

Harmonogram i lista kontrolna wymogów dla Podmiotów Ważnych i Kluczowych

Nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), wdrażająca unijną dyrektywę NIS2, znacząco rozszerza katalog podmiotów objętych obowiązkami prawnymi oraz wprowadza bezpośrednią odpowiedzialność kierownictwa organów zarządzających. Niniejszy dokument stanowi narzędzie weryfikacji gotowości organizacji do samodzielnego spełnienia wymogów stawianych Podmiotom Kluczowym (PK) oraz Podmiotom Ważnym (PW).

CZĘŚĆ I: IDENTYFIKACJA I REJESTRACJA

Uwaga: Zgodnie z nowymi przepisami podmioty spełniające kryteria klasyfikacyjne mają obowiązek samoidentyfikacji oraz złożenia wniosku o wpis do rejestru w wyznaczonym terminie.

Weryfikacja statusu organizacji

Przeprowadzono analizę struktury zatrudnienia oraz obrotów/bilansu rocznego pod kątem progów (średnie / duże przedsiębiorstwo) oraz przypisano działalność do sektorów z załącznika nr 1 lub 2 ustawy.

Zgłoszenie do rejestru podmiotów KSC

Przygotowano i złożono wniosek o wpis do Wykazu Podmiotów Kluczowych i Ważnych za pośrednictwem dedykowanego systemu teleinformatycznego w terminie do 3 miesięcy od spełnienia przesłanek.

Wyznaczenie osób kontaktowych

Wskazano i zgłoszono do organu właściwego oraz właściwego CSIRT (CSIRT NASK, CSIRT GOV lub CSIRT MON) dane kontaktowe osób odpowiedzialnych za obsługę incydentów (dostępność 24/7/365).

CZĘŚĆ II: ZARZĄDZANIE I ODPOWIEDZIALNOŚĆ KIEROWNICTWA

Szkolenia dla kadry zarządzającej

Członkowie zarządu / organu zarządzającego odbyli obowiązkowe szkolenie z zakresu zarządzania ryzykiem w cyberbezpieczeństwie oraz prawnych obowiązków KSC.

Formalne zatwierdzenie dokumentacji SZBI

Kierownictwo organizacji formalnie zatwierdziło polityki zarządzania ryzykiem, procedury obsługi incydentów oraz ciągłości działania.

Budżet na bezpieczeństwo

Wyodrębniono i zatwierdzono dedykowany budżet na wdrożenie, utrzymanie oraz audytowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

CZĘŚĆ III: SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI (SZBI)

Szacowanie i analiza ryzyka

Wdrożono okresowy, udokumentowany proces szacowania ryzyka w cyklu co najmniej rocznym lub po każdej istotnej zmianie w infrastrukturze IT/OT.

Polityka Bezpieczeństwa Teleinformatycznego

Zarządzanie uprawnieniami (IAM / PAM)

Wdrożono zasadę minimalnych uprawnień (Least Privilege) oraz zasadę wiedzy koniecznej (Need-to-Know). Wprowadzono obowiązkowe uwierzytelnianie wieloskładnikowe.

Bezpieczeństwo łańcucha dostaw

Wdrożono procedurę weryfikacji ryzyka cyberbezpieczeństwa u dostawców usług i produktów ICT. Określono minimalne wymagania bezpieczeństwa w umowach z dostawcami.

Kryptografia i szyfrowanie

Wdrożono nakaz szyfrowania danych w spoczynku (Data at Rest) oraz w transmisji (Data in Transit) przy użyciu zweryfikowanych i aktualnych algorytmów.

CZĘŚĆ IV: ZARZĄDZANIE INCYDENTAMI I CIĄGŁOŚCIĄ DZIAŁANIA

Procedura zgłaszania incydentów (rygor czasowy KSC)

Wdrożono procedurę wykrywania i klasyfikacji incydentów umożliwiającą dotrzymanie ustawowych terminów raportowania do CSIRT:

- do 24 godzin: wczesne ostrzeżenie (Early Warning) o incydencie poważnym;
- do 72 godzin: zgłoszenie incydentu wraz z wstępną oceną skutków;
- do 1 miesiąca: raport końcowy z analizy powdrożeniowej i działań naprawczych.

Plan Ciągłości Działania (BCP) i Disaster Recovery (DRP)

Opracowano oraz formalnie przetestowano co najmniej raz w roku plany awaryjne, procedury tworzenia i odzyskiwania kopii zapasowych (Backup) z uwzględnieniem izolacji strefowej (przechowywanie kopii offline / immutable).

CZĘŚĆ V: AUDYT, MONITOROWANIE I KONTROLA

System rejestracji i analizy logów

Wdrożono scentralizowany system gromadzenia oraz analizy dzienników zdarzeń (SIEM / log management) zapewniający integralność logów oraz ich retencję przez wymagany okres.

Niezależny audyt bezpieczeństwa

Zaplanowano lub przeprowadzono niezależny audyt bezpieczeństwa systemu teleinformatycznego używanego do świadczenia usług (wymóg przeprowadzenia audytu co najmniej raz na 2 lata).

Testy penetracyjne i podatności

Wdrożono regularne skanowanie podatności oraz cykliczne testy penetracyjne kluczowej infrastruktury cyfrowej.