Zasady postępowania w przypadku ataku ransomware

1. **Aktywuj procedurę IR i wyznacz role** (lider incydentu, containment, forensics, komunikacja, IT/OT, vendorzy). Ustal bezpieczny kanał łączności poza środowiskiem objętym incydentem.
2. **Natychmiast zatrzymaj rozprzestrzenianie**: odłącz zainfekowane i podejrzane hosty od sieci (LAN/Wi-Fi/VPN), odetnij udziały plików i segmenty, blokuj ruch do/z podejrzanych adresów/domen na FW/Proxy.
3. **Ogranicz uwierzytelnianie i uprawnienia**: zablokuj podejrzane konta, przerwij aktywne sesje, wstrzymaj logowania uprzywilejowane (admin), zabezpiecz konta „break-glass" tylko dla IR.
4. **Nie wyłączaj systemów domyślnie** (zachowanie śladów). Wyłączaj tylko, jeśli trwa aktywne szyfrowanie/niszczenie i izolacja nie wystarcza do zatrzymania incydentu.
5. **Zabezpiecz dowody**: wykonaj zrzuty pamięci/obrazy dysków (kluczowe hosty), eksport logów (EDR, AD/IdP, VPN, firewall, proxy, e-mail/M365, serwery plików), zachowaj łańcuch dowodowy.
6. **Określ zakres incydentu**: które systemy, konta, segmenty i usługi są naruszone (szczególnie: AD/IdP, hypervisory, backupy, narzędzia zdalnego zarządzania/RMM, poczta).
7. **Oceń eksfiltrację danych**: sprawdź oznaki kradzieży danych (nietypowe transfery, archiwizacja, narzędzia typu rclone/megasync), przygotuj listę potencjalnie dotkniętych zbiorów danych.
8. **Zidentyfikuj ransomware i TTP**: na podstawie noty okupu, rozszerzeń plików, IOC, telemetrii EDR. Zweryfikuj, czy istnieją wiarygodne narzędzia deszyfrujące (ale nie zakładaj, że pomogą).
9. **Przyjmij brak zaufania do naruszonych systemów**: traktuj je jako potencjalnie zainstalowane z backdoorem/persistence.
10. **Zabezpiecz kopie zapasowe i repozytoria**: odizoluj backupy, sprawdź niezmienność (immutable), ustal „last known good", wstrzymaj automatyczne zadania backup/replication, jeśli mogą przenosić infekcję.
11. **Nie przywracaj usług przed pełnym opanowaniem sytuacji**: najpierw zatrzymaj wektor ataku, lateral movement i persistence; dopiero potem recovery.
12. **Eradykacja i rotacja sekretów**: usuń mechanizmy trwałości, zaktualizuj/załatataj wektor wejścia; zrotuj hasła, klucze API, certyfikaty, konta serwisowe; jeśli naruszone AD – rozważ pełną procedurę odzysku (w tym reset KRBTGT) i przegląd uprawnień.

K3 System Sp. z o.o.
NIP 9521743814
www.k3system.com.pl

K3 Business Park
Kosmatki 70
03-982 Warszawa

13. **Odbuduj środowisko na czysto**: reinstalacja z golden images, aktualizacje, hardening, minimalne uprawnienia, MFA. Dołączaj do domeny/produkcji dopiero po weryfikacji.
14. **Odtwarzaj dane w sposób kontrolowany**: przywracaj głównie dane użytkowników; blokuj/filtruj wykonywalne i ryzykowne typy (EXE/DLL/MSI/SYS/LNK/JS/VBS/PS1/HTA/ISO/makra), skanuj przed i po restore, stosuj allowlisting tam gdzie możliwe.
15. **Podłączaj do produkcji tylko zweryfikowane systemy**: testy funkcjonalne + testy bezpieczeństwa (EDR, reguły FW, brak podejrzanych usług/zadań, baseline).
16. **Wzmocnij monitoring po odbudowie**: podnieś poziom logowania, alerty na nietypowe logowania, tworzenie kont, zmiany GPO, masowe operacje na plikach, ruch do C2; aktywne threat hunting przez ustalony okres.
17. **Komunikacja i obowiązki formalne**: prowadź spójną komunikację do kierownictwa, użytkowników, vendorów; jeśli dotyczy danych osobowych/kontraktów – uruchom ścieżkę prawną i ocenę obowiązków notyfikacyjnych.
18. **RCA i działania zapobiegawcze**: analiza przyczyny, poprawki procesów i techniki (segmentacja, MFA, zasada najmniejszych uprawnień, backup 3-2-1-1-0, testy odtworzeń, EDR/MDR, patching).
19. **Udokumentuj incydent end-to-end**: oś czasu, decyzje, koszty, wskaźniki kompromitacji, wykonane kroki, wnioski i plan dalszych działań.