GECOS
doradztwo IT · ERP · cyber

NIS2 W PRAKTYCE

Czy Twoja firma podlega i co dokładnie trzeba zrobić?

Dlaczego ten materiał jest ważny?

Nie zaczynaj od wdrożenia. Najpierw sprawdź, czy temat dotyczy Twojej firmy.

Ta część jest kluczowa, bo:

- możesz niepotrzebnie wdrażać coś, co Cię nie dotyczy
- albo odwrotnie — już podlegasz i nic z tym nie robiszds

I. Czy Twoja firma podlega NIS2?

1. Wielkość firmy

Sprawdź formalnie:

- liczba pracowników (FTE)
- roczny obrót lub suma bilansowa

Progi orientacyjne:

- średnia firma: 50–250 pracowników
- duża firma: powyżej 250

Jeśli jesteś średni lub duży — możesz być podmiotem ważnym lub kluczowym

2. Branża i typ działalności

Porównaj swoją działalność z sektorami z ustawy.

- energia, transport, bankowość, zdrowie
- produkcja, żywność, chemia, usługi cyfrowe

3. Działalność faktyczna

- co realnie sprzedajesz
- jakie usługi wykonujesz
- jakie procesy obsługujesz

4. Rola w łańcuchu dostaw

- czy klienci są regulowani
- czy wspierasz ich operacje
- czy brak Twojej usługi zatrzymuje proces

5. Sygnały od Klientów

- ankiety bezpieczeństwa
- wymagania compliance
- zapisy w umowach

6. Zależność od systemów

Czy firma działa bez systemów przez 24–48h?

7. Krytyczny dostawca

- unikalna rola
- brak powoduje zatrzymanie klienta

8. Powiązania kapitałowe

- grupa kapitałowa
- sumowanie danych

9. Dostęp do danych klientów

- dostęp do systemów
- przetwarzanie danych

10. Wniosek

Jeśli spełniasz kilka warunków — **podlegasz NIS2**.

II. 25 RZECZY, KTÓRE TRZEBA SPRAWDZIĆ W FIRMIE

Wymaga wdrożenia:

1. Potwierdzenie statusu

Sprawdź, czy firma formalnie podlega pod NIS2 jako podmiot kluczowy lub ważny. W praktyce analizuje się branżę, skalę działalności i rolę firmy w łańcuchu dostaw.

2. Rejestracja w systemie

Zweryfikuj, czy firma musi zostać zgłoszona do odpowiedniego wykazu lub organu nadzorczego. Brak rejestracji może oznaczać formalną niezgodność z przepisami.

Wymaga wdrożenia:
3. Wyznaczenie odpowiedzialnej osoby Firma powinna mieć konkretną osobę odpowiedzialną za obszar cyberbezpieczeństwa i koordynację działań. Bez właściciela procesu większość organizacji działa chaotycznie.
4. Określenie kontekstu organizacji Trzeba jasno opisać, jak działa firma, od czego zależy i które procesy są kluczowe biznesowo. To fundament całego podejścia do bezpieczeństwa.
5. Identyfikacja procesów krytycznych Sprawdź, które procesy zatrzymałyby firmę w przypadku awarii lub cyberataku. Najczęściej są to produkcja, logistyka, sprzedaż lub obsługa klientów.
6. Mapa systemów Firma powinna wiedzieć, jakie systemy posiada i jak są ze sobą powiązane. W wielu organizacjach taka mapa realnie nie istnieje.
7. Rejestr aktywów Należy przygotować listę urządzeń, serwerów, aplikacji, użytkowników i zasobów IT. Bez tego trudno skutecznie zabezpieczać środowisko.
8. Zarządzanie ryzykiem Sprawdź, czy firma regularnie analizuje ryzyka związane z cyberbezpieczeństwem. Chodzi o świadome zarządzanie zagrożeniami, a nie działania „na wyczucie”.
9. Rejestr ryzyk Ryzyka powinny być opisane, ocenione i przypisane do konkretnych działań naprawczych. To pokazuje, że organizacja świadomie kontroluje zagrożenia.
10. Polityka bezpieczeństwa Firma powinna posiadać formalne zasady bezpieczeństwa i procedury działania. Dokumenty muszą odpowiadać realnym procesom, a nie być tylko „papierem do szafy”.
11. Zaangażowanie zarządu NIS2 przenosi odpowiedzialność za bezpieczeństwo również na zarząd. Kierownictwo powinno rozumieć ryzyka i uczestniczyć w decyzjach dotyczących bezpieczeństwa.
12. Zarządzanie dostępami Sprawdź, kto ma dostęp do systemów i danych oraz czy zakres uprawnień jest uzasadniony. Nadmiarowe dostępy są jedną z najczęstszych luk bezpieczeństwa.

Wymaga wdrożenia:
13. Przeglądy uprawnień Dostępy powinny być regularnie weryfikowane i odbierane po zmianach stanowisk lub odejściu pracowników. W wielu firmach stare konta pozostają aktywne latami.
14. Aktualizacje systemów Systemy i urządzenia powinny być regularnie aktualizowane oraz zabezpieczane przed znanymi podatnościami. Brak aktualizacji to jeden z głównych powodów skutecznych ataków.
15. Monitoring systemów Firma powinna monitorować infrastrukturę pod kątem zagrożeń i nietypowych zdarzeń. Bez monitoringu wiele incydentów jest wykrywanych dopiero po dużych stratach.
16. Zabezpieczenie infrastruktury Należy sprawdzić poziom ochrony sieci, serwerów, komputerów i urządzeń mobilnych. Chodzi zarówno o zabezpieczenia techniczne, jak i organizacyjne.
17. Backup danych Kluczowe dane powinny być regularnie kopiowane i zabezpieczane przed utratą lub ransomware. Sam backup nie wystarczy, jeśli nikt go nie kontroluje.
18. Testy odtworzeniowe Trzeba regularnie sprawdzać, czy dane rzeczywiście da się odzyskać po awarii. Wiele firm odkrywa problemy dopiero podczas kryzysu.
19. Plan Disaster Recovery Firma powinna posiadać plan odtworzenia systemów po poważnej awarii lub cyberataku. Plan musi określać kto, co i w jakiej kolejności robi.
20. Plan ciągłości działania Sprawdź, czy organizacja wie, jak utrzymać działanie biznesu podczas kryzysu. Dotyczy to zarówno IT, jak i procesów operacyjnych.
21. Procedura incydentów Powinny istnieć jasne procedury działania po wykryciu incydentu bezpieczeństwa. Ludzie muszą wiedzieć, co robić w pierwszych godzinach kryzysu.
22. Zgłaszanie incydentów NIS2 nakłada obowiązek raportowania poważnych incydentów w określonych terminach. Firma musi wiedzieć, kiedy i komu zgłaszać zdarzenia.

Wymaga wdrożenia:
23. Rejestr incydentów Wszystkie incydenty bezpieczeństwa powinny być dokumentowane i analizowane. Dzięki temu organizacja wyciąga wnioski i ogranicza ryzyko powtórzenia problemu.
24. Kontrola dostawców Sprawdź poziom bezpieczeństwa firm, które mają dostęp do Twoich systemów lub danych. Coraz więcej ataków zaczyna się właśnie przez słabszych dostawców.
25. Szkolenia pracowników Pracownicy powinni regularnie przechodzić szkolenia z cyberbezpieczeństwa i rozpoznawania zagrożeń. Nawet dobre technologie nie pomogą, jeśli użytkownicy popełniają podstawowe błędy.

Podsumowanie

NIS2 to nie tylko projekt IT.
To przede wszystkim:

- uporządkowanie i zabezpieczenie procesów biznesowych,
- ograniczenie ryzyka operacyjnego,
- utrzymanie ciągłości działania firmy,
- przygotowanie organizacji na wymagania klientów, audyty i nowe obowiązki regulacyjne.

Projekt sfinansowany ze środków EU / CPPC w ramach programu „Cyfrowa Europa”

NCC-PL Krajowe Centrum Kompetencji Cyberbezpieczeństwa
Ministerstwo Cyfryzacji
ECCC European Cybersecurity Competence Centre
Co-funded by the European Union