Cyberodporne centrum danych: od audytu bezpieczeństwa do zgodności z NIS2

Krzysztof Młynarski

krzysztof.mlynarski@security.pl

security.pl

DATACENTER GigaCon™

Wprowadzenie

Rola centrów danych i zagrożenia

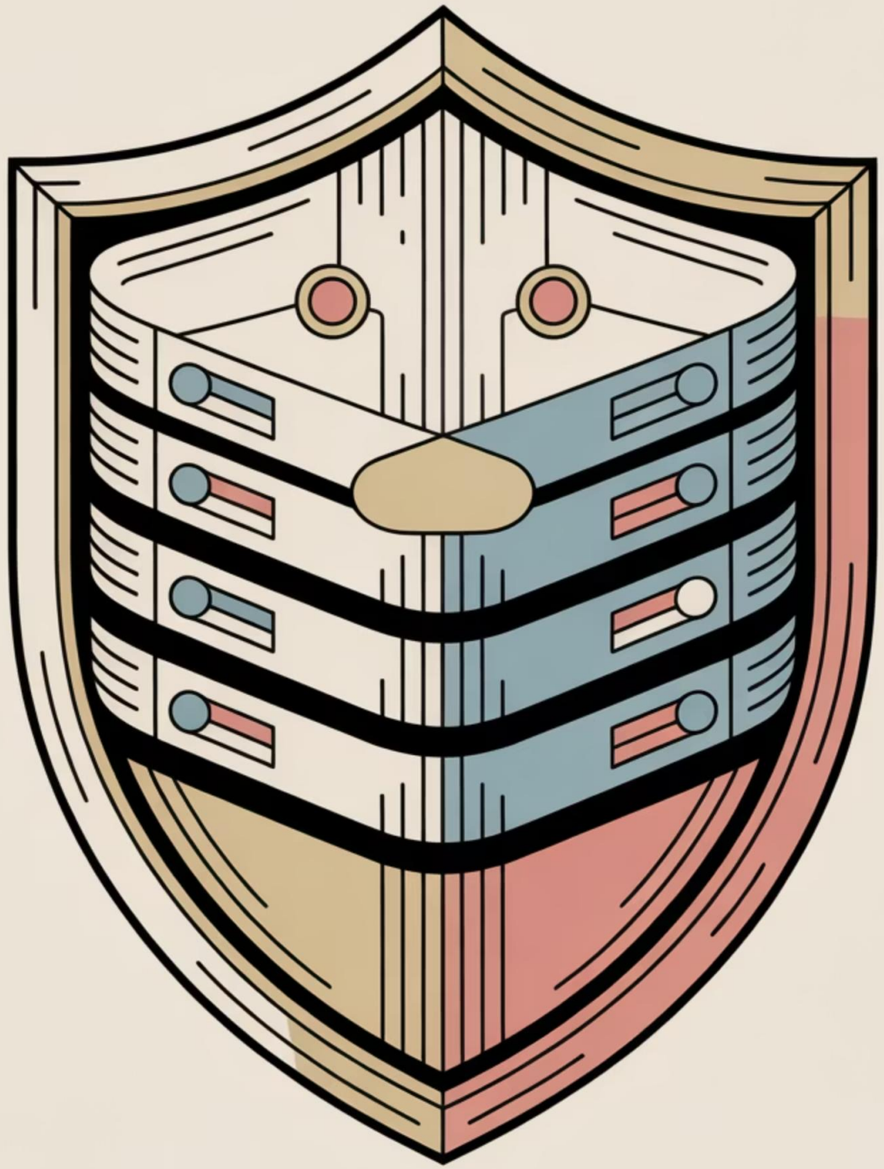
Centrum danych jako infrastruktura krytyczna

Codzienne zagrożenia cyfrowe: ransomware, DDoS

Podejście "all-hazards": odporność fizyczna i cyfrowa

Cyberodporność – co to znaczy?

- Zachowanie usług mimo ataku lub awarii
- Reakcja i szybkie odzyskiwanie sprawności
- Połączenie technologii, procedur i ludzi



NIS2 – nowy paradygmat bezpieczeństwa

NIS2 jako następca dyrektywy NIS1

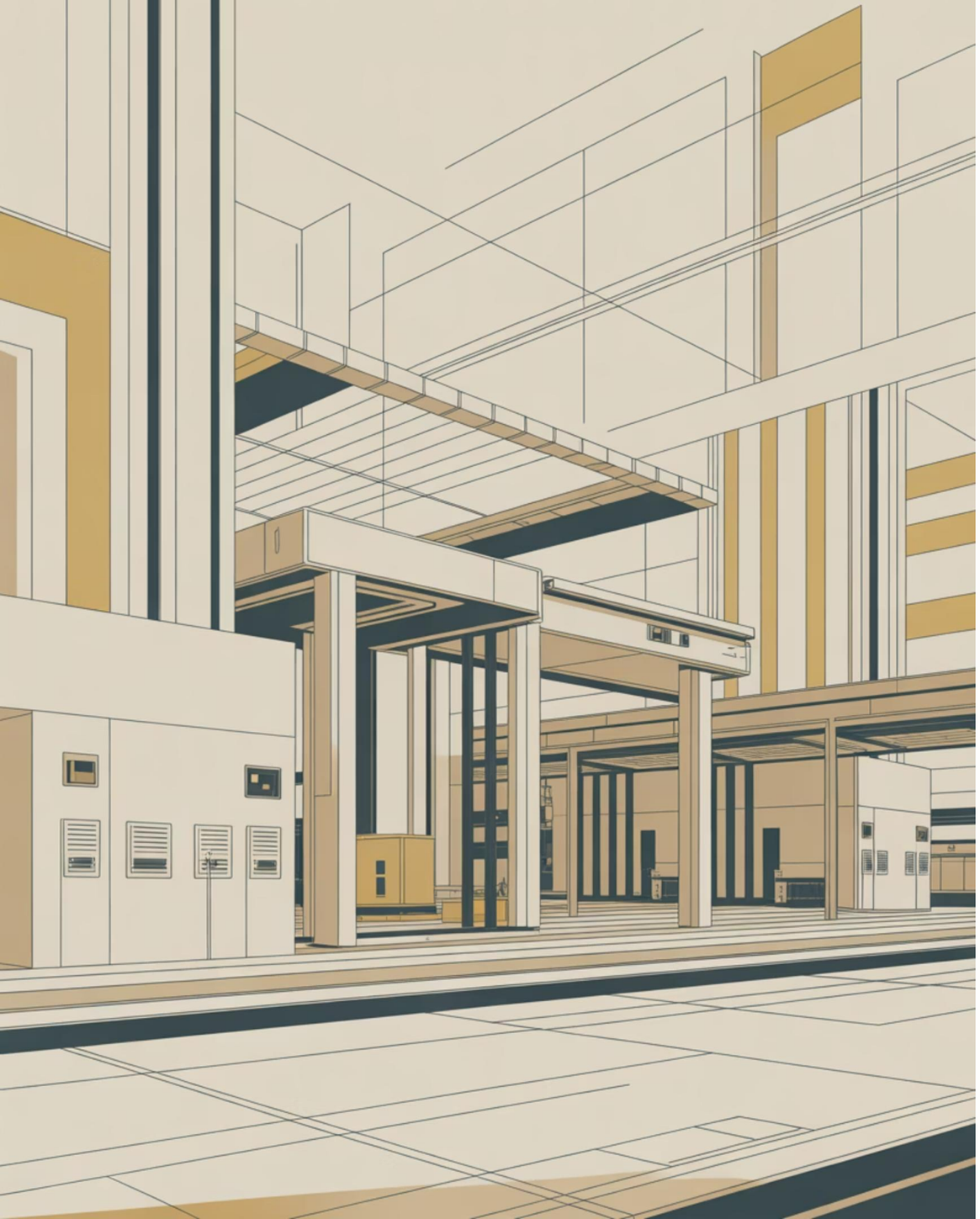
Nowa dyrektywa wprowadza znacznie szersze i bardziej rygorystyczne wymogi bezpieczeństwa dla organizacji w całej Unii Europejskiej.

Rozszerzony zakres: więcej branż i wymagań

Objęcie większej liczby sektorów i podmiotów, z bardziej szczegółowymi wymaganiami technicznymi i organizacyjnymi.

Podniesienie ogólnego poziomu cyberodporności

Cel dyrektywy to wzmocnienie odporności cyfrowej całej Unii poprzez wyższe standardy bezpieczeństwa.



Centra danych jako podmioty kluczowe

1. Podział na podmioty „kluczowe" i „ważne"
2. Centra danych objęte wyższymi wymogami
3. Częstszy nadzór i ryzyko wyższych kar

NIS2 – środki bezpieczeństwa (1/2)

Analiza ryzyka

Analiza ryzyka i aktualizacja polityk

Obsługa incydentów

Obsługa incydentów: wykrycie, reakcja, komunikacja

Ciągłość działania

Planowanie ciągłości działania i Disaster Recovery

NIS2 – środki bezpieczeństwa (2/2)

1

Zarządzanie dostawcami i ocenami ryzyka

Kompleksowa ocena i monitoring łańcucha dostaw oraz partnerów biznesowych.

2

Zarządzanie podatnościami i cykl życia systemów

Systematyczne identyfikowanie, ocena i usuwanie luk bezpieczeństwa w całym cyklu życia systemów.

3

Szyfrowanie, MFA i polityki dostępu

Wdrożenie zaawansowanych mechanizmów ochrony danych i kontroli dostępu do zasobów krytycznych.

Efektywność, higiena i szkolenia

01

Audyty skuteczności środków bezpieczeństwa

Regularne przeglądy i testy weryfikujące działanie wdrożonych zabezpieczeń.

02

Szkolenia i budowanie świadomości użytkowników

Programy edukacyjne podnoszące kompetencje pracowników w zakresie cyberbezpieczeństwa.

03

Minimalne uprawnienia i onboarding/offboarding

Zasada najmniejszych przywilejów oraz procedury zarządzania dostępem przy zmianach kadrowych.

Obowiązki notyfikacyjne i incydenty

Zgłaszanie incydentów w ciągu 24h

Wymóg natychmiastowego raportowania poważnych incydentów bezpieczeństwa do właściwych organów.

Progi notyfikacji dla centrów danych

Określone kryteria i poziomy incydentów wymagające obowiązkowego zgłoszenia.

Gotowość i procedury reagowania

Przygotowane plany działania i zespoły odpowiedzialne za szybką reakcję na zagrożenia.

Audyty i kontrole regulacyjne

→ Inspekcje okresowe i niezapowiedziane

Organy nadzoru mogą przeprowadzać zarówno planowane, jak i niespodziewane kontrole zgodności.

→ Koszty audytu po stronie firmy przy niezgodnościach

W przypadku wykrycia naruszeń, organizacja ponosi koszty przeprowadzonych kontroli.

→ Certyfikaty jako wsparcie, nie gwarancja zgodności

Posiadanie certyfikatów pomaga, ale nie zwalnia z obowiązku pełnej zgodności z NIS2.

Odpowiedzialność zarządu i sankcje

Obowiązki

- Zarząd: obowiązek nadzoru i szkoleń

Członkowie zarządu ponoszą osobistą odpowiedzialność za zapewnienie zgodności i muszą uczestniczyć w szkoleniach z zakresu cyberbezpieczeństwa.

Konsekwencje

- Kary do 10 mln € lub 2% globalnego obrotu
- Wiążące decyzje, zawieszenia i zakazy

Surowe sankcje finansowe oraz możliwość zawieszenia działalności lub zakazu pełnienia funkcji.

Audyt jako pierwszy krok do zgodności

Wykrywanie luk i niezgodności z NIS2

Kompleksowa analiza obecnego stanu bezpieczeństwa i identyfikacja obszarów wymagających poprawy.

Priorytetyzacja i plan naprawczy

Ustalenie kolejności działań naprawczych według poziomu ryzyka i pilności.

Dokumentacja jako dowód należytej staranności

Szczegółowa dokumentacja procesów i działań jako dowód przestrzegania wymogów regulacyjnych.

Od audytu do wdrożenia

Działania naprawcze i zamykanie luk

Systematyczne wdrażanie środków zaradczych dla zidentyfikowanych problemów bezpieczeństwa.

Testy skuteczności wdrożonych środków

Weryfikacja i walidacja poprawności działania nowych zabezpieczeń i procedur.

Potwierdzenie zgodności i gotowości na kontrolę

Finalna weryfikacja pełnej zgodności z wymogami NIS2 i przygotowanie na audyty regulacyjne.

Ciągłe doskonalenie i monitoring

Stałe testy, przeglądy i aktualizacje

Regularne weryfikacje i uaktualnienia systemów bezpieczeństwa zgodnie z ewoluującymi zagrożeniami.

Symulacje incydentów i ćwiczenia IR

Praktyczne scenariusze reagowania na incydenty dla utrzymania gotowości zespołów.

Przegląd polityk i analiza post-mortem

Systematyczna ocena procedur i wyciąganie wniosków z przeszłych zdarzeń bezpieczeństwa.

Wartość zgodności i odporności

Redukcja ryzyka operacyjnego i finansowego

Minimalizacja prawdopodobieństwa wystąpienia kosztownych incydentów bezpieczeństwa i przestojów w działalności.

Wyższa ciągłość usług i zaufanie klientów

Zapewnienie nieprzerwanych usług buduje lojalność klientów i wzmacnia relacje biznesowe.

Wzmocnienie reputacji i pozycji rynkowej

Demonstracja wysokich standardów bezpieczeństwa jako przewaga konkurencyjna i element budowania marki.

Podsumowanie i działanie

Audyt bezpieczeństwa jako fundament

Rozpoczęcie drogi do zgodności od rzetelnej oceny obecnego stanu zabezpieczeń.

Zgodność z NIS2 jako inwestycja

Traktowanie wymogów regulacyjnych jako szansy na wzmocnienie organizacji, a nie tylko jako obowiązku.

Działać proaktywnie – zanim będzie za późno

Wyprzedzające działanie chroni przed sankcjami i minimalizuje ryzyko biznesowe.

Q&A

Dziękuję za uwagę!

Krzysztof Młynarski
krzysztof.mlynarski@security.pl