G DATA academy

Case Study

Symulacje phishingu od G DATA pokazują klientom, gdzie znajduje się problem bezpieczeństwa IT.

Wyzwania:

- Szkolenie jako uzupełnienie portfolio w celu uświadomienia pracownikom zagrożeń cybernetycznych
- Możliwość pokazania firmom potrzeby działania w obszarze świadomości

Korzyści:

- Szkolenie podnoszące świadomość pomaga pracownikom poszerzyć wiedzę na temat bezpieczeństwa
- Symulacja phishingu pomaga sprawdzić świadomość zagrożeń cybernetycznych
- Raport kierownictwa z symulacji phishingu pokazuje potrzebę działania wśród pracowników

Rozwiązanie:

- G DATA Security Awareness Trainings
- G DATA Symulacja phishingu

smartSEC

Branża:
Zarządzanie kryzysowe i zapobieganie cyberatakom

Lokalizacja:
Wernau, Niemcy

Coraz więcej firm korzysta ze szkoleń podnoszących świadomość, aby zwiększyć wiedzę pracowników na temat zagrożeń cybernetycznych. Aby przygotować się na cyberataki, smartSEC opiera się na szkoleniach uświadamiających G DATA CyberDefense. Ponadto start-up wykorzystuje symulacje phishingu, aby pokazać klientom, w jaki sposób dbać o bezpieczeństwo IT w firmie.

smartSEC wie co nieco o cyberatakach: Założony w 2020 r. start-up specjalizuje się w zarządzaniu kryzysowym w przypadku cyberataków. Koncentruje się na kwestiach związanych z zarządzaniem w dotkniętej firmie i koordynacją na miejscu. Eksperci działają również jako „tłumacze" między nietechnicznym kierownictwem a technicznymi ekspertami kryminalistycznymi. Praca ta doprowadziła do drugiego celu dla młodej firmy.

Przygotowanie firm na sytuacje kryzysowe IT. Wspólnie ze swoimi klientami z sektora MŚP, specjaliści opracowują indywidualną instrukcję postępowania w sytuacjach awaryjnych IT i przeprowadzają realistyczne symulacje kryzysowe.

„Prędzej czy później każda firma pada ofiarą cyberataku" - mówi Oliver Filipzik, odpowiedzialny za marketing w smartSEC. „Pomagamy małym i średnim przedsiębiorstwom przygotować się na najgorszy scenariusz, aby w razie zagrożenia szkody były jak najmniejsze. Dlatego też włączyliśmy do naszego portfolio szkolenia uświadamiające G DATA, ponieważ ludzie odgrywają kluczową rolę w obronie przed cyberatakami".

Ludzie i ich zachowanie nadal stanowią główny wektor ataków cybernetycznych. Potrzebne są szkolenia w celu podniesienia świadomości pracowników na temat nowych zagrożeń, aby mogli dostosować swoje zachowanie. Same podręczniki dotyczące zagrożeń informatycznych nie wystarczą. Potrzebne są praktyczne ćwiczenia, aby pracownicy mogli doskonalić swoje umiejętności.

Od samego początku mieliśmy dobre przeczucia co do tego wyboru. Kolejnym plusem jest to, że G DATA jest niemieckim dostawcą. Przekonała nas również symulacja phishingu. Używamy jej do sprawdzania status quo naszych klientów - w połączeniu ze sprawdzeniem słabych puntów pokazujemy, jak podatne są firmy.

Oliver Filipzik
Odpowiedzialny za marketing w smartSEC

SPRAW, ABY ŚWIADOMOŚĆ BEZPIECZEŃSTWA BYŁA MIERZALNA DZIĘKI SYMULACJOM PHISHINGU.

Klienci również dostrzegli tę potrzebę i pytają smartSEC, w jaki sposób mogą zwiększyć świadomość zagrożeń cybernetycznych wśród pracowników.

Zwiększanie świadomości dzięki szkoleniom online
Osoby odpowiedzialne szybko podjęły decyzję o włączeniu szkoleń z zakresu świadomości bezpieczeństwa jako rozwiązania zewnętrznego. Po dogłębnej analizie rynku aktualnych ofert, podjęto decyzję na korzyść G DATA. Przejrzysty interfejs użytkownika, dobra struktura planu nauczania i struktura treści przemawiały na korzyść platformy edukacyjnej.

Zwłaszcza mniejsze firmy są często przekonane, że nie są atrakcyjnym celem dla cyberprzestępców. Tak jednak nie jest: Podczas gdy skanowanie luk w zabezpieczeniach pokazuje, między innymi, otwarte porty, a tym samym potencjalny wektor ataku, symulacja phishingu pokazuje, jak łatwo niektórzy pracownicy dają się nabrać na fałszywe wiadomości e-mail. Ponadto wiele ataków phishingowych jest bardzo dobrze wykonanych i cały czas stają się coraz lepsze. Atakujący dużo inwestują, aby odnieść sukces. Końcowy raport zarządu pokazuje, jak wielka jest potrzeba działania. Opinie klientów są niezmiennie pozytywne.

Cyberatak jest na wyciągnięcie ręki
„Symulacja phishingu dostarcza dobrych argumentów osobom odpowiedzialnym za określenie aktualnego stanu firmy" - mówi Oliver Filipzik. „Jeśli choćby jeden pracownik kliknie w link lub otworzy załącznik, to w rzeczywistości jest już za późno ransomware jest w sieci. Ponadto korzystamy z partnerstwa z G DATA CyberDefense. Ponieważ nazwa ta ma znaczenie dla wielu klientów jako godny zaufania partner".

Podczas symulacji phishingu klienci otrzymują różne wiadomości phishingowe przez okres czterech tygodni. Doświadczenie pokazuje, że chociaż wskaźniki otwarcia różnią się w zależności od poszczególnychscenariuszy, prawie zawsze jest kilku pracowników, którzy zostaliby złapani przez atakujących. Podczas pandemii szczególnie dobrze sprawdzały się wiadomości związane z biurem domowym. Jednak osobiste tematy, takie jak zmiany na firmowym parkingu lub zmiany w jedzeniu w firmowej stołówce, również kuszą wielu pracowników do otwarcia wiadomości, nawet do kliknięcia fałszywego linku lub nawet ujawnienia poufnych danych.

„Współpraca z G DATA jest bardzo przyjemna", mówi Oliver Filipzik. „Specjalne prośby klientów były szybko rozwiązywane przez zespół wsparcia. Bezpośrednia komunikacja między naszymi klientami a G DATA również zawsze przebiegała sprawnie. Czujemy, że jesteśmy w dobrych rękach."

Jesteś ciekawy, jak Ty możesz zabezpieczyć swoją firmę za pomocą G DATA?
Więcej informacji możesz znaleźć tutaj:

gdata.pl/business sales@gdata.pl +48 94 37 29 669

G DATA academy