

Odhalování kybernetických bezpečnostních incidentů a reakce na ně

Rámec spolupráce EU postupuje, ale je pouze částečně účinný z důvodu zpoždění při provádění a omezeného sdílení informací



EVROPSKÝ
ÚČETNÍ DVŮR

Obsah

Body

01–24 | **Hlavní sdělení**

01–08 | Proč je tato oblast důležitá

09–24 | Co jsme zjistili a co doporučujeme

25–01 | **Podrobnější pohled na naše připomínky**

25–75 | Sítě a mechanismy EU v oblasti kybernetické bezpečnosti sice podporují spolupráci a reakci, avšak omezené sdílení informací a neúplné provádění jejich účinnost snižují

25–52 | Sítě EU umožňují spolupráci členských států, ale omezené sdílení informací snižuje jejich přidanou hodnotu

53–62 | Rezerva EU pro kybernetickou bezpečnost umožňuje rychlé nasazení služeb reakce na incidenty

63–75 | Evropský systém varování v oblasti kybernetické bezpečnosti usiluje o zlepšení kapacity pro odhalování hrozeb, ale není funkční

76–01 | Projekty financované EU v rámci programu DIGITAL mají za cíl posílit kybernetickou bezpečnost, ale potýkají se s problémy při provádění a podávání zpráv

76–82 | Zpoždění při jeho zřizování znemožnilo komunitě kompetencí pro kybernetickou bezpečnost utvářet program DIGITAL podle svých potřeb

83–97 | Projekty financované EU sledují relevantní cíle, ale mnoho z nich se potýká s provozními problémy

98–01 | Většina projektů financovaných EU nemá odpovídající výkonnostní rámce a údaje DIGITAL o výkonnosti v oblasti kybernetické bezpečnosti nejsou přesné

Přílohy

Příloha I – O auditu

Příloha II – Prostředí kybernetické bezpečnosti v EU

Příloha III – Vybraná opatření v oblasti kybernetické bezpečnosti

Příloha IV – Hodnocení projektů v oblasti kybernetické bezpečnosti financovaných EU ze strany EÚD

Zkratky

Glosář

Odpovědi Komise

Odpovědi Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC)

Odpovědi Agentury Evropské unie pro kybernetickou bezpečnost (ENISA)

Harmonogram

Auditní tým

01

Hlavní sdělení

Proč je tato oblast důležitá

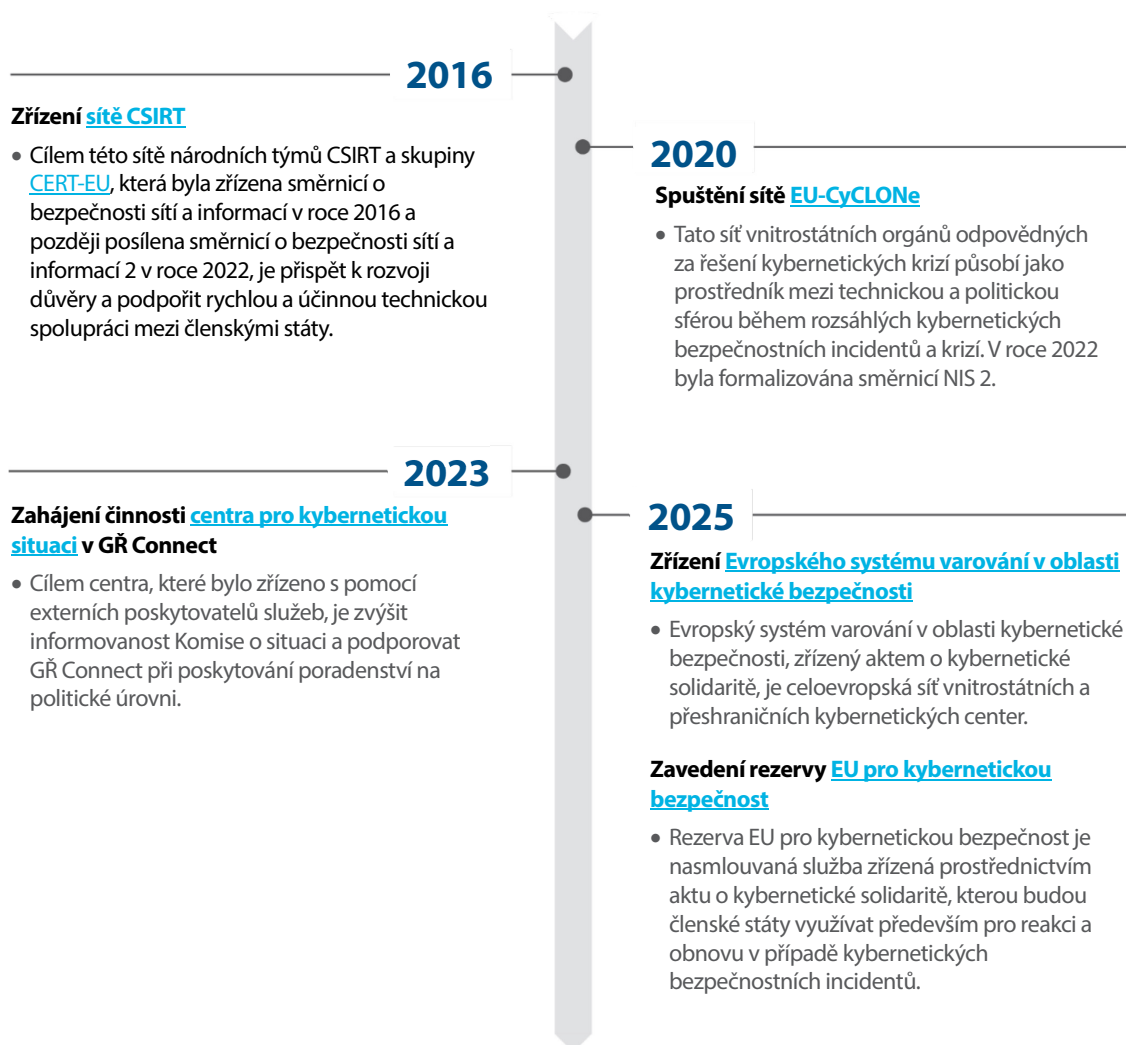
- 01** S rostoucí digitalizací naší ekonomiky a našeho každodenního života se zvyšují i rizika kybernetických útoků. Akt EU o kybernetické bezpečnosti¹ definuje kybernetickou bezpečnost jako „činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami“. Kybernetická bezpečnost vyžaduje holistický přístup k prevenci a odhalování kybernetických hrozeb, reakci na tyto hrozby a zotavení se z jejich následků.
- 02** V prostředí kybernetické bezpečnosti EU se v civilní sféře pohybuje řada veřejných a soukromých subjektů na regionální, národní a unijní úrovni. Kybernetická bezpečnost je také klíčovým prvkem národní bezpečnosti a obrany.
- 03** Hlavní odpovědnost za prevenci kybernetických bezpečnostních incidentů a krizí, které je postihují, a za přípravu a reakci na ně nesou členské státy. Vzhledem k tomu, že tyto incidenty mohou ovlivnit hladké fungování vnitřního trhu, hraje EU důležitou úlohu i v případě významného incidentu nebo krize. Ta v posledních letech posílila svůj vyvíjející se regulační rámec² pro kybernetickou bezpečnost a zavedla síť a mechanismy, jak je uvedeno na obrázku 1 **Obrázek 1** | Síť a mechanismy kybernetické bezpečnosti EU v období 2016–2025

¹ Nařízení (EU) 2019/881 ([akt o kybernetické bezpečnosti](#)).

² Komise například v listopadu 2025 navrhla [souhrnný balíček pro digitální oblast](#) a v lednu 2026 revidovaný [akt EU o kybernetické bezpečnosti](#).

04 níže a v příloze II (*Annex II*).

Obrázek 1 | Sítě a mechanismy kybernetické bezpečnosti EU v období 2016–2025



CSIRT: tým pro reakce na počítačové bezpečnostní incidenty

GŘ Connect: Generální ředitelství pro komunikační sítě, obsah a technologie

EU-CyCLONe: Evropská síť styčných organizací pro řešení kybernetických krizí

Směrnice NIS: směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Směrnice NIS 2: směrnice (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii

Zdroj: EÚD.

05 Ve stávajícím víceletém finančním rámci na období 2021–2027 je hlavním zdrojem financování kybernetické bezpečnosti program Digitální Evropa (DIGITAL). Jeho celkový rozpočet činí 8,1 miliardy EUR, z čehož 1,4 miliardy EUR je vyčleněno na posílení kybernetické bezpečnosti.

06 Cílem auditu bylo posoudit, zda opatření EU pomáhají členským státům účinně odhalovat významné a rozsáhlé kybernetické bezpečnostní incidenty a reagovat na ně. Kontrolovali jsme, zda tomu tak bylo v případě:

- sítí a mechanismů na úrovni EU (tj. síť týmů pro reakce na počítačové bezpečnostní incidenty (síť CSIRT), Evropské síť styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), Evropského systému varování v oblasti kybernetické bezpečnosti, střediska pro kybernetickou situaci a rezerva EU pro kybernetickou bezpečnost);
- opatření financovaných v rámci programu DIGITAL.

07 Očekáváme, že naše zjištění přispějí k posílení kybernetické odolnosti EU zlepšením účinnosti a efektivnosti sítí a mechanismů EU, jakož i zlepšením způsobu výběru a monitorování opatření financovaných EU.

08 Audit se vztahuje na období od roku 2022 do roku 2025. Vychází z dokumentárního přezkumu a analýzy příslušných dokumentů, auditních návštěv ve třech členských státech (Irsku, Řecku a Itálii) a písemných dotazníků a rozhovorů s příslušnými zúčastněnými stranami. Další souvislosti a podrobné informace o rozsahu a koncepci auditu jsou uvedeny v [příloze I](#).

Co jsme zjistili a co doporučujeme

09 Celkově jsme dospěli k závěru, že opatření EU usnadňují odhalování významných a rozsáhlých kybernetických bezpečnostních incidentů a reakci na ně pouze částečně. I když byl postupně zaveden rámec spolupráce, stále probíhají práce na kompletním dokončení systému. Omezené sdílení informací, nedostatky ve vykazování údajů a značná zpoždění při provádění brání sítím a mechanismům EU v dosažení jejich plného potenciálu. Projekty financované programem DIGITAL sledují příslušné cíle, některé z nich se však potýkají s provozními problémy a zpožděními a v celkovém rámci pro monitorování výkonnosti existují nedostatky.

10 Stávající rámec sítí a mechanismů EU pro usnadnění odhalování významných kybernetických bezpečnostních incidentů a reakce na ně vznikl postupně. V roce 2025 přijala Rada [kybernetický plán](#), který stanoví rámec EU pro řešení kybernetických krizí. Zjistili jsme, že kybernetický plán do značné míry vyjasňuje úlohy a povinnosti, pokud jde o řešení kybernetických krizí v EU. Bez ohledu na to je třeba ještě formalizovat procesní opatření týkající se spolupráce mezi sítí CSIRT (zřízenou v roce 2016) a sítí EU-CyCLONe (formalizovanou v roce 2023) (body [25–31](#)).

- 11** Zjistili jsme, že sdílení informací prostřednictvím těchto sítí je omezené. Je to dáno zejména zpožděním při provádění [směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii](#) (směrnice NIS 2), obtížemi při určování toho, zda má incident přeshraniční dopad, a národními bezpečnostními právními předpisy, které brání sdílení informací. Přidaná hodnota sítí se výrazně snižuje, pokud členské státy nejsou ochotny sdílet včasné a použitelné informace (body [32–45](#)).



Doporučení 1

Posílit sdílení informací mezi členskými státy

Aby Komise zlepšila odhalování kybernetických bezpečnostních incidentů a reakci na ně, s podporou Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) by měla:

- a) navrhnout skupině pro spolupráci v oblasti bezpečnosti informačních systémů, aby provedla podrobnou analýzu národních bezpečnostních omezení, která omezují sdílení informací a ovlivňují kybernetickou odolnost EU, a identifikovala právní a technická řešení ke zvýšení sdílení informací při současném respektování hranic národní bezpečnosti;
- b) ve spolupráci s členskými státy zajistit, aniž by byla dotčena rozhodnutí spolunormotvůrců, aby jednotné kontaktní místo pro hlášení incidentů navržené v souhrnném balíčku pro digitální oblast mohlo odhalovat potenciální přeshraniční incidenty;
- c) pracovat na řešeních umožňujících hlášení incidentů agentuře ENISA v reálném čase.

Cílové datum provedení: a) a b) 2027, c) 2028.

- 12** V roce 2022 ustavila Komise své „centrum pro kybernetickou situaci“ s cílem zvýšit svou informovanost o situaci a podpořit své institucionální povinnosti v oblasti řešení krizí. Fungování střediska do značné míry podporováno na smlouvě s externími poskytovateli služeb. Zjistili jsme, že práce prováděná externími poskytovateli služeb částečně zdvojuje stávající kapacitu Agentury Evropské unie pro kybernetickou bezpečnost (ENISA), pokud jde o informovanost o situaci a monitorování hrozeb. Domníváme se, že středisko pro kybernetickou situaci bylo zřízeno způsobem, který dostatečně nevyužil potenciál racionalizace využitím informací, které již byly k dispozici od Komise a agentury ENISA. Skutečnost, že neexistuje komplexní a podrobný plán pro dobu po skončení platnosti smlouvy, navíc představuje riziko pro fungování střediska pro kybernetickou situaci po roce 2026 (body [46–52](#)).



Doporučení 2

Racionalizovat schopnosti EU v oblasti informovanosti o situaci v oblasti kybernetické bezpečnosti a optimalizovat šíření informací

V zájmu zvýšení účinnosti by Komise měla ve spolupráci s agenturou ENISA posoudit proveditelnost společného získávání a analýzy informací pro účely informovanosti o situaci. Rovněž by měla tyto informace a související zprávy o kybernetických hrozbách zpřístupnit příslušným útvarům a agenturám EU.

Cílové datum provedení: 2027

- 13** **Akt o kybernetické solidaritě** z roku 2024 zřizuje rezervu EU pro kybernetickou bezpečnost, jejímž cílem je podpořit reakci členských států na závažné kybernetické bezpečnostní incidenty a obnovu po takových incidentech. Skládá se z vybraných poskytovatelů služeb za každý členský stát, schopných kdykoliv na incidenty zareagovat. Ačkoli tento přístup pomáhá řešit specifické požadavky členských států a budovat důvěru, dostupný rozpočet je mezi ně rozdělen rovným dílem a nezohledňuje specifické potřeby jednotlivých členských států (body [53–58](#)).
- 14** Domníváme se, že využívání předem nasmlouvaných poskytovatelů umožňuje rychlou aktivaci služeb souvisejících s reakcí na incidenty. Ačkoli cílem rezervy EU pro kybernetickou bezpečnost je především podpořit reakci a obnovu, pokud není použita k reakci na incidenty, lze ji použít i na připravenost. Tento flexibilní přístup může zabránit tomu, aby předplacené služby zůstaly nevyužity. Hrozí však, že rezerva bude v rozporu se svým zamýšleným účelem využívána převážně k připravenosti, a nikoli k reakci (body [59–62](#)).
- 15** Evropský systém varování v oblasti kybernetické bezpečnosti je síť národních a přeshraničních kybernetických center, jejichž cílem je zlepšit odhalování a analýzu kybernetických hrozeb a reakci na ně. Zjistili jsme, že v době auditu nebylo ani jedno z obou center (Athena a ENSOC) v důsledku značných zpoždění při zadávání veřejných zakázek na nástroje a služby v provozu a že Evropský systém varování v oblasti kybernetické bezpečnosti zatím nebyl funkční (body [63–71](#)).

- 16** Jedním z klíčových cílů Evropského systému varování v oblasti kybernetické bezpečnosti je podpořit smysluplné sdílení informací mezi klastry členských států. I když to má potenciál vyřešit některé problémy související se sdílením informací, zároveň je velmi náročné začlenit kybernetická střediska do již tak složitého prostředí kybernetické bezpečnosti. Zjistili jsme, že potřebné dohody o spolupráci, společná taxonomie a normy interoperability nezbytné pro plné fungování Evropského systému varování v oblasti kybernetické bezpečnosti dosud nebyly zavedeny (body [72–75](#)).



Doporučení 3

Začlenění Evropského systému varování v oblasti kybernetické bezpečnosti do prostředí kybernetické bezpečnosti EU

Komise by měla společně s agenturou ENISA a členskými státy zajistit, aby byly ustaveny mechanismy spolupráce a zavedeny normy interoperability, a usnadnit tak sdílení informací mezi přeshraničními středisky, která jsou součástí Evropského systému varování v oblasti kybernetické bezpečnosti, sítě CSIRT a sítě EU-CyCLONe.

Cílový termín provedení: 2028.

- 17** V roce 2018 navrhla Komise ustavit Evropské centrum kompetencí pro kybernetickou bezpečnost (ECCC), které by od roku 2021 spravovalo složku kybernetické bezpečnosti programu DIGITAL. [Nařízení o ECCC](#) vyzvalo k vytvoření komunity kompetencí pro kybernetickou bezpečnost složené ze zástupců průmyslu, akademických a výzkumných organizací. Vybraní členové komunity kompetencí pro kybernetickou bezpečnost by pak vytvořili strategickou poradní skupinu (body [76–77](#)).
- 18** Zjistili jsme, že dosažení finanční autonomie centra ECCC a ustavení komunity kompetencí pro kybernetickou bezpečnost a skupiny SAG se zpozdilo. V důsledku toho komunita kompetencí pro kybernetickou bezpečnost a skupina SAG nemohly přispět k utváření pracovních programů DIGITAL. Domníváme se, že se jednalo o promarněnou příležitost (body [78–82](#)).
- 19** Zjistili jsme, že všechny projekty, které jsme prověřovali, sledovaly relevantní cíle, které přispívají k dosažení cílů kybernetické bezpečnosti programu DIGITAL. Zjistili jsme však případy, kdy kvalita nebo dosažené výsledky nebyly uspokojivé, zejména kvůli zpožděním při provádění (body [83–88](#)).

- 20** Nařízení o programu Digitální Evropa stanoví, že z bezpečnostních důvodů může být financování kybernetické bezpečnosti omezeno na subjekty, které jsou usazeny v členských státech a kontrolovány členskými státy nebo jejich občany. Toto posouzení vlastnictví a kontroly provádí jménem centra ECCC Centrální validační služba v [Evropské výkonné agentuře pro výzkum](#) (body [89–92](#)).
- 21** V případě finanční podpory třetím stranám je posouzení vlastnictví a kontroly odpovědností příjemců projektu a vychází z jejich vlastního přístupu a metodiky. Zjistili jsme, že centrum ECCC nevaliduje svou metodiku, ani neprovádí kontroly, aby se ujistilo, že vybrané třetí strany jsou vlastněny a kontrolovány státními příslušníky zemí EU nebo státy EU. Domníváme se, že existuje značné riziko, že příjemci nejsou schopni tyto kontroly řádně provádět. Toto riziko nebylo odpovídajícím způsobem zmírněno a mohlo by vést k expozici citlivé infrastruktury, provozních údajů a technologií kritických z hlediska bezpečnosti (body [93–97](#)).



Doporučení 4

Zajistit důkladné posouzení vlastnictví a kontroly subjektů, které jsou příjemci finančních prostředků EU v rámci programu Digitální Evropa

Evropské centrum kompetencí pro kybernetickou bezpečnost by mělo:

- a) získat přiměřenou jistotu, že příjemci odpovědní za poskytování finanční podpory třetím stranám mají administrativní a technickou kapacitu nezbytnou k provádění odpovídajících posouzení vlastnictví a kontroly, a to na základě stávající metodiky, která je k dispozici příjemcům provádějícím finanční podporu třetím stranám,
- b) na základě vzorku zkontrolovat, zda finanční prostředky EU obdržely pouze způsobilé subjekty.

Cílový termín provedení: a) 2026, b) 2027.

- 22** Příjemci, kteří řídí projekty financované EU, musí ECCC podávat zprávy o svém pokroku a výsledcích s využitím milníků a předmětů dodávky. Ty jsou klíčové pro monitorování projektů a měly by být řádně definovány. Zjistili jsme, že téměř žádný z projektů v našem vzorku se neřídil pokyny, jak vypracovat milníky a předměty dodávky, a že mnohé z nich nebyly pro sledování pokroku užitečné (body [98–100](#)).

- 23** Zjistili jsme, že mnoho ukazatelů výkonnosti používaných příjemci není relevantních nebo měřitelných a chybí jim cíl nebo výchozí hodnota. Kromě toho bylo vykazování těchto ukazatelů nedostatečné, a proto nemůže sloužit jako základ pro posuzování výkonnosti projektů (body [101–103](#)).
- 24** Aby bylo možné sledovat výsledky programu DIGITAL jako celku, musí všechny projekty podávat zprávy o konkrétních ukazatelích programu, které se promítají do ročních [prohlášení Komise o výkonnosti programů](#). Centrum ECCC je odpovědné za shromažďování a ověřování údajů k těmto ukazatelům. Zjistili jsme několik problémů, pokud jde o způsob shromažďování údajů a jejich celkovou kvalitu. Nenašli jsme žádné důkazní informace o tom, že by centrum ECCC ověřovalo přesnost vykázaných údajů. Na základě kontrol našeho vzorku se domníváme, že vykázané údaje přesně neodrážejí dosažené výsledky (body [104–107](#)).



Doporučení 5

Posílit rámec pro sledování výkonnosti složky programu Digitální Evropa týkající se kybernetické bezpečnosti

Aby bylo možné odpovídajícím způsobem sledovat pokrok a výkonnost, mělo by Evropské centrum kompetencí pro kybernetickou bezpečnost:

- (a) před podpisem grantu zajistit, aby všechny projekty měly definované milníky, předměty dodávky a ukazatele výkonnosti, které jsou v souladu s pokyny uvedenými ve formuláři žádosti;
- (b) navrhnout a zavést spolehlivý systém pro shromažďování, sledovatelnost, ověřování a agregaci údajů pro ukazatele výkonnosti složky programu Digitální Evropa týkající se kybernetické bezpečnosti, aby se zajistilo, že ukazatele budou přesně odrážet dosažené výsledky.

Cílové datum provedení: 2027

Podrobnější pohled na naše připomínky

Sítě a mechanismy EU v oblasti kybernetické bezpečnosti sice podporují spolupráci a reakci, avšak omezené sdílení informací a neúplné provádění jejich účinnost snižují

Sítě EU umožňují spolupráci členských států, ale omezené sdílení informací snižuje jejich přidanou hodnotu

- 25** Stávající rámec EU pro sítě a mechanismy usnadňující odhalování významných kybernetických bezpečnostních incidentů a reakci na ně vznikl postupně, počínaje [směrnicí o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii](#)³ (směrnice NIS), která vstoupila v platnost v srpnu 2016. Současnou situaci v EU ilustrujeme v [příloze II](#).

Sítě EU umožňují spolupráci členských států na technické a operativní úrovni

- 26** Směrnice o bezpečnosti sítí a informací zřídila [sít' CSIRT](#), která sdružuje skupinu [CERT-EU](#) (Služba kybernetické bezpečnosti pro orgány, instituce a jiné subjekty Unie) a týmy CSIRT jmenované členskými státy. Cílem této sítě je budovat důvěru mezi národními týmy CSIRT a podporovat rychlou a účinnou operativní spolupráci mezi členskými státy.

³ Směrnice (EU) 2016/1148.

- 27** Síť EU-CyCLONe byla zřízena v roce 2020 jako neformální síť pro spolupráci vnitrostátních orgánů odpovědných za řešení kybernetických krizí. Slouží jako most mezi technickou úrovní, na níž síť CSIRT působí, a politickou úrovní Rady Evropské unie a jejími integrovanými opatřeními pro politickou reakci na krize. V roce 2023 vstoupila v platnost směrnice NIS 2, která formalizovala úlohu sítě EU-CyCLONe a udělila jí jasný mandát.
- 28** Posuzovali jsme, zda jsou úlohy a povinnosti těchto sítí na úrovni EU dobře definovány a zda umožňují spolupráci členských států.
- 29** Agentura ENISA působí jako sekretariát sítě CSIRT a sítě EU-CyCLONe a poskytuje jim zdroje, odborné znalosti, infrastrukturu a nástroje IT nezbytné pro spolupráci a bezpečnou komunikaci pro sdílení informací. Ve svém průzkumu spokojenosti zúčastněných stran⁴ z počátku roku 2025 obdržela agentura ENISA v oblasti fungování sekretariátu těchto sítí dobré hodnocení. Tato pozitivní zpětná vazba nám byla potvrzena i během našich auditních návštěv, během nichž národní orgány pro kybernetickou bezpečnost vyjadřovali své uznání.
- 30** V roce 2025 přijala Rada kybernetický plán, který vymezuje úlohy a povinnosti klíčových aktérů (včetně sítě CSIRT a sítě EU-CyCLONe) a mechanismů používaných při rozsáhlých kybernetických bezpečnostních incidentech nebo kybernetických krizích. Zjistili jsme, že tento kybernetický plán do značné míry vyjasňuje úlohy a povinnosti, pokud jde o řešení kybernetických krizí v EU, a zohledňuje změny v prostředí od prvního kybernetického plánu v roce 2017. Definuje tři úrovně spolupráce: technickou, operační a politickou. Podrobně popisuje nové síť a struktury zřízené od roku 2017 – jako jsou síť EU-CyCLONe, týmy rychlé reakce EU na hybridní hrozby a Evropský systém varování v oblasti kybernetické bezpečnosti – a zabývá se tím, jak by řešení kybernetických krizí mělo být začleněno do širšího rámce EU pro reakci na krize.

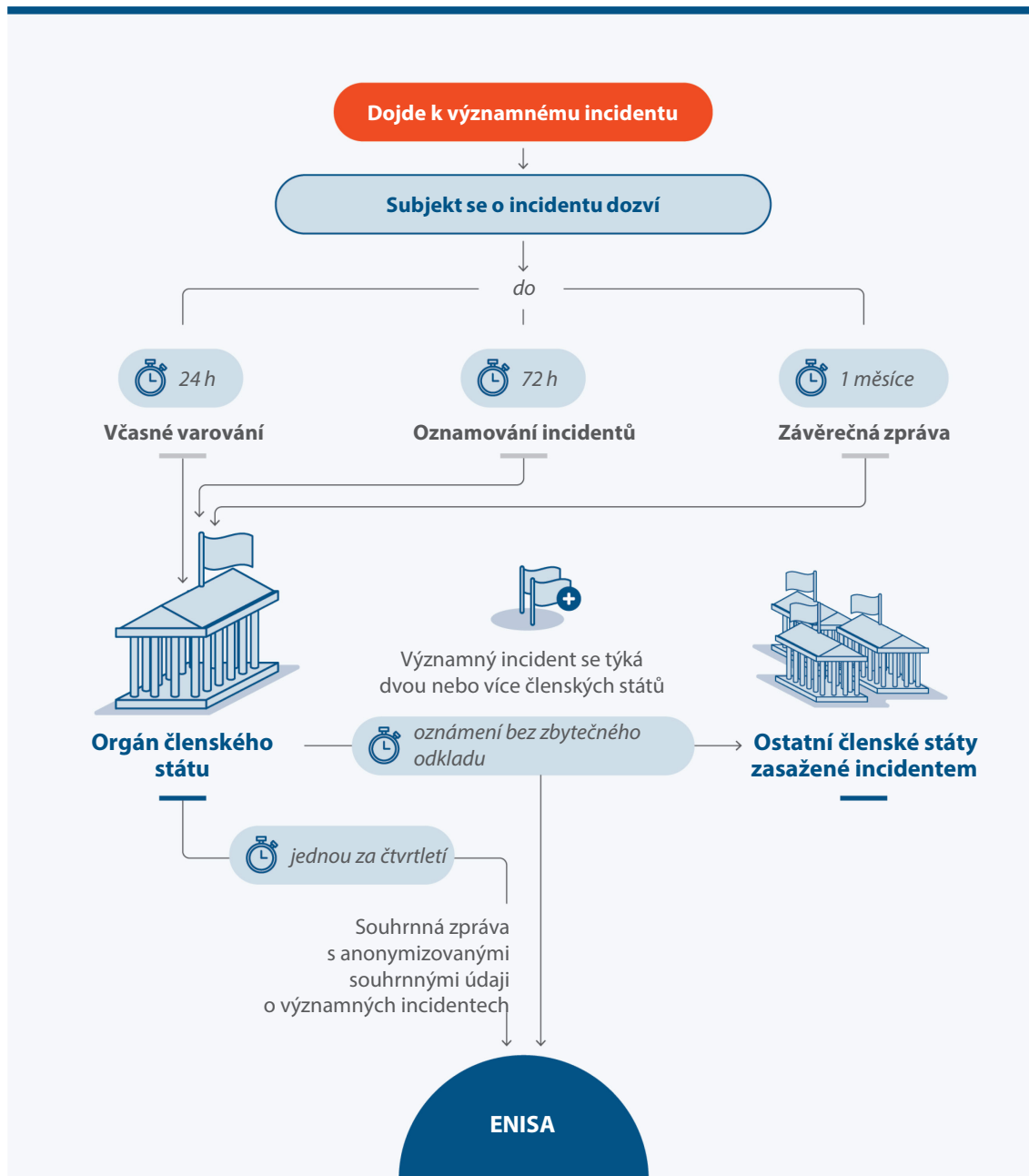
⁴ Konsolidovaná výroční zpráva o činnosti agentury ENISA za rok 2024, s. 33 a 36.

- 31** Navzdory tomu, že síť CSIRT byla formálně ustavena v roce 2016 a síť EU-CyCLONe v roce 2023, dosud nebyla neformalizována procesní ujednání o tom, jak by měly spolupracovat. Tyto sítě se rovněž nedohodly na kritériích pro síť CSIRT, která by síti EU-CyCLONe pomáhala identifikovat, zda zjištěný kybernetický bezpečnostní incident představuje potenciální nebo probíhající rozsáhlý kybernetický bezpečnostní incident. Obě sítě se rovněž musí dohodnout na společné taxonomii úrovní závažnosti incidentů a klíčových pojmů – jako je „hrozba“, „aktér hrozby“, „incident“ nebo „dopad“ –, která je nezbytná automatizovanou výměnu informací. V současné době existuje prostor pro výklad toho, kdy lze incident považovat za významný nebo rozsáhlý. Na neexistenci společné taxonomie poukazovaly i orgány činné v oblasti pro kybernetickou bezpečnost všech tří členských států, které jsme navštívili.

Přidanou hodnotu těchto sítí významně snižuje omezené sdílení informací a podávání zpráv

- 32** Zeměpisné hranice kybernetickým incidentům a útokům a jejich šíření nijak nebrání. Ke zvýšení kybernetické bezpečnosti může významně přispět sdílení informací mezi členskými státy, například o taktice a technikách používaných aktéry hrozeb a o digitálních známkách, že síť nebo informační systém byly narušeny („indikátory kompromitace“).
- 33** Zjistili jsme, že sdílení informací bylo omezené, což výrazně snížilo přidanou hodnotu těchto sítí. Omezení, která jsme zaznamenali, se týkají zejména zpoždění při provádění směrnice NIS 2, problémů s určováním toho, zda má incident přeshraniční dopad, právních předpisů v oblasti národní bezpečnosti, které omezují sdílení informací, a nedostatku důvěry. Směrnice NIS 2 zavádí několik požadavků na podávání zpráv pro subjekty spadající do její oblasti působnosti a pro orgány členských států, jak je znázorněno na [obrázku 2](#).

Obrázek 2 | Časový rámec pro hlášení incidentů podle směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v EU (NIS 2)



Zdroj: EÚD na základě dokumentů agentury ENISA.

- 34** Členské státy měly [směrnici NIS 2 provést ve vnitrostátním právu](#) do října 2024, ale pouze dva z nich lhůtu splnily. Zpoždění při provádění mají významný dopad na sdílení informací, protože subjekty, na něž se vztahuje směrnice NIS 2, nejsou v mezidobí ze zákona povinny hlásit incidenty. Komise odhadla⁵, že směrnice o bezpečnosti sítí a informací se vztahuje na 15 500 subjektů, zatímco do oblasti působnosti směrnice o bezpečnosti sítí a informací 2 spadá více než 110 000 subjektů. Například veřejná správa, která je podle zprávy agentury ENISA o [prostředí hrozeb z roku 2025](#) cílem útoků ze všech odvětví v EU nejčastěji, neměla podle směrnice o bezpečnosti sítí a informací povinnost incidenty hlásit.
- 35** Hlášení údajů o incidentech agentuře ENISA každé tři měsíce (tj. dlouho poté, co k incidentu mohlo dojít) omezuje jeho přidanou hodnotu. Tyto údaje slouží většinou ke statistickým účelům a vykazování historických trendů, nikoli ke zlepšení odhalování a reakce. Agentura ENISA poskytuje členským státům [online nástroj](#) pro podávání zpráv. Šablona pro podávání zpráv obsahuje minimální soubor údajů, které musí být poskytnuty, jako je druh incidentu a dotčené odvětví. Kromě toho agentura ENISA navrhuje, aby členské státy poskytovaly další informace, které umožní podrobnější analýzu údajů, například spojení incidentů s konkrétními zranitelnými místy. Ne všechny členské státy se však rozhodly tyto informace poskytnout, což výrazně snižuje kvalitu a přidanou hodnotu shromažďovaných údajů.
- 36** Agentura ENISA ve své [zprávě o stavu kybernetické bezpečnosti v EU z roku 2024](#) uvedla, že hlášení incidentů je pravděpodobně nedostatečné, protože počet hlášených incidentů se zdá být nízký. V letech 2018 až 2021 nahlásily členské státy agentuře ENISA 100 až 500 incidentů ročně. Tento počet se postupně zvyšoval a v roce 2024 vzrostl na 1 276⁶.

⁵ Evropská komise, 2020, [zpráva o posouzení dopadu](#).

⁶ Údaje CIRAS za rok 2024.

- 37** Agentura ENISA ve své [zprávě o prostředí hrozeb](#) z roku 2025, která se vztahuje na období od června 2024 do června 2025, identifikovala prostřednictvím zpravodajských informací z otevřených zdrojů, jako jsou zpravodajské články, přibližně 4 800 kybernetických bezpečnostních incidentů⁷. Oznamovací povinnost podle směrnice o bezpečnosti sítí a informací 2 se nevztahovala na všechny tyto incidenty, neboť při shromažďování údajů pokrývá agentura ENISA širší spektrum incidentů. A naopak řada významných incidentů se ve zpravodajských informacích z otevřených zdrojů neobjevuje. Vzhledem k tomu, že údaje oznámené členskými státy jsou anonymizovány, agentura ENISA nemůže srovnávat incidenty, které zjistí, s incidenty oznámenými členskými státy. Není proto možné přesně určit rozsah nedostatečného oznamování, domníváme se však, že rozdíl mezi počtem incidentů hlášených členskými státy a incidentů uvedených ve zprávě o prostředí hrozeb ukazuje, že ne všechny významné incidenty jsou hlášeny.
- 38** Dalším ukazatelem nedostatečného oznamování je počet oznámení dalším dotčeným členským státům a agentuře ENISA týkajících se významných přeshraničních incidentů. Podobný požadavek existoval podle směrnice o bezpečnosti sítí a informací, ale byl shledán neúčinným, neboť Komise⁸ v roce 2020 dospěla k závěru, že oznámení byla navzdory této povinnosti zasílána jen zřídka. Připisoval neoznámení absenci jasných způsobů sdílení informací a neexistenci společných cílů motivujících ke sdílení.
- 39** Povinnost informovat ostatní členské státy má zásadní význam pro to, aby se zabránilo přelévání incidentů – pokud se tak neděje, negativně to ovlivňuje kybernetickou bezpečnost EU. V roce 2025 oznámilo sedm členských států pouze 14 významných přeshraničních incidentů. Členské státy předložily dvě zprávy o incidentech v roce 2024, žádnou v roce 2023 a tři s možným přeshraničním dopadem v roce 2022. Z toho je patrné, že míra hlášení významných přeshraničních incidentů je velmi nízká a neodráží skutečný rozsah těchto útoků. Náležitou perspektivu nastiňuje skutečnost, že agentura ENISA ve své [zprávě o prostředí hrozeb z roku 2024](#) identifikovala 322 incidentů, které byly přímo zaměřeny na dva nebo více členských států. Incident ve společnosti Collins Aerospace (viz [rámeček 1](#)) je příkladem případu, kdy členské státy incident neohlásily, přestože měl významný přeshraniční dopad.

⁷ Zpráva agentury ENISA o prostředí hrozeb z roku 2025.

⁸ Evropská komise, 2020, [zpráva o posouzení dopadu](#).

Rámeček 1

Kybernetický bezpečnostní incident, který narušil provoz letišť

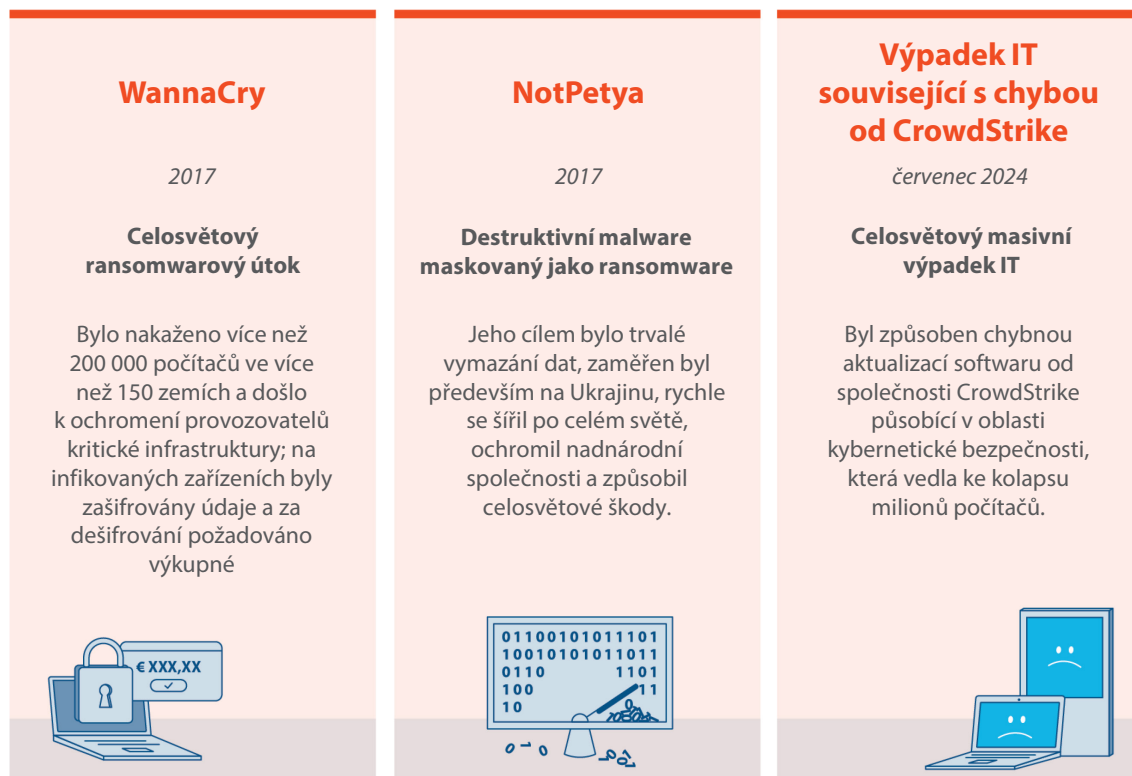
V září 2025 se společnost Collins Aerospace, důležitý poskytovatel technologií pro letecký průmysl, stala cílem významného ransomwarového útoku, který se zaměřil na její software pro zpracování dat o cestujících. Útok přinutil velká evropská letiště, aby se vrátila k manuálnímu provozu, což vedlo k rozsáhlým zpožděním a rušení letů. Narušení bylo nejzávažnější na letišti Londýn-Heathrow, na letišti v Bruselu, na letišti Berlín-Braniborsko a na letišti v Dublinu.

Podle směrnice NIS 2 se incident považuje za „významný“, pokud, mimo jiné, dotčenému subjektu způsobí vážné provozní narušení služeb nebo finanční ztrátu. Přesto ani jeden členský stát k tomuto incidentu nepřistoupil jako k významnému nebo rozsáhlému přeshraničnímu incidentu. Ani jeden dotčený členský stát proto incident formálně neoznámil agentuře ENISA ani jiným členským státům. Síť CSIRT neinformovala síť EU-CyCLONe, která proto nepodporovala koordinované řešení incidentu.

Zdroj: analýza EÚD na základě rozhovorů s pracovníky agentury ENISA.

- 40** Dalším důvodem omezeného oznamování přeshraničních incidentů je skutečnost, že je na každém orgánu členského státu, aby určil, zda má oznámený incident přeshraniční dopad, a aby určil další dotčené členské státy. Na základě informací, které má oznamující subjekt nebo orgán členského státu k dispozici, si přeshraniční povahy některých útoků nemusí být vědom. V současné době neexistuje žádná celounijní platforma, která by dostávala hlášení o incidentech v reálném čase od všech členských států a která by mohla informace o odvětvích nebo indikátorech kompromitace pro odhalování přeshraničních incidentů uvádět do vzájemných souvislostí. Existuje proto značné riziko, že některé přeshraniční incidenty nemusí být identifikovány a hlášeny.
- 41** Od roku 2016 nebyl ani jeden bezpečnostní incident označen ani jedním členským státem za „rozsáhlý“. V zásadě se definice rozsáhlého incidentu vztahuje na jakýkoli incident, který se významně dotýká alespoň dvou členských států. Nicméně ani kybernetické bezpečnostní incidenty, které způsobily celosvětové výpadky a významné škody a jejich příklady jsou uvedeny na [obrázku 3](#), nebyly považovány za rozsáhlé. V důsledku toho nebyl postup eskalace sítě EU-CyCLONe kvůli rozsáhlému kybernetickému bezpečnostnímu incidentu nikdy plně aktivován.

Obrázek 3 | Příklady závažných kybernetických bezpečnostních incidentů



Zdroj: EÚD, převzato z [Cloudflare](#), [ENISA](#), [Europol](#), [Wired](#), [IBM](#), [CrowdStrike](#).

- 42** Cílem vytvoření sítě CSIRT bylo nejen uložit subjektům a členským státům povinnost podávat zprávy, ale také usnadnit sdílení informací. Základem sítě CSIRT, v níž jsou informace sdíleny na dobrovolném základě, je důvěra mezi členskými státy. Pokud členské státy nebudou ochotny sdílet včasné a použitelné informace, přidaná hodnota sítě se výrazně sníží.
- 43** Sdílení informací na úrovni EU je omezeno právními předpisy jednotlivých členských států v oblasti národní bezpečnosti. Pokud se členský stát domnívá, že informace o kritickém subjektu související s kybernetickým útokem jsou tajné nebo že by oznámení konkrétního incidentu poškodilo jeho národní bezpečnost, není povinen tyto informace sdílet. Během našich návštěv v členských státech zástupci sítě CSIRT a sítě EU-CyCLONe uvedli, že sdílení lze provádět pouze v mezích vnitrostátních bezpečnostních právních předpisů. Na úrovni EU nebyla provedena analýza vnitrostátních právních rámců členských států a jejich dopadu na sdílení informací.

- 44** V roce 2016 se síť CSIRT skládala z 28 vnitrostátních týmů CSIRT se dvěma zástupci z každého členského státu. Nedostatečné sdílení informací je trvalým problémem a [Komise ve svém hodnocení](#) směrnice o bezpečnosti sítí a informací připustila, že „členské státy informace mezi sebou systematicky nesdílejí“, což má dopad zejména na účinnost opatření v oblasti kybernetické bezpečnosti a úroveň společné informovanosti o situaci na úrovni EU. Podle směrnice NIS 2 jmenovala řada členských států kromě svých národních týmů CSIRT také odvětvové týmy CSIRT, a síť se tak výrazně rozšířila. V době auditu sestávala ze 42 týmů CSIRT a více než 700 individuálních účastníků. Budování důvěry je proto ještě náročnější, neboť udržování úzkých vazeb mezi všemi členy je obtížné.
- 45** Síť CSIRT si je problému sdílení informací vědoma a zvažuje různá opatření ke zvýšení důvěry v rostoucí síť. Alternativním přístupem k celounijní síti, který může pomoci tuto výzvu řešit, je vytvoření menších klastrů členských států tvořících přeshraniční uzly, jak je podrobně popsáno v bodech [63–75](#).

Služby nasmlouvané střediskem pro kybernetickou situaci částečně duplikují stávající kapacity a jeho budoucí fungování není jasné

- 46** Podle směrnice NIS 2 v případech, kdy potenciální nebo probíhající rozsáhlý kybernetický bezpečnostní incident má nebo pravděpodobně bude mít významný dopad, se Komise stává členem sítě EU-CyCLONe⁹. Tato nová úloha a vývoj prostředí hrozeb vedly Komisi k tomu, že v roce 2022 zřídila v rámci GŘ CNECT pracovní skupinu pro kybernetickou koordinaci. Tato pracovní skupina zahrnuje středisko pro kybernetickou situaci, které by mělo Komisi pomoci zvýšit její informovanost o situaci s cílem podpořit ji v jejích institucionálních povinnostech v oblasti krizového řízení. Měla by rovněž pomáhat GŘ CNECT poskytovat poradenství na politické úrovni.

⁹ Čl. 16 odst. 2 [směrnice NIS 2](#).

- 47** Při zřizování střediska pro kybernetickou situaci Komisi do značné míry podporují externí poskytovatelé služeb, s nimiž byly v prosinci 2022 [uzavřeny smlouvy](#) v hodnotě téměř 18 milionů EUR na dobu čtyř let. Posuzovali jsme zřízení střediska, jeho výstupy a plány Komise na jeho budoucí fungování.
- 48** V rámci poskytovaných služeb vytvořili dodavatelé přehled založený na komerčních zpravodajských informacích o kybernetických hrozbách s cílem prezentovat a sdílet informace o hrozbách. Vypracovávají rovněž různé zpravodajské zprávy o kybernetických hrozbách, včetně denních a týdenních zpráv a tematických zpráv o zemích nebo hospodářských odvětvích. V jedné z budov Komise bylo zřízeno fyzické středisko pro kybernetickou situaci, sestávající z místnosti vybavené počítači na dálku připojenými k přehledu hostovanému dodavateli. V době auditu se centrum pro kybernetickou situaci sestávalo z několika málo zaměstnanců Komise, které podporovalo mnoho analytiků z řad dodavatelů i odborníků z agentury ENISA.
- 49** Zjistili jsme, že činnosti externích poskytovatelů služeb střediska pro kybernetickou situaci částečně duplikují stávající kapacitu agentury ENISA. Agentura ENISA má stálou kapacitu pro informovanost o aktuální kybernetické situaci a monitorování hrozeb. Pravidelně zveřejňuje zprávy o kybernetických hrozbách, včetně bleskových zpráv o konkrétních incidentech, a týdenní zprávy, které poskytují přehled hrozeb. Zprávy jsou založeny na zpravodajských informacích z otevřených zdrojů a podobají se zprávám, které poskytují dodavatelé. Dále v dobách krize agentura ENISA vypracovává rámcové strategické informační přehledy nebo k nim přispívá. Jsou určeny pro tvůrce politik a jsou rovněž podobné tomu, co vytváří středisko pro kybernetickou situaci.
- 50** Údaje používané střediskem pro kybernetickou situaci k vypracování těchto zpráv dále vycházejí z komerčních zpravodajských informací o kybernetických hrozbách a podobají se údajům používaným jinými útvary Komise, jako je Generální ředitelství pro digitální služby a CERT-EU. Domníváme se, že způsob, jakým bylo středisko pro kybernetickou situaci zřízeno, dostatečně nevyužil potenciál racionalizace tím, že by středisko využívalo již dostupné informace Komise a agentury ENISA.
- 51** Smlouva vyprší v prosinci 2026. Po tomto datu již dodavatelé nebudou středisku pro kybernetickou situaci poskytovat služby. Tyto služby zahrnují poskytování údajů uvedených v přehledu, vypracovávání zpráv o hrozbách a personálně tvoří větší část střediska. Přehled bude předán Komisi, ale nebude-li průběžně aktualizován o zpravodajské informace o kybernetických hrozbách, ztratí svou přidanou hodnotu.

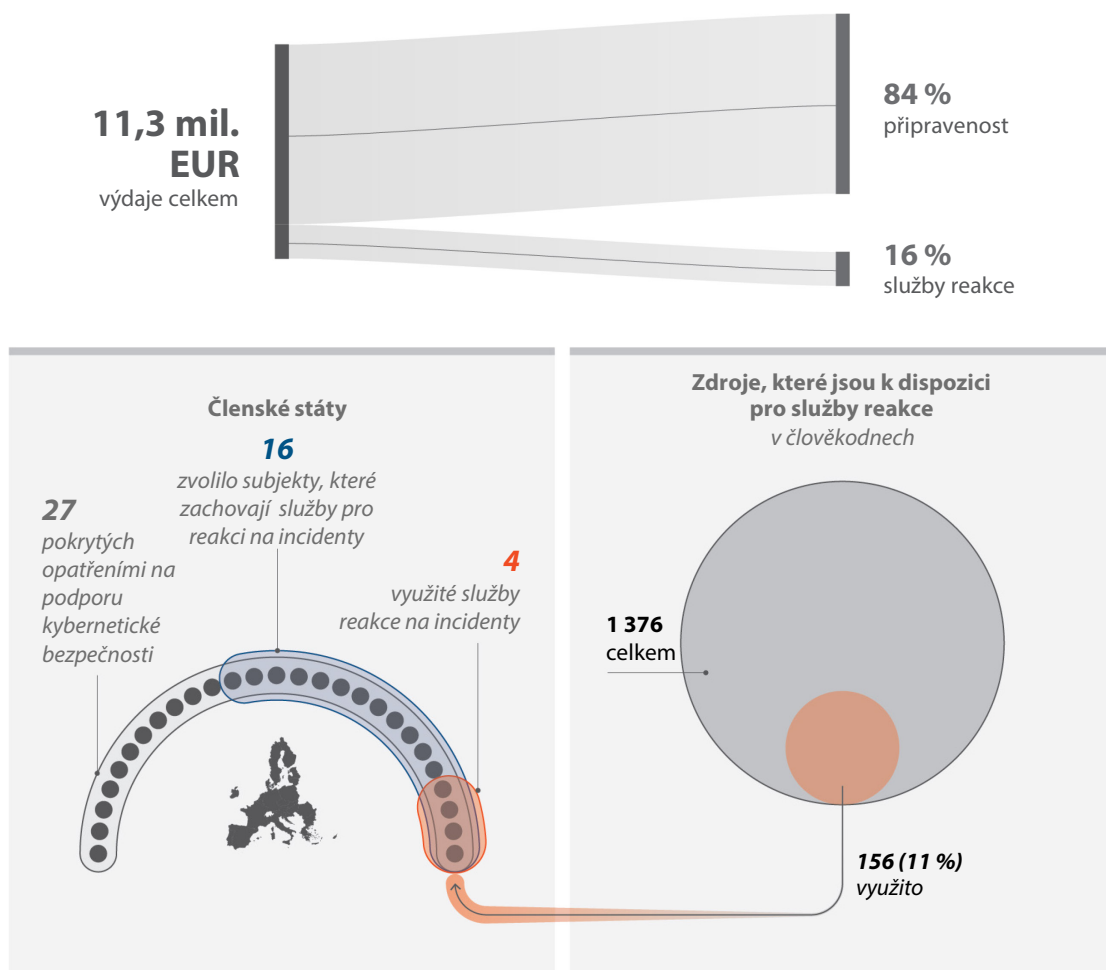
- 52** V době auditu neměla Komise ohledně podpory poskytované externími poskytovateli služeb v souvislosti s provozem střediska pro kybernetickou situaci po skončení platnosti smlouvy žádné plány. Domníváme se, že neexistence komplexního a podrobného plánu pro období po skončení platnosti smlouvy představuje riziko pro provoz střediska po roce 2026.

Rezerva EU pro kybernetickou bezpečnost umožňuje rychlé nasazení služeb reakce na incidenty

- 53** V roce 2022, bezprostředně po vojenské agresi Ruska vůči Ukrajině a s vědomím, že rozsáhlé kybernetické útoky jsou stále rozšířenější, poskytla Komise agentuře ENISA mimořádné finanční prostředky ve výši 15 milionů EUR na pilotní projekt [akce na podporu kybernetické bezpečnosti](#), která byla zahájena v roce 2023. V roce 2023 poskytla Komise další finanční prostředky (přibližně 20 milionů EUR) na prodloužení programu do konce roku 2026.
- 54** Komise rovněž navrhla [nařízení o kybernetické solidaritě](#) – přijaté v prosinci 2024 – s cílem připravit se na řešení rozsáhlých kybernetických bezpečnostních incidentů. Nařízení zřizuje rezervu EU pro kybernetickou bezpečnost, která zahrnuje služby reakce na incidenty od důvěryhodných poskytovatelů. Fungování rezervy začalo postupně v roce 2025 s rozpočtem 36 milionů EUR na období 2025–2027.
- 55** Posuzovali jsme, jak byl akční program na podporu kybernetické bezpečnosti organizován, protože tvoří základ rezervy EU pro kybernetickou bezpečnost. Rovněž jsme kontrolovali, zda při koncipování rezervy EU pro kybernetickou bezpečnost byly využity poznatky získané od roku 2022.
- 56** Agentura ENISA navrhla akci na podporu kybernetické bezpečnosti jako mechanismus pro poskytování služeb na podporu připravenosti a reakce členských států na rozsáhlé kybernetické bezpečnostní incidenty nebo krize. Všechny služby jsou agenturou ENISA předem smluvně dohodnuty, což znamená, že poskytovatelé služeb mohou začít pracovat, jakmile je členské státy potřebují. Je to také dáno systémem fungování agentury ENISA, který zajišťuje, aby byl nepřetržitě k dispozici pracovník, který řeší žádosti členských států.
- 57** Agentura ENISA se rozhodla rozdělit dostupný rozpočet mezi členské státy rovným dílem. V praxi agentura zahájila otevřené zadávací řízení rozdělené na 27 částí, jednu za každý členský stát, s cílem vybrat až tři soukromé poskytovatele bezpečnostních služeb, kteří budou poskytovat služby do konce roku 2026. Agentura ENISA dále vybrala některé poskytovatele v rámci celoevropské části s cílem poskytovat služby způsobilým zemím mimo EU, jakož i orgánům, institucím a jiným subjektům EU nebo podporovat reakci na přeshraniční incidenty.

- 58** Tento přístup umožnil agentuře ENISA zohlednit specifické národní požadavky, včetně jazykových znalostí, národních bezpečnostních prověrek nebo stávajícího působení v členských státech. Na druhé straně však poskytovatelé nebyli vybíráni tak, aby byli schopni poskytovat služby v celé EU, a proto je hlavní nevýhodou tohoto přístupu to, že pokud členský stát předem nasmlouvané služby nevyužije, nemůže být dostupný rozpočet určený na tyto služby v konkrétním členské státě použit na pomoc jinému členskému státu.
- 59** V případě akce na podporu kybernetické bezpečnosti si členské státy mohly vybrat služby připravenosti, nebo reakce, nebo kombinaci obojího. Členské státy se rozhodly využít dostupné finanční prostředky především ke zlepšení své připravenosti (84 % výdajů v roce 2023). Členské státy, které se rozhodly pro službu reakce na incidenty (tj. předem stanovenou danou dohodu s poskytovatelem, která zajišťuje, že členský stát má na požádání přístup ke službám poskytovatele pro rychlou reakci na incidenty v oblasti kybernetické bezpečnosti), ji využívaly zřídka, jak je znázorněno na [obrázku 4](#). Orgány ve třech navštívených členských státech ocenily řízení akce na podporu kybernetické bezpečnosti agenturou ENISA.

Obrázek 4 | Akce agentury ENISA na podporu kybernetické bezpečnosti do roku 2023



Zdroj: EÚD na základě údajů agentury ENISA.

- 60** Na období 2024–2026 požádalo o službu reakce na incidenty pouze devět členských států. Naše rozhovory s agenturou ENISA a orgány ve třech členských státech potvrdily, že výrazně upřednostňují činnosti v oblasti připravenosti.

- 61** Ačkoli cílem rezervy EU pro kybernetickou bezpečnost je především podpořit reakci a obnovu, pokud jde o závažné kybernetické bezpečnostní incidenty, předem příslibené služby z rezervy EU pro kybernetickou bezpečnost, které nejsou využívány pro reakci na incidenty, lze transformovat na služby připravenosti. Tento flexibilní přístup může zabránit tomu, aby předplacené služby zůstávaly nevyužity.
- 62** Domníváme se, že model zvolený pro rezervu EU pro kybernetickou bezpečnost vychází ze zkušeností získaných z akčního programu na podporu kybernetické bezpečnosti. Údaje o využívání akčního programu na podporu kybernetické bezpečnosti však poukazují na riziko, že rezerva EU pro kybernetickou bezpečnost by mohla být primárně využívána pro připravenost, a nikoli pro reakci, což je v rozporu s účelem stanoveným v aktu o kybernetické solidaritě.

Evropský systém varování v oblasti kybernetické bezpečnosti usiluje o zlepšení kapacity pro odhalování hrozeb, ale není funkční

- 63** Jedním z klíčových cílů Evropského systému varování v oblasti kybernetické bezpečnosti je podporovat smysluplné sdílení informací s cílem zlepšit odhalování a analýzu kybernetických hrozeb a reakci na ně. Účast v systému varování je dobrovolná, ale členské státy, které se rozhodnou připojit k přeshraničnímu kybernetickému středisku, se musí zavázat ke sdílení příslušných informací s ostatními členy. Díky spolupráci v klastrech v důvěryhodném a bezpečném prostředí by se členské státy mohly vyhnout některým problémům souvisejícím se sdílením informací uvedeným v bodech [32–45](#).
- 64** V době auditu se pro účast v Evropském systému varování v oblasti kybernetické bezpečnosti 13 rozhodlo členských států a zřídilo dvě přeshraniční centra: Athena a ENSOC. Třetí přeshraniční kybernetické centrum, NBCC, obdrželo finanční prostředky na své zřízení v roce 2026, čímž se počet členů sítě zvýšil na celkem 20 zemí (18 členských států a dále Island a Norsko¹⁰), jak je znázorněno na [obrázku 5](#).

¹⁰ Přidružené země mimo EU v souladu s čl. 10 odst. 1 písm. a) nařízení (EU) 2021/694.

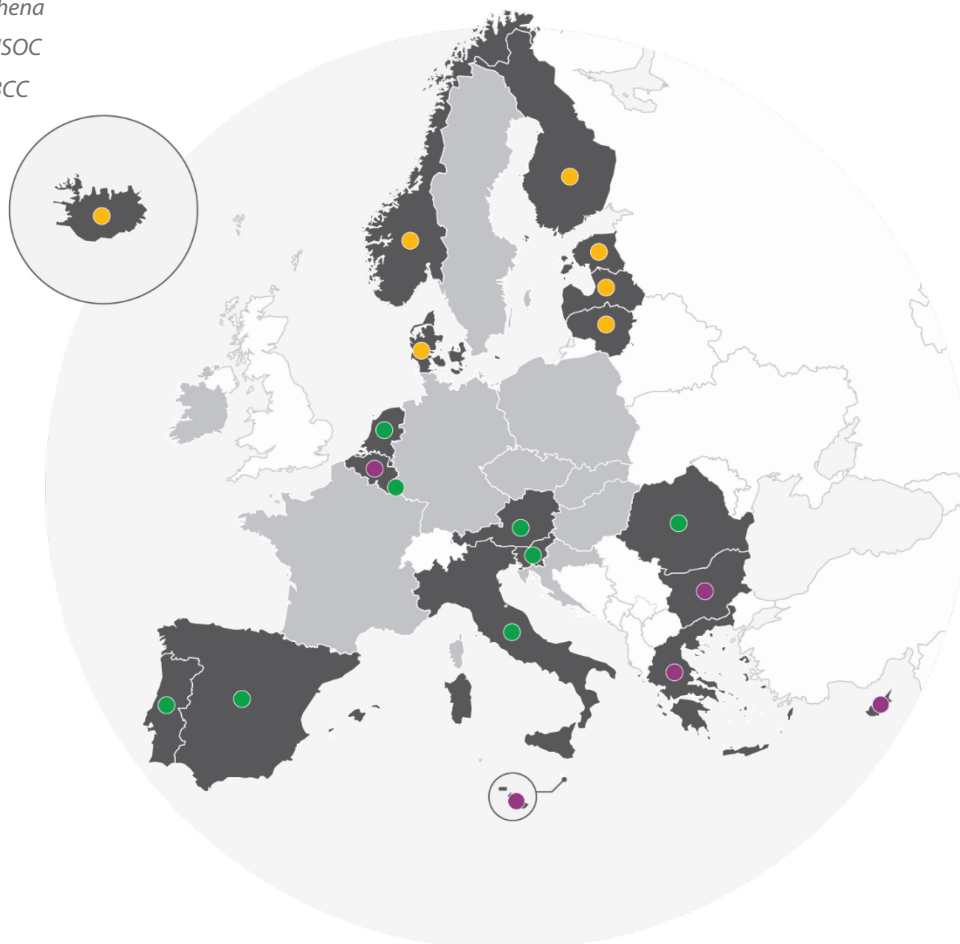
Obrázek 5 | Země v Evropském systému varování v oblasti kybernetické bezpečnosti

■ Země v Evropském systému varování v oblasti kybernetické bezpečnosti

● Athena

● ENSOC

● NBCC



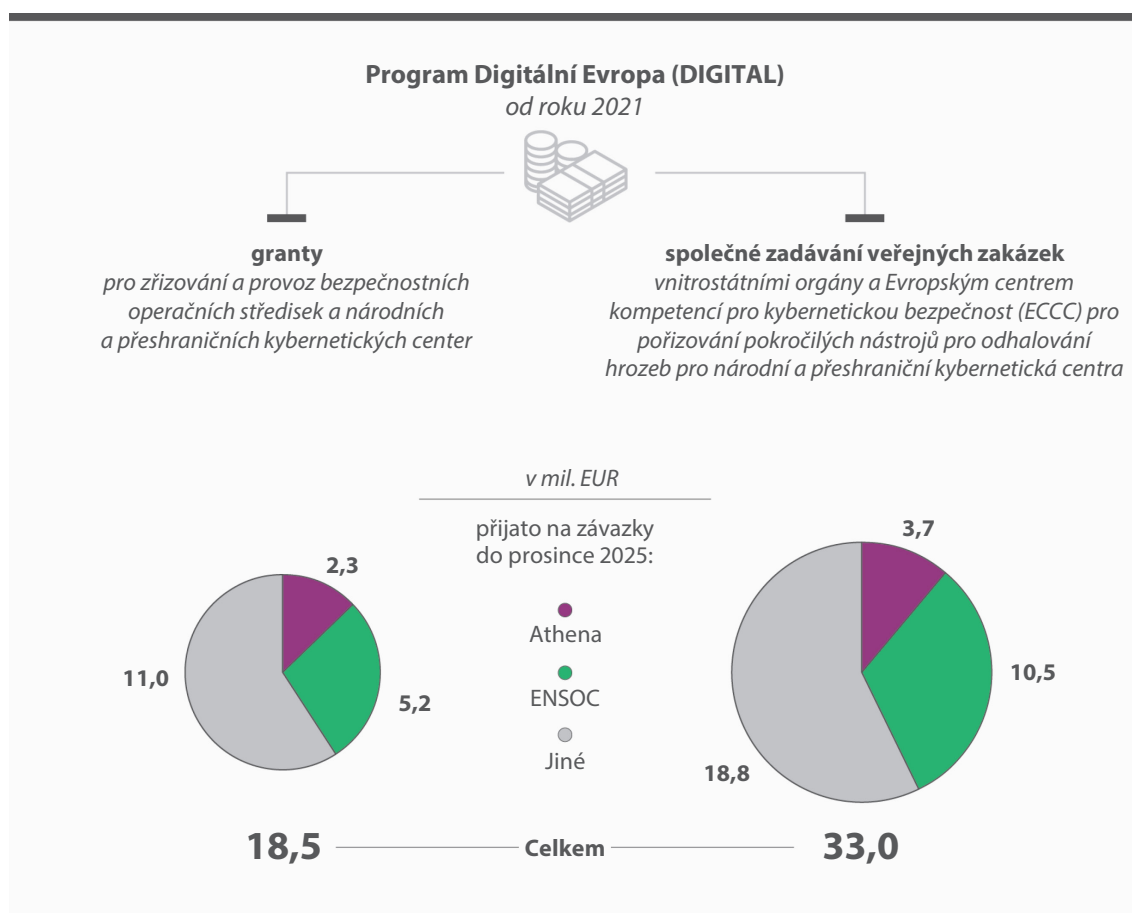
Zdroj: EÚD.

65 Posuzovali jsme, jak byla zřízena první dvě přeshraniční kybernetická centra, jakož i jejich pokrok při plnění cílů Evropského systému varování v oblasti kybernetické bezpečnosti. Zkoumali jsme také, jak zřízení přeshraničních kybernetických center zapadá do širšího prostředí kybernetické bezpečnosti a jak interaguje se stávajícími sítěmi a strukturami.

Vzhledem k podstatným zpožděním při zadávání veřejných zakázek nebylo dosud dosaženo žádných konkrétních výsledků

- 66** Finanční prostředky na podporu zřizování vnitrostátních a přeshraničních kybernetických center jsou od roku 2021 k dispozici prostřednictvím programu DIGITAL. Toto financování je poskytováno prostřednictvím složitého postupu se dvěma paralelními toky: tradiční granty na podporu zřizování a provoz center a společné zadávání veřejných zakázek na pořízení pokročilých nástrojů pro odhalování hrozeb, jak je znázorněno na [obrázku 6](#). Po výzvě k předkládání návrhů v listopadu 2022 Athena a ENSOC zahájily svou činnost v lednu 2024.

Obrázek 6 | Financování kybernetických center z programu Digitální Evropa



Zdroj: EÚD na základě údajů ECCC.

- 67** Členové Atheny a ENSOC, jakož i GR CNECT (první fáze) a nově zřízeného ECCC (druhá fáze) zorganizovali dvoufázová užší zadávací řízení¹¹. Cílem dvoufázového přístupu je omezit oběh citlivých informací tím, že se podrobné technické specifikace poskytnou pouze uchazečům vybraným v první fázi.

¹¹ Výzva k podávání nabídek týkající se sítě ENSOC a výzva k podávání nabídek týkající se mechanismu Atheny.

- 68** První fáze byla zahájena v květnu 2024 pro síť ENSOC a v červenci 2024 pro mechanismus Athena. Společnosti, které projevily zájem, měly na podání žádosti jeden měsíc. Úspěšní uchazeči však byli informováni až v dubnu 2025, téměř rok po zahájení řízení.
- 69** V té době dále nemohla zadávací řízení centra ENSOC, ani mechanismu Athena přejít do druhé fáze, neboť členové centra a ECCC nebyli schopni poskytnout společnostem zařazeným do užšího výběru technické specifikace nezbytné k tomu, aby mohly předložit nabídku, neboť stále pracovali na jejich dokončení.
- 70** Druhá fáze zadávacích řízení byla zahájena až v srpnu 2025 pro některé části ENSOC a pro Athena byla naplánována na začátek roku 2026. V době auditu, 18 měsíců po zahájení zadávacího řízení, nebyla podepsána smlouva na žádnou z těchto částí. Domníváme se, že nedostatečná příprava a složitost zadávacích řízení měly negativní dopad na jejich včasné dokončení.
- 71** Zjistili jsme, že přeshraniční uzly proto nejsou na dobré cestě k dosažení svých cílů. Bez nástrojů pro odhalování hrozeb a sdílení informací je jejich provoz pozastaven a Evropský systém varování v oblasti kybernetické bezpečnosti dosud nefunguje, což zpožďuje účinný rozvoj pokročilých schopností odhalovat kybernetické hrozby a incidenty a předcházet jim. Byly podepsány dodatky prodlužující dobu platnosti grantové dohody, aby se zohlednila dosavadní zpoždění v zadávacích řízeních (o 15 měsíců v případě mechanismu Athena a 18 měsíců v případě ENSOC).

Přeshraniční kybernetická centra vytvářejí další komunikační kanály, které dále zvyšují složitost

- 72** Jedním z klíčových úkolů přeshraničních kybernetických center je sdílet příslušné informace s cílem zlepšit odhalování hrozeb a reakci na ně. Jde například o informace o kybernetických hrozbách, zranitelných místech, indikátorech kompromitace a aktérech hrozeb. Úkoly přeshraničních kybernetických center se částečně překrývají s úkoly vnitrostátních týmů CSIRT a sítě CSIRT, zejména pokud jde o sdílení informací o kybernetických hrozbách a zranitelných místech. Mezi úlohami přeshraničních kybernetických center a týmů CSIRT neexistuje jasná hranice. Podle kybernetického plánu z roku 2025 (bod 30) mají přeshraniční kybernetická centra fungovat jak na technické (vnitrostátní týmy CSIRT a síť CSIRT), tak na provozní úrovni (EU-CyCLONE).

- 73** Akt o kybernetické solidaritě vyžaduje, aby přeshraniční kybernetická centra mezi sebou podepisovala dohody o spolupráci s cílem usnadnit sdílení informací. Agentura ENISA měla vydat pokyny pro interoperabilitu mezi přeshraničními kybernetickými centry do února 2026, jak vyžaduje nařízení o kybernetické solidaritě. Centrum ECCC mezitím v prosinci 2025 udělilo grant na vymezení technického rámce pro interoperabilitu mezi přeshraničními kybernetickými centry konsorciu (zahrnujícímu některé členy sítě ENSOC a mechanismu Athena). Pokyny a rámec však budou dokončeny až poté, co budou přeshraniční kybernetická centra v provozu. Jak jsme upozornili ve svém stanovisku z roku 2023 k návrhu nařízení o kybernetické solidaritě¹², je zde riziko, že bez rychlé dohody by mohly být vyvinuty vzájemně nekompatibilní systémy, což by vedlo ke zvýšeným nákladům.
- 74** Přeshraniční kybernetická centra jsou rovněž povinna bez zbytečného odkladu sdílet příslušné informace o rozsáhlých kybernetických bezpečnostních incidentech se sítí EU-CyCLONE a sítí CSIRT. Na úrovni členských států vytváří ustavení národních kybernetických center a účast v přeshraničních kybernetických centrech další úroveň komunikace. Složitost zvyšuje také koordinace se státy mimo EU¹³, které nejsou členy sítě CSIRT ani sítě EU-CyCLONE.
- 75** K dohodě o společné taxonomii a o způsobu sdílení informací a k zajištění interoperability jsou nezbytné jasné dohody o spolupráci. Zkušenosti získané ze sítě CSIRT ukazují, že se jedná o významnou výzvu. Zjistili jsme, že v době auditu nebyla dohodnuta žádná procesní ujednání o spolupráci a sdílení informací. Domníváme se, že zřízení národních a přeshraničních kybernetických center by mohlo podpořit účinnější sdílení informací. Začlenění přeshraničních center do již tak složitého prostředí kybernetické bezpečnosti však bude náročné a vyžaduje další komunikační kanály a ujednání o spolupráci.

¹² Stanovisko 02/2023 k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně, bod 26.

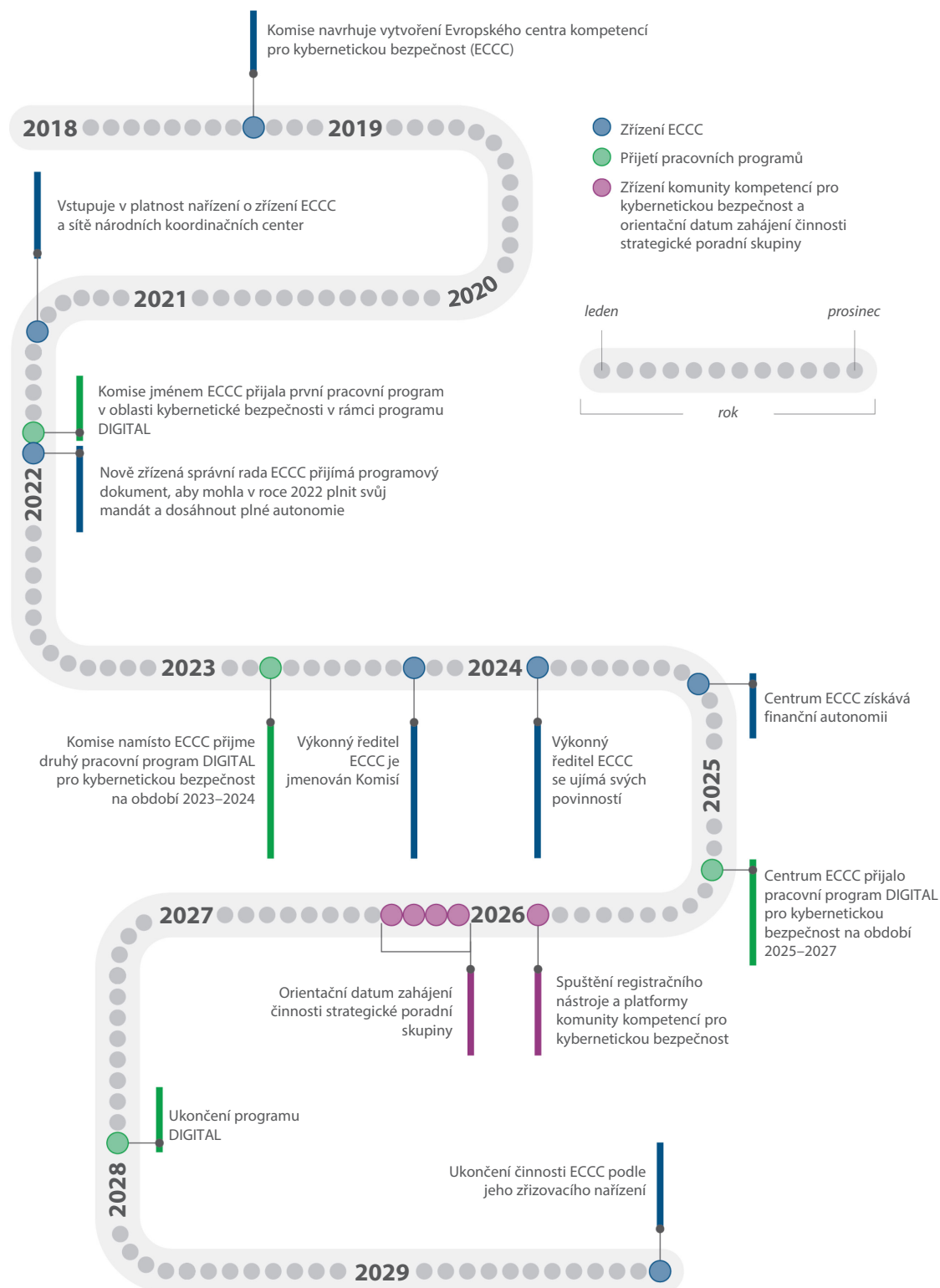
¹³ Island a Norsko.

Projekty financované EU v rámci programu DIGITAL mají za cíl posílit kybernetickou bezpečnost, ale potýkají se s problémy při provádění a podávání zpráv

Zpoždění při jeho zřizování znemožnilo komunitě kompetencí pro kybernetickou bezpečnost utvářet program DIGITAL podle svých potřeb

- 76** Za účelem řízení složky kybernetické bezpečnosti programu DIGITAL navrhla Komise v roce 2018 vytvoření Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC). Nařízení o ECCC předpokládalo, že ECCC bude podporováno sítí 29 národních koordinačních center, jedním v každém členském státě a dále na Islandu a v Norsku. Vyzval rovněž k vytvoření komunity kompetencí pro kybernetickou bezpečnost (dále jen „komunita“) složené ze zástupců průmyslu, akademických a výzkumných organizací, jakož i dalších příslušných sdružení občanské společnosti.
- 77** Do strategické poradní skupiny, která je jednou ze tří složek struktury ECCC, by bylo jmenováno až 20 členů komunity. Jedním z klíčových úkolů strategické poradní skupiny je organizovat veřejné konzultace, které budou podkladem pro program ECCC a pracovní plány programu DIGITAL.
- 78** Posuzovali jsme, zda DIGITAL a jeho pracovní programy byly přijaty na základě důkladné analýzy potřeb a jak byly k těmto pracovním programům schopny přispět centrum ECCC, síť národních koordinačních center, komunita a strategická poradní skupina. V praxi byly ECCC, síť národních koordinačních center, komunita a strategická poradní skupiny zřizovány postupně v průběhu několika let (viz [obrázek 7](#)).

Obrázek 7 | Časová osa zřízení Evropského centra kompetencí pro kybernetickou bezpečnost, sítě národních koordinačních center, komunity a strategické poradní skupiny



Zdroj: EÚD.

- 79** Vzhledem k tomu, že centrum ECCC začalo plně fungovat až v září 2024, přijala Komise jménem centra ECCC pracovní programy na období 2021–2022 a 2023–2024. Tyto dva pracovní programy přijaté Komisí nemohly využít příspěvku komunity.
- 80** Členské státy mezitím začaly zřizovat svá národní koordinační centra, která pro komunitu fungují jako kontaktní místa na národní úrovni. Jejich zřízení a provoz byly spolufinancovány programem DIGITAL, přičemž v době auditu bylo z finančních prostředků EU přiděleno více než 90 milionů EUR, včetně přibližně 44 milionů EUR, které budou dále rozděleny na finanční podporu třetím stranám. Do roku 2027 bylo na podporu národních koordinačních center vyčleněno dalších 38 milionů EUR.
- 81** Zjistili jsme, že v prosinci 2025, čtyři roky po zřízení centra ECCC a sítě národních koordinačních center, nebyla komunita zatím ustavena a strategická poradní skupina ještě nebyla jmenována. Dne 14. března 2025 přijalo centrum ECCC nejnovější pracovní program DIGITAL pro kybernetickou bezpečnost na období 2025–2027. Centrum ECCC sice připravilo a přijalo svůj pracovní program po rozsáhlých konzultacích s členskými státy a sítí národních koordinačních center, nemohlo však těžit z příspěvků a poradenství ze strany komunity nebo strategické poradní skupiny. To je v rozporu s ustanoveními jeho zakládajícího nařízení a my to považujeme za promarněnou příležitost.
- 82** DIGITAL má skončit v roce 2027, a pokud nebude jeho mandát prodloužen, očekává se, že ECCC v roce 2029 ukončí svou činnost. Proto by podpora sítě národních koordinačních center, komunity a strategické poradní skupiny, jakmile budou ustaveny, mohla být relevantní pouze po krátkou dobu.

Projekty financované EU sledují relevantní cíle, ale mnoho z nich se potýká s provozními problémy

- 83** Vybrali jsme vzorek 11 projektů relevantních pro odhalování kybernetických bezpečnostních incidentů a reakci na ně a financovaných v rámci programu DIGITAL v období 2022–2025 (viz [obrázek 5](#) v [příloze I](#) a [příloze III](#)). Posuzovali jsme, zda:
- cíle projektů byly v souladu s očekávanými výsledky vyjádřenými ve výzvách k předkládání návrhů a s celkovými přímými výsledky programu DIGITAL,
 - projekty dosud dosáhly plánovaných výstupů a výsledků,
 - výstupy projektů byly realizovány včas.

Výsledek tohoto posouzení uvádíme v [příloze IV](#).

Některé projekty vykazují první výsledky, ale mnoho z nich se potýká s provozními problémy a zpožděními

- 84** Zjistili jsme, že všechny projekty sledují cíle, které přispívají k dosažení cílů DIGITAL¹⁴ v oblasti kybernetické bezpečnosti, a že se zabývají většinou cílů výzev k podávání návrhů¹⁵.
- 85** Z 11 projektů v našem vzorku byly dva v rané fázi provádění, a proto jsme nemohli dospět k závěru o jejich výkonnosti. Ze zbývajících projektů jsme čtyři vyhodnotili jako uspokojivé z hlediska dosažení plánovaných výstupů a výsledků. Dva projekty vykazovaly podle našeho názoru určité nedostatky a tři jsme vyhodnotili jako neuspokojivé (viz [příloha IV](#)).
- 86** Cílem programu DIGITAL je výslovně zvýšit úroveň kybernetické bezpečnosti malých a středních podniků. V tomto ohledu nabízí několik projektů konkrétní řešení pro malé a střední podniky (viz [rámeček 2](#)).

¹⁴ Článek 6 nařízení (EU) 2021/694, kterým se zavádí program Digitální Evropa.

¹⁵ Výzvy k předkládání návrhů: Budování kapacit bezpečnostních operačních středisek; vývoj sítě národních koordinačních středisek s členskými státy; podpora připravenosti a vzájemná pomoc; nové aplikace umělé inteligence a další základní technologie pro bezpečnostní operační střediska.

Rámeček 2

Příklady projektů přinášejících hmatatelné výsledky malým a středním podnikům

Cílem projektu **GR-SME-SOC** (projekt 6 v *příloze III*) je poskytnout malým a středním podnikům v Řecku nástroje a služby v oblasti kybernetické bezpečnosti zřízením bezpečnostního operačního střediska přizpůsobeného jejich potřebám. Projekt byl zahájen v lednu 2024 a provádí jej konsorcium pěti řeckých organizací. Plánuje se, že po dobu jednoho roku budou 120 malým a středním podnikům bezplatně nabízeny služby v oblasti kybernetické bezpečnosti a po uplynutí této doby budou tyto služby dostupné komerčně. Projekt nabízí malým a středním podnikům pokročilé služby, jako je monitorování v reálném čase, odhalování hrozeb na základě umělé inteligence a agilní reakce na incidenty.

V rámci projektu **NCC-IE** (projekt 3 v *příloze III*) poskytl koordinátor projektu více než 50 irským malým a středním podnikům granty ve výši přibližně 1,8 milionu EUR na zlepšení jejich kybernetické bezpečnosti. Z grantového programu měly prospěch společnosti se 2 až přibližně 200 zaměstnanci, včetně rodinných podniků, začínajících podniků a globálních vývozců v různých odvětvích. Granty byly určeny výhradně společnostem, které předtím prošly přezkumem kybernetické bezpečnosti řízeným vládní agenturou Enterprise Ireland. Grant pokrýval 80 % nákladů (do výše 60 000 EUR) na provedení doporučení z přezkumu.

Zdroj: EÚD.

- 87** Mnoho projektů v našem vzorku má potíže s dodržováním lhůt nebo se potýká s provozními problémy (viz *příloha IV*). Zjistili jsme, že čtyři projekty jsou významně zpožděny. To zahrnuje ENSOC a mechanismus Athena, jak je podrobně uvedeno v bodech **66–71**. V *rámečku 3* uvádíme další příklady.

Rámeček 3

Příklady projektů potýkajících se s provozními problémy a zpožděními

V Irsku je jediným příjemcem grantu na projekt **ILG-SOC** (projekt 8 v [příloze III](#)) místní správní orgán (LGMA). Cílem projektu je zřídit ústřední bezpečnostní operační středisko pro 31 místních orgánů, které budou pro odhalování hrozeb a reakci na ně využívat pokročilé nástroje. Projekt byl zahájen v říjnu 2023 a trval tři roky. Výsledkem přezkumu v polovině období bylo odmítnutí všech předmětů dodávky. Projekt zahrnuje několik zadávacích řízení, která nebyla úspěšná nebo se zpozdila. Doba trvání projektu bude prodloužena (bez dodatečného financování), což by mohlo poskytnout dostatek času na jeho úspěšné dokončení.

V Řecku je cílem projektu **EL-SOC** (projekt 5 v [příloze III](#)) zřídit konsolidované bezpečnostní operační středisko na národní úrovni, které by shromažďovalo informace od odvětvových bezpečnostních operačních středisek. To by zajišťovalo komplexní přehled o situaci v oblasti kybernetické bezpečnosti v reálném čase. Projekt byl realizován od ledna 2024 do prosince 2026. Plánované zadávání veřejných zakázek na hardware a služby se zpozdilo kvůli problémům s dokončením a zveřejněním technických specifikací pro výzvu k podávání nabídek. Jako důvod zpoždění koordinátor projektu rovněž uvedl problémy související se zajištěním národního spolufinancování a omezenou dostupností pracovníků pro zadávání veřejných zakázek.

Zdroj: EÚD.

- 88** Dva další projekty v našem vzorku se potýkají s mírným zpožděním. Výstupy tří projektů byly realizovány včas. Dva projekty jsou v počáteční fázi provádění, a proto u nich nemůžeme vyjádřit žádný závěr.

Bezpečnostní omezení vedla k provozním problémům a s kontrolami prováděnými příjemci se pojí významná rizika

- 89** Nařízení DIGITAL stanoví, že z bezpečnostních důvodů může být financování kybernetické bezpečnosti omezeno na subjekty, které jsou usazeny v EU a kontrolovány členskými státy nebo občany EU. Cílem tohoto omezení je zmírnit riziko vniknutí nebo vlivu států mimo EU a zabránit sdílení citlivých bezpečnostních informací s orgány zemí mimo EU.

- 90** Závazek týkající se unijních požadavků v oblasti vlastnictví a kontroly se vztahuje nejen na příjemce grantů, ale také na jejich subdodavatele a případné příjemce finanční podpory poskytované třetím stranám (FSTP). S výjimkou druhé jmenované kategorie (viz body [93–97](#)) provádí posouzení Centrální ověřovací služba [Evropské výkonné agentury pro výzkum](#). Konečné rozhodnutí o způsobilosti k účasti ve výzvách v rámci užších zadávacích řízení je však stále na orgánu poskytujícím podporu, tj. GŘ CNECT nebo ECCC.
- 91** Během naší auditní činnosti příjemci opakovaně zmiňovali praktické problémy spojené s posuzováním vlastnictví a kontroly. Posouzení unijních požadavků týkajících se vlastnictví a kontroly může být složitý a zdoluhavý proces. Vyžaduje analýzu celé vlastnické struktury a řetězce kontroly každé organizace, včetně všech úrovní vlastnictví až po konečné vlastníky. Centrální ověřovací služba vyžaduje, aby každý subjekt předložil rozsáhlé [písemné doklady](#) o své vlastnické struktuře a konkrétních právech, správě a řízení společnosti a o veškerých obchodních, finančních nebo jiných vazbách poskytujících kontrolu.
- 92** U tří projektů financovaných EU v našem vzorku byl později vyloučen minimálně jeden příjemce konsorcia, protože se mělo za to, že je vlastněn nebo ovládán ze země mimo EU. Vyloučení členů konsorcia ukazuje, že ne všichni účastníci programu DIGITAL plně chápou koncept unijních požadavků týkajících se vlastnictví a kontroly. Na základě údajů Centrální ověřovací služby celkově 7 % všech žadatelů o grant na kybernetickou bezpečnost z programu DIGITAL nebo jejich subdodavatelů v období 2022–2025 v posouzení neuspělo. Podání žádostí nezpůsobilými účastníky v rámci výzvy k předkládání návrhů způsobuje zpoždění, jak je znázorněno v [rámečku 4](#).

Rámeček 4

Příklad případu, kdy byli příjemci vyloučeni poté, co neprošli bezpečnostními kontrolami

Dva členové konsorcia projektu [NG-SOC](#) (projekt 7 v [příloze III](#)) v posouzení unijních požadavků týkajících se vlastnictví a kontroly neuspěli. Výsledek byl oznámen přibližně měsíc před uplynutím lhůty pro podpis grantové dohody. Koordinátor projektu musel souhlasit s převzetím práce, která byla přidělena dvěma vyloučeným členům, protože nebyl čas najít nového partnera. Jeden z vyloučených členů působil ve specifickém odvětví, kde mělo být vyvinuté řešení pilotně vyzkoušeno. Významná část projektu, která se týkala testování řešení v praxi, proto nemohla pokračovat tak, jak bylo zamýšleno. Tato situace byla později napravena změnou grantové dohody tak, aby zahrnovala nové členy.

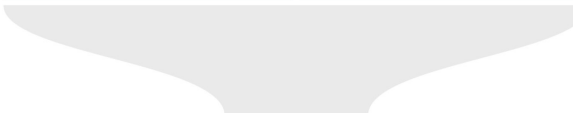
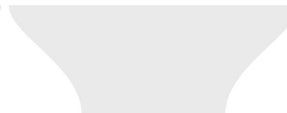
- 93** Dva z projektů, které jsme prověřovali (NCC-IE a CYberSynchrony), poskytují finanční podporu třetím stranám (FSTP). Tento mechanismus financování umožňuje příjemcům grantů využít část grantového financování k financování jiných subjektů prostřednictvím otevřených výzev. FSTP může usnadnit přístup k finančním prostředkům EU. V tomto případě nesou výlučnou odpovědnost za provedení posouzení vlastnictví a kontroly tito příjemci, Centrální ověřovací služba do něj není zapojena.
- 94** V roce 2021 zveřejnila Komise obecné pokyny pro žadatele ve výzvách v rámci užších zadávacích řízení, které byly aktualizovány v roce 2026. Ačkoli FSTP funguje pro výzvy v rámci programu DIGITAL od roku 2021, Komise ani centrum ECCC neposkytly příjemcům podrobnou metodiku, jak provádět posouzení unijních požadavků týkajících se vlastnictví a kontroly ve vztahu k třetím stranám, kterým poskytují finanční podporu. V červenci 2025 sdílelo centrum ECCC nepovinné pokyny, a síť národních koordinačních center tak poskytlo k posuzování unijních požadavků týkajících se vlastnictví a kontroly strukturovaný přístup. Pokyny obsahují obecné zásady a kroky, které lze učinit. Pokyny však neupřesňují, jak by měly být kontroly prováděny, a ponechávají na příjemcích odpovědnost za vypracování vlastního přístupu.
- 95** Zjistili jsme, že centrum ECCC nepotvrzuje metodiku přijatou příjemci ani neprovádí kontroly na základě vzorku, aby se ujistilo, že metodika je dostatečně spolehlivá a že vybraní příjemci finanční podpory skutečně splňují unijní požadavky týkající se vlastnictví a kontroly.
- 96** Ve [výroční zprávě za rok 2024](#) jsme uvedli, že příjemci pověření Komisí řízením finanční podpory určené třetím stranám (v oblasti výzkumu) nejsou povinni prokazovat účinnost svých kontrol k zajištění správnosti výdajů EU. Stejně tak centrum ECCC neposuzuje, zda mají příjemci správnou a technickou kapacitu tato posouzení unijních požadavků týkajících se vlastnictví a kontroly řádně řídit. Jak je podrobně uvedeno v bodě [91](#), toto posouzení může být složité a na úrovni EU je provádí zvláštní útvar se specializovanými odbornými znalostmi.
- 97** Za této situace se domníváme, že existuje značné riziko, že příjemci, kteří jsou odpovědní za provádění kontrol unijních požadavků týkajících se vlastnictví a kontroly, nemají kapacitu tyto kontroly řádně provádět. Vzhledem k povaze financovaných činností by tento nedostatek mohl exponovat citlivou infrastrukturu, provozní údaje a technologie kritické z hlediska bezpečnosti.

Většina projektů financovaných EU nemá odpovídající výkonnostní rámce a údaje DIGITAL o výkonnosti v oblasti kybernetické bezpečnosti nejsou přesné

Většina projektů financovaných EU nemá odpovídající výkonnostní rámce

- 98** Příjemci, kteří řídí projekty financované EU, musí ECCC podávat zprávy o svém pokroku a výsledcích s využitím milníků, předmětů dodávky a ukazatelů, jak je znázorněno na [obrázku 8](#). Posuzovali jsme, zda milníky a předměty dodávky stanovené pro každý projekt odpovídajícím způsobem umožňují monitorování projektů. Posuzovali jsme také, zda jsou jejich ukazatele výkonnosti relevantní a měřitelné a zda mají výchozí hodnotu a cíl.

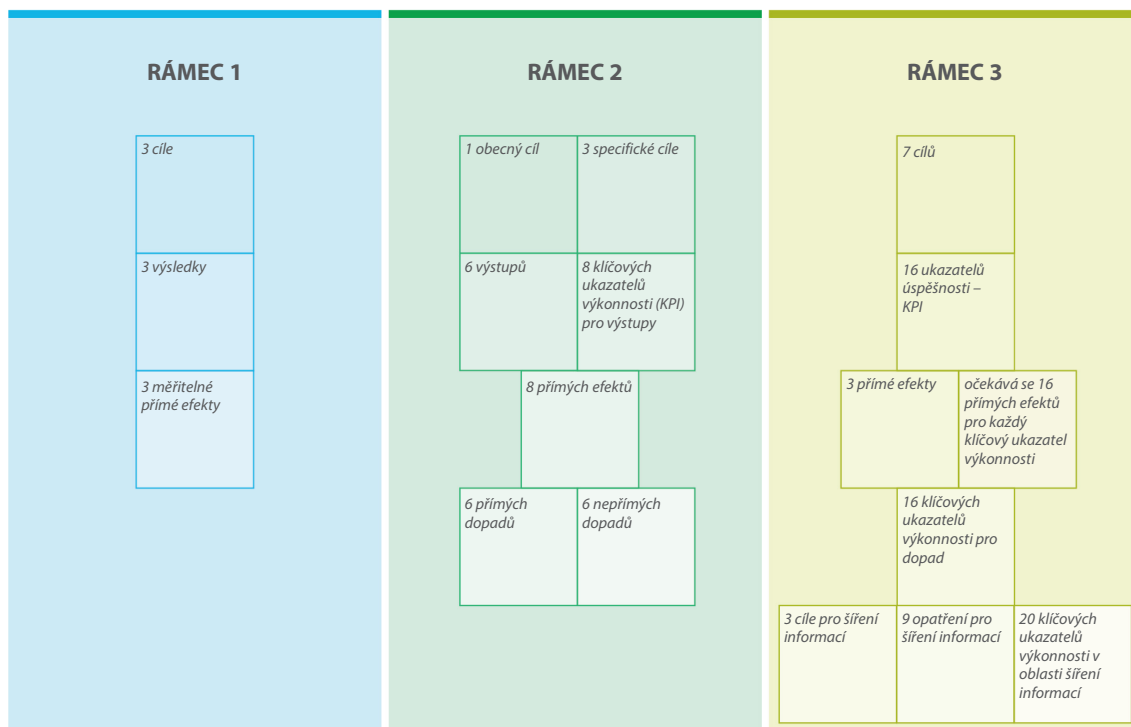
Obrázek 8 | Milníky, předměty dodávky a ukazatele výkonnosti v projektech programu DIGITAL

	 Milníky	 Předměty dodávek	 Ukazatele výkonnosti
Oč jde	kontrolní body v průběhu projektu, které pomáhají mapovat pokrok	předložené výstupy projektu prokazující pokrok	slouží k měření výsledků
Jak je nastavit	souvisí pouze s hlavními (početně omezenými) výstupy	pouze významné výstupy (10 až 15 max. na projekt)	konkrétní, měřitelné, dosažitelné, relevantní a časově vymezené
Příklady	„zahájení pilotní fáze platformy“	„příručka pro uživatele platformy“	„30% zkrácení doby reakce na incident“
	 Strukturovaný přístup, součást on-line systému řízení grantů		 Nestrukturovaný přístup

Zdroj: ECA na základě [formuláře grantové žádosti](#).

- 99** Ve svém návrhu projektu musí příjemci stanovit řadu milníků a předmětů dodávky na základě strukturovaného přístupu uvedeného v pokynech pro žadatele. Všechny milníky a předměty dodávky jsou uvedeny v online systému pro řízení grantů, aby se usnadnila následná kontrola. Centrum ECCC obvykle přezkoumává každý projekt dvakrát: jednou v polovině projektu a jednou po jeho dokončení. Během těchto přezkumů externí odborníci ověřují dosažení milníků a realizaci předmětů dodávky a centrum ECCC je potvrzuje. Milníky a předměty dodávky jsou proto klíčem k monitorování projektů a měly by být řádně stanoveny.
- 100** Zjistili jsme, že téměř žádný z projektů v našem vzorku se neřídil pokyny týkajícími se počtu milníků a předmětů dodávky: počet milníků na projekt se pohybuje od 8 do 39, zatímco počet předmětů dodávky se pohybuje od 8 do 45. Mnoho milníků a předmětů dodávky nebylo vypracováno v souladu s pokyny, a nejsou proto užitečné pro sledování pokroku (například „schůzka za účelem zahájení vypracování výzvy k předkládání návrhů na výzkum“ nebo „úřední zápis ze schůze k projektu“). U tří projektů hodnotící výbor tyto problémy zjistil před podpisem grantu. Ve dvou případech příjemci navrhli pouze drobné změny (např. lhůt), aniž by řešili hlavní problémy, zatímco ve třetím případě nebyly provedeny žádné změny. U šesti dalších projektů v našem vzorku z naší analýzy vyplývá, že milníky nebo předměty dodávky nejsou v souladu s pokyny a nejsou vždy přiměřené. Domníváme se, že špatně definované předměty dodávky nebo milníky nebo příliš velký počet milníků a předmětů dodávky ztěžuje sledování pokroku.
- 101** Na rozdíl od milníků a předmětů dodávky se ukazatele výkonnosti neřídí strukturovaným přístupem a nejsou konsolidovány v tabulce v systému řízení grantů, ale lze je nalézt v různých oddílech návrhu. Tento přístup vedl k tomu, že příjemci navrhli velké množství výkonnostních rámců. Zatímco někteří stanovili pouze projektové cíle spojené s ukazateli výkonnosti, jiní zřídili mnohem složitější výkonnostní rámce. Několik příkladů uvádíme níže na [obrázku 9](#).

Obrázek 9 | Příklad různých výkonnostních rámců navržených pro projekty



Zdroj: EÚD.

102 Na základě naší analýzy jsme dospěli k závěru, že řada ukazatelů výkonnosti používaných v projektech není relevantních nebo měřitelných a chybí jim cíl nebo základní hodnota (viz [rámeček 5](#)). Sedm projektů navíc definovalo 20 nebo více ukazatelů, přičemž jeden projekt má 52 ukazatelů. Výsledek tohoto posouzení uvádíme v [příloze IV](#).

Rámeček 5

Příklady nedostatečných ukazatelů výkonnosti

Neměřitelné:

- „Indikátor kompromitace a dalších poskytovaných služeb posiluje kapacity malých a středních podniků v oblasti kybernetické bezpečnosti“
- „Poskytování nástrojů a metod reakce na incidenty umožňujících integraci s komunikačními kanály sítě EU-CyCLONe“

Není k dispozici základní hodnota nebo cíl:

- „≥ 20% zlepšení připravenosti zaměstnanců“
- „≥ 20% snížení úsilí potřebného k zajištění souladu s příslušnými iniciativami EU v oblasti kybernetické bezpečnosti“

Nesouvisející s výkonností:

- „Závěrečná zpráva o projektu na konci fáze financování“
- „Počet osob, které se zúčastní veškeré odborné přípravy“

Zdroj: EÚD na základě projektové dokumentace.

103 Celkově se domníváme, že monitorování výkonnosti značně komplikuje široká škála výkonnostních rámců, špatné nastavení ukazatelů a jejich nadměrný počet. Není proto možné výkonnost projektu řádně posoudit. To je dále komplikováno skutečností, že šablona pro podávání zpráv neobsahuje zvláštní oddíl o ukazatelích výkonnosti projektů, a většina projektů v našem vzorku je proto nevykazovala.

Údaje o výkonnosti složky kybernetické bezpečnosti programu DIGITAL nejsou přesné

- 104** Za účelem sledování výsledků programu DIGITAL stanoví nařízení programové ukazatele, o nichž musí všechny projekty podávat zprávy, jak je podrobně uvedeno v [rámečku 6](#).

Rámeček 6

Ukazatele programu DIGITAL pro kybernetickou bezpečnost

- 1.a Počet infrastruktur nebo nástrojů kybernetické bezpečnosti nebo obojího pořízených společně, a to i v rámci Evropského systému varování v oblasti kybernetické bezpečnosti
- 1.b Počet zavedených infrastruktur nebo nástrojů kybernetické bezpečnosti nebo obojího
2. Počet uživatelů a uživatelských komunit s přístupem k evropským zařízením kybernetické bezpečnosti
3. Počet akcí na podporu připravenosti a reakce na kybernetické bezpečnostní incidenty v rámci mechanismu pro mimořádné události v oblasti kybernetické bezpečnosti

Zdroj: Příloha II [nařízení \(EU\) 2021/694, kterým se zavádí program Digitální Evropa](#); rámec pro monitorování a hodnocení programu Digitální Evropa ([SWD\(2024\)37](#)).

- 105** Posuzovali jsme, zda projekty v našem vzorku o těchto ukazatelích informovaly, a zkoumali jsme, jak centrum ECCC tyto údaje shromažďuje a ověřuje.
- 106** Všechny projekty musí podávat zprávy o ukazatelích programu DIGITAL před přezkumem v polovině období a konečným přezkumem v systému řízení grantů. Zjistili jsme, že ze sedmi projektů, které byly během našeho auditu v polovině doby provádění, a měly tudíž o těchto ukazatelích podávat zprávy, tak učinily pouze tři. Z těchto tří projektů dva nevykázaly přesné informace: jeden vykázal nesprávný ukazatel, druhý uvedl pouze cílové hodnoty namísto dosažených výsledků.

107 Komise o těchto ukazatelích každoročně informuje ve svých [prohlášeních o výkonnosti programů](#). To zúčastněným stranám umožňuje posoudit, zda program plní své cíle. Podle prohlášení o výkonnosti programů za rok 2024 jsou ukazatele programu DIGITAL pro kybernetickou bezpečnost na dobré cestě. Centrum ECCC nám vysvětlilo, že při kompilaci těchto ukazatelů použilo řadu průzkumů zaslaných příjemcům projektů, místo aby vycházelo ze systému řízení grantů. Přezkoumali jsme rozčleněné údaje poskytnuté centrem ECCC a zjistili jsme řadu problémů týkajících se způsobu shromažďování údajů a jejich celkové kvality. Zjistili jsme, že shromážděné údaje neodpovídají hodnotám uvedeným v prohlášení o výkonnosti programu, takže není jasné, jak byly vykázané hodnoty vypočteny. Nenašli jsme žádné důkazní informace o tom, že by centrum ECCC ověřovalo přesnost vykázaných údajů. Na základě kontrol projektů v našem vzorku se domníváme, že vzhledem k tomu, že většina hodnot chybí nebo je nepřesná, vykázané údaje řádně neodrážejí dosažené výsledky.

Tuto zprávu přijal v Lucemburku na svém zasedání dne 16. června 2026 senát III, jemuž předsedá člen Účetního dvora George-Marius Hyzler.

Za Účetní dvůr

Tony Murphy
předseda

Přílohy

Příloha I – O auditu

- 01** Akt EU o kybernetické bezpečnosti¹ definuje kybernetickou bezpečnost jako „činnosti nezbytné k ochraně sítí a informačních systémů, jejich uživatelů a dalších osob dotčených kybernetickými hrozbami“. Kybernetickou hrozbou se rozumí „jakákoliv potenciální okolnost, událost nebo čin, které mohou poškodit, narušit nebo jinak nepříznivě ovlivnit sítě a informační systémy, jejich uživatele a další osoby“². Kybernetická bezpečnost vyžaduje holistický přístup sestávající z řady vzájemně souvisejících činností, jejichž cílem je předcházet kybernetickým hrozbám, odhalovat je, reagovat na ně a zotavit se z nich, jak je znázorněno na [obrázku 1](#) níže.

¹ Nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti).

² Článek 2 aktu o kybernetické bezpečnosti.

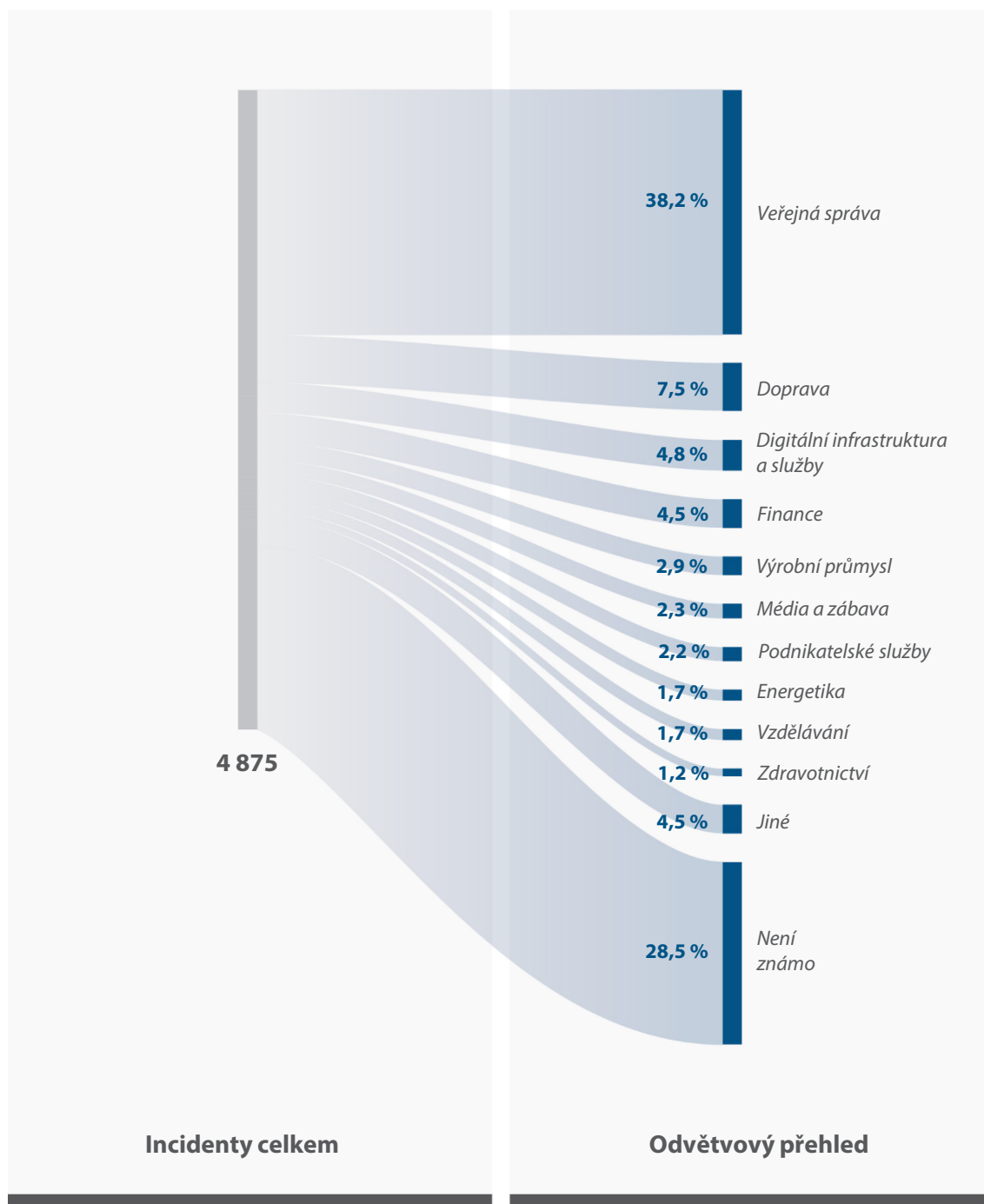
Obrázek 1 | Příklady činností v oblasti kybernetické bezpečnosti

Prevence 	Snížení rizika kybernetických bezpečnostních incidentů a minimalizace jejich potenciálních účinků <i>Příklady: antivirový program, firewally, šifrování, dvoufaktorová autentizace, správa aktualizací softwaru, školení zaměstnanců v oblasti zvyšování povědomí o bezpečnosti</i>
Odhalování 	Odhalování škodlivé činnosti <i>Příklady: monitorování sítě, povědomí o situaci</i>
Reakce 	Řízení a zmírňování kybernetického bezpečnostního incidentu omezením hrozby a prevencí dalších škod <i>Příklady: odstranění hrozby, omezení hrozby izolací serverů, deaktivace narušených účtů a resetování hesel</i>
Obnova 	Obnovení bezpečnosti a provozuschopnosti dotčených systémů, dat a služeb <i>Příklady: opětovná instalace operačních systémů na dotčených serverech, obnova dat ze záloh, vyvození získaných zkušeností, aktualizace politik</i>

Zdroj: EÚD na základě 78. bodu odůvodnění směrnice (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti (směrnice NIS 2).

- 02** [Agentura Evropské unie pro kybernetickou bezpečnost \(ENISA\)](#) považuje úroveň kybernetických bezpečnostních hrozeb za významnou, přičemž konstatuje, že prostředí kybernetických bezpečnostních hrozeb se zkomplikovalo a jeho složitost stále narůstá³. Tyto hrozby zdůrazňují zásadní význam kybernetické bezpečnosti ve stále více digitalizovaných ekonomikách a společnostech. Agentura ENISA ve své [zprávě o prostředí hrozeb](#) z roku 2025 označila za nejkritičtější hrozbu v EU ransomware. Odvětví, na něž se hrozby soustřeďují, jsou uvedeny na [obrázku 2](#).

³ Zpráva agentury ENISA o stavu kybernetické bezpečnosti v Unii za rok 2024.

Obrázek 2 | Odvětví, na něž se zaměřují kybernetické útoky

Zdroj: EÚD na základě informací agentury ENISA.

Významné a rozsáhlé kybernetické bezpečnostní incidenty

03 Kybernetické bezpečnostní incidenty, k nimž patří kybernetické hrozby a neúmyslné události (jako jsou události uvedené na [obrázku 3](#) a v bodě [41](#)), „[m]ohou narušit poskytování veřejných služeb [a] i výkon hospodářských činností [...], způsobit značné finanční ztráty, podkopat důvěru uživatelů, způsobit velké škody hospodářství a demokratickým systémům Unie a mohou mít i následky ohrožující zdraví nebo život“⁴. Kybernetický bezpečnostní incident se považuje za⁵:

- **významný**, pokud dotčenému subjektu způsobil nebo by mohl způsobit závažné provozní narušení služeb nebo finanční ztrátu nebo pokud ovlivnil nebo by mohl ovlivnit jiné fyzické nebo právnické osoby tím, že by způsobil značnou hmotnou či nehmotnou újmu,
- **rozsáhlý**, pokud způsobil míru narušení, která přesahuje schopnost členského státu reagovat nebo která významně ovlivňuje nejméně dva členské státy.

04 Rozsáhlý kybernetický bezpečnostní incident může vyústit v plnohodnotnou **kybernetickou krizi EU**, pokud brání řádnému fungování vnitřního trhu nebo představuje závažná rizika pro veřejnou bezpečnost a ochranu subjektů nebo občanů v několika členských státech nebo v EU jako celku⁶.

⁴ 2. bod odůvodnění nařízení (EU) 2025/38 ([akt o kybernetické solidaritě](#)).

⁵ Články 6 a 23 [směrnice NIS 2](#), dále upřesněné v [prováděcím nařízení Komise \(EU\) 2024/2690](#) pro řadu poskytovatelů v odvětví digitální infrastruktury.

⁶ 69. bod odůvodnění [směrnice NIS 2](#).

Rámec politiky EU

- 05** Kybernetický ekosystém EU je složitý a mnohovýrovný, prochází celou řadou oblastí vnitřních politik, jako je spravedlnost a vnitřní věci, jednotný digitální trh a politiky v oblasti výzkumu⁷. Ve vnější politice má kybernetická bezpečnost svou úlohu v diplomacii a je stále více součástí rozvíjející se obranné politiky EU⁸.
- 06** EU v nedávné době posílila svůj regulační rámec pro oblast kybernetické bezpečnosti. Nejdůležitější právní předpisy a politické nástroje na úrovni EU představuje **obrázek 3**. V souladu s rozsahem našeho auditu (viz body **13–15**) jsme se zaměřili na nástroje, které se zabývají odhalováním významných a rozsáhlých kybernetických bezpečnostních incidentů a reakcí na ně.

⁷ Informační dokument EÚD – Výzvy týkající se účinné politiky EU v oblasti kybernetické bezpečnosti, s. 12.

⁸ Například *Kybernetická pozice Evropské unie* (2022), *rámec pro koordinovanou reakci EU na hybridní kampaně* (2022), *politika EU v oblasti kybernetické obrany* (2023) a *revidovaný soubor nástrojů pro diplomacii v oblasti kybernetiky* (2023).

Obrázek 3 | Příslušné právní předpisy a politické nástroje EU

- Přijímání právních předpisů a politických nástrojů
- Vytváření sítí a struktur



Zdroj: EÚD.

Úlohy a odpovědnost

- 07** V prostředí kybernetické bezpečnosti EU se pohybuje velké množství soukromých i veřejných subjektů působících v civilní sféře na regionální, národní i unijní úrovni, včetně donucovacích orgánů. Kybernetická bezpečnost je také klíčovým prvkem národní bezpečnosti a obrany⁹. Současná situace v EU je znázorněna v [příloze II](#).
- 08** Hlavní odpovědnost za prevenci kybernetických bezpečnostních incidentů a krizí, které je postihují, a za přípravu a reakci na ně nesou členské státy. V souladu s [čl. 4 odst. 2 Smlouvy o Evropské unii](#) zůstává národní bezpečnost výhradní odpovědností každého členského státu. Vzhledem k tomu, že kybernetické bezpečnostní incidenty by mohly narušit a poškodit kritickou informační infrastrukturu, na níž závisí hladké fungování vnitřního trhu, hraje v případě významného incidentu nebo krize důležitou úlohu také EU¹⁰. Hlavní aktéři na úrovni EU jsou uvedeni níže na [obrázku 4](#).

⁹ Stanovisko 02/2023 k navrhovanému aktu o kybernetické solidaritě.

¹⁰ Plán EU pro řešení kybernetických bezpečnostních krizí.

Obrázek 4 | Subjekty na úrovni EU s klíčovou úlohou v oblasti kybernetické bezpečnosti



Zdroj: EÚD.

Financování EU

- 09** Ve stávajícím víceletém finančním rámci na období 2021–2027 je hlavním zdrojem financování kybernetické bezpečnosti [program Digitální Evropa \(DIGITAL\)](#). Jedná se o první program EU, jehož konkrétním cílem je podpořit digitální transformaci EU. Zahájen byl v roce 2021 a jeho celkový rozpočet činí 8,1 miliardy EUR¹¹.
- 10** Z prostředků programu DIGITAL se financují opatření v oblasti kybernetické bezpečnosti v rámci jeho specifického cíle č. 3 – „Kybernetická bezpečnost a důvěra“. Rozpočet konkrétně činí 1,4 miliardy EUR a je určený na:
- posílení koordinace kybernetické bezpečnosti mezi nástroji a datovými infrastrukturami členských států,
 - podporu obecného zavádění řešení kybernetické bezpečnosti napříč celou ekonomikou.
- 11** Většina finančních prostředků programu DIGITAL na kybernetickou bezpečnost je poskytována prostřednictvím výzev k podávání návrhů; od listopadu 2021 do prosince 2025 bylo vyhlášeno 12 výzev. Dostupné financování EU na tyto výzvy činí 825 milionů EUR. Na roky 2026 a 2027 jsou naplánovány nové výzvy k předkládání návrhů, na jejichž základě bude poskytnuto dalších 212 milionů EUR ve formě grantů.
- 12** Dalším významným programem EU na podporu kybernetické bezpečnosti je program [Horizont Evropa](#). Projekty v oblasti kybernetické bezpečnosti jsou financovány především v rámci [klastru 3](#) – „Civilní bezpečnost pro společnost“ – a vzhledem k zaměření programu Horizont Evropa na výzkum a inovace jsou obvykle v rané fázi vyspělosti. Finanční prostředky na opatření v oblasti kybernetické bezpečnosti rovněž poskytuje [Nástroj pro oživení a odolnost](#).

¹¹ [Program Digitální Evropa](#).

Rozsah a koncepce auditu

13 Nárůst kybernetických hrozeb a jejich potenciální dopad poukázaly na nutnost posílit naši kolektivní kybernetickou odolnost. Cílem auditu bylo posoudit, zda opatření EU pomáhají členským státům účinně odhalovat významné a rozsáhlé kybernetické bezpečnostní incidenty a reagovat na ně. Posuzovali jsme zejména, zda tomu tak bylo v případě:

- sítí a mechanismů na úrovni EU (konkrétně síť CSIRT, síť EU-CyCLONe, Evropského systému varování v oblasti kybernetické bezpečnosti, střediska pro kybernetickou situaci a rezervy EU pro kybernetickou bezpečnost),
- akcí financovaných v rámci programu DIGITAL.

Nezabývali jsme se spoluprací v oblasti prosazování práva na úrovni EU ani kybernetickými odrazujícími opatřeními přijatými na úrovni EU prostřednictvím diplomatických opatření nebo obranných činností.

14 Audit se vztahuje na období od roku 2022 do roku 2025. Vychází z dokumentárního přezkumu a analýzy příslušných dokumentů, auditních návštěv ve třech členských státech (Irsku, Řecku a Itálii) a písemných dotazníků a rozhovorů s příslušnými zúčastněnými stranami. Na [obrázku 5](#) je znázorněno, jak jsme získávali podklady pro naše připomínky.

Obrázek 5 | Provedená auditní práce

Prověřovali jsme

- **Právní rámec** pro odhalování významných a rozsáhlých kybernetických bezpečnostních incidentů a reakci na ně
- **Úlohy a povinnosti** sítí a struktur zřízených na úrovni EU

Analýzovali jsme

- Dokumenty o fungování sítě **CSIRT** a sítě **EU-CyCLONe**
 - Dokumentaci k **programování programu DIGITAL a k rámci monitorování výkonnosti**
 - Dokumentaci ke **13 vybraným opatřením financovaným EU** (11 grantů a 2 smlouvy – viz podrobný seznam v příloze III)
- * Vybrali jsme opatření financovaná EU ve třech zemích (Irsko, Řecko a Itálie), kde bylo příslušné financování z programu DIGITAL významnější (materiálnější?). Těchto 11 grantů bylo vybráno ze seznamu 137 projektů financovaných EU, které se týkají odhalování hrozeb a reakce na ně, s cílem získat různorodou kombinaci projektů.

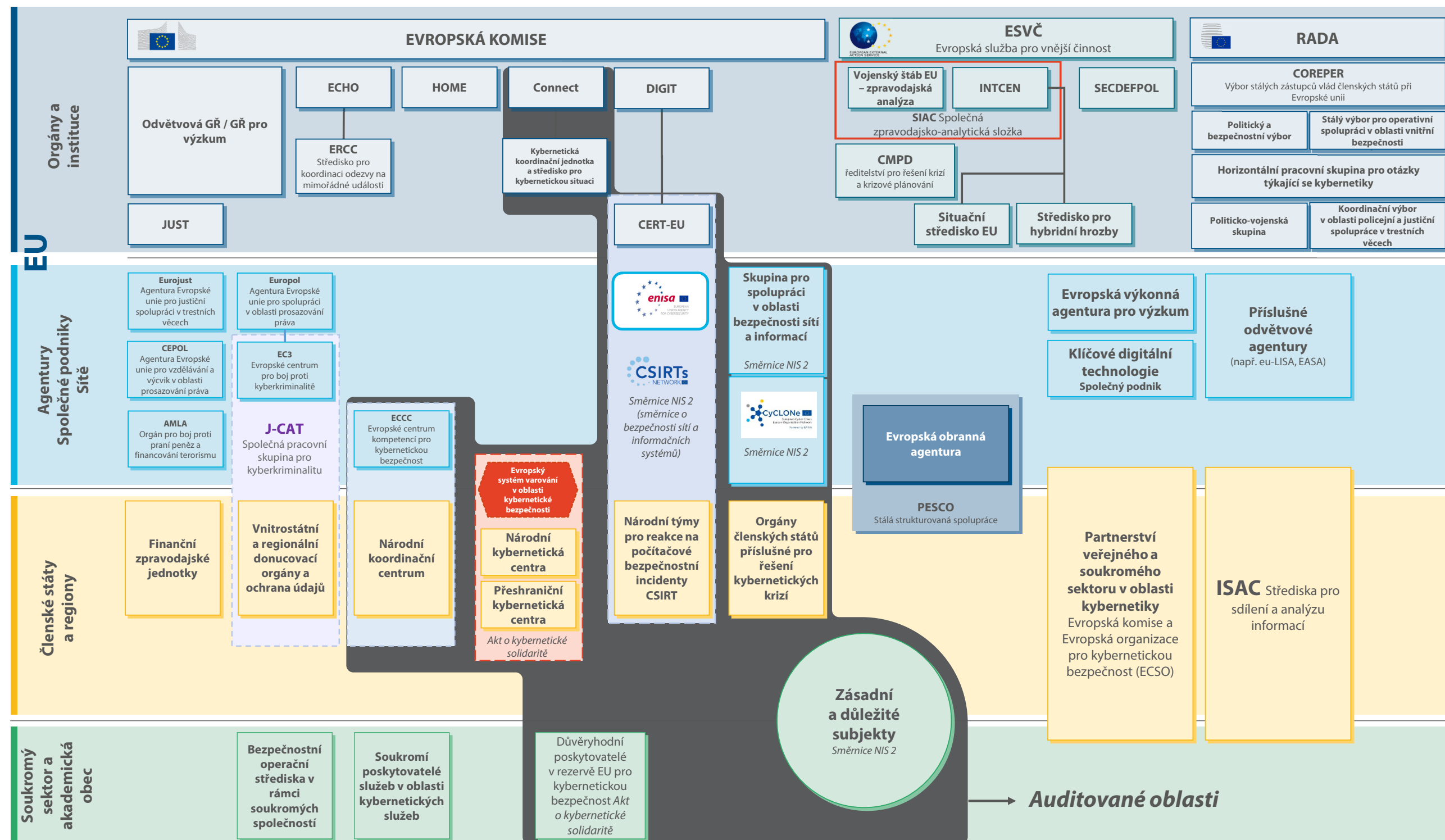
Prováděli jsme dotazování

- U příjemců **11 grantů financovaných EU zařazených do vzorku**
- Zástupců národních orgánů pro kybernetickou bezpečnost ve **třech členských státech** (Irsko, Řecko a Itálie)
- Zástupců Evropské komise (**GR Connect**), agentury **ENISA** a centra **ECCC**

Zdroj: EÚD.

- 15** Očekáváme, že naše zjištění přispějí ke zlepšení účinnosti a účelnosti odhalování významných a rozsáhlých kybernetických bezpečnostních incidentů a reakce EU na ně, jakož i ke zlepšení způsobu výběru a monitorování opatření financovaných EU. Naše [auditní metodika](#) je v souladu s mezinárodními auditorskými standardy vydanými [Mezinárodní organizací nejvyšších kontrolních institucí \(INTOSAI\)](#).

Příloha II – Prostředí kybernetické bezpečnosti v EU



GŘ Connect: Generální ředitelství pro komunikační síť, obsah a technologie
GŘ ECHO: Generální ředitelství pro evropskou civilní ochranu a operace humanitární pomoci

GŘ HOME: Generální ředitelství pro migraci a vnitřní věci
GŘ JUST: Generální ředitelství pro spravedlnost a spotřebitele
DIGIT: Generální ředitelství pro digitální služby
EASA: Agentura Evropské unie pro bezpečnost letectví

EU-CyCLONe: Evropská síť styčných organizací pro řešení kybernetických krizí
eu-LISA: Agentura Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva

INTJEN: Zpravodajské a informační centrum EU
SECDEFPOL: Bezpečnost a obranná politika
SOC: bezpečnostní operační středisko

Příloha III – Vybraná opatření v oblasti kybernetické bezpečnosti

ID	Název	Země	Datum zahájení	Datum ukončení	Celkové náklady (v milionech EUR) a příspěvek EU (v %)	Odkaz na portál EU pro financování a nabídková řízení
Granty pro přeshraniční kybernetická centra, která jsou součástí Evropského systému varování v oblasti kybernetické bezpečnosti						
1	Zřízení přeshraničních bezpečnostních operačních středisek (Athena)	Bulharsko, Řecko, Kypr, Malta	1. 1. 2024	31. 3. 2028	4,7 (50 %)	
2	PŘESHRANIČNÍ PLATFORMA ENSOC (ENSOC)	Španělsko, Itálie, Lucembursko, Nizozemsko, Rakousko, Portugalsko, Rumunsko	1. 1. 2024	30. 6. 2028	10,4 (50 %)	
Granty na zavádění sítě národních koordinačních center v členských státech						
3	Rozvoj a realizace Národního střediska pro koordinaci a rozvoj kybernetické bezpečnosti pro Irsko (NCC-IE)	Irsko	2.10. 2023	1. 10. 2026	4,2 (47 %)	
4	Italské národní koordinační centrum (NCC-IT)	Itálie	1. 11. 2023	31. 10. 2025	2,0 (50 %)	

ID	Název	Země	Datum zahájení	Datum ukončení	Celkové náklady (v milionech EUR) a příspěvek EU (v %)	Odkaz na portál EU pro financování a nabídková řízení
Granty na budování kapacit bezpečnostních operačních středisek, podporu nových aplikací umělé inteligence a dalších základních technologií pro bezpečnostní operační střediska a poskytování podpory v oblasti připravenosti a vzájemné pomoci						
5	Posílení kapacity řeckého konsolidovaného bezpečnostního operačního střediska (EL-SOC)	Řecko, Kypr	1. 1. 2024	31. 12. 2026	9,7 (50 %)	
6	Řecké středisko bezpečnostních operací pro malé a střední podniky (GR-SME-SOC)	Řecko	1. 1. 2024	31. 12. 2026	12,1 (50 %)	
7	Bezpečnostní operační střediska nové generace (NG-SOC)	Řecko, Španělsko, Kypr, Lucembursko, Slovinsko, Norsko	1. 1. 2024	31. 12. 2026	4,8 (50 %)	
8	Bezpečnostní operační středisko irské místní samosprávy (ILG-SOC)	Irsko	1. 10. 2023	30. 9. 2026	8,3 (50 %)	
9	Propojený ekosystém sítí pro koordinaci a reakci v oblasti kybernetické bezpečnosti (Cyber-CORE-Network)	Irsko	1. 1. 2024	31. 12. 2026	3,6 (50 %)	
10	Harmonizace osob, procesů a technologií v zájmu robustní kybernetické bezpečnosti (CYberSynchrony)	Belgie, Řecko, Itálie, Kypr, Nizozemsko	1. 6. 2024	31. 5. 2027	7,0 (100 %)	
11	Pokročilá bezpečnostní operační střediska pro spolupráci (ACSOC)	Řecko, Itálie, Rumunsko	1. 1. 2025	31. 12. 2027	3,0 (50 %)	

ID	Název	Země	Datum zahájení	Datum ukončení	Celkové náklady (v milionech EUR) a příspěvek EU (v %)	Odkaz na portál EU pro financování a nabídková řízení
Rámcová smlouva na akci agentury ENISA na podporu kybernetické bezpečnosti						
12	Podpora agentury ENISA při poskytování služeb v rámci akce na podporu kybernetické bezpečnosti (28 částí)	27 částí pro členské státy 1 celoevropská část	1. 12. 2022 ¹	31. 12. 2025	28,3 (100 %)	
Smlouva o poskytování služeb pro středisko pro kybernetickou situaci GŘ CNECT						
13	Individualizovaná služba na podporu střediska Evropské komise pro analýzu situace v oblasti kybernetiky	–	30. 12. 2022	30. 12. 2026	18,0 (100 %)	

Zdroj: EÚD.

¹ V prosinci 2022 bylo podepsáno několik smluv.

		Uspokojivé	Určité nedostatky	Neuspokojivé	Nelze dospět k závěru (je příliš brzy)	Projekt řeší většinu potřeb identifikovaných ve výzvě	Projekt zatím dosáhl plánovaných výstupů a výsledků	Výstupy projektu byly dodány ve stanovené lhůtě	Ukazatele výkonnosti projektu jsou relevantní, měřitelné a uvádějí výchozí a cílový stav
ID	Projekt								
1	Zřízení přeshraničních bezpečnostních operačních středisek (Athena)								
2	PŘESHRANIČNÍ PLATFORMA ENSOC (ENSOC)								
3	Příprava a zřízení Národního střediska pro koordinaci a rozvoj kybernetické bezpečnosti pro Irsko (NCC-IE)								
4	Italské Národní koordinační středisko (NCC-IT)								
5	Posílení kapacity Řeckého konsolidovaného bezpečnostního operačního střediska (EL-SOC)								
6	Řecké bezpečnostní operační středisko pro malé a střední podniky (GR-SME-SOC)								
7	Bezpečnostní operační střediska nové generace (NG-SOC)								
8	Bezpečnostní operační středisko irské místní samosprávy (ILG-SOC)								
9	Propojený ekosystém sítí pro koordinaci a reakci v oblasti kybernetické bezpečnosti (Cyber-CORE-Network)								
10	Harmonizace osob, procesů a technologií v zájmu robustní kybernetické bezpečnosti (CYBERSynchro)								
11	Bezpečnostní operační střediska pro pokročilou spolupráci (ACSOC)								

Zkratky

Zkratka	Definice/vysvětlení
CSIRT	Tým pro reakce na počítačové bezpečnostní incidenty (<i>Computer Security Incident Response Team</i>)
DIGITAL	Program Digitální Evropa
ECCC	Evropské centrum kompetencí pro kybernetickou bezpečnost
ENISA	Agentura Evropské unie pro kybernetickou bezpečnost
EU-CyCLONe	Evropská síť styčných organizací pro řešení kybernetických krizí
FSTP	Finanční podpora poskytovaná třetím stranám
GŘ CNECT	Generální ředitelství pro komunikační sítě, obsah a technologie
NKC	Národní koordinační centrum

Glosář

Pojem	Definice/vysvětlení
Aktér hrozby	Jednotlivec nebo skupina úmyslně způsobující újmu, narušující služby nebo zcizuje data zneužitím zranitelných míst v informačních systémech, sítích a zařízeních.
Bezpečnostní operační středisko	Organizační jednotka, jejímž úkolem je předcházet kybernetickým hrozbám a incidentům a shromažďovat související zpravodajské informace.
Kybernetická hrozba	Možné využití kyberprostoru k oslabení dostupnosti, pravosti, integrity nebo důvěrné povahy údajů či informačních systémů.
Kybernetické centrum	Centrální platforma sdružující různé služby, nástroje a odborníky v oblasti IT s cílem zlepšit monitorování, odhalování a analýzu kybernetických hrozeb, předcházet kybernetickým bezpečnostním incidentům a podporovat vytváření zpravodajských informací o kybernetických hrozbách.
Kybernetický bezpečnostní incident	Událost oslabující dostupnost, pravost, integritu nebo důvěrnou povahu údajů či informačních systémů.
Ransomware	Malware, který postiženým subjektům odpírá přístup k počítačovému systému nebo činí soubory šifrováním nečitelnými a nutí dotčené subjekty zaplatit za obnovení přístupu výkupné.
Rozsáhlý kybernetický bezpečnostní incident	Kybernetický bezpečnostní incident, který je pro členský stát natolik rušivý, že je nemůže řešit sám, nebo má významný dopad nejméně ve dvou členských státech.
Taxonomie	V kontextu kybernetické bezpečnosti klasifikační systém používaný k organizaci, kategorizaci a strukturování znalostí o klíčových pojmech, jako jsou hrozby a incidenty.
Významný kybernetický bezpečnostní incident	Kybernetický bezpečnostní incident, který způsobil nebo může organizaci způsobit závažné narušení činnosti nebo finanční ztrátu nebo značnou škodu jiným subjektům nebo osobám.

Odpovědi Komise

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

Odpovědi Evropského centra kompetencí pro kybernetickou bezpečnost (ECCC)

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

Odpovědi Agentury Evropské unie pro kybernetickou bezpečnost (ENISA)

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

Harmonogram

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

Auditní tým

Účetní dvůr ve svých zvláštních zprávách informuje o výsledcích auditů politik a programů EU či tématech z oblasti správy a řízení zaměřených na konkrétní oblasti rozpočtu. Vybírá a koncipuje tyto auditní úkoly tak, aby byl jejich dopad co největší, a zohledňuje přitom rizika pro výkonnost nebo zajištění souladu s předpisy, objem příslušných příjmů či výdajů, očekávaný vývoj, politické zájmy a zájem veřejnosti.

Tento audit výkonnosti provedl auditní senát III, který odpovídá za oblast vnější činnosti, bezpečnosti a práva a jemuž předsedá člen EÚD George-Marius Hyzler. Audit vedl člen EÚD George-Marius Hyzler a podporu mu poskytovali vedoucí kabinetu Romuald Kayibanda a tajemnice kabinetu Annette Farrugiaová, vyšší manažer Cyril Messein, vedoucí úkolu Frédéric Soblet, auditoři Jurgen Manjé a Flavia Di Marcová. Jazykovou podporu zajišťovala Zoe Amador Martínezová. Grafickou podporu poskytla Dunja Weibelová.



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

AUTORSKÁ PRÁVA

© Evropská unie, 2026

Politiku opakovaného použití dokumentů Evropského účetního dvora (EÚD) upravuje [rozhodnutí Evropského účetního dvora 6-2019](#) o politice týkající se veřejně přístupných dat a opakovaném použití dokumentů.

Pokud není uvedeno jinak (například v jednotlivých upozorněních o ochraně autorských práv), je obsah EÚD vlastněný EU předmětem licence [Creative Commons Attribution 4.0 International \(CC BY 4.0\) licence](#). Opakované použití je tedy obecně povoleno za podmínky, že je uveden zdroj a případné změny jsou označeny. Osoby opakovaně používající obsah EÚD nesmí měnit jeho původní význam či sdělení. EÚD nenese za jakékoli důsledky opakovaného použití odpovědnost.

Pokud konkrétní obsah zobrazuje identifikovatelné fyzické osoby, například na fotografiích zaměstnanců EÚD, nebo zahrnuje díla třetích stran, je nutno získat další povolení.

Je-li takové povolení poskytnuto, ruší a nahrazuje výše uvedené obecné povolení a musí jasně uvádět veškerá omezení týkající se použití.

K použití nebo reprodukci obsahu, který není ve vlastnictví EU, může být nezbytné požádat o svolení přímo držitele autorských práv.

Fotografie na titulní straně: © 4AXY – stock.adobe.com.

Obrázky 6 a 8 – ikony: tyto obrázky byly vytvořeny s použitím zdrojů z platformy [Flaticon.com](#). © Freepik Company S.L. Všechna práva vyhrazena.

Obrázek 5 – mapa: [Eurostat](#).

Programové vybavení nebo dokumenty, na něž se vztahují práva průmyslového vlastnictví, jako patenty, ochranné známky, zapsané (průmyslové) vzory, loga a názvy, jsou z politiky EÚD pro opakované použití vyloučeny.

Internetové stránky orgánů a institucí Evropské unie využívající doménu europa.eu obsahují odkazy na stránky třetích stran. Protože nad jejich obsahem nemá EÚD žádnou kontrolu, doporučujeme seznámit se s jejich vlastními zásadami ochrany soukromí a politikou v oblasti autorských práv.

Použití loga EÚD

Logo EÚD nesmí být použito bez předchozího souhlasu EÚD.

HTML	ISBN 978-92-849-7851-9	ISSN 1977-5628	doi:10.2865/0725184	QJ-01-26-032-CS-Q
PDF	ISBN 978-92-849-7852-6	ISSN 1977-5628	doi:10.2865/2009039	QJ-01-26-032-CS-N

JAK CITOVAT

Evropský účetní dvůr zveřejnil zvláštní zprávu 19/2026: „Odhalování kybernetických bezpečnostních incidentů a reakce na ně – rámec spolupráce EU postupuje, ale je pouze částečně účinný z důvodu zpoždění při provádění a omezeného sdílení informací“, Úřad pro publikace Evropské unie, 2026.

V posledních letech EU posílila svůj regulační rámec pro kybernetickou bezpečnost a zavedla sítě a mechanismy určené pro zvládání kybernetických bezpečnostních incidentů. EU rovněž financuje projekty v oblasti kybernetické bezpečnosti prostřednictvím programu Digitální Evropa.

Dospěli jsme k závěru, že opatření EU usnadňují odhalování významných a rozsáhlých kybernetických bezpečnostních incidentů a reakci na ně pouze částečně. I když byl postupně zaveden rámec spolupráce, stále probíhají práce na kompletním dokončení systému. Omezené sdílení informací, nedostatky ve vykazování údajů a značná zpoždění při provádění brání sítím a mechanismům EU v dosažení jejich plného potenciálu. Projekty sledují příslušné cíle, ale několik z nich se potýká s provozními problémy a zpožděními. Rámec Komise pro monitorování výkonnosti navíc obecně vykazuje nedostatky. V této zprávě předkládáme doporučení k řešení těchto nedostatků.

Zvláštní zpráva EÚD podle čl. 287 odst. 4 druhého pododstavce Smlouvy o fungování EU.



EVROPSKÝ
ÚČETNÍ DVŮR



Úřad pro publikace
Evropské unie

EVROPSKÝ ÚČETNÍ DVŮR
12, rue Alcide De Gasperi
1615 Luxembourg
LUCEMBURSKO

Tel.: +352 4398-1

Dotazy: eca.europa.eu/cs/contact
Internetová stránka: eca.europa.eu
Sociální sítě: @EUauditors