10. kroków zabezpieczenia danych na potrzeby analizy powłamaniowej v2.0

Zbieranie i zabezpieczanie danych to pierwszy techniczny krok w kierunku obsługi incydentu. Odpowiednie wykonanie poniższych czynności w zaproponowanej kolejności umożliwi sprawną analizę, powstrzymanie oraz likwidację skutków incydentu, a także przywrócenie organizacji do dalszego działania.

01.

Określ zakres incydentu

Oszacuj których elementów infrastruktury (urządzeń i systemów) dotyczy incydent.

02.

Odseparuj/odłącz zainfekowaną infrastrukturę od sieci Internet

Łącza dostępowe do sieci Internet należy odłączyć w sposób fizyczny od routera brzegowego bądź poprzez wyłączenie odpowiednich interfejsów urządzenia. Odseparuj część zdrową sieci od zakażonej. Nie wyłączaj samych urządzeń sieciowych!

03.

Nie restartuj i nie wyłączaj!

Pozostaw aplikacje, systemy i urządzenia włączone w celu zebrania danych ulotnych.

W razie wątpliwości skontaktuj się ze specjalistą od analizy powłamaniowej.

04.

Dane ulotne

Zbierz szczegółowe informacje o systemie operacyjnym, konfiguracji sieci i połączeniach, działających procesach, zawartości cache DNS i ARP, usługach, zaplanowanych zadaniach, użytkownikach i sesjach.

05.

Pamięć RAM

Zabezpiecz pamięć RAM działającej maszyny.

W przypadku maszyn wirtualnych rozważ wykonanie migawki (snapshot).

06.

010011
110100

Kopia binarna

Selektywnie zabezpiecz dane lub wykonaj kopię partycji systemowej działającego komputera lub wyłącz urządzenie i wykonaj pełną kopię binarną nośnika.

W przypadku macierzy RAID rozważ wykonanie kopii działającego systemu operacyjnego.

07.

Logi

Zabezpiecz logi z dostępnych urządzeń sieciowych.

08.

Nie przeprowadzaj analizy na zainfekowanym urządzeniu!

Nie zacieraj śladów poprzez instalowanie nowego oprogramowania, nadpisywanie danych, skanowanie programem antywirusowym.

09.

Raport

Sporządź raport z informacjami o incydencie i wykonanych czynnościach.

10.

Analiza powłamaniowa

Przekaż do odpowiedniego specjalisty w celu przeprowadzenia analizy śledczej.

Pogotowie 24h/7 **500 16 26 36**

Wersja 2 dokumentu