Audyt odporności na scenariusz destrukcyjny (Wiper)

Poniższy zestaw pytań kontrolnych pomaga ocenić poziom przygotowania organizacji na atak typu wiper, taki jak incydent z udziałem DynoWipera. Celem jest identyfikacja słabych punktów w obszarach backupu, odzyskiwania danych i bezpieczeństwa OT/IT - nie ocena pracowników, lecz weryfikacja odporności systemu.

1. Kwestia “Być albo nie być” (Backup i Odtwarzanie)

Pamiętaj: Wiper nie szyfruje, on niszczy. Jeśli backup jest widoczny w sieci, też zostanie zniszczony.

[ ] Czy mamy kopie zapasowe “Cold/Offline”? - Czy istnieje kopia kluczowych systemów (szczególnie konfiguracji SCADA/OT), która jest fizycznie odłączona od sieci (na taśmie, dysku w sejfie)?

[ ] Czy backupy są “Immutable” (niezmienialne)? - Czy stosujemy technologię, która uniemożliwia nadpisanie lub skasowanie backupu przez określony czas, nawet z uprawnieniami administratora?

[ ] Kiedy ostatnio zrobiliśmy test "Bare Metal Recovery"? - Czy próbowaliśmy odtworzyć środowisko od zera na czystym sprzęcie, zakładając, że stary sprzęt jest uceglony (trwale uszkodzony programowo i nie nadaje się do użytku)?

[ ] Jaki jest nasz realny RTO (Recovery Time Objective) dla OZE/OT? – Ile godzin/dni zajmie nam ręczne przeprogramowanie sterowników na farmach wiatrowych/słonecznych, jeśli nie zadziała automatyczne przywracanie?

2. Segmentacja i Izolacja (Zatrzymanie intruza)

Atakujący często wchodzą przez sieć biurową (IT) i przeskakuje do sieci przemysłowej (OT).

[ ] Czy istnieje “sztywny” podział IT/OT? – Czy z komputera księgowej lub recepcji można w jakikolwiek sposób “dopingować” (ping/RDP/SSH) urządzenia w sieci sterującej infrastrukturą?

[ ] Jak zabezpieczony jest styk sieci? – Czy pomiędzy strefami jest tylko firewall, czy stosujemy **Data Diode** (jednokierunkowy przepływ danych) lub serwery przesiadkowe (**Jumphost**) z wymuszonym **MFA**?

[ ] Czy Active Directory jest wspólne? – Czy przejęcie Kontrolera Domeny w biurze daje automatycznie klucze do logowania się na stacjach inżynierskich w elektrowni/zakładzie?

3. Detekcja i "Living off the Land"

DynoWiper był odpalany po cichym rekonesansie. Musisz wykryć ich, zanim odpalą ładunek.

[ ] Czy monitorujemy użycie legalnych narzędzi w dziwnych porach? - Czy nasz SOC dostanie alert, jeśli ktoś o 3:00 w nocy użyje PowerShell, PsExec lub WMI do komunikacji z wieloma hostami naraz?

[ ] Czy widzimy ruch wychodzący z sieci OT? - Czy zauważymy, jeśli sterownik PLC lub stacja operatorska zacznie próbować łączyć się z serwerem w Internecie Command & Control (C2)?

[ ] Czy mamy EDR na stacjach inżynierskich? - Czy na komputerach zarządzających infrastrukturą jest oprogramowanie, które zablokuje proces próbujący masowo kasować pliki systemowe (zachowanie wipera)?

4. Łańcuch Dostaw (Supply Chain) – Lekcja z OZE

Atakujący wchodzą "tylnymi drzwiami" przez serwisantów.

[ ] Kto ma stały dostęp zdalny? - Czy serwisanci turbin/paneli mają otwarte tunele VPN 24/7, czy dostęp jest włączany "na żądanie" (Just-in-Time Access)?

[ ] Czy logujemy sesje dostawców? - Czy wiemy, co dokładnie robił zewnętrzny inżynier podczas ostatniego połączenia?

[ ] Jak uwierzytelniają się podwykonawcy? - Czy wymuszamy na nich MFA (uwierzytelnianie wieloskładnikowe), czy współdzielą jedno hasło typu "Serwis2025!"?

5. Procedury na "Godzinę W"

Gdy ekrany gasną, nie ma czasu na czytanie PDF-ów na serwerze, który właśnie zniknął.

[ ] Czy mamy procedury w wersji papierowej? - Jeśli atakujący wyczyści dyski i zaszyfruje SharePointa, czy mamy wydrukowane plany działania i numery telefonów?

[ ] Kto ma uprawnienia do fizycznego odcięcia sieci ("Kill Switch")? - Czy kierownik zmiany wie, który kabel wypiąć, aby odciąć atak, zanim rozprzestrzeni się na resztę infrastruktury i czy ma na to zgodę zarządu "in blanco"?