Symulacje ataku

IstroSec oferuje możliwość przetestowania skuteczności i wydajności środków bezpieczeństwa poprzez symulowane ataki. W ten sposób można zweryfikować, czy pracownicy są wystarczająco świadomi i potrafią wytrzymać cyberzagrożenia oraz czy środki zapobiegawcze, śledcze i reaktywne działają zgodnie z przeznaczeniem. Oferujemy symulacje ataków za pomocą socjotechniki oraz symulacje atakującego obecnego w infrastrukturze firmy.

> *Podczas symulacji ataku możesz sprawdzić, czy zarówno zespół reagowania na incydenty, jak i kierownictwo mogą szybko i skutecznie reagować na incydenty.*

Symulacje socjotechniczne:

- Phishing
- Vishing
- Spearphishing
- Smishing
- Whaling
- Socjotechnika osobista

Symulacje ataków socjotechnicznych

Kompleksową odporność na ataki socjotechniką można osiągnąć dzięki zaawansowanemu programowi szkoleniowemu pracowników, odpowiednim środkom technicznym oraz regularnym testom ich skuteczności. **Istro**Sec jest gotowy, aby pomóc Ci zwiększyć Twoją gotowość i odporność na tego typu ataki.

Symulacje phishingowe

Nasi eksperci przygotują i wdrożą kampanię phishingową, która nie będzie wymierzona w konkretnych pracowników, wykorzystywane technologie czy usługi. W ramach tej kampanii zostanie opracowana lista adresów e-mail pracowników na podstawie publicznie dostępnych danych. Następnie na te adresy zostanie wysłana wiadomość e-mail mająca na celu wyłudzenie informacji dotyczących danych logowania, danych osobowych lub innych poufnych informacji, lub skłonienie do pobrania załącznika.

Symulacje spearphishingowe

Spearphishing to bardziej zaawansowany i skuteczniejszy rodzaj phishingu. W tej symulacji nasi eksperci wykorzystują technikę białego wywiadu (open-source intelligence, OSINT) do pozyskania danych potrzebnych do przygotowania ukierunkowanej i wysoce skutecznej kampanii, która uwzględni specyfikę technologii, pracowników lub wykorzystywanych usług. Wykorzystywane są bardzo podobne domeny, omijające uwierzytelnianie wieloskładnikowe lub wdrażające określone złośliwe oprogramowanie napisane przez naszych analityków malware'ów.

Whaling

W ramach symulacji ataku whaling nasi eksperci przeprowadzą kampanię phishingową ukierunkowaną na kierownictwo najwyższego szczebla. To właśnie atak na tę grupę może wyrządzić znaczące szkody dla firmy, osoby te mają bowiem dostęp do istotnych informacji, a styl ich pracy jest często bardzo dynamiczny.

Vishing

Ataki głosowego phishingu mogą być bardzo skutecznym sposobem na wyłudzanie poufnych informacji od pracowników. Nasi eksperci przeprowadzą atak telefoniczny przy użyciu informacji z OSINT i zastosują manipulacje psychologiczne, podszywanie się i nieuczciwe sztuczki.

Smishing

Wyślemy phishingowe wiadomości SMS do pracowników firmy, aby uzyskać dane do logowania, dane osobowe lub inne poufne informacje lub skłonić ich do pobrania załącznika do wiadomości e-mail.

Socjotechnika osobista

Nasi eksperci odwiedzą miejsce pracy i poprzez komunikację z pracownikami poszukają informacji, które mogą zostać wykorzystane do przeprowadzenia innych ataków, zainstalowania złośliwego oprogramowania, pozyskania haseł, danych wrażliwych lub zmuszenia pracowników do wykonywania czynności naruszających politykę bezpieczeństwa firmy.

Symulacje atakującego już obecnego w infrastrukturze

Symulacje konkretnych działań atakującego

Symulacje konkretnych działań atakującego w organizacji mogą składać się z działań, takich jak ruchy boczne, rozprzestrzenianie złośliwego kodu, zbieranie i filtrowanie danych, omijanie zabezpieczeń w organizacji itp.

Symulacja złożonego ataku na organizację

Podczas tego typu symulacji testujemy możliwości wykrywania i reagowania zespołu ds. bezpieczeństwa pod kątem taktyk, technik i procedur (TTP) zaawansowanych trwałych zagrożeń (APT). Jeśli konkretna grupa APT koncentruje się obecnie na twoim sektorze biznesowym, możemy pomóc ci zwiększyć twoją zdolność do wytrzymania określonych TTP. Na przykład w przypadku grupy APT41 może to być spearphishing ze złośliwym załącznikiem, WMI, zaplanowanymi zadaniami, PowerShell, DLL Side-Loading, SMB / Windows Admin Shares, keyloggerem lub szyfrowaniem danych jako strategią wyjścia.

Dlaczego IstroSec?

Oprócz wysokich umiejętności samodzielnego wykonywania symulacji, eksperci **Istro**Sec dokładnie badają taktykę, techniki i procedury stosowane przez prawdziwych atakujących. Dzięki takiemu połączeniu klient może bezpiecznie przetestować swoją odporność i gotowość na realne ataki.

Studium przypadku

Rodzaj firmy: instytucja finansowa
Świadczona usługa: symulacja spearphishingu
Rozwiązanie: Test spearphishingu i tworzenie złośliwego oprogramowania
Organizacja była zainteresowana weryfikacją konfiguracji już istniejących zabezpieczeń rozwiązań pocztowych, a także zachowań wszystkich pracowników, gdy otrzymują niechciane wiadomości e-mail w firmowej skrzynce e-mail. Taki przypadek można było przetestować za pomocą usług **Istro**Sec, takich jak symulacja phishingu lub - jak w tym przypadku - ukierunkowana i skuteczniejsza kampania spearphishingowa.
W początkowej fazie (rozpoznawczej) obejmowało to uzyskanie informacji o firmie i pracownikach. Dzięki temu uzyskaliśmy m.in. adresy e-mail pracowników, informacje o infrastrukturze pocztowej i stosowanych zabezpieczeniach. Następnie przygotowano kampanię, która może zawierać np. link do strony symulującej stronę pierwotną w celu uzyskania danych dostępowych oraz drugi czynnik uwierzytelniający. Alternatywnie możemy stworzyć złośliwe oprogramowanie na potrzeby zaawansowanej kampanii, która może symulować oprogramowanie ransomware lub inne formy zachowania prawdziwego atakującego. Podczas tworzenia treści użytkowej proponowana jest ostateczna wiadomość e-mail, która zostanie następnie wysłana do wybranej grupy pracowników w określonym czasie. Po wysłaniu kampanii wyniki są analizowane, a po jej zakończeniu końcowy raport przekazywany jest klientowi. Raport zawiera podsumowanie wykonawcze, zidentyfikowane słabości, szczegółowe statystyki, takie jak liczba wysłanych wiadomości e-mail, kliknięcia linków, wysłane dane, lista urządzeń, z których uzyskano dostęp do strony phishingowej itp.