SULI CYBERSECURITY

Checklista NIS2 dla instytucji publicznych

25 punktow kontrolnych zgodnosci
z Dyrektywa UE 2022/2555

Darmowy material | Kwiecien 2026

suli.pl | m@suli.pl | 691 10 20 10

Czym jest NIS2 i kogo dotyczy?

Dyrektywa NIS2 (UE 2022/2555) to najwazniejsza europejska regulacja cyberbezpieczenstwa. Weszla w zycie w styczniu 2023 roku, a panstwa czlonkowskie musza ja implementowac do prawa krajowego. NIS2 znaczaco rozszerza zakres podmiotow objetych obowiazkami cyberbezpieczenstwa w porownaniu do poprzedniej dyrektywy NIS.

NIS2 dotyczy m.in.: jednostek administracji publicznej (urzedy gmin, starostwa, urzedy marszalkowskie), podmiotow swiadczacych uslugi kluczowe (energetyka, transport, zdrowie, woda), podmiotow swiadczacych uslugi wazne (pocztowe, odpady, zywnosc, produkcja). Dla instytucji publicznych kluczowe sa wymogi dotyczace analizy ryzyka, zarzadzania incydentami, ciaglolsci dzialania i szkolen.

⚖ Kary za brak zgodnosci

NIS2 wprowadza kary finansowe za niespelnienie wymogów: do 10 mln EUR lub 2% rocznego obrotu globalnego (whichever is higher) dla podmiotow kluczowych. Dla podmiotow waznych: do 7 mln EUR lub 1.4% obrotu. Ponadto -- odpowiedzialnosc osobista kadry zarzadzajacej.

ZARZADZANIE RYZYKIEM

- ☐ Przeprowadzono formalna analize ryzyka cyberbezpieczenstwa (np. wg ISO 31000 / NIST CSF)
- ☐ Istnieje rejestr aktywow IT (serwery, stacje robocze, urzadzenia sieciowe, oprogramowanie)
- ☐ Zidentyfikowano krytyczne systemy i dane, od ktorych zalezy ciaglosc dzialania urzedu
- ☐ Okreslono wlascicieli ryzyk i osobe odpowiedzialna za cyberbezpieczenstwo

POLITYKI I PROCEDURY

- ☐ Istnieje aktualna Polityka Bezpieczenstwa Informacji zatwierdzona przez kierownictwo
- ☐ Wdrozono procedure zarzadzania incydentami z jasnymi krokami eskalacji
- ☐ Istnieje plan ciaglolsci dzialania (BCP) i plan disaster recovery (DRP)
- ☐ Wdrozono procedure zarzadzania dostepem i przegladow uprawnien
- ☐ Istnieje polityka bezpiecznej pracy zdalnej

OCHRONA TECHNICZNA

- ☐ Systemy operacyjne i oprogramowanie sa regularnie aktualizowane (patch management)
- ☐ Stosowane sa zapory ogniowe (firewall) i systemy IDS/IPS
- ☐ Wdrozono rozwiazanie antywirusowe/EDR na wszystkich stacjach i serwerach
- ☐ Dane sa szyfrowane w transmisji (HTTPS, VPN) i w spoczynku

- [ ] Stosowane jest uwierzytelnianie wieloskladnikowe (MFA) dla krytycznych systemow
- [ ] Konfiguracja serwerow i urzadzen jest wzmocniona (hardening wg CIS Benchmarks)

BACKUP I ODPORNOSC

- [ ] Wykonywane sa regularne kopie zapasowe wg zasady 3-2-1
- [ ] Backup jest testowany -- przeprowadzono probne odtworzenie w ciagu ostatnich 6 miesiecy
- [ ] Kopie zapasowe sa przechowywane offline lub w izolowanej lokalizacji

SZKOLENIA I SWIADOMOSC

- [ ] Wszyscy pracownicy przeszli szkolenie z cyberbezpieczenstwa w ciagu ostatnich 12 miesiecy
- [ ] Przeprowadzono symulacje phishingowe
- [ ] IOD (Inspektor Ochrony Danych) jest wyznaczony i przeszkolony

RAPORTOWANIE I ZGODNOSC

- [ ] Urzad wie, do którego CSIRT (NASK / GOV) nalezy raportowac incydenty
- [ ] Ustanowiono procedure raportowania w ciagu 24h (wczesne ostrzezenie) i 72h (raport)
- [ ] Dokumentacja jest gotowa na kontrole zewnetrzna (NIK, UODO, CSIRT)
- [ ] Prowadzony jest rejestr incydentow bezpieczenstwa

20-25	12-19	0-11
Dobra ochrona Kontynuujcie	Wymaga pracy Priorytetowe braki	Krytyczny Pilny audyt