LABYRINTH

CASE STUDY

O Kliencie

Klientem jest spółka holdingowa, która zrzesza ponad 10 firm o różnych profilach - produkcyjnych, handlowych, budowlanych, ubezpieczeniowych, usługowych i innych.

Infrastruktura obejmuje do 100 podsieci VLAN.

Wyzwanie

W wyniku testowania i modelowania zagrożeń, zastosowanego w różnych segmentach infrastruktury sieciowej Klienta, zidentyfikowano słabe punkty w wykrywaniu zdarzeń w obrębie sieci firmowej.

Zdarzenia zostały sklasyfikowane jako związane z etapami eksploracji sieci przez atakujących oraz jako próby wykorzystania uzyskanych usług sieciowych w segmentach sieci lokalnej.

Ustalono również, że wymagana jest dodatkowa warstwa ochrony na poziomie stacji roboczych w postaci wabików plikowych dla intruzów, którzy już wcześniej uzyskali dostęp do stacji, na przykład poprzez atak phishing'owy.

Aby poprawić jakość badania incydentów, należało m.in. zmniejszyć czas reakcji SOC, przy jednoczesnym odwróceniu uwagi atakujących od rzeczywistych zasobów IT.

Realizacja

Platforma decepcji Labyrint została wdrożona w konfiguracji z wieloma maszynami wirtualnymi Worker, ponieważ istniała potrzeba pokrycia kilku rozproszonych segmentów sieci: biur i centrów danych.

Podczas procesu wdrażania wykorzystano wszystkie dostępne typy wabików sieciowych (Points) i przeprowadzono dwukierunkową integrację z systemem klasy SIEM.

Dla większości wewnętrznych usług sieciowych, zostały stworzone pułapki oparte na wabiku typu UniversalWebPoint.

Rozwiązanie

Wdrożenie systemu Labyrinth i pokrycie ochroną decepcji infrastruktury Klienta zostało zapewnione w kilku kierunkach:

1. Zidentyfikowano krytyczne dla procesów biznesowych wewnętrzne aplikacje internetowe i utworzono kilka wabików sieciowych dla każdej z nich, w oparciu o UniversalWebPoint, w celu zwiększenia prawdopodobieństwa wykrycia atakującego, który koncentruje się na znalezieniu i wykorzystaniu wewnętrznych zasobów sieciowych.

2. Wszystkie dostępne typy wabików sieciowych (Punktów) zostały wdrożone w celu stworzenia jak największej powierzchni ataku. Większość segmentów sieci klienta została pokryta sieciami wabików.

3. Skonfigurowano dwustronną integrację systemów SIEM i Labyrinth. W oparciu o tę integrację wdrożono i sformalizowano dodatkowe procedury, które będą wykorzystywane w procesie dochodzeniowym i reagowaniu na incydenty. Proces obsługi incydentów Labyrinth został zintegrowany ze wspólnym procesem zarządzania incydentami bezpieczeństwa w organizacji.

4. Na rzeczywistych hostach zaimitowano wiele różnych typów wabików plikowych w celu wykrycia atakującego na etapie po wykorzystaniu podatności (jeśli intruz uzyskałby dostęp do rzeczywistego hosta za pomocą phishing'u, dostępu fizycznego, itp.).

Rezultaty

Dzięki funkcjonalności systemu Labyrinth, możliwe było zwiększenie widoczności sieci, tak, by zidentyfikować wszelkie możliwe próby uzyskania nieautoryzowanego dostępu oraz rozeznania struktury i zawartości hostów w segmentach sieci. Dzięki wykorzystaniu funkcjonalności Web-deception, sekwencje działań atakujących na wewnętrznych aplikacjach sieciowych były wykrywane i dokładnie klasyfikowane.

W oparciu o dane zebrane przez system Labyrinth, wartość informacyjna wykrytych incydentów została znacznie zwiększona, co doprowadziło do szybszego podejmowania decyzji dla każdej z badanych spraw.

O firmie Labyrinth

Labyrinth to zespół doświadczonych inżynierów cyberbezpieczeństwa i testerów penetracyjnych, który specjalizuje się w opracowywaniu rozwiązań do wczesnego wykrywania cyberzagrożeń i zapobiegania im.

NASZĄ WIZJĄ jest przesunięcie układu sił na korzyść obrońców. NASZĄ MISJĄ jest dostarczenie wszelkiego rodzaju organizacjom prostego i wydajnego narzędzia do jak najwcześniejszego wykrywania napastników wewnątrz sieci korporacyjnej.