú sledovanie pokroku.
- 100** Na rozdiel od míľnikov a výstupov sa ukazovatele výkonnosti neriadia štruktúrovaným prístupom a nie sú konsolidované v tabuľke v systéme riadenia grantov. Namiesto toho ich možno nájsť v rôznych oddieloch návrhu. Tento prístup viedol k tomu, že prijímatelia navrhli množstvo výkonnostných rámcov. Zatiaľ čo niektorí stanovili len ciele projektu spojené s ukazovateľmi výkonnosti, iní vytvorili oveľa zložitejšie výkonnostné rámce. Niektoré príklady uvádzame na [ilustrácii 9](#).

Ilustrácia 9 | Príklad rôznych výkonnostných rámcov navrhnutých pre projekty



Zdroj: EDA.

101 Z našej analýzy vyplýva, že mnohé ukazovatele výkonnosti, ktoré sa používajú pri projektoch, nie sú relevantné alebo merateľné a chýba im cieľová alebo východisková hodnota (pozri [rámček 5](#)). Okrem toho sa v rámci siedmich projektov vymedzilo 20 alebo viac ukazovateľov, pričom jeden projekt mal 52 ukazovateľov. Výsledok nášho posúdenia uvádzame v [prílohe IV](#).

Rámček 5

Príklady neprimeraných ukazovateľov výkonnosti

Nemerateľné:

- „Ukazovateľ narušenia a iných poskytovaných služieb posilňuje kapacity MSP v oblasti kybernetickej bezpečnosti“
- „Dodanie nástrojov a metód reakcie na incidenty, ktoré umožňujú integráciu s komunikačnými kanálmi siete EU-CyCLONe“

Bez východiskovej alebo cieľovej hodnoty:

- „≥ 20 % zlepšenie pripravenosti zamestnancov“
- „≥ 20 % zníženie úsilia potrebného na zosúladenie s príslušnými iniciatívami EÚ v oblasti kybernetickej bezpečnosti a ich dodržiavanie“

Nesúvisiace s výkonnosťou:

- „Záverečná správa o projekte na konci fázy financovania“
- „Počet účastníkov odbornej prípravy, ktorí sa zúčastnia na všetkých školeniach“

Zdroj: EDA na základe projektovej dokumentácie.

102 Celkovo zastávame názor, že široká škála výkonnostných rámcov, nedostatočné nastavenie ukazovateľov a ich nadmerný počet výrazne komplikujú monitorovanie výkonnosti. Preto nie je možné náležite posúdiť výkonnosť projektov. Komplikuje to aj skutočnosť, že vzor na podávanie správ neobsahuje osobitný oddiel o ukazovateľoch výkonnosti projektov, v dôsledku čoho neboli vykázané vo väčšine projektov v našej vzorke.

Údaje o výkonnosti kybernetickobezpečnostnej zložky programu Digitálna Európa nie sú presné

- 103** Na monitorovanie výsledkov projektov programu Digitálna Európa sa v nariadení stanovujú programové ukazovatele, ktoré sa musia vykazovať za všetky projekty, ako sa podrobne uvádza v [rámčeku 6](#).

Rámček 6

Ukazovatele kybernetickej bezpečnosti programu Digitálna Európa

1. a) Počet infraštruktúr alebo nástrojov kybernetickej bezpečnosti alebo oboje, získaných prostredníctvom spoločného verejného obstarávania, a to aj v kontexte európskeho systému varovania pred kybernetickobezpečnostnými hrozbami
1. b) Počet infraštruktúr alebo nástrojov kybernetickej bezpečnosti alebo oboje, získaných prostredníctvom spoločného verejného obstarávania
2. Počet používateľov a používateľských komunít s prístupom k európskym zariadeniam kybernetickej bezpečnosti.
3. Počet akcií, ktorými sa podporuje pripravenosť na kybernetické bezpečnostné incidenty a reakcia na ne v rámci mechanizmu na riešenie kybernetickobezpečnostných núdzových situácií.

Zdroj: Príloha II k [nariadeniu \(EÚ\) 2021/694](#), ktorým sa zriaďuje program Digitálna Európa; rámec monitorovania a hodnotenia programu Digitálna Európa [[SWD\(2024\) 37](#)].

- 104** Posúdili sme, či sa v rámci projektov v našej vzorke vykazovali tieto ukazovatele, a preskúmali sme, ako ECCC zbiera a overuje tieto údaje.
- 105** Pri všetkých projektoch sa vyžaduje, aby sa vykazovali ukazovatele programu Digitálna Európa pred ich strednodobým a záverečným preskúmaním v systéme riadenia grantov. Zistili sme, že zo siedmich projektov, ktoré boli v polovici trvania počas nášho auditu a za ktoré preto mali byť vykázané tieto ukazovatele, boli vykázané len za tri projekty. Z týchto troch projektov za dva projekty neboli vykázané presné informácie: za jeden projekt sa vykázal nesprávny ukazovateľ, za druhý sa poskytli cieľové hodnoty namiesto dosiahnutých výsledkov.

106 Komisia každý rok informuje o týchto ukazovateľoch vo svojich [vyhláseniach o výkonnosti programov](#). To umožňuje zainteresovaným stranám posúdiť, či program plní svoje ciele. Podľa vyhlásení o výkonnosti programu za rok 2024 sú ukazovatele kybernetickej bezpečnosti programu Digitálna Európa na dobrej ceste. ECCC nám vysvetlilo, že na zostavenie týchto ukazovateľov použilo rad prieskumov zaslaných prijímateľom projektov namiesto toho, aby ich založilo na systéme riadenia grantov. Preskúmali sme rozčlenené údaje, ktoré nám poskytlo ECCC, a zistili sme mnohé problémy v spôsobe zberu údajov a ich celkovej kvalite. Zistili sme, že zozbierané údaje nezodpovedajú hodnotám uvedeným vo vyhlásení o výkonnosti programu, takže nie je jasné, ako boli vykázané hodnoty vypočítané. Nenašli sme žiadne dôkazy o tom, že by ECCC overovalo presnosť vykázaných údajov. Na základe kontrol projektov v našej vzorke zastávame názor, že vykázané údaje náležite neodrážajú dosiahnuté výsledky, keďže väčšina hodnôt chýba alebo je nepresná.

Túto správu prijala komora III, ktorej predsedá George Marius Hyzler, člen Dvora audítorov, v Luxemburgu na svojom zasadnutí dňa 16. júna 2026.

Za Dvor audítorov

Tony Murphy
predseda

Prílohy

Príloha I – O tomto audite

- 01** Kybernetická bezpečnosť sa vymedzuje ako „činnosti potrebné na ochranu sietí a informačných systémov, užívateľov takýchto systémov a iných osôb dotknutých kybernetickými hrozbami“¹. Kybernetická hrozba je „každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, používateľov takýchto systémov a iné osoby“². Kybernetická bezpečnosť si vyžaduje holistický prístup pozostávajúci zo série vzájomne súvisiacich činností na predchádzanie kybernetickým hrozbám, ich odhaľovanie, reakciu na ne a zotavenie sa z nich, ako je znázornené na *ilustrácii 1*.

¹ Nariadenie (EÚ) 2019/881 (akt o kybernetickej bezpečnosti).

² Článok 2 aktu o kybernetickej bezpečnosti.

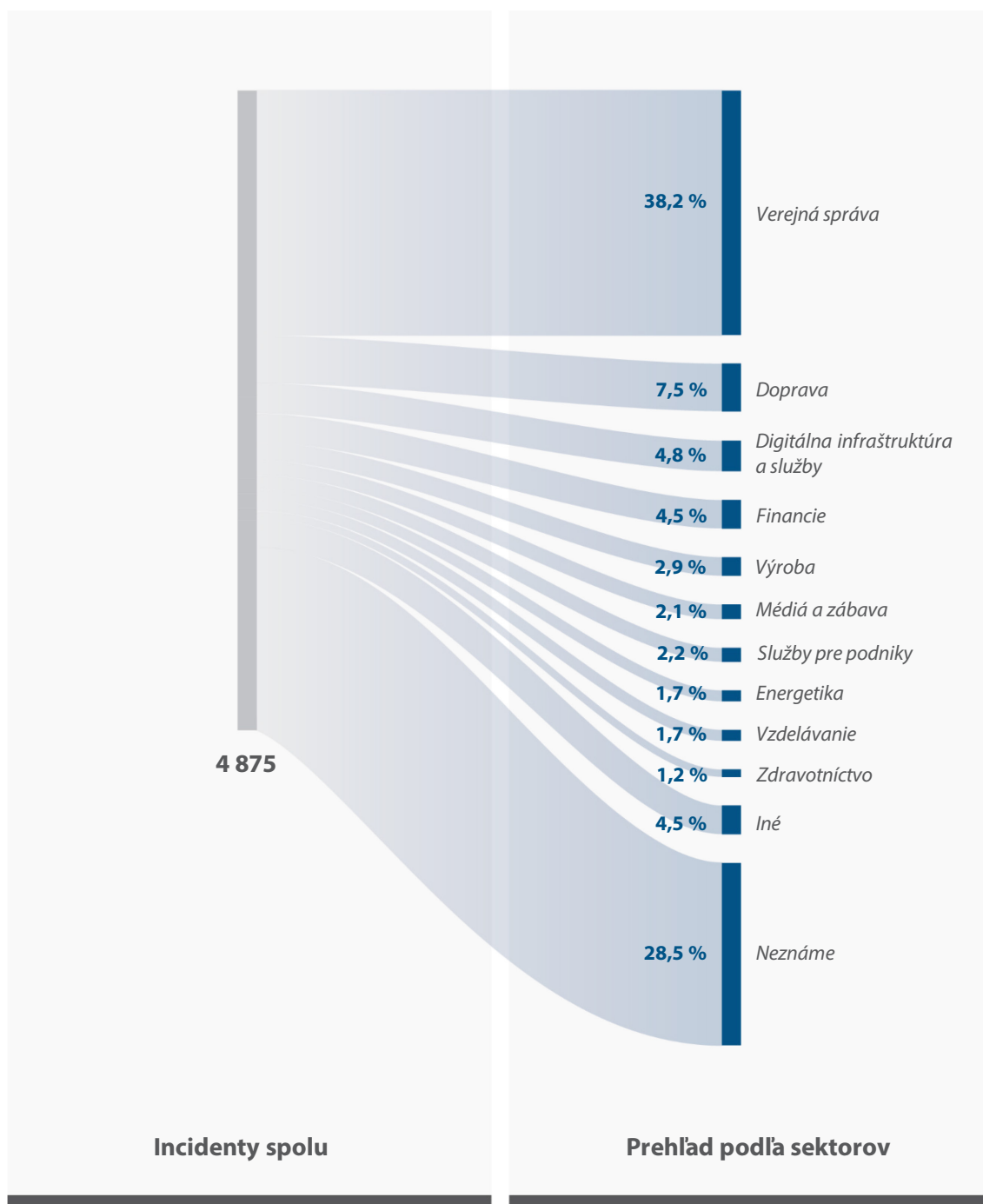
Ilustrácia 1 | Príklady kybernetických činností

Prevencia 	Zníženie rizika kybernetických bezpečnostných incidentov a minimalizácia ich potenciálnych účinkov <i>Príklady: antivírus, firewally, šifrovanie, dvojstupňová autentifikácia, riadenie aktualizácií softvéru, odborná príprava zamestnancov v oblasti informovanosti o bezpečnosti</i>
Odhaľovanie 	Odhaľovanie škodlivej činnosti <i>Príklady: monitorovanie siete, situačná informovanosť</i>
Reakcia 	Riadenie a zmierňovanie kybernetickobezpečnostného incidentu obmedzením hrozby a predchádzaním ďalším škodám <i>Príklady: odstránenie hrozby, zamedzenie šírenia izolovaním serverov, deaktivácia kompromitovaných účtov a resetovanie hesiel</i>
Obnova 	Obnovenie bezpečného a funkčného stavu ovplyvnených systémov, údajov a služieb <i>Príklady: opätovná inštalácia operačných systémov na ovplyvnených serveroch, obnova údajov zo záloh, vyvodenie získaných ponaučení, aktualizácia politík</i>

Zdroj: EDA na základe odôvodnenia 78 smernice (EÚ) 2022/2555 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (smernica NIS 2).

02 Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA) považuje úroveň kybernetických hrozieb za významnú, pričom poznamenáva, že situácia v súvislosti s kybernetickými hrozbami sa stala a naďalej je výrazne zložitejšia³. Tieto hrozby poukazujú na zásadný význam kybernetickej bezpečnosti v čoraz digitálnejších hospodárstvach a spoločnostiach. Agentúra ENISA vo svojej [správe o panoráme hrozieb](#) z roku 2025 označila ransomvér za najkritickejšiu hrozbu v EÚ. Na [ilustrácii 2](#) sú uvedené cieľové sektory.

³ Správa agentúry ENISA o stave kybernetickej bezpečnosti v Únii za rok 2024.

Ilustrácia 2 | Sektory, na ktoré sú zamerané kybernetické útoky

Zdroj: EDA na základe agentúry [ENISA](#).

Významné a rozsiahle kybernetické bezpečnostné incidenty

03 Kybernetické bezpečnostné incidenty, ktoré zahŕňajú kybernetické hrozby a neúmyselné udalosti (napríklad tie, ktoré sú uvedené na [ilustrácii 3](#) a v bode [40](#)), „môžu zabraňovať poskytovaniu verejných služieb [a] realizácii hospodárskych činností, ... spôsobovať značné finančné straty, narúšať dôveru používateľa, spôsobovať značné škody na hospodárstve a na demokratických systémoch Únie a dokonca by mohli mať zdravie alebo život ohrozujúce dôsledky“⁴. Kybernetický bezpečnostný incident sa považuje za⁵:

- **významný**, ak spôsobil alebo má schopnosť spôsobiť dotknutému subjektu závažné prevádzkové narušenie služieb alebo finančnú stratu, alebo ak zasiahol alebo má schopnosť zasiahnuť iné fyzické alebo právnické osoby tým, že im spôsobí značnú majetkovú alebo nemajetkovú ujmu,
- **rozsiahly**, ak spôsobil narušenie na úrovni presahujúcej schopnosť členského štátu naň reagovať alebo ktorý má významný vplyv aspoň na dva členské štáty.

04 Rozsiahly kybernetický bezpečnostný incident sa môže vystupňovať a naplno prepuknúť v **kybernetickú krízu EÚ**, ak znemožňuje riadne fungovanie vnútorného trhu alebo predstavuje vážne riziká pre verejnú bezpečnosť a ochranu subjektov alebo občanov v niekoľkých členských štátoch alebo v EÚ ako celku⁶.

⁴ Odôvodnenie 2 nariadenia (EÚ) 2025/38 (akt o kybernetickej solidarite).

⁵ Článok 6 a článok 23 [smernice NIS 2](#), ktoré sú bližšie špecifikované vo [vykonávacom nariadení Komisie \(EÚ\) 2024/2690](#) pre viacerých poskytovateľov v odvetví digitálnej infraštruktúry.

⁶ Odôvodnenie 69 [smernice NIS 2](#).

Rámec politiky EÚ

- 05** Ekosystém kybernetickej bezpečnosti v EÚ je komplexný a mnohohrstevný, dotýka sa množstva oblastí vnútornej politiky, ako sú politiky v oblasti spravodlivosti a vnútorných vecí, digitálneho jednotného trhu a výskumu⁷. V prípade vonkajšej politiky zohráva kybernetická bezpečnosť úlohu v diplomacii a čoraz viac sa stáva súčasťou vznikajúcej obrannej politiky EÚ⁸.
- 06** EÚ za posledné roky posilnila svoj regulačný rámec kybernetickej bezpečnosti. Na *ilustrácii 3* sú uvedené najrelevantnejšie právne predpisy a politické nástroje na úrovni EÚ. V súlade s rozsahom nášho auditu (pozri body **13** – **14**) sme sa zamerali na nástroje, ktoré sa zaoberajú odhaľovaním významných a rozsiahlych kybernetických bezpečnostných incidentov a reakciou na ne.

⁷ Informačný dokument EDA o prekážkach účinnej politiky EÚ v oblasti kybernetickej bezpečnosti, s. 12.

⁸ Napríklad *postoj Európskej únie ku kybernetickej bezpečnosti* (2022), *rámec pre koordinovanú reakciu EÚ na hybridné kampane* (2022), *politika EÚ v oblasti kybernetickej obrany* (2023) a *revidovaný súbor nástrojov kybernetickej diplomacie* (2023).

Ilustrácia 3 | Príslušné právne predpisy a politické nástroje EÚ

- Prijatie právnych predpisov a politických nástrojov
- Vytvorenie sietí a štruktúr



Zdroj: EDA.

Úlohy a zodpovednosti

- 07** Prostredie kybernetickej bezpečnosti EÚ zahŕňa množstvo súkromných a verejných aktérov na regionálnej, národnej a európskej úrovni v civilnej oblasti vrátane orgánov presadzovania práva. Kybernetická bezpečnosť je tiež kľúčovým prvkom národnej bezpečnosti a obrany⁹. Súčasná situácia v EÚ je znázornená v [prílohe II](#).
- 08** Členské štáty nesú primárnu zodpovednosť za predchádzanie kybernetickým bezpečnostným incidentom a krízam, ktoré ich postihujú, za prípravu a reakciu na ne. Podľa [článku 4 ods. 2 Zmluvy o Európskej únii](#) národná bezpečnosť zostáva vo výlučnej zodpovednosti každého členského štátu. Keďže kybernetické bezpečnostné incidenty môžu narušiť a poškodiť kritickú informačnú infraštruktúru, od ktorej závisí hladké fungovanie vnútorného trhu, aj EÚ zohráva dôležitú úlohu v prípade významného incidentu alebo krízy¹⁰. Hlavné subjekty na úrovni EÚ sú uvedené na [ilustrácii 4](#).

⁹ Stanovisko 02/2023 k navrhovanému aktu o kybernetickej solidarite.

¹⁰ Koncepcia EÚ pre riadenie kybernetickobezpečnostných kríz.

Ilustrácia 4 | Subjekty na úrovni EÚ s kľúčovou úlohou v oblasti kybernetickej bezpečnosti



Zdroj: EDA.

Financovanie zo strany EÚ

- 09** V súčasnom viacročnom finančnom rámci na roky 2021 – 2027 je hlavným zdrojom financovania kybernetickej bezpečnosti [program Digitálna Európa \(DIGITAL\)](#). Tento program sa začal v roku 2021 a je prvým programom EÚ, ktorý sa osobitne zameriava na podporu digitálnej transformácie EÚ. Jeho celkový rozpočet je 8,1 mld. EUR¹¹.
- 10** Z programu Digitálna Európa sa financujú opatrenia v oblasti kybernetickej bezpečnosti v rámci špecifického cieľa 3 – „Kybernetická bezpečnosť a dôvera“. Presnejšie povedané, rozpočet vo výške 1,4 mld. EUR je určený na:
- posilnenie koordinácie kybernetickej bezpečnosti medzi nástrojmi a dátovou infraštruktúrou členských štátov,
 - podporu plošného zavádzania kybernetickobezpečnostných riešení v celom hospodárstve.
- 11** Väčšina finančných prostriedkov programu Digitálna Európa na kybernetickú bezpečnosť sa poskytuje prostredníctvom výziev na predkladanie návrhov, pričom od novembra 2021 do decembra 2025 bolo vyhlásených 12 výziev. Dostupné financovanie týchto výziev zo strany EÚ bolo vo výške 825 mil. EUR. Na roky 2026 a 2027 sú naplánované nové výzvy na poskytnutie ďalších 212 mil. EUR vo forme grantov.
- 12** Ďalším významným programom EÚ na podporu kybernetickej bezpečnosti je program [Horizont Európa](#). Projekty v oblasti kybernetickej bezpečnosti sú financované najmä v rámci [klastra 3](#) „Civilná bezpečnosť pre spoločnosť“ a zvyčajne sú v počiatočnom štádiu z dôvodu zamerania programu Horizont Európa na výskum a inovácie. Z [Mechanizmu na podporu obnovy a odolnosti](#) sa tiež poskytujú finančné prostriedky na opatrenia v oblasti kybernetickej bezpečnosti.

¹¹ [Program Digitálna Európa](#).

Rozsah auditu a audítorský prístup

13 Nárast kybernetických hrozieb a ich potenciálny vplyv zdôraznili potrebu posilniť našu kolektívnu kybernetickú odolnosť. Cieľom nášho auditu bolo posúdiť, či opatrenia EÚ pomáhajú pri odhaľovaní významných a rozsiahlych kybernetických bezpečnostných incidentov a reakcii na ne. Konkrétne sme posúdili, či tomu tak bolo v prípade:

- siete a mechanizmov na úrovni EÚ (konkrétne sieť jednotiek CSIRT, sieť EU-CyCLONe, Európsky systém varovania pred kybernetickobezpečnostnými hrozbami, kybernetické situačné centrum a rezerva EÚ na účely kybernetickej bezpečnosti),
- opatrení financovaných v rámci programu Digitálna Európa.

Audit sa nevzťahoval na spoluprácu v oblasti presadzovania práva na úrovni EÚ ani opatrení na odrádzanie od kybernetických útokov prijatých na úrovni EÚ prostredníctvom diplomatických opatrení alebo obranných činností.

14 Audit sa týkal obdobia od roku 2022 do roku 2025. Vychádza z administratívnej kontroly a analýzy príslušných dokumentov, audítorských návštev v troch členských štátoch, Írsku, Grécku a Taliansku a písomných dotazníkov a rozhovorov s príslušnými zainteresovanými stranami. Na [ilustrácii 5](#) je zobrazené, ako sme získali dôkazy pre naše pripomienky.

Ilustrácia 5 | Vykonané audítorské činnosti

Preskúmali sme

- **právny rámec** uplatniteľný na odhaľovanie významných a rozsiahlych kybernetických incidentov a reakciu na ne,
- **úlohy a povinnosti** sietí a štruktúr zriadených na úrovni EÚ

Analyzovali sme

- dokumenty o fungovaní **siete jednotiek CSIRT** a **siete EU-CyCLONE**,
 - dokumentáciu k **plánovaniu a rámcu monitorovania výkonnosti programu Digitálna Európa**,
 - dokumentáciu o **13 vybraných opatreniach financovaných EÚ** (11 grantov a 2 zmluvy – pozri podrobný zoznam v prílohe III).
- * Vybrali sme opatrenia financované EÚ v troch krajinách (Írsko, Grécko a Taliansko), v ktorých bolo príslušné financovanie z programu Digitálna Európa významnejšie. Týchto 11 grantov sa čerpalo zo zoznamu 137 projektov financovaných EÚ, ktoré sú relevantné pre odhaľovanie hrozieb a reakciu na ne, s cieľom pokryť rôznorodú kombináciu projektov.

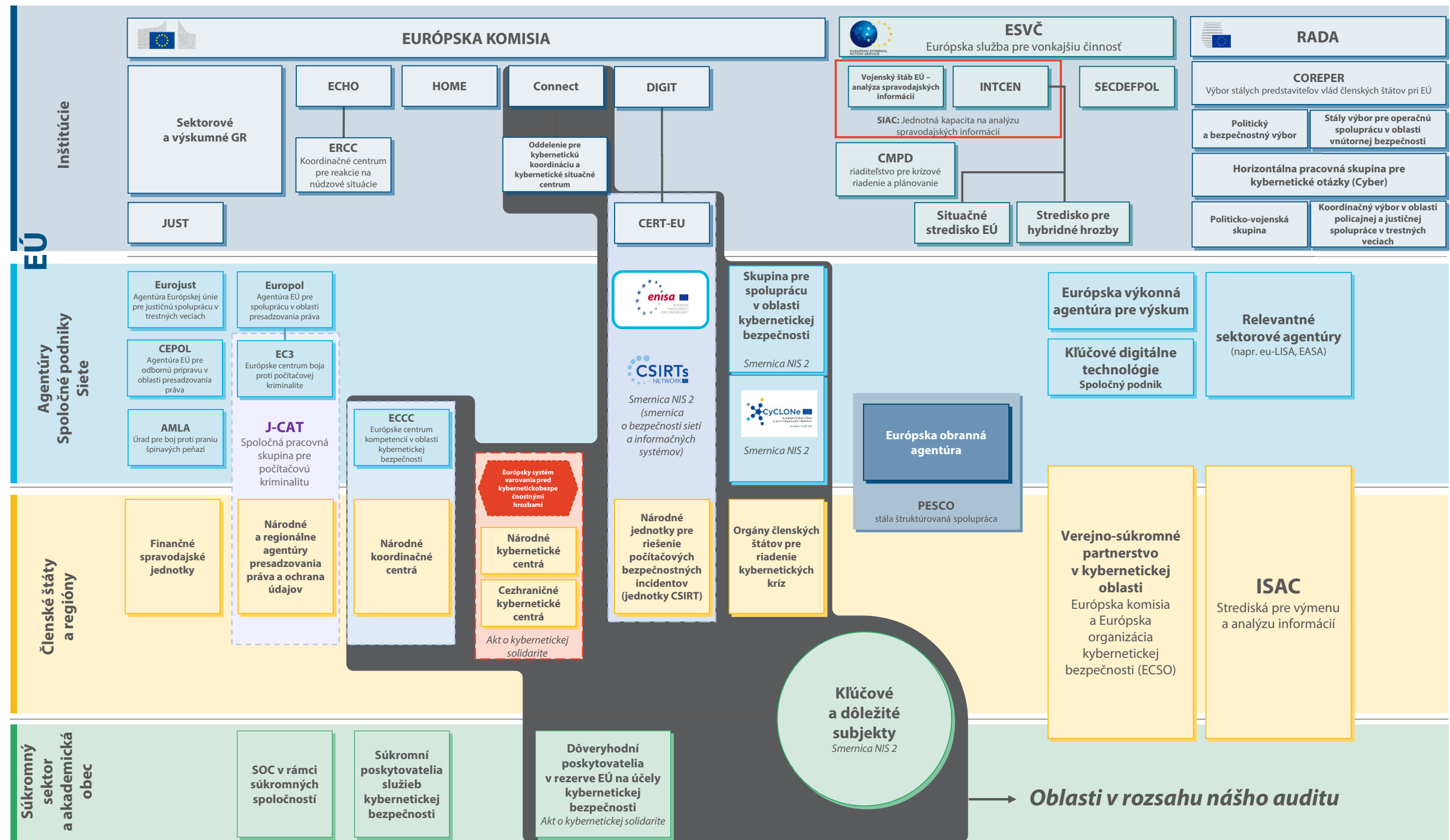
Uskutočnili sme rozhovory

- s prijímateľmi **11 grantov financovaných EÚ vybraných do vzorky**,
- zástupcami vnútroštátnych orgánov pre kybernetickú bezpečnosť v **troch členských štátoch** (Írsko, Grécko a Taliansko),
- zástupcami Európskej komisie (**GR Connect**), agentúry **ENISA** a centra **ECCC**.

Zdroj: EDA.

- 15** Očakávame, že naše zistenia prispejú k zlepšeniu účinnosti a efektívnosti odhaľovania významných a rozsiahlych kybernetických bezpečnostných incidentov a reakcie EÚ na ne, ako aj k zlepšeniu spôsobu výberu a monitorovania opatrení financovaných EÚ. Naša [metodika auditu](#) je v súlade s medzinárodnými audítorskými štandardmi vydanými Medzinárodnou organizáciou najvyšších kontrolných inštitúcií (INTOSAI).

Príloha II – Prostredie kybernetickej bezpečnosti v EÚ



GR CONNECT: Generálne riaditeľstvo pre komunikačné siete, obsah a technológie
GR ECHO: Generálne riaditeľstvo pre civilnú ochranu a operácie humanitárnej pomoci EÚ

GR HOME: GR pre migráciu a vnútorné záležitosti
GR JUST: GR pre spravodlivosť a spotrebiteľov
DIGIT: Generálne riaditeľstvo pre digitálne služby
EASA: Agentúra Európskej únie pre bezpečnosť letectva

EU-CyCLONE: Európska sieť styčných organizácií pre kybernetické krízy
eu-LISA: Agentúra Európskej únie na prevádzkové riadenie rozsiahlych informačných systémov v priestore slobody, bezpečnosti a spravodlivosti
INTCEN: Spravodajské a situačné centrum Európskej únie

SECDEFPOL: bezpečnostná a obranná politika
SOC: Centrum bezpečnostných operácií

Príloha III – Vybrané opatrenia v oblasti kybernetickej bezpečnosti

ID	Názov	Krajiny	Dátum začiatku	Dátum ukončenia	Celkové náklady (v mil. EUR) a príspevok EÚ (v %)	Odkaz na portál EÚ pre financovanie a ponuky
Granty pre cezhraničné kybernetické centrá, ktoré sú súčasťou európskeho systému varovania pred kybernetickobezpečnostnými hrozbami						
1	Zriadenie cezhraničných centier bezpečnostných operácií (ATHENA)	Bulharsko, Grécko, Cyprus, Malta	1. 1. 2024	31. 3. 2028	4,7 (50 %)	
2	CEZHRANIČNÁ PLATFORMA ENSOC (ENSOC)	Španielsko, Taliansko, Luxembursko, Holandsko, Rakúsko, Portugalsko, Rumunsko	1. 1. 2024	30. 6. 2028	10,4 (50 %)	
Granty na zavedenie siete národných koordinačných centier (NKC) v členských štátoch						
3	Rozvoj a vykonávanie Národného centra pre koordináciu a rozvoj kybernetickej bezpečnosti pre Írsko (NCC-IE)	Írsko	2. 10. 2023	1. 10. 2026	4,2 (47 %)	
4	Talianske národné koordinačné centrum (NCC-IT)	Taliansko	1. 11. 2023	31. 10. 2025	2,0 (50 %)	

ID	Názov	Krajiny	Dátum začiatku	Dátum ukončenia	Celkové náklady (v mil. EUR) a príspevok EÚ (v %)	Odkaz na portál EÚ pre financovanie a ponuky
Granty na budovanie kapacít centier bezpečnostných operácií, podporu nových aplikácií umelej inteligencie a iných podporných technológií pre centrá bezpečnostných operácií a poskytovanie podpory pripravenosti a vzájomnej pomoci						
5	Posilnenie kapacity gréckeho konsolidovaného centra bezpečnostných operácií (EL-SOC)	Grécko, Cyprus	1. 1. 2024	31. 12. 2026	9,7 (50 %)	
6	Grécke centrum bezpečnostných operácií pre malé a stredné podniky (GR-SME-SOC)	Grécko	1. 1. 2024	31. 12. 2026	12,1 (50 %)	
7	Centrá bezpečnostných operácií novej generácie (NG-SOC)	Grécko, Španielsko, Cyprus, Luxembursko, Slovinsko, Nórsko	1. 1. 2024	31. 12. 2026	4,8 (50 %)	
8	Írske centrum bezpečnostných operácií miestnej samosprávy (ILG-SOC)	Írsko	1. 10. 2023	30. 9. 2026	8,3 (50 %)	
9	Prepojený ekosystém sietí pre koordináciu kybernetickej bezpečnosti a reakcie (kybernetická sieť CORE)	Írsko	1. 1. 2024	31. 12. 2026	3,6 (50 %)	
10	Harmonizácia ľudí, procesov a technológií pre spoľahlivú kybernetickú bezpečnosť (CYberSynchrony)	Belgicko, Grécko, Taliansko, Cyprus, Holandsko	1. 6. 2024	31. 5. 2027	7,0 (100 %)	
11	Pokročilé kooperatívne centrá bezpečnostných operácií (ACSOC)	Grécko, Taliansko, Rumunsko	1. 1. 2025	31. 12. 2027	3,0 (50 %)	

ID	Názov	Krajiny	Dátum začiatku	Dátum ukončenia	Celkové náklady (v mil. EUR) a príspevok EÚ (v %)	Odkaz na portál EÚ pre financovanie a ponuky
Rámcová zmluva na akciu agentúry ENISA na podporu kybernetickej bezpečnosti						
12	Podpora agentúry ENISA pri poskytovaní služieb v rámci opatrenia na podporu kybernetickej bezpečnosti (28 častí)	27 častí pre členské štáty 1 celoeurópska časť	1. 12. 2022 ¹	31. 12. 2025	28,3 (100 %)	
Zmluva o poskytovaní služieb pre kybernetické situačné centrum GR Connect						
13	Individualizovaná služba na podporu Centra pre kybernetickú situáciu a analýzu pre Európsku komisiu	-	30. 12. 2022	30. 12. 2026	18,0 (100 %)	

Zdroj: EDA.

¹ Viacero zmlúv podpísaných v priebehu decembra 2022.

Príloha IV – Posúdenie projektov v oblasti kybernetickej bezpečnosti financovaných EÚ zo strany Európskeho dvora audítorov

		Projekt rieši väčšinu potrieb identifikovaných vo výzve	Projekt doteraz dosiahol plánované výstupy a výsledky	Výstupy projektu boli dodané v stanovenom termíne	Ukazovatele výkonnosti projektu sú relevantné, merateľné a majú východiskovú a cieľovú hodnotu
		Uspokojivé	Určité nedostatky	Neuspokojivé	Nie je možné dospieť k záveru (príliš skoro)
ID	Projekt				
1	Zriadenie cezhraničných centier bezpečnostných operácií (ATHENA)				
2	CEZHRANIČNÁ PLATFORMA ENSOC (ENSOC)				
3	Rozvoj a vykonávanie Národného centra pre koordináciu a rozvoj kybernetickej bezpečnosti pre Írsko (NCC-IE)				
4	Talianske národné koordinačné centrum (NCC-IT)				
5	Posilnenie kapacity gréckeho konsolidovaného centra bezpečnostných operácií (EL-SOC)				
6	Grécke centrum bezpečnostných operácií pre malé a stredné podniky (GR-SME-SOC)				
7	Centrá bezpečnostných operácií novej generácie (NG-SOC)				
8	Írske centrum bezpečnostných operácií miestnej samosprávy (ILG-SOC)				
9	Prepojený ekosystém sietí pre koordináciu kybernetickej bezpečnosti a reakcie (sieť Cyber-CORE)				
10	Harmonizácia ľudí, procesov a technológií pre spoľahlivú kybernetickú bezpečnosť (CYberSynchrony)				
11	Pokročilé kooperatívne centrá bezpečnostných operácií (ACSOC)				

Skratky

Skratka	Definícia/vysvetlenie
CSIRT	Jednotka pre riešenie počítačových bezpečnostných incidentov
DIGITAL	Program Digitálna Európa
ECCC	Európske centrum kompetencií v oblasti kybernetickej bezpečnosti
ENISA	Agentúra Európskej únie pre kybernetickú bezpečnosť
EU-CyCLONe	Európska sieť styčných organizácií pre kybernetické krízy
FSTP	Finančná podpora pre tretie strany
GR CONNECT	Generálne riaditeľstvo pre komunikačné siete, obsah a technológie
MSP	Malé a stredné podniky
NIS	Bezpečnosť sietí a informačných systémov
NKC	Národné koordinačné centrum
PVK	Posúdenie vlastníctva a kontroly
SAG	Strategická poradná skupina
SOC	Centrum bezpečnostných operácií

Glosár

Termín	Definícia/vysvetlenie
Aktér hrozby	Jednotlivec alebo skupina, ktorá úmyselne spôsobí ujmu, naruší služby alebo ukradne údaje využitím zraniteľných miest v IT systémoch, sieťach a zariadeniach.
Centrum bezpečnostných operácií	Organizačná jednotka, ktorej úlohou je predchádzať kybernetickým hrozbám a incidentom a zhromažďovať súvisiace spravodajské informácie.
Kybernetická hrozba	Možné využitie kybernetického priestoru na oslabenie dostupnosti, pravosti, integrity alebo dôvernosti údajov či informačných systémov.
Kybernetické centrum	Centrálna platforma spájajúca rôzne služby, nástroje a odborníkov v oblasti IT s cieľom zlepšiť monitorovanie, odhaľovanie a analýzu kybernetických hrozieb, predchádzať kybernetickým bezpečnostným incidentom a podporovať tvorbu spravodajských informácií o kybernetických hrozbách.
Kybernetický bezpečnostný incident	Udalosť oslabujúca dostupnosť, pravosť, integritu alebo dôvernú povahu údajov či informačných systémov.
Ransomvér	Malvér, ktorý obetiam bráni v prístupe do počítačového systému alebo znemožňuje čitateľnosť súborov ich šifrovaním, čo obeť zvyčajne núti k tomu, aby na obnovenie prístupu zaplatila výkupné.
Rozsiahly kybernetický bezpečnostný incident	Kybernetický bezpečnostný incident, ktorý je pre členský štát natoľko rušivý, že ho nemôže riešiť sám, alebo má významný dosah najmenej vo dvoch členských štátoch.
Taxonómia	V kontexte kybernetickej bezpečnosti klasifikačný systém používaný na organizáciu, kategorizáciu a štruktúrovanie poznatkov o kľúčových koncepciách, ako sú hrozby a incidenty.
Významný kybernetický bezpečnostný incident	Kybernetický bezpečnostný incident, ktorý spôsobil alebo môže spôsobiť vážne narušenie činnosti organizácie alebo finančnú stratu alebo značné škody iným subjektom alebo osobám.

Odpovede Komisie

<https://www.eca.europa.eu/sk/publications/SR-2026-19>

Odpovede Európskeho centra kompetencií v oblasti kybernetickej bezpečnosti (ECCC)

<https://www.eca.europa.eu/sk/publications/SR-2026-19>

Odpovede Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA)

<https://www.eca.europa.eu/sk/publications/SR-2026-19>

Harmonogram

<https://www.eca.europa.eu/sk/publications/SR-2026-19>

Audítorský tím

V osobitných správach EDA sa predkladajú výsledky jeho auditov, ktoré sa týkajú politik a programov EÚ alebo tém súvisiacich s riadením z konkrétnych rozpočtových oblastí. EDA vyberá a navrhuje tieto audítorské úlohy tak, aby mali maximálny vplyv, pričom sa zohľadňujú riziká z hľadiska výkonnosti či zhody, výška súvisiacich príjmov alebo výdavkov, budúci vývoj a politický a verejný záujem.

Tento audit výkonnosti uskutočnila audítorská komora III – Vonkajšia činnosť, bezpečnosť a spravodlivosť, ktorej predsedá člen EDA George-Marius Hyzler. Audit viedol člen EDA George-Marius Hyzler, podporu mu poskytli vedúci kabinetu Romuald Kayibanda a ataše kabinetu Annette Farrugia, hlavný manažér Cyril Messein, vedúci úlohy Frédéric Soblet a audítori Jurgen Manjé a Flavia Di Marco. Jazykovú podporu poskytla Zoe Amador Martínez. Dunja Weibel poskytla grafickú podporu.



Zľava doprava: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

AUTORSKÉ PRÁVA

© Európska únia, 2026

Politika týkajúca sa opakovaného použitia materiálov Európskeho dvora audítorov (EDA) je stanovená v [rozhodnutí EDA č. 6/2019](#) o politike otvoreného prístupu a opakovanom použití dokumentov.

Pokiaľ sa nestanovuje inak (napr. v osobitnom upozornení o autorských právach), obsah materiálov EDA vo vlastníctve EÚ podlieha licencií [Creative Commons Attribution 4.0 International \(CC BY 4.0\)](#). Vo všeobecnosti je preto opakované použitie povolené pod podmienkou, že sa náležite uvedie zdroj a označia prípadné zmeny. Tí, ktorí používajú obsah EDA, nesmú skresliť pôvodný význam alebo odkaz. EDA nenesie zodpovednosť za žiadne dôsledky použitia takéhoto obsahu.

V prípade, že konkrétny materiál zobrazuje alebo opisuje identifikovateľné súkromné osoby, napr. fotografie zamestnancov EDA, alebo ak obsahuje prácu tretej strany, je potrebné získať dodatočné povolenie.

Ak je tento súhlas udelený, ruší a nahrádza sa ním uvedené všeobecné povolenie a jasne sa vymedzí každé prípadné obmedzenie týkajúce sa použitia.

V prípade použitia či šírenia obsahu materiálov, ktoré EÚ nevlastní, je potrebné žiadať povolenie priamo od držiteľov autorských práv.

Fotografia na titulnej strane: © 4AXY – stock.adobe.com.

Ilustrácie 6 a 8 – ikony: tieto ilustrácie boli vytvorené pomocou zdrojov z platformy [Flaticon.com](#). © Freepik Company S.L. Všetky práva vyhradené.

Ilustrácia 5 – mapa: [Eurostat](#).

Politika EDA týkajúca sa použitia materiálov sa nevzťahuje na softvér ani dokumenty, ktoré podliehajú právam priemyselného vlastníctva, ako sú patenty, ochranné známky, zapísané dizajny, logá a názvy.

Na súbore webových sídiel inštitúcií Európskej únie v rámci domény europa.eu sa poskytujú odkazy na sídla tretích strán. Keďže sú mimo kontroly EDA, odporúčame vám oboznámiť sa s ich politikami ochrany osobných údajov a autorských práv.

Použitie loga EDA

Logo EDA sa nesmie použiť bez predchádzajúceho súhlasu Európskeho dvora audítorov.

HTML	ISBN 978-92-849-7891-5	ISSN 1977-5776	doi:10.2865/9781035	QJ-01-26-032-SK-Q
PDF	ISBN 978-92-849-7892-2	ISSN 1977-5776	doi:10.2865/7783161	QJ-01-26-032-SK-N

AKO CITOVAŤ

Európsky dvor audítorov, [osobitná správa 19/2026](#) *Odhaľovanie kybernetických bezpečnostných incidentov a reakcia na ne – Rámec spolupráce EÚ napreduje, ale je len čiastočne účinný pre oneskorenia vo vykonávaní a obmedzenú výmenu informácií*, Úrad pre vydávanie publikácií Európskej únie, 2026.

V posledných rokoch EÚ posilnila svoj regulačný rámec v oblasti kybernetickej bezpečnosti a zriadila siete a mechanizmy na riešenie kybernetických bezpečnostných incidentov. EÚ tiež financuje projekty v oblasti kybernetickej bezpečnosti prostredníctvom programu Digitálna Európa.

Dospeli sme k záveru, že opatrenia EÚ len čiastočne uľahčujú odhaľovanie významných a rozsiahlych kybernetických bezpečnostných incidentov a reakciu na ne. Hoci sa postupne zavádzal rámec spolupráce, stále sa pracuje na dosiahnutí jeho úplného využitia. Obmedzená výmena informácií, nedostatky v podávaní správ a značné oneskorenia vo vykonávaní bránia tomu, aby siete a mechanizmy EÚ dosiahli svoj plný potenciál. Projekty sledujú príslušné ciele, ale viaceré z nich čelia operačným výzvam a oneskoreniam. V celkovom rámci monitorovania výkonnosti navyše existujú nedostatky. Predkladáme odporúčania na riešenie týchto nedostatkov.

Osobitná správa EDA podľa článku 287 ods. 4 druhého pododseku ZFEÚ.



EURÓPSKY
DVOR
AUDÍTOROV



Úrad pre vydávanie publikácií
Európskej únie

EURÓPSKY DVOR AUDÍTOROV
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Otázky: eca.europa.eu/sk/contact
Webová stránka: eca.europa.eu
Sociálne siete: @EUauditors