MANOWIECKI
CYBERSECURITY LAW

# Procedura
# reakcji na incydent poważny dla działu IT

## 0. Od czego zacząć?

- Nie restartuj pochopnie zainfekowanych serwerów (utracisz logi z pamięci RAM).
- Odłączaj urządzenia od sieci, a nie od prądu.
- Czas liczony jest od momentu potwierdzenia, że anomalia to faktyczny incydent.:

## 1. Identyfikacja

Celem jest potwierdzenie incydentu, ocena skali i zabezpieczenie dowodów:

- Zrób zrzut pamięci RAM (jeśli możliwe) i natychmiast zabezpiecz logi systemowe/sieciowe przed nadpisaniem (np. logi z firewalli, Active Directory, EDR/antywirusa).
- Określ, z czym masz do czynienia:
  - Ransomware?
  - Phishing z przejęciem konta?
  - Wyciek danych?
  - Atak DDoS?
- Oceń wpływ:
  - Które systemy niedomagają?
  - Czy incydent dotyczy systemów kluczowych dla ciągłości biznesowej organizacji?

## 2. Powstrzymanie i izolacja

Celem jest powstrzymanie rozprzestrzeniania się zagrożenia na resztę sieci.:

- Natychmiast odłącz zainfekowane maszyny od sieci LAN/Internetu. Nie wyłączaj ich zasilania!
- Na firewallu zablokuj ruch do/z podejrzanych adresów IP lub domen (tzw. wskaźników kompromitacji).
- Wymuś reset haseł dla skompromitowanych kont. Zablokuj konta administracyjne, jeśli zachodzi podejrzenie ich przejęcia.
- Upewnij się, że repozytoria kopii zapasowych są odizolowane i zabezpieczone przed zaszyfrowaniem (np. odłącz nośniki offline, zablokuj dostęp z sieci).

## 3. Komunikacja

| Czas reakcji | Działanie IT | Odbiorca |
|---|---|---|

Adresat procedury: **Dział IT**

| | | |
|---|---|---|
| Do 24 godzin | Zgłoszenie wczesnego ostrzeżenia. Przekazanie wstępnych danych technicznych. | Właściwy CSIRT sektorowy (przez system S46) |
| Do 72 godzin | Zgłoszenie oficjalne incydentu. Raport o skutkach, skali (ile stacji/kont), wektorze ataku i podjętych działaniach. | Właściwy CSIRT sektorowy (przez system S46), PUODO (jeśli wyciekły dane osobowe) |
| W trakcie | Raportowanie postępów, informowanie użytkowników o zagrożeniu (np. przymusowy reset haseł). | Zarząd, Użytkownicy |

## 4. Usunięcie i odtwarzanie

Przywrócenie normalnego funkcjonowania systemu i usunięcie luki, która pozwoliła na atak.

- Znajdź wektor ataku (np. niezałatany VPN, złośliwy załącznik z e-maila) i załataj lukę.
- Przeprowadź głębokie skanowanie i weryfikację integralności pozostałych systemów.
- Przywracaj systemy wyłącznie ze zweryfikowanych, bezpiecznych kopii zapasowych.
- Uruchom przywrócone systemy, ale przez co najmniej 48 godzin zachowaj podwyższony rygor monitorowania sieci pod kątem ponownej infekcji.
- Upewnij się, że pierwotna podatność została skutecznie zablokowana (np. luki załatane, hasła zmienione, stacje robocze oczyszczone ze złośliwego kodu), a systemy powróciły do stabilnego działania.
- Przygotujcie dokument zawierający wnioski z analizy. Wypiszcie szczegółowo wskaźniki kompromitacji (np. złośliwe adresy IP, hashe plików), wdrożone środki zaradcze oraz ewentualne straty.

## 5. Sprawozdanie końcowe

Sprawozdanie końcowe z obsługi incydentu poważnego musi zostać przekazane nie później niż w ciągu miesiąca od dnia zgłoszenia tego incydentu. Sprawozdanie końcowe musi stanowić merytoryczne i wyczerpujące podsumowanie zdarzenia. Zgodnie z ustawą, dokumentacja przesyłana po incydencie powinna w szczególności zawierać:

- Opis wpływu incydentu na usługi świadczone przez dany podmiot.
- Szczegółowy opis przyczyn wystąpienia incydentu (np. zidentyfikowana luka w oprogramowaniu, atak socjotechniczny, błąd konfiguracji).

- Informacje o działaniach podjętych w celu opanowania sytuacji i ograniczenia skutków.

Sprawozdanie końcowe z obsługi incydentu powinno zostać wprowadzone do systemu S46 i oficjalnie wysłane do CSIRT sektorowego przed upływem miesiąca od daty pierwszego zgłoszenia incydentu poważnego tj. zgłoszenia dokonanego niepóźniej niż w ciągu 72 godzin od momentu jego wykrycia.

## 6. Aktualizacja polityk

Ostatnim etapem jest wdrożenie wniosków z zaistniałego incydentu do codziennych operacji. W tym celu:

- Zaktualizuj polityki bezpieczeństwa.
- Zaktualizuj procedury reagowania.
- Zaktualizuj reguły na firewallu.
- Zaplanuj dodatkowe szkolenia dla pracowników, aby zminimalizować ryzyko powtórzenia się podobnego scenariusza.

## 7. Ważne kontakty

| Rola w incydencie: | Imię i Nazwisko: | Kontakt: |
|---|---|---|
| Wyznaczony członek zarządu | … | adres e-mail: …<br>nr tel.: … |
| Bezpośredni przełożony | … | adres e-mail: …<br>nr tel.: … |
| Pełnomocnik ds. SZBI | … | adres e-mail: …<br>nr tel.: … |
| IOD (jeśli wyznaczono) | … | adres e-mail: …<br>nr tel.: … |
| Zewnętrzny dostawca wsparcia IT (jeśli występuje) | … | adres e-mail: …<br>nr tel.: … |