Rada
Evropské unie

Brusel 16. ledna 2025
(OR. en)

5426/25

CYBER 21
SAN 15

PRŮVODNÍ POZNÁMKA

Odesílatel:	Martine DEPREZOVÁ, ředitelka, za generální tajemnici Evropské komise
Datum přijetí:	15. ledna 2025
Příjemce:	Thérèse BLANCHETOVÁ, generální tajemnice Rady Evropské unie
Č. dok. Komise:	COM(2025) 10 final
Předmět:	SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ Evropský akční plán pro kybernetickou bezpečnost nemocnic a poskytovatelů zdravotní péče

Delegace naleznou v příloze dokument COM(2025) 10 final.

Příloha: COM(2025) 10 final

EVROPSKÁ
KOMISE

V Bruselu dne 15.1.2025
COM(2025) 10 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

Evropský akční plán pro kybernetickou bezpečnost nemocnic a poskytovatelů zdravotní péče

1. Úvod

Bezpečnostní prostředí v EU se rychle mění; dochází k eskalaci hybridních útoků a kybernetických útoků, jejichž cílem je destabilizovat naši společnost, rozdělovat a rozvracet, ale také z kybernetické kriminality profitovat. Evropa proto musí urychleně posílit svou připravenost na tuto novou realitu a odolnost vůči ní, a to ve všech odvětvích a v souladu s celospolečenským a mezirezortním přístupem, jak požaduje zpráva zvláštního poradce předsedkyně Evropské komise Sauliho Niinistöa.

Bezpečné a odolné systémy zdravotní péče jsou základem sociálního modelu EU. Nemocnice a systémy zdravotní péče však čelí rostoucím hrozbám, zejména ze strany gangů využívajících ransomware, jež se na ně zaměřují kvůli finančnímu zisku, který přináší vysoká hodnota údajů o pacientech, včetně elektronických zdravotních záznamů. Zdravotnictví se v posledních čtyřech letech stalo nejvíce napadaným odvětvím v EU, a to i během pandemie COVID-19, kdy byla zdravotnická infrastruktura stále častěji terčem kybernetických útoků. Kybernetické útoky na nemocnice a poskytovatele zdravotní péče způsobují přímé škody lidem, zdržují lékařské zákroky, blokují pohotovosti a v krajním případě mohou vést až ke ztrátám na životech.

V sázce je ještě více, protože toto odvětví prochází zásadní digitální transformací. Digitální zdravotnictví a využívání a opakované používání zdravotních údajů může dát vzniknout modelům péče, které budou lépe vyhovovat potřebám a preferencím lidí a pacientů, a to tím, že předejdou vzniku onemocnění nebo umožní dřívější léčbu. Integrace digitálních nástrojů a řešení do klinických procesů, jakož i využívání a opakované používání zdravotních údajů mohou sloužit k lepšímu klinickému rozhodování a přispět k automatizaci ve zdravotnictví a k rychlejší a kvalitnější péči o pacienty. Digitální nástroje, využívání dat a zdravotnické prostředky, které jsou často připojeny k internetu a postaveny na umělé inteligenci, jsou také klíčem k řešení problémů, jako je nedostatek zdravotnických pracovníků.

Digitální nástroje však zároveň rozšiřují okruh potenciálních cílů pachatelů kybernetické kriminality. Navíc se útokům na zdravotnická zařízení nevyhýbají někteří státní aktéři, o čemž svědčí probíhající útočná válka Ruska proti Ukrajině. Proto je toto odvětví potenciálním cílem kybernetických útoků v rámci širší hybridní kampaně. Kybernetické útoky ohrožují nejenom bezpečnost pacientů, ale také podkopávají důvěru veřejnosti ve zdravotnickou infrastrukturu a jsou spojeny se značnými náklady na obnovu. Kromě ochrany před kybernetickými útoky je odolná a bezpečná digitální infrastruktura nezbytná také pro podporu zavedení a plného využívání evropského prostoru pro zdravotní data[1] (EHDS).

Proto je načase posílit kybernetickou bezpečnost a odolnost evropských nemocnic a poskytovatelů zdravotní péče a zvýšit její úroveň, jak zdůraznila předsedkyně von der Leyenová ve svých politických směrech pro Komisi na období 2024–2029[2]. Tento akční plán reaguje na naléhavost situace a jedinečné hrozby, kterým toto odvětví čelí. Na problémy v oblasti kybernetické bezpečnosti ve zdravotnictví neexistuje žádný zázračný lék. Akční plán místo toho vyzývá k posílení prevence a připravenosti, ke koordinovanějšímu přístupu k solidaritě a zároveň k využití odborných znalostí evropského odvětví kybernetické bezpečnosti. Akční plán jako takový odráží přístup EU k bezpečnosti, který bude dále

[1] https://www.consilium.europa.eu/cs/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_cs

rozpracován a formalizován v připravované Evropské strategii vnitřní bezpečnosti, jež definuje komplexní reakci na všechny hrozby pro vnitřní bezpečnost a zaměří se na schopnost předvídat hrozby, předcházet škodám a chránit lidi prostřednictvím opatření na všech úrovních a celospolečenského přístupu.

Odvětví zdravotnictví zahrnuje širokou škálu subjektů a aktérů, mezi něž patří nemocnice, kliniky, pečovatelské domy, rehabilitační centra a různí poskytovatelé zdravotní péče, dále farmaceutický, lékařský a biotechnologický průmysl, výrobci zdravotnických prostředků a zdravotnické výzkumné instituce. Tento akční plán se převážně zaměřuje na kybernetickou bezpečnost nemocnic a poskytovatelů zdravotní péče, kterými se rozumí fyzická nebo právnická osoba nebo jiný subjekt, který zákonným způsobem poskytuje zdravotní péči na území členského státu[3]. Nemocnice a poskytovatelé zdravotní péče jsou vzájemně závislí na dalších zdravotnických subjektech a jsou nejblíže lidem. Opatření na zvýšení kybernetické bezpečnosti nemocnic a poskytovatelů zdravotní péče by se zároveň měla zabývat i riziky, jež ovlivňují širší dodavatelský řetězec a ekosystém a jejichž zdrojem jsou například subjekty, které využívají zdravotní údaje pro výzkum a strojové učení nebo které vyrábějí zdravotnické prostředky, zejména zdravotnické prostředky s digitálními technologiemi, které se připojují k internetu nebo jiným zařízením („internet věcí“).

Zajištění bezpečnosti systémů zdravotní péče je sice primárně v kompetenci členských států, ale podle směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS 2)[4] je zdravotnictví rovněž kritickým odvětvím. Pachatelé kybernetické kriminality a další aktéři hrozeb působí přes hranice států a výzvy v oblasti kybernetické bezpečnosti, kterým čelí zdravotnické organizace, jsou také v různých členských státech podobné. Spolupráce na evropské úrovni je cenná pro sdílení a rozšiřování osvědčených postupů na úrovni EU a na vnitrostátní úrovni. Akční plán proto navrhuje koordinaci a opatření na úrovni EU a zároveň vyzývá členské státy, aby přijaly opatření, která zdravotní péči a širšímu zdravotnickému ekosystému pomohou.

Akční plán se zaměřuje na budování kapacit odvětví především pokud jde o **předcházení** kybernetickým bezpečnostním incidentům, protože prevence je vždy lepší než léčba. Zadruhé akční plán podrobně popisuje opatření ke zlepšení sdílení informací souvisejících s kybernetickou bezpečností a schopnosti **odhalovat** kybernetické hrozby, což umožní rychlejší reakci. Zatřetí stanoví opatření pro lepší **reakci** na incidenty a pro **obnovení** po incidentech. V neposlední řadě akční plán stanoví způsoby, jak **odrazovat** aktéry kybernetických hrozeb od útoků na systémy zdravotní péče v Evropě.

Akční plán bude prováděn ve spolupráci s poskytovateli zdravotní péče a širším zdravotnickým ekosystémem, členskými státy a komunitou zabývající se kybernetickou bezpečností. Klíčem k dalšímu definování a zdokonalení nejúčinnějších opatření je přístup založený na spolupráci, aby z těchto opatření mohli mít prospěch všichni evropští poskytovatelé kritické zdravotní péče. Proto bude toto sdělení doprovázeno zahájením komplexní konzultace se zúčastněnými stranami, odvětvím a členskými státy. Kybernetické hrozby mají přeshraniční a vzájemně propojenou povahu, a proto je pro kybernetickou

[3] Ustanovení čl. 3 písm. g) směrnice Evropského parlamentu a Rady 2011/24/EU o uplatňování práv pacientů v přeshraniční zdravotní péči, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:32011L0024

[4] Směrnice (EU) 2022/2555 Evropského parlamentu a Rady ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (směrnice NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555

bezpečnost důležitá mezinárodní spolupráce. Srovnatelné hrozby pro kybernetickou bezpečnost existují také v zemích procesu rozšíření a evropského sousedství a v dalších strategických partnerských zemích EU. To může v konečném důsledku ohrozit bezpečnost kritické infrastruktury v EU. Proto bude důležité zohlednit zkušenosti získané při provádění akčního plánu také v rámci spolupráce EU jak se zeměmi procesu rozšíření, tak s dalšími partnerskými zeměmi, a to s ohledem na míru ohrožení, kterému jsou vystaveny.

2. Výzvy v oblasti kybernetické bezpečnosti, kterým čelí nemocnice a poskytovatelé zdravotní péče

Kybernetické hrozby pro odvětví zdravotnictví

Kybernetické útoky jsou celosvětově i v rámci EU na vzestupu a situace v oblasti hrozeb je stále složitější a dynamičtější. Pokroky v oblasti umělé inteligence poskytují pachatelům trestné a nekalé činnosti výkonné nástroje, které zvyšují přesnost a dopad jejich operací, a zároveň mění možnosti kybernetické obrany tím, že umožňují automatizované zásahy proti útokům v reálném čase.

Kritickým problémem kybernetické bezpečnosti v EU i celosvětově je i nadále ransomware, přičemž jedna zpráva odhaduje, že do roku 2031 budou celosvětové roční náklady přesahovat 250 miliard EUR[5]. Když pachatelé ransomwarových útoků útočí, nejenže zašifrují data obětí a požadují výkupné, ale stále častěji také nechávají uniknout citlivé informace, aby vyvíjeli další nátlak. Další významnou výzvou jsou zranitelnosti softwaru a hardwaru: podle Agentury Evropské unie pro kybernetickou bezpečnost (ENISA)[6] je zdravotnictví odvětvím, které ohlásilo nejvíce bezpečnostních incidentů souvisejících s těmito zranitelnostmi.[7] K dalším rostoucím hrozbám patří útoky DDoS, jejichž cílem je zahltit cílový systém záplavou provozu a znepřístupnit jej legitimním uživatelům[8].

Odvětví zdravotnictví čelí podobným trendům kybernetických hrozeb s výrazným důrazem na ransomwarové útoky. Podle agentury ENISA představoval ransomware v letech 2021–2023 54 % analyzovaných kybernetických bezpečnostních incidentů v odvětví zdravotnictví. 83 % útoků bylo motivováno finančně, a to kvůli vysoké hodnotě zdravotnických údajů, zatímco 10 % útoků mělo ideologickou motivaci[9]. Podobně zpráva Komise z roku 2024 zjistila, že 71 % útoků s dopadem na péči

[5] Cybersecurity Ventures (1. června 2024): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031* (Předpokládá se, že globální náklady na škody způsobené ransomwarem přesáhnou do roku 2031 265 miliard dolarů). K dispozici na adrese https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

[6] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

[7] *ENISA Threat Landscape: Health Sector* (zpráva agentury ENISA o situaci v oblasti hrozeb: odvětví zdravotnictví, červenec 2023).

[8] *ENISA Threat Landscape* (zpráva agentury ENISA o situaci v oblasti hrozeb), 2024.

[9] *ENISA Threat Landscape: Health Sector* (zpráva agentury ENISA o situaci v oblasti hrozeb: odvětví zdravotnictví, červenec 2023). Zpráva analyzovala poskytovatele zdravotní péče, jakož i další typy organizací, včetně organizací provádějících

o pacienty, jako je opožděná léčba, diagnostika a zhoršený přístup k pohotovostním službám, bylo provedeno pomocí ransomwaru[10]. Ransomwarové útoky mohou mít na poskytování zdravotních služeb obzvláště narušující účinek a ohrozit bezpečnost pacientů. Navíc jsou ransomwarové útoky často spojeny s narušením ochrany údajů o pacientech[11], což často zahrnuje citlivé údaje týkající se zdraví a porušuje základní právo na ochranu osobních údajů.

S rostoucí digitalizací zdravotnictví se zároveň zvětšuje prostor pro útoky. Podle zprávy o stavu digitální dekády z roku 2024 má v průměru 79 % občanů EU online přístup ke svým elektronickým zdravotním záznamům v primární péči[12]. Elektronické zdravotní záznamy, klinické informační systémy, nemocniční pracovní systémy, informační systémy pro úhradu léčby, lékařské zobrazovací systémy a zdravotnické prostředky používané pro diagnostické účely nebo pro monitorování pacientů jsou příklady digitálních nástrojů, které mohou hrát významnou roli při zvyšování efektivity a výkonnosti zdravotnictví, ale jsou také potenciálním cílem kybernetického bezpečnostního útoku. Kybernetickými útoky jsou ohroženy zejména specifické zdravotnické činnosti, jako je intenzivní péče a radiologické zobrazování, nebo lékařské obory, jako je onkologie a kardiologie, které jsou vysoce závislé na digitálních zařízeních. Kromě toho mohou problémy v dodavatelském řetězci vést k pořizování zařízení s nedostatečnou kybernetickou bezpečností, což zhoršuje stávající obecná rizika.

Například během pandemie COVID-19 ochromil ransomwarový útok velkou část irského zdravotnického systému, což vedlo ke zrušení alespoň některých služeb v 31 z 54 nemocnic zajišťujících akutní péči v den incidentu.[13] Zdravotnické služby se musely vrátit k papírovým záznamům, což zpomalilo efektivitu provozu. Útok pocházel z podvodného e-mailu se škodlivou přílohou.[14] Incident ukázal, jak se kybernetické útoky mohou šířit napříč různými systémy, a tedy jak je důležité chránit celý prostor zdravotnické organizace, kde může dojít k útoku. Zdůraznil také význam zajištění základní kybernetické hygieny a kultury kybernetické bezpečnosti v organizacích.

Vyspělost nemocnic a poskytovatelů zdravotní péče v oblasti kybernetické bezpečnosti

výzkum v oblasti zdraví, subjektů vyrábějících určité výrobky související se zdravím, zdravotnických orgánů, zdravotních pojišťoven a zařízení pro ústavní léčbu a poskytovatelů sociálních služeb. K dispozici na adrese https://www.enisa.europa.eu/publications/health-threat-landscape

[10] Evropská komise: Společné výzkumné středisko, Reina, V. a Griesinger, C., *Cyber security in the health and medicine sector – A study on available evidence of patient health consequences resulting from cyber incidents in healthcare settings* (Kybernetická bezpečnost ve zdravotnictví – studie o dostupných důkazech o zdravotních následcích kybernetických incidentů ve zdravotnickém prostředí), Úřad pro publikace EU, 2024, https://data.europa.eu/doi/10.2760/693487

[11] Podle zprávy *ENISA Threat Landscape for the Health Sector* (zpráva o situaci v oblasti hrozeb v odvětví zdravotnictví) byly narušení bezpečnosti údajů nebo jejich krádež potvrzeny u 43 % analyzovaných ransomwarových incidentů.

[12] Zpráva o stavu digitální dekády 2024

[13] Irish Health Service Executive (Irský výkonný orgán v oblasti zdravotnictví, 2021): *Conti cyber attack on the HSE: Independent Post Incident Review* (Kybernetický útok skupiny Conti na výkonný orgán v oblasti zdravotnictví: Nezávislý přezkum po incidentu).

[14] Irish Health Service Executive (Irský výkonný orgán v oblasti zdravotnictví): *Cyber-attack and HSE response* (Kybernetický útok a reakce výkonného orgánu v oblasti zdravotnictví). K dispozici na adrese https://www2.hse.ie/services/cyber-attack/what-happened/

Prostředí zdravotní péče v EU je velmi rozmanité, neboť nemocnice a další poskytovatelé zdravotní péče se v jednotlivých členských státech značně liší z hlediska vlastnictví, struktury a velikosti. V některých případech může být řízení zdravotní péče založeno na centralizovaném přístupu na celostátní úrovni, v jiných na regionální a místní úrovni; poskytovatelé zdravotní péče mohou být ve veřejném nebo soukromém vlastnictví. Rozdíly mohou navíc existovat i v rámci jedné země, například tam, kde existují značné socioekonomické a územní rozdíly mezi regiony, čímž vzniká složitá situace. Toto složité prostředí zdravotní péče může být ohroženo významnými zdravotními krizemi v důsledku přenosných nemocí, jako je pandemie COVID-19, ale také dalšími zdravotními riziky, například v souvislosti se změnou klimatu. V neposlední řadě existuje značná variabilita a roztříštěnost v úrovni digitalizace a zavádění technologií na straně poskytovatelů zdravotní péče. Příkladem této složitosti je, že nedostupnost služeb způsobená kybernetickým bezpečnostním incidentem může mít za následek vážné škody a újmu pacientů i v malých zdravotnických zařízeních, včetně klinik nebo pohotovostních lékařských služeb, které poskytují základní služby relativně malému počtu uživatelů.

Podle zprávy agentury ENISA o stavu kybernetické bezpečnosti v Unii v roce 2024[15] je vyspělost kybernetické bezpečnosti v odvětví zdravotnictví v EU mírná a mezi jednotlivými subjekty zdravotní péče v Evropě existují v úrovni vyspělosti kybernetické bezpečnosti velké rozdíly. Nedostatky lze pozorovat v klíčových oblastech, jako je dostatek lidských zdrojů, znalost organizací o jejich dodavatelských řetězcích informačních a komunikačních technologií (IKT) a instalace aktuálních bezpečnostních prvků do produktů. Odvětví má problémy se základní kybernetickou hygienou a základními bezpečnostními opatřeními, což dokládá skutečnost, že téměř všechny dotázané zdravotnické organizace se potýkají s problémy, pokud jde o posuzování kybernetických bezpečnostních rizik, přičemž téměř polovina z nich nikdy analýzu rizik neprovedla[16].

Další významnou výzvou pro kybernetickou bezpečnost nemocnic je průnik informačních technologií a provozních technologií, kde se setkávají různé bezpečnostní priority, pokud jde o důvěrnost, dostupnost a spolehlivost, a kde narušení v jedné oblasti může ovlivnit druhou oblast. Zpráva agentury ENISA o stavu kybernetické bezpečnosti v Unii v roce 2024 dále zdůrazňuje, že odvětví zdravotnictví si při zajišťování bezpečnosti produktů a procesů IKT, které používá, nevede dostatečně, a to z důvodu velké rozmanitosti zdravotnických subjektů, zařízení a produktů.

Tato různorodost spolu s různou úrovní informovanosti o kybernetické bezpečnosti mezi zaměstnanci a vedoucími pracovníky nemocnic představuje z hlediska zajištění kybernetické bezpečnosti zdravotnických systémů komplexní výzvu. Například podle průzkumu Eurobarometr 2024 o kybernetických dovednostech pouze 25 % dotázaných společností v odvětví zdravotnictví, vzdělávání a sociální péče poskytlo v předchozích 12 měsících školení nebo zvýšilo informovanost o kybernetické bezpečnosti[17]. Je třeba přijmout opatření na podporu kultury informovanosti o kybernetické bezpečnosti mezi zdravotnickými pracovníky v první linii. Dalšími zdroji zranitelností ovlivňujícími kybernetickou

[15] ENISA: Zpráva o stavu kybernetické bezpečnosti v Unii v roce 2024 (září 2024). K dispozici na adrese https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[16] *ENISA Threat Landscape* (zpráva agentury ENISA o situaci v oblasti hrozeb): Odvětví zdravotnictví (červenec 2023). K dispozici na adrese https://www.enisa.europa.eu/publications/health-threat-landscape

[17] Bleskový průzkum Eurobarometr 547 o kybernetických dovednostech (květen 2024). K dispozici na adrese https://europa.eu/eurobarometer/surveys/detail/3176

bezpečnost poskytovatelů zdravotní péče jsou například střídání zaměstnanců, používání sdílených pracovních stanic, špatná správa ověřování a používání vyměnitelných médií[18].

V mnoha případech jsou informační a provozní technologie alespoň částečně zajišťovány externě. Průzkum Eurobarometr 2024 zjistil, že podíl společností, které si externě zajišťují alespoň některé aspekty kybernetické bezpečnosti, je nejvyšší v odvětví zdravotnictví, vzdělávání a sociální péče, kde tak činí 57 % dotázaných společností[19]. Stejně tak je patrný silný trend přechodu na cloud computing, který je motivován potřebou škálovatelného ukládání a správy dat, nákladovou efektivitou, lepší spoluprací a podporou pokročilých technologií, jako je umělá inteligence a internet lékařských věcí. V roce 2022 využívalo 58 % zdravotnických organizací nějakou cloudovou platformu pro digitální zdravotnictví[20]. Tento posun sice může přinést výrazné zvýšení efektivity, ale zároveň s sebou nese rizika, která vyžadují informovaná rozhodnutí o nákupu a bezpečné konfiguraci.

Nad všemi těmito výzvami se vznáší otázka budování kapacit a financování. Financování kybernetické bezpečnosti v odvětví zdravotnictví je omezené a zůstává všeobecným problémem v celé EU[21]. Tyto problémy s financováním navíc vyvstávají v situaci, kdy se očekává, že stárnutí obyvatelstva bude v nadcházejících desetiletích vyvíjet na evropské systémy zdravotní péče v mnoha oblastech rozpočtové tlaky.

Pokračující používání zastaralých nástrojů a starších systémů, omezené zdroje na prevenci incidentů nebo reakci na ně a nedostatky ve vyspělosti kybernetické bezpečnosti často pramení z nedostatku finančních prostředků. Nemocnice se neustále potýkají s výzvou, jak najít rovnováhu mezi investicemi do moderní bezpečné a digitální infrastruktury a dalšími investicemi nezbytnými pro zlepšení péče o pacienty, jako je najímání lékařů a dalších zdravotnických pracovníků, zavádění nových diagnostických a léčebných metod a pořizování přístrojů. Podle agentury ENISA[22] se odvětví zdravotnictví řadí až na 7. místo z 12 zkoumaných odvětví, pokud jde o podíl výdajů na informační bezpečnost z celkových výdajů na IT, přičemž medián v odvětví zdravotnictví činí 8,3 %.

3. Evropské centrum podpory kybernetické bezpečnosti pro nemocnice a poskytovatele zdravotní péče

Rámec EU pro kybernetickou bezpečnost nabízí širokou škálu nástrojů, které by měly být využity ke zlepšení bezpečnosti a odolnosti nemocnic a poskytovatelů zdravotní péče. K řešení výše uvedených

[18] Panacea – People-centric cybersecurity in healthcare (2021): *White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres* (Bílá kniha – Poznatky z projektu PANACEA o kybernetické ochraně nemocnic a středisek péče).
[19] Bleskový průzkum Eurobarometr 547 o kybernetických dovednostech (květen 2024). K dispozici na adrese https://europa.eu/eurobarometer/surveys/detail/3176
[20] ENISA: *NIS Investments Report 2022* (Zpráva o investicích do bezpečnosti sítí a informací, listopad 2022). K dispozici na adrese https://www.enisa.europa.eu/publications/nis-investments-2022
[21] Organizace a poskytování zdravotních služeb a lékařské péče spadá podle článku 168 Smlouvy o fungování Evropské unie do pravomoci členských států a financování systémů zdravotní péče se v jednotlivých členských státech liší.
[22] ENISA: *NIS Investments Report 2022* (Zpráva o investicích do bezpečnosti sítí a informací, listopad 2022). K dispozici na adrese https://www.enisa.europa.eu/publications/nis-investments-2022

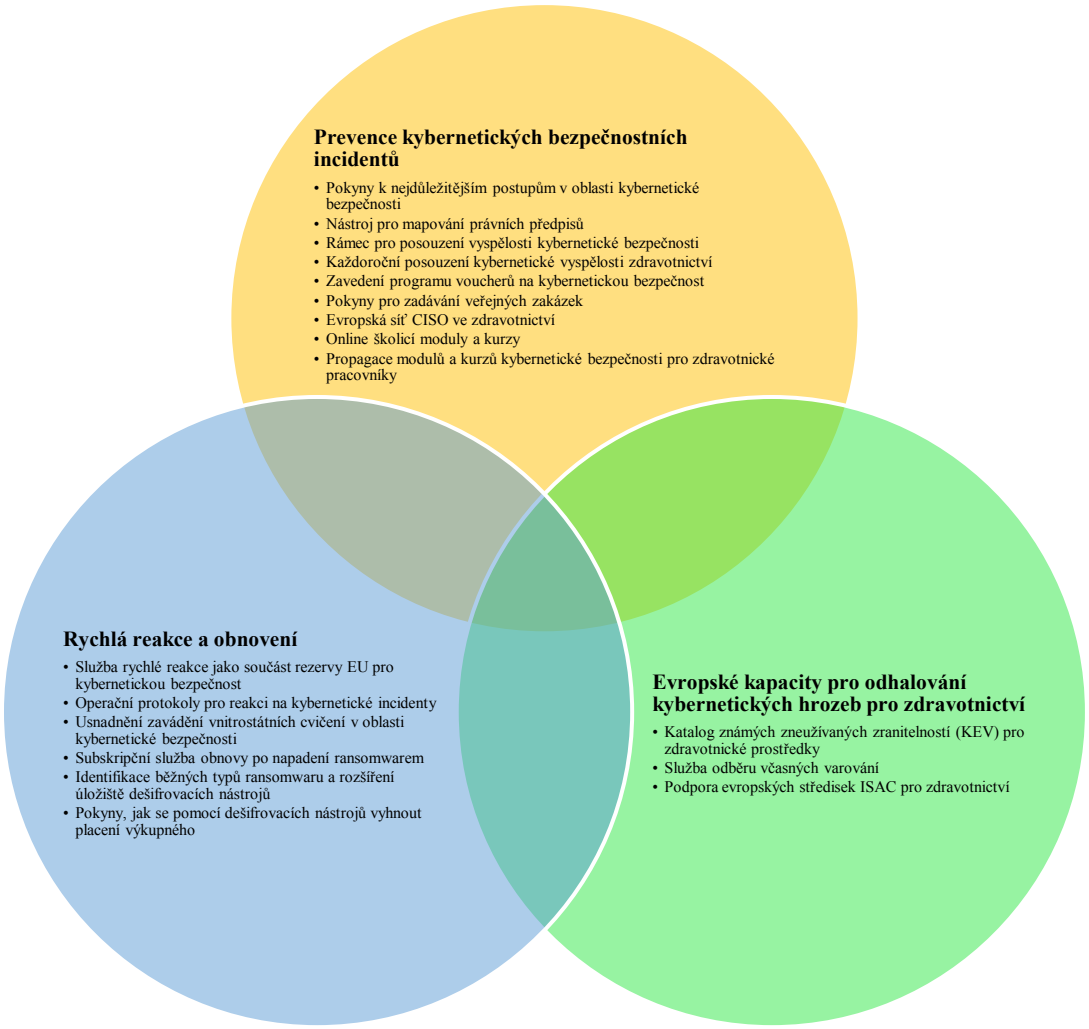
četných problémů je nutné vyvinout jednotný strategický přístup na úrovni EU, který by spojil potřebné zdroje, odborné znalosti a nástroje k účinnému řešení kybernetických hrozeb. Komplexní přehled, jakož i lepší plánování a koordinace jsou nezbytné pro posílení obrany poskytovatelů zdravotní péče v celé EU. K dosažení tohoto cíle je nejvhodnější, aby agentura ENISA v rámci své organizace zřídila specializované **Evropské centrum podpory kybernetické bezpečnosti pro nemocnice a poskytovatele zdravotní péče**[23] jako součást svého mandátu[24] k ochraně a podpoře kritické infrastruktury EU.

Centrum podpory by mělo postupně **vytvořit komplexní katalog služeb pro potřeby nemocnic a poskytovatelů zdravotní péče,** v němž by byla uvedena nabídka dostupných služeb v oblasti připravenosti, prevence, detekce a reakce. Ve spolupráci s orgány členských států a na základě zkušeností nemocnic a poskytovatelů zdravotní péče by centrum podpory mělo vytvořit uživatelsky přívětivé a snadno přístupné úložiště všech dostupných nástrojů na evropské, vnitrostátní a regionální úrovni. Při provádění svých činností by mělo zajistit řádnou koordinaci s členskými státy a podporovat stanovení priorit a provádění opatření podle potřeby v reálném čase.

Jako důležitý stavební kámen pro vytvoření katalogu služeb centra podpory Komise navrhne zahájit pilotní projekty v celé EU s cílem vyvinout osvědčené postupy pro kybernetickou hygienu a posouzení bezpečnostních rizik a řešit potřebu nepřetržitého monitorování kybernetické bezpečnosti, operativních informací o hrozbách a reakce na incidenty s využitím nejmodernějších řešení v oblasti kybernetické bezpečnosti. Výsledky těchto pilotních projektů, které budou financovány z programu Digitální Evropa a prováděny Evropským centrem kompetencí pro kybernetickou bezpečnost (ECCC), budou sloužit jako podklad pro další opatření na úrovni EU, včetně práce centra podpory.

[23] V tomto dokumentu je ve stejném významu používán pojem „centrum podpory“.

[24] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15).



Graf 1: Koncepty katalogu služeb centra podpory pro nemocnice a poskytovatele zdravotní péče

3.1 Prevence kybernetických bezpečnostních incidentů

Jednoduchá opatření, která zvyšují šance

Základní opatření kybernetické bezpečnosti, například zajištění aktualizace systémů, správa záloh a zavedení vícefaktorového ověřování, mohou podle jednoho odhadu ochránit organizace až před 98 % útoků[25]. Mnohá z nejúčinnějších opatření kybernetické hygieny a řízení rizik jsou relativně jednoduchá, takže představují snadno dostupnou možnost, jak zlepšit kybernetickou bezpečnost. Jednou z klíčových

[25] *Microsoft Digital Defense Report 2022* (Zpráva společnosti Microsoft o digitální obraně, 2022). K dispozici na adrese https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022

rolí centra podpory by proto mělo být **vypracování jasných a cílených pokynů, které upozorní na nejdůležitější postupy v oblasti kybernetické bezpečnosti a pomohou poskytovatelům zdravotní péče při jejich zavádění**. Tato podpora musí přesáhnout rámec velkých nemocnic a zahrnovat i poradenství šité na míru menším subjektům, jako jsou místní ordinace praktických lékařů a specializované kliniky, které často nemají prostředky na specializované týmy pro kybernetickou bezpečnost, ale jsou vůči útokům stejně zranitelné. Dále je třeba zohlednit regionální význam konkrétních zdravotnických subjektů pro zajištění péče o pacienty, například v řídce osídlených oblastech. Také zdravotnické výzkumné ústavy, které zpracovávají velké množství citlivých osobních údajů, by mohly využít poradenství ohledně základních opatření kybernetické bezpečnosti, aby zvýšily svou odolnost.

Na zdravotnické organizace se rovněž vztahuje řada povinností souvisejících s kybernetickou bezpečností, které vyplývají z právních předpisů EU[26]. Ačkoli jsou tyto povinnosti zásadní pro zajištění vysoké společné základní úrovně kybernetické bezpečnosti a bezpečnosti údajů, je nezbytné zajistit, aby orientace v regulačním prostředí nebyla zbytečně obtížná a zatěžující. Velký důraz na dodržování předpisů by neměl být v rozporu s cílem podporovat silnou kulturu kybernetické bezpečnosti. **S minimalizací administrativní zátěže subjektů, na které se vztahuje více regulačních nástrojů, může pomoci snadno přístupný nástroj pro mapování právních předpisů.** Kromě vypracovávání pokynů a souborů nástrojů by mělo centrum podpory úzce spolupracovat s Komisí a členskými státy na co nejrychlejším vývoji a šíření takového nástroje. Centrum podpory by proto hrálo důležitou roli při zajišťování, aby pravidla kybernetické bezpečnosti byla snadno pochopitelná a proveditelná, například poskytováním pokynů k implementaci[27] a v případě potřeby prosazováním příslušných norem.

Dalším nástrojem, který usnadní jednoduché zavádění správných postupů kybernetické hygieny, jsou připravované **evropské peněženky digitální identity**. Zásadní význam pro zmírnění rizik neoprávněného přístupu ke zdravotním údajům má snížení závislosti na slabých identifikačních mechanismech, jako jsou hesla. Přechod na řešení bezpečného přihlašování založená na spolehlivé identifikaci má rozhodující význam. Evropská peněženka digitální identity nabízí pro zdravotnické pracovníky harmonizovaný celounijní přístup k elektronické identifikaci a od konce roku 2026 poskytne

[26] Například směrnice NIS 2; nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky (akt o kybernetické odolnosti), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng; nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích *in vitro*, https://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679; nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci), https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32024R1689; návrh nařízení Evropského parlamentu a Rady o evropském prostoru pro zdravotní data, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52022PC0197. Jednání byla uzavřena politickou dohodou na jaře 2024 a po dokončení se očekává zveřejnění v Úředním věstníku na jaře 2025.

[27] Za vypracování pokynů k výkladu obecného nařízení o ochraně osobních údajů (GDPR) odpovídá Evropský sbor pro ochranu osobních údajů (EDPB). Agentura ENISA by měla při vypracovávání pokynů plně respektovat výsady EDPB.

robustní a jednotné řešení. Všechny online zdravotnické informační systémy, které musí zavést silnou autentizaci uživatelů, budou od konce roku 2027 povinny tuto peněženku přijímat pro účely identifikace[28].

Připravenost a cílená podpora

Testování připravenosti zahrnující činnosti, jako je penetrační testování, je základem účinné kybernetické bezpečnosti a Komise již agentuře ENISA přidělila finanční prostředky na pilotní iniciativy v oblasti připravenosti, které odhalily, že odvětví zdravotnictví patří mezi oblasti, v nichž je největší poptávka po testování a dalším hodnocení s cílem zjistit nedostatky ve vyspělosti kybernetické bezpečnosti. Jakmile vstoupí v platnost nařízení o kybernetické solidaritě, toto úsilí se výrazně rozšíří a vedení se ujme ECCC. V reakci na tuto potřebu Komise po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, sítí EU-CyCLONe[29] a agenturou ENISA navrhne, aby odvětví zdravotnictví bylo určeno jako odvětví, kterému lze poskytnout podporu na **koordinované testování připravenosti** v rámci nařízení o kybernetické solidaritě. Centrum podpory by dále mělo vypracovat **rámec pro posouzení vyspělosti kybernetické bezpečnosti specificky přizpůsobený pro odvětví zdravotnictví**. Taková posouzení vyspělosti by subjektům poskytla praktické informace o jejich zranitelnostech a zároveň jim umožnila prokázat pacientům a zúčastněným stranám svou připravenost v oblasti kybernetické bezpečnosti, což by zvýšilo důvěru v jejich služby. Centrum podpory by mělo na souhrnné úrovni provádět **každoroční posouzení kybernetické vyspělosti zdravotnictví**, které by poskytlo jasný přehled o kybernetické bezpečnosti v odvětví zdravotnictví na vnitrostátní úrovni i na úrovni EU.

Odvětví zdravotnictví se v oblasti služeb kybernetické bezpečnosti ve velké míře spoléhá na externí dodavatele[30], což zdůrazňuje potřebu cílené podpory pro posílení obrany. V návaznosti na úspěšné iniciativy, jako jsou inovační vouchery EU, **by členské státy měly zvážit cílená opatření, jako jsou vouchery na kybernetickou bezpečnost pro mikro-, malé a středně velké nemocnice a poskytovatele zdravotní péče**. Tyto vouchery by poskytovaly finanční pomoc na zavedení konkrétních opatření kybernetické bezpečnosti. Při určování priorit pro přidělování voucherů by se mělo vycházet ze závěrů testování připravenosti a posouzení vyspělosti.

Pro účinné zavádění voucherů nebo jiných podpůrných programů jsou zásadní místní znalosti a kontext, které zajišťují relevanci a dostupnost. Fondy EU, jako je Evropský fond pro regionální rozvoj, již aktivně podporují iniciativy v oblasti kybernetické bezpečnosti a digitálního zdraví, a mohly by proto sloužit jako nástroj pro vytvoření cílených programů voucherů na kybernetickou bezpečnost pro poskytovatele zdravotní péče. V rámci tohoto úsilí by centrum podpory spolupracovalo s členskými státy a orgány odpovědnými za regionální programy na podpoře rozvoje takových regionálních systémů voucherů,

[28] Ustanovení čl. 5f odst. 1 až 2 nařízení (EU) 910/2014.
[29] Evropská síť styčných organizací pro řešení kybernetických krizí.
[30] Viz zpráva agentury ENISA o investicích do bezpečnosti sítí a informací v roce 2023 (listopad 2023), která zdůrazňuje význam externí podpory pro audit kybernetické bezpečnosti a dodržování předpisů. K dispozici na adrese https://www.enisa.europa.eu/publications/nis-investments-2023

přičemž by využilo poznatky ze stávajících vnitrostátních projektů i z opatření financovaných v rámci programu Digitální Evropa, aby zajistilo praktické a účinné provádění.

Od roku 2014 se na financování řady výzkumných iniciativ zaměřených na zvyšování odolnosti zdravotnických zařízení, jako jsou nemocnice, proti kybernetickým hrozbám a na zmírnění rizik spojených se zneužitím nově vznikajících technologií podílejí programy Horizont. Výsledné produkty zahrnují sadu specializovaných nástrojů, rámců a systémů, jako jsou nástroje pro posuzování rizik, platformy pro sdílení dat chránící soukromí, kryptografická řešení, školicí programy pro zvyšování informovanosti o kybernetické bezpečnosti a systémy pro detekci hrozeb v reálném čase. Tato řešení byla zejména důkladně ověřena v pilotních implementacích v reálných zdravotnických prostředích, což zaručuje jejich účinnost a praktickou použitelnost při ochraně před kybernetickými hrozbami.

Zabezpečení dodavatelských řetězců v odvětví zdravotnictví

Klíčovou výzvou pro zdravotnické organizace je řízení komplexních dodavatelských řetězců IKT, které zahrnují řadu produktů, jako jsou zdravotnické prostředky připojené k internetu, systémy elektronických zdravotních záznamů a kancelářský hardware. Nemocnice a poskytovatelé zdravotní péče potřebují pro svůj provoz spolehlivé a bezpečné systémy a služby IKT. S cílem pomoci řešit problémy kybernetické bezpečnosti ve zdravotnictví by skupina pro spolupráci v oblasti bezpečnosti sítí a informací měla provést **koordinované posouzení bezpečnostních rizik, jež vyhodnotí technická i strategická rizika související s dodavatelskými řetězci zdravotnických prostředků a navrhne opatření na jejich zmírnění**[31]**.** Skupina pro spolupráci v oblasti bezpečnosti sítí a informací by měla podle potřeby spolupracovat s Koordinační skupinou pro zdravotnické prostředky.

Akt o kybernetické odolnosti je nový, komplexní rámec, který stanoví požadavky na kybernetickou bezpečnost, pokud jde o plánování, navrhování a vývoj, jakož i zpracování, opravování a hlášení aktivně zneužívaných zranitelností, a to pro téměř všechny hardwarové a softwarové produkty v každé fázi hodnotového řetězce[32]. Zdravotnické prostředky jsou typem výrobku, který se používá v jedné z nejcitlivějších oblastí naší společnosti. Požadavky na kybernetickou bezpečnost těchto výrobků vyplývají z již existujícího nařízení o zdravotnických prostředcích a nařízení o diagnostických zdravotnických prostředcích *in vitro*[33]. V rámci probíhajícího hodnocení těchto nařízení se zkoumá možnost větší soudržnosti a součinnosti mezi těmito rámci, aby bylo zaručeno zjednodušení a nejmodernější kybernetická bezpečnost.

Zjištění plynoucí z posouzení rizik by navíc měla zdravotnickým organizacím pomoci při přezkumu jejich postupů v oblasti kybernetické bezpečnosti dodavatelského řetězce, jak to vyžaduje směrnice

[31] Podle článku 22 směrnice NIS 2.
[32] V prvním kroku budou muset široké kategorie rádiových zařízení, které nespadají do oblasti působnosti nařízení o zdravotnických prostředcích a nařízení o diagnostických zdravotnických prostředcích *in vitro*, od 1. srpna 2025 při uvádění na jednotný trh splňovat základní požadavky směrnice o rádiových zařízeních, které se týkají kybernetické bezpečnosti. Ve druhé fázi, od 11. prosince 2027, se začne uplatňovat akt o kybernetické odolnosti.
[33] V prosinci 2019 vydala Koordinační skupina pro zdravotnické prostředky pokyny ke kybernetické bezpečnosti zdravotnických prostředků, které podporují výrobce při plnění požadavků přílohy I obou nařízení: https://ec.europa.eu/docsroom/documents/41863

NIS 2, a mohla by být podkladem pro vypracování nových **pokynů pro zadávání veřejných zakázek**[34]. Tyto pokyny, které vypracuje agentura ENISA prostřednictvím svého centra podpory, by měly odrážet nejnovější trendy, jako je přechod na ukládání údajů o pacientech v cloudu, včetně potřeby bezpečné migrace elektronických zdravotních údajů do cloudového prostředí. Nové pokyny by navíc měly organizacím nabídnout praktické nástroje pro sledování jejich dodavatelských řetězců, včetně poskytovatelů řízených bezpečnostních služeb, atestačních zpráv nebo posuzování rizik, která představují třetí strany.

V případě cloudu je třeba přijmout další opatření k řešení jedinečných problémů spojených se správou citlivých zdravotních údajů, včetně zvýšených bezpečnostních a provozních rizik a rizik souvisejících s ochranou soukromí. Pro posílení ochranných opatření doporučují odborníci přistupovat k cloudovým službám podle zásady „Security by Default and by Design“ (bezpečnost jako standard a již od fáze návrhu). Tento přístup upřednostňuje bezpečnou infrastrukturu, proaktivní správu zranitelností a kombinaci státních a soukromých cloudových řešení. Pro zajištění robustních bezpečnostních postupů je rovněž nezbytné průběžné monitorování a osvědčení specifická pro dodavatele – například certifikace poskytovatelů zabezpečení a audity shody s vnitrostátními a mezinárodními normami.

U služeb, jako jsou infrastruktura jako služba (IaaS), platforma jako služba (PaaS) a software jako služba (SaaS), je implementace bezpečnosti často na zákaznících. Mnohé zdravotnické organizace však nemají dostatek zdrojů, aby tyto požadavky mohly plnit samostatně. V rámci řešení tohoto problému **by poskytovatelé cloudových služeb měli být podporováni v zavádění základních bezpečnostních opatření jako standardního prvku**. Tato opatření by snížila riziko chybných konfigurací, zachovala konzistentní ochranu v prostředích spravovaných zákazníky a poskytla větší jistotu uživatelům. Při stanovení výchozí základní úrovně bezpečnosti by bylo cílem najít rovnováhu mezi spolehlivou ochranou a praktičností a zajistit použitelnost pro širokou škálu zdravotnických organizací. Toto úsilí by zahrnovalo úzkou spolupráci mezi poskytovateli cloudových služeb a odvětvím zdravotnictví s využitím osvědčených postupů v daných odvětvích k vytvoření účinných a škálovatelných řešení.

Odborná příprava a rozvoj dovedností

Pro dlouhodobě udržitelný růst a konkurenceschopnost v Evropě, stejně jako pro vysoce kvalitní služby, včetně zdravotnických služeb, je důležitá pracovní síla s požadovanými dovednostmi. Nedostatek kvalifikovaných odborníků na kybernetickou bezpečnost je v celé Evropě významným problémem, přičemž se odhaduje, že k uspokojení potřeb, pokud jde o pracovní sílu, v EU chybí 299 000 odborníků[35]. Podle průzkumu Eurobarometr 2024 o kybernetických dovednostech[36]považuje 81 % společností potíže s najímáním pracovníků v oblasti kybernetické bezpečnosti za klíčové riziko co do potenciálních

[34] V návaznosti na pokyny agentury ENISA pro zadávání veřejných zakázek v oblasti kybernetické bezpečnosti v nemocnicích z roku 2020 (únor 2020). K dispozici na adrese https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

[35] *The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study* (Kybernetická bezpečnost v roce 2024: poznatky ze studie ISC2 o pracovní síle v oblasti kybernetické bezpečnosti) | Platforma pro digitální dovednosti a pracovní místa

[36] Bleskový průzkum Eurobarometr 547 o kybernetických dovednostech.

kybernetických útoků. V odvětví vzdělávání, zdravotnictví a sociální práce je 66 % pozic v oblasti kybernetické bezpečnosti obsazeno zaměstnanci, kteří přecházejí z jiných pozic, než je kybernetická bezpečnost, což poukazuje na naléhavou potřebu rekvalifikací a prohlubování dovedností.

V zájmu řešení této výzvy by mělo centrum podpory spolupracovat s budoucím konsorciem evropské digitální infrastruktury (EDIC) pro kybernetické dovednosti, které je stanoveno ve sdělení Komise o Akademii dovedností v oblasti kybernetické bezpečnosti[37]. Tato práce by měla usnadnit výměnu informací mezi odborníky na kybernetickou bezpečnost ve zdravotnictví, jako jsou vedoucí pracovníci pro bezpečnost informací (CISO). Jedním z možných opatření by bylo vytvoření **Evropské sítě CISO ve zdravotnictví**, počínaje skupinou odborníků, kteří by sdíleli a rozvíjeli osvědčené postupy, strategie pro udržení talentů a řešení pro přilákání odborníků na kybernetickou bezpečnost do zdravotnictví. Kromě toho by měly být pod záštitou Akademie dovedností v oblasti kybernetické bezpečnosti vytvářeny zdroje pro posílení pracovních sil v oblasti kybernetické bezpečnosti ve zdravotnictví s podporou odvětví a akademické obce. V tomto ohledu by měly být zúčastněné strany v odvětví vybízeny, aby se zavázaly k podpoře zlepšování odborné přípravy v oblasti kybernetické bezpečnosti.

Hlavním faktorem přispívajícím ke kybernetickým bezpečnostním incidentům ve zdravotnictví jsou i nadále lidské chyby, což podtrhuje zásadní potřebu komplexní odborné přípravy personálu a informovanosti o kybernetické bezpečnosti. Vzhledem k tomu, že zdravotničtí pracovníci často používají digitální nástroje, je nezbytné je vybavit znalostmi bezpečných postupů. Cílená školení a osvětové kampaně mohou výrazně snížit rizika. V zájmu řešení tohoto problému by mělo centrum podpory spolupracovat se zdravotnickými pracovníky a poskytovateli zdravotní péče a společně s poskytovateli vzdělávání nebo odborné přípravy, průmyslem, konsorciem EDIC pro kybernetické dovednosti a orgány členských států vytvářet a šířit **rozsáhlé a snadno přístupné online vzdělávací moduly a kurzy**.

Pro vybudování pevných základů kybernetické bezpečnosti ve zdravotnictví je nezbytné začlenit do vzdělávacích osnov moduly digitálních kompetencí a kybernetické bezpečnosti. Tyto moduly by se měly zabývat otázkami specifickými pro dané odvětví, jako je ochrana údajů o pacientech a zranitelnosti zabezpečení zdravotnických prostředků. Vývoj těchto zdrojů by měl zohlednit předchozí kroky, jako je projekt BeWell financovaný v rámci programu Erasmus+[38] a projekt PANACEA financovaný v rámci programu Horizont 2020[39].

[37] Sdělení Komise Evropskému parlamentu a Radě: Řešení nedostatku talentů v oblasti kybernetické bezpečnosti za účelem posílení konkurenceschopnosti, růstu a odolnosti EU („Akademie dovedností v oblasti kybernetické bezpečnosti“). COM(2023) 207 final.

[38] BeWell – *Blueprint alliance for a future health workforce strategy on digital and green skills* (Plán aliance pro budoucí strategii v oblasti pracovní síly ve zdravotnictví a digitálních a zelených dovedností). K dispozici na adrese https://bewell-project.eu/

[39] PANACEA – *Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people* (Ochrana a soukromí nemocničních a zdravotnických infrastruktur pomocí inteligentní kybernetické bezpečnosti a sada nástrojů pro kybernetické hrozby pro údaje a člověka). K dispozici na adrese https://cordis.europa.eu/project/id/826293

3.2 Evropské kapacity pro odhalování kybernetických hrozeb pro zdravotnictví

Rychlá reakce na incidenty se neobejde bez účinné detekce kybernetických hrozeb. Aktéři hrozeb mohou využívat techniky, které znesnadňují odhalení průniku a umožňují, aby nepovolený přístup do systému přetrvával po dlouhou dobu[40]. Lepší schopnosti detekce hrozeb proto mohou pomoci zastavit kybernetické útoky v jejich počátcích. Například v případě ransomwarového útoku na finského poskytovatele psychoterapeutických služeb Vastaamo, při kterém pachatel vydíral pacienty, jejichž důvěrná zdravotnická dokumentace byla odcizena, došlo k prvotnímu průniku v roce 2018, ale poskytovatel se o něm dozvěděl až v roce 2020[41].

Efektivní sdílení informací a spolupráce jsou nezbytné pro lepší odhalování hrozeb a situační orientaci v celé EU. Důležitou roli při přijímání zpráv o incidentech, významných událostech a potenciálních hrozbách hrají týmy pro reakce na počítačové bezpečnostní incidenty (CSIRT), které poskytují pokyny k opatřením na zmírnění dopadů na vnitrostátní úrovni. **Členské státy se** však **důrazně vyzývají, aby všechna oznámení o kybernetických incidentech z nemocnic a od poskytovatelů zdravotní péče sdílely rovněž s centrem podpory agentury ENISA, a umožnily tak situační orientaci na úrovni EU**. V ideálním případě by to mělo být doprovázeno smysluplnou charakteristikou různých relevantních rozměrů incidentu, včetně známých základních zranitelností, dopadů na zdravotnické služby a nežádoucích událostí u pacientů. Výrobci zdravotnických prostředků a diagnostických prostředků *in vitro* se dále vyzývají, aby prostřednictvím jednotné platformy pro podávání zpráv, kterou zřídí a bude spravovat agentura ENISA v rámci aktu o kybernetické odolnosti, dobrovolně hlásili aktivně zneužívané zranitelnosti nebo závažné kybernetické incidenty, které mají dopad na bezpečnost těchto prostředků, jakož i případné další zranitelnosti, incidenty, závažné události nebo kybernetické hrozby, jež mohou ovlivnit rizikový profil těchto prostředků.

Pokud informace obsažené ve zprávách již nejsou citlivé, mohlo by centrum podpory vytvořit pod záštitou agentury ENISA evropský katalog známých zneužívaných zranitelností (KEV) týkajících se zdravotnických prostředků, systémů elektronických zdravotních záznamů a poskytovatelů vybavení a softwaru IKT ve zdravotnictví. K řešení významných problémů při odhalování hrozeb by centrum podpory mělo zavést **celoevropskou službu odběru včasných varování pro odvětví zdravotnictví, která by poskytovala výstrahy téměř v reálném čase**. Tato služba by čerpala ze zpracovaných údajů od týmů CSIRT, zdravotnických subjektů a výrobců, zpravodajských informací z otevřených zdrojů (OSINT) a dalších relevantních subjektů, jako jsou kybernetická centra, střediska pro sdílení a analýzu informací (ISAC) a donucovací orgány. Situační orientaci by dále zvýšila posílená spolupráce mezi agenturou ENISA a Agenturou Evropské unie pro spolupráci v oblasti prosazování práva (Europol) – například v oblasti vzorců kybernetické kriminality zaměřené proti odvětví zdravotnictví.

Střediska ISAC slouží jako ústřední zdroj operativních informací o kybernetických hrozbách, čímž podporují obousměrné sdílení informací mezi veřejným a soukromým sektorem a budování důvěry. Centrum podpory by mělo posílit podporu **evropského střediska ISAC pro zdravotnictví**

[40] *ENISA Health Threat Landscape* (zpráva agentury ENISA o situaci v oblasti hrozeb ve zdravotnictví), 2023.
[41] Rozhodnutí finského ombudsmana pro ochranu údajů č. 1150/161/2021.

prostřednictvím nástrojů a výměny informací, odvětvových zpráv o situační orientaci a také podporou důvěryhodného společenství pro taktickou a strategickou spolupráci. Členské státy by měly podporovat rozvoj vnitrostátních středisek ISAC pro zdravotnictví[42]. Střediska ISAC by měla být rovněž vybízena, aby nastolila spolupráci poskytovatelů zdravotní péče s výrobci, aby společně porozuměli hrozbám kybernetické bezpečnosti, a to i v dodavatelském řetězci, a k usnadnění dialogu o bezpečném návrhu produktů, který by skutečně zohledňoval realitu nasazení v praxi.

3.3 Rychlá reakce a obnovení

Vzhledem k vysoké citlivosti zdravotních údajů pacientů a potenciálně devastujícím dopadům kybernetických útoků na zdravotnické služby má pro zajištění bezpečnosti pacientů zásadní význam rychlá a účinná reakce na kybernetické bezpečnostní incidenty. Pokud nemocnice nebo poskytovatel zdravotní péče čelí kybernetickému útoku, je prvním kontaktním místem příslušný vnitrostátní CSIRT[43]. Úkolem týmu CSIRT je poskytovat včasnou podporu, ideálně do 24 hodin, a pomáhat tak zvládat významné incidenty. Pokud však incident přesáhne kapacitu týmu CSIRT, měla by být k dispozici podpora EU, aby byla zajištěna rychlá a účinná reakce.

Rezerva EU pro kybernetickou bezpečnost, zřízená na základě nařízení o kybernetické solidaritě, poskytuje služby reakce na incidenty od důvěryhodných poskytovatelů řízených bezpečnostních služeb na pomoc při významných nebo rozsáhlých kybernetických bezpečnostních incidentech a při počátečním úsilí o obnovení. Tato rezerva má doplnit úsilí týmů CSIRT členských států a umožnit jim požádat o další podporu v případech týkajících se kritických odvětví, jako je zdravotnictví. V zájmu posílení tohoto systému **by Komise a agentura ENISA měly zajistit, aby rezerva zahrnovala službu rychlé reakce speciálně určenou pro zdravotnictví.** Tato služba, která by doplňovala další stávající rámce, by nasazovala odborníky, kteří by bez prodlení řešili významné nebo rozsáhlé kybernetické bezpečnostní incidenty ve zdravotnictví, pokud by podpora na vnitrostátní úrovni nebyla dostatečná.

Pro zlepšení reakce a obnovení by mělo centrum podpory ve spolupráci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, sítí CSIRT a v příslušných případech Europolem vypracovat **operační protokoly pro reakci na kybernetické incidenty přizpůsobené odvětví zdravotnictví**. Tyto operační protokoly by byly vodítkem pro týmy CSIRT i zdravotnické organizace při reakci na konkrétní kybernetické bezpečnostní hrozby, včetně ransomwaru. Vzhledem k významu účinné spolupráce mezi týmy CSIRT a donucovacími orgány při reakci na kybernetické bezpečnostní incidenty kriminální povahy a jejich vyšetřování by operační protokoly měly mimo jiné poskytovat jasné pokyny pro hlášení takových incidentů donucovacím orgánům. Centrum podpory by dále mohlo **usnadnit rozsáhlé zavádění vnitrostátních cvičení v oblasti kybernetické bezpečnosti na základě zkušeností ze**

[42] Například Finsko má národní ISAC pro oblast sociální péče a zdravotnictví. Viz *Finnish National Cybersecurity Centre: ISAC information sharing groups* (Finské národní centrum kybernetické bezpečnosti: Skupiny pro sdílení informací ISAC), k dispozici na adrese https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups

[43] Ustanovení čl. 23 odst. 1 směrnice NIS 2 stanoví, že základní a důležité subjekty mají povinnost oznamovat významné incidenty příslušnému týmu CSIRT nebo případně příslušnému orgánu.

cvičení, jako bylo cvičení agentury ENISA Cyber Europe 2022, s cílem tyto operační protokoly vyzkoušet a posílit protokoly pro reakci na incidenty.

Pro informovanou tvorbu politik a hodnocení účinnosti opatření přijatých proti ransomwarovým útokům je nutné shromažďovat další údaje. Za tímto účelem by členské státy měly požadovat, aby subjekty, na které se vztahuje směrnice NIS 2, včetně zdravotnických organizací, podávaly zprávy o všech platbách výkupného, které provedly nebo hodlají provést, spolu s dalšími informacemi, které poskytují při hlášení významných kybernetických bezpečnostních incidentů. Takové podávání zpráv podporuje účinné vyšetřování ransomwarových incidentů, včetně sledování plateb na platformách pro směnu kryptoměn s cílem identifikovat příjemce.

Rychlost obnovení je rozhodujícím faktorem pro udržení odolnosti a důvěry veřejnosti, zejména ve zdravotnictví, kde výpadky mohou narušit péči o pacienty. Pro účinné obnovení po ransomwarových útocích musí mít poskytovatelé zdravotní péče bezpečné, aktuální a izolované zálohy, které lze rychle obnovit. Centrum podpory by mohlo v rámci svého katalogu služeb nabízet **subskripční službu obnovy po napadení ransomwarem, která by nemocnicím a poskytovatelům zdravotní péče pomohla předem připravit plány obnovení**. Agentury ENISA a Europol by měly spolupracovat na identifikaci nejčastějších typů ransomwaru zaměřených na zdravotnické organizace a **rozšířit úložiště dešifrovacích nástrojů** dostupné v rámci projektu „No More Ransom“[44]. Měly by také vypracovat a propagovat dostupné pokyny, které pomohou poskytovatelům zdravotní péče využít dešifrovací nástroje a vyhnout se tak placení výkupného.

Mezinárodní iniciativa pro boj proti ransomwaru[45] je cennou platformou pro výměnu informací o konkrétních ransomwarových incidentech a pro budování kapacit členských států s cílem posílit jejich rámce pro kybernetickou bezpečnost a vyšetřovací kapacity vůči aktérům používajícím ransomware. Komise bude společně s vysokou představitelkou pokračovat v rozvoji spolupráce v rámci této iniciativy, a to i v boji proti ransomwarovým hrozbám pro odvětví zdravotnictví. Kromě toho bude Komise usilovat o spolupráci v **pracovní skupině G7 pro kybernetickou bezpečnost** s cílem posílit kybernetickou bezpečnost ve zdravotnictví. Pracovní skupina by mohla zejména zvážit možnosti podpory zdravotnictví v boji proti hrozbám, jako je ransomware, a vycházet přitom z úvah obsažených například ve společném prohlášení o ransomwarových útocích na zdravotnická zařízení, které bylo předloženo dne 8. listopadu 2024 v rámci Rady bezpečnosti OSN[46].

[44] https://www.nomoreransom.org/en/index.html
[45] https://www.counter-ransomware.org/
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

4. Vnitrostátní opatření

Schopnost tohoto akčního plánu zlepšit kybernetickou bezpečnost v odvětví zdravotnictví závisí na aktivním zapojení a závazku členských států. Pro úspěšnou realizaci akčního plánu by členské státy mohly jmenovat **národní centra podpory kybernetické bezpečnosti, která by byla určena speciálně pro nemocnice a** poskytovatele **zdravotní péče**. Tato centra by fungovala jako hlavní kontaktní místa pro zdravotnictví na vnitrostátní úrovni a úzce spolupracovala s centrem podpory agentury ENISA. Pokud je to možné a relevantní, měly by členské státy určit jako národní centra podpory kybernetické bezpečnosti stávající subjekty, jako jsou vnitrostátní týmy CSIRT pro zdravotnictví nebo příslušné orgány.

Členské státy se rovněž vyzývají, aby vytvořily **národní akční plány zaměřené na kybernetickou bezpečnost v odvětví zdravotnictví**. V těchto plánech by byla uvedena konkrétní rizika kybernetické bezpečnosti, kterým zdravotnické systémy čelí, a opatření, která jsou na vnitrostátní úrovni přijímána k jejich řešení, a zároveň by bylo zajištěno účinné využívání zdrojů a postupů na evropské úrovni. Centrum podpory agentury ENISA může při vypracovávání těchto plánů pomoci, přičemž zohlední již existující národní plány a bude koordinovat úsilí, aby se zdroje a strategie jednotlivých členských států vzájemně doplňovaly.

Dalším klíčovým tématem pro členské státy je usnadnění sdílení zdrojů mezi poskytovateli zdravotní péče, čehož lze dosáhnout prostřednictvím **společného zadávání veřejných zakázek nebo sdružování zdrojů** na vnitrostátní, regionální, nebo dokonce evropské úrovni. Tento přístup by snížil finanční zátěž jednotlivých subjektů a zároveň zvýšil jejich vyjednávací sílu při jednání s poskytovateli služeb kybernetické bezpečnosti.

Například francouzský program CaRE[47] zavedl na vnitrostátní a regionální úrovni řadu opatření, která mají řešit problémy se získáváním zdrojů: kybernetický katalog poskytuje přehled kybernetických řešení a balíčků, které jsou nemocnicím k dispozici prostřednictvím národní agentury pro kybernetickou bezpečnost, agentury pro digitální zdravotnictví, regionálních agentur a národních nákupních organizací, jakož i komerčních řešení. To je doplněno dalšími finančními prostředky pro regionální agentury, které nabízejí sdílené zdroje.

Členské státy by se rovněž měly zabývat nedostatečnou úrovní investic do kybernetické bezpečnosti ve zdravotnictví. Aby zajistily dostatečné financování, měly by stanovit **nezávazné referenční úrovně a sledovat cíle financování zaměřené konkrétně na kybernetickou bezpečnost** a zároveň zajistit, aby tyto investice nebyly na újmu základní péči o pacienty. Tyto cíle financování by se měly rovněž zaměřit na začlenění bezpečnostních aspektů do všech digitálních investic v tomto odvětví. Členské státy si

[47] Francouzská agentura pro digitální zdraví: *Cybersécurité acceleration et Résilience des Établissements (CaRE)*. K dispozici na adrese https://esante.gouv.fr/strategie-nationale/cybersecurite

mohou vyměňovat osvědčené postupy a rady týkající se těchto cílů prostřednictvím platforem, jako je síť pro elektronické zdravotnictví[48].

5. Spolupráce veřejného a soukromého sektoru

Pro úspěšnou realizaci akčního plánu je zásadní spolupráce veřejného a soukromého sektoru a konzultace s poskytovateli zdravotní péče, dalšími subjekty ve zdravotnictví a příslušnými subjekty z odvětví kybernetické bezpečnosti. Aby **Komise** dále přispívala k práci centra podpory, zřídí **s podporou agentury ENISA společný poradní výbor pro kybernetickou bezpečnost ve zdravotnictví**, v němž zasednou vysocí představitelé obou oborů, zdravotnictví i kybernetické bezpečnosti, a který může Komisi a centru podpory poskytovat poradenství ohledně účinných opatření a projednávat další rozvoj partnerství veřejného a soukromého sektoru v této oblasti. Výbor bude vycházet ze stávajícího úsilí o partnerství veřejného a soukromého sektoru, včetně vnitrostátních středisek ISAC pro zdravotnictví.

Komise dále zveřejní **výzvu k přijetí opatření** pro společnosti, nadace, vzdělávací instituce a zúčastněné strany z odvětví kybernetické bezpečnosti, **aby se zavázaly k opatřením zaměřeným na řešení problémů v tomto odvětví**. V návaznosti na zkušenosti s Akademií dovedností v oblasti kybernetické bezpečnosti by takové závazky mohly být například přísliby v rámci Akademie dovedností v oblasti kybernetické bezpečnosti, které by zahrnovaly poskytování vzdělávacích kurzů a materiálů se zaměřením na odvětví zdravotnictví pro odborníky v oblasti kybernetické bezpečnosti[49]. Další závazky by se mohly týkat také činností zaměřených na zvyšování informovanosti nebo poskytování řízených bezpečnostních služeb zvláště zranitelným subjektům zdarma nebo za sníženou cenu, aby se zvýšila jejich připravenost a odolnost v oblasti kybernetické bezpečnosti. Kromě toho by tyto závazky mohly spočívat ve sdílení operativních informací o kybernetických hrozbách s centrem podpory agentury ENISA. Centrum podpory by si mělo udržovat přehled o závazcích přijatých v rámci výzvy k přijetí opatření s cílem zajistit jejich soudržnost a vzájemné doplňování.

6. Odrazování aktérů kybernetických hrozeb

Vnitřní a vnější politiky EU v oblasti kybernetické bezpečnosti by měly podporovat cíl odradit aktéry kybernetických hrozeb od útoků na evropské systémy zdravotní péče. Kybernetické útoky na zdravotnické organizace jsou obzvláště nepřijatelným typem škodlivé kybernetické činnosti, protože mohou ohrozit bezpečnost pacientů a lidské životy. Proto je třeba využít všech odstrašujících schopností EU v oblasti kybernetické bezpečnosti a vymáhání práva, aby byl narušen celkový obchodní model aktérů hrozeb, kteří se zaměřují na odvětví zdravotnictví, a tito aktéři byli připraveni o snadné zisky. To by zahrnovalo podporu přeshraničního vyšetřování prostřednictvím lepšího sdílení indikátorů kompromitace a dalších relevantních údajů a zvýšené zaměření na cíle s vysokou hodnotou a klíčové

[48] Síť pro elektronické zdravotnictví je dobrovolná síť vnitrostátních orgánů odpovědných za elektronické zdravotnictví, jež určily členské státy, zřízená na základě článku 14 směrnice 2011/24/EU.

[49] Akademie dovedností v oblasti kybernetické bezpečnosti: Zapojte se | Platforma pro digitální dovednosti a pracovní místa

prvky napomáhající trestné činnosti, jako jsou například „neprůstřelné“ hostingové služby nebo služby mixování kryptoměn.

Soubor nástrojů pro diplomacii v oblasti kybernetiky nabízí rámec pro předcházení kybernetickým útokům proti EU, členským státům a partnerům, odrazování od těchto útoků a reakci na ně. Vysoká představitelka bude i nadále využívat stávající rámec kybernetických sankcí k reakci na hrozby zaměřené na systémy zdravotní péče.

Důležitým odrazujícím prvkem je činit pachatele trestné činnosti zodpovědné za jejich skutky. Členské státy by proto měly zajistit, aby vymáhání práva bylo plně začleněno do jejich národních akčních plánů. Zejména by měly plně využívat ustanovení směrnice o útocích na informační systémy[50] a Budapešťské úmluvy Rady Evropy o počítačové kriminalitě, aby odrazovaly od útoků, předávaly pachatele spravedlnosti a likvidovaly zločinecké infrastruktury napomáhající útokům[51]. Úspěšná implementace těchto nástrojů by měla zajistit, aby byly trestné a škodlivé činy proti zdravotnictví trestány.

7. Provádění a monitorování akčního plánu

V tomto akčním plánu se počítá s řadou úkolů, které má centrum podpory zřízené v rámci agentury ENISA plnit. Tím je zajištěno ucelené a soudržné provádění akčního plánu a zároveň se zamezí vytváření nových subjektů, což by mohlo vést k překrývání činností a režijním nákladům. Komise má v úmyslu zajistit pro centrum podpory odpovídající zdroje.

Po zahájení činnosti centra podpory by agentura ENISA měla po konzultaci s Komisí pravidelně poskytovat aktuální informace o práci centra podpory správní radě agentury ENISA a příslušným sítím členských států, zejména skupině pro spolupráci v oblasti bezpečnosti sítí a informací, síti CSIRT, síti pro elektronické zdravotnictví a v příslušných případech Radě pro evropský prostor pro zdravotní údaje. Agentura ENISA by si dále měla průběžně vyměňovat informace o provádění opatření zajištěných centrem podpory s veřejně-soukromým poradním výborem pro kybernetickou bezpečnost ve zdravotnictví.

Pravidelné zprávy agentury ENISA, jako je zpráva o stavu kybernetické bezpečnosti v Unii, která poskytuje souhrnné posouzení úrovně vyspělosti schopností a zdrojů v oblasti kybernetické bezpečnosti v celé EU, včetně odvětví zdravotnictví, by měly sloužit jako příležitost ke zveřejnění příslušných údajů, což podpoří monitorování akčního plánu. Kromě toho může index kybernetické bezpečnosti EU agentury ENISA[52] poskytnout kvantitativní a kvalitativní údaje, které poslouží jako důkazní základna pro posouzení kritičnosti a vyspělosti odvětví zdravotnictví.

---

[50] Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

[51] Úmluva o počítačové kriminalitě (Budapešťská úmluva, ETS č. 185) a její protokoly: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[52] ENISA, *EU Cybersecurity Index, Framework and Methodological Note* (Index kybernetické bezpečnosti EU, rámec a metodická poznámka, 2024). K dispozici na adrese https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf

8. Další kroky

Toto sdělení stanovilo ambiciózní program pro kyberneticky bezpečnější odvětví zdravotnictví v EU. Akční plán navrhuje rozvoj centra podpory kybernetické bezpečnosti pro nemocnice a poskytovatele zdravotní péče jako ústředního prvku agentury ENISA, a vytyčuje tak cestu k vytvoření soudržného a sdíleného evropského přístupu k výzvám týkajícím se kybernetické bezpečnosti v tomto odvětví.

Toto sdělení by mělo být považováno za začátek procesu zlepšování kybernetické bezpečnosti v odvětví zdravotnictví. Proto bude přijetí akčního plánu doprovázeno zahájením komplexních konzultací se zúčastněnými stranami a pokračováním výměn s členskými státy a příslušnými sítěmi za účelem shromáždění poznatků. Na základě výsledků konzultací hodlá Komise ve čtvrtém čtvrtletí roku 2025 předložit doporučení k dalšímu upřesnění akčního plánu.

Komise vyzývá členské státy a všechny zúčastněné strany, aby spolupracovaly na naplnění ambicí akčního plánu.

PŘÍLOHA – Přehled navrhovaných opatření

Komise:

Centrum podpory kybernetické bezpečnosti agentury ENISA pro nemocnice a poskytovatele zdravotní péče	
Zajistit odpovídající prostředky pro centrum podpory kybernetické bezpečnosti Spolupracovat s centrem ECCC na zahájení pilotních projektů s cílem vyvinout osvědčené postupy pro kybernetickou hygienu a posouzení bezpečnostních rizik a řešit potřebu nepřetržitého monitorování kybernetické bezpečnosti, operativních informací o hrozbách a reakce na incidenty s využitím nejmodernějších řešení v oblasti kybernetické bezpečnosti, s cílem vytvořit katalog služeb Evropského centra podpory kybernetické bezpečnosti	2025
Prevence kybernetických bezpečnostních incidentů	
Po konzultaci se skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, sítí EU-CyCLONe a agenturou ENISA prozkoumat možnost určit zdravotnictví jako odvětví, kterému lze poskytnout podporu na koordinované testování připravenosti v rámci nařízení o kybernetické solidaritě	1. čtvrtletí 2025
Rychlá reakce a obnovení	
Společně s agenturou ENISA zajistit, aby rezerva EU pro kybernetickou bezpečnost zahrnovala službu rychlé reakce speciálně pro odvětví zdravotnictví	4. čtvrtletí 2025
Spolupráce veřejného a soukromého sektoru	
S podporou agentury ENISA zřídit společný poradní výbor pro kybernetickou bezpečnost ve zdravotnictví	1. čtvrtletí 2025
Vyhlásit výzvu k přijetí opatření pro společnosti, nadace, vzdělávací instituce a zúčastněné strany z odvětví kybernetické bezpečnosti, aby se zavázaly k opatřením k řešení problémů v odvětví zdravotnictví	2. čtvrtletí 2025
Odrazování aktérů kybernetických hrozeb	
Společně s vysokou představitelkou prozkoumat využití opatření souboru nástrojů pro diplomacii v oblasti kybernetiky k předcházení nepřátelské činnosti	2025

vůči systémům zdravotní péče, odrazování a odstrašování od této činnosti a k reakci na ni	
Společně s vysokou představitelkou pokročit v mezinárodní spolupráci v boji proti aktérům používajícím ransomware, zejména v rámci mezinárodní iniciativy pro boj proti ransomwaru	2025–2026
Usilovat o spolupráci v pracovní skupině G7 pro kybernetickou bezpečnost s cílem posílit kybernetickou bezpečnost v odvětví zdravotnictví	2025–2026
Další kroky	
Zahájit komplexní konzultace se zúčastněnými stranami	1. čtvrtletí 2025
Přijmout doporučení k dalšímu upřesnění akčního plánu	4. čtvrtletí 2025

ENISA:

Evropské centrum podpory kybernetické bezpečnosti pro nemocnice a poskytovatele zdravotní péče	
Zahájit práce na zřízení Evropského centra podpory kybernetické bezpečnosti pro nemocnice a poskytovatele zdravotní péče	2. čtvrtletí 2025
Vypracovat komplexní katalog služeb, které bude centrum podpory kybernetické bezpečnosti poskytovat	Od 4. čtvrtletí 2025
Prevence kybernetických bezpečnostních incidentů	
Vydat pokyny, které vyzdvihnou nejdůležitější postupy v oblasti kybernetické bezpečnosti a pomohou poskytovatelům zdravotní péče při jejich implementaci	3. čtvrtletí 2025
V úzké spolupráci s Komisí a členskými státy vyvinout nástroj pro mapování právních předpisů	1. čtvrtletí 2025
Vyvinout rámec pro posouzení vyspělosti kybernetické bezpečnosti specifický pro zdravotnictví	3. čtvrtletí 2025
Provádět každoroční posouzení kybernetické vyspělosti zdravotnictví	2025–2026

Spolupracovat s členskými státy a orgány odpovídajícími za regionální programy na vytvoření modelových programů voucherů na kybernetickou bezpečnost	2025–2026
Vypracovat nové pokyny pro zadávání veřejných zakázek v oblasti kybernetické bezpečnosti nemocnic a poskytovatelů zdravotní péče	3. čtvrtletí 2025
Vytvořit Evropskou síť CISO ve zdravotnictví	1. čtvrtletí 2026
Vytvořit a propagovat vzdělávací moduly a kurzy pro zdravotnické pracovníky	1. čtvrtletí 2026
Evropské kapacity pro odhalování kybernetických hrozeb pro zdravotnictví	
Vytvořit evropský katalog známých zneužívaných zranitelností (KEV) pro zdravotnické prostředky, systémy elektronických zdravotních záznamů a poskytovatele zařízení a softwaru IKT v odvětví zdravotnictví	4. čtvrtletí 2025
Zavést celoevropskou službu odběru včasných varování pro odvětví zdravotnictví	Od roku 2026
Podporovat evropské středisko ISAC pro zdravotnictví nástroji a výměnou informací	2025–2026
Rychlá reakce a obnovení	
Společně s Komisí zajistit, aby rezerva EU pro kybernetickou bezpečnost zahrnovala službu rychlé reakce speciálně pro odvětví zdravotnictví	4. čtvrtletí 2025
Ve spolupráci se sítí CSIRT vypracovat operační protokoly pro reakci na kybernetické incidenty přizpůsobené pro zdravotnictví	3. čtvrtletí 2025
Usnadnit rozsáhlé zavedení vnitrostátních cvičení kybernetické bezpečnosti s cílem operační protokoly vyzkoušet a posílit protokoly pro reakci na incidenty	Od 4. čtvrtletí 2025
Poskytovat subskripční službu obnovy po napadení ransomwarem	Od roku 2026
Společně s Europolem identifikovat nejčastější typy ransomwaru zaměřeného na zdravotnické organizace a rozšířit úložiště dešifrovacích nástrojů prostřednictvím projektu „No More Ransom“	4. čtvrtletí 2025

Společně s Europolem vypracovat přístupné pokyny, které pomohou poskytovatelům zdravotní péče vyhnout se placení výkupného	3. čtvrtletí 2025
Vnitrostátní opatření	
Pomáhat členským státům při vypracovávání národních akčních plánů	2025
Koordinovat úsilí s cílem zajistit, aby se zdroje a strategie jednotlivých členských států vzájemně doplňovaly	2025–2026
Provádění a monitorování akčního plánu	
Po konzultaci s Komisí pravidelně poskytovat příslušným sítím členských států aktuální informace o práci centra podpory kybernetické bezpečnosti	2025–2026
Průběžně si vyměňovat informace s poradním výborem pro kybernetickou bezpečnost ve zdravotnictví	2025–2026

Členské státy:

Evropské kapacity pro odhalování kybernetických hrozeb pro zdravotnictví	
Sdílet oznámení o incidentech od nemocnic a poskytovatelů zdravotní péče v rámci NIS 2 s Evropským centrem podpory kybernetické bezpečnosti	Od 4. čtvrtletí 2025
Podporovat rozvoj vnitrostátních středisek ISAC pro zdravotnictví	2025–2026
Prevence kybernetických bezpečnostních incidentů	
V rámci skupiny pro spolupráci v oblasti bezpečnosti sítí a informací provést koordinované posouzení bezpečnostních rizik a vyhodnotit technická i strategická rizika související s dodavatelskými řetězci zdravotnických prostředků	4. čtvrtletí 2025
Rychlá reakce a obnovení	
Zavést vnitrostátní cvičení kybernetické bezpečnosti s cílem vyzkoušet operační protokoly a posílit protokoly pro reakci na incidenty	Od roku 2026

Vnitrostátní opatření	
Určit národní centra podpory kybernetické bezpečnosti pro nemocnice a poskytovatele zdravotní péče	2. čtvrtletí 2025
Vytvořit národní akční plány zaměřené na kybernetickou bezpečnost v odvětví zdravotnictví	4. čtvrtletí 2025
Usnadnit sdílení zdrojů mezi poskytovateli zdravotní péče	2025–2026
Stanovit nezávazné referenční úrovně a sledovat cíle financování zaměřené konkrétně na kybernetickou bezpečnost	4. čtvrtletí 2025
Požadovat, aby zdravotnické organizace a další subjekty, na které se vztahuje směrnice NIS 2, oznamovaly své záměry zaplatit výkupné	4. čtvrtletí 2025