STUDIUM PRZYPADKU

Wdrażanie rozwiązań bezpieczeństwa Sophos po ataku phishingowym wykorzystującym klienta

synchroworks.pl
biuro@synchroworks.net
+48 32 889 83 44

PRZEGLĄD/PROBLEM

Jeden z klientów profesjonalnych usług Synchroworks padł ofiarą wyrafinowanego ataku phishingowego wykorzystującego socjotechnikę. Klient otrzymał autentycznie wyglądającą wiadomość e-mail od firmy Microsoft z prośbą o zresetowanie hasła. Ufając wiarygodności wiadomości e-mail, klient postępował zgodnie z instrukcjami resetowania, co ostatecznie doprowadziło do przejęcia konta.

Ponieważ sztuczna inteligencja (AI) nadal szybko się rozwija, techniki phishingu oparte na AI stały się bardziej wyrafinowane i trudne do wykrycia, wykorzystując realistyczny język, personalizację i ukierunkowanie na określone osoby/organizacje. Ataki te mogą podszywać się pod zaufanych nadawców i omijać tradycyjne rozwiązania bezpieczeństwa, co czyni je jeszcze bardziej niebezpiecznymi i trudnymi do zwalczenia. Incydent ten ujawnił pilną potrzebę kompleksowych środków cyberbezpieczeństwa w celu ochrony poufnych danych i zapobiegania przyszłym atakom.

MOŻLIWOŚCI I ROZWIĄZANIA

Synchroworks przeprowadził kompleksową ocenę istniejących praktyk bezpieczeństwa i infrastruktury klienta oraz zidentyfikował ich kluczowe słabe punkty. Nasz zespół przedstawił sugestie dotyczące cyberbezpieczeństwa w chmurze, które najlepiej pasowałyby do istniejącej infrastruktury. W oparciu o budżet i preferencje klienta, ostatecznie wdrożyliśmy 2 główne rozwiązania, aby zapobiec przyszłym atakom phishingowym:

1. Wdrożenie Sophos Email Security oraz Intercept X Endpoint

Jako złoty partner Sophos, Synchroworks był w stanie wdrożyć dwa rozwiązania zabezpieczeń Sophos, które współpracują ze sobą, aby skutecznie wykrywać, zapobiegać i chronić urządzenia przed złośliwym oprogramowaniem, ransomware i innymi ewoluującymi zagrożeniami, zmniejszając ryzyko przyszłych naruszeń.

Sophos Email zawiera funkcje takie jak filtrowanie treści, szyfrowanie wiadomości e-mail i analiza zagrożeń, aby zapewnić bezpieczną komunikację.

Sophos Intercept X to rozwiązanie do ochrony punktów końcowych, które łączy różne technologie bezpieczeństwa w celu ochrony przed szeroką gamą cyberzagrożeń, w tym ransomware i lukami typu zero-day. Rozwiązanie to wykorzystuje zaawansowane techniki, takie jak głębokie uczenie się i analiza zachowań, aby proaktywnie identyfikować i blokować zagrożenia, zanim będą mogły wyrządzić szkody w punktach końcowych i sieciach

2. Szkolenie pracowników w zakresie cyberbezpieczeństwa

Firma Synchroworks przeprowadziła dla wszystkich pracowników kompleksową sesję szkoleniową z zakresu cyberbezpieczeństwa, która obejmowała szereg tematów, aby zapewnić wszechstronną wiedzę i gotowość

W SKRÓCIE

PROBLEMY

- Wyrafinowany atak phishingowy
- Brak pracowników
- Szkolenia w zakresie cyberbezpieczeństwa
- Brak zabezpieczeń poczty elektronicznej

ROZWIĄZANIA

- Sophos Email Protection
- Sophos Intercept X Endpoint

KORZYŚCI

- Ulepszone wykrywanie zagrożeń i ich zapobieganie
- Uproszczone zarządzanie bezpieczeństwem
- Świadomość pracowników

KLIENT ZYSKUJE NIEZBĘDNE NARZĘDZIA I SZKOLENIA WYMAGANE DO IDENTYFIKACJI I ZAPOBIEGANIA TYPOWYM ZAGROŻENIOM CYBERBEZPIECZEŃSTWA , OSTATECZNIE CHRONIĄC SWOJĄ FIRMĘ PRZED WYRAFINOWANYMI ATAKAMI.

KLUCZOWE KORZYŚCI

Ulepszone wykrywanie i zapobieganie zagrożeniom

Sophos Intercept X Endpoint i Email Protection zapewnia zaawansowane funkcje wykrywania zagrożeń w celu identyfikacji i blokowania zaawansowanego złośliwego oprogramowania, ransomware i ataków phishingowych. Klient może teraz znacznie zmniejszyć ryzyko padnięcia ofiarą cyberataków, chroniąc swoje wrażliwe dane i krytyczne systemy.

Uproszczone zarządzanie bezpieczeństwem

Rozwiązania wdrożone przez Synchroworks oferują scentralizowaną konsolę zarządzania, umożliwiającą klientowi zarządzanie i monitorowanie bezpieczeństwa punktów końcowych w całej sieci z poziomu jednego interfejsu. Takie scentralizowane podejście umożliwia wydajne wdrażanie zasad bezpieczeństwa, aktualizacji i poprawek, upraszczając administrację i zapewniając wgląd w czasie rzeczywistym w stan bezpieczeństwa wszystkich punktów końcowych.

Świadomość pracowników

Kompleksowe szkolenie Synchroworks wyposażyło pracowników w umiejętności identyfikowania powszechnych technik phishingu, takich jak zwodnicze wiadomości e-mail, złośliwe załączniki i podejrzane linki do stron internetowych. Uczą się oni analizować nadawców wiadomości e-mail, oceniać ich treść i szukać czerwonych flag, które wskazują na potencjalną próbę phishingu. Dzięki odpowiedniemu szkoleniu pracownicy stają się bardziej czujni i mogą szybko identyfikować i zgłaszać ataki phishingowe, zapobiegając nieautoryzowanemu dostępowi do systemów firmowych i poufnych danych.

SYNCHROWORKS CONSULTING

Sophos Gold Partner