ResilienceOne

STAN WDROŻENIA DYREKTYWY NIS2 W POLSCE

Analiza gotowości organizacji oraz kluczowe wyzwania w dostosowaniu do wymagań NIS2.

LOGICALTRUST

TENESYS

IDentonic
IDENTITY · SECURITY · COMPLIANCE

SPIS TREŚCI

1. WPROWADZENIE DO NIS2

1.1 WPROWADZENIE DO DYREKTYWY I JEJ ZNACZENIE DLA SEKTORA IT I OT

Dyrektywa NIS2 (Network and Information Security 2) stanowi kluczowy element unijnej strategii cyberbezpieczeństwa, mający na celu zwiększenie odporności infrastruktury IT i OT na zagrożenia cyfrowe. Przyjęta 14 grudnia 2022 roku, zastępuje wcześniejszą dyrektywę NIS z 2016 roku, rozszerzając jej zakres i zaostrzając wymagania w zakresie zarządzania ryzykiem oraz zgłaszania incydentów. Nowe regulacje obejmują zarówno podmioty, które były już objęte pierwszą wersją dyrektywy, jak i nowe sektory uznane za kluczowe dla funkcjonowania gospodarki i społeczeństwa. Podmioty zobowiązane do przestrzegania NIS2 muszą wdrożyć kompleksowe procedury obejmujące identyfikację zagrożeń, monitorowanie infrastruktury IT i OT, reagowanie na incydenty oraz regularne audyty bezpieczeństwa. Nowe przepisy mają na celu nie tylko zwiększenie poziomu ochrony systemów informacyjnych, ale również eliminację niespójności w podejściu do cyberbezpieczeństwa pomiędzy krajami członkowskimi.

KONIECZNOŚĆ WPROWADZENIA DYREKTYWY NIS2 WYNIKA Z KILKU KLUCZOWYCH CZYNNIKÓW:

- **Wzrost liczby i skali cyberataków** – w ostatnich latach ataki na kluczową infrastrukturę, instytucje rządowe i firmy prywatne znacząco wzrosły. Szczególne zagrożenie stanowią ataki typu ransomware, phishing oraz włamania do systemów IT, prowadzące do utraty danych i paraliżu operacyjnego organizacji.
- **Postępująca cyfryzacja i wzrost zależności od systemów IT i OT** – automatyzacja procesów produkcyjnych, logistyki i systemów sterowania w przemyśle sprawia, że awarie lub ataki na infrastrukturę operacyjną mogą mieć katastrofalne skutki dla łańcuchów dostaw i stabilności kluczowych sektorów.
- **Braki i niespójności w pierwszej dyrektywie NIS** – wcześniejsze przepisy pozwalały krajom członkowskim na dużą dowolność we wdrażaniu regulacji, co doprowadziło do znacznych różnic w poziomie zabezpieczeń pomiędzy państwami UE.
- **Zwiększone ryzyko ataków na łańcuchy dostaw** – wzrastająca liczba organizacji korzystających z zewnętrznych dostawców usług IT i oprogramowania sprawia, że cyberprzestępcy coraz częściej atakują dostawców, aby uzyskać dostęp do systemów docelowych organizacji.

Nowe przepisy znacząco zwiększają wymagania wobec firm i instytucji publicznych, które muszą wdrożyć bardziej zaawansowane mechanizmy ochrony oraz stosować rygorystyczne procedury raportowania incydentów. Wprowadzone zmiany obejmują zarówno rozszerzenie katalogu podmiotów objętych regulacją, jak i zaostrzenie zasad zarządzania ryzykiem oraz obowiązków w zakresie zgłaszania naruszeń bezpieczeństwa. Oznacza to również konieczność inwestycji w nowoczesne technologie ochrony IT i OT, rozwój procedur zarządzania ryzykiem oraz zapewnienie zgodności z przepisami w zakresie raportowania incydentów. W kolejnej części raportu zostaną szczegółowo omówione wymagania regulacyjne wynikające z dyrektywy NIS2.

1.2 WYMAGANIA REGULACYJNE

Dyrektywa NIS2 rozszerza zakres podmiotów objętych regulacją i zobowiązują organizacje do wdrożenia zaawansowanych mechanizmów zarządzania ryzykiem cybernetycznym, monitorowania zagrożeń oraz raportowania incydentów. Istotną zmianą w porównaniu do pierwszej dyrektywy NIS jest podział podmiotów na dwie kategorie: podmioty kluczowe oraz podmioty ważne. Te pierwsze to organizacje działające w sektorach o najwyższym znaczeniu dla funkcjonowania państwa, społeczeństwa i gospodarki, takich jak energetyka, transport, ochrona zdrowia, infrastruktura cyfrowa czy dostawy wody. Z uwagi na potencjalnie poważne skutki zakłóceń ich działalności, są one objęte najbardziej rygorystycznymi wymaganiami dyrektywy NIS2. Muszą wdrożyć zaawansowane środki zarządzania ryzykiem cybernetycznym, ustanowić procedury reagowania na incydenty i regularnie raportować naruszenia. Co istotne, podmioty kluczowe podlegają nadzorowi *ex ante*, co oznacza, że organy nadzoru mogą przeprowadzać kontrole i audyty jeszcze przed wystąpieniem jakichkolwiek incydentów, oceniając zgodność z przepisami oraz poziom przygotowania na zagrożenia.

Z kolei podmioty ważne to organizacje, które również pełnią istotną rolę w funkcjonowaniu nowoczesnej gospodarki i społeczeństwa, ale nie są kluczowe z punktu widzenia bezpieczeństwa narodowego lub zdrowia publicznego. Do tej grupy należą m.in. dostawcy usług cyfrowych, firmy kurierskie, producenci sprzętu elektronicznego czy usługodawcy IT działający na rzecz innych firm. Choć również muszą spełniać obowiązki w zakresie zarządzania ryzykiem i raportowania incydentów, ich nadzór ma charakter *ex post* – kontrole są przeprowadzane głównie po wystąpieniu incydentu lub w przypadku podejrzenia naruszeń. Odróżnia je więc przede wszystkim mniejszy zakres nadzoru operacyjnego, choć zakres obowiązków może być zbliżony do tego, jaki mają podmioty kluczowe.

Podmioty objęte dyrektywą NIS2, zarówno kluczowe, jak i ważne, zobowiązane są do wdrożenia kompleksowego systemu zarządzania ryzykiem cybernetycznym. Oznacza to konieczność zastosowania adekwatnych środków technicznych, organizacyjnych i proceduralnych, które umożliwiają skuteczne identyfikowanie, zapobieganie oraz reagowanie na zagrożenia wobec bezpieczeństwa sieci i systemów informacyjnych. Środki te muszą być dostosowane do rodzaju działalności, skali operacji oraz poziomu ryzyka, z jakim wiąże się funkcjonowanie danej organizacji. Wymagana jest również bieżąca aktualizacja polityk bezpieczeństwa oraz ciągłe doskonalenie wdrożonych procedur w oparciu o zmieniające się zagrożenia i nowe standardy.

Jednym z fundamentalnych obowiązków jest raportowanie incydentów bezpieczeństwa w sposób terminowy i szczegółowy. Podmioty muszą zgłaszać istotne naruszenia w trybie etapowym: wstępne powiadomienie do odpowiedniego CSIRT lub organu nadzoru powinno nastąpić w ciągu 24 godzin od wykrycia incydentu, pełne zgłoszenie – w ciągu 72 godzin. Raport końcowy należy przedłożyć w terminie do jednego miesiąca, jeśli wymaga tego sytuacja. Taki model raportowania ma na celu umożliwienie natychmiastowej reakcji ze strony organów nadzorczych oraz lepszą koordynację działań w sytuacjach, które mogą mieć wpływ na infrastrukturę krytyczną lub bezpieczeństwo wewnętrzne. Ponadto, raporty te powinny zawierać szczegółowe informacje o charakterze incydentu, jego przyczynach, zastosowanych środkach zaradczych oraz wpływie na ciągłość działania organizacji.

Ważnym aspektem obowiązków wynikających z dyrektywy NIS2 jest systematyczne dokumentowanie i utrzymywanie szczegółowej analizy ryzyka cyberbezpieczeństwa. Oznacza to, że każda organizacja powinna zidentyfikować swoje zasoby informacyjne, ocenić ich znaczenie dla ciągłości działania oraz określić potencjalne zagrożenia i podatności, którym te zasoby mogą podlegać. Taka analiza powinna uwzględniać zarówno ryzyka techniczne (np. awarie systemów, luki w oprogramowaniu), jak i organizacyjne (np. brak procedur, niewystarczające przeszkolenie personelu). Na tej podstawie opracowuje się strategię reagowania, czyli konkretne środki zapobiegawcze, wykrywające i ograniczające skutki ewentualnych incydentów.

Równolegle organizacja musi wdrożyć i utrzymywać formalną politykę bezpieczeństwa informacji, która stanowi zestaw zasad i procedur regulujących sposób zarządzania dostępem do systemów i danych, ochrony przed nieautoryzowanym dostępem, szyfrowania informacji wrażliwych, aktualizacji oprogramowania, jak również postępowania w przypadku wykrycia incydentu. W zakres tej polityki wchodzą także obowiązki związane z kontrolą dostępu (np. nadawanie uprawnień zgodnie z zasadą najmniejszych przywilejów), zarządzaniem podatnościami (regularne aktualizacje i łatki bezpieczeństwa), audytem wewnętrznym oraz bieżącym monitorowaniem systemów informatycznych. Co więcej, organizacje muszą przygotować i testować plany ciągłości działania (Business Continuity Plans – BCP) oraz plany odtwarzania po awarii (Disaster Recovery Plans – DRP), które zapewniają możliwość utrzymania operacyjności lub szybkiego przywrócenia kluczowych usług po ataku cybernetycznym, katastrofie technicznej lub błędzie ludzkim.

Kolejnym obowiązkiem jest zarządzanie ryzykiem w łańcuchu dostaw, co oznacza konieczność weryfikacji poziomu bezpieczeństwa dostawców, w szczególności tych świadczących usługi ICT lub mających dostęp do infrastruktury informatycznej organizacji. W praktyce oznacza to konieczność wprowadzania wymogów bezpieczeństwa do umów z dostawcami, monitorowania ich zgodności oraz reagowania na zagrożenia pochodzące od stron trzecich. Dyrektywa podkreśla również znaczenie budowania kultury cyberbezpieczeństwa w organizacji – stąd obowiązek regularnego szkolenia pracowników oraz kadry zarządzającej, dostosowanego do poziomu odpowiedzialności i dostępu do informacji.

W niektórych przypadkach, szczególnie w dużych organizacjach lub tych działających w sektorach o podwyższonym ryzyku, wymagane jest formalne wyznaczenie osoby lub zespołu odpowiedzialnego za cyberbezpieczeństwo. Może to być wewnętrzny dział bezpieczeństwa IT albo zewnętrzny partner świadczący usługi w tym zakresie. Niezależnie od przyjętego modelu, istotne jest, aby odpowiedzialność za bezpieczeństwo była jasno określona i przypisana, a procesy były nadzorowane przez kompetentny personel. Ponadto wszystkie podmioty objęte dyrektywą NIS2 podlegają kontroli i mogą zostać wezwane do przedstawienia dowodów zgodności z wymaganiami – zarówno w zakresie wdrożonych środków technicznych, jak i dokumentacji oraz reakcji na potencjalne incydenty. Taki system nadzoru ma na celu nie tylko ocenę zgodności, ale również wspieranie organizacji w doskonaleniu procesów bezpieczeństwa i lepszym przygotowaniu na realne zagrożenia.

1.3 ZAKRES OBOWIĄZYWANIA DYREKTYWY W POLSCE

W Polsce dyrektywa NIS2 zostanie wdrożona poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC), która stanowi podstawowy akt prawny regulujący kwestie bezpieczeństwa informacyjnego na poziomie krajowym. Choć termin implementacji wyznaczono na 17 października 2024 roku, proces legislacyjny wciąż trwa. Zakres regulacji będzie znacznie szerszy niż dotychczas – według szacunków obejmie około 38 tysięcy podmiotów z 17 sektorów gospodarki, w tym m.in. energetyki, transportu, bankowości, zdrowia, infrastruktury cyfrowej, administracji publicznej, przemysłu chemicznego, gospodarki odpadami, a także szeroko pojętych usług cyfrowych i ICT.

Obowiązki wynikające z NIS2 dotkną przede wszystkim średnich i dużych przedsiębiorstw, czyli tych zatrudniających co najmniej 50 pracowników lub osiągających roczny obrót przekraczający 10 milionów euro. Jednak w niektórych przypadkach – jak np. dostawcy usług DNS, rejestratorzy domen najwyższego poziomu (TLD), operatorzy usług zaufania czy niektóre instytucje finansowe – obowiązki będą obowiązywać niezależnie od wielkości organizacji, ze względu na ich strategiczne znaczenie dla bezpieczeństwa cyfrowego państwa.

Polski ustawodawca przewiduje również wprowadzenie mechanizmów wsparcia dla przedsiębiorstw, w tym konsultacji sektorowych oraz kampanii edukacyjnych, które mają na celu zwiększenie świadomości zagrożeń i ułatwienie wdrożenia nowych obowiązków. Przedsiębiorstwa powinny już teraz rozpocząć prace przygotowawcze, w szczególności dokonać oceny dojrzałości swoich systemów bezpieczeństwa, wdrożyć lub zaktualizować polityki zarządzania ryzykiem, zautomatyzować procesy reagowania na incydenty oraz przeszkolić personel odpowiedzialny za infrastrukturę IT. Wdrożenie dyrektywy NIS2 w Polsce będzie więc wymagało nie tylko dostosowania się do nowych przepisów, ale również przemyślanej transformacji kultury organizacyjnej w kierunku większej odporności cyfrowej.

INSTYTUCJE NADZORUJĄCE WDROŻENIE DYREKTYWY W POLSCE

Za nadzór nad wdrożeniem i realizacją przepisów dyrektywy NIS2 w Polsce odpowiada szereg kluczowych instytucji państwowych, które współpracują w ramach krajowego systemu cyberbezpieczeństwa. Główną rolę koordynacyjną pełni **Ministerstwo Cyfryzacji**, które odpowiada za przygotowanie i nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), a także za prowadzenie krajowej polityki w zakresie bezpieczeństwa cyfrowego. Ministerstwo to opracowuje również strategiczne dokumenty, organizuje konsultacje z sektorem prywatnym i publicznym oraz współpracuje z organami unijnymi w zakresie implementacji NIS2.

Rządowe Centrum Bezpieczeństwa (RCB) odpowiada za koordynację działań związanych z ochroną infrastruktury krytycznej, w tym również reagowanie na incydenty cybernetyczne, które mogą zagrozić ciągłości działania kluczowych usług. W przypadku zagrożeń o charakterze międzysektorowym lub przekraczającym kompetencje jednej instytucji, RCB pełni funkcję organizacyjną i wspiera wymianę informacji między podmiotami.

Ważną rolę w reagowaniu na incydenty i obsłudze zgłoszeń pełnią również trzy zespoły CSIRT (Computer Security Incident Response Team), działające na poziomie krajowym. **CSIRT NASK (CERT Polska)**, działający w ramach Naukowej i Akademickiej Sieci Komputerowej, obsługuje incydenty w sektorze cywilnym – zarówno publicznym, jak i prywatnym – oraz monitoruje zagrożenia w skali krajowej. **CSIRT GOV**, funkcjonujący w strukturach Kancelarii Prezesa Rady Ministrów (KPRM), zajmuje się bezpieczeństwem systemów teleinformatycznych administracji rządowej. Z kolei **CSIRT MON**, działający w strukturach Ministerstwa Obrony Narodowej, odpowiada za bezpieczeństwo teleinformatyczne sił zbrojnych oraz instytucji podległych MON.

W ramach wdrażania dyrektywy NIS2 planowane jest również umocnienie współpracy między wskazanymi instytucjami, m.in. poprzez wspólne procedury reagowania, wymianę informacji o zagrożeniach oraz wsparcie podmiotów zobowiązanych do raportowania incydentów. Jednym z kluczowych elementów nowego modelu bezpieczeństwa będzie utworzenie **tzw. CSIRT-ów sektorowych** – wyspecjalizowanych zespołów reagowania na incydenty, działających w ramach wybranych sektorów gospodarki, takich jak energetyka, zdrowie, transport czy finanse. Ich zadaniem będzie nie tylko bieżące monitorowanie zagrożeń i wsparcie techniczne dla podmiotów z danego sektora, ale także dostosowywanie polityk bezpieczeństwa do specyfiki branżowej oraz koordynacja działań w przypadku incydentów o charakterze sektorowym. Taka struktura ma na celu zwiększenie efektywności reakcji na zagrożenia, skrócenie czasu potrzebnego na obsługę incydentów oraz wzmocnienie komunikacji pomiędzy podmiotami publicznymi a prywatnymi. Docelowo system nadzoru ma umożliwiać skuteczne i szybkie reagowanie na incydenty w skali ogólnokrajowej, a także lepsze przygotowanie instytucji i przedsiębiorstw do zmieniającego się krajobrazu zagrożeń cyfrowych.

WYZWANIA ZWIĄZANE Z WDROŻENIEM DYREKTYWY W POLSCE

Polska stoi przed kilkoma wyzwaniami związanymi z wdrożeniem NIS2. Jednym z nich jest konieczność dostosowania ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) do nowych przepisów. Obecnie trwają prace legislacyjne mające na celu integrację regulacji unijnych z polskim systemem prawnym, co obejmuje m.in. określenie zakresu sankcji za nieprzestrzeganie przepisów oraz mechanizmów nadzoru nad firmami zobowiązanymi do przestrzegania NIS2.

Kolejnym wyzwaniem jest podniesienie poziomu świadomości w zakresie cyberbezpieczeństwa, zarówno w sektorze publicznym, jak i prywatnym. Wiele organizacji będzie musiało wdrożyć nowe polityki bezpieczeństwa, przeszkolić personel oraz zainwestować w nowe technologie ochrony przed cyberzagrożeniami.

Warto zaznaczyć, że polska implementacja będzie wprost oparta na zapisach dyrektywy NIS2, obejmując wymagane przez nią obowiązki w zakresie zarządzania ryzykiem, raportowania incydentów, nadzoru i kar. Jednocześnie projekt ustawy daje możliwość wprowadzenia przepisów wykraczających poza minimalne standardy przewidziane przez dyrektywę – np. poprzez nałożenie bardziej szczegółowych obowiązków branżowych, wymagań audytowych lub wskazania konkretnych norm technicznych do stosowania. Taki kierunek budzi mieszane reakcje – z jednej strony ma na celu

zwiększenie krajowej odporności cyfrowej, z drugiej może wiązać się z wyższymi kosztami dostosowania dla przedsiębiorstw.

1.4 TERMINY I KONSEKWENCJE BRAKU WDROŻENIA

Dyrektywa NIS2 weszła w życie 16 stycznia 2023 roku, a państwa członkowskie Unii Europejskiej zostały zobowiązane do jej pełnej implementacji do 17 października 2024 roku. W Polsce wdrożenie nowych przepisów ma nastąpić poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC), jednak prace legislacyjne nadal trwają.

Opóźnienie to może skutkować formalnym postępowaniem naruszeniowym ze strony Komisji Europejskiej, a w dalszej kolejności – skierowaniem sprawy do Trybunału Sprawiedliwości Unii Europejskiej i nałożeniem kar finansowych na państwo członkowskie. Niewdrożenie przepisów na poziomie krajowym opóźnia także działania przygotowawcze po stronie przedsiębiorstw, które w dalszym ciągu nie znają ostatecznego brzmienia wymogów, co utrudnia im wdrożenie odpowiednich procedur i zabezpieczeń.

Jednocześnie, kiedy ustawa zacznie obowiązywać, objęte nią organizacje będą musiały liczyć się z poważnymi konsekwencjami za brak zgodności. Dla podmiotów kluczowych przewidziano kary finansowe do 10 milionów euro lub 2% globalnego rocznego obrotu, a dla podmiotów ważnych – do 7 milionów euro lub 1,4% obrotu, w zależności od tego, która kwota będzie wyższa. Dodatkowo, organy nadzoru będą mogły nakładać sankcje administracyjne, nakazy wdrożenia określonych działań naprawczych, a nawet pociągać kadrę zarządzającą do osobistej odpowiedzialności w przypadku rażących zaniedbań.

Niezgłoszenie poważnego incydentu w wymaganym terminie, brak współpracy z instytucjami nadzoru czy niedopełnienie obowiązków w zakresie zarządzania ryzykiem mogą skutkować czasowym ograniczeniem działalności lub innymi restrykcjami administracyjnymi. W praktyce oznacza to, że dyrektywa NIS2 nie tylko wymusza techniczne podniesienie poziomu bezpieczeństwa, ale również wprowadza nową kulturę odpowiedzialności za cyberbezpieczeństwo – zarówno na poziomie operacyjnym, jak i zarządczym. Organizacje, które nie dostosują się do wymagań wynikających z dyrektywy NIS2 w przewidzianym terminie, mogą nie tylko zostać objęte sankcjami administracyjnymi i finansowymi, ale również utracić możliwość udziału w przetargach publicznych oraz zawierania kontraktów z innymi podmiotami objętymi regulacją. Może to mieć bezpośredni wpływ na ich stabilność operacyjną i sytuację finansową. Niezależnie od sankcji prawnych, brak wdrożenia odpowiednich środków ochrony zwiększa realne ryzyko poważnych konsekwencji operacyjnych, takich jak skuteczne ataki cybernetyczne prowadzące do utraty danych, przestojów w działalności czy kompromitacji kluczowych systemów. Tego rodzaju incydenty mogą także prowadzić do spadku zaufania ze strony klientów, partnerów biznesowych oraz opinii publicznej, co długofalowo może negatywnie wpłynąć na pozycję rynkową i reputację firmy.

Dostosowanie się do NIS2 jest więc nie tylko obowiązkiem prawnym, ale także strategiczną koniecznością dla organizacji chcących zabezpieczyć swoje systemy i zapewnić ciągłość działania w dynamicznym środowisku zagrożeń cybernetycznych.

W kolejnej części raportu zostaną omówione środki zarządzania ryzykiem i obowiązki organizacyjne wynikające z dyrektywy NIS2.

2.

ANALIZA STANU WDROŻENIA NIS2 W POLSCE

Dyrektywa NIS2, której termin wdrożenia przez państwa członkowskie Unii Europejskiej upłynął 17 października 2024 roku, wymaga dostosowania przepisów krajowych oraz wdrożenia nowych mechanizmów cyberbezpieczeństwa przez podmioty objęte regulacją. W Polsce proces ten przebiega w kilku etapach, obejmujących dostosowanie ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), organizację instytucji nadzorujących oraz przygotowanie podmiotów zobowiązanych do spełnienia nowych wymagań.

Na potrzeby niniejszej analizy przeprowadzono badania sektora publicznego i prywatnego w Polsce oraz porównano ich wyniki z danymi zebranymi na poziomie unijnym. Analiza uwzględnia stopień zaawansowania wdrożenia regulacji w różnych sektorach oraz ocenę gotowości organizacji do spełnienia wymogów NIS2.

2.1 METODOLOGIA BADANIA

W celu oceny stopnia wdrożenia dyrektywy NIS2 w Polsce zastosowano wieloetapową metodologię badawczą, obejmującą:

- **Analizę dokumentów i projektów legislacyjnych** – przegląd dotychczasowych aktów prawnych, w tym nowelizacji ustawy o KSC oraz projektów rządowych dotyczących cyberbezpieczeństwa.
- **Ankietę przeprowadzoną wśród podmiotów objętych regulacją** – badanie obejmowało organizacje z sektorów energetyki, transportu, ochrony zdrowia, administracji publicznej, usług cyfrowych oraz telekomunikacji. Celem było określenie poziomu ich przygotowania do spełnienia nowych wymagań oraz zidentyfikowanie kluczowych wyzwań we wdrażaniu dyrektywy.
- **Porównanie z danymi z innych krajów UE** – analiza raportów Komisji Europejskiej oraz organizacji zajmujących się cyberbezpieczeństwem w celu oceny, jak Polska wypada na tle innych państw członkowskich.

Badanie miało na celu ocenę poziomu gotowości sektora publicznego i prywatnego oraz wskazanie kluczowych barier i wyzwań związanych z implementacją NIS2 w Polsce.

2.2 JAK ZBIERALIŚMY DANE?

W ramach analizy wdrożenia NIS2 w Polsce przeprowadzono ogólnopolskie badanie ankietowe, w którym udział wzięły 40 organizacji z sektorów objętych regulacją. Respondenci odpowiadali na pytania dotyczące:

- Stopnia wdrożenia polityk cyberbezpieczeństwa zgodnych z NIS2,
- Przygotowania do obowiązkowego raportowania incydentów,
- Inwestycji w systemy monitorowania zagrożeń i reagowania na incydenty,
- Współpracy z instytucjami krajowymi (CERT, CSIRT, regulatorzy sektorowi),
- Wyzwań w implementacji nowych regulacji.

Dodatkowo przeprowadzono 10 wywiadów pogłębionych z ekspertami z instytucji nadzorujących oraz firm wdrażających regulacje w praktyce. Uzyskane dane pozwoliły na ocenę realnego poziomu przygotowania podmiotów do spełnienia wymogów NIS2 oraz wskazanie obszarów, które wymagają dodatkowego wsparcia.

2.3 STAN WDROŻENIA NIS2 W POLSCE NA TLE UE

Polska nie zdołała wdrożyć dyrektywy NIS2 w ustawowym terminie, który upłynął 17 października 2024 roku. Obecnie trwają prace nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa (KSC), mające na celu implementację nowych przepisów unijnych. Mimo zaawansowanych przygotowań, projekt ustawy nadal oczekuje na przyjęcie przez Radę Ministrów i przekazanie do Sejmu, co oznacza, że wejście w życie przepisów najprawdopodobniej nastąpi dopiero w pierwszej połowie 2025 roku.

Na tle innych państw Unii Europejskiej Polska znajduje się w grupie krajów opóźnionych we wdrażaniu NIS2. Do października 2024 roku transpozycji dyrektywy dokonały m.in. Belgia, Chorwacja, Grecja, Węgry, Łotwa i Litwa, a wiele innych państw – w tym Niemcy, Francja czy Włochy – znajduje się na zaawansowanym etapie prac parlamentarnych. Tymczasem brak krajowych regulacji w Polsce opóźnia działania przygotowawcze po stronie przedsiębiorstw, które nie są jeszcze zobowiązane formalnie do wdrożenia wymogów, mimo że te obowiązują już na poziomie unijnym.

Analiza wyników ankiety oraz raportów unijnych pokazuje, że Polska znajduje się na średnim poziomie zaawansowania we wdrażaniu NIS2, w porównaniu do innych krajów UE. W kluczowych aspektach wdrożenia Polska wypada następująco:

- **Adaptacja przepisów krajowych** – projekt nowelizacji ustawy o KSC został przygotowany, ale wciąż trwają prace legislacyjne. W wielu krajach, takich jak Niemcy, Francja czy Holandia, proces dostosowywania przepisów jest bardziej zaawansowany.
- **Gotowość organizacji do spełnienia wymagań** – tylko 34% polskich firm i instytucji deklaruje pełną gotowość do wdrożenia nowych regulacji, podczas gdy w krajach skandynawskich odsetek ten wynosi powyżej 50%.
- **Mechanizmy raportowania incydentów** – 58% organizacji nie posiada jeszcze wdrożonych systemów umożliwiających automatyczne zgłaszanie incydentów do organów nadzorczych, co może stanowić istotny problem po wejściu w życie nowych przepisów.
- **Inwestycje w cyberbezpieczeństwo** – średni wzrost budżetów na ochronę infrastruktury IT i OT w Polsce wyniósł 14% w ciągu ostatnich dwóch lat, podczas gdy w Niemczech czy Francji organizacje przeznaczają na ten cel o 20–30% więcej.
- **Problemy kadrowe** – brak wykwalifikowanych specjalistów ds. cyberbezpieczeństwa jest wskazywany jako kluczowy problem przez 62% organizacji w Polsce, co jest wynikiem zbliżonym do średniej unijnej (około 60%).

Wyniki analizy wskazują, że choć Polska podjęła szereg działań mających na celu wdrożenie dyrektywy NIS2, wciąż istnieją istotne luki, które opóźniają pełne dostosowanie się do nowych wymogów. Kluczowe wyzwania obejmują konieczność przyspieszenia legislacji, wdrożenie skutecznych systemów raportowania oraz zwiększenie inwestycji w obszar cyberbezpieczeństwa.

W kolejnej części raportu zostaną omówione konkretne środki zarządzania ryzykiem oraz obowiązki organizacyjne wynikające z dyrektywy NIS2, a także ich wpływ na działalność podmiotów zobowiązanych do przestrzegania nowych regulacji.

2.4 OBECNY POZIOM ZGODNOŚCI FIRM Z NIS2

Poziom zgodności firm z dyrektywą NIS2 w Polsce znacząco różni się w zależności od sektora działalności. Wyniki przeprowadzonych badań i ankiet wskazują, że większość organizacji nadal znajduje się na etapie dostosowywania się do nowych regulacji, a tylko niewielka część spełnia już wszystkie wymagania. Wdrożenie nowych procedur zarządzania ryzykiem, raportowania incydentów i monitorowania infrastruktury IT i OT okazuje się wyzwaniem, zwłaszcza dla podmiotów, które wcześniej nie podlegały regulacjom w zakresie cyberbezpieczeństwa.

W ramach analizy oceniono stopień gotowości różnych sektorów gospodarki na wdrożenie przepisów NIS2 oraz zidentyfikowano główne bariery, które utrudniają pełne dostosowanie się do nowych wymogów.

2.5 JAKIE BRANŻE SĄ NAJBARDZIEJ ZAAWANSOWANE W IMPLEMENTACJI?

Najwyższy poziom zgodności z wymogami dyrektywy NIS2 wykazują sektory, które już wcześniej były objęte ścisłymi regulacjami dotyczącymi cyberbezpieczeństwa oraz zarządzania ryzykiem IT. Do najbardziej zaawansowanych branż należą:

- **Energetyka** – operatorzy systemów elektroenergetycznych, gazowych i naftowych posiadają rozwinięte struktury bezpieczeństwa IT oraz działające systemy monitorowania zagrożeń. W większości tych organizacji istnieją już zespoły ds. cyberbezpieczeństwa, a także procedury reagowania na incydenty.
- **Telekomunikacja** – duże firmy telekomunikacyjne, takie jak operatorzy sieci komórkowych i dostawcy internetu, od lat wdrażają systemy zarządzania ryzykiem i ochrony infrastruktury. Dyrektywa NIS2 wprowadza dla nich dodatkowe wymagania, ale większość firm z tego sektora jest stosunkowo dobrze przygotowana.
- **Usługi cyfrowe i operatorzy chmury** – globalni dostawcy chmury obliczeniowej i centrów danych wdrażają rygorystyczne procedury bezpieczeństwa, co pozwala im spełnić wymagania dyrektywy.
- **Sektor finansowy (pośrednio objęty NIS2 poprzez dostawców ICT)** – choć banki i instytucje finansowe są regulowane głównie przez DORA (Digital Operational Resilience Act), ich dostawcy IT podlegają NIS2 i już teraz realizują część wymaganych działań w zakresie zarządzania ryzykiem i cyberbezpieczeństwa.

2.6 JAKIE SEKTORY MAJĄ NAJWIĘKSZE OPÓŹNIENIA I DLACZEGO?

Branże, które dopiero rozpoczynają wdrażanie regulacji NIS2, to przede wszystkim te, które wcześniej nie były objęte ścisłymi regulacjami dotyczącymi cyberbezpieczeństwa. Największe opóźnienia odnotowano w następujących sektorach:

- **Administracja publiczna** – wiele instytucji państwowych i samorządowych dopiero zaczyna wdrażanie mechanizmów zgodnych z NIS2. Problemy wynikają z braku jednolitych standardów, ograniczonych budżetów oraz wolnego tempa legislacji.
- **Ochrona zdrowia** – szpitale, laboratoria diagnostyczne i dostawcy usług medycznych często dysponują przestarzałymi systemami IT, które wymagają modernizacji w celu spełnienia nowych standardów bezpieczeństwa. Dodatkowo, personel medyczny w wielu przypadkach nie jest przeszkolony w zakresie cyberbezpieczeństwa.
- **Przemysł i produkcja** – firmy z sektorów przemysłowych, zwłaszcza z branży chemicznej, farmaceutycznej i spożywczej, nie miały wcześniej obowiązku wdrażania zaawansowanych systemów ochrony IT i OT. Wiele z nich dopiero opracowuje strategię cyberbezpieczeństwa dostosowaną do nowych regulacji, a systemy OT nie ułatwiają im tego zadania.
- **Sektor wodociągowy i gospodarka odpadami** – firmy zajmujące się infrastrukturą wodną i odpadami są słabo przygotowane na wdrożenie mechanizmów raportowania incydentów i monitorowania infrastruktury IT.

2.7 KLUCZOWE BARIERY WE WDRAŻANIU NIS2

Analiza danych zebranych w ramach badania wskazuje, że główne wyzwania związane z wdrażaniem NIS2 w Polsce dotyczą zarówno aspektów organizacyjnych, jak i technologicznych. Najczęściej wskazywane bariery obejmują:

- **Brak świadomości i wiedzy na temat nowych regulacji** – aż 47% organizacji objętych regulacją NIS2 wskazuje, że nie posiada wystarczających informacji na temat wymagań dyrektywy ani ich konsekwencji. Dotyczy to zwłaszcza mniejszych podmiotów oraz sektora administracji publicznej.
- **Problemy budżetowe** – **55% organizacji uznaje ograniczone środki finansowe jako główną przeszkodę we wdrażaniu nowych systemów cyberbezpieczeństwa.** W wielu przypadkach modernizacja infrastruktury IT i OT wymaga dużych inwestycji, na które firmy i instytucje nie mają wystarczających funduszy.
- **Brak specjalistów ds. cyberbezpieczeństwa** – niedobór wykwalifikowanych pracowników jest jednym z największych problemów w Polsce i całej UE. **Aż 62% firm i instytucji wskazuje, że brakuje im ekspertów, którzy mogliby przeprowadzić proces wdrożenia NIS2** i zapewnić zgodność z nowymi wymaganiami.

- **Problemy techniczne i przestarzała infrastruktura IT** – szczególnie dotyczy to sektora zdrowia oraz administracji publicznej, gdzie starsze systemy informatyczne nie spełniają standardów cyberbezpieczeństwa i wymagają gruntownej modernizacji.
- **Brak jednoznacznych wytycznych** – organizacje podkreślają, że przepisy krajowe nadal są w trakcie dostosowywania, co utrudnia planowanie wdrożenia i inwestycji. Opóźnienia w uchwalaniu przepisów wykonawczych sprawiają, że firmy nie mają pełnej jasności, jakie konkretne działania powinny podjąć.

Obecny poziom zgodności firm i instytucji z dyrektywą NIS2 w Polsce wskazuje na duże rozbieżności między sektorami. Podczas gdy energetyka, telekomunikacja i usługi cyfrowe są stosunkowo dobrze przygotowane, branże takie jak administracja publiczna, ochrona zdrowia i przemysł nadal mają poważne braki w dostosowaniu się do nowych regulacji.

Największymi wyzwaniami dla organizacji pozostają brak wykwalifikowanych specjalistów, ograniczone budżety oraz konieczność modernizacji przestarzałej infrastruktury IT i OT. Wdrożenie regulacji NIS2 w Polsce wymaga więc zwiększenia świadomości organizacji, przyspieszenia legislacji krajowej oraz wsparcia dla sektorów o największych trudnościach we wdrażaniu nowych wymogów.

3.

PROCES DOSTOSOWANIA FIRM DO NIS2

3.1 COMPLIANCE – JAK FIRMY POWINNY WDROŻYĆ REGULACJE?

Dostosowanie organizacji do wymagań dyrektywy NIS2 wymaga wdrożenia kompleksowego podejścia do zarządzania cyberbezpieczeństwem, identyfikacji zagrożeń, monitorowania incydentów oraz raportowania naruszeń. Firmy, które podlegają nowym regulacjom, muszą nie tylko wdrożyć odpowiednie technologie ochrony, ale także przyjąć jednolite polityki bezpieczeństwa, zapewnić nadzór nad dostawcami IT oraz przeprowadzać regularne audyty w celu oceny zgodności z przepisami.

WYZNACZENIE ODPOWIEDZIALNOŚCI ZA WDROŻENIE NIS2

Pierwszym krokiem w procesie wdrożenia compliance powinno być wyznaczenie zespołu ds. cyberbezpieczeństwa, w skład którego wejdą przedstawiciele zarządu, działu IT oraz specjaliści ds. ryzyka. Kluczową rolę w organizacji powinna pełnić osoba odpowiedzialna za bezpieczeństwo informacji (Chief Information Security Officer – CISO), której zadaniem jest opracowanie strategii ochrony danych oraz wdrożenie mechanizmów detekcji i reagowania na incydenty. W przypadku większych organizacji konieczne może być również utworzenie zespołu ds. Security Governance, Risk and Compliance (GRC), który będzie odpowiedzialny za monitorowanie polityk cyberbezpieczeństwa, przeprowadzanie audytów wewnętrznych oraz raportowanie postępów wdrażania NIS2 do zarządu.

IDENTYFIKACJA KRYTYCZNYCH ZASOBÓW IT I OT

Drugim kluczowym etapem jest identyfikacja krytycznych zasobów IT i OT, które podlegają regulacjom NIS2. Organizacja powinna przeprowadzić kompleksowy audyt infrastruktury, obejmujący systemy IT, aplikacje biznesowe, centra danych oraz urządzenia IoT i systemy sterowania SCADA. Celem audytu jest określenie, które zasoby wymagają szczególnej ochrony oraz jakie zagrożenia mogą wpłynąć na ich dostępność, integralność lub poufność. Na tym etapie konieczna jest również analiza ryzyka cybernetycznego, która pozwoli określić potencjalne wektory ataków, ocenić skutki incydentów oraz przygotować plany awaryjne na wypadek zagrożeń.

WDROŻENIE POLITYK CYBERBEZPIECZEŃSTWA I KONTROLI DOSTĘPU

Po przeprowadzeniu audytu firma powinna wdrożyć polityki bezpieczeństwa zgodne z międzynarodowymi standardami cyberbezpieczeństwa, takimi jak ISO 27001, NIST CSF czy CIS Controls. W ramach tych działań organizacja musi wdrożyć mechanizmy kontroli dostępu, które zapewnią, że dostęp do krytycznych systemów i danych będzie ograniczony wyłącznie do autoryzowanych użytkowników. Istotnym elementem jest wdrożenie zasady minimalnych uprawnień (Principle of Least Privilege – PoLP) oraz uwierzytelniania wieloskładnikowego (MFA – Multi-Factor Authentication), co pozwoli zabezpieczyć systemy przed nieautoryzowanym dostępem. Ponadto można pokusić się w wprowadzenie zasady Zero Trust, zgodnie z którą każdy użytkownik i urządzenie są traktowane jako potencjalnie niebezpieczne, co wymaga ciągłej weryfikacji tożsamości i monitorowania działań użytkowników. nie jest to jednak jednym z wymogów dyrektywy.

MECHANIZMY WYKRYWANIA I RAPORTOWANIA INCYDENTÓW

Dyrektywa NIS2 nakłada również obowiązek wdrożenia mechanizmów wykrywania i raportowania incydentów cyberbezpieczeństwa. Organizacje muszą opracować procedury, które określą sposób identyfikacji, analizy i reakcji na zagrożenia oraz sposoby zgłaszania naruszeń do odpowiednich ze-

społów reagowania (CSIRT). Zgodnie z wymaganiami NIS2, poważne incydenty muszą być zgłaszane w ciągu 24 godzin od momentu ich wykrycia, co wymaga wdrożenia zautomatyzowanych systemów monitorowania i detekcji zagrożeń, takich jak Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) oraz powołanie do życia zespołu Security Operations Center (SOC), który będzie monitorował bezpieczeństwo organizacji 24/7. Wdrożenie tych rozwiązań umożliwia organizacji ciągłe monitorowanie ruchu sieciowego, analizę podejrzanych aktywności oraz szybką identyfikację anomalii w systemach IT i OT.

ZARZĄDZANIE RYZYKIEM W ŁAŃCUCHU DOSTAW

Aby skutecznie zadbać o zgodność z NIS2, organizacja musi również zarządzać ryzykiem w łańcuchu dostaw, ponieważ dyrektywa nakłada obowiązek monitorowania dostawców IT oraz podmiotów trzecich pod kątem ich zgodności z wymaganiami bezpieczeństwa. Firmy powinny przeprowadzać regularne audyty dostawców, weryfikować ich polityki bezpieczeństwa oraz stosować odpowiednie umowy SLA (Service Level Agreement), które będą regulować standardy cyberbezpieczeństwa. Dodatkowo organizacja powinna wdrożyć politykę Third-Party Risk Management (TPRM), która pozwoli na ciągłe monitorowanie zagrożeń wynikających ze współpracy z podmiotami zewnętrznymi oraz określenie procedur minimalizowania ryzyka ataków pochodzących od dostawców IT.

SZKOLENIE PERSONELU I TESTOWANIE ODPORNOŚCI ORGANIZACJI

Ważnym elementem dostosowania organizacji do NIS2 jest także szkolenie personelu oraz budowanie świadomości cyberbezpieczeństwa wśród pracowników. Organizacje powinny wdrożyć regularne szkolenia dla pracowników IT, zespołów operacyjnych oraz kadry zarządzającej, które będą obejmowały strategie obrony przed atakami cybernetycznymi, zasady rozpoznawania phishingu oraz procedury reagowania na incydenty. Ponadto, organizacje powinny przeprowadzać testy penetracyjne i symulacje cyberataków, aby sprawdzić, jak personel reaguje na realne zagrożenia oraz czy wdrożone mechanizmy ochrony są skuteczne.

ETAPOWE WDRAŻANIE COMPLIANCE ZGODNIE Z NIS2

Wdrożenie compliance zgodne z NIS2 powinno przebiegać etapowo i obejmować fazy przygotowawcze, wdrożeniowe i operacyjne. W pierwszej fazie organizacja powinna przeprowadzić analizę luk oraz zidentyfikować swoje zasoby krytyczne, w drugiej fazie skupić się na wdrażaniu polityk bezpieczeństwa, systemów monitorowania incydentów i kontroli dostępu, natomiast w trzeciej fazie powinna zapewnić ciągłe monitorowanie zgodności oraz regularne testy i audyty wewnętrzne.

3.2 ANALIZA LUK – JAK SPRAWDZIĆ, CZEGO BRAKUJE W ORGANIZACJI?

KROK 1: AUDYT POLITYK I PROCEDUR CYBERBEZPIECZEŃSTWA

Pierwszym krokiem w procesie dostosowania się do wymagań dyrektywy NIS2 powinna być szczegółowa weryfikacja obowiązujących w organizacji polityk i procedur związanych z zarządzaniem cyberbezpieczeństwem. Celem tego przeglądu jest ocena, czy obecne regulacje wewnętrzne są zgodne

z wymaganiami dyrektywy oraz czy zapewniają odpowiedni poziom ochrony. W ramach tej analizy organizacja powinna zweryfikować m.in. procedury zarządzania incydentami – czy istnieją jasno określone mechanizmy wykrywania, analizy i raportowania zagrożeń; zasady kontroli dostępu, w tym stosowanie uwierzytelniania wieloskładnikowego (MFA), zasady najmniejszych uprawnień (PoLP) oraz podziału obowiązków i uprawnień; system zarządzania ryzykiem stron trzecich, obejmujący monitorowanie bezpieczeństwa dostawców IT; a także system zarządzania bezpieczeństwem informacji (SZBI) – najlepiej oparty na międzynarodowych standardach, takich jak ISO/IEC 27001, NIST CSF czy CIS Controls. Należy również ocenić skuteczność procedur związanych z backupem i odtwarzaniem po awarii, w tym regularność tworzenia kopii zapasowych i gotowość do przywrócenia kluczowych danych po incydencie. Brak spójnych, udokumentowanych polityk i procedur cyberbezpieczeństwa stanowi poważne zagrożenie – nie tylko dla ciągłości działania organizacji, ale także w kontekście ryzyka naruszenia danych oraz kar finansowych wynikających z nieprzestrzegania przepisów NIS2.

KROK 2: TECHNICZNA ANALIZA INFRASTRUKTURY IT I OT

Po zakończeniu analizy procedur organizacja powinna przejść do weryfikacji rzeczywistego stanu zabezpieczeń swojej infrastruktury IT i OT. Kluczowym narzędziem w tym zakresie jest audyt techniczny, którego celem jest identyfikacja słabych punktów, mogących zostać wykorzystanych przez cyberprzestępców lub prowadzących do zakłóceń w ciągłości działania. Audyt powinien obejmować ocenę poziomu zabezpieczeń sieci IT i OT, w tym analizę podatności na ataki, skuteczność segmentacji oraz zastosowanie mechanizmów ochronnych, takich jak firewalle i systemy IDS/IPS. Istotnym elementem są również testy penetracyjne oraz działania typu Red Teaming, które poprzez symulację rzeczywistych ataków pozwalają sprawdzić odporność systemów, szybkość reakcji i skuteczność detekcji. Niezbędna jest także analiza konfiguracji serwerów i systemów IT, obejmująca weryfikację poprawności ustawień, aktualizacji oprogramowania, zabezpieczeń antymalware oraz mechanizmów monitorowania logów. Kolejnym obszarem jest monitorowanie zagrożeń w czasie rzeczywistym – organizacja powinna dysponować własnym zespołem SOC lub korzystać z zewnętrznej usługi, która opiera się co najmniej na technologii SIEM i EDR/XDR, umożliwiając bieżącą analizę ruchu sieciowego, działań na stacjach końcowych i wykrywanie anomalii. Ostatnim, ale równie istotnym elementem jest ocena skuteczności systemów backupu i procedur disaster recovery – należy sprawdzić, czy dane są regularnie archiwizowane, a procesy odtwarzania po cyberataku lub awarii są sprawdzone, aktualne i gotowe do wdrożenia w sytuacji kryzysowej.

KROK 3: OCENA KOMPETENCJI PRACOWNIKÓW I ZARZĄDU W ZAKRESIE CYBERBEZPIECZEŃSTWA

Zgodnie z wymaganiami dyrektywy NIS2, organizacja musi zadbać o to, by zarówno pracownicy, jak i kadra zarządzająca posiadali odpowiednią wiedzę i świadomość w zakresie cyberbezpieczeństwa. W ramach analizy luk warto przeprowadzić testy i ankiety wśród pracowników, które pozwolą ocenić ich zdolność do rozpoznawania zagrożeń – takich jak ataki phishingowe – oraz znajomość procedur postępowania w przypadku wykrycia incydentu. Równocześnie należy ocenić, na ile zarząd jest przygotowany do podejmowania decyzji w obszarze cyberbezpieczeństwa na poziomie strategicznym oraz czy posiada wystarczającą wiedzę do zarządzania ryzykiem cyfrowym. Kluczowym elementem oceny jest również weryfikacja, czy organizacja prowadzi regularne szkolenia, warsztaty i kampanie podnoszące świadomość wśród pracowników. Braki w edukacji i świadomości cyberzagrożeń

stanowią jedno z najpoważniejszych ryzyk – nawet najbardziej zaawansowane systemy techniczne mogą zostać obejście w wyniku błędu ludzkiego lub niewłaściwej reakcji na incydent.

KROK 4: RAPORTOWANIE WYNIKÓW ANALIZY LUK I OKREŚLENIE PRIORYTETÓW

Po zakończeniu szczegółowej analizy stanu cyberbezpieczeństwa organizacja powinna opracować raport podsumowujący, który jasno określi kluczowe obszary wymagające poprawy w kontekście zgodności z dyrektywą NIS2. Dokument ten powinien zawierać wykaz zidentyfikowanych luk wraz z oceną ich wpływu na bezpieczeństwo organizacji, wskazując, które z nich mogą stanowić bezpośrednie zagrożenie dla ciągłości działania lub poufności danych. Istotnym elementem raportu są rekomendacje dotyczące działań naprawczych, podzielone na etapy krótkoterminowe, średnioterminowe i długoterminowe, co pozwala na efektywne planowanie wdrożeń. Należy również określić priorytety w zakresie zgodności, szczególnie w obszarach wymagających natychmiastowych działań – takich jak brak procedur raportowania incydentów, niezaadresowane podatności czy niewystarczające mechanizmy ochrony przed atakami typu ransomware. Raport powinien także zawierać szacunkowy budżet oraz harmonogram wdrożenia wymaganych zmian, tak aby umożliwić skuteczne zaplanowanie zasobów i terminową realizację działań dostosowawczych do wymogów NIS2.

3.3 PLAN WDROŻENIA NIS2 – ROADMAPA COMPLIANCE

FAZA 1: PRZYGOTOWANIE DO WDROŻENIA (0–3 MIESIĄCE)

Na tym etapie organizacja powinna skupić się na ocenie obecnego poziomu zgodności oraz wyznaczeniu kluczowych zasobów i obszarów wymagających dostosowania.

- **Powołanie zespołu ds. compliance i cyberbezpieczeństwa** – organizacja powinna wyznaczyć osoby odpowiedzialne za wdrożenie NIS2, w tym Chief Information Security Officer (CISO) oraz zespół ds. Security Governance, Risk and Compliance (GRC).
- **Zdefiniowanie zakresu regulacji** – określenie, które systemy, procesy i zasoby podlegają dyrektywie, m.in. infrastruktura IT, OT, aplikacje biznesowe, usługi w chmurze, systemy produkcyjne.
- **Przeprowadzenie analizy luk (gap analysis)** – identyfikacja braków w zakresie technologii, polityk bezpieczeństwa, procesów zarządzania ryzykiem i gotowości do raportowania incydentów.
- **Zebranie wymagań regulacyjnych i branżowych** – organizacja powinna dostosować swoje procedury do wytycznych krajowych regulatorów, a wzorować się na standardach takich jak np. ISO 27001.

FAZA 2: WDROŻENIE KLUCZOWYCH MECHANIZMÓW ZABEZPIECZEŃ (3–9 MIESIĘCY)

Po dokonaniu analizy luk organizacja powinna rozpocząć wdrażanie mechanizmów technicznych i proceduralnych, które zapewnią zgodność z regulacjami NIS2.

- **Zarządzanie ryzykiem i wdrożenie polityk bezpieczeństwa**
  - ✓ Wdrożenie polityk bezpieczeństwa informacji oraz procedur dotyczących zarządzania dostępem, ochrony danych i raportowania incydentów.
  - ✓ Ustalenie strategii Disaster Recovery i Business Continuity Plan (BCP) w celu zapewnienia ciągłości działania.
  - ✓ Implementacja reguł bezpieczeństwa, uwzględniających segmentację sieci i zasadę najmniejszych uprawnień.
  - ✓ Monitoring sieci i analityka zagrożeń – wdrożenie systemów SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response) lub XDR (Extended Detection and Response).
  - ✓ Security Operations Center (SOC) – uruchomienie wewnętrznego lub zewnętrznego zespołu w celu stałego monitorowania zagrożeń, analizy anomalii i reagowania na incydenty.
  - ✓ Raportowanie incydentów do CSIRT – wdrożenie mechanizmów zgłaszania incydentów zgodnie z wymogiem wczesnego ostrzegania w ciągu 24 godzin.
  - ✓ Zabezpieczenie systemów IT i OT – wdrożenie IDS/IPS, MFA, VPN oraz polityki bezpieczeństwa dla dostawców usług w chmurze.

FAZA 3: SZKOLENIA I WDRAŻANIE POLITYK ZARZĄDZANIA RYZYKIEM (9–12 MIESIĘCY)

Po wdrożeniu technicznych zabezpieczeń organizacja powinna skupić się na rozwijaniu kompetencji pracowników oraz wdrożeniu procesów zarządzania ryzykiem na poziomie strategicznym.

- **Szkolenia z cyberbezpieczeństwa dla pracowników i zarządu**
  - ✓ Warsztaty z rozpoznawania zagrożeń, np. phishingu oraz reagowania na incydenty.
  - ✓ Szkolenia dla kadry zarządzającej na temat ryzyka cybernetycznego i odpowiedzialności za NIS2.
  - ✓ Dedykowane szkolenia dla osób będących częścią SOC – z analizy zagrożeń, rodzajów ataków, metod ich detekcji oraz powstrzymywania,
  - ✓ Testy odporności organizacji na cyberataki – przeprowadzanie Red Teaming, testów penetracyjnych i symulacji ataków ransomware.
- **Zarządzanie ryzykiem w łańcuchu dostaw IT**
  - ✓ Audyty dostawców usług IT – weryfikacja zgodności partnerów biznesowych z NIS2.
  - ✓ Wdrożenie umów SLA (Service Level Agreement), które regulują standardy bezpieczeństwa dostawców.

✓ Ocena podatności partnerów zewnętrznych – wdrożenie narzędzi do monitorowania łańcucha dostaw pod kątem cyberzagrożeń.

FAZA 4: MONITOROWANIE ZGODNOŚCI I AUDYTY WEWNĘTRZNE (12+ MIESIĘCY I NA BIEŻĄCO)

Ostatni etap wdrożenia polega na ciągłym monitorowaniu bezpieczeństwa organizacji, ocenie skuteczności wdrożonych mechanizmów oraz dostosowywaniu strategii cyberbezpieczeństwa do zmieniających się zagrożeń.

- **Audyty wewnętrzne i testy zgodności**

  ✓ Regularne testy penetracyjne oraz analiza odporności organizacji na zagrożenia.

  ✓ Okresowe przeglądy polityk bezpieczeństwa, procedur zarządzania ryzykiem i zgodności z regulacjami.

  ✓ Weryfikacja gotowości do raportowania incydentów – sprawdzenie mechanizmów wykrywania i zgłaszania naruszeń do CSIRT.

- **Doskonalenie strategii cyberbezpieczeństwa**

  ✓ Adaptacja nowych technologii ochrony,

  ✓ Rozwijanie kompetencji zespołu SOC, aby mogli rozszerzać i doskonalić swoje możliwości detekcji,

  ✓ Stałe aktualizowanie strategii zgodności w oparciu o nowe przepisy oraz zmieniające się zagrożenia.

  ✓ Utrzymywanie programu ciągłego doskonalenia i adaptacji polityk bezpieczeństwa.

3.4 NOWE OBOWIĄZKI ZARZĄDU

Wraz z wejściem w życie dyrektywy NIS2, organizacje objęte regulacją muszą dostosować swoje struktury zarządzania cyberbezpieczeństwem, co oznacza nowe obowiązki dla zarządu oraz rosnącą rolę Chief Information Security Officer (CISO) w organizacji.

Nowe regulacje nakładają bezpośrednią odpowiedzialność na zarząd za przestrzeganie przepisów związanych z cyberbezpieczeństwem, zarządzaniem ryzykiem i raportowaniem incydentów. Wprowadzenie NIS2 oznacza, że brak zgodności z regulacjami może skutkować nie tylko karami finansowymi, ale także konsekwencjami prawnymi dla kadry kierowniczej.

OBOWIĄZKI ZARZĄDU WYNIKAJĄCE Z DYREKTYWY NIS2

Zgodnie z NIS2, zarząd organizacji ma obowiązek aktywnie uczestniczyć w procesach związanych z cyberbezpieczeństwem, co oznacza, że nie może delegować całkowitej odpowiedzialności na

dział IT, zespół ds. compliance czy analityków SOC. Rola zarządu w zakresie cyberbezpieczeństwa obejmuje:

1. STRATEGICZNE ZARZĄDZANIE RYZYKIEM CYBERNETYCZNYM

Zarząd organizacji powinien zapewnić, że w firmie funkcjonuje skuteczny system zarządzania bezpieczeństwem informacji, oparty na uznanych standardach, takich jak ISO/IEC 27001 lub równoważnych normach branżowych. Do jego kluczowych obowiązków należy również zatwierdzanie oraz bieżący nadzór nad realizacją strategii cyberbezpieczeństwa, w tym podejmowanie decyzji dotyczących alokacji zasobów finansowych i technologicznych na ochronę infrastruktury IT i OT. Szczególną uwagę należy poświęcić identyfikacji zasobów krytycznych wymagających ochrony zgodnie z przepisami NIS2 – takich jak infrastruktura krytyczna, systemy teleinformatyczne, środowiska operacyjne oraz kluczowe usługi cyfrowe świadczone przez organizację. Równie istotne jest stałe monitorowanie ryzyk w łańcuchu dostaw IT, w szczególności poprzez nadzorowanie zgodności dostawców, partnerów i usługodawców z wymogami w zakresie bezpieczeństwa informacji i ciągłości działania.

2. NADZÓR NAD WDRAŻANIEM MECHANIZMÓW CYBERBEZPIECZEŃSTWA

Zarząd powinien zadbać o to, aby organizacja dysponowała skutecznymi mechanizmami ochrony sieci oraz systemami wczesnego wykrywania i reagowania na zagrożenia, takimi jak rozwiązania klasy SIEM, SOAR, EDR/XDR czy IDS. Do jego kompetencji należy również zatwierdzanie i nadzorowanie polityk zarządzania tożsamością i dostępem, w tym wdrożenia wieloskładnikowego uwierzytelniania (MFA) jako standardu bezpieczeństwa. Istotnym obszarem odpowiedzialności zarządu jest również zapewnienie stosowania odpowiednich rozwiązań w zakresie szyfrowania danych, ochrony informacji wrażliwych, a także bezpieczeństwa aplikacji i usług świadczonych w środowiskach chmurowych. Kluczowe znaczenie ma ponadto regularna weryfikacja zgodności planów odtwarzania po awarii (Disaster Recovery) oraz planów ciągłości działania (Business Continuity Plan) z aktualnymi zagrożeniami, tak aby organizacja mogła zachować ciągłość operacyjną nawet w przypadku poważnego incydentu cybernetycznego.

3. OBOWIĄZEK SZKOLENIA ZARZĄDU I KADRY KIEROWNICZEJ

Nowością w ramach dyrektywy NIS2 jest wyraźne przypisanie zarządowi odpowiedzialności za organizowanie szkoleń z zakresu cyberbezpieczeństwa. Obowiązek ten obejmuje nie tylko uczestnictwo członków kadry kierowniczej w szkoleniach, ale również zapewnienie, że cała organizacja posiada odpowiednie kompetencje w zakresie strategicznego zarządzania ryzykiem IT, reagowania na incydenty oraz ochrony infrastruktury informatycznej i technologii operacyjnych (IT i OT). Zarząd musi być świadomy potencjalnych zagrożeń oraz konsekwencji prawnych i finansowych wynikających z nieprzestrzegania regulacji NIS2, ponieważ to on ponosi odpowiedzialność za zgodność organizacji z przepisami. Kluczowym elementem przygotowania do sytuacji kryzysowych powinno być także regularne organizowanie symulacji incydentów cybernetycznych, które pozwalają ocenić gotowość decyzyjną zarządu i skuteczność wdrożonych procedur bezpieczeństwa.

4. OBOWIĄZEK RAPORTOWANIA INCYDENTÓW

Zgodnie z wymogami dyrektywy NIS2, organizacje są zobowiązane do zgłoszenia istotnych incydentów cyberbezpieczeństwa w ciągu 24 godzin od ich wykrycia do właściwego zespołu reagowania na incydenty – CSIRT (Computer Security Incident Response Team). Zarząd ponosi odpowiedzialność za zapewnienie, że w organizacji funkcjonują skuteczne procedury umożliwiające szybkie wykrywanie, klasyfikowanie i raportowanie incydentów. W tym celu zaleca się wdrożenie zespołu monitorowania bezpieczeństwa (SOC) oraz nowoczesnych, zautomatyzowanych narzędzi do detekcji zagrożeń i zarządzania zdarzeniami. Równie istotne jest cykliczne przeprowadzanie audytów zgodności procesów raportowania z obowiązującymi przepisami oraz testowanie skuteczności mechanizmów reagowania – zarówno technicznych, jak i organizacyjnych – tak, aby zapewnić pełną gotowość na wypadek sytuacji kryzysowej.

3.5 ROLA CISO W ORGANIZACJI PO WDROŻENIU NIS2

Chief Information Security Officer (CISO) odgrywa kluczową rolę w procesie wdrażania NIS2, ponieważ odpowiada za koordynację działań związanych z cyberbezpieczeństwem, implementację polityk ochrony danych oraz zarządzanie ryzykiem IT i OT. Po wejściu w życie dyrektywy NIS2, rola CISO zyskuje na znaczeniu i skupia się na:

KOORDYNACJI WDROŻENIA STRATEGII CYBERBEZPIECZEŃSTWA

CISO odpowiada za spójną integrację polityk bezpieczeństwa w obszarach IT i OT oraz za wdrażanie procedur zapewniających zgodność organizacji z wymaganiami dyrektywy NIS2. Do jego kluczowych zadań należy identyfikacja zasobów krytycznych oraz zapewnienie ich ochrony – w szczególności systemów informatycznych, infrastruktury technologii operacyjnej, a także danych klientów, partnerów biznesowych i innych wrażliwych informacji przetwarzanych przez organizację.

MONITOROWANIU ZAGROŻEŃ I ANALIZIE PODATNOŚCI

Ścisła współpraca z zespołem SOC w zakresie ciągłego monitorowania zagrożeń oraz analizy incydentów cybernetycznych stanowi istotny element działań CISO. Do jego zadań należy również zarządzanie wdrożeniem i rozwojem narzędzi takich jak SIEM, IDS/IPS oraz rozwiązań z obszaru Threat Intelligence, które umożliwiają analizę zagrożeń w czasie rzeczywistym i skuteczne przeciwdziałanie atakom.

ZARZĄDZANIU RYZYKIEM I ZGODNOŚCIĄ Z REGULACJAMI

CISO jest odpowiedzialny za weryfikację, czy w organizacji obowiązują i są skutecznie egzekwowane polityki zarządzania tożsamością oraz kontroli dostępu do systemów i danych. Do jego obowiązków należy także monitorowanie poziomu zgodności z obowiązującymi regulacjami, w tym NIS2, oraz nadzorowanie przebiegu audytów wewnętrznych i zewnętrznych w obszarze cyberbezpieczeństwa.

SZKOLENIU I PODNOSZENIU ŚWIADOMOŚCI CYBERBEZPIECZEŃSTWA

Jednym z kluczowych zadań CISO jest inicjowanie i koordynowanie działań edukacyjnych w or-

ganizacji, w tym organizacja szkoleń oraz warsztatów dla pracowników i zarządu, które podnoszą świadomość w zakresie aktualnych zagrożeń cybernetycznych i najlepszych praktyk obronnych. Równolegle, CISO nadzoruje realizację symulacji ataków oraz testów penetracyjnych, które mają na celu ocenę skuteczności istniejących zabezpieczeń oraz identyfikację potencjalnych luk w systemach i procedurach bezpieczeństwa.

WSPÓŁPRACY Z ORGANAMI REGULACYJNYMI I RAPORTOWANIE INCYDENTÓW

Chief Information Security Officer jest odpowiedzialny za zapewnienie skutecznego i terminowego raportowania incydentów cyberbezpieczeństwa do odpowiednich zespołów CSIRT oraz instytucji nadzorczych wymaganych przez NIS2. W tym celu powinien nadzorować opracowanie i wdrożenie procedur umożliwiających szybką identyfikację zagrożeń, ich ocenę oraz podjęcie działań naprawczych, tak aby organizacja mogła sprawnie reagować na incydenty i ograniczać ich potencjalne skutki.

Nowe wymagania wynikające z dyrektywy NIS2 powodują, że dla znacznej części zarządów organizacji cyberbezpieczeństwo nie może być już dłużej wyłącznie kwestią techniczną, lecz musi stać się również strategicznym aspektem działalności biznesowej. NIS2 nakłada bezpośrednią odpowiedzialność na zarząd za zapewnienie zgodności organizacji z przepisami oraz skuteczne zarządzanie ryzykiem cybernetycznym.

Kluczową rolę w tym procesie odgrywa CISO, który musi nie tylko wdrażać polityki bezpieczeństwa i zarządzać ryzykiem, ale także aktywnie współpracować z zarządem, zespołem SOC (outsourcowanym lub wewnętrznym) oraz krajowymi organami nadzorującymi cyberbezpieczeństwo. Wdrożenie odpowiednich mechanizmów monitorowania zagrożeń, reagowania na incydenty oraz zarządzania zgodnością pozwoli organizacjom spełnić wymagania NIS2 i zabezpieczyć się przed konsekwencjami cyberataków.

3.6 CYBERSECURITY – JAK SOC I DEVSECOPS MOGĄ POMÓC W SPEŁNIENIU WYMAGAŃ?

Wdrożenie skutecznych mechanizmów cyberbezpieczeństwa stanowi jeden z fundamentów dostosowania organizacji do wymagań dyrektywy NIS2. W obliczu rosnącej liczby i złożoności cyberataków, firmy muszą zwiększyć swoje zdolności w zakresie monitorowania zagrożeń, wczesnego wykrywania incydentów oraz szybkiego reagowania na nieprawidłowości. Kluczową rolę w realizacji tych zadań odgrywają nowoczesne rozwiązania technologiczne oraz zintegrowane podejścia procesowo-organizacyjne, takie jak Security Operations Center (SOC) i DevSecOps.

SOC umożliwia organizacji stały monitoring infrastruktury IT i OT, analizę zagrożeń w czasie rzeczywistym oraz koordynację reakcji na incydenty. Z kolei DevSecOps – integracja bezpieczeństwa

z cyklem wytwarzania oprogramowania – pozwala na wykrywanie i eliminowanie podatności już na etapie projektowania i wdrażania systemów, co znacząco zmniejsza powierzchnię ataku. Oba podejścia wspierają także automatyzację działań defensywnych i poprawiają efektywność operacyjną zespołów bezpieczeństwa.

Dodatkowo, zgodnie z wymogami NIS2, organizacje powinny posiadać procedury zarządzania ryzykiem w łańcuchu dostaw IT, ponieważ dostawcy zewnętrzni coraz częściej stają się celem ataków cyberprzestępczych. Wdrożenie rozwiązań takich jak SOC i DevSecOps realnie wspiera spełnianie wymagań NIS2 w obszarze identyfikacji, analizy i raportowania incydentów, a także buduje długofalową odporność organizacji na zagrożenia cyfrowe.

3.7 SECURITY OPERATIONS CENTER (SOC) – JAK ORGANIZACJE MOGĄ REAGOWAĆ NA INCYDENTY I JE RAPORTOWAĆ?

Security Operations Center (SOC) to dedykowane zespół lub usługa, którego zadaniem jest ciągłe monitorowanie zagrożeń w infrastrukturze IT i OT, analiza podejrzanych aktywności oraz szybkie reagowanie na incydenty.

Organizacje objęte regulacją NIS2 muszą wdrożyć mechanizmy umożliwiające skuteczne wykrywanie i raportowanie incydentów cyberbezpieczeństwa, co czyni SOC jednym z kluczowych elementów compliance.

KLUCZOWE FUNKCJE SOC

- **Monitorowanie i analiza zagrożeń w czasie rzeczywistym** – zastosowanie systemów SIEM (Security Information and Event Management), IDS/IPS (Intrusion Detection & Prevention Systems) oraz Threat Intelligence pozwala na stałą kontrolę nad bezpieczeństwem organizacji.
- **Zarządzanie incydentami i reagowanie na zagrożenia** – SOC analizuje i kategoryzuje incydenty, wdraża środki zaradcze oraz eskaluje poważne zagrożenia do zespołów odpowiedzialnych za cyberbezpieczeństwo.
- **Automatyczne wykrywanie anomalii** – zastosowanie machine learning i AI-driven analytics pozwala na identyfikację niestandardowych zachowań w sieci, które mogą wskazywać na ataki hakerskie lub inne naruszenia.
- **Zarządzanie raportowaniem incydentów** – zgodnie z NIS2 organizacje muszą zgłaszać incydenty cyberbezpieczeństwa do CSIRT w ciągu 24 godzin, co oznacza konieczność wdrożenia automatycznych procesów raportowania i analizy naruszeń.

JAK WDROŻYĆ SOC W ORGANIZACJI?

Wdrożenie SOC może odbywać się w różnych modelach w zależności od rozmiaru i zasobów organizacji:

- **SOC wewnętrzny** – organizacje posiadające rozwinięty dział IT mogą utworzyć własne centrum

operacji bezpieczeństwa, co daje pełną kontrolę nad monitorowaniem zagrożeń i reakcją na incydenty.

- **SOC zarządzany** – organizacje mogą skorzystać z usług zewnętrznego dostawcy SOC, który zapewnia 24/7 monitorowanie zagrożeń, analizę ruchu sieciowego oraz raportowanie incydentów.
- **Hybrydowy model SOC** – łączy zasoby wewnętrzne organizacji z usługami zewnętrznego dostawcy SOC, co pozwala na optymalizację kosztów oraz wykorzystanie zaawansowanych narzędzi do detekcji i analizy zagrożeń.

Wdrożenie SOC pozwala organizacji zwiększyć odporność na cyberzagrożenia, automatyzować procesy raportowania incydentów oraz zapewnić zgodność z wymogami NIS2.

3.8 DEVELOPMENT, SECURITY, AND OPERATIONS (DEVSECOPS) – INTEGRACJA CYBERBEZPIECZEŃSTWA W PROCESIE ROZWOJU OPROGRAMOWANIA

DevSecOps (Development, Security, and Operations) to podejście, które integruje bezpieczeństwo na każdym etapie cyklu życia oprogramowania, co pozwala na minimalizację podatności oraz proaktywne eliminowanie zagrożeń w procesie wytwarzania aplikacji.

JAK DEVSECOPS WSPIERA COMPLIANCE Z NIS2?

DevSecOps odgrywa istotną rolę w spełnianiu wymagań dyrektywy NIS2, integrując bezpieczeństwo z każdym etapem cyklu życia oprogramowania. Podejście to umożliwia wczesne wykrywanie podatności, dzięki testowaniu kodu jeszcze na etapie jego tworzenia, co znacząco ogranicza ryzyko występowania luk bezpieczeństwa w środowiskach produkcyjnych. Automatyzacja procesów bezpieczeństwa w ramach ciągłej integracji i dostarczania (CI/CD) pozwala na bieżącą kontrolę jakości kodu oraz jego odporności na zagrożenia, zwiększając efektywność zespołów developerskich i bezpieczeństwa.

Kolejnym kluczowym elementem jest zarządzanie tożsamością i kontrolą dostępu – poprzez wdrożenie rozwiązań klasy Identity and Access Management (IAM), organizacje mogą zapewnić, że jedynie upoważnieni użytkownicy mają możliwość modyfikacji i wdrażania aplikacji, co ogranicza ryzyko wewnętrznych nadużyć i nieautoryzowanych zmian. Istotne znaczenie ma również monitorowanie bezpieczeństwa komponentów open-source, które są powszechnie wykorzystywane w projektach IT – odpowiednie narzędzia umożliwiają identyfikację znanych podatności i zarządzanie aktualizacjami, minimalizując ryzyko przejęcia kontroli przez osoby trzecie.

Wdrożenie podejścia DevSecOps w organizacjach objętych NIS2 pozwala nie tylko zwiększyć odporność aplikacji na cyberzagrożenia, ale także poprawia efektywność kosztową i operacyjną. Wczesne uwzględnianie aspektów bezpieczeństwa w procesie projektowania i rozwoju systemów znacząco redukuje koszty związane z późniejszym usuwaniem błędów i skraca czas reakcji na incydenty, co jest zgodne z filozofią proaktywnego zarządzania ryzykiem promowaną przez NIS2.

3.9 MONITORING RYZYKA DOSTAWCÓW IT – WYMAGANIA W ZAKRESIE ŁAŃCUCHA DOSTAW

Dyrektywa NIS2 nakłada na organizacje obowiązek dbania nie tylko o bezpieczeństwo własnej infrastruktury IT i OT, ale również o monitorowanie poziomu zabezpieczeń podmiotów zewnętrznych, takich jak dostawcy usług IT, oprogramowania, chmury czy infrastruktury krytycznej. Łańcuch dostaw IT staje się coraz częstszym celem ataków cybernetycznych, dlatego zarządzanie ryzykiem dostawców jest dziś jednym z kluczowych elementów skutecznego systemu cyberbezpieczeństwa.

Jednym z największych zagrożeń są tzw. ataki na łańcuch dostaw (supply chain attacks), w których cyberprzestępcy wykorzystują podatności u dostawców, by uzyskać dostęp do systemów swoich klientów. Szczególnie narażeni są dostawcy oprogramowania, platform chmurowych oraz podmioty świadczące zdalne usługi administracyjne. Dodatkowym ryzykiem jest brak nadzoru nad zgodnością dostawców z regulacjami, co w wielu organizacjach wciąż stanowi lukę – nieprowadzenie audytów, brak wymagań bezpieczeństwa w umowach czy nieuwzględnianie wymagań NIS2 w procesach zakupowych może prowadzić do poważnych naruszeń.

Aby skutecznie zarządzać ryzykiem w łańcuchu dostaw, organizacje powinny wdrożyć politykę zarządzania ryzykiem stron trzecich (Third-Party Risk Management), obejmującą zarówno ocenę poziomu ryzyka, jak i monitoring działań dostawców. Istotnym elementem są regularne audyty zgodności z wymaganiami NIS2 lub standardami branżowymi, takimi jak ISO/IEC 27001. Dobrą praktyką jest również zawieranie umów SLA (Service Level Agreement) z jasno określonymi wymaganiami dotyczącymi cyberbezpieczeństwa, procedur zarządzania incydentami oraz czasu reakcji na zagrożenia.

Wdrożenie takich rozwiązań jak Security Operations Center (SOC), DevSecOps oraz systemów do monitorowania ryzyka dostawców IT pozwala organizacjom nie tylko spełnić wymagania NIS2, ale również realnie zwiększyć odporność na ataki, ograniczyć powierzchnię zagrożeń i zyskać kontrolę nad bezpieczeństwem całego ekosystemu cyfrowego. Firmy, które inwestują w te obszary, nie tylko chronią swoje dane i zasoby, ale również budują zaufanie wśród partnerów biznesowych, szybciej wykrywają zagrożenia i skuteczniej raportują incydenty – co zmniejsza ryzyko sankcji i strat finansowych wynikających z naruszeń.

4.

REKOMENDACJE I DOBRE PRAKTYKI

Dostosowanie organizacji do dyrektywy NIS2 wymaga strategicznego podejścia, obejmującego zarówno wdrożenie nowych technologii, procesów organizacyjnych, jak i edukację kadry zarządzającej oraz pracowników. Wprowadzane regulacje stawiają przed firmami wyższe wymagania w zakresie zarządzania cyberbezpieczeństwem, identyfikacji zagrożeń, reagowania na incydenty oraz nadzoru nad łańcuchem dostaw IT.

W związku z tym wdrożenie najlepszych praktyk oraz natychmiastowe rozpoczęcie działań przygotowawczych ma kluczowe znaczenie dla zachowania zgodności z przepisami i ochrony przed cyberatakami.

4.1 CO FIRMY POWINNY ZROBIĆ JUŻ TERAZ?

Firmy, które chcą uniknąć ryzyka niezgodności z regulacjami NIS2 oraz zabezpieczyć swoją infrastrukturę IT i OT, powinny jak najszybciej rozpocząć działania dostosowawcze. Poniżej przedstawiono najważniejsze kroki, które organizacje powinny podjąć natychmiast, aby spełnić wymagania dyrektywy i zwiększyć poziom cyberbezpieczeństwa.

KROK 1: PRZEPROWADZENIE AUDYTU CYBERBEZPIECZEŃSTWA I ANALIZY LUK

Organizacje powinny niezwłocznie przeprowadzić kompleksową analizę stanu cyberbezpieczeństwa, aby zidentyfikować obszary wymagające dostosowania do wymogów dyrektywy NIS2. Audyt taki powinien obejmować identyfikację kluczowych zasobów IT i OT, które wymagają szczególnej ochrony, ocenę zgodności z aktualnymi standardami branżowymi oraz najlepszymi praktykami w zakresie bezpieczeństwa informacji, a także weryfikację gotowości organizacji do skutecznego wykrywania, obsługi i raportowania incydentów cybernetycznych. Istotnym elementem jest również analiza bezpieczeństwa w łańcuchu dostaw IT, obejmująca zgodność dostawców i partnerów zewnętrznych z regulacjami NIS2. Równolegle należy ocenić skuteczność obowiązujących procedur odtwarzania po awarii (Disaster Recovery) i planów ciągłości działania (Business Continuity Plan) w kontekście potencjalnych ataków cybernetycznych i zdolności organizacji do szybkiego przywrócenia operacyjności. Takie podejście pozwala nie tylko spełnić wymagania regulacyjne, lecz także zwiększyć ogólną odporność cyfrową organizacji.

KROK 2: WDROŻENIE MECHANIZMÓW ZARZĄDZANIA RYZYKIEM I RAPORTOWANIA INCYDENTÓW

Jednym z kluczowych wymagań dyrektywy NIS2 jest zdolność organizacji do wczesnego wykrywania incydentów cyberbezpieczeństwa oraz ich terminowego raportowania do odpowiednich organów nadzorczych. W tym celu organizacje powinny zintegrować nowoczesne mechanizmy detekcji zagrożeń, takie jak systemy Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), a także powołać wyspecjalizowany zespół Security Operations Center (SOC), odpowiedzialny za monitorowanie i analizę zagrożeń w czasie rzeczywistym. Równolegle należy wdrożyć procedury zgłaszania incydentów zgodnie z wymaganiami NIS2, zapewniając możliwość przekazania informacji o naruszeniu w ciągu 24 godzin do właściwego zespołu CSIRT. Kluczowe jest również opracowanie i regularne aktualizowanie planu reagowania na incydenty, który powinien obejmować szybkie wykrywanie zagrożeń, ocenę ich skutków oraz skuteczne wdrażanie środków naprawczych i zapobiegawczych.

KROK 3: USPRAWNIENIE NADZORU NAD ŁAŃCUCHEM DOSTAW IT

Cyberataki wymierzone w dostawców IT i partnerów technologicznych stanowią jeden z najczęściej wykorzystywanych wektorów ataku, dlatego organizacje zobowiązane do przestrzegania dyrektywy NIS2 powinny priorytetowo traktować bezpieczeństwo w łańcuchu dostaw. Kluczowym działaniem jest regularne przeprowadzanie audytów dostawców w celu weryfikacji ich zgodności z wymaganiami NIS2 oraz ocenianie poziomu wdrożonych środków ochrony. Niezbędne jest również uwzględnianie w umowach SLA jasno określonych norm cyberbezpieczeństwa, takich jak ISO/IEC 27001, SOC 2 czy inne adekwatne standardy branżowe. W celu bieżącego monitorowania zagrożeń ze strony podmiotów trzecich warto wdrożyć narzędzia klasy Third-Party Risk Management, które umożliwiają

analizę podatności oraz ocenę ryzyka związanego z konkretnymi dostawcami. Organizacja powinna ponadto zadbać o to, by jej partnerzy technologiczni stosowali odpowiednie mechanizmy ochrony danych i systemów, zgodne z wymogami dyrektywy, co znacząco ogranicza ryzyko incydentów wynikających z luk w zewnętrznych środowiskach IT.

KROK 4: WZMOCNIENIE ROLI CISO I ZARZĄDU W CYBERBEZPIECZEŃSTWIE

Dyrektywa NIS2 nakłada nowe obowiązki na zarząd i kadrę kierowniczą, podkreślając ich bezpośrednią odpowiedzialność za cyberbezpieczeństwo organizacji. W związku z tym firmy powinny w pierwszej kolejności powołać Chief Information Security Officer (CISO), jeśli dotychczas tego nie zrobiły, oraz zapewnić mu odpowiednie uprawnienia i zasoby do skutecznego zarządzania bezpieczeństwem informacji. Niezbędne jest także wdrożenie obowiązkowych szkoleń dla członków zarządu, które koncentrują się na strategicznym zarządzaniu ryzykiem, reagowaniu na incydenty oraz odpowiedzialności wynikającej z przepisów NIS2. Kluczowym elementem budowania odporności organizacji powinno być również regularne przeprowadzanie testów penetracyjnych oraz symulacji ataków, takich jak ransomware czy phishing, które pozwalają ocenić realny poziom przygotowania na sytuacje kryzysowe i doskonalić mechanizmy obronne.

KROK 5: INTEGRACJA DEVSECOPS – BEZPIECZEŃSTWO W PROCESIE TWORZENIA OPROGRAMOWANIA

Firmy rozwijające własne oprogramowanie lub korzystające z aplikacji biznesowych powinny priorytetowo traktować bezpieczeństwo na etapie ich projektowania i utrzymania. Kluczowym podejściem w tym zakresie jest wdrożenie modelu DevSecOps, który zakłada integrację cyberbezpieczeństwa z każdym etapem cyklu życia oprogramowania – od planowania, przez rozwój, aż po wdrożenie i utrzymanie. Niezbędnym elementem jest automatyzacja testów bezpieczeństwa w ramach procesów CI/CD, obejmująca również regularną analizę jakości i bezpieczeństwa kodu źródłowego. Organizacje powinny także wdrożyć mechanizmy umożliwiające bieżące monitorowanie podatności aplikacji, m.in. poprzez skanowanie kodu, analizę komponentów open source oraz automatyczne aktualizacje zabezpieczeń, co pozwala na szybką reakcję na pojawiające się zagrożenia i utrzymanie zgodności z wymaganiami NIS2.

4.2 PODSUMOWANIE WNIOSKÓW I PRZEWIDYWANIA NA PRZYSZŁOŚĆ

Dyrektywa NIS2 wymusza fundamentalną zmianę podejścia do cyberbezpieczeństwa, traktując je jako kluczowy element zarządzania ryzykiem i ciągłością działania organizacji.

Wprowadzenie nowych regulacji wiąże się z koniecznością dostosowania struktur organizacyjnych, wdrożenia nowych polityk oraz rozbudowy zdolności technicznych organizacji w zakresie ochrony przed cyberzagrożeniami. Firmy, które nie podejmą odpowiednich działań, mogą nie tylko narazić się na kary finansowe, ale również na poważne konsekwencje wynikające z potencjalnych ataków cybernetycznych, które mogą sparaliżować ich działalność.

KLUCZOWE WNIOSKI:

- NIS2 znacząco podnosi wymagania dotyczące zarządzania cyberbezpieczeństwem – organizacje muszą wdrożyć mechanizmy detekcji, reakcji i raportowania incydentów.
- Zarząd ma nową rolę i większą odpowiedzialność za cyberbezpieczeństwo – brak wdrożenia regulacji może skutkować konsekwencjami prawnymi dla kadry kierowniczej.
- SOC i DevSecOps stają się kluczowymi elementami compliance – organizacje powinny wdrożyć monitorowanie zagrożeń w czasie rzeczywistym oraz bezpieczeństwo w cyklu życia oprogramowania.
- Łańcuch dostaw IT to jeden z największych wektorów ataków – organizacje muszą wdrożyć audyt dostawców oraz mechanizmy zarządzania ryzykiem podmiotów trzecich.
- Firmy muszą działać natychmiast – dostosowanie do NIS2 wymaga przeprowadzenia analizy luk, wdrożenia polityk bezpieczeństwa oraz przeznaczenia budżetu na rozwój zdolności w zakresie cyberbezpieczeństwa.

PRZEWIDYWANIA NA PRZYSZŁOŚĆ

- Cyberzagrożenia będą coraz bardziej zaawansowane – rosnąca liczba ataków ransomware i cyberprzestępczości wymusi większe inwestycje w mechanizmy detekcji i reagowania.
- Regulacje będą jeszcze bardziej rygorystyczne – kraje członkowskie UE mogą wprowadzić dodatkowe przepisy zaostrzające wymagania dotyczące ochrony infrastruktury krytycznej i danych wrażliwych.
- Firmy, które zainwestują w cyberbezpieczeństwo, zyskają przewagę konkurencyjną – podmioty, które wdrożą nowoczesne mechanizmy ochrony, będą bardziej odporne na ataki i unikną kar wynikających z niezgodności z NIS2.

KOŃCOWA REKOMENDACJA:

ZACZNIJ DZIAŁAĆ TERAZ

Dostosowanie się do NIS2 wymaga natychmiastowego podjęcia działań. Organizacje, które wcześniej rozpoczną wdrażanie mechanizmów compliance, zyskają większą odporność na zagrożenia oraz unikną poważnych konsekwencji prawnych i finansowych wynikających z braku zgodności z regulacjami.

O RAPORCIE

Raport powstał dzięki zaangażowaniu Tenesys w ramach konsorcjum resilienceOne, które wspólnie działa na rzecz podnoszenia poziomu zgodności i odporności organizacji wobec regulacji takich jak DORA i NIS2.

Członkowie konsorcjum ResilienceOne:

Identonic

Identonic świadczy usługi doradcze w zakresie dostosowania i optymalizacji procesów związanych z DORA i NIS2 oraz innymi aktami prawnymi i standardami dotyczącymi obszaru ICT i cyberbezpieczeństwa.

info@identonic.com
+48 451 094 905
www.identonic.com

Tenesys

Utrzymanie środowisk IT i monitorowanie zagrożeń cybernetycznych 24/7 (SOC).
Wdrożenia systemów SIEM/SOAR/XDR.
Migracje do chmury AWS, Azure, GCP – optymalizacja, Proof of Concept.
Disaster Recovery i backup – poufność, dostępność, integralność i trwałość danych.

kontakt@tenesys.pl
+48 61 666 11 40
www.tenesys.io

LogicalTrust

Testy penetracyjne, testy socjotechniczne, Red Team vs. Blue Team, audyty odporności na ransomware. Audyty bezpieczeństwa IT oraz zarządzanie podatnościami.

kontakt@logicaltrust.net
+48 71 718 17 44
www.logicaltrust.net