Pytania i odpowiedzi dotyczące cyberbezpieczeństwa szpitali i świadczeniodawców

Posted on 2025-02-28

Dlaczego Komisja Europejska zaproponowała plan działania na rzecz cyberbezpieczeństwa w

opiece zdrowotnej?

Cyberzagrożenia dla systemów opieki zdrowotnej rosną, zarówno pod względem częstotliwości, jak i zaawansowania. Szpitale i podmioty świadczące opiekę zdrowotną, które stanowią infrastrukturę krytyczną naszych systemów opieki zdrowotnej, są szczególnie narażone na cyberataki, takie jak oprogramowanie szantażujące lub naruszenia ochrony danych. Incydenty te mogą zakłócić kluczowe usługi medyczne i zagrozić bezpieczeństwu pacjentów i ich danych. Komisja działa w trybie pilnym, aby sprostać tym wyzwaniom, zapewniając zarówno bezpieczeństwo, jak i wiarygodność transformacji cyfrowej opieki zdrowotnej.

W jaki sposób plan działania zwiększa zaufanie pacjentów i pracowników służby zdrowia?

Zaufanie jest podstawą cyfrowej opieki zdrowotnej. Zapewniając bezpieczeństwo i odporność systemów, plan działania zapewnia pacjentów, że ich dane są bezpieczne, a ich opieka nie zostanie zakłócona. Dla pracowników służby zdrowia plan zapewnia narzędzia i szkolenia, które pomogą im pewnie poruszać się po platformach cyfrowych. To podwójne podejście – chroniące zarówno pacjentów, jak i pracowników służby zdrowia – tworzy środowisko opieki zdrowotnej, w którym narzędzia cyfrowe są akceptowane i cieszą się

zaufaniem.

W jaki sposób niniejszy plan działania uzupełnia obowiązujące przepisy UE, takie jak dyrektywa NIS 2?

Plan działania opiera się na istniejących ramach prawnych w dziedzinie cyberbezpieczeństwa – w szczególności na dyrektywie NIS 2, akcie w sprawie cybersolidarności (w tym mechanizmie cyberkryzysowym), akcie w sprawie cyberbezpieczeństwa (w tym europejskiej certyfikacji cyberbezpieczeństwa), rozporządzeniu w sprawie wyrobów medycznych i akcie w sprawie cyberodporności. Zapewniają one wysoki wspólny poziom cyberbezpieczeństwa w całej UE. W dyrektywie NIS 2, w której określono obowiązki sektorów krytycznych, w tym opieki zdrowotnej, rozszerzono zakres wymogów cyberbezpieczeństwa na usługi podstawowe obejmujące laboratoria referencyjne UE, podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych, producentów podstawowych produktów i preparatów farmaceutycznych (w tym szczepionek), producentów wyrobów medycznych uznanych za krytyczne podczas stanu zagrożenia zdrowia publicznego. Jeśli chodzi o plan działania, skupiono się w szczególności na wyjątkowych podatnościach i potrzebach szpitali i placówek opieki zdrowotnej.

Plan działania ma przede wszystkim na celu wspieranie sektora w podejmowaniu podstawowych środków w zakresie cyberbezpieczeństwa, o których wiemy, że zmienią prawdopodobieństwo wystąpienia cyberincydentu. Gwarantuje to, że systemy opieki

zdrowotnej są przygotowane do radzenia sobie z konkretnymi zagrożeniami, na które są narażone. Szczególną uwagę poświęca budowaniu zdolności, inwestycjom oraz pomaganiu szpitalom i świadczeniodawcom w podejmowaniu niezbędnych środków gotowości w zakresie cyberbezpieczeństwa. Ustanawia również sposoby pomocy takim podmiotom w przypadku wystąpienia incydentu, aby zapewnić jak najszybsze i najskuteczniejsze reagowanie i odzyskiwanie danych, tak aby można było szybko przywrócić normalne operacje.

Jaka będzie rola nowego Europejskiego Centrum Wsparcia w dziedzinie Cyberbezpieczeństwa dla szpitali i świadczeniodawców?

W planie działania proponuje się m.in. utworzenie ogólnoeuropejskiego centrum wsparcia cyberbezpieczeństwa dla szpitali i świadczeniodawców, aby zapewnić im dostosowane do potrzeb wytyczne, narzędzia i usługi. ENISA, unijna agencja ds. cyberbezpieczeństwa, ustanowi Centrum w ramach swoich własnych struktur. Zapewni on realizację planu działania w sposób spójny i usprawniony, unikając jednocześnie tworzenia nowych struktur administracyjnych. Centrum Wsparcia opracuje kompleksowy katalog usług konkretnych

rozwiązań wzmacniających cyberbezpieczeństwo sektora. Będzie współpracować z państwami członkowskimi i korzystać z praktycznych doświadczeń organizacji opieki zdrowotnej.

W jaki sposób niniejszy plan działania wspiera europejską przestrzeń danych dotyczących zdrowia?

Europejska przestrzeń danych dotyczących zdrowia (EHDS) to sztandarowy projekt UE mający na celu cyfryzację opieki zdrowotnej, w którym ustanowiono jasne zasady wykorzystywania danych dotyczących zdrowia do lepszego świadczenia opieki zdrowotnej, badań naukowych, innowacji i kształtowania polityki. Odporna i bezpieczna infrastruktura ma zasadnicze znaczenie dla wdrożenia europejskiej przestrzeni danych dotyczących zdrowia. W niniejszym planie określono konkretne działania mające na celu zapewnienie przetwarzania danych w szpitalach i świadczeniodawcach, którzy działają zarówno jako świadczeniodawcy, jak i użytkownicy danych odnoszących się do zdrowia w europejskiej przestrzeni danych dotyczących zdrowia.

Oprócz niniejszego planu działania i przepisów dotyczących cyberbezpieczeństwa przyszłe rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia przewiduje również szczególne zabezpieczenia w odniesieniu do przetwarzania danych osobowych dotyczących zdrowia. Zawiera ono na przykład zabezpieczenia obejmujące zarządzania logowaniem i identyfikacją w systemach elektronicznej dokumentacji medycznej lub

ponownego wykorzystywania danych w bezpiecznych środowiskach przetwarzania.

W jaki sposób plan działania zagwarantuje, że cyberincydenty nie zakłócą opieki nad pacjentem?

Jednym z głównych filarów planu działania jest szybkie reagowanie i odbudowa.

Obejmuje to:

- Opracowanie usługi subskrypcji odzyskiwania oprogramowania ransomware i rozszerzenie repozytorium dostępnych narzędzi do odszyfrowywania oprogramowania ransomware.
- Zachęcanie szpitali do stosowania solidnych systemów tworzenia kopii zapasowych w celu ochrony krytycznych danych.
- Zwiększenie zdolności reagowania kryzysowego poprzez szkolenia i współpracę na szczeblu UE.
  Środki te mają na celu zminimalizowanie wpływu cyberincydentów na usługi opieki zdrowotnej, zapewniając pacjentom nieprzerwaną opiekę.

Jaką rolę w realizacji tego planu działania odgrywają państwa członkowskie?

Państwa członkowskie odegrają kluczową rolę we wdrażaniu planu działania poprzez:

- Koordynację krajowych strategii cyberbezpieczeństwa w opiece zdrowotnej.
- Dzielenie się informacjami na temat zagrożeń i najlepszymi praktykami ponad granicami.
- Wspieranie szpitali i świadczeniodawców w przyjmowaniu niezbędnych środków. Zachęca się państwa członkowskie do opracowania krajowych planów działania ukierunkowanych na cyberbezpieczeństwo w sektorze opieki zdrowotnej. Plany te określałyby konkretne zagrożenia dla cyberbezpieczeństwa, na jakie narażone są systemy opieki zdrowotnej, oraz krajowe działania
podejmowane w celu zaradzenia tym zagrożeniom, przy jednoczesnym zapewnieniu skutecznego wykorzystania zasobów i praktyk na szczeblu europejskim.

W jaki sposób będzie mierzony sukces planu

działania?

Aby zmierzyć powodzenie tego planu, ENISA, w porozumieniu z Komisją, będzie regularnie składać sprawozdania z postępów odpowiednim grupom i organizacjom. Sprawozdania te będą zawierać dane z unijnego indeksu cyberbezpieczeństwa, który pomoże ocenić, jak dobrze sektor opieki zdrowotnej radzi sobie pod względem cyberbezpieczeństwa. Informacje te pokażą, czy plan działa
i wywiera pozytywny wpływ.

Co mogą zrobić pacjenci, aby wesprzeć realizację celów planu działania?

Pacjenci mogą wnieść swój wkład, informując o cyberbezpieczeństwie i podejmując kroki w celu ochrony własnych cyfrowych danych dotyczących zdrowia. Na przykład:

- Korzystanie z wiarygodnych mechanizmów uwierzytelniania (np. unijnego portfela tożsamości cyfrowej) na potrzeby internetowych portali zdrowotnych.
- Zgłaszanie podejrzanych działań, takich jak próby phishingu.
- Zaufanie do świadczeniodawców, którzy stosują się do zalecanych przez UE środków w zakresie cyberbezpieczeństwa.
  Bezpieczny ekosystem opieki zdrowotnej zależy od aktywnego uczestnictwa wszystkich.

Jaki jest harmonogram realizacji planu działania?

W niniejszym komunikacie przedstawiono jasny plan zwiększenia bezpieczeństwa europejskiego sektora opieki zdrowotnej przed zagrożeniami cybernetycznymi. Plan tworzy centralne centrum wsparcia cyberbezpieczeństwa, ułatwiając szpitalom i świadczeniodawcom współpracę w celu zachowania bezpieczeństwa w internecie. Ten plan to dopiero początek. Komisja rozpoczyna szerszą rozmowę ze wszystkimi zainteresowanymi stronami, w tym świadczeniodawcami, rządami i ekspertami, aby wysłuchać ich pomysłów i informacji zwrotnych. Komisja wykorzysta ten wkład, aby uczynić plan bardziej szczegółowym i ukierunkowanym na potrzeby szpitali i innych świadczeniodawców. Zalecenia te zostaną udostępnione do końca 2025 r. Aby osiągnąć ten cel, Komisja wzywa wszystkie państwa członkowskie i zainteresowane strony do współpracy na rzecz zwiększenia cyberbezpieczeństwa sektora opieki zdrowotnej.

Aby uzyskać więcej informacji:

- Plan działania w sprawie cyberbezpieczeństwa szpitali i świadczeniodawców
- Komunikat prasowy
- Zestawienie informacji

Źródło:

Pytania i odpowiedzi dotyczące cyberbezpieczeństwa szpitali i świadczeniodawców przygotowane przez Komisję Europejską