Hakerskie włamanie?

Sposób postępowania w przypadku **ataku hakerskiego** jest szalenie istotny nie tylko z uwagi na **materiał dowodowy**, ale również aby odpowiedzieć na bardzo istotne pytania z punktu widzenia **cyberbezpieczeństwa**: jak doszło do włamania? jakie były kolejne kroki atakującego? do czego cyberprzestępca uzyskał dostęp?

KROK 01

Włamanie, i co teraz?

Pierwszą podstawową czynnością powinien być kontakt z **ekspertem informatyki śledczej**, potrafiącym prawidłowo **zabezpieczyć materiał dowodowy** czyli **ślady włamania**

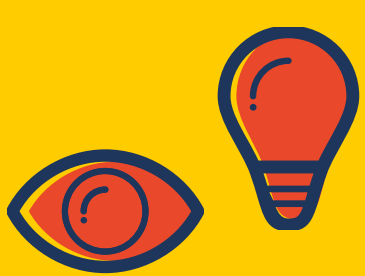
UWAGA!

Prawidłowa reakcja i należyte zabezpieczenie danych jest **najważniejszą czynnością**, niejednokrotnie przesądzającą o możliwościach analizy. Brak zabezpieczenia danych i dokonywanie operacji w systemie, jego wyłączanie, restarty, upływający czas działającego systemu – wszystko to ma **wpływ** na zachowanie **śladów aktywności** i powodzenie **analizy powłamaniowej**

KROK 02

Zabezpieczenie

Ekspert **informatyki śledczej** podejmuje z klientem decyzję o sposobie zabezpieczenia **materiału dowodowego** – nie każde zabezpieczenie przebiega tak samo



Same logi **nie są** wystarczającym materiałem do analizy **śladów włamania**

KROK 03

Analiza danych

Doświadczony **informatyk śledczy** przy pomocy profesjonalnego oprogramowania analizuje zabezpieczone dane

Wykorzystanie zaawansowanych komercyjnych narzędzi dedykowanych **informatyce śledczej** wpływa nie tylko na szybkość analizy ale również na jej wnikliwość

KROK 04

Wstępne wyniki analizy

Ekspert kontaktuje się z klientem celem wskazania ewentualnych kolejnych zasobów, które trzeba **zabezpieczyć** z uwagi na możliwość eskalacji analizowanego ataku

KROK 05

Raport z analizy

Ostatnim elementem analizy jest dostarczenie klientowi raportu z wykonanych czynności i przebiegu **analizy powłamaniowej**

Prawidłowo wykonana analiza oraz raport zawierający szczegółowe informacje może przesądzić o ewentualnym dopuszczeniu go jako **dowodu** w przypadku procesu sądowego (decyduje sędzia)

WWW.REDTEAM.PL INFO@REDTEAM.PL
EKSPERCKIE USŁUGI CYBERBEZPIECZEŃSTWA