SynergyIT

OFICJALNY PRZEWODNIK INŻYNIERSKI B2B

Checklista Odporności na Ransomware i Audytu Wdrożenia Dyrektywy NIS2

Praktyczny przewodnik techniczno-prawny dla Członków Zarządów, Dyrektorów IT i CISO przedsiębiorstw zatrudniających 50–250 pracowników.

⚠️ **Istotna uwaga prawna (Dyrektywa NIS2):** Brak wdrożonych procedur zarządzania ryzykiem, natychmiastowego odzyskiwania danych oraz zgłaszania incydentów skutkuje osobistą odpowiedzialnością członków zarządu i karami finansowymi sięgającymi 10 000 000 EUR lub 2% rocznego światowego obrotu.

CZĘŚĆ 1: OCHRONA PUNKTÓW KOŃCOWYCH I ODPORNOŚĆ NA RANSOMWARE

STATUS	WYMÓG TECHNICZNY	WYTYCZNE INŻYNIERSKIE SYNERGY IT
☐	**1. Aktywna ochrona heurystyczna AI**	Tradycyjne antywirusy sygnaturowe zawodzą w starciu z atakami Living-off-the-Land. Wymagany monitoring behawioralny wykrywający nietypowe procesy szyfrowania w czasie <3 sekundy.
☐	**2. Lokalny natychmiastowy rollback**	Wdrożenie technologii automatycznego odwracania zmian z chronionego, ukrytego bufora bez konieczności płacenia okupu ani przywracania całej maszyny z chmury.
☐	**3. Ochrona przed modyfikacją kopii (WORM)**	Nowoczesne ransomware najpierw wyszukuje i kasuje lokalne backupy. Wymagana niezmienność danych (Immutable Storage) uniemożliwiająca usunięcie kopii nawet z uprawnieniami administratora domenowego.
☐	**4. Zabezpieczenie protokołów SMB i RDP**	Całkowite odcięcie portów RDP/SMB od publicznego Internetu, wymuszenie VPN z uwierzytelnianiem wieloskładnikowym (MFA) dla każdego dostępu zdalnego.

CZĘŚĆ 2: CIĄGŁOŚĆ DZIAŁANIA I DISASTER RECOVERY (DRAAS)

STATUS	WYMÓG TECHNICZNY	WYTYCZNE INŻYNIERSKIE SYNERGY IT
☐	**5. Reguła kopii 3-2-1-1-0**	3 kopie danych, 2 różne nośniki, 1 kopia w zewnętrznym polskim Data Center Tier III, 1 kopia offline/niezmienna, 0 błędów podczas automatycznej weryfikacji restore.
☐	**6. Zdefiniowane i przetestowane RTO/RPO**	Maksymalny dopuszczalny czas niedostępności (RTO) <15 minut oraz maksymalna akceptowalna utrata danych (RPO) <1 godzina w środowisku Disaster Recovery as a Service (DRaaS).

STATUS	WYMÓG TECHNICZNY	WYTYCZNE INŻYNIERSKIE SYNERGY IT
☐	**7. Cykliczny Disaster Recovery Drill**	Minimum raz na kwartał testowe uruchomienie kluczowych maszyn (ERP, bazy SQL, kontrolery domeny) w izolowanej sieci chmurowej bez wpływu na produkcję.

CZĘŚĆ 3: PROCEDURY ZGODNOŚCI I ZARZĄDZANIE INCYDENTAMI (NIS2)

STATUS	WYMÓG DYREKTYWY	PROCEDURA OPERACYJNA
☐	**8. Zgłaszanie incydentów w 24h**	Zgodnie z art. 23 NIS2 wdrożona procedura wczesnego ostrzegania (Early Warning) do właściwego zespołu CSIRT w ciągu 24h od wykrycia ataku oraz raport wstępny w 72h.
☐	**9. Audyt łańcucha dostaw (Supply Chain)**	Weryfikacja dostawców oprogramowania, integratorów oraz usług chmurowych pod kątem spełniania norm ISO 27001 oraz certyfikacji centrów przetwarzania danych.
☐	**10. Obowiązkowe szkolenia zarządu i kadr**	Udokumentowane szkolenia dla kadry zarządzającej z zakresu odpowiedzialności osobistej oraz cykliczne testy phishingowe dla pracowników.

Potrzebujesz wsparcia inżynierskiego lub bezpłatnego audytu wstępnego?

Inżynierowie poziomu L3 w Synergy IT od ponad 20 lat wdrażają zaawansowane środowiska backupu, wirtualizacji i cyberbezpieczeństwa. Skorzystaj z bezpłatnego 30-dniowego testu rozwiązania **SynergyIT Total Protect** (opartego o technologię Acronis Cyber Protect Cloud w polskim Data Center) z pełną asystą wdrożeniową.

Bezpośredni telefon do inżyniera: +48 793 555 001 **E-mail: pawel.sadowski@synergyit.com.pl**

© 2026 Synergy IT Sp. z o.o. • Wszelkie prawa zastrzeżone