CyberPOLICY
NASK

JAK CYBERBEZPIECZNA JEST EUROPA?

RAPORT ENISA "NIS360 – 2024"

SPIS TREŚCI

METODOLOGIA BADANIA

- Energia
- *Transport*
- *Finanse*
- *Zdrowie*
- *Woda pitna i ścieki*
- *Infrastruktura cyfrowa*
- *Zarządzanie usługami ICT*
- *Administracja publiczna*
- *Przestrzeń kosmiczna*

Badanie, którego efektem jest opublikowany raport NIS360, przedstawia ogólnounijną perspektywę dojrzałości i krytyczności sektorów w kontekście cyberbezpieczeństwa. Autorzy raportu podkreślają istotność uznania, że państwa członkowskie mają odrębne konteksty regulacyjne i operacyjne, a same sektory są bardzo zróżnicowane. . Podmioty w tych sektorach różnią się wielkością, modelami operacyjnymi, poziomem ryzyka, na jakie są narażone, zdolnościami w zakresie cyberbezpieczeństwa, zasobami cyberbezpieczeństwa itp. W rezultacie, podczas gdy ocena NIS360 opiera się na połączeniu różnych perspektyw, obserwacje są często uogólniane w celu odzwierciedlenia ogólnounijnego krajobrazu, co może sprawić, że nie oddają one [PP1] dokładnie statusu poszczególnych podmiotów lub państw członkowskich.

W zakresie badania NIS360 2024 znalazły się 22 (pod)sektory zidentyfikowane jako krytyczne na mocy załącznika I do dyrektywy NIS2, w ramach 9 sektorów wymienionych po lewej stronie.

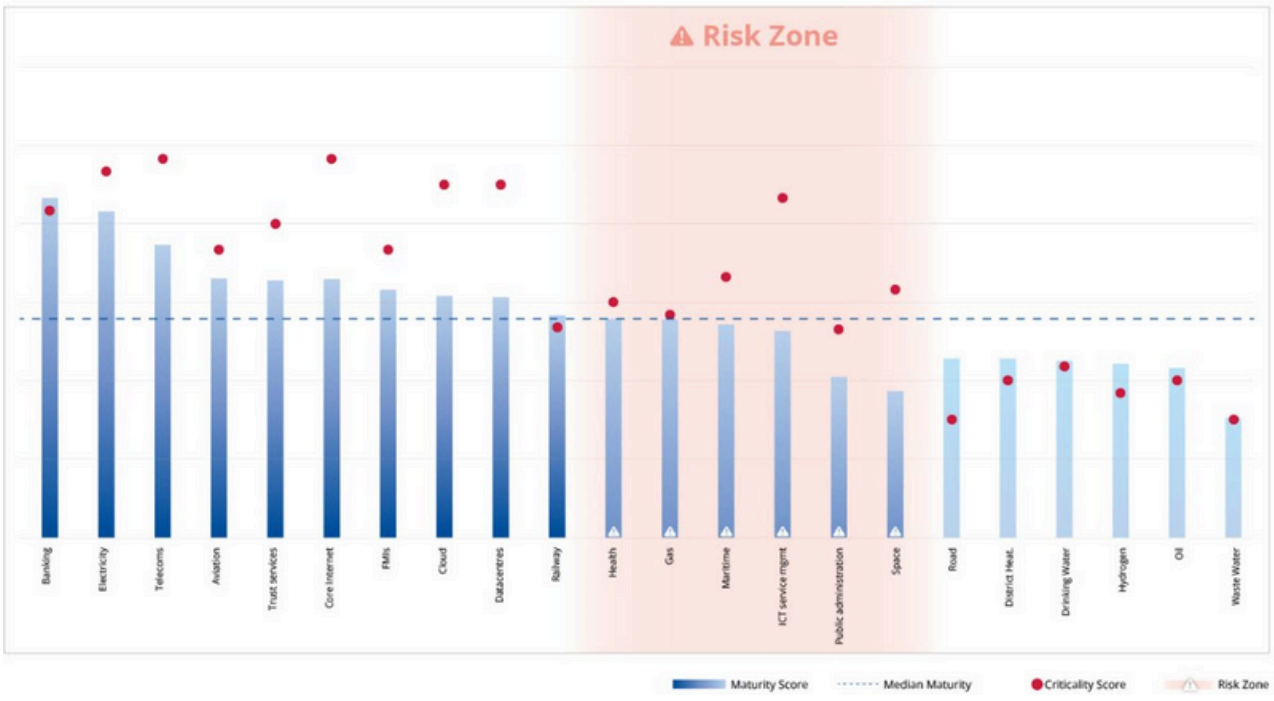
METODOLOGIA BADANIA

Dojrzałość cyfrową i krytyczność każdego z powyższych sektorów oceniono w odniesieniu do określonych wymiarów dojrzałości i krytyczności, zgodnie z metodyką NIS360 opisaną w załączniku A.

Wyniki każdego sektora w odniesieniu do zdefiniowanych wymiarów dojrzałości i krytyczności są oceniane za pomocą szeregu wskaźników. Dla każdego wskaźnika zidentyfikowano odpowiednie źródło danych i określono algorytm punktacji, który definiuje sposób, w jaki zebrane dane zostaną przełożone na wynik. Zastosowanie algorytmu ma na celu zapewnienie, że każdy sektor jest oceniany w oparciu o znormalizowane ramy, które pozwalają na porównania między sektorami .

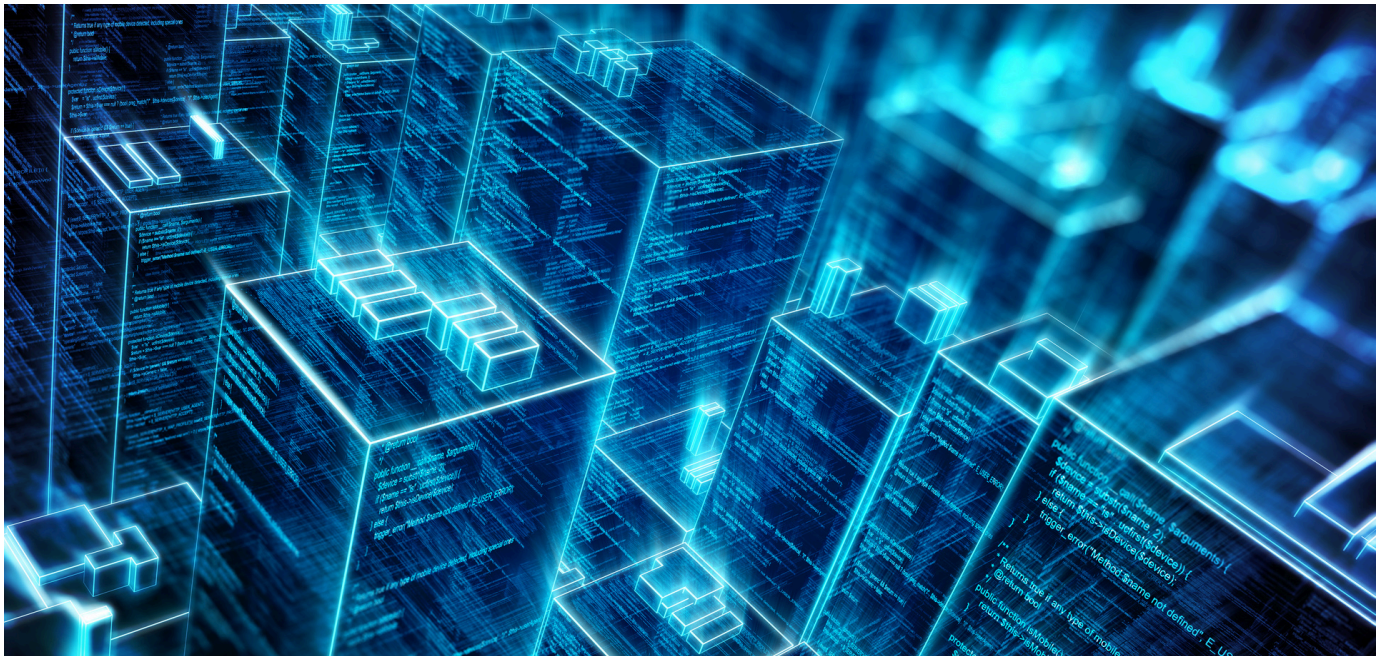
Po przypisaniu wyników do poszczególnych sektorów, przeprowadzono analizę post-scoringową, aby zidentyfikować sektory należące do „strefy ryzyka”.

Sektory ryzyka to sektory, które plasują się stosunkowo niżej niż inne pod względem dojrzałości, ale mają wynik krytyczności, który jest wyższy niż ich wynik dojrzałości. Identyfikacja „strefy ryzyka” umożliwia ustalenie priorytetów. Sektory poza strefą ryzyka są albo na dobrej drodze do osiągnięcia dojrzałości zgodnej z ich krytycznością, albo nie znajdują się jeszcze na etapie, na którym ryzyko cyberbezpieczeństwa stanowi poważne zagrożenie dla ich podstawowych operacji.



Rys. 1 Raport ENISA NIS360 2024. ENISA Cybersecurity Maturity & Criticality Assessment of NIS2 sectors, s. 59.

OCENA DOJRZAŁOŚCI SEKTORÓW



OCENA DOJRZAŁOŚCI SEKTORÓW

Wszystkie sektory ocenione w ramach raportu NIS360 cechują się znaczną wewnętrzną różnorodnością. W ich obrębie działają podmioty o bardzo zróżnicowanym charakterze – od wysoce krytycznych, dużych organizacji, po mniejsze jednostki o ograniczonym wpływie na funkcjonowanie sektora jako całości. To zróżnicowanie dotyczy również poziomu dojrzałości w zakresie cyberbezpieczeństwa i świadomości ryzyk.

- Energia
- Telekomunikacja
- Bankowość

Trzy sektory (wymienione po lewej) wyróżniają się na tle innych. Stanowią one podstawę odpornej i wzajemnie połączonej gospodarki, zapewniając stabilność, łączność i bezpieczeństwo finansowe.

Z biegiem czasu sektory te skorzystały ze znacznego nadzoru regulacyjnego, globalnych inwestycji, koncentracji politycznej i solidnych partnerstw publiczno-prywatnych, co umożliwiło im osiągnięcie najwyższego poziomu dojrzałości spośród badanych sektorów.

Analizując ogólne poziomy dojrzałości oraz czynniki, które na nie wpłynęły, można zauważyć, że sektory charakteryzujące się wyższą dojrzałością cyfrową korzystają z kilku istotnych przewag:

Posiadają lepiej rozwiniętą gotowość operacyjną dzięki opracowanym i przetestowanym planom działania na poziomie organizacyjnym, krajowym i europejskim.

Cieszą się silniejszym wsparciem i nadzorem zarówno na poziomie unijnym, jak i krajowym, ze strony organów posiadających wiedzę o specyfice danego sektora i jego wyzwaniach

Wykazują głębsze zrozumienie krajobrazu ryzyk właściwych dla danego sektora, co przekłada się na wdrażanie skuteczniejszych mechanizmów zarządzania ryzykiem i lepsze zabezpieczenie cyfrowej infrastruktury

Charakteryzują się wyższym poziomem współpracy oraz wymiany informacji między wszystkimi interesariuszami sektora – zarówno pomiędzy samymi podmiotami, jak i między nimi a organami nadzorczymi – na poziomie jednostkowym, krajowym i unijnym.

Otrzymują bardziej szczegółowe wytyczne dotyczące cyberbezpieczeństwa, które mogą przyjmować formę przepisów sektorowych, standardów branżowych lub dostosowanych do specyfiki sektora wytycznych.

OCENA DOJRZAŁOŚCI SEKTORÓW

Sektor infrastruktury cyfrowej

Należy do sektorów o wyższym poziomie dojrzałości. Biorąc pod uwagę, że cyfryzacja jest jego główną domeną usług, nie jest zaskoczeniem, że sektor ten osiąga wysokie wyniki w niektórych ocenianych obszarach dojrzałości cyfrowej. Niemniej jednak, podsektory w ramach sektora stoją również przed kilkoma wyzwaniami, wynikającymi z ich nieodłącznej heterogeniczności oraz ich transgranicznego charakteru. Dodatkowo, objęcie zakresem regulacji podmiotów wcześniej nieregulowanych stanowi podwójne wyzwanie: wymogi są dla tych firm zupełnie nowe, a organy krajowe często nie są zaznajomione z rynkiem, który mają teraz nadzorować.

Sektor zarządzania usługami ICT

Choć wykazuje pewne podobieństwa do infrastruktury cyfrowej ma odrębny profil dojrzałości. Sektor ten jest oceniany jako umiarkowanie dojrzały, ale plasuje się znacznie niżej niż pozostałe sektory cyfrowe. Jako nowo regulowany sektor w ramach NIS2, stoi przed kilkoma wyzwaniami, takimi jak: brak spójności oraz zasobów, które umożliwiłyby nadążanie za rosnącą złożonością wsparcia operacji cyfrowych w innych sektorach, brak znajomości sektora przez organy odpowiedzialne za jego nadzór, obecność podmiotów działających transgranicznie oraz słaba współpraca pomiędzy nimi.

Sektor kosmiczny

Mimo że odgrywa kluczową rolę w zapewnianiu globalnej łączności – umożliwiając transmisję danych, dostęp do internetu, nadawanie telewizyjne, nawigację i komunikację w czasie rzeczywistym – jego dojrzałość mieści się jedynie w zakresie „umiarkowanym” i należy do najniższych spośród wszystkich ocenianych sektorów. Jako sektor nowo objęty regulacją w ramach dyrektywy NIS2, znajduje się dopiero na wczesnym etapie dostosowywania się do jej wymagań, co stanowi wyzwanie zarówno dla podmiotów, jak i dla krajowych organów nadzorczych.

Znaczna zależność tego sektora od łańcuchów dostaw oraz komercyjnych produktów, w połączeniu z ograniczonymi inwestycjami w cyberbezpieczeństwo, dodatkowo potęguje te trudności. Jednocześnie, współpraca i wymiana informacji w obrębie sektora pozostają na bardzo wczesnym etapie, mimo powołania Europejskiego ISAC sektora kosmicznego (EU Space ISAC) w 2024 roku.

OCENA DOJRZAŁOŚCI SEKTORÓW

W poziomach dojrzałości podsektorów w obrębie poszczególnych sektorów UE występuje duża różnorodność.

W sektorze energetycznym podsektor energii elektrycznej wykazuje wysoką dojrzałość, plasując się w czołówce ocenianych obszarów, podczas gdy gaz charakteryzuje się umiarkowaną dojrzałością i znajduje się bliżej środka stawki. Ciepłownictwo i chłodnictwo sieciowe, wodór oraz ropa naftowa wypadają znacznie słabiej i należą do grupy o najniższych wskaźnikach dojrzałości.

W sektorze finansowym bankowość wykazuje wyższy poziom dojrzałości niż infrastruktura rynku finansowego (FMIs), choć oba podsektory plasują się wysoko w porównaniu z innymi.

Sektor transportu również wykazuje zróżnicowanie. Lotnictwo cechuje się wysokim poziomem dojrzałości i znajduje się w czołówce, natomiast kolejnictwo i transport morski plasują się w środku zestawienia. Transport drogowy natomiast uzyskał zdecydowanie niższą ocenę.

W sektorze wodnym woda pitna osiąga lepsze wyniki niż ścieki, jednak oba znajdują się na dolnym końcu rankingu dojrzałości.

OCENA DOJRZAŁOŚCI SEKTORÓW

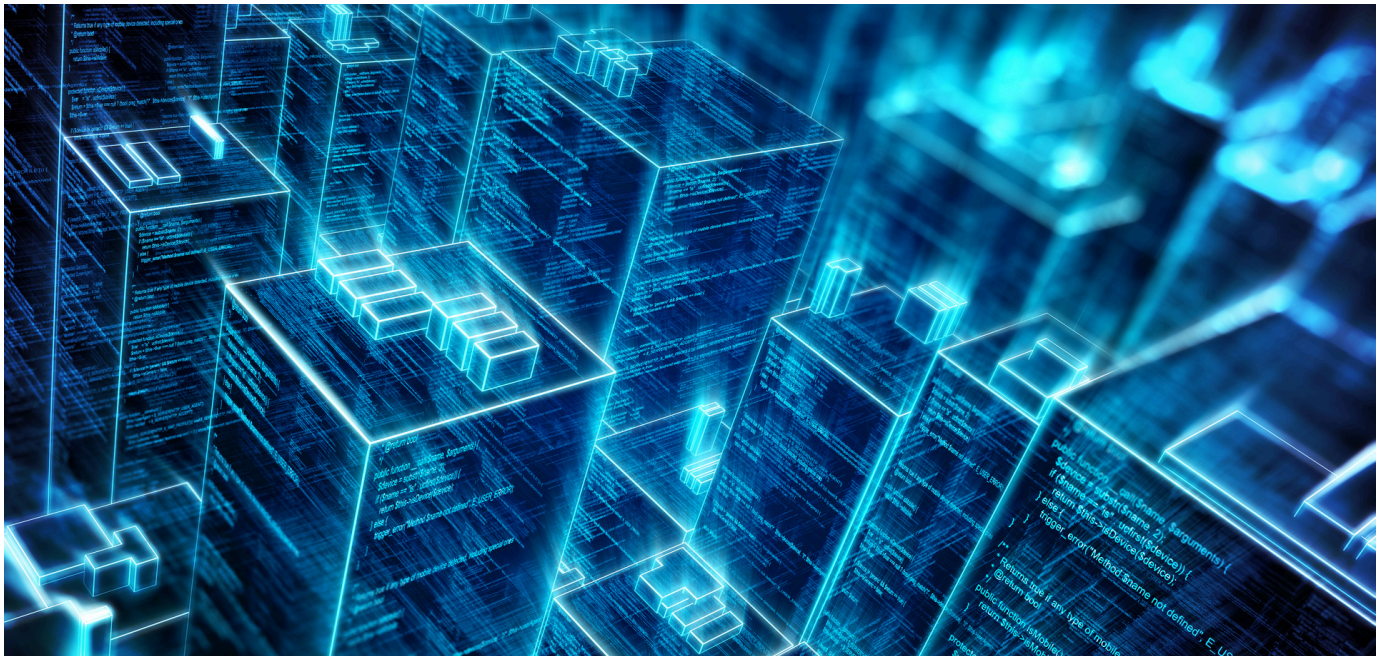
Sektor ochrony zdrowia plasuje się w górnej części kategorii „umiarkowanej" dojrzałości, osiągając średni wynik w porównaniu z innymi sektorami. W ramach dyrektywy NIS2 zakres tego sektora został znacząco rozszerzony, co jeszcze bardziej komplikuje sytuację w i tak już bardzo zróżnicowanym środowisku. Sektor ten obejmuje zarówno duże podmioty, które zazwyczaj wykazują wyższy poziom dojrzałości i silniejsze mechanizmy cyberbezpieczeństwa, jak i mniejsze jednostki, które często mają trudności nawet z podstawową cyberhigieną.

Jednym z najbardziej palących problemów jest **duża rozbieżność w poziomie rozumienia cyberzagrożeń wśród różnych podmiotów** – większe organizacje lepiej rozpoznają ryzyka i są w stanie wdrażać bardziej zaawansowane środki zaradcze, podczas gdy mniejsze placówki często nie posiadają nawet podstawowej wiedzy w tym zakresie. Fragmentacja sektora oraz ograniczone zrozumienie cyberzagrożeń tylko pogłębiają te trudności. Sytuację dodatkowo pogarsza silne uzależnienie sektora od złożonych łańcuchów dostaw, a także zależność od przestarzałych systemów oraz słabo zabezpieczonych urządzeń medycznych.

Do najmniej dojrzałych spośród wszystkich ocenianych sektorów należy sektor administracji publicznej. Mimo swojej kluczowej roli w zapewnianiu efektywnego zarządzania i świadczenia usług publicznych, jako sektor nowo objęty regulacjami w ramach dyrektywy NIS2, znajduje się dopiero na wczesnym etapie dostosowania do jej wymagań. Brakuje mu ugruntowanego wsparcia instytucjonalnego i doświadczenia, które charakteryzują bardziej dojrzałe sektory.

Na poziomie UE nie istnieje jeszcze spójne, sektorowe rozumienie ryzyk, z jakimi mierzy się administracja publiczna. Nie ustalono też w pełni, jakie zasoby i zagrożenia powinny być objęte zakresem tej regulacji, co utrudnia opracowanie skutecznych praktyk w zakresie zarządzania ryzykiem.

OCENA KRYTYCZNOŚCI SEKTORÓW



OCENA KRYTYCZNOŚCI SEKTORÓW

Krytyczność sektorów oceniano na podstawie kilku kluczowych czynników, takich jak ich wpływ społeczno-gospodarczy, potencjał do zakłócania funkcjonowania innych sektorów, zależność od ICT oraz czas, w jakim skutki incydentu są odczuwalne w społeczeństwie lub gospodarce.

- sektory najbardziej krytyczne
- sektory kluczowe
- sektory istotne
- sektory ważne
- sektory umiarkowane
- sektory o najniższej krytyczności

Sektory o większym znaczeniu społeczno-gospodarczym oraz wyższym poziomie powiązań i zależności od ICT – takie jak energetyka, telekomunikacja i finanse – doświadczają poważniejszych skutków cyberincydentów i wymagają szybszych reakcji, by zapobiec eskalacji. Z kolei sektory takie jak woda pitna, ciepłownictwo, ropa naftowa, wodór, transport drogowy i ścieki, choć ważne, są mniej krytyczne w bezpośrednim następstwie ataku. Dzięki niższemu uzależnieniu od infrastruktury cyfrowej i dostępnym środkom awaryjnym są w stanie stopniowo się odbudować bez długoterminowych skutków czy istotnych oddziaływań międzysektorowych.

OCENA KRYTYCZNOŚCI SEKTORÓW

SEKTORY KRYTYCZNE

Cztery najbardziej krytyczne (pod)sektory dla gospodarki i społeczeństwa to telekomunikacja, energia elektryczna oraz dwa podsektory w ramach infrastruktury cyfrowej - Internet bazowy, a także chmura i centra danych.

Incydenty w tych sektorach mają natychmiastowy i poważny wpływ. Zakłócenia w telekomunikacji zatrzymałyby funkcjonowanie służb ratunkowych oraz wpłynęłyby negatywnie na takie sektory jak płatności cyfrowe i handel internetowy. Przerwy w działaniu krajowych domen najwyższego poziomu (TLD), dostawców DNS, punktów wymiany ruchu (IXP) czy dostawców treści (CDN) spowolniłyby ruch internetowy, co miałoby przełożenie na działalność firm i usług cyfrowych. Cyberatak na dostawcę usług chmurowych mógłby spowodować masowe przerwy w działalności firm i znaczne straty finansowe. Podobnie, awaria zasilania mogłaby zakłócić działanie płatności elektronicznych, uniemożliwić sprzedaż i świadczenie usług oraz wpłynąć na działanie sieci telekomunikacyjnych, zwiększając skalę zakłóceń w gospodarce.

Sektory te cechują się wysoką krytycznością czasową, ponieważ skutki incydentu są odczuwalne niemal natychmiast i poważnie wpływają na inne sektory, które są zależne od infrastruktury cyfrowej i energii elektrycznej.

SEKTORY KLUCZOWE

Sektory zarządzania usługami ICT, zaufania cyfrowego oraz finansów są kluczowe dla stabilności gospodarczej UE, rozwoju usług cyfrowych i wzrostu gospodarczego.

Tworzą one drugą grupę sektorów krytycznych. Zarządzanie usługami ICT oraz zaufanie cyfrowe to obszary z natury cyfrowe, natomiast sektor finansowy całkowicie opiera się na ICT w swoich operacjach. Sektor bankowy korzysta z infrastruktury cyfrowej do obsługi płatności oraz usług międzybankowych, podczas gdy infrastruktura rynku finansowego (FMIs), np. giełdy papierów wartościowych czy izby rozliczeniowe, wykorzystuje ICT do przetwarzania danych w czasie rzeczywistym, zarządzania ryzykiem i handlu.

Poważny incydent w tym sektorze mógłby zatrzymać płatności, powodując zakłócenia w działalności firm i sytuacji finansowej obywateli. Zakłócenia w sektorze zaufania cyfrowego mogą wpłynąć na działanie usług online opartych na certyfikatach internetowych, co może wywołać efekt domina w sektorach zmuszonych do przejścia na procesy offline. Ze względu na wysoką krytyczność czasową, skutki poważnych incydentów w tych sektorach są odczuwalne bardzo szybko, a sektory od nich uzależnione również cierpią.

OCENA KRYTYCZNOŚCI SEKTORÓW

SEKTORY ISTOTNE

Sektory lotnictwa, transportu morskiego i przestrzeni kosmicznej są istotne dla gospodarki UE.

Transport lotniczy odpowiada za 13,1% przewozów pasażerskich, a morski za 67,8% przewozów towarowych, wspierając globalny handel i turystykę. Sektor kosmiczny rozwija się dynamicznie, dostarczając krytycznych usług dla branż takich jak transport, finanse i energetyka, a jego rola rośnie wraz z upowszechnieniem się systemów satelitarnych, takich jak konwergencja 5G i GPS.

Wszystkie trzy sektory są silnie uzależnione od technologii ICT. Najbardziej zaawansowany cyfrowo jest transport lotniczy. Z kolei sektor morski zmaga się z przestarzałą technologią, a sektor kosmiczny w dużej mierze opiera się na ICT w swoich podstawowych procesach. Cyberincydenty w tych sektorach mają wysoki stopień krytyczności czasowej. Opóźnienia w reakcji mogą prowadzić do poważnych konsekwencji – także w innych branżach. Zakłócenia w sektorze kosmicznym mogą wpływać na lotnictwo, transport morski i służby ratunkowe, które są zależne od precyzyjnych danych satelitarnych.

SEKTORY WAŻNE

Sektor ochrony zdrowia odgrywa ważną rolę w gospodarce UE, odpowiadając za 7,4% przedsiębiorstw, średnio 8,4% zatrudnienia oraz 6,2% wartości dodanej brutto w biznesie.

Jednak jego bezpośredni wpływ na inne sektory jest jednak mniejszy w porównaniu do wcześniej wymienionych. Mimo dużego uzależnienia od systemów ICT, skutki cyberincydentów są zazwyczaj możliwe do opanowania, choć podatność łańcuchów dostaw zwiększa poziom ryzyka.

Cyberataki, takie jak ransomware, mogą generować wysokie koszty, ale ich wpływ na całą gospodarkę jest ograniczony. Niemniej jednak, poważne incydenty wymagają szybkiej reakcji w celu zapewnienia ciągłości działania i ochrony wrażliwych usług. Ze względu na wrażliwość danych pacjentów oraz potencjalnie katastrofalny wpływ cyberataków na świadczenie opieki zdrowotnej, kluczowe jest zapewnienie sprawnej i skutecznej reakcji na incydenty w celu ochrony zdrowia pacjentów i utrzymania funkcji krytycznych sektora.

OCENA KRYTYCZNOŚCI SEKTORÓW

SEKTORY UMIARKOWANE

Sektory kolei, gazu i administracji publicznej mają umiarkowane znaczenie gospodarcze, a zakłócenia w nich zazwyczaj mają charakter krajowy.

Przewozy towarowe koleją stanowią 5% rynku UE, podczas gdy sektor centralnej administracji publicznej odpowiada za 2% PKB UE, z prawie połową populacji korzystającą z cyfrowych usług publicznych. Sektor gazowy jest powiązany z wieloma branżami – w tym z produkcją energii elektrycznej, ogrzewaniem i przemysłem – co zwiększa potencjalny wpływ zakłóceń.

Zależność od ICT w tych sektorach jest umiarkowana, a postępująca cyfryzacja jest równoważona przez obecność przestarzałych systemów oraz zależność od dostawców zewnętrznych w zakresie aktualizacji i utrzymania. Choć poważny incydent może wywołać tymczasowe przerwy w usługach i umiarkowane zakłócenia społeczno-gospodarcze, długoterminowe szkody są mało prawdopodobne. Ataki mogą zakłócić dostępność usług, ale kopie zapasowe i działania manualne pomagają zminimalizować skutki społeczne, utrzymując krótko- i średnioterminowe skutki na akceptowalnym poziomie. Skutki poważnych incydentów w tych sektorach są zazwyczaj odczuwalne w ciągu kilku godzin przez społeczeństwo lub inne zależne sektory.

SEKTORY NAJNIŻSZEJ KRYTYCZNOŚCI

Sektorami o najniższej krytyczności są: woda pitna, ciepłownictwo sieciowe, ropa naftowa, wodór, transport drogowy i ścieki.

Ich mniejsze uzależnienie od infrastruktury cyfrowej oraz dostępność alternatywnych rozwiązań ograniczają bezpośredni wpływ cyberincydentów. Wszystkie te sektory korzystają z technologii operacyjnej (OT) w różnym stopniu – do kontroli, monitorowania i utrzymania infrastruktury krytycznej oraz działań operacyjnych. Złożoność i zakres systemów OT są jednak zróżnicowane: np. sektor ropy naftowej i wody pitnej jest bardziej zależny od OT pod względem bezpieczeństwa i efektywności niż transport drogowy czy wodór.

Choć incydenty w tych sektorach mogą powodować skutki operacyjne i społeczne, nie prowadzą zwykle do szeroko zakrojonych zakłóceń ani efektów domina w innych branżach.

WSPÓLNE PROBLEMY

ZRÓŻNICOWANA ODPOWIEDZIALNOŚĆ

1 Brak ustandaryzowanych i spójnych mechanizmów nadzoru

Różnice w podejściu organów krajowych do interpretacji i egzekwowania przepisów NIS2 skutkują fragmentacją, która utrudnia jednolitą implementację środków bezpieczeństwa. Dotyczy to zwłaszcza usług zarządzanych ICT oraz zaufania cyfrowego, gdzie wielu dostawców działa równocześnie w kilku państwach członkowskich.

2 Deficyt kompetencji

Nie tylko wśród podmiotów kluczowych i ważnych, ale także w organach nadzorczych. Wiele instytucji publicznych wciąż nie posiada wystarczających zasobów kadrowych ani dostępu do narzędzi analitycznych pozwalających na skuteczne egzekwowanie wymogów NIS2. Luka kompetencyjna jest szczególnie dotkliwa w sektorach nowo objętych regulacją – takich jak przestrzeń kosmiczna, administracja publiczna czy sektor ciepłowniczy – gdzie brakuje nie tylko praktyki, ale często także świadomości zagrożeń.

3 Niski poziom współpracy i wymiany informacji

Brakuje rozwiniętych mechanizmów koordynacji na poziomie krajowym i unijnym, zwłaszcza w sektorach o mniejszej dojrzałości, które nie posiadają własnych ISAC (*Information Sharing and Analysis Centre*). Choć ENISA promuje tworzenie takich struktur – jak np. EU Space ISAC uruchomiony w 2024 roku – to ich realne oddziaływanie na zwiększenie odporności jest jeszcze ograniczone.

4 Brak odpowiednio dopasowanych planów gotowości operacyjnej

Sektory o niskiej dojrzałości rzadko biorą udział w ćwiczeniach typu „table-top" lub „red teaming", a ich plany zarządzania kryzysowego nie są wystarczająco testowane. Ćwiczenie Cyber Europe 2022 unaoczniło, jak duże różnice występują pomiędzy sektorami.

5 Różny poziom uwagi politycznej

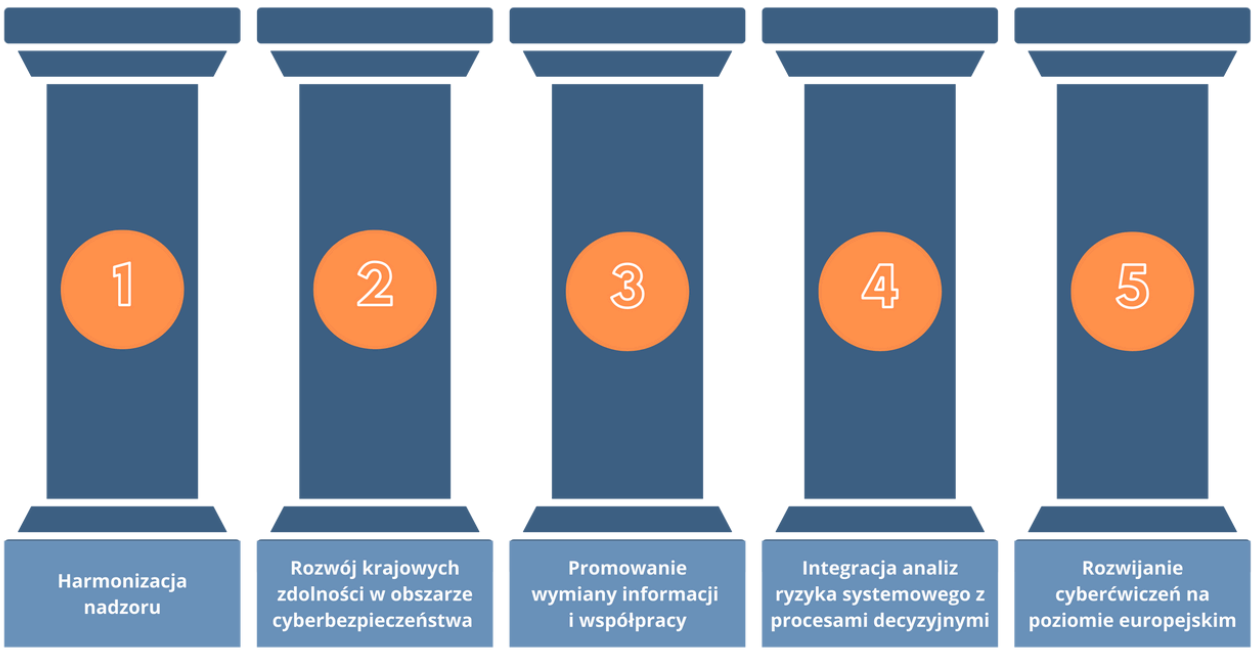
Sektory takie jak energia elektryczna, gaz czy finanse znajdują się pod stałym nadzorem strategicznym, co przekłada się na większe inwestycje, lepsze wsparcie instytucjonalne oraz częstsze analizy ryzyka o zasięgu unijnym. Tymczasem inne sektory – choć również istotne dla ciągłości państwa – nie otrzymują podobnego wsparcia, co osłabia zarówno presję na inwestycje w cyberbezpieczeństwo, jak i rozwój specjalistycznych regulacji.

WNIOSKI STRATEGICZNE

KIERUNKI ROZWOJU

Raport ENISA NIS360 – 2024 nie tylko identyfikuje istniejące luki i zagrożenia, lecz także oferuje kompleksowy zestaw rekomendacji strategicznych skierowanych do państw członkowskich, organów nadzorczych i samych sektorów objętych dyrektywą NIS2. Wśród rekomendacji ENISA pojawiają się postulaty dotyczące praktycznego wdrażania dyrektywy NIS2 z uwzględnieniem specyfiki sektorów.

5 filarów rozwoju - rekomendacje ENISA



WNIOSKI STRATEGICZNE

KIERUNKI ROZWOJU

ENISA zaleca dalszą harmonizację podejścia nadzorczego w całej Unii Europejskiej. Oznacza to nie tylko spójność w zakresie interpretacji przepisów NIS2, ale także synchronizację nadzoru transgranicznego, szczególnie w kontekście podmiotów działających w wielu krajach, np. dostawców usług chmurowych czy operatorów domen najwyższego poziomu (TLD). Kluczowe będzie tu wypracowanie wspólnych metod oceny ryzyka, ram reagowania na incydenty oraz mechanizmów audytu i monitorowania.

ENISA wskazuje na konieczność rozwoju krajowych zdolności w zakresie cyberbezpieczeństwa, ze szczególnym uwzględnieniem sektorów znajdujących się w tzw. strefie ryzyka. ENISA proponuje stworzenie dedykowanych programów wsparcia technicznego i merytorycznego dla organów regulacyjnych oraz organizacji sektora publicznego. Ważne jest również zwiększenie dostępności specjalistycznych szkoleń, ćwiczeń z zakresu cyberbezpieczeństwa oraz narzędzi wspierających analizę ryzyka i reagowanie na incydenty.

ENISA kładzie silny nacisk na potrzebę promowania wymiany informacji i współpracy międzysektorowej. Sugeruje się tu rozszerzenie roli struktur takich jak ISAC (Information Sharing and Analysis Centres), które powinny funkcjonować nie tylko na poziomie krajowym, ale również europejskim. Wspólne ćwiczenia, współdzielenie scenariuszy zagrożeń oraz rozwój platform wymiany informacji są kluczowe dla zwiększenia świadomości i gotowości.

Czwartym filarem proponowanych działań jest integracja analiz ryzyka sektorowego z procesami decyzyjnymi na poziomie polityk publicznych. Wskazuje się, że niektóre sektory – jak energetyka czy bankowość – już korzystają z takich podejść, jednak potrzebne jest rozszerzenie tej praktyki na kolejne branże, szczególnie w sektorach wrażliwych, takich jak zdrowie, administracja publiczna czy ICT services. Powinno to prowadzić do lepszego planowania zasobów, inwestycji oraz skuteczniejszego wdrażania strategii bezpieczeństwa cyfrowego.

ENISA rekomenduje dalsze rozwijanie ćwiczeń z obszaru cyberbezpieczeństwa na poziomie europejskim. Ćwiczenia typu Cyber Europe, obejmujące scenariusze awarii międzysektorowych, powinny być rozszerzane o komponenty technologii operacyjnych (OT), łańcuchów dostaw oraz krytycznych zależności międzysektorowych. Szczególne znaczenie ma tu integracja sektorów, które dotychczas rzadko brały udział w tego typu wydarzeniach, jak np. przestrzeń kosmiczna, ciepłownictwo czy wodór