Rada
Európskej únie

V Bruseli 16. januára 2025
(OR. en)

5426/25

CYBER 21
SAN 15

SPRIEVODNÁ POZNÁMKA

Od:	Martine DEPREZOVÁ, riaditeľka, v zastúpení generálnej tajomníčky Európskej komisie
Dátum doručenia:	15. januára 2025
Komu:	Thérèse BLANCHETOVÁ, generálna tajomníčka Rady Európskej únie
Č. dok. Kom.:	COM(2025) 10 final
Predmet:	OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV Európsky akčný plán pre kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti

Delegáciám v prílohe zasielame dokument COM(2025) 10 final.

Príloha: COM(2025) 10 final

EURÓPSKA
KOMISIA

V Bruseli 15. 1. 2025
COM(2025) 10 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

Európsky akčný plán pre kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti

1. Úvod

Bezpečnostné prostredie EÚ sa rýchlo mení a dochádza k eskalácii hybridných útokov a kybernetických útokov, ktorých cieľom je nielen destabilizovať našu spoločnosť, rozdeliť ju a narušiť jej fungovanie, ale aj profitovať z počítačovej kriminality. Európa preto musí urýchlene posilniť svoju pripravenosť na túto novú realitu a odolnosť voči nej, a to vo všetkých sektoroch a v súlade s „celospoločenským“ a „nadrezortným“ prístupom, ako sa požaduje v správe osobitného poradcu predsedníčky Európskej komisie Sauliho Niinistöa.

Bezpečné a odolné systémy zdravotnej starostlivosti sú základom sociálneho modelu EÚ. Nemocnice a systémy zdravotnej starostlivosti však čelia čoraz väčším hrozbám, najmä zo strany ransomvérových gangov, ktoré sa na ne zameriavajú s cieľom dosiahnuť finančný zisk, a to z dôvodu vysokej hodnoty údajov pacientov vrátane elektronických zdravotných záznamov. Sektor zdravotníctva sa za posledné štyri roky skutočne stal sektorom, ktorý bol v EÚ najčastejšie vystavený útokom, a to aj počas pandémie ochorenia COVID-19, keď bola zdravotnícka infraštruktúra v rastúcej miere terčom kybernetických útokov. Kybernetické útoky na nemocnice a poskytovateľov zdravotnej starostlivosti spôsobujú priame škody ľuďom, vedú k odďaľovaniu lekárskych postupov, spôsobujú zablokovanie centrálnych príjmov a v extrémnych prípadoch môžu viesť až k stratám na životoch.

V stávke je ešte viac, keďže tento sektor prechádza zásadnou digitálnou transformáciou. Vďaka elektronickému zdravotníctvu a využívaniu a opätovnému používaniu zdravotných údajov môžu existovať modely starostlivosti, ktoré lepšie vyhovujú potrebám a preferenciám obyvateľov a pacientov, a to tým, že predchádzajú vzniku ochorenia alebo umožňujú skoršiu liečbu. Integrácia digitálnych nástrojov a riešení do klinických procesov, ako aj využívanie a opakované používanie zdravotných údajov môžu prispieť k lepším klinickým rozhodnutiam, k automatizácii v zdravotníctve, ako aj k rýchlejšej a kvalitnejšej starostlivosti o pacientov. Digitálne nástroje, využívanie údajov a zdravotnícke pomôcky, ktoré sú často pripojené na internet a využívajú umelú inteligenciu, sú takisto kľúčom k riešeniu výziev, medzi ktoré patrí nedostatok zdravotníckych pracovníkov.

Digitálne nástroje zároveň rozširujú okruh potenciálnych cieľov páchateľov počítačovej kriminality. Okrem toho sa niektorí štátni aktéri nevyhýbajú útokom na zdravotnícke zariadenia, ako o tom svedčí prebiehajúca útočná vojna Ruska proti Ukrajine. Sektor zdravotníctva sa tak stáva potenciálnym cieľom kybernetických útokov v rámci širšej hybridnej kampane. Kybernetické útoky nielen ohrozujú bezpečnosť pacientov, ale aj narúšajú dôveru verejnosti v zdravotnícku infraštruktúru a sú spojené so značnými nákladmi na obnovu. Odolná a bezpečná digitálna infraštruktúra nielenže poskytuje ochranu pred kybernetickými útokmi, ale má aj zásadný význam pre podporu implementácie a úplného zavedenia európskeho priestoru pre zdravotné údaje[1] (EHDS).

Preto je načase zvýšiť úroveň kybernetickej bezpečnosti a odolnosti európskych nemocníc a poskytovateľov zdravotnej starostlivosti a posilniť ich, ako zdôraznila predsedníčka von der Leyenová vo svojich politických usmerneniach pre Komisiu na roky 2024 – 2029[2]. Tento akčný plán je reakciou na naliehavosť situácie a jedinečné hrozby, ktorým sektor zdravotníctva čelí. Neexistuje jednoduché

[1] https://www.consilium.europa.eu/sk/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_sk.

„zázračné“ riešenie výziev v oblasti kybernetickej bezpečnosti v zdravotníctve. Namiesto toho akčný plán vyzýva na posilnenie prevencie a pripravenosti a na koordinovanejší prístup k solidarite so súčasným využitím odborných znalostí európskeho odvetvia kybernetickej bezpečnosti. Akčný plán ako taký odzrkadľuje prístup EÚ k bezpečnosti, ktorý sa bude ďalej rozvíjať a formalizovať v pripravovanej európskej stratégii vnútornej bezpečnosti, ktorá má definovať komplexnú reakciu na všetky hrozby v oblasti vnútornej bezpečnosti so zameraním na schopnosť predvídať hrozby, predchádzať škodám a chrániť ľudí, a to konaním na všetkých úrovniach na základe celospoločenského prístupu.

Sektor zdravotníctva zahŕňa široký počet subjektov a aktérov, medzi ktorých patria nemocnice, kliniky, zariadenia opatrovateľskej služby, rehabilitačné centrá a rôzni poskytovatelia zdravotnej starostlivosti, ako aj farmaceutické, medicínske a biotechnologické sektory, výrobcovia zdravotníckych pomôcok a zdravotnícke výskumné inštitúcie. Tento akčný plán sa zameriava predovšetkým na kybernetickú bezpečnosť nemocníc a poskytovateľov zdravotnej starostlivosti, ktorými sa rozumie akákoľvek fyzická alebo právnická osoba – alebo akýkoľvek iný subjekt – legálne poskytujúci zdravotnú starostlivosť na území členského štátu[3]. Nemocnice a poskytovatelia zdravotnej starostlivosti sú vzájomne prepojení s inými zdravotníckymi subjektmi a sú najbližšie k ľuďom. Zároveň by sa opatrenia na zvýšenie kybernetickej bezpečnosti nemocníc a poskytovateľov zdravotnej starostlivosti mali zamerať aj na riziká, ktoré ovplyvňujú širší dodávateľský reťazec a ekosystém, pričom vznikajú napríklad u subjektov, ktoré využívajú zdravotné údaje na výskum a strojové učenie alebo ktoré vyrábajú zdravotnícke pomôcky, najmä digitálne podporované zdravotnícke pomôcky, ktoré sa pripájajú na internet alebo k iným zariadeniam („internet vecí“).

Hoci je zabezpečenie systémov zdravotnej starostlivosti predovšetkým v kompetencii jednotlivých štátov, zdravotníctvo je kritickým odvetvím aj podľa smernice o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (NIS 2)[4]. Páchatelia počítačovej kriminality a iní aktéri hrozieb pôsobia cezhranične a aj výzvy v oblasti kybernetickej bezpečnosti, ktorým čelia zdravotnícke organizácie, sú podobné vo všetkých členských štátoch. Spolupráca na európskej úrovni je cenná z hľadiska spoločného využívania a rozširovania najlepších postupov na úrovni EÚ a na vnútroštátnej úrovni. V akčnom pláne sa preto navrhuje koordinácia a opatrenia na úrovni EÚ a zároveň sa v ňom členské štáty vyzývajú, aby prijali opatrenia, ktoré môžu v tejto súvislosti priniesť zmenu v oblasti zdravotnej starostlivosti a širšieho ekosystému zdravotníctva.

Akčný plán sa zameriava na budovanie kapacít sektora, aby sa prvom rade **predchádzalo** kybernetickým bezpečnostným incidentom, pretože prevencia je vždy lepšia ako liečba. Po druhé, v akčnom pláne sa podrobne opisujú opatrenia na zlepšenie zdieľania informácií o kybernetickej bezpečnosti a spôsobilosti **odhaľovať** kybernetické hrozby, vďaka čomu bude možné rýchlejšie reagovať. Po tretie, uvádzajú sa v ňom opatrenia s cieľom lepšie **reagovať** na incidenty a **zotaviť sa** z nich. V akčnom pláne sa takisto

[3] Článok 3 písm. g) smernice Európskeho parlamentu a Rady 2011/24/EÚ o uplatňovaní práv pacientov pri cezhraničnej zdravotnej starostlivosti, https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32011L0024.

[4] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii (smernica NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

predpokladajú spôsoby, ako **odradiť** aktérov kybernetických hrozieb od útokov na systémy zdravotnej starostlivosti v Európe.

Akčný plán sa bude realizovať v spolupráci s poskytovateľmi zdravotnej starostlivosti a so širším ekosystémom zdravotníctva, s členskými štátmi a komunitou kybernetickej bezpečnosti. Kľúčom k ďalšiemu vymedzeniu a zdokonaleniu opatrení s najväčším vplyvom je prístup založený na spolupráci, aby z nich mohli mať prospech všetci kritickí poskytovatelia zdravotnej starostlivosti v Európe. Spolu s týmto oznámením sa preto začnú komplexné konzultácie so zainteresovanými stranami, odvetvím a členskými štátmi. Medzinárodná spolupráca je v prípade kybernetickej bezpečnosti dôležitá vzhľadom na prepojenú povahu kybernetických hrozieb, ktoré nepoznajú hranice. Porovnateľné kybernetické hrozby existujú aj v krajinách zapojených do procesu rozširovania a v krajinách európskeho susedstva, ako aj v ďalších strategických partnerských krajinách EÚ. To môže v konečnom dôsledku ohroziť bezpečnosť kritickej infraštruktúry v EÚ. Poznatky získané pri vykonávaní akčného plánu bude preto dôležité zohľadniť aj pri spolupráci EÚ s krajinami zapojenými do procesu rozširovania, ako aj s ďalšími partnerskými krajinami, a to vzhľadom na úrovne hrozieb, ktorým sú jednotlivé krajiny vystavené.

2. Výzvy v oblasti kybernetickej bezpečnosti týkajúce sa nemocníc a poskytovateľov zdravotnej starostlivosti

Kybernetické hrozby pre sektor zdravotníctva

Kybernetické útoky sú na vzostupe na celom svete aj v rámci EÚ, pričom panoráma hrozieb je čoraz komplexnejšia a dynamickejšia. Pokroky v oblasti umelej inteligencie poskytujú zločineckým a zlomyseľným aktérom výkonné nástroje na zvýšenie presnosti a vplyvu ich operácií a zároveň menia možnosti kybernetickej obrany tým, že umožňujú automatizované opatrenia proti útokom v reálnom čase.

Kritickou výzvou v oblasti kybernetickej bezpečnosti v EÚ a na celom svete zostáva ransomvér, pričom podľa jednej správy sa v dôsledku ransomvéru do roku 2031 odhadujú celosvetové ročné náklady vo výške viac ako 250 miliárd EUR[5]. Pri útoku pomocou ransomvéru páchatelia nielenže zašifrujú údaje obetí a požadujú výkupné, ale čoraz častejšie vynášajú citlivé informácie s cieľom vyvíjať ďalší tlak. Ďalšou významnou výzvou sú zraniteľnosti softvéru a hardvéru: podľa Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA)[6] je zdravotníctvo sektorom s najväčším počtom nahlásených bezpečnostných incidentov súvisiacich s takýmito zraniteľnosťami[7]. K ďalším rastúcim hrozbám patria

[5] Morgan S., „*Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*“ (Predpokladá sa, že celosvetové škody spôsobené ransomvérom prekročia 265 miliárd USD do roku 2031), Cybersecurity Ventures (naposledy konzultované 1. júna 2024). K dispozícii na https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (akt o kybernetickej bezpečnosti), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

[7] *ENISA Threat Landscape: Health Sector* (Panoráma hrozieb pre sektor zdravotníctva podľa agentúry ENISA) (júl 2023).

distribuované útoky na vyradenie služby (DDoS), ktorých cieľom je zahltiť cieľový systém veľkým objemom komunikácie, čím sa stane neprístupným pre legitímnych používateľov[8].

Sektor zdravotníctva čelí podobným trendom kybernetických hrozieb, pričom výrazne dominujú ransomvérové útoky. Podľa agentúry ENISA tvoril ransomvér 54 % analyzovaných kybernetických bezpečnostných incidentov v sektore zdravotníctva v rokoch 2021 – 2023. 83 % útokov bolo motivovaných finančne, a to z dôvodu vysokej hodnoty údajov o zdravotnej starostlivosti, zatiaľ čo 10 % útokov malo ideologickú motiváciu[9]. Podobne sa v správe Komisie z roku 2024 uvádzalo, že 71 % útokov s vplyvom na starostlivosť o pacientov, ako je napríklad oneskorená liečba, diagnostika a zhoršený prístup k záchranným službám, bolo ransomvérového typu[10]. Ransomvérové útoky môžu mať obzvlášť rušivý vplyv na poskytovanie služieb zdravotnej starostlivosti a ohroziť bezpečnosť pacientov. Ransomvérové útoky sú navyše mnohokrát spojené s narušením ochrany údajov pacientov[11], ktoré často obsahujú citlivé údaje týkajúce sa zdravia, čím sa porušuje základné právo osôb na ochranu osobných údajov.

S rastúcou digitalizáciou zdravotnej starostlivosti sa zároveň zväčšuje priestor na útoky. Podľa správy o stave digitálneho desaťročia za rok 2024 má v priemere 79 % občanov EÚ online prístup k svojim elektronickým zdravotným záznamom v rámci primárnej zdravotnej starostlivosti[12]. Elektronické zdravotné záznamy, klinické informačné systémy, nemocničné pracovné systémy, informačné systémy na úhradu liečby, systémy na diagnostické zobrazovanie a zdravotnícke pomôcky používané na diagnostické účely alebo na monitorovanie pacientov – to všetko sú príklady digitálnych nástrojov, ktoré môžu zohrávať významnú úlohu pri zvyšovaní efektívnosti a výkonnosti sektora zdravotníctva, ale zároveň sú potenciálnymi cieľmi kybernetického útoku. Osobitnému riziku kybernetických útokov sú vystavené špecifické zdravotnícke činnosti, ako je intenzívna starostlivosť a rádiologické zobrazovanie, alebo lekárske odbory, ako je onkológia a kardiológia, ktoré sú vo veľkej miere závislé od digitálne podporovaných zariadení. Okrem toho môžu problémy v dodávateľskom reťazci viesť k obstarávaniu zariadení s nedostatočnou kybernetickou bezpečnosťou, čím sa zhoršujú existujúce všeobecné riziká.

Napríklad počas pandémie ochorenia COVID-19 ochromil ransomvérový útok rozsiahle časti írskeho systému zdravotnej starostlivosti, čo ráno v deň incidentu viedlo k zrušeniu prinajmenšom niektorých

---

8 *ENISA Threat Landscape 2024* (Panoráma hrozieb v roku 2024 podľa agentúry ENISA).

9 *ENISA Threat Landscape: Health Sector* (Panoráma hrozieb pre sektor zdravotníctva podľa agentúry ENISA) (júl 2023). V správe sa analyzovali poskytovatelia zdravotnej starostlivosti, ako aj iné druhy organizácií vrátane organizácií vykonávajúcich výskum v oblasti zdravia, subjektov, ktoré vyrábajú určité výrobky týkajúce sa zdravia, zdravotníckych orgánov, organizácií v oblasti zdravotného poistenia, pobytových liečebných zariadení a poskytovateľov sociálnych služieb. K dispozícii na https://www.enisa.europa.eu/publications/health-threat-landscape.

10 Európska komisia: Spoločné výskumné centrum, 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 bezpečnosť v sektore zdravotníctva a medicíny – štúdia o dostupných dôkazoch o zdravotných dôsledkoch kybernetických incidentov v prostredí zdravotníctva), Úrad pre vydávanie publikácií Európskej únie, 2024, https://data.europa.eu/doi/10.2760/693487.

11 Podľa štúdie *ENISA Threat Landscape for the Health Sector* (Panoráma hrozieb pre sektor zdravotníctva podľa agentúry ENISA) sa narušenie ochrany alebo krádež údajov potvrdili v 43 % analyzovaných ransomvérových incidentov.

12 Správa o stave digitálneho desaťročia za rok 2024.

služieb v 31 z 54 nemocníc poskytujúcich akútnu starostlivosť[13]. V rámci zdravotníckych služieb sa muselo prejsť späť na používanie papierových záznamov, čím sa spomalila efektívnosť prevádzky. Útok vznikol na základe podvodného e-mailu obsahujúceho škodlivú prílohu[14]. Incident preukázal potenciál kybernetických útokov, ktoré sa šíria v rôznych systémoch, a tým aj dôležitosť ochrany celého priestoru zdravotníckej organizácie, ktorý je vystavený útokom. Podčiarkol sa tým aj význam zabezpečenia základných postupov v oblasti kybernetickej hygieny a kultúry kybernetickej bezpečnosti v rámci celých organizácií.

Vyspelosť nemocníc a poskytovateľov zdravotnej starostlivosti v oblasti kybernetickej bezpečnosti

Prostredie zdravotnej starostlivosti v EÚ je veľmi rôznorodé, pričom nemocnice a iní poskytovatelia zdravotnej starostlivosti sa v jednotlivých členských štátoch výrazne líšia z hľadiska vlastníctva, štruktúry a veľkosti. V niektorých prípadoch môže byť riadenie zdravotnej starostlivosti založené na centralizovanom prístupe na celoštátnej úrovni, v iných na regionálnej a miestnej úrovni; poskytovatelia zdravotnej starostlivosti môžu byť vo verejnom alebo v súkromnom vlastníctve. Okrem toho môžu existovať rozdiely aj v rámci tej istej krajiny, napríklad v prípade výrazných sociálno-ekonomických a územných rozdielov medzi regiónmi, čím vzniká zložitý celkový obraz. Toto zložité prostredie zdravotnej starostlivosti môže byť ohrozené závažnými zdravotnými krízami v dôsledku prenosných ochorení, ako je pandémia ochorenia COVID-19, ale aj inými zdravotnými rizikami, napríklad v súvislosti so zmenou klímy. V neposlednom rade existuje značná variabilita a fragmentácia, pokiaľ ide o úroveň digitalizácie a zavádzania technológií poskytovateľmi zdravotnej starostlivosti. Príkladom tejto zložitosti je to, že nedostupnosť služieb spôsobená kybernetickým bezpečnostným incidentom môže mať za následok vážne škody a poškodenie pacientov aj v malých zdravotníckych zariadeniach vrátane kliník alebo záchranných zdravotných služieb, ktoré poskytujú základné služby relatívne malému počtu používateľov.

Podľa správy agentúry ENISA o stave kybernetickej bezpečnosti v Únii za rok 2024[15] je úroveň vyspelosti kybernetickej bezpečnosti v sektore zdravotníctva v EÚ stredná a medzi jednotlivými subjektmi zdravotnej starostlivosti v Európe existujú veľké rozdiely v tejto oblasti. Nedostatky možno pozorovať v kľúčových oblastiach, ako je dostatok ľudských zdrojov, znalosť organizácií o dodávateľských reťazcoch ich informačných a komunikačných technológií (IKT) a inštalácia aktuálnych bezpečnostných prvkov do produktov. Sektor zdravotníctva má problémy so základnou kybernetickou hygienou a základnými bezpečnostnými opatreniami, čo ilustruje skutočnosť, že takmer všetky zdravotnícke organizácie, ktoré boli predmetom prieskumu, čelia problémom, pokiaľ ide

[13] Írsky výkonný orgán v oblasti zdravia (2021): *„Conti cyber attack on the HSE: Independent Post Incident Review“* (Kybernetický útok na HSE ransomvérom Conti: Nezávislé preskúmanie po incidente).

[14] Írsky výkonný orgán v oblasti zdravia: *„Cyber-attack and HSE response“* (Kybernetický útok a reakcia HSE). K dispozícii na https://www2.hse.ie/services/cyber-attack/what-happened/.

[15] Agentúra ENISA: Správa o stave kybernetickej bezpečnosti v Únii za rok 2024 (september 2024). K dispozícii na https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

o vykonávanie posúdenia kybernetickobezpečnostných rizík, pričom takmer polovica z nich nikdy nevykonala analýzu rizík[16].

Ďalšou významnou výzvou pre kybernetickú bezpečnosť nemocníc je prienik informačných technológií a prevádzkových technológií, kde sa stretávajú rôzne bezpečnostné priority, pokiaľ ide o dôvernosť, dostupnosť a spoľahlivosť, a kde narušenie jednej oblasti môže ovplyvniť druhú. V správe agentúry ENISA o stave kybernetickej bezpečnosti v Únii za rok 2024 sa ďalej zdôrazňuje, že v sektore zdravotníctva sa nedosahujú primerané výsledky pri zaisťovaní bezpečnosti produktov a procesov IKT, ktoré sa v ňom používajú, a to z dôvodu veľkej rôznorodosti zdravotníckych subjektov, zariadení a produktov.

Z tejto rôznorodosti v kombinácii s rôznou úrovňou informovanosti zamestnancov a manažmentu nemocníc o kybernetickej bezpečnosti vyplývajú zložité výzvy, pokiaľ ide o zabezpečenie kybernetickej bezpečnosti systémov zdravotnej starostlivosti. Napríklad podľa prieskumu Eurobarometra o kybernetických zručnostiach v roku 2024 iba 25 % oslovených spoločností v sektore zdravotníctva, vzdelávania a sociálnej starostlivosti zabezpečilo v predchádzajúcich 12 mesiacoch odbornú prípravu alebo zvyšovanie informovanosti o kybernetickej bezpečnosti[17]. Je potrebné prijať opatrenia na podporu kultúry informovanosti o kybernetickej bezpečnosti medzi zdravotníckymi pracovníkmi v prvej línii. Ďalšími zdrojmi zraniteľností, ktoré ovplyvňujú kybernetickú bezpečnosť poskytovateľov zdravotnej starostlivosti, sú napríklad striedanie zamestnancov, používanie zdieľaných pracovných staníc, nedostatočná správa autentifikácie a používanie vymeniteľných médií[18].

V mnohých prípadoch sú informačné technológie a prevádzkové technológie aspoň čiastočne zabezpečované externými dodávateľmi. V prieskume Eurobarometra 2024 sa zistilo, že podiel spoločností, ktoré aspoň niektoré aspekty kybernetickej bezpečnosti zabezpečujú externými dodávateľmi, je najvyšší v sektore zdravotníctva, vzdelávania a sociálnej starostlivosti, kde takto postupuje 57 % oslovených spoločností[19]. Podobne tu existuje výrazný trend prechodu na cloud computing, ktorý je spôsobený potrebou škálovateľného ukladania a správy údajov, nákladovej efektívnosti, lepšej spolupráce a podpory pokročilých technológií, ako je umelá inteligencia a internet vecí v zdravotníctve. V roku 2022 používalo cloudovú platformu elektronického zdravotníctva 58 % zdravotníckych organizácií[20]. Hoci tento posun môže viesť k významnému zvýšeniu efektivity, prináša so sebou aj riziká, ktoré si vyžadujú kvalifikované rozhodnutia týkajúce sa verejného obstarávania a bezpečnej konfigurácie.

---

16 *ENISA Threat Landscape: Health Sector* (Panoráma hrozieb pre sektor zdravotníctva podľa agentúry ENISA) (júl 2023). K dispozícii na https://www.enisa.europa.eu/publications/health-threat-landscape.

17 Rýchly prieskum Eurobarometra 547 o kybernetických zručnostiach (máj 2024). K dispozícii na https://europa.eu/eurobarometer/surveys/detail/3176.

18 *Panacea – People-centric cybersecurity in healthcare (2021): White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres* [Panacea – Kybernetická bezpečnosť v zdravotníctve so zameraním na ľudí (2021): Biela kniha – Poznatky získané z projektu PANACEA o kybernetickej ochrane nemocníc a centrálnych príjmov].

19 Rýchly prieskum Eurobarometra 547 o kybernetických zručnostiach (máj 2024). K dispozícii na https://europa.eu/eurobarometer/surveys/detail/3176.

20 *ENISA: NIS Investments Report 2022* (ENISA: Správa o investíciách do bezpečnosti sietí a informačných systémov za rok 2022) (november 2022). K dispozícii na https://www.enisa.europa.eu/publications/nis-investments-2022.

Nad všetkými týmito výzvami stojí otázka budovania kapacít a financovania. Financovanie kybernetickej bezpečnosti v sektore zdravotníctva je obmedzené a zostáva všeobecnou výzvou v celej EÚ[21]. Okrem toho tieto výzvy v oblasti financovania vznikajú v situácii starnutia obyvateľstva, ktoré podľa očakávaní v nasledujúcich desaťročiach spôsobí rozsiahle rozpočtové tlaky na európske systémy zdravotnej starostlivosti.

Pretrvávajúce používanie zastaraných nástrojov a starších systémov, obmedzené zdroje na prevenciu incidentov a reakciu na ne a nedostatky vo vyspelosti v oblasti kybernetickej bezpečnosti často vyplývajú z nedostatku finančných prostriedkov. Nemocnice čelia neustálej výzve vyvážiť modernú bezpečnú a digitálnu infraštruktúru s ďalšími nevyhnutnými investíciami na zlepšenie starostlivosti o pacientov, ako je napríklad prijímanie lekárov a iných zdravotníckych pracovníkov, zavádzanie nových diagnostických a liečebných metód a nákup prístrojov. Podľa agentúry ENISA[22] je sektor zdravotníctva až na 7. mieste z 12 skúmaných sektorov, pokiaľ ide o podiel výdavkov na informačnú bezpečnosť na celkových výdavkoch na IT, pričom medián v sektore zdravotníctva je 8,3 %.

3. Európske centrum na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti

Rámec kybernetickej bezpečnosti EÚ ponúka širokú škálu nástrojov, ktoré by sa mali využiť na zlepšenie bezpečnosti a odolnosti nemocníc a poskytovateľov zdravotnej starostlivosti. Na riešenie mnohých uvedených výziev je potrebné vytvoriť jednotný strategický prístup na úrovni EÚ, v ktorom by sa spojili potrebné zdroje, odborné znalosti a nástroje na účinný boj proti kybernetickým hrozbám. Komplexný prehľad, ako aj lepšie plánovanie a koordinácia sú nevyhnutnou podmienkou pomoci poskytovateľom zdravotnej starostlivosti v celej EÚ pri posilnení ich obrany. V záujme dosiahnutia tohto cieľa má agentúra ENISA najlepšie predpoklady na zriadenie v rámci svojej organizácie špecializovaného **Európskeho centra na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti**[23] ako súčasť svojho mandátu[24] na ochranu a podporu kritickej infraštruktúry EÚ.

Centrum podpory by malo postupne **vypracovať komplexný katalóg služieb pre potreby nemocníc a poskytovateľov zdravotnej starostlivosti**, v ktorom by sa uvádzal rozsah dostupných služieb v oblasti pripravenosti, prevencie, odhaľovania a reakcie. V spolupráci s orgánmi členských štátov a na základe skúseností nemocníc a poskytovateľov zdravotnej starostlivosti by centrum podpory malo vytvoriť používateľsky ústretový a ľahko dostupný archív všetkých dostupných nástrojov na európskej, vnútroštátnej a regionálnej úrovni. Pri vykonávaní svojich činností by malo zabezpečiť riadnu

---

21 Organizácia a poskytovanie zdravotníckych služieb a zdravotnej starostlivosti je podľa článku 168 Zmluvy o fungovaní Európskej únie v kompetencii jednotlivých štátov a financovanie systémov zdravotnej starostlivosti sa v jednotlivých členských štátoch líši.

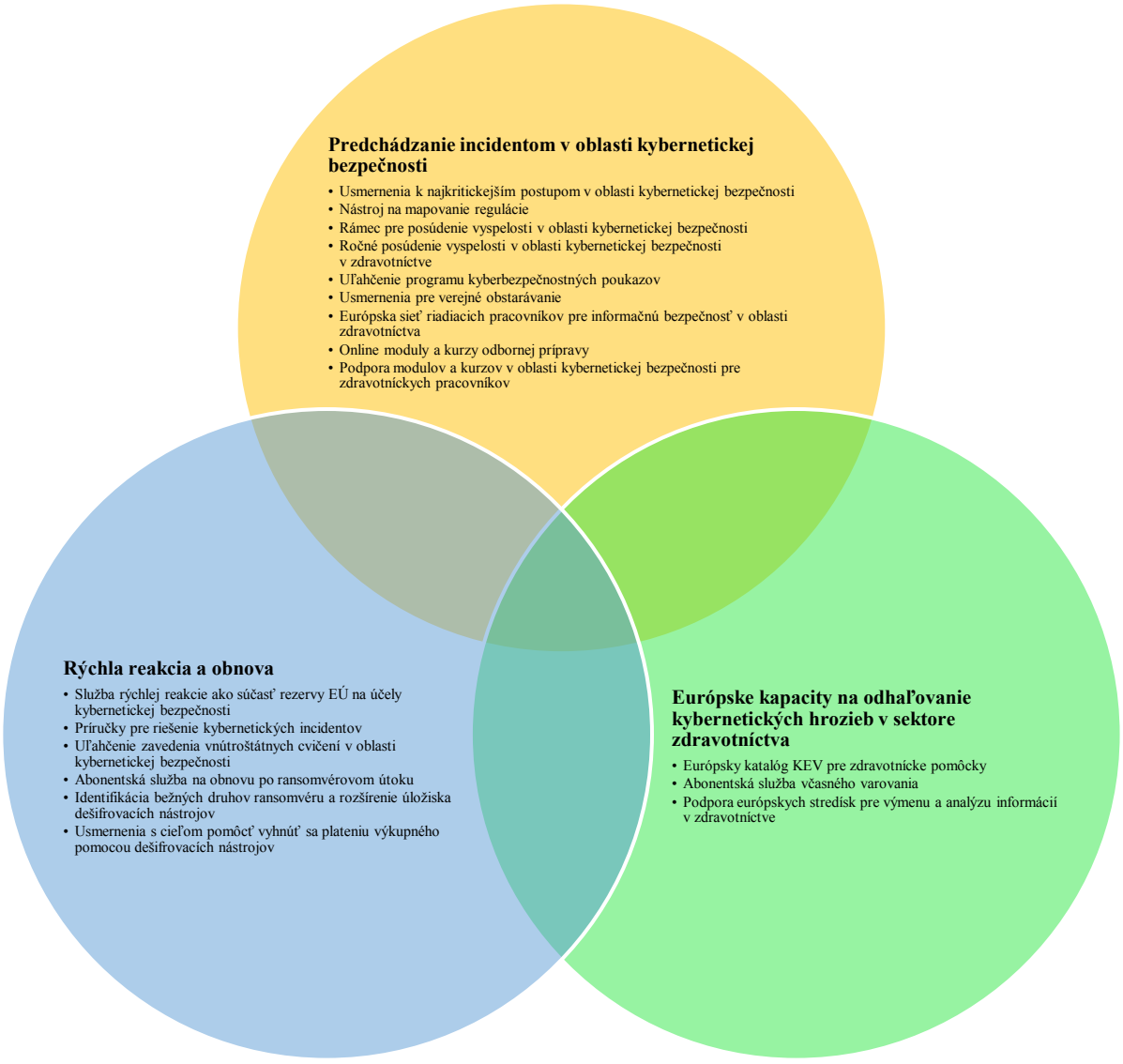
22 *ENISA: NIS Investments Report 2022* (ENISA: Správa o investíciách do bezpečnosti sietí a informačných systémov za rok 2022) (november 2022). K dispozícii na https://www.enisa.europa.eu/publications/nis-investments-2022.

23 V tomto dokumente sa pojem „centrum podpory“ používa zameniteľne.

24 Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15 – 69).

koordináciu s členskými štátmi a podporovať stanovenie priorít a realizáciu opatrení podľa potreby v reálnom čase.

Ako dôležitý stavebný prvok pre rozvoj katalógu služieb centra podpory Komisia navrhne začať pilotné projekty v celej EÚ s cieľom vyvinúť najlepšie postupy pre kybernetickú hygienu a hodnotenie bezpečnostných rizík, ako aj riešiť potrebu nepretržitého monitorovania kybernetickej bezpečnosti, spravodajských informácií o hrozbách a reakcie na incidenty s využitím najmodernejších riešení v oblasti kybernetickej bezpečnosti. Výsledky týchto pilotných projektov, ktoré budú financované z programu Digitálna Európa a realizované Európskym centrom kompetencií v oblasti kybernetickej bezpečnosti, budú slúžiť ako základ pre ďalšie opatrenia na úrovni EÚ vrátane práce centra podpory.



Obrázok 1: Koncepcie katalógu služieb centra podpory pre nemocnice a poskytovateľov zdravotnej starostlivosti

3.1. Predchádzanie incidentom v oblasti kybernetickej bezpečnosti

Jednoduché opatrenia, ktoré znižujú pravdepodobnosť incidentov

Podľa jedného odhadu môžu základné opatrenia kybernetickej bezpečnosti, ako je zabezpečenie aktualizácie systémov, správa záloh a zavedenie viacstupňovej autentifikácie, ochrániť organizácie až pred 98 % útokov[25]. Mnohé z opatrení v oblasti kybernetickej hygieny a riadenia rizík, ktoré majú najväčší vplyv, možno prijať pomerne jednoducho, vďaka čomu predstavujú ľahko dostupnú možnosť zlepšenia kybernetickej bezpečnosti. Jednou z najdôležitejších úloh centra podpory by preto malo byť **vypracovanie jasných a cielených usmernení, v ktorých by sa zdôrazňovali najkritickejšie postupy v oblasti kybernetickej bezpečnosti a ktoré by pomáhali poskytovateľom zdravotnej starostlivosti pri zavádzaní uvedených postupov**. Táto podpora sa musí rozšíriť nad rámec veľkých nemocníc, aby jej súčasťou bolo poradenstvo prispôsobené menším subjektom, ako sú miestne ordinácie všeobecných lekárov a špecializované kliniky, ktoré často nemajú zdroje na špecializované tímy kybernetickej bezpečnosti, zostávajú však rovnako zraniteľné voči útokom. Okrem toho je potrebné zohľadniť regionálny význam konkrétnych zdravotníckych zariadení pre zabezpečenie starostlivosti o pacientov, napríklad v riedko osídlených oblastiach. Usmernenia o základných opatreniach kybernetickej bezpečnosti by na zvýšenie svojej odolnosti mohli využiť aj zdravotnícke výskumné ústavy, ktoré spracúvajú veľké množstvo citlivých osobných údajov.

Na zdravotnícke organizácie sa vzťahuje aj celý rad povinností súvisiacich s kybernetickou bezpečnosťou, ktoré vyplývajú z právnych predpisov EÚ[26]. Hoci sú tieto povinnosti kľúčové pre zabezpečenie spoločnej vysokej úrovne kybernetickej bezpečnosti a bezpečnosti údajov, je nevyhnutné zabezpečiť, aby orientácia v regulačnom prostredí nebola zbytočne zložitá a zaťažujúca. Veľký dôraz na dodržiavanie predpisov by nemal byť v rozpore s cieľom podporovať silnú kultúru kybernetickej

---

[25] Správa Microsoftu o digitálnej ochrane z roku 2022. K dispozícii na https://www.microsoft.com/sk-sk/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Napríklad smernica NIS 2; nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami (akt o kybernetickej odolnosti), https://eur-lex.europa.eu/eli/reg/2024/2847/oj/enghttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng; nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, https://eur-lex.europa.eu/eli/reg/2017/745/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/745/oj/eng (nariadenie o zdravotníckych pomôckach), https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng, nariadenie o zdravotníckych pomôckach; nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach *in vitro* (nariadenie o diagnostických zdravotníckych pomôckach *in vitro*), https://eur-lex.europa.eu/eli/reg/2017/746/oj/enghttps://eur-lex.europa.eu/eli/reg/2017/746/oj/eng; nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov), https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32016R0679; nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii), https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:32024R1689; návrh NARIADENIE EURÓPSKEHO PARLAMENTU A RADY o európskom priestore pre zdravotné údaje [COM(2022) 197 final], https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:52022PC0197. Rokovania sa uzavreli politickou dohodou na jar 2024 a po finalizácii sa očakáva uverejnenie v úradnom vestníku na jar 2025.

bezpečnosti. **Ľahko dostupný nástroj na mapovanie regulácie môže pomôcť minimalizovať administratívne zaťaženie subjektov, na ktoré sa vzťahuje viacero regulačných nástrojov**. Popri vypracovaní usmernení a súborov nástrojov by malo centrum podpory úzko spolupracovať s Komisiou a členskými štátmi na čo najskoršom vypracovaní a šírení takéhoto nástroja. Centrum podpory by preto zohrávalo dôležitú úlohu pri zabezpečovaní jednoduchšieho pochopenia a vykonávania pravidiel kybernetickej bezpečnosti, napríklad poskytovaním usmernení k vykonávaniu[27] a v prípade potreby podporovaním príslušných noriem.

Ďalším nástrojom na uľahčenie jednoduchého uplatňovania správnych postupov kybernetickej hygieny sú pripravované **európske peňaženky digitálnej identity**. Na zmiernenie rizík neoprávneného prístupu k zdravotným údajom je nevyhnutné zníženie závislosti od slabých identifikačných mechanizmov, ako sú heslá. Rozhodujúci je prechod na riešenia bezpečného prihlasovania založené na spoľahlivej identifikácii. Európska peňaženka digitálnej identity ponúka harmonizovaný celoúnijný prístup k elektronickej identifikácii zdravotníckych pracovníkov a od konca roka 2026 bude poskytovať spoľahlivé a jednotné riešenie. Všetky online zdravotnícke informačné systémy, v ktorých sa vyžaduje zavedenie silnej autentifikácie používateľa, budú od konca roka 2027 povinné akceptovať uvedenú peňaženku na účely identifikácie[28].

Pripravenosť a cielená podpora

Testovanie pripravenosti, ktoré zahŕňa činnosti, ako je napríklad penetračné testovanie, je základom účinnej kybernetickej bezpečnosti a Komisia už pridelila agentúre ENISA finančné prostriedky na pilotné iniciatívy v oblasti pripravenosti, v rámci ktorých sa odhalilo, že sektor zdravotníctva patrí medzi najžiadanejšie oblasti na testovanie a ďalšie posudzovanie s cieľom identifikovať nedostatky vo vyspelosti v oblasti kybernetickej bezpečnosti. Po nadobudnutí účinnosti aktu o kybernetickej solidarite sa toto úsilie výrazne rozšíri, pričom vedúcu úlohu prevezme Európske centrum kompetencií v oblasti kybernetickej bezpečnosti. S cieľom riešiť túto potrebu Komisia po konzultácii so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieťou EU-CyCLONe[29] a agentúrou ENISA navrhne určiť zdravotníctvo ako sektor, ktorému možno poskytnúť podporu na **koordinované testovanie pripravenosti** na základe aktu o kybernetickej solidarite. Centrum podpory by okrem toho malo vypracovať **prispôsobený rámec pre posúdenia vyspelosti v oblasti kybernetickej bezpečnosti so špecifickým zameraním na zdravotníctvo**. Na základe takýchto posúdení vyspelosti by subjekty získali využiteľné poznatky o svojich zraniteľnostiach a zároveň by mohli preukázať pacientom a zainteresovaným stranám svoju pripravenosť v oblasti kybernetickej bezpečnosti, čím by sa zvýšila dôvera v ich služby. Centrum podpory by malo na súhrnnej úrovni **každoročne vykonávať posúdenie vyspelosti zdravotníctva v oblasti kybernetickej bezpečnosti**, ktorým by sa poskytol jasný prehľad o kybernetickej bezpečnosti v sektore zdravotníctva na vnútroštátnej úrovni aj na úrovni EÚ.

---

[27] Vypracovanie usmernení týkajúcich sa výkladu všeobecného nariadenia o ochrane údajov patrí do pôsobnosti Európskeho výboru pre ochranu údajov. Agentúra ENISA by mala pri vypracúvaní usmernení plne rešpektovať výsadné práva Európskeho výboru pre ochranu údajov.

[28] Článok 5f ods. 1 až 2 nariadenia (EÚ) č. 910/2014.

[29] Európska sieť styčných organizácií pre kybernetické krízy.

Pokiaľ ide o služby kybernetickej bezpečnosti, sektor zdravotníctva sa vo veľkej miere spolieha na externých dodávateľov[30], čo poukazuje na potrebu cielenej podpory na posilnenie obrany. Na základe úspešných iniciatív, ako sú inovačné poukazy EÚ, **by členské štáty mali zvážiť cielené opatrenia, ako sú kyberbezpečnostné poukazy pre veľmi malé, malé a stredné nemocnice a poskytovateľov zdravotnej starostlivosti**. Prostredníctvom uvedených poukazov by sa poskytovala finančná pomoc na zavedenie konkrétnych opatrení kybernetickej bezpečnosti. Pri určovaní priorít pri prideľovaní poukazov by sa malo vychádzať zo zistení z testovania pripravenosti a posúdení vyspelosti.

Miestne znalosti a kontext sú kľúčové pre účinné zavádzanie poukazov alebo iných podporných programov, pretože sa nimi garantuje relevantnosť a dostupnosť. Z fondov EÚ, ako je napríklad Európsky fond regionálneho rozvoja, sa už aktívne podporujú iniciatívy v oblasti kybernetickej bezpečnosti a elektronického zdravotníctva, preto by mohli slúžiť ako nástroj na vytvorenie cielených schém kyberbezpečnostných poukazov pre poskytovateľov zdravotnej starostlivosti. Na podporu tohto úsilia by centrum podpory spolupracovalo s členskými štátmi a regionálnymi orgánmi pre príslušné programy s cieľom podporiť rozvoj takýchto regionálnych schém poukazov, pričom by využilo skúsenosti z existujúcich vnútroštátnych projektov, ako aj z opatrení financovaných v rámci programu Digitálna Európa s cieľom zabezpečiť praktické a účinné vykonávanie.

Okrem toho sa programy Horizont od roku 2014 podieľajú na financovaní celého radu výskumných iniciatív zameraných na zvýšenie odolnosti zdravotníckych zariadení, ako sú nemocnice, voči kybernetickým hrozbám a zmiernenie rizík spojených so zneužitím nových technológií. Výsledné výstupy zahŕňajú súbor špecializovaných nástrojov, rámcov a systémov, ako sú nástroje na hodnotenie rizík, platformy na zdieľanie údajov so zachovaním súkromia, kryptografické riešenia, programy odbornej prípravy v oblasti zvyšovania informovanosti o kybernetickej bezpečnosti a systémy na odhaľovanie hrozieb v reálnom čase. Tieto riešenia boli dôkladne overené prostredníctvom pilotných prípadov zavedenia v reálnom prostredí zdravotnej starostlivosti, čím sa zabezpečila ich účinnosť a praktická použiteľnosť pri ochrane pred kybernetickými hrozbami.

Zabezpečenie dodávateľských reťazcov v zdravotníctve

Kľúčovou výzvou pre zdravotnícke organizácie je riadenie komplexných dodávateľských reťazcov IKT, ktoré zahŕňajú celý rad produktov, ako sú pripojené zdravotnícke pomôcky, systémy elektronických zdravotných záznamov a kancelársky hardvér. Nemocnice a poskytovatelia zdravotnej starostlivosti potrebujú pre svoju prevádzku spoľahlivé a bezpečné systémy a služby IKT. S cieľom pomôcť riešiť výzvy v oblasti kybernetickej bezpečnosti v sektore zdravotníctva by skupina pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti mala vykonávať **koordinované posúdenie bezpečnostných rizík, v rámci ktorého by sa posudzovali technické aj strategické riziká súvisiace s dodávateľskými reťazcami zdravotníckych pomôcok a navrhovali by sa opatrenia na ich zmiernenie**[31]**.** Skupina pre

[30] Pozri správu agentúry ENISA o investíciách do bezpečnosti sietí a informačných systémov za rok 2023 (november 2023), v ktorej sa zdôrazňuje význam externej podpory pre audit a dodržiavanie predpisov v oblasti kybernetickej bezpečnosti. K dispozícii na https://www.enisa.europa.eu/publications/nis-investments-2023.

[31] Podľa článku 22 smernice NIS 2.

spoluprácu v oblasti sieťovej a informačnej bezpečnosti by mala podľa potreby spolupracovať s Koordinačnou skupinou pre zdravotnícke pomôcky.

Akt o kybernetickej odolnosti je nový, komplexný rámec, ktorým sa stanovujú požiadavky na kybernetickú bezpečnosť v oblasti plánovania, navrhovania, vývoja, ako aj riešenia, opráv a oznamovania aktívne zneužívaných zraniteľností týkajúcich sa takmer všetkých hardvérových a softvérových produktov v každej fáze hodnotového reťazca[32]. Zdravotnícke pomôcky sú tým druhom výrobkov, ktoré sa používajú v jednej z najcitlivejších oblastí našej spoločnosti. Požiadavky na kybernetickú bezpečnosť týchto výrobkov vyplývajú z existujúceho nariadenia o zdravotníckych pomôckach a nariadenia o diagnostických zdravotníckych pomôckach *in vitro*[33]. V rámci prebiehajúceho hodnotenia týchto nariadení sa skúma potenciál väčšej súdržnosti a synergií medzi uvedenými rámcami s cieľom zaručiť zjednodušenie a špičkovú kybernetickú bezpečnosť.

Okrem toho by zistenia z posúdenia rizík mali zdravotníckym organizáciám pomôcť pri preskúmaní ich postupov kybernetickej bezpečnosti dodávateľského reťazca, ako sa vyžaduje v smernici NIS 2, a mohli by byť podkladom pre vypracovanie nových **usmernení pre verejné obstarávanie**[34]. Uvedené usmernenia, ktoré by vypracovala agentúra ENISA prostredníctvom svojho centra podpory, by mali zohľadňovať najnovšie trendy, ako je napríklad presun uchovávania údajov o pacientoch na cloud vrátane potreby bezpečnej migrácie elektronických zdravotných údajov do cloudových prostredí. Okrem toho by nové usmernenia mali organizáciám ponúknuť praktické nástroje na sledovanie ich dodávateľských reťazcov vrátane poskytovateľov riadených bezpečnostných služieb, správ o osvedčovaní alebo posúdení rizika pochádzajúceho od tretích strán.

V prípade cloudu sú potrebné ďalšie opatrenia na riešenie osobitných výziev spojených so správou citlivých údajov v oblasti zdravotnej starostlivosti vrátane zvýšených bezpečnostných rizík, rizík týkajúcich sa ochrany súkromia a prevádzkových rizík. Na posilnenie záruk odborníci odporúčajú, aby sa do cloudových služieb začlenili princípy „bezpečnosť ako štandard“ a „bezpečnosť už v štádiu návrhu“. Takýmto prístupom sa uprednostňuje bezpečná infraštruktúra, proaktívna správa zraniteľností a kombinácia štátnych a súkromných cloudových riešení. Na zabezpečenie spoľahlivých bezpečnostných postupov sú takisto nevyhnutné nepretržité monitorovanie a osvedčenia pre konkrétneho dodávateľa, ako sú certifikácie poskytovateľov zabezpečenia a audity súladu s vnútroštátnymi a medzinárodnými normami.

V prípade služieb, ako je infraštruktúra ako služba (IaaS), platforma ako služba (PaaS) a softvér ako služba (SaaS), je implementácia zabezpečenia často v kompetencii zákazníka. Mnohé zdravotnícke

---

32 V prvom kroku sa od 1. augusta 2025 bude vyžadovať, aby široké kategórie rádiových zariadení, ktoré nepatria do rozsahu pôsobnosti nariadenia o zdravotníckych pomôckach a nariadenia o diagnostických zdravotníckych pomôckach *in vitro*, spĺňali pri uvádzaní na jednotný trh základné požiadavky smernice o rádiových zariadeniach, ktoré sa týkajú kybernetickej bezpečnosti. V druhej fáze sa od 11. decembra 2027 začne uplatňovať akt o kybernetickej odolnosti.

33 Koordinačná skupina pre zdravotnícke pomôcky vydala v decembri 2019 usmernenie o kybernetickej bezpečnosti zdravotníckych pomôcok, ktorým sa výrobcom poskytuje podpora pri plnení požiadaviek prílohy I k obom uvedeným nariadeniam: https://ec.europa.eu/docsroom/documents/41863.

34 Na základe usmernení agentúry ENISA pre verejné obstarávanie v oblasti kybernetickej bezpečnosti v nemocniciach na rok 2020 (február 2020). K dispozícii na https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

organizácie však nemajú dostatok zdrojov na splnenie týchto požiadaviek vlastnými silami. V záujme riešenia tohto problému **by sa poskytovatelia cloudových služieb mali povzbudzovať, aby zaviedli základné bezpečnostné opatrenia ako štandardnú funkciu**. Uvedenými opatreniami by sa znížilo riziko nesprávnej konfigurácie, zachovala by sa konzistentná ochrana v prostrediach spravovaných zákazníkom a používateľom by sa poskytla väčšia istota. Cieľom stanovenia štandardného bezpečnostného scenára by bolo nájsť rovnováhu medzi spoľahlivou ochranou a praktickosťou, čím by sa zabezpečila použiteľnosť pre širokú škálu zdravotníckych organizácií. Toto úsilie by zahŕňalo úzku spoluprácu medzi poskytovateľmi cloudových služieb a sektorom zdravotníctva, pričom by sa využili najlepšie postupy v odvetví na vytvorenie účinných a škálovateľných riešení.

Odborná príprava a rozvoj zručností

Pracovná sila s požadovanými zručnosťami je dôležitá pre dlhodobý udržateľný rast a konkurencieschopnosť v Európe, ako aj pre vysokokvalitné služby vrátane služieb zdravotnej starostlivosti. V celej Európe je významným problémom nedostatok kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti, pričom sa odhaduje, že v EÚ chýba 299 000 odborníkov, ktorí by naplnili potreby z hľadiska pracovnej sily[35]. Podľa prieskumu Eurobarometra 2024 o kybernetických zručnostiach[36] 81 % spoločností považuje ťažkosti pri prijímaní zamestnancov v oblasti kybernetickej bezpečnosti za kľúčové riziko potenciálnych kybernetických útokov. V sektoroch vzdelávania, zdravotníctva a sociálnej práce je 66 % pozícií v oblasti kybernetickej bezpečnosti obsadených zamestnancami, ktorí tam prechádzajú z pozícií mimo kybernetickej bezpečnosti, čo poukazuje na naliehavú potrebu rekvalifikácie a zvyšovania úrovne zručností.

S cieľom riešiť túto výzvu by centrum podpory malo na účely zručností v oblasti kybernetickej bezpečnosti spolupracovať s budúcim Konzorciom pre európsku digitálnu infraštruktúru, ktorého vznik sa predpokladá v oznámení Komisie o akadémii zručností v oblasti kybernetickej bezpečnosti[37]. Touto prácou by sa mala uľahčiť výmena informácií medzi odborníkmi na kybernetickú bezpečnosť v sektore zdravotníctva, ako sú napríklad riadiaci pracovníci pre informačnú bezpečnosť (CISO). Jedným z možných opatrení by bolo vytvorenie **európskej siete riadiacich pracovníkov pre informačnú bezpečnosť v oblasti zdravotníctva**, ktorá by so skupinou odborníkov začala výmenu a rozvoj najlepších postupov, stratégií na udržanie talentov a riešení na prilákanie odborníkov na kybernetickú bezpečnosť do sektora zdravotníctva. Okrem toho by sa pod záštitou Akadémie zručností v oblasti kybernetickej bezpečnosti mali rozvíjať zdroje na posilnenie pracovnej sily v oblasti kybernetickej bezpečnosti v sektore zdravotníctva s podporou odvetvia a akademickej obce. V tejto súvislosti by sa

35 *The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform* (Kybernetická bezpečnosť v roku 2024: poznatky zo štúdie ISC2 o kybernetickej bezpečnosti | Platforma pre digitálne zručnosti a pracovné miesta).

36 Rýchly prieskum Eurobarometra 547 o kybernetických zručnostiach.

37 Oznámenie Komisie Európskemu parlamentu a Rade: Riešenie nedostatku odborníkov v oblasti kybernetickej bezpečnosti s cieľom posilniť konkurencieschopnosť, rast a odolnosť EÚ (Akadémia zručností v oblasti kybernetickej bezpečnosti) [COM(2023) 207 final].

mali zainteresované strany z odvetvia podnecovať, aby prisľúbili podporu na zlepšenie odbornej prípravy v oblasti kybernetickej bezpečnosti.

K incidentom v oblasti kybernetickej bezpečnosti v zdravotníctve naďalej významne prispievajú ľudské chyby, čo podčiarkuje zásadnú potrebu komplexnej odbornej prípravy pracovníkov a informovanosti o kybernetickej bezpečnosti. Vzhľadom na časté používanie digitálnych nástrojov zdravotníckymi pracovníkmi je nevyhnutné, aby sa im poskytli znalosti bezpečných postupov. Cielená odborná príprava a kampane na zvýšenie povedomia môžu výrazne znížiť riziká. Vzhľadom na to by malo centrum podpory spolupracovať so zdravotníckymi pracovníkmi a poskytovateľmi a prostredníctvom spolupráce s poskytovateľmi vzdelávania a odbornej prípravy, odvetvím, Konzorciom pre európsku digitálnu infraštruktúru na účely zručností v oblasti kybernetickej bezpečnosti, ako aj s orgánmi členských štátov vytvoriť a šíriť **rozsiahle a ľahko dostupné online moduly a kurzy odbornej prípravy**.

Zaradenie modulov digitálnych kompetencií a kybernetickej bezpečnosti do vzdelávacích programov je kľúčové pre vybudovanie pevných základov kybernetickej bezpečnosti v zdravotníctve. Tieto moduly by sa mali zameriavať na otázky špecifické pre daný sektor, ako je ochrana údajov o pacientoch a zraniteľnosti v oblasti bezpečnosti zdravotníckych pomôcok. Pri vytváraní týchto zdrojov by sa mali zohľadniť predchádzajúce opatrenia, ako je napríklad projekt BeWell financovaný v rámci programu Erasmus+[38] a projekt PANACEA financovaný v rámci programu Horizont 2020[39].

3.2. Európske kapacity na odhaľovanie kybernetických hrozieb v sektore zdravotníctva

Účinné odhaľovanie kybernetických hrozieb je nutnou podmienkou rýchlej reakcie na incidenty. Aktéri hrozieb môžu využívať techniky, ktoré sťažujú odhalenie narušenia a umožňujú dlhšie obdobie nepovoleného prístupu do systému[40]. Lepšie spôsobilosti na odhaľovanie hrozieb preto môžu pomôcť zastaviť kybernetické útoky hneď v zárodku. Napríklad pri ransomvérovom útoku na fínskeho poskytovateľa psychoterapeutických služieb Vastaamo, počas ktorého páchateľ vydieral pacientov, ktorých dôverné záznamy boli odcudzené, došlo k prvotnému narušeniu v roku 2018, poskytovateľ sa však o ňom dozvedel až v roku 2020[41].

Účinná výmena informácií a spolupráca sú nevyhnutné na zlepšenie odhaľovania hrozieb a situačného povedomia v celej EÚ. Jednotky pre riešenie počítačových bezpečnostných incidentov (CSIRT) zohrávajú dôležitú úlohu pri prijímaní hlásení o incidentoch, udalostiach odvrátených v poslednej chvíli a potenciálnych hrozbách, pričom ponúkajú usmernenia o zmierňujúcich opatreniach na vnútroštátnej úrovni. **Členským štátom sa však dôrazne odporúča, aby všetky oznámenia o kybernetických**

---

38 BeWell – Koncepcia aliancie pre budúcu stratégiu v oblasti digitálnych a zelených zručností zdravotníckych pracovníkov. K dispozícii na https://bewell-project.eu/.

39 PANACEA – Ochrana a súkromie nemocničných a zdravotníckych infraštruktúr so súborom nástrojov v oblasti kybernetickej bezpečnosti a kybernetických hrozieb z hľadiska údajov a ľudí. K dispozícii na https://cordis.europa.eu/project/id/826293.

40 *ENISA Health Threat Landscape 2023* (Panoráma hrozieb pre sektor zdravotníctva podľa agentúry ENISA za rok 2023).

41 Rozhodnutie fínskeho ombudsmana pre ochranu údajov č. 1150/161/2021.

incidentoch od nemocníc a poskytovateľov zdravotnej starostlivosti poskytli aj centru podpory agentúry ENISA, aby sa umožnilo situačné povedomie na úrovni EÚ. V ideálnom prípade by tieto oznámenia mala sprevádzať zmysluplná charakteristika rôznych relevantných rozmerov incidentu vrátane známych základných zraniteľností, vplyvov na služby zdravotnej starostlivosti a nežiaducich udalostí týkajúcich sa pacientov. Okrem toho sa výrobcovia zdravotníckych pomôcok a diagnostických pomôcok *in vitro* vyzývajú, aby prostredníctvom jednotnej platformy na podávanie správ, ktorú má zriadiť a spravovať agentúra ENISA v rámci aktu o kybernetickej odolnosti, dobrovoľne nahlasovali aktívne zneužívané zraniteľnosti alebo závažné kybernetické incidenty, ktoré majú vplyv na bezpečnosť týchto pomôcok, ako aj iné potenciálne zraniteľnosti, incidenty, udalosti odvrátené v poslednej chvíli alebo kybernetické hrozby, ktoré môžu ovplyvniť rizikový profil uvedených pomôcok.

V prípade, že informácie obsiahnuté v správach už nie sú citlivé, centrum podpory by mohlo vytvoriť európsky katalóg známych zneužívaných zraniteľností (KEV) pre zdravotnícke pomôcky, systémy elektronických zdravotných záznamov a poskytovateľov zariadení IKT a softvéru v zdravotníctve, ktorý by podporovala agentúra ENISA. Na riešenie významných výziev pri odhaľovaní hrozieb by malo centrum podpory zaviesť **celoúnijnú abonentskú službu včasného varovania pre sektor zdravotníctva, ktorá by poskytovala výstrahy takmer v reálnom čase**. Táto služba by využívala spracované údaje od jednotiek pre riešenie počítačových bezpečnostných incidentov, zdravotníckych zariadení a výrobcov, spravodajské informácie z otvorených zdrojov (OSINT) a údaje od ďalších relevantných aktérov, ako sú kybernetické centrá, strediská pre výmenu a analýzu informácií a orgány presadzovania práva. Situačné povedomie by sa ďalej zvýšilo posilnenou spoluprácou medzi agentúrou ENISA a Agentúrou Európskej únie pre spoluprácu v oblasti presadzovania práva (Europol) – napríklad v oblasti vzorcov počítačovej kriminality proti sektoru zdravotníctva.

Strediská pre výmenu a analýzu informácií slúžia ako ústredné zdroje spravodajských informácií o kybernetických hrozbách, podporujú obojstrannú výmenu informácií medzi verejným a súkromným sektorom a podporujú budovanie dôvery. Centrum podpory by malo zintenzívniť podporu **európskeho strediska pre výmenu a analýzu informácií v zdravotníctve** prostredníctvom nástrojov a výmeny informácií, sektorových správ o situačnom povedomí, ako aj podpory dôveryhodného spoločenstva pre taktickú a strategickú spoluprácu. Členské štáty by mali podnecovať rozvoj vnútroštátnych stredísk pre výmenu a analýzu informácií v zdravotníctve[42]. Strediská pre výmenu a analýzu informácií by sa takisto mali nabádať, aby spájali poskytovateľov zdravotnej starostlivosti s výrobcami s cieľom dosiahnuť spoločné porozumenie o kybernetických hrozbách, a to aj v dodávateľskom reťazci, a uľahčiť dialóg o bezpečnom navrhovaní výrobkov, pri ktorom sa skutočne zohľadňujú reálne podmienky nasadenia v praxi.

[42] Napríklad Fínsko má vnútroštátne stredisko pre výmenu a analýzu informácií pre sektor sociálnej a zdravotnej starostlivosti. Pozri Fínske národné centrum kybernetickej bezpečnosti: *„ISAC information sharing groups“* (Skupiny na výmenu informácií v rámci strediska pre výmenu a analýzu informácií), dostupné na https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

3.3.Rýchla reakcia a obnova

Vzhľadom na vysokú citlivosť zdravotných údajov pacientov a potenciálne ničivé účinky kybernetických útokov na služby zdravotnej starostlivosti má rýchla a účinná reakcia na kybernetické incidenty zásadný význam pre zaistenie bezpečnosti pacientov. Keď nemocnica alebo poskytovateľ zdravotnej starostlivosti čelí kybernetickému útoku, prvým kontaktným miestom je príslušná vnútroštátna jednotka CSIRT[43]. Jednotka CSIRT zodpovedá za poskytnutie včasnej podpory, v ideálnom prípade do 24 hodín, s cieľom pomôcť zvládnuť významné incidenty. Ak však incident presiahne kapacitu jednotky CSIRT, mala by byť k dispozícii podpora EÚ, aby sa zabezpečila rýchla a účinná reakcia.

Rezerva EÚ na účely kybernetickej bezpečnosti, zriadená na základe aktu o kybernetickej solidarite, poskytuje služby reakcie na incidenty od dôveryhodných poskytovateľov riadených bezpečnostných služieb s cieľom pomôcť pri významných alebo rozsiahlych kybernetických incidentoch a pri úsilí o počiatočnú obnovu. Táto rezerva má dopĺňať úsilie jednotiek CSIRT členských štátov a umožniť im požiadať o dodatočnú podporu v prípadoch týkajúcich sa kritických sektorov, ako je zdravotníctvo. S cieľom posilniť tento systém **by Komisia a agentúra ENISA mali zabezpečiť, aby rezerva zahŕňala službu rýchlej reakcie osobitne pre sektor zdravotníctva.** Prostredníctvom tejto služby, ktorá by dopĺňala iné existujúce rámce, by sa v prípade nedostatočnej podpory na vnútroštátnej úrovni nasadili odborníci na bezodkladné zvládnutie významných alebo rozsiahlych kybernetických incidentov v zdravotníctve.

Na zlepšenie reakcie a obnovy by malo centrum podpory v spolupráci so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieťou jednotiek CSIRT a prípadne Europolom vypracovať **príručky pre riešenie kybernetických incidentov prispôsobené pre zdravotníctvo**. Uvedené príručky by obsahovali usmernenia pre jednotky CSIRT aj zdravotnícke organizácie pri reakcii na konkrétne kybernetické hrozby vrátane ransomvéru. Vzhľadom na dôležitosť účinnej spolupráce medzi jednotkami CSIRT a orgánmi presadzovania práva pri reakcii na kybernetické incidenty trestnoprávnej povahy a ich vyšetrovaní by mali príručky okrem iných aspektov poskytovať jasné usmernenia týkajúce sa oznamovania takýchto incidentov orgánom presadzovania práva. Centrum podpory by okrem toho mohlo **uľahčiť rozsiahle zavádzanie vnútroštátnych cvičení v oblasti kybernetickej bezpečnosti, pričom by sa mohlo opierať o skúsenosti z cvičení, ako je cvičenie agentúry ENISA pod názvom Cyber Europe 2022, s cieľom otestovať príručky a posilniť protokoly reakcie na incidenty.**

Na účely poskytovania podkladov pre politiky a hodnotenia účinnosti opatrení prijatých proti ransomvérovým útokom je potrebné zhromažďovať ďalšie údaje. Na tento účel by členské štáty mali od subjektov, na ktoré sa vzťahuje smernica NIS 2, vrátane zdravotníckych organizácií, požadovať, aby spolu s ďalšími informáciami, ktoré poskytujú pri podávaní správ o významných kybernetických incidentoch, podávali správy o všetkých uskutočnených platbách výkupného a o platbách výkupného, ktoré plánujú uskutočniť. Podávaním takýchto správ sa podporuje účinné vyšetrovanie ransomvérových

[43] V článku 23 ods. 1 smernice NIS 2 sa stanovuje požiadavka, aby kľúčové a dôležité subjekty oznamovali významné incidenty príslušnej jednotke CSIRT alebo v náležitých prípadoch príslušnému orgánu.

incidentov vrátane sledovania platieb na platformách na výmenu kryptomien s cieľom identifikovať príjemcov.

Rýchlosť obnovy je rozhodujúcim faktorom pri udržiavaní odolnosti a dôvery verejnosti, najmä v zdravotníctve, kde výpadky môžu narušiť starostlivosť o pacientov. Na účinnú obnovu po ransomvérových útokoch musia mať poskytovatelia zdravotnej starostlivosti bezpečné, aktuálne a izolované zálohy, ktoré sa dajú rýchlo obnoviť. Centrum podpory by mohlo v rámci svojho katalógu služieb ponúkať **abonentskú službu na obnovu po ransomvérovom útoku, čím by sa nemocniciam a poskytovateľom zdravotnej starostlivosti pomohlo ešte pred útokmi pripraviť plány obnovy**. Agentúra ENISA a Europol by mali spolupracovať na identifikácii najčastejších druhov ransomvéru, ktoré sa zameriavajú na zdravotnícke organizácie, a **rozšíriť úložisko dešifrovacích nástrojov** dostupných prostredníctvom projektu No More Ransom[44]. Takisto by mali vypracovať a propagovať dostupné usmernenia, ktoré pomôžu poskytovateľom zdravotnej starostlivosti vyhnúť sa plateniu výkupného vďaka použitiu dešifrovacích nástrojov.

Cenným priestorom na výmenu informácií o konkrétnych ransomvérových incidentoch, ako aj na budovanie kapacít členských krajín na posilnenie ich rámcov kybernetickej bezpečnosti a vyšetrovacích kapacít proti ransomvérovým aktérom, je **Medzinárodná iniciatíva na boj proti ransomvéru**[45]. Komisia bude v spolupráci s vysokou predstaviteľkou naďalej rozvíjať spoluprácu v rámci iniciatívy na boj proti ransomvéru, a to aj proti ransomvérovým hrozbám v sektore zdravotníctva. Okrem toho sa Komisia bude usilovať o spoluprácu v rámci **pracovnej skupiny G7 pre kybernetickú bezpečnosť** s cieľom posilniť kybernetickú bezpečnosť v sektore zdravotníctva. Pracovná skupina by mohla zvážiť najmä možnosti podpory sektora zdravotníctva v boji proti hrozbám, ako je ransomvér, pričom by mohla vychádzať z úvah, ako je spoločné vyhlásenie o ransomvérových útokoch na zdravotnícke zariadenia z 8. novembra 2024, ktoré bolo predložené v rámci Bezpečnostnej rady OSN[46].

4. Opatrenia na úrovni členských štátov

Schopnosť tohto akčného plánu zlepšiť kybernetickú bezpečnosť v sektore zdravotníctva závisí od aktívnej účasti a angažovanosti členských štátov. Na úspešné vykonávanie akčného plánu by členské štáty mohli určiť **národné centrá na podporu kybernetickej bezpečnosti osobitne pre nemocnice a poskytovateľov zdravotnej starostlivosti**. Tieto centrá by pôsobili ako hlavné kontaktné miesta pre sektor zdravotníctva na vnútroštátnej úrovni a úzko by spolupracovali s centrom podpory agentúry ENISA. Ak je to možné a relevantné, členské štáty by mali ako národné centrá na podporu kybernetickej

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

bezpečnosti určiť existujúce orgány, ako sú národné zdravotnícke jednotky CSIRT alebo príslušné orgány.

Členské štáty sa takisto vyzývajú, aby vytvorili **národné akčné plány zamerané na kybernetickú bezpečnosť v sektore zdravotníctva**. V týchto plánoch by sa uvádzali konkrétne kybernetické riziká, ktorým čelia systémy zdravotnej starostlivosti, a vnútroštátne opatrenia, ktoré sa prijímajú na ich riešenie, pričom by sa zabezpečilo aj účinné využívanie zdrojov a postupov na európskej úrovni. Centrum podpory agentúry ENISA môže pomôcť pri vypracúvaní uvedených plánov, pričom by sa zohľadnili už existujúce národné plány a koordinovalo by sa úsilie s cieľom zabezpečiť, aby sa zdroje a stratégie jednotlivých členských štátov navzájom dopĺňali.

Ďalším kľúčovým cieľom členských štátov je uľahčiť spoločné využívanie zdrojov medzi poskytovateľmi zdravotnej starostlivosti, čo by sa mohlo dosiahnuť prostredníctvom **spoločného obstarávania alebo združených zdrojov** na celoštátnej, regionálnej alebo dokonca európskej úrovni. Uvedeným prístupom by sa znížilo finančné zaťaženie jednotlivých subjektov a zároveň by sa zvýšila ich vyjednávacia sila s poskytovateľmi služieb kybernetickej bezpečnosti.

Napríklad v rámci francúzskeho programu CaRE[47] sa na celoštátnej a regionálnej úrovni zaviedlo viacero opatrení na riešenie výziev v oblasti zabezpečenia zdrojov: kybernetický katalóg poskytuje prehľad kybernetických riešení a balíkov, ktoré sú nemocniciam k dispozícii prostredníctvom národnej agentúry pre kybernetickú bezpečnosť, agentúry pre elektronické zdravotníctvo, regionálnych agentúr, národných obstarávacích organizácií, ako aj komerčných riešení. Dopĺňajú ich ďalšie finančné prostriedky pre regionálne agentúry, aby ponúkali zdieľané zdroje.

Členské štáty by sa mali zaoberať aj nedostatočnou úrovňou investícií do kybernetickej bezpečnosti v sektore zdravotníctva. Na zabezpečenie primeraného financovania by mali stanoviť **nezáväzné referenčné hodnoty a monitorovať ciele financovania zamerané konkrétne na kybernetickú bezpečnosť**, pričom by mali zabezpečiť, aby tieto investície neovplyvňovali základnú starostlivosť o pacientov. Tieto ciele financovania by sa mali zamerať aj na začlenenie bezpečnostných aspektov do všetkých digitálnych investícií v sektore. Členské štáty si môžu vymieňať najlepšie postupy a rady týkajúce sa týchto cieľov prostredníctvom platforiem, ako je sieť elektronického zdravotníctva[48].

5. Spolupráca verejného a súkromného sektora

Na úspešnú realizáciu akčného plánu je nevyhnutná spolupráca verejného a súkromného sektora a konzultácie s poskytovateľmi zdravotnej starostlivosti, ďalšími subjektmi v sektore zdravotníctva, ako aj s príslušnými aktérmi v odvetví kybernetickej bezpečnosti. V záujme ďalšieho posilnenia činnosti centra podpory **Komisia s podporou agentúry ENISA zriadi spoločný poradný výbor pre**

[47] Francúzska agentúra pre elektronické zdravotníctvo: Cybersécurité acceleration et Résilience des Établissements (CaRE). K dispozícii na https://esante.gouv.fr/strategie-nationale/cybersecurite.

[48] Sieť elektronického zdravotníctva je dobrovoľná sieť vnútroštátnych orgánov určených členskými štátmi, ktoré zodpovedajú za elektronické zdravotníctvo, a je zriadená na základe článku 14 smernice 2011/24/EÚ.

kybernetickú bezpečnosť v zdravotníctve, v ktorom budú pôsobiť vysokopostavení zástupcovia oboch oblastí, zdravotníctva aj kybernetickej bezpečnosti a v rámci ktorého možno Komisii a centru podpory poskytovať poradenstvo v oblasti účinných opatrení a diskutovať o ďalšom rozvoji verejno-súkromných partnerstiev v tejto oblasti. Výbor nadviaže na súčasné úsilie o budovanie verejno-súkromných partnerstiev vrátane európskeho strediska pre výmenu a analýzu informácií v zdravotníctve.

Okrem toho Komisia otvorí **výzvu na činnosť** pre spoločnosti, nadácie, vzdelávacie inštitúcie a zainteresované strany z odvetvia kybernetickej bezpečnosti, **aby prisľúbili konať v záujme riešenia výziev v tomto sektore**. Na základe skúseností s Akadémiou zručností v oblasti kybernetickej bezpečnosti by takéto záväzky mohli predstavovať napríklad prísľuby v rámci Akadémie zručností v oblasti kybernetickej bezpečnosti, ktoré by zahŕňali poskytovanie kurzov a materiálov odbornej prípravy so zameraním na sektor zdravotníctva pre odborníkov v oblasti kybernetickej bezpečnosti[49]. Ďalšie záväzky by sa mohli týkať aj činností na zvyšovanie informovanosti alebo poskytovanie riadených bezpečnostných služieb osobitne zraniteľným subjektom bezplatne alebo za zníženú cenu s cieľom zvýšiť ich pripravenosť a odolnosť v oblasti kybernetickej bezpečnosti. Okrem toho by záväzky mohli spočívať v zdieľaní spravodajských informácií o kybernetických hrozbách s centrom podpory agentúry ENISA. Centrum podpory by malo viesť prehľad prísľubov uskutočnených v rámci výzvy na činnosť s cieľom zabezpečiť ich súdržnosť a komplementárnosť.

6. Odradenie aktérov kybernetických hrozieb

Vnútorné a vonkajšie politiky EÚ v oblasti kybernetickej bezpečnosti by mali podporovať cieľ, ktorým je odradiť aktérov kybernetických hrozieb od útokov na európske systémy zdravotnej starostlivosti. Kybernetické útoky na zdravotnícke organizácie sú obzvlášť neprijateľným druhom škodlivej kybernetickej činnosti, a to vzhľadom na ich schopnosť ohroziť bezpečnosť pacientov a ľudské životy. Preto by sa mala plne využiť sila odstrašujúcich kapacít EÚ v oblasti kybernetickej bezpečnosti a presadzovania práva, aby sa oslabil celkový obchodný model aktérov hrozieb zameraných na sektor zdravotníctva a aby títo aktéri prišli o ľahké zisky. Zahŕňalo by to podporu cezhraničných vyšetrovaní prostredníctvom posilneného zdieľania indikátorov kompromitácie a iných relevantných údajov a väčšie sústredenie sa na ciele s vysokou hodnotou a na kľúčových poskytovateľov pomoci na páchanie trestných činov, ako sú napríklad služby hostingu tolerujúceho nezákonný obsah a aktivity (*bulletproof hosting*) alebo miešania kryptomien.

Rámec na predchádzanie kybernetickým útokom na EÚ, členské štáty a partnerov, na odrádzanie od nich a na reakciu na ne ponúka **súbor nástrojov kybernetickej diplomacie**. Vysoká predstaviteľka bude naďalej využívať existujúci rámec kybernetických sankcií na reakciu na hrozby zamerané na systémy zdravotnej starostlivosti.

Dôležitým odstrašujúcim prostriedkom je vyvodzovanie zodpovednosti voči páchateľom trestnej činnosti za ich činy. Členské štáty by preto mali zabezpečiť, aby bolo presadzovanie práva v plnej miere začlenené do ich národných akčných plánov. Mali by najmä v plnej miere využívať ustanovenia smernice

[49] *Cyber Skills Academy: Get Involved|Digital Skills and Jobs Platform* (Akadémia zručností v oblasti kybernetickej bezpečnosti: Zapojte sa | Platforma pre digitálne zručnosti a pracovné miesta).

o útokoch na informačné systémy[50] a Budapeštianskeho dohovoru Rady Európy o počítačovej kriminalite s cieľom odrádzať od útokov, postaviť páchateľov pred súd a rozložiť zločinecké infraštruktúry, ktoré uľahčujú útoky[51]. Úspešným zavedením uvedených nástrojov by sa malo zabezpečiť potrestanie kriminálneho a škodlivého konania proti zdravotníctvu.

7. Vykonávanie a monitorovanie akčného plánu

V celom tomto akčnom pláne sa predpokladá viacero úloh, ktoré by malo plniť centrum podpory, ktoré sa má zriadiť v rámci agentúry ENISA. Zabezpečí sa tým ucelené a koherentné vykonávanie akčného plánu a zároveň sa zabráni vytváraniu nových subjektov, čo by mohlo viesť k prekrývaniu a vzniku režijných nákladov. Komisia má v úmysle zabezpečiť primerané zdroje pre centrum podpory.

Po spustení centra podpory by agentúra ENISA po konzultácii s Komisiou mala pravidelne poskytovať aktuálne informácie o práci centra podpory správnej rade agentúry ENISA, ako aj príslušným sieťam členských štátov, najmä skupine pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieti jednotiek CSIRT, sieti elektronického zdravotníctva a v relevantných prípadoch aj Rade európskeho priestoru pre zdravotné údaje. Okrem toho by si agentúra ENISA mala s verejno-súkromným poradným výborom pre kybernetickú bezpečnosť v zdravotníctve priebežne vymieňať informácie o vykonávaní opatrení, ktoré poskytuje centrum podpory.

Ako príležitosť na uverejnenie príslušných údajov by mali slúžiť pravidelné správy agentúry ENISA, napríklad správa o stave kybernetickej bezpečnosti v Únii, v ktorej sa poskytuje súhrnné posúdenie úrovne vyspelosti spôsobilostí a zdrojov v oblasti kybernetickej bezpečnosti v celej EÚ vrátane sektora zdravotníctva, čím by sa podporilo monitorovanie akčného plánu. Okrem toho index kybernetickej bezpečnosti EÚ agentúry ENISA[52] môže poskytnúť kvantitatívne a kvalitatívne údaje, ktoré slúžia ako dôkazová základňa na posúdenie kritickosti a vyspelosti sektora zdravotníctva.

8. Ďalšie kroky

V tomto oznámení sa stanovuje ambiciózny program pre kyberneticky bezpečnejší sektor zdravotníctva v EÚ. Akčný plán, v ktorom sa navrhuje vytvorenie Centra na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti v rámci agentúry ENISA, predstavuje cestu k vytvoreniu koherentného a spoločného európskeho prístupu k riešeniu problémov kybernetickej bezpečnosti v tomto sektore.

Toto oznámenie by sa malo považovať za začiatok procesu zlepšovania kybernetickej bezpečnosti v sektore zdravotníctva. Zároveň s prijatím akčného plánu sa preto začnú komplexné konzultácie so

---

50 Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.

51 Dohovor o počítačovej kriminalite (Budapeštiansky dohovor, ETS č. 185) a jeho protokoly: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

52 ENISA, *EU Cybersecurity Index, Framework and Methodological Note* (Index kybernetickej bezpečnosti EÚ, rámec a metodické poznámky) (2024). K dispozícii na https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

zainteresovanými stranami a bude pokračovať výmena informácií s členskými štátmi a príslušnými sieťami s cieľom zhromaždiť poznatky. Na základe výsledkov konzultácií zamýšľa Komisia vo štvrtom štvrťroku 2025 predložiť odporúčania na ďalšie spresnenie akčného plánu.

Komisia vyzýva členské štáty a všetky zainteresované strany, aby spolupracovali pri napĺňaní ambícií akčného plánu.

PRÍLOHA – Prehľad navrhovaných opatrení

Komisia:

Centrum na podporu kybernetickej bezpečnosti agentúry ENISA pre nemocnice a poskytovateľov zdravotnej starostlivosti	
Zabezpečenie primeraných zdrojov pre centrum na podporu kybernetickej bezpečnosti Spolupráca s Európskym centrom kompetencií v oblasti kybernetickej bezpečnosti na spustení pilotných projektov s cieľom vyvinúť najlepšie postupy pre kybernetickú hygienu a posúdenie bezpečnostných rizík a riešiť potrebu nepretržitého monitorovania kybernetickej bezpečnosti, spravodajských informácií o hrozbách a reakcie na incidenty s využitím najmodernejších riešení v oblasti kybernetickej bezpečnosti na účely rozvoja katalógu služieb Európskeho centra na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti	2025
Predchádzanie incidentom v oblasti kybernetickej bezpečnosti	
Preskúmanie možnosti určenia zdravotníctva ako sektora, ktorému možno poskytnúť podporu na koordinované testovanie pripravenosti na základe aktu o kybernetickej solidarite, a to na základe konzultácií so skupinou pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti, sieťou EU-CyCLONe a agentúrou ENISA	1. štvrťrok 2025
Rýchla reakcia a obnova	
Zabezpečenie, aby rezerva EÚ na účely kybernetickej bezpečnosti zahŕňala službu rýchlej reakcie osobitne pre sektor zdravotníctva, a to spolu s agentúrou ENISA	4. štvrťrok 2025
Spolupráca verejného a súkromného sektora	
Zriadenie spoločného poradného výboru pre kybernetickú bezpečnosť v zdravotníctve, a to s podporou agentúry ENISA	1. štvrťrok 2025
Otvorenie výzvy na činnosť pre spoločnosti, nadácie, vzdelávacie inštitúcie a zainteresované strany z odvetvia kybernetickej bezpečnosti, aby prisľúbili	2. štvrťrok 2025

konať v záujme riešenia výziev v sektore zdravotníctva	
Odradenie aktérov kybernetických hrozieb	
Preskúmanie využitia opatrení súboru nástrojov kybernetickej diplomacie na predchádzanie škodlivým činnostiam proti zdravotníckym systémom, na odrádzanie od nich a na reakciu na ne, a to spolu s vysokou predstaviteľkou	2025
Rozširovanie medzinárodnej spolupráce proti aktérom ransomvéru, najmä v rámci medzinárodnej iniciatívy na boj proti ransomvéru, a to v spolupráci s vysokou predstaviteľkou	2025 – 2026
Úsilie o spoluprácu v rámci pracovnej skupiny G7 pre kybernetickú bezpečnosť s cieľom posilniť kybernetickú bezpečnosť v sektore zdravotníctva	2025 – 2026
Ďalšie kroky	
Začatie komplexných konzultácií so zainteresovanými stranami	1. štvrťrok 2025
Prijatie odporúčaní na ďalšie spresnenie akčného plánu	4. štvrťrok 2025

Agentúra ENISA:

Európske centrum na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti	
Začatie prác na zriadení Európskeho centra na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti	2. štvrťrok 2025
Vypracovanie komplexného katalógu služieb, ktoré bude poskytovať centrum na podporu kybernetickej bezpečnosti	od 4. štvrťroka 2025
Predchádzanie incidentom v oblasti kybernetickej bezpečnosti	
Vydanie usmernení, ktorými sa upozorní na najkritickejšie postupy v oblasti kybernetickej bezpečnosti a pomôže sa poskytovateľom zdravotnej starostlivosti pri ich zavádzaní	3. štvrťrok 2025

Vytvorenie nástroja na mapovanie regulácie v úzkej spolupráci s Komisiou a členskými štátmi	1. štvrťrok 2025
Vypracovanie rámca pre posúdenie vyspelosti v oblasti kybernetickej bezpečnosti so špecifickým zameraním na zdravotníctvo	3. štvrťrok 2025
Vykonanie ročného posúdenia vyspelosti v oblasti kybernetickej bezpečnosti v zdravotníctve	2025 – 2026
Spolupráca s členskými štátmi a regionálnymi orgánmi pre príslušné programy pri vytváraní modelových programov kyberbezpečnostných poukazov	2025 – 2026
Vypracovanie nových usmernení pre verejné obstarávanie v oblasti kybernetickej bezpečnosti nemocníc a poskytovateľov zdravotnej starostlivosti	3. štvrťrok 2025
Vytvorenie európskej siete riadiacich pracovníkov pre informačnú bezpečnosť v oblasti zdravotníctva	1. štvrťrok 2026
Návrh a podpora modulov a kurzov odbornej prípravy v oblasti kybernetickej bezpečnosti pre zdravotníckych pracovníkov	1. štvrťrok 2026
Európske kapacity na odhaľovanie kybernetických hrozieb v sektore zdravotníctva	
Vytvorenie európskeho katalógu známych zneužívaných zraniteľností (KEV) pre zdravotnícke pomôcky, systémy elektronických zdravotných záznamov a poskytovateľov zariadení IKT a softvéru v zdravotníctve	4. štvrťrok 2025
Zavedenie celoúnijnej abonentskej služby včasného varovania pre sektor zdravotníctva	od roku 2026
Podpora európskeho strediska pre výmenu a analýzu informácií v zdravotníctve prostredníctvom nástrojov a výmeny informácií	2025 – 2026
Rýchla reakcia a obnova	
Zabezpečenie, aby rezerva EÚ na účely kybernetickej bezpečnosti zahŕňala službu rýchlej reakcie osobitne pre sektor zdravotníctva, a to spolu s Komisiou	4. štvrťrok 2025
Vypracovanie príručiek pre riešenie kybernetických incidentov prispôsobených pre zdravotníctvo v spolupráci so sieťou jednotiek CSIRT	3. štvrťrok 2025

Uľahčenie rozsiahleho zavedenia vnútroštátnych cvičení v oblasti kybernetickej bezpečnosti s cieľom otestovať príručky a posilniť protokoly reakcie na incidenty	Od 4. štvrťroka 2025
Poskytovanie abonentskej služby na obnovu po ransomvérovom útoku	od roku 2026
Identifikácia najčastejších druhov ransomvéru, ktoré sa zameriavajú na zdravotnícke organizácie, a rozšírenie úložiska dešifrovacích nástrojov prostredníctvom projektu No More Ransom, a to spolu s Europolom	4. štvrťrok 2025
Vypracovanie dostupných usmernení, ktoré pomôžu poskytovateľom zdravotnej starostlivosti vyhnúť sa plateniu výkupného, a to spolu s Europolom	3. štvrťrok 2025
Opatrenia na úrovni členských štátov	
Pomoc členským štátom pri vypracúvaní národných akčných plánov	2025
Koordinácia úsilia s cieľom zabezpečiť, aby sa zdroje a stratégie jednotlivých členských štátov navzájom dopĺňali	2025 – 2026
Vykonávanie a monitorovanie akčného plánu	
Pravidelné poskytovanie aktuálnych informácií o práci centra na podporu kybernetickej bezpečnosti príslušným sieťam členských štátov na základe konzultácií s Komisiou	2025 – 2026
Priebežná výmena informácií s poradným výborom pre kybernetickú bezpečnosť v zdravotníctve	2025 – 2026

Členské štáty:

Európske kapacity na odhaľovanie kybernetických hrozieb v sektore zdravotníctva	
Zdieľanie oznámení o incidentoch od nemocníc a poskytovateľov zdravotnej starostlivosti na základe smernice NIS 2 s Európskym centrom na podporu kybernetickej bezpečnosti pre nemocnice a poskytovateľov zdravotnej starostlivosti	Od 4. štvrťroka 2025

Podnecovanie rozvoja vnútroštátnych stredísk pre výmenu a analýzu informácií v zdravotníctve	2025 – 2026
Predchádzanie incidentom v oblasti kybernetickej bezpečnosti	
Vykonanie koordinovaného posúdenia bezpečnostných rizík, ktorým by sa posudzovali technické aj strategické riziká súvisiace s dodávateľskými reťazcami zdravotníckych pomôcok, a to v rámci skupiny pre spoluprácu v oblasti sieťovej a informačnej bezpečnosti	4. štvrťrok 2025
Rýchla reakcia a obnova	
Zavedenie vnútroštátnych cvičení v oblasti kybernetickej bezpečnosti s cieľom otestovať príručky a posilniť protokoly reakcie na incidenty	od roku 2026
Opatrenia na úrovni členských štátov	
Určenie národných centier na podporu kybernetickej bezpečnosti osobitne pre nemocnice a poskytovateľov zdravotnej starostlivosti	2. štvrťrok 2025
Vytvorenie národných akčných plánov zameraných na kybernetickú bezpečnosť v sektore zdravotníctva	4. štvrťrok 2025
Uľahčenie zdieľania zdrojov medzi poskytovateľmi zdravotnej starostlivosti	2025 – 2026
Stanovenie nezáväzných referenčných hodnôt a monitorovanie cieľov financovania zameraných konkrétne na kybernetickú bezpečnosť	4. štvrťrok 2025
Požiadavka na zdravotnícke organizácie a iné subjekty, na ktoré sa vzťahuje smernica NIS 2, aby oznámili svoje zámery zaplatiť výkupné	4. štvrťrok 2025