IS CONSULTING

WHITE PAPER

NIS2 & CRA

Nowe Unijne Regulacje, Nowa Szansa?

Wpływ na MŚP oraz NGO, co powinny wiedzieć i jak się przygotować.

8 Kwietnia 2025

Kontekst legislacyjny NIS2 i CRA

Dyrektywa NIS2 oraz rozporządzenie Cyber Resilience Act to dwa kluczowe akty prawne Unii Europejskiej w obszarze cyberbezpieczeństwa, wprowadzone z myślą o podniesieniu odporności cyfrowej gospodarki.

Dyrektywa NIS2, przyjęta 14 grudnia 2022 r., rozszerza zakres poprzedniej dyrektywy NIS z 2016 r. i ma na celu osiągnięcie wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w całej UE. NIS2 znacząco poszerza listę sektorów objętych obowiązkami – z 9 do 18 – dodając m.in. branżę produkcyjną, pocztową, żywnościową czy gospodarkę odpadami. W rezultacie, w miejsce dotychczasowych 397 operatorów usług kluczowych (OUK) w Polsce, nowymi przepisami zostanie objętych kilkanaście tysięcy podmiotów. Co istotne, dyrektywa dzieli instytucje na *podmioty kluczowe* i *podmioty ważne*, w zależności od wielkości i znaczenia – przy czym te pierwsze to przeważnie duże firmy, a drugie to najczęściej MŚP. Termin implementacji NIS2 do prawa krajowego upłynął w październiku 2024 r., co oznacza, że liczne polskie organizacje będą podlegać nowym wymogom dopiero w połowie 2025 r..

Cyber Resilience Act (CRA) z kolei to unijne rozporządzenie (wejdzie w pełni w życie bezpośrednio we wszystkich państwach UE) ustanawiające obowiązkowe wymogi cyberbezpieczeństwa dla produktów zawierających elementy cyfrowe. Uchwalony w 2024 r. CRA jest pierwszym aktem prawnym UE, który tak kompleksowo reguluje bezpieczeństwo zarówno sprzętu, jak i oprogramowania na rynku wewnętrznym. Rozporządzenie nakłada na producentów i dystrybutorów obowiązek zapewnienia cyberbezpieczeństwa urządzeń oraz aplikacji *we wszystkich fazach cyklu życia produktu* – od etapu projektowania i rozwoju, po utrzymanie i aktualizacje. Celem jest wyeliminowanie powszechnego dziś problemu niskiego poziomu zabezpieczeń w wielu urządzeniach oraz braku regularnych aktualizacji usuwających podatności. W praktyce oznacza to zwiększenie odpowiedzialności producentów za bezpieczeństwo wyrobów: będą oni musieli m.in. dostarczać aktualizacje usuwające wykryte luki oraz informować użytkowników o ewentualnych zagrożeniach. Produkty spełniające wymogi CRA otrzymają oznaczenie CE potwierdzające zgodność z nowymi standardami. Główne obowiązki wynikające z CRA zaczną obowiązywać od grudnia 2027 r., dając firmom czas na dostosowanie się, lecz już teraz rozporządzenie to sygnalizuje istotną zmianę podejścia do bezpieczeństwa cyfrowego produktów w UE.

Znaczenie obu regulacji jest ogromne – razem stanowią one filary europejskiej strategii cyberbezpieczeństwa. NIS2 koncentruje się na odporności systemów i sieci w organizacjach świadczących kluczowe usługi (od energetyki, przez transport, po opiekę zdrowotną i administrację), zaś CRA uzupełnia te wysiłki, dbając o bezpieczeństwo produktów cyfrowych dostępnych na rynku. Dla polskich małych i średnich przedsiębiorstw oraz organizacji pozarządowych (NGO) oznacza to konieczność zrozumienia nowych wymogów i podjęcia odpowiednich kroków.

"Jeśli chodzi o bezpieczeństwo cybernetyczne, które leży u podstaw szerszego portfolio w zakresie bezpieczeństwa, chciałbym dążyć do promowania programu bezpieczeństwa cybernetycznego obejmującego całe społeczeństwo już na etapie projektowania. Skupiłbym się na wdrażaniu i egzekwowaniu nowych przepisów zarówno w zakresie cyberbezpieczeństwa podmiotów krytycznych (NIS2), jak i bezpieczeństwa produktów (Cyber Resilience Act) w sposób innowacyjny i przyjazny dla biznesu. "

- Henna Virkkunen

1. MŚP cyfryzacja i cyberbezpieczeństwo

W 2023 roku w Polsce działało około 2,3 mln przedsiębiorstw niefinansowych, z czego 99,8% to firmy z sektora MŚP. W tej grupie przeważają mikroprzedsiębiorstwa (do 9 pracowników), które stanowią aż 97,2% wszystkich firm. MŚP generują blisko 45% PKB kraju oraz zapewniają ponad 2/3 miejsc pracy w sektorze przedsiębiorstw. Pod względem branżowym większość polskich MŚP działa w usługach (55%), handlu (20%) i budownictwie (15%), podczas gdy udział sektora przemysłowego wynosi ok. 9%. Dane te pokazują, że MŚP są motorem napędowym gospodarki, ale również wskazują na ich rozdrobnienie i ograniczone zasoby – typowy polski przedsiębiorca to niewielka firma o lokalnym zasięgu. Organizacje pozarządowe (fundacje, stowarzyszenia i inne NGO) również odgrywają ważną rolę społeczną i gospodarczą. Według najnowszych danych, na koniec 2023 r. w Polsce było zarejestrowanych ponad 155 tysięcy stowarzyszeń i fundacji. Liczba NGO systematycznie rośnie – w ciągu ostatnich 15 lat przybyło ok. 50 tys. organizacji, co oznacza wzrost o połowę względem 2010 r.. Spośród zarejestrowanych organizacji około 121 tys. to stowarzyszenia, a ok. 34 tys. – fundacje. Warto zaznaczyć, że nie wszystkie zarejestrowane podmioty są aktywne, jednak nawet ostrożne szacunki mówią o ponad 100 tys. działających NGO. Sektor pozarządowy cechuje zróżnicowanie wielkości (od małych lokalnych stowarzyszeń po ogólnopolskie fundacje) oraz ograniczone zasoby finansowe – średni roczny budżet polskiej

organizacji pozarządowej wynosił ok. 26 tys. zł (2020 r.), a tylko 25% NGO posiada jakiekolwiek rezerwy finansowe. Mimo skromnych budżetów, większość NGO stara się korzystać z narzędzi cyfrowych – 92% organizacji deklaruje obecność w Internecie (np. własna strona lub profil w social media). To pokazuje, że trzeci sektor dostrzega potrzebę cyfryzacji, ale brak funduszy i sprzętu stanowi barierę dla 67% NGO, co utrudnia inwestycje w nowoczesne technologie i bezpieczeństwo.

Poziom Cyfryzacji Polskich Firm

80 %

Duże

60 %

Średnie

<50%

Małe

Poziom cyfryzacji polskich MŚP systematycznie rośnie, choć nadal pozostaje nieco niższy niż średnia unijna. Szacuje się, że ok. 60% średnich firm i niecała połowa małych firm w Polsce korzysta z zaawansowanych technologii cyfrowych, podczas gdy w przypadku dużych przedsiębiorstw odsetek ten sięga ~80%. Mikro firmy – mimo niewielkiej skali – również coraz częściej sięgają po narzędzia cyfrowe (ok. 60% deklaruje użycie zaawansowanych rozwiązań cyfrowych), choć wiele z nich ogranicza się do podstawowej obecności online. W dobie post pandemicznej transformacji sporo firm (zwłaszcza większych) przyspieszyło cyfryzację – np. niemal 60% dużych przedsiębiorstw w Polsce zwiększyło wykorzystanie technologii podczas pandemii, wobec ok. 40% średnich i małych firm. Nadal jednak tylko 30% mikroprzedsiębiorstw w UE traktuje cyfryzację jako priorytet (wobec 62% wśród dużych firm), co wskazuje na lukę świadomości i możliwości między najmniejszymi a największymi podmiotami.

Gotowość w zakresie cyberbezpieczeństwa MŚP i NGO pozostaje wyzwaniem. Wiele małych organizacji nie posiada sformalizowanych polityk bezpieczeństwa ani dedykowanych kadr IT. Jak zauważa dyrektor Cisco Polska, zaledwie 7% polskich firm ma w pełni dojrzałe systemy cyberbezpieczeństwa – plasuje to nasz kraj w dolnej części globalnego rankingu. Braki kadrowe są szczególnie dotkliwe: niemal żadna mała czy średnia firma nie zatrudnia osoby odpowiedzialnej wyłącznie za bezpieczeństwo IT. Zagrożenia często bywają niedoceniane – niska świadomość ryzyka cyberataków oraz przekonanie „to nas nie dotyczy” nadal jest

powszechne w sektorze MŚP. Niestety, statystyki wskazują, że realia są inne: np. według badań unijnych niemal jedna trzecia europejskich MŚP doświadczyła incydentu cyberbezpieczeństwa w ostatnich latach. W Polsce niepokojące są także wyniki badań dotyczących ochrony danych w MŚP – *tylko 31%* firm z sektora MŚP zabezpiecza wrażliwe dane pracowników, wysyłając je zaszyfrowanymi e-mailami z hasłowanymi załącznikami. Aż *14%* przyznaje wprost, że zdarza im się wysyłać dane personalne podwykonawcom otwartym e-mailem bez żadnego szyfrowania. Ponad *9%* firm przechowuje również niezaszyfrowane dokumenty w chmurze i udostępnia je zewnętrznym partnerom. Te alarmujące praktyki – obecne zwłaszcza w mniejszych przedsiębiorstwach – potwierdzają, że część MŚP ignoruje podstawowe zasady cyberbezpieczeństwa, wystawiając siebie i swoich klientów na poważne ryzyko.

Podsumowując, polski sektor MŚP i NGO jest liczny i zróżnicowany, ale jego poziom dojrzałości cyfrowej i zabezpieczeń informatycznych bywa niewystarczający wobec rosnących zagrożeń. To właśnie w tym kontekście nadejście regulacji takich jak NIS2 i CRA nabiera szczególnego znaczenia – mogą one stać się impulsem do nadrobienia zaległości w obszarze cyberbezpieczeństwa, ale stanowią też duże wyzwanie organizacyjne i finansowe dla niewielkich podmiotów.

2. Analiza wpływu NIS2 i CRA na MŚP i NGO

Nowe regulacje niosą za sobą zarówno szanse (korzyści), jak i obciążenia (koszty, ryzyka) dla małych i średnich przedsiębiorstw oraz organizacji pozarządowych. Poniżej przedstawiono kluczowe obszary wpływu:

Korzyści i pozytywne skutki

- **Podniesienie poziomu bezpieczeństwa** – NIS2 wymusza wdrożenie rygorystycznych standardów ochrony sieci i systemów. W dłuższej perspektywie MŚP i NGO, które dostosują się do wymogów (np. wprowadzą polityki zarządzania ryzykiem, szyfrowanie, dwuskładnikowe uwierzytelnianie, monitorowanie incydentów), staną się mniej podatne na ataki i incydenty. To oznacza mniejsze ryzyko kosztownych przestojów, wycieków danych czy strat finansowych wskutek cyberataków. Wzmocnienie ochrony własnej infrastruktury to także ochrona interesów klientów, beneficjentów i partnerów tych organizacji.
- **Wzrost zaufania i wiarygodności** – spełnienie wymogów NIS2 (dla podmiotów objętych) lub dobrowolne dostosowanie się do dobrych praktyk wynikających z dyrektywy może stać się atutem konkurencyjnym. Kontrahenci i klienci coraz większą wagę przywiązują do bezpieczeństwa – firma mogąca wykazać certyfikaty, zgodność z normami lub członkostwo w branżowych inicjatywach

bezpieczeństwa zyskuje przewagę. Podobnie NGO dbające o cyberbezpieczeństwo budują zaufanie darczyńców i odbiorców swoich usług (np. chroniąc powierzane dane wrażliwe). Wspólnotowy znak CE dla produktów IT (na mocy CRA) będzie natomiast sygnałem dla odbiorców, że produkt spełnia wysokie standardy – producent (nawet mały) legitymujący się takim znakiem może łatwiej zdobyć rynek dzięki zwiększonemu zaufaniu klientów.

- **Pełniejszy dostęp do rynku i zamówień** – w wielu sektorach (np. energetyka, sektor publiczny) posiadanie odpowiednich zabezpieczeń stanie się warunkiem koniecznym dla dostawców. MŚP, które zainwestują w cyberbezpieczeństwo, będą mogły uczestniczyć w łańcuchach dostaw kluczowych usług oraz startować w przetargach wymagających spełnienia norm NIS2. Ci, którzy zignorują te wymogi, mogą zostać wykluczeni z pewnych rynków. Innymi słowy, dostosowanie się oznacza utrzymanie i rozszerzenie możliwości biznesowych, podczas gdy brak zgodności – ryzyko utraty kontraktów.

DYREKTYWA NIS2

„Środki zarządzania ryzykiem w zakresie cyberbezpieczeństwa obejmują ocenę i uwzględnienie ryzyk związanych z bezpieczeństwem w relacjach z dostawcami i usługodawcami, w tym w łańcuchu dostaw”

- Artykuł 21, ust. 2 lit. d

- **Lepsza ochrona konsumentów i organizacji dzięki CRA** – Cyber Resilience Act przyniesie korzyści również odbiorcom produktów cyfrowych. MŚP i NGO, jako użytkownicy sprzętu i oprogramowania, skorzystają na ogólnym podniesieniu poprzeczki bezpieczeństwa produktów dostępnych na rynku. Urządzenia IoT, systemy teleinformatyczne czy aplikacje, z których korzystają na co dzień, będą musiały spełniać określone wymogi (m.in. brak znanych podatności, bezpieczna konfiguracja domyślna, dostępność aktualizacji bezpieczeństwa). To zmniejszy ryzyko, że np. luka w tanim routerze czy kamerze IP narazi firmę na atak. Ponadto CRA zwiększy przejrzystość informacji o bezpieczeństwie produktu – łatwiej będzie ocenić, które rozwiązania są godne zaufania. Dzięki temu nawet mniejsze podmioty, nie dysponujące własnymi ekspertami, będą mogły podejmować bardziej świadome decyzje zakupowe i wybierać produkty gwarantujące wyższy poziom ochrony.
- **Efekt domina – podniesienie standardów w całej gospodarce** – wprowadzenie nowych regulacji zmusza największe firmy i infrastrukturę krytyczną do inwestycji w bezpieczeństwo, co pośrednio poprawia

bezpieczeństwo całego ekosystemu, w którym działają MŚP i NGO. Np. telekomy czy banki (objęte NIS2 jako podmioty kluczowe) wzmocnią swoje zabezpieczenia, czyniąc usługi, z których korzystają mali klienci, bardziej odpornymi. To samo dotyczy producentów sprzętu podlegających CRA – bardziej bezpieczne produkty trafią także do sektora MŚP/NGO. Sumarycznie, wzrost ogólnego poziomu „cyber higieny" w gospodarce przynosi korzyść wszystkim uczestnikom rynku, zmniejszając ogólną podatność na ataki.

GŁÓWNE KORZYŚCI

Wdrożenie odpowiednich działań w zakresie cyberbezpieczeństwa przyczynia się do podniesienia poziomu bezpieczeństwa, zwiększa zaufanie i wiarygodność organizacji, umożliwia dostęp do rynku zamówień, zapewnia lepszą ochronę konsumentów oraz wspiera podniesienie standardów całej gospodarki.

Koszty i obciążenia dla MŚP/NGO

- **Koszty wdrożenia środków bezpieczeństwa** – dostosowanie się do wymogów NIS2 wiąże się z koniecznością wdrożenia wielu środków technicznych i organizacyjnych. Dla MŚP może to oznaczać znaczne wydatki, m.in. na: modernizację infrastruktury IT (zapory sieciowe, systemy wykrywania włamań, kopie zapasowe), zakup oprogramowania zabezpieczającego, audyty bezpieczeństwa, opracowanie dokumentacji (polityk, procedur) czy szkolenia personelu. Wdrożenie systemu zarządzania bezpieczeństwem (np. zgodnie z normą ISO 27001) bywa kosztowne i czasochłonne. Dla NGO, działających non-profit, nawet relatywnie niewielkie wydatki mogą być trudne do udźwignięcia przy ograniczonym budżecie.
- **Konieczność zatrudnienia lub outsourcingu ekspertów** – większość małych organizacji nie ma wewnętrznych specjalistów ds. cyberbezpieczeństwa. W obliczu nowych wymagań będą one musiały pozyskać odpowiednie kompetencje, czy to poprzez zatrudnienie pracownika (co bywa nierealne z powodu braków kadrowych i wysokich stawek na rynku), czy poprzez zlecenie usług firmom zewnętrznym. Korzystanie z zewnętrznych doradców lub tzw. usług zarządzanych (Managed Security Services) generuje stałe koszty operacyjne, które dla mikro i małych firm mogą być znaczącym obciążeniem. Pojawia się też wyzwanie znalezienia zaufanych i wykwalifikowanych partnerów

– popyt na usługi bezpieczeństwa wzrośnie lawinowo wraz z wdrażaniem NIS2, co może zwiększyć ich cenę.

- **Rozbudowa biurokracji i procesów** – NIS2 narzuca nie tylko wdrożenie zabezpieczeń, ale także szereg formalnych obowiązków: konieczność przeprowadzania analiz ryzyka, raportowania incydentów do właściwych organów w ściśle określonym czasie, utrzymywania kontaktu z CSIRT (Computer Security Incident Response Team), uczestnictwa w kontrolach i audytach ze strony organów nadzoru. Dla małych firm oznacza to nowe zadania administracyjne, które mogą odciągać uwagę od ich podstawowej działalności. Przykładowo, incydent cyberbezpieczeństwa w podmiocie objętym NIS2 będzie musiał zostać zgłoszony wstępnie w ciągu 24 godzin, a następnie szczegółowo w ciągu 72 godzin od wykrycia – wymaga to posiadania procedur i gotowości do szybkiego działania. Ponadto kierownictwo firmy będzie musiało angażować się w kwestie bezpieczeństwa (dyrektywa przewiduje odpowiedzialność menedżerską za przestrzeganie wymogów). Te nowe procesy wewnętrzne mogą być trudne do zaabsorbowania dla małych organizacji, które dotąd działały mniej formalnie.

SPECJALISTA PILNIE POSZUKIWANY

Średni koszt zatrudnienia doświadczonego specjalisty ds. cyberbezpieczeństwa to około ***20 tysięcy złotych*** *brutto miesięcznie. 48% organizacji w Europie ma problem z rekrutacją kandydatów o odpowiednich kwalifikacjach i doświadczeniu.*

- **Jednorazowe inwestycje i koszty ciągłe** – warto zauważyć, że dostosowanie się do regulacji to nie jednorazowy wysiłek, ale ciągłe zobowiązanie. Cyberbezpieczeństwo wymaga permanentnego utrzymania – regularnych aktualizacji systemów, testów penetracyjnych, szkoleń pracowników (bo rotacja personelu powoduje, że nowi muszą przechodzić edukację), audytów zgodności itp. Dla MŚP i NGO oznacza to stałe koszty operacyjne związane z bezpieczeństwem. Nawet jeśli częściowo pokryją je fundusze unijne czy wsparcie rządowe (np. programy dotacyjne na poprawę cyberbezpieczeństwa), to i tak organizacja musi przygotować się na wygospodarowanie budżetu utrzymaniowego, co może wymagać cięć w innych obszarach.

- **Wpływ CRA na koszty produkcji i zgodności** – firmy z sektora MŚP, które zajmują się wytwarzaniem oprogramowania lub elektroniki, odczują również ciężar wymogów Cyber Resilience Act. Rozporządzenie to obliguje producentów do przeprowadzenia oceny ryzyka cyberbezpieczeństwa dla każdego produktu, dokumentowania spełnienia wymagań, a w niektórych przypadkach – poddania produktu certyfikacji przez trzecią stronę (dotyczy to tzw. krytycznych produktów wysokiego ryzyka). Dla małego producenta urządzeń IoT czy start-upu software'owego może to być spore wyzwanie finansowe i proceduralne. Konieczne będzie m.in. wdrożenie Secure by Design w cyklu tworzenia produktu, co wydłuży czas i zwiększy koszty R&D. Niespełnienie wymogów będzie zaś oznaczać brak możliwości legalnej sprzedaży produktu na rynku UE po 2027 r., a także potencjalne kary administracyjne. Z perspektywy mikrofirm, które często konkurują ceną i szybkością działania, dostosowanie się do CRA może wymagać przedefiniowania modelu biznesowego i znalezienia dodatkowych zasobów (np. poprzez inwestora, partnerstwo lub specjalne programy akceleracyjne nastawione na bezpieczeństwo).

ZWIĘKSZENIE KOSZTÓW

Wdrożenie skutecznych środków cyberbezpieczeństwa wiąże się z wysokimi kosztami początkowymi, koniecznością zatrudnienia lub outsourcingu ekspertów, rozbudowaniem procesów oraz zwiększeniem zarówno jednorazowych inwestycji, jak i kosztów bieżącego utrzymania, co często przekłada się na wzrost kosztów produkcji niezbędny do zapewnienia zgodności z wymaganiami bezpieczeństwa.

Ryzyka i wyzwania

- **Ryzyko sankcji i odpowiedzialności prawnej** – niewypełnienie obowiązków wynikających z NIS2 grozi dotkliwymi karami finansowymi. Ustalone w dyrektywie widełki sięgają do 10 mln euro (lub 2% rocznego obrotu) dla podmiotów kluczowych i do 7 mln euro (lub 1,4% obrotu) dla podmiotów ważnych. Choć najwyższe kary dotyczyć będą raczej dużych graczy, to nawet średnie firmy mogą zostać ukarane kwotami, które zagrożą ich płynności. Ponadto menedżerowie mogą ponosić odpowiedzialność za zaniedbania (w skrajnych wypadkach w grę może wchodzić też odpowiedzialność karna, np.

jeśli dojdzie do poważnego incydentu wskutek rażącego niedbalstwa). Dla NGO brak bezpośrednich sankcji finansowych (nie są przedsiębiorstwami), ale np. fundacje realizujące zadania publiczne mogą utracić zaufanie organów zlecających zadania lub sponsorów w razie rażących naruszeń bezpieczeństwa.

- **Zwiększona ekspozycja na ataki w okresie przejściowym** – paradoksalnie, okres wdrażania nowych regulacji może być czasem wzmożonego ryzyka. Cyberprzestępcy doskonale wiedzą o „bólu transformacji", z jakim mierzą się firmy. MŚP zajęte implementacją nowych systemów bezpieczeństwa lub testowaniem procedur mogą tymczasowo być bardziej podatne (np. jeśli odłożą pewne aktualizacje na czas wdrażania większych zmian). Ponadto same działania dostosowawcze mogą ujawnić nieznane wcześniej luki (np. podczas audytu może wyjść na jaw, że pewne dane są słabo chronione – co staje się atrakcyjnym celem). Atakujący mogą też celować w dostawców w łańcuchu dostaw tuż przed tym, jak wejdą oni pod rygor przepisów, licząc na ich obecne słabsze zabezpieczenia. To oznacza, że najbliższe 1-2 lata (2026-2027) będą krytyczne – organizacje muszą zachować czujność i utrzymać bieżącą ochronę równolegle z procesem wdrażania nowych wymogów.

ŚREDNI KOSZT CYBERATAKU

*Średni koszt naruszenia danych w 2024 roku **wyniósł 4.88 miliona dolarów** co stanowi wzrost o 10% w porównaniu do roku poprzedniego i jest najwyższych odnotowanym kosztem w historii. Ilość ataków ciągle wzrasta, zgodnie z danymi Europejskiej Agencji ds. Cyberbezpieczeństwa w roku 2024 odnotowano aż **11 079 incydentów.***

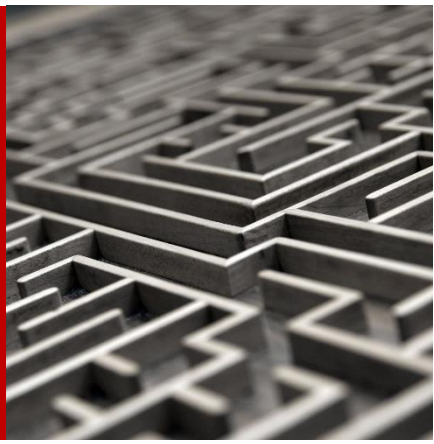
- **Ryzyko utraty biznesu przy braku zgodności** – dla podmiotów formalnie nieobjętych NIS2 istnieje niebezpieczeństwo, że *mogą zostać wykluczone pośrednio*. Na przykład duże firmy (objęte regulacją) będą przeprowadzać oceny bezpieczeństwa swoich kontrahentów. Jeśli mała firma nie będzie spełniać minimalnych standardów (np. nie będzie szyfrować danych czy nie wdroży kontroli dostępu), może stracić kontrakty na rzecz bardziej zabezpieczonych konkurentów. Podobnie NGO współpracujące z administracją lub biznesem mogą zostać poproszone o wykazanie pewnego poziomu dojrzałości cyberbezpieczeństwa – brak takiego przygotowania to ryzyko utraty partnerstw, grantów czy zleceń. Innymi słowy, cyberbezpieczeństwo stanie się warunkiem zaufania biznesowego – kto go nie spełni, ten wypadnie z gry.
- **Ataki na łańcuch dostaw i „najsłabsze ogniwo"** – jednym z motywatorów wprowadzenia NIS2 była obserwacja, że przestępcy często atakują nie

bezpośrednio dobrze zabezpieczone korporacje, ale ich słabszych partnerów (dostawców oprogramowania, małe firmy usługowe) jako furtkę. Nowe regulacje starają się temu przeciwdziałać, lecz *do czasu pełnego wdrożenia* to zjawisko będzie nadal aktualne. MŚP i NGO mogą być postrzegane jako takie potencjalnie najsłabsze ogniwa. Już teraz ponad 60% incydentów dotykających duże firmy ma swój początek w naruszeniu bezpieczeństwa u dostawcy lub podwykonawcy. Dlatego na mniejsze organizacje spada ryzyko, że staną się celem ataku nie ze względu na własne dane, ale jako wektor ataku na większą instytucję. Jeżeli np. mała firma informatyczna obsługuje systemy samorządowe, to atakujący mogą uderzyć w tę firmę, by poprzez nią dostać się do sieci urzędu. To rodzi dodatkową odpowiedzialność – MŚP/NGO musi chronić nie tylko siebie, ale i swoich klientów. NIS2 wprowadza co prawda wymóg zarządzania ryzykiem dostawców przez podmioty kluczowe, lecz zanim praktyki te okrzepną, mniejsi partnerzy będą szczególnie narażeni.

- **Adaptacja do zmieniających się przepisów i standardów** – cyberbezpieczeństwo to dziedzina dynamiczna, a regulacje będą z czasem aktualizowane. Już teraz trwają prace nad aktami delegowanymi i standardami technicznymi do CRA, które doprecyzują wymagania dla poszczególnych kategorii produktów. Istnieje ryzyko, że małe organizacje mogą pogubić się w gąszczu wymogów prawnych i norm (np. normy europejskie EN, standardy ISO/IEC, wytyczne ENISA), co wprowadza niepewność prawną. Błąd w interpretacji przepisów może skutkować albo nadmiernymi kosztami (wdrożenie zbyt surowych środków ponad to, co wymagane) albo lukami w zgodności (pominięcie jakiegoś obowiązku). Dlatego wyzwaniem staje się *śledzenie na bieżąco zmian prawnych i najlepszych praktyk*. Dla NGO, które często nie mają działu prawnego ani compliance, jest to szczególnie trudne. Niektóre organizacje mogą potrzebować wsparcia zewnętrznego doradcy prawnego, co generuje kolejne koszty.

GŁÓWNE WYZWANIA

Organizacje stoją dziś wobec rosnącego ryzyka sankcji i odpowiedzialności prawnej, zwiększonej ekspozycji na ataki w okresie przejściowym, zagrożenia utratą kontraktów w przypadku braku zgodności, rosnącej liczby ataków na łańcuch dostaw wykorzystujących najsłabsze ogniwa, a także konieczności nieustannej adaptacji do zmieniających się przepisów i standardów.



Obowiązki pośrednie i wpływ łańcucha dostaw

Wiele małych firm i organizacji pozarządowych, choć nie znajdzie się bezpośrednio w wykazie podmiotów objętych NIS2, odczuje wpływ regulacji w sposób pośredni. Dyrektywa wprost przewiduje sytuacje, w których MŚP zostaną włączone w wymogi bezpieczeństwa poprzez relacje z większymi partnerami. Przykładowo, jeśli MŚP jest dostawcą lub podwykonawcą firmy podlegającej NIS2, ta większa firma może nakładać na nią określone oczekiwania w zakresie bezpieczeństwa łańcucha dostaw. Oznacza to, że duży podmiot będzie „wymuszał" podniesienie standardów u swoich kontrahentów, aby zabezpieczyć się przed ryzykiem przenikającym przez łańcuch dostaw. Takie wymagania mogą znaleźć się w umowach handlowych (np. klauzule dotyczące stosowania szyfrowania, audytu bezpieczeństwa dostawcy, certyfikacji ISO 27001, posiadania planu ciągłości działania itp.). MŚP, które ich nie spełnią, nie podpiszą kontraktu lub stracą istniejący.

Podobny mechanizm działa w sektorze publicznym. Administracja objęta NIS2 (np. większe urzędy, jednostki samorządu) prawdopodobnie zacznie weryfikować bezpieczeństwo NGO, którym zleca zadania publiczne lub którym powierza dane obywateli. Formalnie NGO nie są „operatorami usług kluczowych", ale jeśli współpracują przy realizacji np. usług opieki zdrowotnej, edukacyjnych czy socjalnych, mogą zostać poproszone o przestrzeganie określonych standardów. Już teraz wiele fundacji przetwarza dane osobowe wrażliwe (np. dane zdrowotne pacjentów hospicjów prowadzonych przez organizacje charytatywne) – w takim przypadku wymogi RODO oraz dobra praktyka wymuszały pewien poziom zabezpieczeń. Teraz jednak wchodzą dodatkowe kryteria: np. czy dana organizacja ma przygotowany plan reagowania na incydent cyberbezpieczeństwa, czy wyznaczyła osobę kontaktową ds. cyber (wymagane dla podmiotów z NIS2), czy prowadzi szkolenia personelu z bezpieczeństwa. Jeśli nie, urząd lub szpital może zdecydować o ograniczeniu współpracy z taką organizacją ze względu na ryzyko.

Cyber Resilience Act także ma efekt pośredni – dystrybutorzy i sprzedawcy produktów (w tym MŚP, np. sklepy z elektroniką, firmy integratorskie) będą ponosić odpowiedzialność za wprowadzanie do obrotu wyłącznie zgodnych, certyfikowanych urządzeń. Małe sklepy internetowe sprzedające importowane gadżety IoT będą

musiały upewnić się, że ich dostawcy dostarczyli produkty z oznaczeniem CE (CRA). Jeśli nie, to sklep naraża się na sankcje ze strony organów nadzoru rynku. Zatem nawet podmiot, który niczego nie produkuje, ale handluje sprzętem lub oprogramowaniem, stanie się ogniwem w łańcuchu zapewnienia zgodności z CRA. Dla pewności, sprzedawcy mogą wprowadzać własne procedury kontroli – np. żądać od dostawców deklaracji zgodności z CRA, uważniej dobierać asortyment, a w razie wykrycia luki bezpieczeństwa w sprzedanym produkcie – współpracować przy akcjach naprawczych/aktualizacyjnych. To dodatkowe obowiązki, które wcześniej nie występowały.

Wreszcie, warto wspomnieć o kulturze dobrowolnego raportowania incydentów. NIS2 zachęca podmioty spoza katalogu do zgłaszania poważnych incydentów na zasadzie dobrowolności, co może pomóc w budowaniu szerszego obrazu zagrożeń. Jeśli MŚP lub NGO padnie ofiarą ataku ransomware, może (choć nie musi) powiadomić właściwy CSIRT. Taka praktyka – choć nieobligatoryjna – będzie coraz bardziej promowana jako element społecznej odpowiedzialności i współpracy na rzecz bezpiecznego cyfrowego ekosystemu. Organizacje, które wejdą w ten nurt (np. zgłoszą incydent i podzielą się informacjami o wektorze ataku), mogą liczyć na pomoc zespołów reagowania i jednocześnie przyczyniają się do ochrony innych przed podobnymi zagrożeniami. To aspekt budowania wspólnej odporności, który NIS2 stara się rozwijać, a który wymaga zaangażowania także podmiotów nieobjętych bezpośrednio przepisami.

Rekomendacje – jak MŚP i NGO mogą przygotować się na NIS2 i CRA

W obliczu nadchodzących zmian legislacyjnych małe firmy i organizacje pozarządowe powinny podjąć proaktywne działania, by zmniejszyć obciążenia i wykorzystać szanse wynikające z NIS2 oraz CRA. Poniżej zestawiono rekomendacje kroków przygotowawczych:

1. **Przeprowadzenie analizy wpływu i oceny ryzyka:** Każda organizacja powinna najpierw ustalić, czy *bezpośrednio* podlega nowym regulacjom. Należy sprawdzić kryteria NIS2 – czy działamy w sektorze uznanym za krytyczny i czy przekraczamy progi (≥50 pracowników lub ≥10 mln euro obrotu), ewentualnie czy możemy zostać uznani za podmiot o znaczeniu krytycznym (np. świadczymy kluczową usługę na poziomie lokalnym). Jeśli tak, konieczne będzie pełne wdrożenie wymagań (patrz niżej). Jeśli nie, warto zidentyfikować obszary pośredniego ryzyka – np. kluczowych klientów/partnerów, którzy mogą stawiać nam wymogi bezpieczeństwa, albo produkty które sprzedajemy i które podpadną pod CRA. Równolegle trzeba przeprowadzić klasyczną analizę ryzyka IT w organizacji: zidentyfikować zasoby (systemy, dane) i zagrożenia, ocenić skutki potencjalnych incydentów. To pozwoli priorytetyzować działania – skupić

się na ochronie najcenniejszych zasobów i najbardziej prawdopodobnych scenariuszach ataku.

2. **Podniesienie poziomu zabezpieczeń krok po kroku:** Na podstawie oceny ryzyka należy wdrożyć adekwatne środki techniczne i organizacyjne. Dla wielu MŚP/NGO punktem wyjścia będą podstawy cyberhigieny, takie jak:
    - *Aktualizacja oprogramowania* – upewnienie się, że wszystkie systemy i aplikacje są na bieżąco aktualizowane (łatki bezpieczeństwa).
    - *Kopie zapasowe* – wprowadzenie regularnego backupu kluczowych danych (i odseparowanie kopii od sieci produkcyjnej), co uchroni przed skutkami ataków typu ransomware.
    - *Kontrola dostępu* – przegląd uprawnień użytkowników, wdrożenie zasady minimalnych uprawnień, usunięcie zbędnych kont. W miarę możliwości włączenie uwierzytelniania dwuskładnikowego (2FA) do systemów krytycznych.
    - *Szyfrowanie i zabezpieczenie danych* – zapewnienie szyfrowania nośników z wrażliwymi danymi (dyski laptopów, pamięci USB), szyfrowanie przesyłanych informacji (VPN, SSL/TLS w usługach web), a także bezpieczne przekazywanie danych partnerom (unikanie wysyłania otwartych e-maili z wrażliwymi załącznikami – co niestety wciąż robi 14% firm). Jeśli współpracujemy z biurem rachunkowym lub innym podwykonawcą – uzgodnienie bezpiecznych metod wymiany dokumentów (np. zaszyfrowane pliki z hasłem przekazywanym oddzielnie).
    - *Systemy ochronne* – zainstalowanie i aktualizacja oprogramowania antywirusowego/anty-malware na komputerach, wdrożenie firewalla na styku z internetem, rozważenie prostych rozwiązań EDR (Endpoint Detection & Response) dostosowanych do MŚP, które monitorują nietypowe działania na urządzeniach.
    - *Szkolenie pracowników i polityka bezpieczeństwa* – nawet niewielka firma czy fundacja powinna przeszkolić swój personel (także wolontariuszy) z podstaw bezpieczeństwa: rozpoznawania phishingu, bezpiecznego korzystania z maila, używania menedżerów haseł zamiast notatek itp. Warto stworzyć krótką *politykę cyberbezpieczeństwa* wewnątrz organizacji – spis zasad, do których wszyscy się stosują (np. zakaz używania prywatnych pendrive, wymóg zmiany hasła co X miesięcy, procedura zgłaszania incydentu itp.). Dokument ten będzie też

dowodem świadomego podejścia – co zaprocentuje przy rozmowach z partnerami biznesowymi.

Te podstawowe kroki są zbieżne z wymogami NIS2 w zakresie środków zarządzania ryzykiem – dyrektywa explicite wymaga m.in. kontroli dostępu, świadomości zagrożeń, kryptografii, zarządzania ciągłością działania itd.. Od nich należy zacząć, zanim przejdzie się do bardziej zaawansowanych inwestycji.

3. **Dostosowanie do wymogów formalnych (jeśli dotyczy):** Jeśli po analizie okaże się, że organizacja będzie objęta NIS2 jako podmiot ważny lub kluczowy, należy zaplanować spełnienie konkretnych obowiązków prawnych. Oznacza to m.in.:
    - *Wyznaczenie osoby kontaktowej ds. cyberbezpieczeństwa* – wymaganej do komunikacji z organami (w przypadku NGO może to być np. członek zarządu odpowiedzialny za IT, w firmie – kierownik IT lub zewnętrzny specjalista na umowie).
    - *Opracowanie formalnej strategii zarządzania ryzykiem* – dokumentu opisującego podejście organizacji do identyfikacji i minimalizacji ryzyk cyber (może być częścią szerszej polityki bezpieczeństwa informacji).
    - *Procedury obsługi incydentów i zgłaszania naruszeń* – należy przygotować instrukcje, co robić w razie wykrycia incydentu (kogo powiadomić wewnątrz, jak zabezpieczyć dowody, jak przywrócić działanie) oraz jak zgłaszać incydent na zewnątrz (do CSIRT GOV lub CSIRT MON w Polsce, zgodnie z krajowym systemem cyberbezpieczeństwa). Warto wyznaczyć scenariusze incydentów (np. ransomware, atak DDoS, kradzież laptopa) i przećwiczyć je w ramach zespołu.
    - *Rejestrowanie zdarzeń i monitoring* – by móc w ogóle wykryć incydent i dotrzymać terminów raportowania, organizacja musi gromadzić logi zdarzeń z systemów, mieć podstawowe mechanizmy monitorowania (np. alerty o próbach nieautoryzowanego dostępu). Małe firmy mogą skorzystać z prostych usług typu *Security as a Service* oferowanych w chmurze, które nie wymagają własnej rozbudowanej infrastruktury.
    - *Audyt zgodności i testy bezpieczeństwa* – dobrze jest przeprowadzić przegląd kontrolny (np. z pomocą zewnętrznego audytora) czy wszystkie wymagania dyrektywy zostały spełnione. Testy penetracyjne (choćby uproszczone) pomogą ocenić realny stan bezpieczeństwa. W razie

wykrycia niezgodności lub podatności, trzeba zaplanować działania korygujące przed wejściem przepisów w życie.

Warto tutaj kierować się zasadą proporcjonalności – wdrażamy to, co jest konieczne i uzasadnione skalą działalności. Dyrektywa NIS2 sama mówi o podejściu opartym na ryzyku i proporcjonalności środków. Małe podmioty nie muszą od razu sięgać po najdroższe rozwiązania klasy enterprise; istotne, by spełnić intencję przepisów (zabezpieczyć newralgiczne elementy, mieć świadomość ryzyk i procedury działania). Ewentualne krajowe wytyczne implementacyjne doprecyzują te obowiązki – warto śledzić komunikaty Ministerstwa Cyfryzacji w tym zakresie.

4. **Współpraca branżowa i wymiana informacji:** Jednym z najskuteczniejszych sposobów na podniesienie bezpieczeństwa małych podmiotów jest działanie w grupie. Zaleca się:
    - **Dołączenie do sektorowych inicjatyw wymiany informacji o zagrożeniach (ISAC)** – tzw. **Information Sharing and Analysis Centers** to platformy współpracy, gdzie organizacje z danej branży dzielą się wiedzą o incydentach, podatnościach i najlepszych praktykach. W wielu sektorach (finanse, energia, transport) powstają już polskie ISAC wspierane przez administrację. Członkostwo w takiej sieci umożliwia małej firmie otrzymywanie wczesnych ostrzeżeń o zagrożeniach i uczenie się na cudzych błędach. Przykładowo, jeśli inny podmiot w branży padł ofiarą nowego rodzaju phishingu, ISAC ostrzeże resztę, co pozwoli im wdrożyć prewencję. Współpraca w ramach ISAC jest poufna i oparta na zaufaniu, co sprzyja otwartości – a razem łatwiej obronić się przed wrogiem. NGO mogą szukać podobnych sieci wsparcia w swoim obszarze (np. organizacje humanitarne wymieniające się poradami jak chronić dane beneficjentów).
    - **Korzystanie z wiedzy branżowej i wytycznych** – warto śledzić publikacje i alerty wydawane przez krajowy CSIRT (np. CERT Polska/NASK) oraz przez agencje takie jak ENISA. Te podmioty często publikują poradniki skierowane do MŚP z konkretnymi zaleceniami. Uczestnictwo w konferencjach, webinarach czy szkoleniach branżowych z zakresu cyberbezpieczeństwa również pomoże kadrze zarządzającej zrozumieć aktualne zagrożenia. Dla NGO dostępne są programy szkoleń organizowane przez wyspecjalizowane fundacje lub firmy technologiczne w ramach społecznej odpowiedzialności biznesu (warto poszukać np. projektów typu TechSoup czy ofert pro bono od firm IT).

- **Kooperacja z innymi firmami w ramach ekosystemu** – jeśli działamy w ramach klastrów, stowarzyszeń branżowych czy lokalnych izb gospodarczych, warto podnieść temat cyberbezpieczeństwa na forum tych organizacji. Wspólne wypracowanie rozwiązań (np. grupowe przeszkolenie pracowników kilku firm naraz, co obniży koszt jednostkowy; wynegocjowanie rabatu grupowego u dostawcy rozwiązań bezpieczeństwa; dzielenie się sprawdzonymi procedurami czy politykami) może być bardzo korzystne. Solidarność branżowa w obliczu nowych wymogów pozwoli uniknąć sytuacji, gdzie część mniej przygotowanych podmiotów odstaje – co jak wskazano, i tak oddziałuje na całą branżę.

Wykorzystanie Dostępnych Zasobów

5. **Wykorzystanie dostępnego wsparcia i zasobów:** Rządy i instytucje dostrzegają, że MŚP i NGO mogą potrzebować pomocy we wdrożeniu nowych regulacji. Rekomenduje się poszukiwanie i korzystanie z:
   - *Programów dofinansowania i dotacji* – sprawdzenia, czy np. Polska Agencja Rozwoju Przedsiębiorczości (PARP) oferuje bony na cyfryzację lub dofinansowanie projektów poprawy bezpieczeństwa (w przeszłości były takie inicjatywy). Środki z UE w nowej perspektywie (2021-2027) zawierają komponenty wspierające transformację cyfrową, z których mogą skorzystać także NGO (np. granty na podniesienie kompetencji cyfrowych).
   - *Poradników i narzędzi od ENISA/Komisji Europejskiej* – ENISA (Agencja UE ds. Cyberbezpieczeństwa) publikuje darmowe materiały, w tym dedykowane toolkity dla tworzenia ISAC czy przewodniki zgodności z NIS2. Komisja Europejska powołała też grupę ekspercką CRA, która zapewne przygotuje wytyczne ułatwiające firmom interpretację nowego rozporządzenia. Warto śledzić oficjalne strony (np. Cybersecurity Atlas lub portale Digital Innovation Hubs) – często znajdują się tam sekcje dla MŚP.
   - *Wsparcia od dużych partnerów* – jeżeli MŚP/NGO współpracuje z korporacją, można spróbować nawiązać dialog: zapytać, jakie standardy bezpieczeństwa będą wymagane, poprosić o wskazówki czy nawet pomoc. Część odpowiedzialnych społecznie firm większych uruchamia programy mentoringowe dla swoich dostawców w zakresie cyberbezpieczeństwa, zdając sobie sprawę, że ich własne bezpieczeństwo zależy od zabezpieczeń partnerów. Warto z takiej pomocy skorzystać, traktując ją jako inwestycję w relacje B2B.

6. **Podejście pragmatyczne – bezpieczeństwo jako usługa:** Jeśli brakuje możliwości budowy własnego zespołu IT, rozważ outsourcing funkcji bezpieczeństwa. Na rynku pojawia się coraz więcej ofert skierowanych do MŚP, np. usługi *Security Operations Center as a Service*, gdzie zewnętrzny operator monitoruje sieć klienta 24/7 i informuje o incydentach. Istnieją również tzw. usługi w modelu MSSP (Managed Security Service Provider) obejmujące kompleksową opiekę: od wdrożenia zabezpieczeń, po ich ciągłe zarządzanie. Choć wiąże się to z kosztem abonamentowym, może okazać się tańsze niż samodzielne zatrudnienie specjalisty – a przede wszystkim realnie podniesie poziom ochrony. Ważne jest, by dobierać usługi dostosowane do skali – czasem zamiast rozbudowanych systemów lepsze będzie prostsze, ale właściwie skonfigurowane rozwiązanie chmurowe.

7. **Budowanie kultury cyberodporności:** Regulacje regulacjami, ale kluczowe jest, by wewnątrz organizacji zapanowała odpowiednia kultura. Liderzy MŚP i NGO powinni dawać przykład w kwestii dbałości o bezpieczeństwo (np. sami przestrzegać ustalonych zasad, interesować się tematem, komunikować jasno, że to priorytet). Warto włączyć elementy cyberbezpieczeństwa do codziennego funkcjonowania – krótkie rozmowy o nowych zagrożeniach na zebraniach, dzielenie się ciekawymi przypadkami z mediów („uczymy się na cudzych błędach"), nagradzanie pracowników za wychwycenie i zgłoszenie potencjalnej podatności lub pomysł na usprawnienie bezpieczeństwa. Im bardziej *ludzki czynnik* będzie sprzymierzeńcem, a nie najsłabszym ogniwem, tym łatwiej sprostać zarówno faktycznym zagrożeniom, jak i wymogom formalnym. W perspektywie długofalowej celem jest, aby cyberbezpieczeństwo stało się integralną częścią strategii firmy/organizacji, a nie przykrą koniecznością „bo przepisy każą". Taka zmiana myślenia to najlepsza gwarancja odporności.

3. Długofalowe Korzyści inwestycji w Cyberbezpieczeństwo

Wejście w życie dyrektywy NIS2 oraz rozporządzenia CRA zwiastuje nową erę w podejściu do bezpieczeństwa cyfrowego w Europie. Dla polskich MŚP i NGO początkowy wysiłek dostosowania się może wydawać się znaczący – wiąże się z nim konieczność zdobycia nowych kompetencji, poniesienia kosztów i przeorganizowania niektórych procesów. Jednak w dłuższej perspektywie inwestycja ta przyniesie wymierne, długofalowe korzyści.

Przede wszystkim, zwiększona cyberodporność oznacza mniejsze straty i przestoje spowodowane incydentami. Koszty cyberataków (takie jak odzyskiwanie danych po ransomware, kary za wyciek danych osobowych, utrata reputacji) potrafią wielokrotnie przewyższyć wydatki na prewencję. Każda udaremniona próba włamania to

zaoszczędzone pieniądze i zachowana ciągłość działania biznesu lub misji społecznej NGO. Ponadto silne zabezpieczenia umożliwiają spokojniejszy rozwój – organizacja może z większą pewnością rozszerzać swoją działalność w cyfrowe kanały (e-commerce, usługi online), bo ryzyko związane z atakami jest pod kontrolą.

Po drugie, dostosowanie się do nowych regulacji wpisuje się w globalny trend rosnących wymagań bezpieczeństwa. Można się spodziewać, że kolejne lata przyniosą następne inicjatywy prawne i standardy (choćby wymogi dot. sztucznej inteligencji, ochrony danych w chmurze itp.). Podmioty, które już teraz zbudują fundamenty zgodności i dobre praktyki, zyskają *elastyczność i łatwość adaptacji* do przyszłych wymogów. Będzie to ich przewaga konkurencyjna. Polska gospodarka jako całość również na tym skorzysta – bezpieczne MŚP to stabilniejsze łańcuchy dostaw, większa atrakcyjność inwestycyjna i unikanie czarnych scenariuszy (jak paraliż krytycznych usług publicznych przez cyberatak).

REKOMENDACJE

Skuteczne podnoszenie poziomu cyberbezpieczeństwa w Małych i Średnich Przedsiębiorstwach oraz NGO, wymaga przeprowadzenia analizy wpływu i oceny ryzyka, stopniowego wdrażania działań dostosowanych do nowych wymogów (jeśli mają zastosowanie), oparcia się na współpracy branżowej i wymianie informacji, wykorzystania dostępnego wsparcia i zasobów, przyjęcia pragmatycznego podejścia opartego na modelu bezpieczeństwa jako usługi oraz budowania trwałej kultury cyberodporności w organizacji.

Ponadto dostosowanie do nowych wymogów wpłynie korzystnie na pozycję rynkową tych podmiotów. Wysokie standardy bezpieczeństwa będą coraz częściej postrzegane jako atut – firmy bezpieczne są bardziej wiarygodne, przyciągają świadomych klientów i mogą nawiązywać partnerstwa z wymagającymi kontrahentami. NGO, które zadbają o ochronę danych i infrastruktur, zyskają zaufanie grantodawców oraz beneficjentów. Można więc powiedzieć, że cyberodporność staje się synonimem jakości i zaufania w oczach interesariuszy.

W skali makro natomiast, realizacja założeń NIS2 i CRA przyczyni się do podniesienia ogólnego poziomu bezpieczeństwa w polskiej gospodarce oraz administracji. Im więcej podmiotów – w tym tych mniejszych – będzie chronionych przed atakami, tym trudniej cyberprzestępcom będzie wyrządzić systemowe szkody. Z czasem zmniejszy się liczba udanych incydentów, co odciąży organy ścigania i zespoły reagowania, a

zasoby będą mogły być skierowane na proaktywny rozwój, a nie gaszenie pożarów. Odporna cyfrowo gospodarka to także atrakcyjniejszy ekosystem do inwestowania i rozwijania innowacji – firmy nie będą obawiały się, że jeden atak przekreśli ich dorobek, co sprzyja podejmowaniu śmielszych przedsięwzięć technologicznych.

Podsumowując, wdrożenie regulacji NIS2 i CRA to wyzwanie, które warto podjąć. Zachowanie zgodności z nowymi przepisami nie powinno być traktowane jedynie jako obowiązek prawny, ale jako impuls do rozwoju – szansa na wzmocnienie fundamentów bezpieczeństwa, zwiększenie konkurencyjności i zaufania. W dynamicznie cyfryzującym się świecie inwestycja w cyberbezpieczeństwo jest inwestycją w przyszłość. Organizacje, które już teraz zadbają o cyberodporność, będą lepiej przygotowane na kolejne fale cyfrowej transformacji i będą mogły z niej czerpać pełne korzyści, budując swoją działalność na solidnym, bezpiecznym fundamencie.

Kim Jesteśmy – IS Consulting

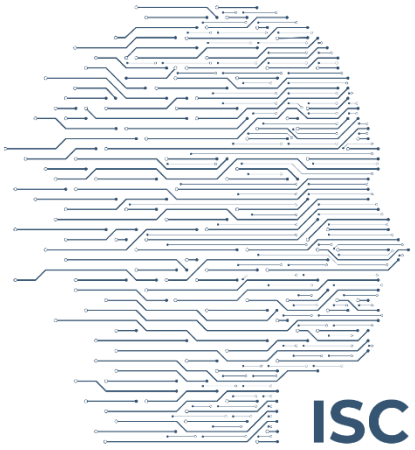
IS Consulting to niezależna firma doradcza oraz prywatny think-tank specjalizujący się w bezpieczeństwie cyfrowym. Działamy z misją wspierania małych i średnich przedsiębiorstw oraz organizacji pozarządowych w budowaniu odporności na zagrożenia cyfrowe – zgodnie z naszym mottem: *Everyone Deserves to be Secure*.

W oparciu o rekomendacje zawarte w tym dokumencie, IS Consulting oferuje swoim klientom, niezależnie od branży i rozmiaru, praktyczne wsparcie dostosowane do realiów małych organizacji, m.in.:

- Prosty audyt zgodności z NIS2/CRA – sprawdzenie gotowości w 6 obszarach
- Gotowe szablony dokumentów i polityk – dostosowane do potrzeb MŚP i NGO
- Szkolenia i webinary dla zarządów i pracowników (również nietechnicznych)
- Subskrypcja ISAC – ostrzeżenia, checklisty i rekomendacje
- Konsultacje 1:1 – omówienie Twojej sytuacji, ryzyk i priorytetów

Źródła:

- Biznes.gov.pl – Walka z cyberprzestępczością – nowe obowiązki firm w Dyrektywie NIS2 - *https://www.biznes.gov.pl/pl/portal/005120*
- Gazeta Prawna – NIS2: czy Polska zostaje w tyle? (artykuł partnerski EY) - *https://biznes.gazetaprawna.pl/artykuly/9468335,nis2-czy-polska-zostaje-w-tyle.html*
- UODO / ChronPESEL.pl – raport z badania dot. bezpieczeństwa danych w MŚP - *https://uodo.gov.pl/pl/138/3258*
- ITReseller – Wdrożenie dyrektywy NIS-2 a bezpieczeństwo cyfrowe MŚP - *https://itreseller.pl/wdrozenie-dyrektywy-nis-2-a-bezpieczenstwo-cyfrowe-msp-wymagany-bedzie-pragmatyzm-podkresla-przemyslaw-kania-dyrektor-generalny-cisco-w-polsce/*
- PARP – Raport o stanie sektora MŚP w Polsce 2024 - *https://www.parp.gov.pl/component/publications/publication/raport-o-stanie-sektora-malych-i-srednich-przedsiebiorstw-w-polsce-2024*
- PAP – Barometr dobroczynności: liczba organizacji pożytku publicznego - *https://www.pap.pl/mediaroom/barometr-dobroczynnosci-srednio-kazdego-dnia-w-polsce-przybywa-dziewiec-organizacji*
- Publicystyka.ngo.pl – Czy NGO mogą sobie pozwolić na unikanie cyfryzacji? - *https://publicystyka.ngo.pl/czy-ngo-moga-sobie-pozwolic-na-unikanie-cyfryzacji*
- SecurityMagazine.pl – Ustawa o odporności cybernetycznej (CRA) - *https://www.securitymagazine.pl/pl/a/ustawa-o-odpornosci-cybernetycznej-juz-obowiazuje*
- Strona KE – Cyber Resilience Act (Shaping Europe's Digital Future) - *https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act*
- Europejski Bank Inwestycyjny – raport o cyfryzacji w UE (2023) - *https://www.eib.org/en/press/all/2023-203-digitalisation-in-the-european-union-progress-challenges-and-future-opportunities?lang=pl*



IS Consulting

www.isconsulting.pl

contact@isconsulting.pl

ul. Żelazna 51/53

00-843 Warszawa