RAPORT OPERACYJNY Z OBSŁUGI INCYDENTU

Realizacja art. 11 ust. 1 pkt 1 Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC)

Operator Usługi Kluczowej:	EneXis Dystrybucja Sp. z o.o. (Sektor: Energia)	**Identyfikator:**	INC-2026-0482
Usługa Kluczowa:	Dystrybucja energii elektrycznej	**Krytyczność:**	WYSOKA (KRYTYCZNY)
Klasyfikacja (KSC):	Incydent Istotny (Zgłoszenie do CSIRT MON/ NASK/GOV)	**Model realizacji:**	Hybrydowy (Zewnętrzny SOC MSSP + Wewnętrzny Koordynator)

Scenariusz: Atak Ransomware na stację inżynieryjną w podsieci IT/OT

Poniższy dokument przedstawia symulację i szczegółowy przebieg obsługi incydentu bezpieczeństwa zgodnie z wymaganiami polskiej Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC) oraz normami ISO/IEC 27035 i NIST SP 800-61. Incydent dotyczy próby infekcji złośliwym oprogramowaniem szyfrującym na stacji operatorskiej posiadającej dostęp do segmentu zarządzania siecią dystrybucyjną.

Pełen przebieg osi czasu (System Ticketowy)

Czas	Faza procesu	Opis działania i przebieg techniczny	Odpowiedzialność
02:14:10	I: WYKRYWANIE	System EDR na stacji `SRV-ENG-04` generuje alert o uruchomieniu nieznanego skryptu PowerShell próbującego wyłączyć usługę Volume Shadow Copy (VSS).	Zautomatyzowany EDR / SIEM
02:18:00	II: ANALIZA	Analityk L1 SOC (MSSP) weryfikuje alert. Wyklucza false-positive. Potwierdza obecność skompromitowanych poświadczeń administratora lokalnego. Status: Realny Incydent.	Analityk L1 SOC (Zewnętrzny)
02:25:00	II: TRIAŻ / ESKALACJA	Klasyfikacja wpływu: Stacja ma bezpośrednie połączenie ze strefą DMZ systemów SCADA. Eskalacja do Koordynatora OUK oraz powiadomienie L2 zgodnie z matrycą eskalacji.	Analityk L2 SOC / SPOC
02:35:00	III: POWSTRZYMANIE	**Containment:** Zdalna izolacja sieciowa hosta `SRV-ENG-04` za pomocą agenta EDR. Blokada konta domenowego administratora na kontrolerze AD.	Inżynier L3 SOC / Koordynator Decyzyjny OUK

Czas	Faza procesu	Opis działania i przebieg techniczny	Odpowiedzialność
03:10:00	II: GŁĘBOKA ANALIZA	Analiza śledcza (Forensics): Wykryto wektor wejścia – podatność w usłudze VPN (niezaktualizowana poprawka). Potwierdzono brak lateral movement do strefy OT.	Zespół Forensics / CSIRT
05:30:00	RAPORTOWANIE KSC	Weryfikacja progów incydentu istotnego. Koordynator OUK wysyła formalne zgłoszenie incydentu do właściwego CSIRT poziomu krajowego w czasie poniżej 24h.	Koordynator Decyzyjny OUK
08:45:00	III: ERADYKACJA	Wycofanie podatnej sesji VPN, wymuszenie zmiany haseł dla wszystkich kont uprzywilejowanych. Pełne skanowanie antywirusowe systemów sąsiadujących.	Zespół IT / Bezpieczeństwa OUK
11:15:00	III: ODTWARZANIE	Instalacja czystego obrazu systemu operacyjnego na `SRV-ENG-04` z verified backup. Przywrócenie konfiguracji i wdrożenie brakujących łatek (patching).	Administratorzy Systemowi OUK
14:00:00	IV: ZAMKNIĘCIE	Testy integralności połączeń z DMZ SCADA. Brak anomalii. Oficjalne zamknięcie zgłoszenia w systemie ticketowym. Usługa kluczowa działa bez zakłóceń.	Koordynator Decyzyjny OUK / SOC

Kluczowa Rola Koordynatora OUK w Modelu Outsourcingu (MSSP)

Mimo że monitoring i techniczna izolacja były realizowane przez zewnętrzny SOC, to **Koordynator Decyzyjny po stronie Operatora Usługi Kluczowej** podjął kluczowe decyzje: zgodę na izolację stacji inżynieryjnej w trakcie pracy operacyjnej oraz formalne zgłoszenie incydentu do CSIRT poziomu krajowego (zgodnie z prawem KSC odpowiedzialność ta nie może zostać w pełni wyoutsorsowana).

Działania poincydentalne (Faza IV — Analiza Post-Mortem)

W dniu następnym zwołano spotkanie zespołu kryzysowego w celu wyciągnięcia wniosków i minimalizacji ryzyka ponownego wystąpienia incydentu o podobnym wektorze.

Wnioski i podjęte działania korygujące:

- **Aktualizacja Playbooks:** Zmiana procedury weryfikacji podatności na bramach VPN – wdrożenie rygorystycznego okna serwisowego na poprawki krytyczne (maksymalnie 48h od publikacji vendor-patcha).
- **Modyfikacja Architektury:** Wprowadzenie bezwzględnego uwierzytelniania wieloskładnikowego (MFA) dla wszystkich sesji VPN, w szczególności dla kont administracyjnych i personelu inżynieryjnego.
- **Przegląd SLA i procedur:** Potwierdzono, że zewnętrzny partner SOC zareagował w czasie 4 minut (SLA wynosiło 15 minut dla priorytetu Krytycznego). Raport techniczny z ćwiczeń cybernetycznych zostanie zaktualizowany o ten scenariusz w IV kwartale.