HEALTH AI & CYBERSECURITY SUMMIT 2026

Projekt ASCLEPIUS

Jak oddolne inicjatywy pomagają sprostać wyzwaniom cyberbezpieczeństwa w ochronie zdrowia

Michał Zdunowski | IS Consulting | 16 czerwca 2026 | Centrum Nauki Kopernik, Warszawa

ASCLEPIUS
CYBERSECURITY FOR HEALTHCARE

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union

Cyberbezpieczeństwo dla ochrony zdrowia

Projekt realizowany przez konsorcjum polskich mikroorganizacji, finansowany z Digital Europe Programme za pośrednictwem ECCC. Usługi cyberbezpieczeństwa świadczyliśmy pro bono na rzecz europejskich placówek ochrony zdrowia.

Model	Doradczy i vendor agnostic, koncentracja na dojrzałości i przygotowaniu
Finansowanie	Digital Europe Programme, nadzór ECCC
Realizacja	Konsorcjum polskich mikrofirm, koordynator IS Consulting
Beneficjenci	Usługi świadczone pro bono

3,2 mln €
wartość projektu

3 lata
czas trwania

7
instytucji beneficjentów

pro bono
dla beneficjentów

Co-funded by the European Union

02 KONSORCJUM I MODEL DZIAŁANIA

Oddolny model: polskie mikrofirmy koordynujące program o zasięgu kontynentalnym.

Konsorcjum mikroorganizacji

Koordynator IS Consulting wraz z partnerami, w całości polskie mikrofirmy. Dowód, że mała skala nie wyklucza realizacji ambitnych programów.

Podejście vendor agnostic

Bez wiązania beneficjentów z konkretnym dostawcą. Rekomendacje oparte na ryzyku, standardach i realnej wykonalności.

Beneficjenci końcowi

Dwa duże szpitale, w tym jeden instytut badawczy. Trzy szpitale prywatne z sektora MŚP. Krytyczny podmiot w łańcuchu dostaw leków.

Zakres wsparcia

Szkolenia i budowanie świadomości, testy bezpieczeństwa, ocena dojrzałości i dostawców, ćwiczenia odpornościowe oraz dokumentacja i polityki.

Co-funded by the European Union

03 LUDZIE I ŚWIADOMOŚĆ

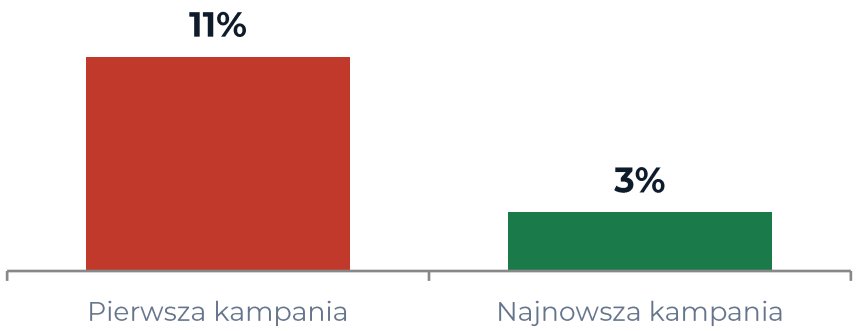
Człowiek jest najsłabszym i najsilniejszym ogniwem. Tu skupiliśmy największy wysiłek.

1200+
przeszkolonych pracowników sektora

12
kampanii phishingowych

40
osób w bootcampie do certyfikatu SSCP

Efektywna klikalność w linki phishingowe



Trend spadkowy w 12 kampaniach

Efektywna klikalność w linki spadła z 11% do 3%. Obecnie 10% odbiorców otwiera wiadomość, a 30% z nich klika w link. Spadek to wymierny dowód, że cykliczne szkolenia i symulacje realnie zmieniają zachowania pracowników.

04 TESTY I ZAPEWNIENIE BEZPIECZEŃSTWA

Systematyczne wykrywanie podatności w kodzie, infrastrukturze i aplikacjach.

37
skanów kodu (Static Code Analysis)

14
skanów podatności infrastruktury

8
przetestowanych aplikacji webowych

Bezpieczeństwo w cyklu wytwarzania

Analizę statyczną kodu prowadziliśmy cyklicznie, w trakcie powstawania rozwiązań. Wyniki przekładaliśmy na konkretne rekomendacje naprawcze, a remediację realizowały zespoły beneficjentów jeszcze przed wdrożeniem na produkcję.

Powierzchnia ataku infrastruktury

Skany podatności infrastruktury oraz testy aplikacji webowych pozwoliły uporządkować priorytety. Efekt to mierzalne ograniczenie powierzchni ataku i jasna lista działań naprawczych dla każdego beneficjenta.

Co-funded by the European Union

05 GOVERNANCE I ODPORNOŚĆ

Dojrzałość, łańcuch dostaw i zdolność reakcji na incydenty.

7
analiz dojrzałości organizacji

15
ocenionych dostawców krytycznych

~40h
ćwiczeń tabletop z beneficjentami

Dojrzałość i łańcuch dostaw

Siedem organizacji otrzymało ocenę dojrzałości z punktem wyjścia i ścieżką rozwoju. Równolegle systematycznie oceniamy dostawców krytycznych, piętnastu już przeszło ocenę. To realne zarządzanie ryzykiem stron trzecich.

Ćwiczenia, procedury i szablony

Wykoane 20 ćwiczeń tabletop, różne scenariusze incydentów z zespołami beneficjentów. Powstały nowe procedury, standardy i polityki cyberbezpieczeństwa, pozostawione jako gotowe szablony do wielokrotnego użycia.

Co-funded by the European Union

06 EFEKT DLA BENEFICJENTÓW

Bezpieczeństwo, które wspiera lekarzy, pielęgniarki i dyrektorów, a nie ich blokuje.

- **Mniej skutecznych ataków** efektywna klikalność w phishingu spadła z 11% do 3%.
- **Realne kompetencje** ponad 1000 przeszkolonych, 40 osób na ścieżce do certyfikatu SSCP.
- **Mniejsza powierzchnia ataku** podatności wykryte i naprawione w kodzie, infrastrukturze i aplikacjach.
- **Trwałe zasoby** gotowe polityki, procedury i szablony pozostały u beneficjentów.
- **Większa odporność** przećwiczone scenariusze incydentów i oceniony łańcuch dostaw.

Co-funded by the European Union

07 POWTARZALNY MODEL

ASCLEPIUS to nie wyjątek, to model gotowy do powielenia.

+400%

powyżej założonych KPI projektu

Niższy budżet

efekt osiągnięty przy budżecie niższym niż zakładano

Realizacja wskaźników projektu znacząco przekroczyła założenia, około 400% powyżej planowanych KPI, przy jednocześnie niższym budżecie. Oddolne inicjatywy mają sens, a mikrodziałalności w cyberbezpieczeństwie potrafią dowieźć efekt. Trzeba im tylko dać szansę.

Co działa: konsorcjum mikrofirm, usługi pro bono, podejście vendor agnostic.
Co jest potrzebne: koordynacja, zaufanie między partnerami i stabilne ramy finansowania.

Co-funded by the European Union

PODSUMOWANIE

Dowiezione.

Oddolne inicjatywy w cyberbezpieczeństwie ochrony zdrowia działają. Mikrofirmy potrafią dostarczyć efekt na skalę kontynentalną. Trzeba tylko dać im szansę.

- Wskaźniki projektu około 400% powyżej KPI, przy niższym budżecie.
- Ponad 1000 przeszkolonych, efektywna klikalność w phishingu z 11% do 3%.
- Testy kodu, infrastruktury i aplikacji oraz oceniony łańcuch dostaw.
- Polityki, procedury i szablony pozostawione beneficjentom, model gotowy do powielenia.

Michał Zdunowski | IS Consulting | media@isconsulting.pl

ASCLEPIUS CYBERSECURITY FOR HEALTHCARE

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union