CSIRT CeZ

Centrum e-Zdrowia

ATAK RANSOMWARE – CO ROBIĆ?

One-pager dla podmiotów ochrony zdrowia

PIERWSZE 60 MINUT - gdy podejrzewasz ransomware

Nie wyłączaj. Nie płać. Nie czyść.

IZOLUJ, NIE WYŁĄCZAJ

Odłącz LAN/Wi-Fi, włącz EDR remote isolation, blokadę MAC
Nie restartuj i nie wyłączaj — utracisz dowody z pamięci

ZABEZPIECZ DOWODY

Zrób zdjęcia/zrzuty ekranu (notatka okupu, podejrzane procesy)
Zachowaj logi: AD, EDR, firewall, VPN, e-mail, kopie zapasowe

ZWOŁAJ SZTAB KRYZYSOWY

Kierownik podmiotu, ASI, IOD, IOSI, dyrektor medyczny, rzecznik
Wyznacz osobę do kontaktu z CSIRT i jeden kanał komunikacji poza firmową siecią

ZGŁOŚ DO CSIRT CeZ

e-mail incydent@csirt.cez.gov.pl
Skonkaktuj się od razu, nawet jeśli nie masz pełnych danych

URUCHOM PLAN CIĄGŁOŚCI (BCP)

Tryb papierowy: izba przyjęć, oddziały, apteka, diagnostyka
Priorytet: bezpieczeństwo pacjenta i świadczenia ratujące życie

ZABEZPIECZ KOPIE ZAPASOWE

Fizycznie odłącz backupy od sieci. Sprawdź integralność ostatnich kopii, zanim zaczniesz odtwarzanie. Nie podłączaj backupu do zainfekowanej sieci

NIE NEGOCJUJ I NIE PŁAĆ OKUPU

Płatność nie gwarantuje odzyskania danych, może naruszać sankcje i finansuje kolejne ataki. Komunikacja z atakującym — tylko przez profesjonalistów (DFIR)

KOGO I KIEDY ZAWIADOMIĆ

24H CSIRT CeZ (SEKTOROWY)

+48 573 205 962 • incydent@csirt.cez.gov.pl
Wstępne zgłoszenie incydentu poważnego — niezwłocznie, nie później niż 24 h od wykrycia (KSC)

24H CSIRT NASK / CSIRT GOV (KRAJOWY) — OPCJONALNIE

NASK/CERT Polska: incydent.cert.pl • cert@cert.pl
CSIRT GOV (jednostki rządowe): dyżurny +48 22 585 93 73 • csirt.gov.pl

72H UODO — NARUSZENIE DANYCH OSOBOWYCH

Formularz: uodo.gov.pl lub biznes.gov.pl • podpis ePUAP/kwalifikowany
Art. 33 RODO; powiadomienie osób — art. 34 (przy wysokim ryzyku)

POLICJA / CBZC — ZAWIADOMIENIE O PRZESTĘPSTWIE

Centralne Biuro Zwalczania Cyberprzestępczości: cbzc.policja.gov.pl
Lokalna jednostka Policji, art. 269a, 287 k.k. Zachowaj dowody do postępowania

WEWNĄTRZ: KIEROWNICTWO, MZ, NFZ, PODMIOT TWORZĄCY

Kierownik podmiotu, organ założycielski, właściwy oddział NFZ, MZ — jeśli incydent wpływa na ciągłość świadczeń zdrowotnych

CZEGO NIE ROBIĆ

Nie wyłączaj i nie restartuj zainfekowanych maszyn — stracisz dowody (RAM, klucze).

Nie usuwaj „podejrzanych" plików, nie czyść systemu, nie kasuj logów.

Nie płać okupu i nie negocjuj samodzielnie z atakującym.

Nie podłączaj kopii zapasowych do „brudnej" sieci — zaszyfrujesz również backup.

Nie publikuj szczegółów technicznych ataku w mediach społecznościowych.

Nie używaj firmowej poczty/komunikatorów do koordynacji — mogą być monitorowane.

Nie odtwarzaj produkcji bez potwierdzenia, że środowisko jest czyste (DFIR).

PRZYGOTUJ SIĘ, ZANIM DOJDZIE DO ATAKU - to znacznie zmniejsza jego skutki

PLAN IRP + BCP/DRP

Aktualny, testowany min. raz w roku (tabletop)

MFA I SEGMENTACJA SIECI

MFA na kontach uprzywilejowanych, VPN, poczcie; izolacja AD

BACKUP 3-2-1 + WORM

Min. jedna kopia offline; testy odtworzenia

EDR + CENTRALNE LOGI (SIEM)

Retencja ≥ 12 mies.: AD, firewall, VPN, EDR, e-mail

MONITOROWANIE ZDARZEŃ

Całodobowa obserwacja logów, np. usługa SOC

OSOBA KONTAKTOWA W CSIRT CEZ

Zgłoś: cez.gov.pl/zglos-osobe-do-kontaktu

PROCEDURY „TRYBU PAPIEROWEGO"

Izba przyjęć, oddziały, apteka, diagnostyka

ŚWIADOMOŚĆ PERSONELU

Szkolenia phishingowe i jasna ścieżka zgłaszania

RETAINER DFIR

Zewnętrzny zespół reagowania 24/7 — przed incydentem

CSIRT CeZ — 24/7 dla podmiotów ochrony zdrowia • incydent@csirt.cez.gov.pl

Formularz: https://cez.gov.pl/pl/page/zglos-incydent • Sprawy ogólne: info@csirt.cez.gov.pl • TLP / PGP zalecane