Rada
Unii Europejskiej

Bruksela, 16 stycznia 2025 r.
(OR. en)

5426/25

CYBER 21
SAN 15

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	15 stycznia 2025 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2025) 10 final
Dotyczy:	KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW Europejski plan działania w sprawie cyberbezpieczeństwa szpitali i świadczeniodawców

Delegacje otrzymują w załączeniu dokument COM(2025) 10 final.

Zał.: COM(2025) 10 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 15.1.2025 r.
COM(2025) 10 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO, RADY, EUROPEJSKIEGO KOMITETU EKONOMICZNO-SPOŁECZNEGO I KOMITETU REGIONÓW

Europejski plan działania w sprawie cyberbezpieczeństwa szpitali i świadczeniodawców

1. Wprowadzenie

Środowisko bezpieczeństwa w UE zmienia się w szybkim tempie: ataki hybrydowe i cyberataki stają się coraz bardziej powszechne, a ich celem jest destabilizacja naszego społeczeństwa poprzez wywoływanie podziałów i zakłóceń, a także osiąganie zysków z cyberprzestępczości. W obliczu tych zagrożeń Europa musi pilnie zwiększyć swoją gotowość i odporność na nowe wyzwania, podejmując działania we wszystkich sektorach i zgodnie z podejściem obejmującym całe społeczeństwo i całą administrację rządową, na podstawie zaleceń zawartych w sprawozdaniu specjalnego doradcy przewodniczącej Komisji Europejskiej, Sauliego Niinistö.

Bezpieczne i odporne systemy opieki zdrowotnej stanowią fundament modelu społecznego UE. Jednak szpitale i systemy opieki zdrowotnej są coraz bardziej narażone na zagrożenia, zwłaszcza ze strony grup przestępczych, które wykorzystują oprogramowanie szantażujące do uzyskania korzyści finansowych ze względu na wysoką wartość danych pacjentów, w tym elektronicznej dokumentacji medycznej. W ciągu ostatnich czterech lat sektor zdrowia był najczęściej atakowanym sektorem w UE, w tym podczas pandemii COVID-19, kiedy to celem cyberataków była w coraz większym stopniu infrastruktura zdrowotna. Cyberataki na szpitale i świadczeniodawców powodują bezpośrednie szkody dla ludzi, opóźniają procedury medyczne, prowadzą do zatorów w szpitalnych izbach przyjęć, a w skrajnych przypadkach mogą prowadzić do ofiar śmiertelnych.

Zagrożenie jest tym większe, że sektor zdrowia przechodzi głęboką transformację cyfrową. E-zdrowie oraz wykorzystywanie i ponowne wykorzystywanie danych dotyczących zdrowia mogą przyczynić się do tworzenia modeli opieki zdrowotnej lepiej dostosowanych do potrzeb i preferencji pacjentów, a także wspierać profilaktykę lub umożliwiać wcześniejsze leczenie. Włączenie narzędzi i rozwiązań cyfrowych do procesów klinicznych oraz wykorzystywanie i ponowne wykorzystywanie danych dotyczących zdrowia pozwala na podejmowanie trafniejszych decyzji klinicznych, przyczynia się do automatyzacji procesów w ochronie zdrowia oraz umożliwia szybszą i bardziej efektywną opiekę nad pacjentami. Narzędzia cyfrowe, wykorzystanie danych i wyroby medyczne, które są często podłączone do internetu i wspierane sztuczną inteligencją (AI), również odgrywają kluczową rolę w radzeniu sobie z wyzwaniami takimi jak niedobór pracowników opieki zdrowotnej.

Jednocześnie wzrost zastosowania narzędzi cyfrowych prowadzi również do zwiększenia liczby potencjalnych celów dla cyberprzestępców. Ponadto działania niektórych państw – takich jak Rosja, która prowadzi wojnę napastniczą przeciwko Ukrainie – pokazują, że placówki opieki zdrowotnej mogą stać się celem cyberataków. To sprawia, że sektor zdrowia jest potencjalnym celem cyberataków będących częścią szerszych kampanii hybrydowych. Cyberataki nie tylko zagrażają bezpieczeństwu pacjentów, lecz także osłabiają zaufanie publiczne do infrastruktury zdrowotnej i wiążą się z wysokimi kosztami związanymi z przywracaniem sprawności operacyjnej. Oprócz zapewnienia ochrony przed cyberatakami odporna i bezpieczna infrastruktura cyfrowa jest kluczowa dla efektywnego i pełnego wdrożenia europejskiej przestrzeni danych dotyczących zdrowia[1] (EHDS).

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

W związku z tym nadszedł czas, aby zwiększyć cyberbezpieczeństwo i odporność europejskich szpitali i świadczeniodawców, co podkreśliła przewodnicząca Ursula von der Leyen w wytycznych politycznych na następną kadencję Komisji Europejskiej na lata 2024–2029[2]. Niniejszy plan działania stanowi odpowiedź na pilne wyzwania oraz wyjątkowe zagrożenia, przed którymi stoi sektor. Nie ma jednego, uniwersalnego rozwiązania dla kwestii związanych z cyberbezpieczeństwem w opiece zdrowotnej. Zamiast tego plan kładzie nacisk na intensyfikację działań w zakresie zapobiegania, zwiększenia gotowości oraz bardziej skoordynowanego podejścia do solidarności, przy jednoczesnym wykorzystaniu wiedzy fachowej europejskiego sektora cyberbezpieczeństwa. Plan działania odzwierciedla podejście UE do bezpieczeństwa, które będzie dalej rozwijane i sformalizowane w przyszłej europejskiej strategii bezpieczeństwa wewnętrznego, a także określa kompleksową reakcję na wszystkie zagrożenia dla bezpieczeństwa wewnętrznego i koncentruje się na zdolności do przewidywania zagrożeń, zapobiegania szkodom oraz ochronie ludzi, przy jednoczesnym zaangażowaniu wszystkich szczebli administracji i zgodnie z podejściem obejmującym całe społeczeństwo.

Sektor zdrowia obejmuje szerokie spektrum podmiotów, takich jak szpitale, kliniki, domy opieki, ośrodki rehabilitacji i różnych świadczeniodawców, a także przemysł farmaceutyczny, medyczny i biotechnologiczny, producentów wyrobów medycznych i instytucje badawcze w dziedzinie zdrowia. Niniejszy plan działania koncentruje się głównie na cyberbezpieczeństwie szpitali i świadczeniodawców, rozumianych jako każda osoba fizyczna lub prawna lub inna jednostka organizacyjna legalnie świadcząca opiekę zdrowotną na terenie państwa członkowskiego[3]. Szpitale i świadczeniodawcy są wzajemnie powiązani z innymi placówkami opieki zdrowotnej i znajdują się najbliżej ludzi. Jednocześnie działania na rzecz cyberbezpieczeństwa szpitali i świadczeniodawców powinny również uwzględniać zagrożenia wpływające na szerszy łańcuch dostaw i ekosystem, co dotyczy na przykład podmiotów wykorzystujących dane dotyczące zdrowia do celów badań naukowych i uczenia maszynowego lub produkujących wyroby medyczne, w szczególności wyroby medyczne wyposażone w funkcje cyfrowe, które łączą się z internetem lub innymi wyrobami („internet rzeczy”).

Chociaż zabezpieczenie systemów opieki zdrowotnej należy przede wszystkim do kompetencji krajowych, sektor zdrowotny jest również sektorem krytycznym na mocy dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS 2)[4]. Cyberprzestępcy i inni agresorzy działają ponad granicami, a wyzwania w zakresie cyberbezpieczeństwa, przed którymi stoją organizacje opieki zdrowotnej, są również podobne we wszystkich państwach członkowskich. Współpraca na szczeblu europejskim odgrywa kluczową rolę w wymianie i upowszechnianiu najlepszych praktyk – zarówno unijnych, jak i krajowych. Dlatego w niniejszym planie działania zaproponowano koordynację oraz wdrożenie środków na szczeblu UE,

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_pl.
[3] Art. 3 lit. g) dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32011L0024.
[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555.

a jednocześnie wezwano państwa członkowskie do podjęcia działań zmierzających do transformacji opieki zdrowotnej i szeroko rozumianego ekosystemu zdrowotnego.

Plan działania koncentruje się przede wszystkim na budowaniu zdolności sektora do **zapobiegania** cyberincydentom, ponieważ zawsze lepiej jest zapobiegać, niż leczyć. Po drugie, przewiduje działania mające na celu poprawę wymiany informacji na temat cyberbezpieczeństwa i zdolności do **wykrywania** cyberzagrożeń, co pozwoli na szybszą reakcję. Po trzecie, zakłada wdrożenie środków mających na celu lepsze **reagowanie** na incydenty i **usuwanie** ich skutków. Ponadto przewidziano w nim sposoby **zniechęcania** podmiotów powodujących cyberzagrożenie do przeprowadzania ataków na systemy opieki zdrowotnej w Europie.

Realizacja planu będzie przebiegać we współpracy ze świadczeniodawcami i szerzej rozumianym ekosystemem zdrowia, państwami członkowskimi i społecznością zajmującą się cyberbezpieczeństwem. Podejście oparte na współpracy ma kluczowe znaczenie dla lepszego zdefiniowania i udoskonalenia najskuteczniejszych działań, tak aby wszyscy świadczeniodawcy o krytycznym znaczeniu w Europie mogli z nich skorzystać. W związku z tym niniejszemu komunikatowi towarzyszyć będzie rozpoczęcie kompleksowych konsultacji z zainteresowanymi stronami, sektorem i państwami członkowskimi. Ze względu na transgraniczny i wzajemnie powiązany charakter cyberzagrożeń współpraca międzynarodowa odgrywa kluczową rolę w zakresie cyberbezpieczeństwa. Podobne zagrożenia cyberbezpieczeństwa występują również w krajach objętych procesem rozszerzenia i krajach objętych polityką sąsiedztwa oraz w innych strategicznych krajach partnerskich UE. Sytuacja ta może ostatecznie zagrozić bezpieczeństwu infrastruktury krytycznej w UE. Dlatego ważne będzie, aby wnioski wyciągnięte z realizacji planu działania znalazły odzwierciedlenie również we współpracy UE zarówno z krajami objętymi procesem rozszerzenia, jak i z innymi krajami partnerskimi, biorąc pod uwagę poziomy zagrożeń, na które są one narażone.

2. Wyzwania związane z cyberbezpieczeństwem szpitali i świadczeniodawców

Cyberzagrożenia w sektorze zdrowia

Cyberataki na całym świecie i w UE są coraz powszechniejsze, a krajobraz zagrożeń staje się coraz bardziej złożony i dynamiczny. Rozwój sztucznej inteligencji wyposaża przestępców i podmioty działające w złych zamiarach w potężne narzędzia zwiększające precyzję i wpływ ich działań, a jednocześnie zmienia możliwości cyberobrony i umożliwia zautomatyzowane działania w czasie rzeczywistym przeciwko atakom.

Jednym z kluczowych wyzwań w zakresie cyberbezpieczeństwa w UE i na świecie pozostaje oprogramowanie szantażujące. Szacuje się, że do 2031 r. globalny roczny koszt związany z atakami z jego użyciem wyniesie ponad 250 mld EUR[5]. Przestępcy wykorzystujący oprogramowanie

[5] Cybersecurity Ventures (1 czerwca 2024 r.): „Przewiduje się, że globalne koszty szkód związanych z oprogramowaniem szantażującym przekroczą 265 mld USD do 2031 r.”. Dostępne pod adresem: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

szantażujące nie tylko szyfrują dane ofiar dla okupu, lecz także coraz częściej ujawniają informacje wrażliwe w celu wywarcia dodatkowej presji. Kolejnym istotnym wyzwaniem są luki w zabezpieczeniach oprogramowania i sprzętu: według Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[6] to właśnie sektor opieki zdrowotnej zgłosił najwięcej incydentów bezpieczeństwa związanych z takimi podatnościami[7]. Inne rosnące zagrożenia to rozproszone ataki typu „odmowa usługi" (DDoS), których celem jest przeciążenie docelowego systemu ogromną ilością ruchu i w efekcie uczynienie go niedostępnym dla uprawnionych użytkowników[8].

Sektor zdrowia boryka się z podobnymi tendencjami w zakresie cyberzagrożeń, ze szczególnym naciskiem na ataki z użyciem oprogramowania szantażującego. Według ENISA w latach 2021–2023 oprogramowanie szantażujące odpowiadało za 54 % przeanalizowanych cyberincydentów w sektorze zdrowia. 83 % ataków było motywowanych finansowo, co wynikało z wysokiej wartości danych dotyczących opieki zdrowotnej, a 10 % ataków miało motywację ideologiczną[9]. Sprawozdanie Komisji z 2024 r. wskazuje, że 71 % ataków mających wpływ na opiekę nad pacjentami i skutkujących na przykład opóźnieniem leczenia, diagnozy i utrudnionym dostępem do służb ratunkowych stanowiły ataki z użyciem oprogramowania szantażującego[10]. Ataki z użyciem oprogramowania szantażującego mogą w szczególnie dotkliwy sposób zakłócać świadczenie usług opieki zdrowotnej i zagrażać bezpieczeństwu pacjentów. Ponadto atakom tym często towarzyszą naruszenia ochrony danych pacjentów[11], które często obejmują wrażliwe dane dotyczące zdrowia i naruszają podstawowe prawo człowieka do ochrony danych osobowych.

Wraz z postępującą cyfryzacją opieki zdrowotnej rośnie jednocześnie powierzchnia ataku. Zgodnie ze sprawozdaniem na temat stanu cyfrowej dekady za 2024 r. średnio 79 % obywateli UE ma dostęp online do swojej elektronicznej dokumentacji medycznej w placówkach podstawowej opieki zdrowotnej[12]. Elektroniczna dokumentacja medyczna, systemy informacji klinicznej, systemy przepływu pracy szpitali, systemy informatyczne do obsługi zwrotu kosztów leczenia, systemy obrazowania medycznego i wyroby medyczne wykorzystywane do celów diagnostycznych lub do monitorowania pacjentów to

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie), https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[7] ENISA Threat Landscape: Health Sector [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor zdrowia] (lipiec 2023 r.).

[8] ENISA Threat Landscape 2024 [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń z 2024 r.].

[9] ENISA Threat Landscape: Health Sector [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor zdrowia] (lipiec 2023 r.). W sprawozdaniu przeanalizowano świadczeniodawców, a także inne rodzaje organizacji, w tym organizacje prowadzące badania w dziedzinie zdrowia, podmioty wytwarzające niektóre produkty związane ze zdrowiem, organy ds. zdrowia, organizacje ubezpieczeń zdrowotnych oraz zamknięte ośrodki leczenia i podmioty świadczące usługi społeczne. Dostępne pod adresem: https://www.enisa.europa.eu/publications/health-threat-landscape.

[10] Komisja Europejska: Wspólne Centrum Badawcze, Reina, V. i 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 [Cyberbezpieczeństwo w sektorze zdrowia i medycyny – badanie dotyczące dostępnych dowodów na konsekwencje zdrowotne dla pacjentów wynikające z cyberincydentów w placówkach opieki zdrowotnej], Urząd Publikacji UE, 2024, https://data.europa.eu/doi/10.2760/693487.

[11] Według sprawozdania ENISA dotyczącego krajobrazu zagrożeń w sektorze zdrowia naruszenie ochrony lub kradzież danych potwierdzono w 43 % przeanalizowanych incydentów z użyciem oprogramowania szantażującego.

[12] Sprawozdanie na temat stanu cyfrowej dekady za 2024 r.

przykłady narzędzi cyfrowych, które mogą odegrać istotną rolę w zwiększaniu wydajności i poprawie wyników sektora zdrowia, ale są również potencjalnymi celami cyberataków. Szczególnie narażone na cyberataki są konkretne rodzaje działalności w zakresie opieki zdrowotnej, takie jak intensywna opieka medyczna i obrazowanie radiologiczne, lub dziedziny medyczne, takie jak onkologia i kardiologia, które są w dużym stopniu zależne od urządzeń opartych na technologiach cyfrowych. Ponadto problemy związane z łańcuchem dostaw mogą prowadzić do zamawiania urządzeń z niewystarczającymi cyberzabezpieczeniami, co zwiększa istniejące ryzyko ogólne.

Na przykład podczas pandemii COVID-19 atak z użyciem oprogramowania szantażującego sparaliżował dużą część irlandzkiego systemu opieki zdrowotnej, co w dniu wystąpienia incydentu doprowadziło do odwołania niektórych usług w 31 z 54 szpitali opieki krótkoterminowej[13]. Placówki zdrowotne musiały przywrócić papierową dokumentację, co zmniejszyło wydajność ich działalności. Atak pochodził z phishingowej wiadomości e-mail zawierającej złośliwy załącznik[14]. Incydent pokazał potencjał cyberataków rozprzestrzeniających się w różnych systemach, a w konsekwencji znaczenie ochrony całej powierzchni ataku organizacji opieki zdrowotnej. Uwypuklił również znaczenie zapewnienia podstawowej higieny cyberbezpieczeństwa i kultury cyberbezpieczeństwa we wszystkich organizacjach.

Dojrzałość w zakresie cyberbezpieczeństwa szpitali i świadczeniodawców

Krajobraz opieki zdrowotnej w UE jest bardzo zróżnicowany, a szpitale i inni świadczeniodawcy różnią się znacznie pod względem własności, struktury i wielkości w poszczególnych państwach członkowskich. W niektórych przypadkach zarządzanie opieką zdrowotną może opierać się na scentralizowanym podejściu na szczeblu krajowym, a w innych – na szczeblu regionalnym i lokalnym, przy czym świadczeniodawcy mogą być podmiotami publicznymi lub prywatnymi. Ponadto różnice mogą występować również w obrębie jednego państwa, na przykład w przypadku znacznych różnic społeczno-gospodarczych i terytorialnych między regionami, co daje złożony obraz sytuacji. Temu złożonemu krajobrazowi opieki zdrowotnej mogą zagrażać poważne kryzysy zdrowotne spowodowane chorobami zakaźnymi, takie jak pandemia COVID-19, ale również innymi zagrożeniami dla zdrowia, na przykład związanymi ze zmianą klimatu. Ponadto poziom cyfryzacji i wdrażania technologii przez świadczeniodawców cechuje się znaczną zmiennością i fragmentacją. Przykładem takiej złożoności jest to, że niedostępność usługi spowodowana cyberincydentem może powodować poważne szkody dla pacjentów nawet w małych placówkach opieki zdrowotnej, w tym w poradniach lub oddziałach ratunkowych, które świadczą usługę podstawową dla stosunkowo niewielkiej liczby użytkowników.

Zgodnie ze sprawozdaniem ENISA o stanie cyberbezpieczeństwa w Unii z 2024 r.[15] dojrzałość unijnego sektora zdrowia w tym obszarze jest umiarkowana. Ponadto istnieją znaczące różnice w poziomie dojrzałości w zakresie cyberbezpieczeństwa między podmiotami opieki zdrowotnej w różnych krajach Europy. Niedociągnięcia można zaobserwować w kluczowych obszarach, takich jak kwestia

[13] Irlandzki zarząd służby zdrowia Health Service Executive (2021): „Conti cyber attack on the HSE: Independent Post Incident Review" [Cyberatak na HSE z wykorzystaniem oprogramowania Conti: niezależna ocena po incydencie].
[14] Irlandzki zarząd służby zdrowia Health Service Executive: „Cyber-attack and HSE response" [Cyberatak i reakcja HSE]. Dostępne pod adresem: https://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA: 2024 Report on the State of Cybersecurity in the Union [Sprawozdanie o stanie cyberbezpieczeństwa w Unii z 2024 r.] (wrzesień 2024 r.). Dostępne pod adresem: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

wystarczających zasobów ludzkich, wiedza organizacji na temat wykorzystywanych przez nie łańcuchów dostaw technologii informacyjno-komunikacyjnych (ICT) oraz instalacja aktualnych zabezpieczeń w produktach. Sektor ten zmaga się z problemami w zakresie podstawowej higieny cyberbezpieczeństwa i wdrażania podstawowych środków bezpieczeństwa, o czym świadczy fakt, że prawie wszystkie badane organizacje opieki zdrowotnej napotykają trudności w przeprowadzaniu ocen ryzyka w cyberprzestrzeni, a niemal połowa z nich nigdy nie przeprowadziła analizy ryzyka[16].

Kolejnym istotnym wyzwaniem dla cyberbezpieczeństwa szpitali jest skrzyżowanie technologii informacyjnej (IT) i technologii operacyjnej (OT), gdzie spotykają się różne priorytety w zakresie bezpieczeństwa w odniesieniu do poufności, dostępności i niezawodności, a naruszenie w jednym obszarze może mieć wpływ na drugi. W sprawozdaniu ENISA na temat stanu cyberbezpieczeństwa w Unii z 2024 r. podkreślono ponadto, że sektor zdrowia nie osiąga odpowiednich wyników w zapewnianiu bezpieczeństwa wykorzystywanych przez niego produktów i procesów ICT ze względu na dużą różnorodność podmiotów, wyrobów i produktów w dziedzinie zdrowia.

Ta różnorodność, w połączeniu ze zróżnicowanym poziomem wiedzy na temat cyberbezpieczeństwa wśród pracowników i kadry kierowniczej szpitali, stanowi złożone wyzwanie dla zapewnienia cyberbezpieczeństwa systemów opieki zdrowotnej. Na przykład według badania Eurobarometr dotyczącego umiejętności w dziedzinie cyberbezpieczeństwa z 2024 r. w ciągu ostatnich 12 miesięcy tylko 25 % badanych przedsiębiorstw w sektorze opieki zdrowotnej, edukacji i opieki społecznej przeprowadziło szkolenia lub działania informacyjne na temat cyberbezpieczeństwa[17]. Konieczne jest podjęcie działań promujących kulturę wiedzy na temat cyberbezpieczeństwa wśród pracowników opieki zdrowotnej pierwszej linii kontaktu. Na przykład rotacja pracowników, korzystanie ze wspólnych stanowisk pracy, złe zarządzanie uwierzytelnianiem i korzystanie z nośników wymiennych stanowią dodatkowe źródła podatności na zagrożenia wpływające na cyberbezpieczeństwo świadczeniodawców[18].

W wielu przypadkach usługi w zakresie IT i OT są przynajmniej częściowo zlecane na zewnątrz. Z badania Eurobarometr z 2024 r. wynika, że odsetek przedsiębiorstw zlecających na zewnątrz co najmniej część działań związanych z cyberbezpieczeństwem jest najwyższy w sektorach opieki zdrowotnej, edukacji i opieki społecznej, przy czym takie podejście stosuje 57 % ankietowanych przedsiębiorstw[19]. Obserwuje się również silną tendencję do migracji do chmury obliczeniowej, wynikającą z potrzeby skalowalnego przechowywania danych i zarządzania nimi, redukcji kosztów, usprawnienia współpracy oraz wsparcia dla zaawansowanych technologii, takich jak sztuczna inteligencja i internet rzeczy medycznych. W 2022 r. 58 % organizacji sektora opieki zdrowotnej korzystało z cyfrowej platformy zdrowia opartej na chmurze obliczeniowej[20]. Choć ta zmiana może

[16] ENISA Threat Landscape: Health Sector [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń: sektor zdrowia] (lipiec 2023 r.). Dostępne pod adresem: https://www.enisa.europa.eu/publications/health-threat-landscape.
[17] Badanie Eurobarometr Flash 547 dotyczące umiejętności w dziedzinie cyberbezpieczeństwa (maj 2024 r.). Dostępne pod adresem: https://europa.eu/eurobarometer/surveys/detail/3176.
[18] Panacea – Cyberbezpieczeństwo zorientowane na ludzi w opiece zdrowotnej (2021): Biała księga – Wnioski z PANACEA na temat cyberochrony szpitali i ośrodków opieki.
[19] Badanie Eurobarometr Flash 547 dotyczące umiejętności w dziedzinie cyberbezpieczeństwa (maj 2024 r.). Dostępne pod adresem: https://europa.eu/eurobarometer/surveys/detail/3176.
[20] ENISA: Sprawozdanie dotyczące inwestycji w zakresie bezpieczeństwa sieci i informacji za 2022 r. (listopad 2022 r.). Dostępne pod adresem: https://www.enisa.europa.eu/publications/nis-investments-2022.

prowadzić do znaczących usprawnień, niesie również ze sobą ryzyko, które wymaga podejmowania świadomych decyzji w zakresie zamówień oraz zapewnienia bezpiecznej konfiguracji systemów.

Nadrzędnym wyzwaniem w obliczu tych problemów jest budowanie zdolności oraz finansowanie. Cyberbezpieczeństwo w sektorze zdrowia jest niedofinansowane, co stanowi powszechny problem w całej UE[21]. Sytuację dodatkowo komplikuje starzejące się społeczeństwo, co w nadchodzących dziesięcioleciach prawdopodobnie wywrze powszechną presję budżetową na europejskie systemy opieki zdrowotnej.

Dalsze wykorzystywanie przestarzałych narzędzi i systemów, ograniczone zasoby na zapobieganie incydentom lub reagowanie na nie, a także luki w dojrzałości w zakresie cyberbezpieczeństwa często wynikają z braków w finansowaniu. Szpitale muszą nieustannie mierzyć się z wyzwaniem polegającym na znalezieniu równowagi między inwestowaniem w nowoczesną, bezpieczną i cyfrową infrastrukturę a innymi niezbędnymi inwestycjami służącymi poprawie opieki nad pacjentami, takimi jak zatrudnianie lekarzy i innych pracowników opieki zdrowotnej, wdrażanie nowatorskich metod diagnostyki i leczenia czy zakup wyrobów medycznych. Według ENISA[22] sektor zdrowia zajmuje dopiero 7. miejsce spośród 12 zbadanych sektorów pod względem udziału wydatków na bezpieczeństwo informacji w całkowitych wydatkach na IT, przy czym mediana tego udziału w sektorze opieki zdrowotnej wynosi 8,3 %.

3. Europejskie Centrum Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej

Unijne ramy cyberbezpieczeństwa oferują szeroki wachlarz narzędzi, które należy wykorzystać do poprawy bezpieczeństwa i odporności szpitali i świadczeniodawców. Aby sprostać licznym wyzwaniom opisanym powyżej, konieczne jest wypracowanie jednolitego, strategicznego podejścia na szczeblu UE, które połączy niezbędne zasoby, wiedzę fachową i narzędzia i umożliwi skuteczne zwalczanie cyberzagrożeń. Kompleksowy przegląd sytuacji, a także lepsze planowanie i koordynacja, mają zasadnicze znaczenie, aby pomóc świadczeniodawcom w całej UE wzmocnić ich systemy obrony przed cyberzagrożeniami. W tym kontekście ENISA jest najlepiej przygotowana do ustanowienia w swojej strukturze specjalnego **Europejskiego Centrum Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej**[23]. Centrum to, działając w ramach mandatu ENISA[24], miałoby na celu ochronę oraz wspieranie infrastruktury krytycznej UE.

Centrum Wsparcia powinno stopniowo **opracowywać kompleksowy katalog usług, który będzie dostosowany do potrzeb szpitali i świadczeniodawców** i będzie określał zakres dostępnych usług

[21] Organizacja i świadczenie usług zdrowotnych i opieki medycznej należy do kompetencji krajowych na mocy art. 168 Traktatu o funkcjonowaniu Unii Europejskiej, a systemy finansowania opieki zdrowotnej różnią się w poszczególnych państwach członkowskich.

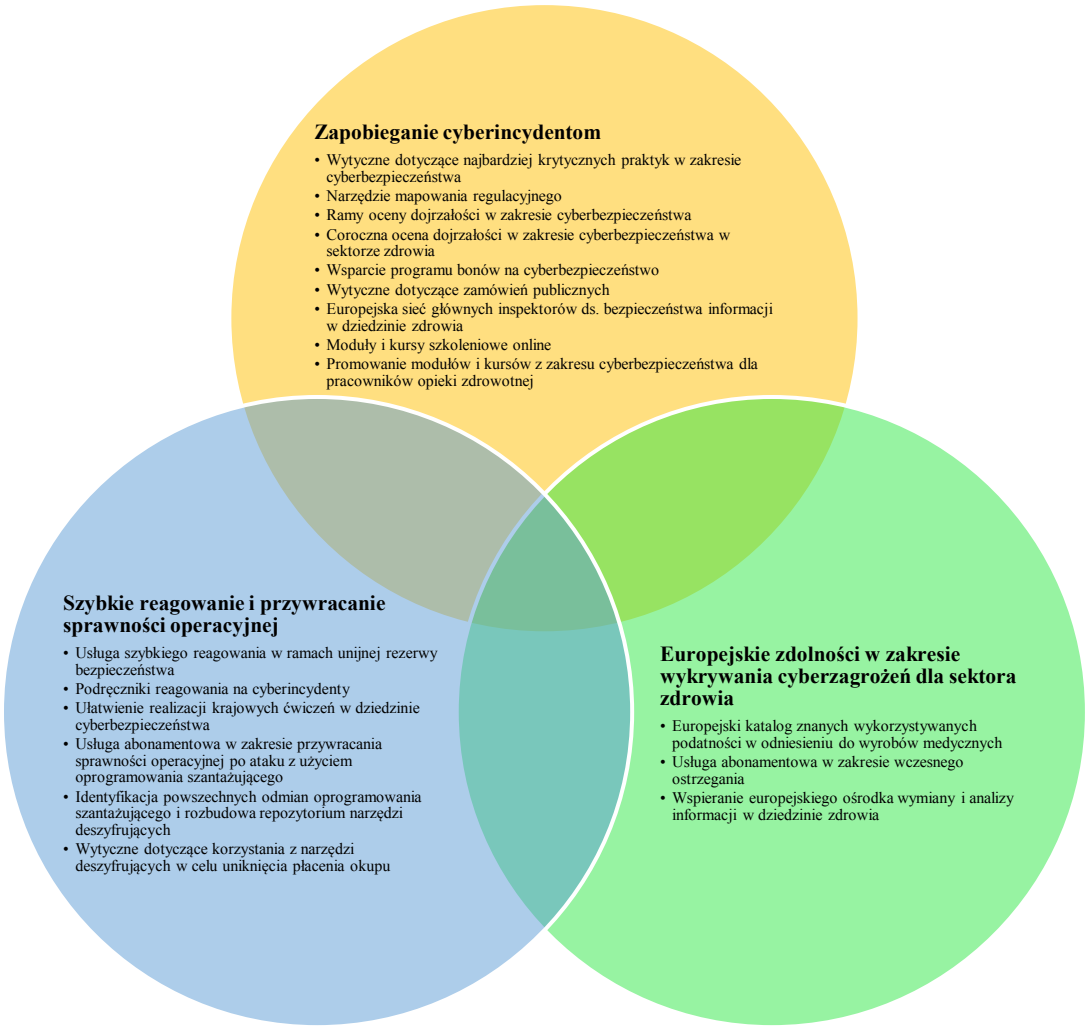
[22] ENISA: Sprawozdanie dotyczące inwestycji w zakresie bezpieczeństwa sieci i informacji za 2022 r. (listopad 2022 r.). Dostępne pod adresem: https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] W niniejszym dokumencie nazwa „Centrum Wsparcia" jest używana zamiennie.

[24] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

w obszarze gotowości, zapobiegania, wykrywania i reagowania. We współpracy z organami państw członkowskich oraz w oparciu o doświadczenia szpitali i świadczeniodawców Centrum Wsparcia powinno stworzyć przyjazne dla użytkownika i łatwo dostępne repozytorium zawierające wszystkie dostępne instrumenty na poziomie europejskim, krajowym i regionalnym. Przy realizacji swoich zadań Centrum Wsparcia powinno zapewnić odpowiednią koordynację z państwami członkowskimi oraz wspierać ustalanie priorytetów i realizację działań, które odpowiadają na bieżące potrzeby w czasie rzeczywistym.

Ważnym elementem opracowywania katalogu usług Centrum Wsparcia będzie zaproponowane przez Komisję uruchomienie projektów pilotażowych w całej UE. Celem tych projektów będzie opracowanie najlepszych praktyk w zakresie higieny cyberbezpieczeństwa i oceny ryzyka związanego z bezpieczeństwem, a także zaspokojenie potrzeby stałego monitorowania cyberbezpieczeństwa, rozpoznawania zagrożeń i reagowania na incydenty, z wykorzystaniem najnowocześniejszych rozwiązań w dziedzinie cyberbezpieczeństwa. Wyniki tych projektów pilotażowych, które będą finansowane z programu „Cyfrowa Europa", realizowanego przez Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC), będą stanowić podstawę dalszych działań na szczeblu UE, w tym prac Centrum Wsparcia.



Rysunek 1: Koncepcje katalogu usług Centrum Wsparcia dla szpitali i świadczeniodawców

3.1.Zapobieganie cyberincydentom

Proste działania, które zwiększają szanse

Podstawowe środki w zakresie cyberbezpieczeństwa, takie jak regularne aktualizowanie systemów, zarządzanie kopiami zapasowymi oraz wdrażanie uwierzytelniania wieloskładnikowego, mogą – według jednego z szacunków – chronić organizacje przed nawet 98 % ataków[25]. Wiele z najskuteczniejszych środków higieny cyberbezpieczeństwa i zarządzania ryzykiem jest stosunkowo prostych do wdrożenia,

[25] Sprawozdanie Microsoft Digital Defense Report z 2022 r. Dostępne pod adresem: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

co sprawia, że pozwalają one w łatwy sposób poprawić poziom cyberbezpieczeństwa. Jednym z kluczowych zadań Centrum Wsparcia powinno być zatem **opracowanie jasnych, ukierunkowanych wytycznych, które kładłyby nacisk na najbardziej krytyczne praktyki w zakresie cyberbezpieczeństwa i pomagały świadczeniodawcom w ich wdrażaniu**. Wsparcie to powinno dotyczyć nie tylko dużych szpitali, ale obejmować również dostosowane do potrzeb doradztwo dla mniejszych podmiotów, takich jak lokalne gabinety lekarzy podstawowej opieki zdrowotnej i poradnie specjalistyczne. Te placówki często nie dysponują zasobami na specjalne zespoły ds. cyberbezpieczeństwa, a są równie narażone na ataki. Ponadto konieczne jest uwzględnienie znaczenia, jakie dla zapewnienia opieki nad pacjentem mają poszczególne podmioty opieki zdrowotnej w danym regionie, na przykład na obszarach słabo zaludnionych. Wytyczne dotyczące podstawowych środków cyberbezpieczeństwa mogłyby również zwiększyć odporność instytutów badawczych w dziedzinie zdrowia, które przetwarzają duże ilości wrażliwych danych osobowych.

Organizacje opieki zdrowotnej podlegają również szeregowi obowiązków związanych z cyberbezpieczeństwem wynikających z prawodawstwa UE[26]. Chociaż obowiązki te są kluczowe dla zapewnienia wysokiego wspólnego poziomu bazowego w zakresie cyberbezpieczeństwa i bezpieczeństwa danych, równie istotne jest, aby otoczenie regulacyjne nie stało się niepotrzebnie skomplikowane i uciążliwe. Duży nacisk na przestrzeganie przepisów nie powinien kolidować z celem, jakim jest wspieranie silnej kultury cyberbezpieczeństwa. **Łatwo dostępne narzędzie mapowania regulacyjnego może pomóc podmiotom podlegającym wielu instrumentom regulacyjnym zminimalizować obciążenie administracyjne.** Oprócz opracowywania wytycznych i zestawów narzędzi Centrum Wsparcia powinno ściśle współpracować z Komisją i państwami członkowskimi w celu jak najszybszego opracowania i rozpowszechnienia takiego narzędzia. Centrum Wsparcia odgrywałoby zatem kluczową rolę w ułatwianiu zrozumienia i wdrażania przepisów dotyczących

[26] Takiego jak dyrektywa NIS 2; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (akt o cyberodporności), https://eur-lex.europa.eu/eli/reg/2024/2847/ojhttps://eur-lex.europa.eu/eli/reg/2024/2847/oj; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, https://eur-lex.europa.eu/eli/reg/2017/745/ojhttps://eur-lex.europa.eu/eli/reg/2017/745/oj (rozporządzenie w sprawie wyrobów medycznych), https://eur-lex.europa.eu/eli/reg/2017/745/oj, rozporządzenie w sprawie wyrobów medycznych; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki *in vitro* (rozporządzenie w sprawie wyrobów medycznych do diagnostyki *in vitro*), https://eur-lex.europa.eu/eli/reg/2017/746/ojhttps://eur-lex.europa.eu/eli/reg/2017/746/oj; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016R0679; rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt w sprawie sztucznej inteligencji), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689; wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie europejskiej przestrzeni danych dotyczących zdrowia, COM(2022) 197 final, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52022PC0197. Negocjacje zakończyły się porozumieniem politycznym wiosną 2024 r., a po finalizacji szczegółów publikacja w Dzienniku Urzędowym planowana jest na wiosnę 2025 r.

cyberbezpieczeństwa, na przykład poprzez dostarczanie wytycznych dotyczących wdrażania tych przepisów oraz[27], w stosownych przypadkach, promowanie stosowania właściwych norm.

Przygotowywane **europejskie portfele tożsamości cyfrowej** są kolejnym narzędziem ułatwiającym proste wdrażanie dobrych praktyk w zakresie higieny cyberbezpieczeństwa. Zmniejszenie zależności od słabych mechanizmów identyfikacji, takich jak hasła, ma zasadnicze znaczenie dla ograniczenia ryzyka nieuprawnionego dostępu do danych dotyczących zdrowia. Niezbędne jest przejście na bezpieczne rozwiązania w zakresie logowania, oparte na niezawodnym mechanizmie identyfikacji. Unijny portfel tożsamości cyfrowej oferuje zharmonizowane, ogólnounijne podejście do identyfikacji elektronicznej dla pracowników opieki zdrowotnej i stanowi solidne, jednolite rozwiązanie, które wejdzie w życie pod koniec 2026 r. Wszystkie internetowe systemy informacji zdrowotnej zobowiązane do wdrożenia funkcji silnego uwierzytelniania użytkowników będą musiały zaakceptować portfel do celów identyfikacji do końca 2027 r.[28]

Gotowość i ukierunkowane wsparcie

Testowanie gotowości, obejmujące działania takie jak testy penetracyjne, jest kluczowym elementem skutecznego dbania o cyberbezpieczeństwo. Komisja już przeznaczyła środki finansowe dla ENISA na pilotażowe inicjatywy w zakresie gotowości, które ujawniły, że sektor zdrowia wymaga szczególnej uwagi pod względem testowania i dalszych ocen, umożliwiających identyfikację luk w dojrzałości w zakresie cyberbezpieczeństwa. Po wejściu w życie aktu w sprawie cybersolidarności działania te zostaną znacznie rozszerzone, a ECCC przejmie wiodącą rolę. W odpowiedzi na tę potrzebę Komisja, w porozumieniu z Grupą Współpracy NIS, EU-CyCLONe[29] i ENISA, zaproponuje wskazanie sektora zdrowia jako sektora, któremu można udzielić wsparcia na rzecz **skoordynowanego testowania gotowości** na podstawie aktu w sprawie cybersolidarności. Ponadto Centrum Wsparcia powinno opracować **ramy oceny dojrzałości w zakresie cyberbezpieczeństwa, dostosowane do specyficznych potrzeb sektora opieki zdrowotnej**. Takie oceny dojrzałości dostarczą podmiotom praktycznych informacji na temat ich podatności na zagrożenia, a jednocześnie umożliwią im wykazanie gotowości do zapewnienia cyberbezpieczeństwa pacjentom oraz innym zainteresowanym stronom, co przyczyni się do budowania zaufania do świadczonych usług. W ujęciu zbiorczym Centrum Wsparcia powinno przeprowadzać **coroczną ocenę dojrzałości w zakresie cyberbezpieczeństwa w sektorze zdrowia**, która dostarczałaby jasnego obrazu stanu cyberbezpieczeństwa tego sektora zarówno na poziomie krajowym, jak i unijnym.

Sektor zdrowia w dużym stopniu korzysta z zewnętrznych wykonawców usług w zakresie cyberbezpieczeństwa[30], co uwydatnia potrzebę ukierunkowanego wsparcia na wzmocnienie ochrony. Na

[27] Za opracowanie wytycznych dotyczących interpretacji ogólnego rozporządzenia o ochronie danych (RODO) odpowiada Europejska Rada Ochrony Danych (EROD). Opracowanie wytycznych przez ENISA powinno odbywać się z pełnym poszanowaniem prerogatyw EROD.
[28] Art. 5f ust. 1 i 2 rozporządzenia (UE) 910/2014.
[29] Europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa.
[30] Zob. sprawozdanie ENISA dotyczące inwestycji w zakresie bezpieczeństwa sieci i informacji za 2023 r. (listopad 2023 r.), w którym podkreślono znaczenie zewnętrznego wsparcia na rzecz audytu cyberbezpieczeństwa i zgodności z przepisami. Dostępne pod adresem: https://www.enisa.europa.eu/publications/nis-investments-2023.

podstawie udanych inicjatyw, takich jak unijne bony na innowacje, **państwa członkowskie powinny rozważyć wprowadzenie ukierunkowanych rozwiązań, takich jak bony cyberbezpieczeństwa dla mikroszpitali oraz małych i średnich szpitali oraz innych świadczeniodawców**. Bony te zapewniłyby pomoc finansową na wprowadzenie konkretnych środków w zakresie cyberbezpieczeństwa. Priorytety w zakresie przydzielania bonów powinny być ustalane na podstawie wyników testów gotowości i ocen dojrzałości.

Lokalna wiedza i kontekst mają kluczowe znaczenie dla skutecznego wdrażania bonów lub innych programów wsparcia, ponieważ zapewniają adekwatność i dostępność. Fundusze UE, takie jak Europejski Fundusz Rozwoju Regionalnego, wspierają już aktywnie inicjatywy w zakresie cyberbezpieczeństwa i e-zdrowia, a zatem mogłyby służyć za narzędzie opracowywania ukierunkowanych systemów bonów na cyberbezpieczeństwo dla świadczeniodawców. Centrum Wsparcia, we współpracy z państwami członkowskimi i regionalnymi organami odpowiedzialnymi za programy, wspierałoby rozwój regionalnych systemów bonów, opierając się na doświadczeniach z dotychczasowych projektów krajowych oraz działań finansowanych w ramach programu „Cyfrowa Europa". Taki model współpracy miałby na celu zapewnienie praktycznej i efektywnej realizacji tych inicjatyw.

Ponadto od 2014 r. programy „Horyzont" odgrywają kluczową rolę w finansowaniu licznych inicjatyw badawczych ukierunkowanych na zwiększenie odporności instytucji opieki zdrowotnej, takich jak szpitale, na cyberzagrożenia oraz ograniczenie ryzyka związanego z niewłaściwym wykorzystaniem nowo pojawiających się technologii. Rezultaty tych inicjatyw obejmują szeroki wachlarz specjalistycznych narzędzi, ram i systemów, takich jak narzędzia oceny ryzyka, platformy wymiany danych zapewniające ochronę prywatności, rozwiązania kryptograficzne, programy szkoleniowe zwiększające świadomość w zakresie cyberbezpieczeństwa oraz systemy umożliwiające wykrywanie zagrożeń w czasie rzeczywistym. Co ważne, rozwiązania te zostały rygorystycznie zweryfikowane za pomocą rzeczywistych wdrożeń pilotażowych w środowiskach opieki zdrowotnej, co gwarantuje ich skuteczność i praktyczne zastosowanie w ochronie przed cyberzagrożeniami.

Zabezpieczenie łańcuchów dostaw w obszarze opieki zdrowotnej

Zarządzanie złożonymi łańcuchami dostaw ICT stanowi jedno z kluczowych wyzwań dla organizacji opieki zdrowotnej. Łańcuchy te obejmują szeroką gamę produktów, w tym podłączone do internetu wyroby medyczne, systemy elektronicznej dokumentacji medycznej i biurowy sprzęt komputerowy. Działalność szpitali i świadczeniodawców wymaga niezawodnych i bezpiecznych systemów oraz usług ICT. Aby sprostać wyzwaniom związanym z cyberbezpieczeństwem w sektorze zdrowia, Grupa Współpracy NIS powinna przeprowadzić **skoordynowaną ocenę ryzyka w zakresie bezpieczeństwa, która pozwoli ocenić zarówno techniczne, jak i strategiczne zagrożenia związane z łańcuchami dostaw wyrobów medycznych, oraz zaproponować środki ograniczające ryzyko**[31]**.** W stosownych

[31] Na podstawie art. 22 dyrektywy NIS 2.

przypadkach Grupa Współpracy NIS powinna współpracować z Grupą Koordynacyjną ds. Wyrobów Medycznych.

Akt dotyczący cyberodporności to nowe, kompleksowe ramy, które określają wymagania w zakresie cyberbezpieczeństwa na każdym etapie łańcucha wartości prawie każdego sprzętu i oprogramowania. Wymagania te obejmują planowanie, projektowanie, rozwój oraz reagowanie na aktywne wykorzystywanie podatności, a także wprowadzanie poprawek i zgłaszanie takich zagrożeń[32]. Wyroby medyczne to rodzaj produktów wykorzystywanych w jednym z najbardziej wrażliwych obszarów naszego społeczeństwa. Wymagania w zakresie cyberbezpieczeństwa dotyczące tych produktów wynikają z istniejącego rozporządzenia w sprawie wyrobów medycznych oraz rozporządzenia w sprawie wyrobów medycznych do diagnostyki *in vitro*[33]. W ramach trwającej oceny tych rozporządzeń analizowany jest potencjał większej spójności i synergii między obowiązującymi ramami, co ma zagwarantować uproszczenie wymagań oraz zgodność wdrażanych rozwiązań w zakresie cyberbezpieczeństwa z najnowszymi normami i technologiami.

Dodatkowo wyniki oceny ryzyka powinny wspierać organizacje opieki zdrowotnej w analizie ich praktyk związanych z cyberbezpieczeństwem w łańcuchu dostaw zgodnie z wymogami dyrektywy NIS 2 i mogłyby także posłużyć za podstawę do opracowania nowych **wytycznych dotyczących zamówień publicznych**[34]. Wytyczne te, opracowane przez ENISA za pośrednictwem Centrum Wsparcia, powinny odzwierciedlać najnowsze tendencje, takie jak przechowywanie danych pacjentów w chmurze, w tym potrzebę bezpiecznej migracji elektronicznych danych dotyczących zdrowia do środowiska chmury obliczeniowej. Ponadto nowe wytyczne powinny dostarczać organizacjom praktycznych narzędzi do monitorowania ich łańcuchów dostaw, z uwzględnieniem dostawców usług zarządzanych w zakresie bezpieczeństwa, sprawozdań z atestacji lub ocen ryzyka przeprowadzanych przez osoby trzecie.

W kontekście chmury niezbędne są dalsze działania, aby sprostać wyjątkowym wyzwaniom związanym z zarządzaniem wrażliwymi danymi dotyczącymi opieki zdrowotnej, w tym w zakresie zwiększania bezpieczeństwa, ochrony prywatności i ograniczania ryzyka operacyjnego. Aby wzmocnić zabezpieczenia, eksperci zalecają włączenie do usług w chmurze zasady „uwzględniania bezpieczeństwa w sposób domyślny i już na etapie projektowania". To podejście koncentruje się na zapewnieniu bezpiecznej infrastruktury, proaktywnym zarządzaniu podatnościami oraz integracji rządowych i prywatnych rozwiązań w chmurze. Również stałe monitorowanie oraz certyfikacja dostawców, obejmująca certyfikaty bezpieczeństwa i audyty zgodności z normami krajowymi i międzynarodowymi, odgrywają kluczową rolę w utrzymaniu solidnych praktyk w zakresie bezpieczeństwa.

[32] Na pierwszym etapie, od dnia 1 sierpnia 2025 r., szerokie kategorie urządzeń radiowych, nieobjęte zakresem rozporządzenia w sprawie wyrobów medycznych i rozporządzenia w sprawie wyrobów medycznych do diagnostyki *in vitro*, będą musiały spełniać zasadnicze wymagania dyrektywy w sprawie urządzeń radiowych dotyczące cyberbezpieczeństwa, gdy będą wprowadzane na jednolity rynek. Na drugim etapie, od dnia 11 grudnia 2027 r., wejdzie w życie akt dotyczący cyberodporności.

[33] W grudniu 2019 r. Grupa Koordynacyjna ds. Wyrobów Medycznych wydała wytyczne dotyczące cyberbezpieczeństwa wyrobów medycznych, wspierające producentów w spełnianiu wymagań określonych w załączniku I do obu tych rozporządzeń: https://ec.europa.eu/docsroom/documents/41863?locale=pl.

[34] Na podstawie wytycznych ENISA z 2020 r. w sprawie zamówień publicznych dotyczących cyberbezpieczeństwa w szpitalach (luty 2020 r.). Dostępne pod adresem: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

W przypadku usług takich jak infrastruktura jako usługa (IaaS), platforma jako usługa (PaaS) i oprogramowanie jako usługa (SaaS) wdrożenie praktyk w zakresie bezpieczeństwa często spoczywa na kliencie. Wiele organizacji opieki zdrowotnej nie dysponuje jednak środkami umożliwiającymi samodzielne spełnienie tych wymagań. Aby rozwiązać ten problem, **należy zachęcać dostawców usług w chmurze do wdrażania podstawowych środków bezpieczeństwa jako standardowej funkcji**. Takie środki ograniczyłyby ryzyko błędnej konfiguracji, zapewniłyby spójną ochronę we wszystkich środowiskach zarządzanych przez klienta oraz zwiększyłyby zaufanie użytkowników. Wprowadzenie domyślnego podstawowego poziomu bezpieczeństwa pozwoliłoby połączyć skuteczną ochronę z praktycznym zastosowaniem, czyniąc go odpowiednim dla różnych organizacji opieki zdrowotnej. Te działania wymagałyby bliskiej współpracy między dostawcami usług w chmurze a sektorem zdrowia oraz wykorzystania najlepszych praktyk branżowych do opracowania skutecznych i skalowalnych rozwiązań.

Szkolenia i rozwój umiejętności

Dysponowanie siłą roboczą posiadającą najbardziej pożądane umiejętności jest kluczowe dla długoterminowego, zrównoważonego wzrostu i konkurencyjności Europy, a także dla zapewnienia wysokiej jakości usług, w tym opieki zdrowotnej. Niedobór wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa stanowi poważne wyzwanie w całej Europie. Szacuje się, że aby zaspokoić potrzeby rynku pracy w UE, brakuje około 299 000 specjalistów w dziedzinie cyberbezpieczeństwa[35]. Według badania Eurobarometr dotyczącego umiejętności w dziedzinie cyberbezpieczeństwa z 2024 r.[36] 81 % przedsiębiorstw postrzega trudności w zatrudnianiu specjalistów w dziedzinie cyberbezpieczeństwa jako jedno z głównych zagrożeń w kontekście potencjalnych cyberataków. W sektorach edukacji, zdrowia i pomocy społecznej 66 % stanowisk związanych z cyberbezpieczeństwem jest obsadzanych przez pracowników, którzy przechodzą z innych ról, co uwypukla pilną potrzebę przekwalifikowania i podnoszenia kwalifikacji w tej dziedzinie.

Aby sprostać temu wyzwaniu, Centrum Wsparcia powinno współpracować z przyszłym konsorcjum na rzecz europejskiej infrastruktury cyfrowej (EDIC) dla umiejętności w dziedzinie cyberbezpieczeństwa, przewidzianym w komunikacie Komisji w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa[37]. Te działania powinny ułatwiać wymianę między specjalistami ds. cyberbezpieczeństwa w sektorze zdrowia, takimi jak główni inspektorzy ds. bezpieczeństwa informacji. Jednym z potencjalnych działań byłoby utworzenie **europejskiej sieci głównych inspektorów ds. bezpieczeństwa informacji w dziedzinie zdrowia**, począwszy od powołania zespołu ekspertów, którzy skupiliby się na wymianie i opracowaniu najlepszych praktyk, strategii zatrzymywania talentów oraz tworzeniu rozwiązań mających na celu przyciągnięcie specjalistów

[35] The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study [Krajobraz cyberbezpieczeństwa w 2024 r.: wnioski z badania ISC2 dotyczącego pracowników ds. cyberbezpieczeństwa] | Platforma na rzecz umiejętności cyfrowych i zatrudnienia.

[36] Badanie Eurobarometr Flash 547 dotyczące umiejętności w dziedzinie cyberbezpieczeństwa.

[37] Komunikat Komisji do Parlamentu Europejskiego i Rady: Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE („Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa"). COM(2023) 207 final.

w dziedzinie cyberbezpieczeństwa do sektora zdrowia. Ponadto w ramach Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa należy opracować zasoby w celu zwiększenia liczby pracowników w dziedzinie cyberbezpieczeństwa w sektorze zdrowia przy wsparciu ze strony sektora i środowiska akademickiego. W związku z tym należy zachęcać zainteresowane strony z sektora do zadeklarowania wsparcia na rzecz ulepszania szkoleń w dziedzinie cyberbezpieczeństwa.

Istotnym czynnikiem przyczyniającym się do cyberincydentów w opiece zdrowotnej jest nadal błąd ludzki, co wskazuje na pilną potrzebę kompleksowego szkolenia pracowników oraz zwiększenia ich świadomości w zakresie cyberbezpieczeństwa. W kontekście powszechnego korzystania z narzędzi cyfrowych przez pracowników służby zdrowia niezbędne jest zapewnienie im wiedzy na temat bezpiecznych praktyk. Ukierunkowane szkolenia oraz kampanie uświadamiające mogą znacząco obniżyć ryzyko związane z cyberzagrożeniami. Aby zająć się tym problemem, Centrum Wsparcia powinno współpracować z pracownikami służby zdrowia i świadczeniodawcami oraz z organizatorami kształcenia lub szkolenia, sektorem, EDIC dla umiejętności w dziedzinie cyberbezpieczeństwa, a także z organami państw członkowskich w celu tworzenia i rozpowszechniania **kompleksowych, łatwo dostępnych internetowych modułów szkoleniowych i kursów**.

Włączenie modułów kompetencji cyfrowych i cyberbezpieczeństwa do programów nauczania ma kluczowe znaczenie dla budowania solidnych podstaw cyberbezpieczeństwa w opiece zdrowotnej. Moduły te powinny dotyczyć kwestii specyficznych dla danego sektora, takich jak ochrona danych pacjentów oraz podatności w zakresie bezpieczeństwa wyrobów medycznych. Przy opracowywaniu tych zasobów należy uwzględnić wcześniejsze działania, takie jak projekt BeWell finansowany w ramach programu Erasmus+[38] oraz projekt PANACEA finansowany w ramach programu „Horyzont 2020”[39].

3.2.Europejskie zdolności w zakresie wykrywania cyberzagrożeń dla sektora zdrowia

Skuteczne wykrywanie cyberzagrożeń ma zasadnicze znaczenie dla szybkiego reagowania na incydenty. Podmioty stwarzające zagrożenie mogą stosować techniki mające na celu utrudnienie wykrywania włamań, co umożliwia im utrzymanie niedozwolonego dostępu do systemu przez dłuższy czas[40]. W związku z tym rozwój lepszych zdolności w zakresie wykrywania zagrożeń może skutecznie powstrzymać cyberataki na ich wczesnym etapie. Przykładem może być atak z użyciem oprogramowania szantażującego wymierzony w fińskiego dostawcę usług psychoterapeutycznych Vastaamo. Podczas ataku sprawca domagał się okupu od pacjentów, których poufna dokumentacja

[38] BeWell – Sojusz na rzecz przyszłej strategii na rzecz pracowników służby zdrowia w zakresie umiejętności cyfrowych i ekologicznych. Dostępne pod adresem: https://bewell-project.eu/.
[39] PANACEA – Ochrona i prywatność infrastruktury szpitali i placówek opieki zdrowotnej dzięki inteligentnemu systemowi cyberbezpieczeństwa i zestawowi narzędzi do walki z cyberzagrożeniami w odniesieniu do danych i osób. Dostępne pod adresem: https://cordis.europa.eu/project/id/826293/pl.
[40] ENISA Health Threat Landscape 2023 [Sprawozdanie ENISA dotyczące krajobrazu zagrożeń w sektorze zdrowia z 2023 r.].

medyczna została skradziona. Włamanie miało miejsce w 2018 r., ale dostawca dowiedział się o nim dopiero w 2020 r.[41]

Skuteczna wymiana informacji i współpraca mają zasadnicze znaczenie dla poprawy wykrywania zagrożeń i orientacji sytuacyjnej w całej UE. Zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) odgrywają kluczową rolę w przyjmowaniu zgłoszeń incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa i potencjalnych zagrożeń, a także dostarczają wytycznych dotyczących środków łagodzących na poziomie krajowym. Zdecydowanie zachęca się jednak **państwa członkowskie do przekazywania Centrum Wsparcia ENISA wszystkich zgłoszeń cyberincydentów, które dotyczą szpitali i świadczeniodawców, aby umożliwić orientację sytuacyjną na poziomie UE**. Wskazane byłoby, aby takim zgłoszeniom towarzyszyła szczegółowa charakterystyka różnych istotnych wymiarów incydentów, w tym znanych podatności, skutków dla usług opieki zdrowotnej oraz zdarzeń niepożądanych wpływających na pacjentów. Ponadto zachęca się producentów wyrobów medycznych i wyrobów do diagnostyki *in vitro* do dobrowolnego przesyłania zgłoszeń, za pośrednictwem pojedynczej platformy sprawozdawczej, która ma zostać ustanowiona i którą ma zarządzać ENISA w ramach aktu o cyberodporności. Zgłoszenia te powinny dotyczyć aktywnie wykorzystywanych podatności, poważnych cyberincydentów mających wpływ na bezpieczeństwo tych wyrobów, a także ewentualnych innych podatności, incydentów, potencjalnych zdarzeń dla cyberbezpieczeństwa lub cyberzagrożeń, które mogą wpłynąć na profil ryzyka tych wyrobów.

Gdy informacje zawarte w zgłoszeniach nie będą już wrażliwe, Centrum Wsparcia mogłoby opracować finansowany przez ENISA europejski katalog znanych wykorzystywanych podatności obejmujący wyroby medyczne, systemy elektronicznej dokumentacji medycznej oraz dostawców sprzętu ICT i oprogramowania w dziedzinie zdrowia. Aby sprostać poważnym wyzwaniom związanym z wykrywaniem zagrożeń, Centrum Wsparcia powinno wprowadzić **ogólnounijną usługę abonamentową w zakresie wczesnego ostrzegania dla sektora zdrowia, zapewniającą ostrzeżenia w czasie zbliżonym do rzeczywistego**. Usługa ta opierałaby się na danych pozyskanych od CSIRT, podmiotów opieki zdrowotnej i producentów, a także na informacjach uzyskanych za pomocą wywiadu ze źródeł jawnych (OSINT) oraz od innych odpowiednich podmiotów, takich jak centra cyberbezpieczeństwa, ośrodki wymiany i analizy informacji oraz organy ścigania. Wzmocniona współpraca między ENISA a Agencją Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) – na przykład w zakresie wzorców cyberprzestępczości ukierunkowanej na sektor zdrowia, mogłaby jeszcze bardziej poprawić orientację sytuacyjną.

Ośrodki wymiany i analizy informacji pełnią funkcję centralnych zasobów na potrzeby analizy cyberzagrożeń, umożliwiają dwukierunkową wymianę informacji między sektorem publicznym i prywatnym oraz wspierają proces budowania zaufania. Centrum Wsparcia powinno zwiększyć wsparcie dla **europejskiego ośrodka wymiany i analizy informacji w dziedzinie zdrowia**, oferując narzędzia i wymianę informacji, sektorowe sprawozdania na temat orientacji sytuacyjnej oraz wspierając zaufaną społeczność, która będzie współpracować zarówno na poziomie taktycznym, jak

[41] Decyzja nr 1150/161/2021 fińskiego Rzecznika Ochrony Danych.

i strategicznym. Państwa członkowskie powinny zachęcać do rozwoju krajowych ośrodków wymiany i analizy informacji w dziedzinie zdrowia[42]. Ośrodki wymiany i analizy informacji w dziedzinie zdrowia powinny być również zachęcane do zapewniania możliwości kontaktów świadczeniodawców opieki zdrowotnej z producentami, aby mogli oni wypracować wspólne zrozumienie zagrożeń cyberbezpieczeństwa, w tym w łańcuchu dostaw, oraz ułatwiania dialogu na temat bezpiecznego projektowania produktów, które uwzględniają realia wdrażania w terenie.

3.3.Szybkie reagowanie i przywracanie sprawności operacyjnej

Biorąc pod uwagę wysoką wrażliwość danych dotyczących zdrowia pacjentów oraz potencjalnie niszczycielskie skutki cyberataków dla usług opieki zdrowotnej, szybka i skuteczna reakcja na cyberincydenty jest kluczowa dla zapewnienia bezpieczeństwa pacjentów. W przypadku cyberataku na szpital lub świadczeniodawcę pierwszym punktem kontaktowym jest odpowiedni krajowy CSIRT[43]. CSIRT odpowiada za terminowe udzielanie wsparcia, najlepiej w ciągu 24 godzin, i pomaga w zarządzaniu poważnymi incydentami. Jeżeli jednak incydent przekroczy zdolności danego CSIRT, powinno być dostępne wsparcie ze strony UE, aby zapewnić szybką i skuteczną reakcję.

Rezerwa cyberbezpieczeństwa UE, ustanowiona na mocy aktu w sprawie cybersolidarności, oferuje usługi reagowania na incydenty, świadczone przez zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa, w celu zapewnienia wsparcia w przypadku poważnych cyberincydentów lub cyberincydentów na dużą skalę oraz przy podejmowaniu początkowych działań służących usunięciu skutków incydentu. Rezerwa ma uzupełniać działania CSIRT państw członkowskich poprzez umożliwienie im zwrócenia się o dodatkowe wsparcie w przypadkach dotyczących sektorów krytycznych, takich jak sektor zdrowia. Aby wzmocnić ten system, **Komisja i ENISA powinny zadbać o to, by rezerwa obejmowała usługę szybkiego reagowania przeznaczoną specjalnie dla sektora zdrowia.** W uzupełnieniu do innych istniejących ram usługa ta polegałaby na bezzwłocznym oddelegowaniu ekspertów do zarządzania poważnymi cyberincydentami lub cyberincydentami na dużą skalę w opiece zdrowotnej, gdy wsparcie krajowe byłoby niewystarczające.

Aby usprawnić reagowanie i przywracanie sprawności operacyjnej, Centrum Wsparcia, we współpracy z Grupą Współpracy NIS, siecią CSIRT oraz, w stosownych przypadkach, z Europolem, powinno opracować **podręczniki reagowania na cyberincydenty dostosowane do potrzeb opieki zdrowotnej**. Podręczniki te byłyby pomocne zarówno dla CSIRT, jak i dla organizacji opieki zdrowotnej w reagowaniu na konkretne cyberzagrożenia, w tym na oprogramowanie szantażujące. Biorąc pod uwagę kluczową rolę skutecznej współpracy między CSIRT a organami ścigania w reagowaniu na

[42] Na przykład Finlandia ustanowiła krajowy ośrodek wymiany i analizy informacji w odniesieniu do sektorów opieki społecznej i opieki zdrowotnej. Zob. dokument fińskiego Krajowego Centrum ds. Cyberbezpieczeństwa pt. „Grupy wymiany informacji w ramach ośrodka wymiany i analizy informacji", dostępny pod adresem: https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] Art. 23 ust. 1 dyrektywy NIS 2 nakłada na podmioty kluczowe i ważne wymóg zgłaszania poważnych incydentów odpowiedniemu CSIRT lub, w stosownych przypadkach, właściwemu organowi.

cyberincydenty o charakterze przestępczym i w prowadzeniu dochodzeń, podręczniki te powinny zawierać m.in. precyzyjne wytyczne dotyczące zgłaszania takich incydentów organom ścigania. Ponadto Centrum Wsparcia mogłoby **wspierać szeroko zakrojone wdrażanie krajowych ćwiczeń w dziedzinie cyberbezpieczeństwa, bazując na doświadczeniach z takich inicjatyw jak ćwiczenia ENISA „Cyber Europe 2022", w celu przetestowania opracowanych podręczników oraz udoskonalenia protokołów reagowania na incydenty.**

Aby dostarczyć informacji na potrzeby polityki oraz ocenić skuteczność środków mających na celu przeciwdziałanie atakom z użyciem oprogramowania szantażującego, niezbędne jest gromadzenie dodatkowych danych. W tym celu państwa członkowskie powinny zobowiązać podmioty objęte dyrektywą NIS 2, w tym organizacje opieki zdrowotnej, do zgłaszania wszelkich dokonanych oraz planowanych płatności z tytułu okupu, wraz z innymi informacjami, które przekazują przy zgłaszaniu poważnych cyberincydentów. Tego typu zgłoszenia wspierają skuteczne śledztwa w sprawie incydentów związanych z oprogramowaniem szantażującym, w tym monitorowanie płatności na platformach wymiany kryptowalut w celu identyfikacji odbiorców.

Szybkość przywracania sprawności operacyjnej jest kluczowa dla utrzymania odporności i zaufania publicznego, zwłaszcza w opiece zdrowotnej, gdzie przestoje mogą zakłócić opiekę nad pacjentami. Aby skutecznie przywrócić sprawność operacyjną po atakach z użyciem oprogramowania szantażującego, świadczeniodawcy muszą dysponować bezpiecznymi, aktualnymi i odosobnionymi kopiami zapasowymi danych, które w razie potrzeby mogą zostać szybko odzyskane. W ramach katalogu usług Centrum Wsparcia mogłaby zostać wprowadzona **usługa abonamentowa w zakresie przywracania sprawności operacyjnej po ataku z użyciem oprogramowania szantażującego, która pomogłaby szpitalom i świadczeniodawcom w przygotowaniu z wyprzedzeniem odpowiednich planów awaryjnych**. ENISA i Europol powinny współpracować w celu określenia najpowszechniejszych odmian oprogramowania szantażującego atakującego organizacje opieki zdrowotnej oraz **rozbudować repozytorium narzędzi deszyfrujących** dostępnych w ramach projektu „No More Ransom"[44]. Powinny również opracować i rozpowszechnić łatwo dostępne wytyczne, które pomogą świadczeniodawcom unikać płacenia okupu dzięki stosowaniu narzędzi deszyfrujących.

Międzynarodowa inicjatywa na rzecz walki z oprogramowaniem szantażującym[45] jest wartościową platformą wymiany informacji na temat konkretnych incydentów związanych z oprogramowaniem szantażującym, a także budowania zdolności państw członkowskich w zakresie wzmacniania ich ram cyberbezpieczeństwa oraz zdolności dochodzeniowych w walce z podmiotami dokonującymi ataków z użyciem oprogramowania szantażującego. Komisja, we współpracy z wysokim przedstawicielem, będzie kontynuować rozwój współpracy w ramach inicjatywy na rzecz walki z oprogramowaniem szantażującym, w tym w zakresie zagrożeń dla sektora zdrowia związanych z oprogramowaniem szantażującym. Ponadto Komisja będzie dążyć do współpracy w ramach **grupy roboczej G-7 ds. cyberbezpieczeństwa**, aby wzmocnić cyberbezpieczeństwo sektora zdrowia. W szczególności grupa robocza mogłaby rozważyć możliwości wsparcia sektora zdrowia w walce z zagrożeniami, takimi jak

[44] https://www.nomoreransom.org/pl/index.html.
[45] https://www.counter-ransomware.org/.

oprogramowanie szantażujące, w oparciu o wnioski zawarte we wspólnym oświadczeniu w sprawie ataków z użyciem oprogramowania szantażującego na placówki opieki zdrowotnej z dnia 8 listopada 2024 r., przedstawionym w kontekście Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych[46].

4. Działania krajowe

Zdolność niniejszego planu działania do poprawy cyberbezpieczeństwa w sektorze zdrowia zależy od aktywnego zaangażowania państw członkowskich. Aby skutecznie wdrożyć niniejszy plan działania, państwa członkowskie mogłyby wyznaczyć **krajowe centra wsparcia cyberbezpieczeństwa** specjalnie dla szpitali i świadczeniodawców. Centra pełniłyby funkcję głównych punktów kontaktowych dla sektora zdrowia na szczeblu krajowym, w ścisłej współpracy z Centrum Wsparcia ENISA. W miarę możliwości i w stosownych przypadkach państwa członkowskie powinny wyznaczyć istniejące organy, takie jak krajowe CSIRT w sektorze zdrowia lub inne odpowiednie instytucje, na krajowe centra wsparcia w dziedzinie cyberbezpieczeństwa.

Państwa członkowskie zachęca się również do opracowania **krajowych planów działania, które będą koncentrować się na cyberbezpieczeństwie w sektorze zdrowia**. Plany powinny uwzględniać konkretne zagrożenia dla cyberbezpieczeństwa, na jakie narażone są systemy opieki zdrowotnej, oraz działania podejmowane na poziomie krajowym w celu ich wyeliminowania, przy jednoczesnym zapewnieniu skutecznego wykorzystania zasobów i praktyk na poziomie europejskim. Centrum Wsparcia ENISA może pomóc w opracowaniu tych planów, biorąc pod uwagę już istniejące plany krajowe i koordynując wysiłki w celu zapewnienia wzajemnego uzupełniania się zasobów oraz strategii poszczególnych państw członkowskich.

Kolejnym kluczowym celem państw członkowskich jest ułatwienie dzielenia się zasobami między świadczeniodawcami, co można osiągnąć poprzez **wspólne udzielanie zamówień lub łączenie zasobów** na poziomie krajowym, regionalnym, a nawet europejskim. Takie podejście zmniejszyłoby obciążenie finansowe poszczególnych podmiotów, a jednocześnie zwiększyłoby ich siłę przetargową w stosunku do dostawców usług cyberbezpieczeństwa.

Przykładem jest francuski program CaRE[47], w ramach którego wprowadzono na poziomie krajowym i regionalnym szereg środków mających na celu sprostanie wyzwaniom związanym z pozyskiwaniem zasobów. Program ten obejmuje katalog cyberbezpieczeństwa zawierający przegląd rozwiązań i pakietów cybernetycznych udostępnianych szpitalom za pośrednictwem krajowej agencji ds. cyberbezpieczeństwa, agencji ds. e-zdrowia, agencji regionalnych i krajowych organizacji

[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.
[47] Francuska Agencja ds. E-Zdrowia: Cybersécurité acceleration et Résilience des Établissements (CaRE). Dostępne pod adresem: https://esante.gouv.fr/strategie-nationale/cybersecurite.

zakupowych. Katalog obejmuje również rozwiązania komercyjne. Dodatkowo agencje regionalne otrzymują dodatkowe finansowanie w celu oferowania wspólnych zasobów.

Państwa członkowskie powinny również zająć się problemem niewystarczających inwestycji w cyberbezpieczeństwo w sektorze zdrowia. Aby zapewnić odpowiednie finansowanie, powinny one ustanowić **niewiążące poziomy odniesienia oraz monitorować cele w zakresie finansowania ukierunkowane konkretnie na cyberbezpieczeństwo**, dbając jednocześnie o to, aby inwestycje te nie wpływały negatywnie na jakość podstawowej opieki nad pacjentami. Te cele w zakresie finansowania powinny również obejmować uwzględnienie kwestii bezpieczeństwa we wszystkich inwestycjach cyfrowych w sektorze. Państwa członkowskie mogą wymieniać się najlepszymi praktykami i wskazówkami dotyczącymi tych celów za pośrednictwem platform takich jak sieć e-zdrowie[48].

5. Współpraca publiczno-prywatna

Współpraca publiczno-prywatna oraz konsultacje ze świadczeniodawcami, z innymi podmiotami sektora opieki zdrowotnej, a także z odpowiednimi podmiotami sektora cyberbezpieczeństwa mają zasadnicze znaczenie dla pomyślnej realizacji planu działania. Aby wspierać prace Centrum Wsparcia, **Komisja, we współpracy z ENISA, ustanowi wspólną Radę Konsultacyjną ds. Cyberbezpieczeństwa w dziedzinie Zdrowia**. Rada ta, składająca się z przedstawicieli wysokiego szczebla z obu dziedzin – opieki zdrowotnej i cyberbezpieczeństwa – będzie mogła doradzać Komisji oraz Centrum Wsparcia w zakresie skutecznych działań, a także omawiać dalszy rozwój partnerstw publiczno-prywatnych w tej dziedzinie. Rada będzie bazować na dotychczasowych działaniach związanych z partnerstwami publiczno-prywatnymi, w tym na inicjatywach takich jak europejski ośrodek wymiany i analizy informacji w dziedzinie zdrowia.

Ponadto Komisja ogłosi **wezwanie do działania** skierowane do przedsiębiorstw specjalizujących się w cyberbezpieczeństwie, fundacji, instytucji edukacyjnych i zainteresowanych stron z branży, aby **zobowiązały się one do podjęcia działań mających na celu sprostanie wyzwaniom w sektorze zdrowia**. W oparciu o doświadczenia Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa takie zobowiązania mogłyby obejmować na przykład oferowanie szkoleń i materiałów edukacyjnych dla specjalistów w dziedzinie cyberbezpieczeństwa, dostosowanych do specyfiki sektora zdrowia[49]. Inne zobowiązania mogą obejmować działania informacyjne lub świadczenie usług zarządzanych w zakresie bezpieczeństwa dla podmiotów szczególnie wrażliwych, bezpłatnie lub w obniżonych cenach, aby zwiększyć ich gotowość i odporność na cyberzagrożenia. Ponadto zobowiązania mogłyby obejmować wymianę danych dotyczących analizy cyberzagrożeń z Centrum Wsparcia ENISA. Centrum Wsparcia powinno regularnie dokonywać przeglądu zobowiązań podjętych w ramach wezwania do działania, aby zapewnić ich spójność i komplementarność

[48] Sieć e-zdrowie jest dobrowolną siecią organów krajowych odpowiedzialnych za e-zdrowie i wyznaczonych przez państwa członkowskie, którą utworzono na podstawie art. 14 dyrektywy 2011/24/UE.

[49] Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa: Zaangażuj się | Platforma na rzecz umiejętności cyfrowych i zatrudnienia.

6. Zniechęcanie podmiotów powodujących cyberzagrożenia

Polityka UE w zakresie cyberbezpieczeństwa, zarówno wewnętrzna, jak i zewnętrzna, powinna przyczyniać się do realizacji celu, jakim jest zniechęcenie podmiotów powodujących cyberzagrożenia do ataków na europejskie systemy opieki zdrowotnej. Cyberataki na organizacje opieki zdrowotnej są szczególnie niepożądanym rodzajem szkodliwych działań w cyberprzestrzeni, ponieważ mogą zagrażać bezpieczeństwu pacjentów i życiu ludzkiemu. Dlatego UE powinna w pełni wykorzystać swoje zdolności odstraszające w dziedzinie cyberbezpieczeństwa oraz narzędzia egzekwowania prawa, aby ograniczyć możliwości działania cyberprzestępców zagrażających sektorowi zdrowia i pozbawić ich łatwych zysków. Działania w tym zakresie mogą obejmować wspieranie dochodzeń transgranicznych, polegające na sprawniejszej wymianie wskaźników dotyczących oznak naruszenia integralności systemu oraz innych istotnych danych, a także skoncentrowanie się na celach o wysokiej wartości i kluczowych usługach ułatwiających działalność przestępczą, takich jak *bulletproof hosting* lub usługi mieszania kryptowalut.

Zestaw narzędzi dla dyplomacji cyfrowej oferuje ramy zapobiegania cyberatakom na UE, państwa członkowskie i partnerów, a także ich powstrzymywania i reagowania na nie. Wysoki przedstawiciel nadal będzie stosować istniejące ramy sankcji cybernetycznych w odpowiedzi na zagrożenia wymierzone w systemy opieki zdrowotnej.

Pociąganie cyberprzestępców do odpowiedzialności odgrywa kluczową rolę w odstraszaniu potencjalnych sprawców. Dlatego państwa członkowskie powinny w swoich krajowych planach działania w pełni uwzględnić egzekwowanie prawa. Szczególnie istotne jest skuteczne wykorzystanie przepisów dyrektywy dotyczącej ataków na systemy informatyczne[50] oraz budapesztańskiej konwencji Rady Europy o cyberprzestępczości, aby powstrzymywać ataki, ścigać sprawców oraz eliminować infrastrukturę przestępczą ułatwiającą ataki[51]. Skuteczne wdrożenie tych narzędzi powinno zagwarantować, że przestępcze i szkodliwe działania wymierzone w sektor opieki zdrowotnej będą odpowiednio karane.

7. Wdrażanie i monitorowanie planu działania

Plan działania przewiduje szereg zadań związanych z utworzeniem Centrum Wsparcia w ramach ENISA. Takie podejście zapewnia całościową i spójną realizację założeń, a jednocześnie eliminuje konieczność tworzenia nowych podmiotów, co mogłoby prowadzić do nakładania się obszarów kompetencji i dodatkowych kosztów. Komisja zamierza zagwarantować Centrum Wsparcia odpowiednie zasoby.

Po jego uruchomieniu ENISA, w porozumieniu z Komisją, powinna regularnie informować zarząd ENISA o postępach, a także przekazywać aktualizacje odpowiednim sieciom państw członkowskich, w szczególności Grupie Współpracy NIS, sieci CSIRT, sieci e-zdrowie oraz, w stosownych

[50] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW: https://eur-lex.europa.eu/eli/dir/2013/40/oj.
[51] Konwencja o cyberprzestępczości (konwencja budapesztańska, ETS nr 185) i protokoły do niej: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

przypadkach, Radzie ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia. Ponadto ENISA powinna prowadzić stałą wymianę informacji z publiczno-prywatną Radą Konsultacyjną ds. Cyberbezpieczeństwa w dziedzinie Zdrowia na temat działań realizowanych przez Centrum Wsparcia.

Regularne sprawozdania ENISA – takie jak sprawozdanie o stanie cyberbezpieczeństwa w Unii, które zawiera zbiorczą ocenę poziomu dojrzałości zdolności i zasobów w zakresie cyberbezpieczeństwa w całej UE, w tym w sektorze zdrowia– powinny również służyć do publikowania danych wspierających monitorowanie realizacji planu działania. Ponadto unijny indeks cyberbezpieczeństwa ENISA[52] może dostarczać zarówno ilościowych, jak i jakościowych danych, oraz służyć jako podstawa do oceny krytyczności i dojrzałości sektora zdrowia.

8. Dalsze działania

W niniejszym komunikacie przedstawiono ambitny program na rzecz zwiększenia cyberbezpieczeństwa w sektorze zdrowia w UE. Plan działania zawiera propozycję utworzenia Centrum Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej w ramach ENISA i tym samym wyznacza drogę do spójnego i wspólnego europejskiego podejścia do wyzwań związanych z cyberbezpieczeństwem w sektorze.

Niniejszy komunikat należy postrzegać jako początek procesu poprawy cyberbezpieczeństwa w sektorze zdrowia. Przyjęcie planu działania będzie się wiązać z rozpoczęciem kompleksowych konsultacji z zainteresowanymi stronami oraz dalszą wymianą informacji z państwami członkowskimi i odpowiednimi sieciami, aby zebrać cenne spostrzeżenia. Na podstawie wyników konsultacji Komisja zamierza przedstawić w czwartym kwartale 2025 r. zalecenia dotyczące dalszego udoskonalenia planu działania.

Komisja wzywa państwa członkowskie i wszystkie zainteresowane strony do współpracy na rzecz realizacji ambitnych celów tego planu.

[52] ENISA, EU Cybersecurity Index, Framework and Methodological Note [ENISA, unijny indeks cyberbezpieczeństwa, ramy i nota dotycząca metodyki] (2024). Dostępne pod adresem: https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

ZAŁĄCZNIK – Zestawienie proponowanych działań

Komisja:

Centrum Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej w ramach ENISA	
Zapewnienie odpowiednich zasobów dla Centrum Wsparcia Cyberbezpieczeństwa Współpraca z ECCC w celu uruchomienia projektów pilotażowych służących opracowaniu najlepszych praktyk w zakresie higieny cyberbezpieczeństwa i oceny ryzyka związanego z bezpieczeństwem oraz dążeniu do zaspokojenia potrzeby stałego monitorowania cyberbezpieczeństwa, rozpoznawania zagrożeń i reagowania na incydenty z wykorzystaniem najnowocześniejszych rozwiązań w tej dziedzinie. Efektem współpracy będzie opracowanie katalogu usług Europejskiego Centrum Wsparcia Cyberbezpieczeństwa	2025 r.
Zapobieganie cyberincydentom	
Zbadanie, w porozumieniu z Grupą Współpracy NIS, EU-CyCLONe i ENISA, możliwości wskazania sektora zdrowia jako sektora, któremu można udzielić wsparcia na rzecz skoordynowanego testowania gotowości na podstawie aktu w sprawie cybersolidarności	I kw. 2025 r.
Szybkie reagowanie i przywracanie sprawności operacyjnej	
Dopilnowanie wspólnie z ENISA, aby rezerwa cyberbezpieczeństwa UE obejmowała usługę szybkiego reagowania przeznaczoną specjalnie dla sektora zdrowia	IV kw. 2025 r.
Współpraca publiczno-prywatna	
Ustanowienie przy wsparciu ENISA wspólnej Rady Konsultacyjnej ds. Cyberbezpieczeństwa w dziedzinie Zdrowia	I kw. 2025 r.
Ogłoszenie wezwania do działania skierowanego do przedsiębiorstw specjalizujących się w cyberbezpieczeństwie, fundacji, instytucji edukacyjnych i zainteresowanych stron z branży, aby	II kw. 2025 r.

zobowiązały się one do podjęcia działań mających na celu sprostanie wyzwaniom w sektorze zdrowia	
Zniechęcanie podmiotów powodujących cyberzagrożenia	
We współpracy z wysokim przedstawicielem zbadanie możliwości wykorzystania zestawu narzędzi dla dyplomacji cyfrowej, który mógłby służyć zapobieganiu szkodliwym działaniom skierowanym przeciwko systemom opieki zdrowotnej. Narzędzia te powinny obejmować mechanizmy zniechęcania do takich działań, a także środki umożliwiające ich powstrzymywanie i skuteczne reagowanie na incydenty	2025 r.
Zacieśnianie współpracy międzynarodowej w walce przeciwko podmiotom dokonującym ataków z użyciem oprogramowania szantażującego, zwłaszcza w ramach międzynarodowej inicjatywy na rzecz walki z oprogramowaniem szantażującym, we współpracy z wysokim przedstawicielem	2025–2026
Dążenie do współpracy w ramach grupy roboczej G-7 ds. cyberbezpieczeństwa w celu wzmocnienia cyberbezpieczeństwa w sektorze zdrowia	2025–2026
Dalsze działania	
Rozpoczęcie kompleksowych konsultacji z zainteresowanymi stronami	I kw. 2025 r.
Przyjęcie zaleceń w sprawie dalszego dopracowania planu działania	IV kw. 2025 r.

ENISA:

Europejskie Centrum Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej	
Rozpoczęcie prac nad utworzeniem Europejskiego Centrum Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej	II kw. 2025 r.
Opracowanie kompleksowego katalogu usług, który ma być oferowany przez Centrum Wsparcia Cyberbezpieczeństwa	Od IV kw. 2025 r.

Zapobieganie cyberincydentom	
Wydanie wytycznych, w których podkreśla się najbardziej krytyczne praktyki w zakresie cyberbezpieczeństwa, oraz zapewnianie świadczeniodawcom pomocy w ich wdrażaniu	III kw. 2025 r.
Opracowanie, w ścisłej współpracy z Komisją i państwami członkowskimi, narzędzia mapowania regulacyjnego	I kw. 2025 r.
Opracowanie ram oceny dojrzałości w zakresie cyberbezpieczeństwa w odniesieniu do opieki zdrowotnej	III kw. 2025 r.
Przeprowadzanie corocznej oceny dojrzałości w zakresie cyberbezpieczeństwa w sektorze zdrowia	2025–2026
Współpraca z państwami członkowskimi i regionalnymi organami odpowiedzialnymi za programy w celu stworzenia modelowych programów bonów na cyberbezpieczeństwo	2025–2026
Opracowanie nowych wytycznych dotyczących zamówień publicznych na potrzeby cyberbezpieczeństwa szpitali i świadczeniodawców	III kw. 2025 r.
Utworzenie europejskiej sieci głównych inspektorów ds. bezpieczeństwa informacji w dziedzinie zdrowia	I kw. 2026 r.
Opracowanie i rozpropagowanie modułów szkoleniowych i kursów dla pracowników opieki zdrowotnej	I kw. 2026 r.
Europejskie zdolności w zakresie wykrywania cyberzagrożeń dla sektora zdrowia	
Stworzenie europejskiego katalogu znanych wykorzystywanych podatności w odniesieniu do wyrobów medycznych, systemów elektronicznej dokumentacji medycznej oraz dostawców sprzętu i oprogramowania ICT w dziedzinie zdrowia	IV kw. 2025 r.
Wprowadzenie ogólnounijnej usługi abonamentowej w zakresie wczesnego ostrzegania dla sektora zdrowia	Od 2026 r.
Wspieranie europejskiego ośrodka wymiany i analizy informacji w dziedzinie zdrowia za pomocą narzędzi i wymiany informacji	2025–2026

Szybkie reagowanie i przywracanie sprawności operacyjnej	
Zapewnienie, we współpracy z Komisją, aby rezerwa cyberbezpieczeństwa UE obejmowała usługę szybkiego reagowania przeznaczoną specjalnie dla sektora zdrowia	IV kw. 2025 r.
Opracowanie, we współpracy z siecią CSIRT, podręczników reagowania na cyberincydenty, dostosowanych do specyficznych potrzeb sektora opieki zdrowotnej	III kw. 2025 r.
Ułatwienie szeroko zakrojonego wdrożenia krajowych ćwiczeń w dziedzinie cyberbezpieczeństwa w celu przetestowania podręczników oraz wzmocnienia skuteczności protokołów reagowania na incydenty	Od IV kw. 2025 r.
Świadczenie usługi abonamentowej w zakresie przywracania sprawności operacyjnej po ataku z użyciem oprogramowania szantażującego	Od 2026 r.
Identyfikacja, we współpracy z Europolem, najpowszechniejszych odmian oprogramowania szantażującego atakującego organizacje opieki zdrowotnej oraz rozbudowa repozytorium narzędzi deszyfrujących dostępnych w ramach projektu „No More Ransom”	IV kw. 2025 r.
Opracowanie, we współpracy z Europolem, dostępnych wytycznych, aby pomóc świadczeniodawcom w unikaniu płacenia okupów	III kw. 2025 r.
Działania krajowe	
Wspieranie państw członkowskich w opracowywaniu krajowych planów działania	2025 r.
Koordynacja działań mających zapewnić wzajemne uzupełnianie się zasobów i strategii poszczególnych państw członkowskich	2025–2026
Wdrażanie i monitorowanie planu działania	
Regularne przekazywanie, w porozumieniu z Komisją, aktualnych informacji na temat prac Centrum Wsparcia Cyberbezpieczeństwa odpowiednim sieciom państw członkowskich	2025–2026

Stała wymiana poglądów z Radą Konsultacyjną ds. Cyberbezpieczeństwa w dziedzinie Zdrowia	2025–2026

Państwa członkowskie:

Europejskie zdolności w zakresie wykrywania cyberzagrożeń dla sektora zdrowia	
Przekazywanie Europejskiemu Centrum Wsparcia Cyberbezpieczeństwa powiadomień o incydentach od szpitali i świadczeniodawców na podstawie NIS 2	Od IV kw. 2025 r.
Zachęcanie do rozwoju krajowych ośrodków wymiany i analizy informacji w dziedzinie zdrowia	2025–2026
Zapobieganie cyberincydentom	
W ramach Grupy Współpracy NIS dokonywanie skoordynowanej oceny ryzyka dla bezpieczeństwa, uwzględniającej zarówno techniczne, jak i strategiczne zagrożenia związane z łańcuchami dostaw wyrobów medycznych	IV kw. 2025 r.
Szybkie reagowanie i przywracanie sprawności operacyjnej	
Przeprowadzenie krajowych ćwiczeń w dziedzinie cyberbezpieczeństwa w celu przetestowania podręczników oraz wzmocnienia skuteczności protokołów reagowania na incydenty	Od 2026 r.
Działania krajowe	
Wyznaczenie krajowych Centrów Wsparcia Cyberbezpieczeństwa dla Szpitali i Świadczeniodawców Opieki Zdrowotnej	II kw. 2025 r.
Opracowanie krajowych planów działania koncentrujących się na cyberbezpieczeństwie w sektorze zdrowia	IV kw. 2025 r.
Ułatwianie dzielenia się zasobami między świadczeniodawcami	2025–2026
Ustanowienie niewiążących poziomów odniesienia i monitorowanie celów w zakresie finansowania ukierunkowanych konkretnie na cyberbezpieczeństwo	IV kw. 2025 r.

Wezwanie organizacji opieki zdrowotnej i innych podmiotów podlegających dyrektywie NIS 2 do zgłaszania zamiaru zapłacenia okupu	IV kw. 2025 r.