Wyróżnione ryzyko: zagrożenia występujące po dostarczeniu wiadomości e-mail

Działania podejmowane po tym, jak złośliwy e-mail ominie zabezpieczenia organizacji i znajdzie się w skrzynce odbiorczej użytkownika, mogą być równie ważne, jak to, co dzieje się w momencie zablokowania zagrożeń na wcześniejszym etapie.

Analitycy z firmy Barracudy, aby lepiej zrozumieć wzorce zagrożeń i praktyki reagowania na nie, przeanalizowali działania i wzorce zachowań ponad 3500 organizacji. Okazało się, że przeciętna organizacja licząca 1100 użytkowników doświadcza miesięcznie około 15 incydentów związanych z bezpieczeństwem poczty elektronicznej, a każdy atak phishingowy, który zdoła się przedostać, dotyka średnio 10 pracowników.

Stwierdzono również, że 3% pracowników kliknie na link w złośliwym e-mailu, narażając całą organizację na atak. Mimo, że liczby bezwzględne mogą wydawać się niewielkie, jednak potencjalna skala zagrożenia jest znacząca, ponieważ hakerom wystarczy jedno kliknięcie lub odpowiedź, aby atak zakończył się sukcesem.

Zidentyfikowano także działania, które mogą przynieść wymierne korzyści po dostarczeniu wiadomości. Analiza wykazała, że organizacje, które przeszkolą swoich użytkowników, już po dwóch kampaniach szkoleniowych odnotują 73-procentowy wzrost w dokładności zgłoszeń podejrzanych wiadomości e-mail od użytkowników.

Oto bliższe spojrzenie na wzorce zagrożeń i praktyki reagowania, które odkryli analitycy firmy Barracuda, a także kroki, które można podjąć, aby usprawnić reakcję organizacji na zagrożenia związane z wiadomościami e-mail po ich dostarczeniu.

Wyróżnione ryzyko

Zagrożenia występujące po dostarczeniu wiadomości e-mail — Działania prowadzone w celu zarządzania następstwami naruszenia bezpieczeństwa i zagrożeniami występującymi po dostarczeniu wiadomości e-mail są powszechnie określane mianem reagowania na incydenty. Skuteczna reakcja na incydenty ma na celu szybkie usunięcie zagrożenia, aby zatrzymać rozprzestrzenianie się ataku i zminimalizować potencjalne szkody.

Rozwijające się ataki z wykorzystaniem poczty elektronicznej stanowią poważne zagrożenie dla organizacji. Ponieważ hakerzy wykorzystują coraz bardziej wyrafinowane techniki socjotechniczne, zagrożenia związane z pocztą elektroniczną stają się trudne do wykrycia zarówno przez mechanizmy kontroli technicznej, jak i dla użytkowników poczty elektronicznej. Nie istnieje żadne rozwiązanie zabezpieczające, które mogłoby zapobiec 100% ataków. Użytkownicy też nie zawsze zgłaszają podejrzane wiadomości e-mail, ponieważ nie przeszli odpowiedniego szkolenia lub po prostu zapominają o konkretnych procedurach

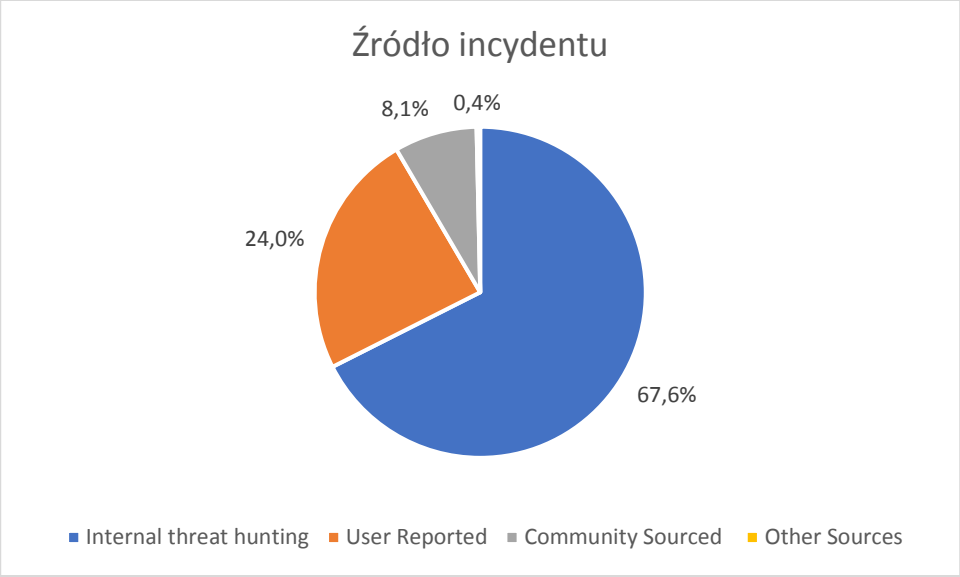
bezpieczeństwa. Natomiast jeśli pracownicy zaraportują incydent, to często dokładność zgłaszanych wiadomości jest niska, co prowadzi do marnowania zasobów IT. Bez skutecznej strategii reagowania na incydenty, zagrożenia mogą często pozostać niewykryte, dopóki nie jest za późno.

Szczegóły

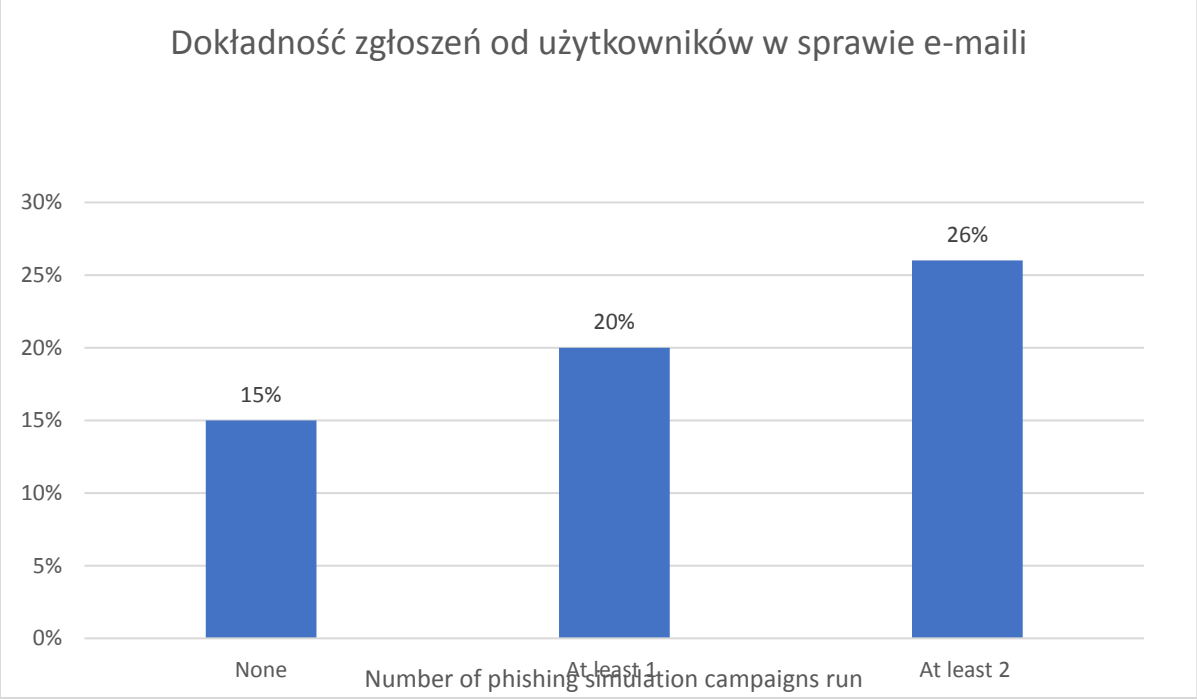
Zgodnie z raportem przygotowanym przez ekspertów firmy Barracuda wśród ponad 3500 podmiotów, przeciętna organizacja licząca 1100 użytkowników doświadcza około 15 incydentów związanych z bezpieczeństwem poczty elektronicznej miesięcznie. „Incydent" w tym przypadku odnosi się do złośliwych wiadomości e-mail, które przedostały się przez techniczne rozwiązania zabezpieczające do skrzynek odbiorczych użytkowników. Po zidentyfikowaniu, incydenty te wymagają ustalenia priorytetów, zbadania ich zakresu i poziomu zagrożenia, a jeśli zostaną uznane za zagrożenie, wymagają również podjęcia działań zaradczych.

Jest wiele sposobów, w jaki organizacje mogą identyfikować zagrożenia dla poczty elektronicznej występujące po dostarczeniu wiadomości: zgłoszenia od użytkowników, wewnętrzne programy wykrywania zagrożeń uruchamiane przez działy IT lub informacje od społeczności w innych organizacjach, które zajmują się usuwaniem skutków ataków. Dane o usuniętych zagrożeniach, współdzielone przez organizacje, są zazwyczaj bardziej wiarygodne niż dane zgłoszone przez użytkowników.

Analitycy firmy Barracuda ustalili, że większość incydentów (67,6%) została odkryta w wyniku wewnętrznych dochodzeń dotyczących zagrożeń, wszczętych przez zespół IT. Dochodzenia te mogą być inicjowane na różne sposoby. Powszechne praktyki obejmują przeszukiwanie logów wiadomości lub wyszukiwanie słów kluczowych lub nadawców w już dostarczonej poczcie. Kolejne 24% incydentów zostało stworzonych na podstawie wiadomości e-mail zgłoszonych przez użytkowników, 8,1% odkryto przy użyciu wywiadu środowiskowego, a pozostałe 0,4% poprzez inne źródła, takie jak zautomatyzowane lub wcześniej rozwiązane incydenty.



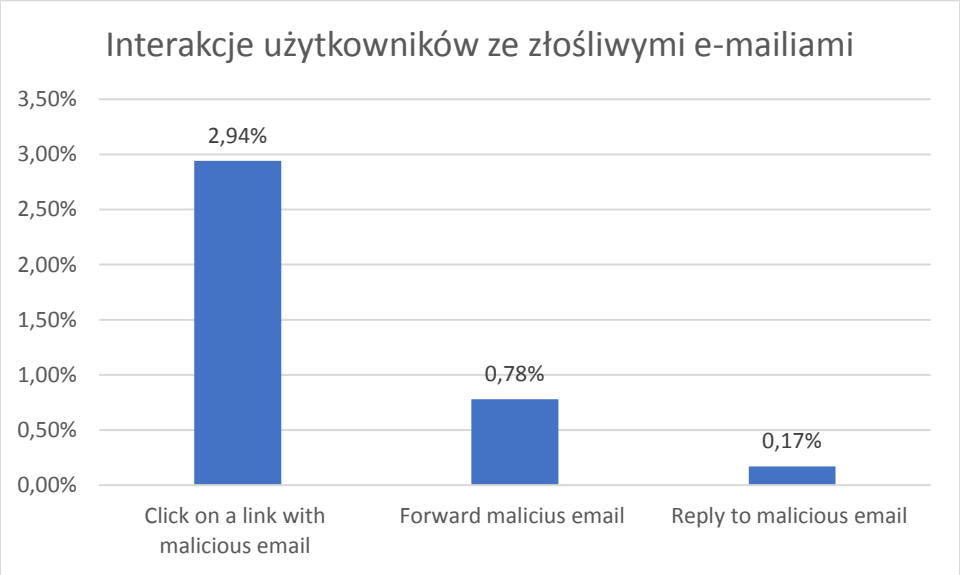
Organizacje powinny zawsze zachęcać użytkowników do zgłaszania podejrzanych wiadomości e-mail, ale napływ zgłoszeń może być uciążliwy dla zespołów IT dysponujących ograniczonymi zasobami. Dobrym sposobem na zwiększenie dokładności zgłoszeń jest konsekwentne prowadzenie szkoleń z zakresu świadomości bezpieczeństwa. Nasze badania wykazały, że organizacje, które szkolą swoich użytkowników, już po dwóch kampaniach szkoleniowych odnotowują 73% wzrost dokładności raportowanych przez nich wiadomości e-mail.



3% użytkowników klika na linki w złośliwych e-mailach

Po zidentyfikowaniu i potwierdzeniu złośliwych wiadomości e-mail, administratorzy IT muszą zbadać potencjalny zakres i wpływ ataku. Identyfikacja wszystkich osób w organizacji, które otrzymały złośliwe wiadomości może być niezwykle czasochłonna bez odpowiednich narzędzi. Badania Barracudy wykazały, że średnio 10 pracowników jest dotkniętych każdym atakiem phishingowym, który zdoła się przedostać.

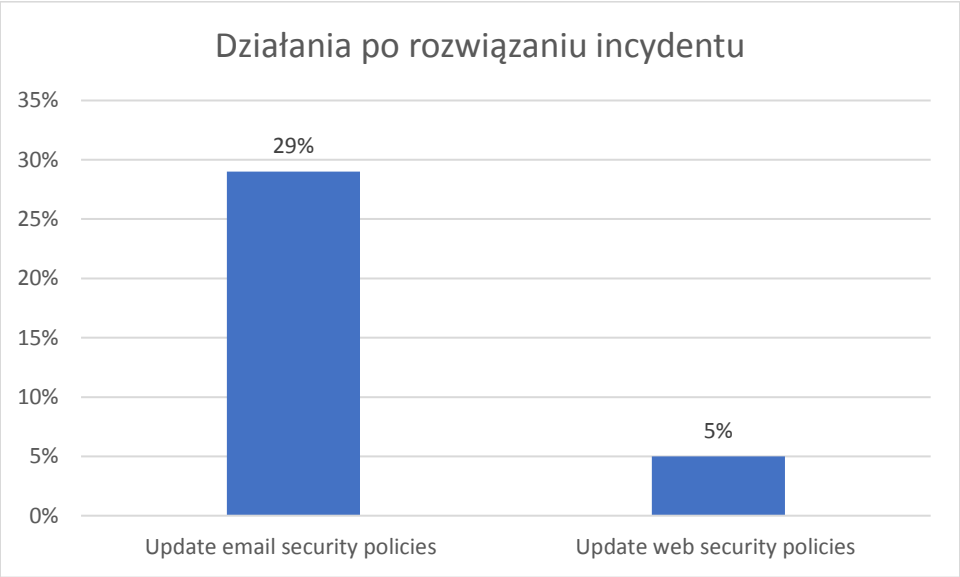
Ponadto, 3% pracowników kliknie na link w złośliwym e-mailu, narażając całą organizację na atak. Innymi słowy, przeciętna organizacja licząca 1100 użytkowników będzie miała około pięciu użytkowników, którzy klikną na link w złośliwej wiadomości e-mail każdego miesiąca. Pracownicy będą również przesyłać dalej lub odpowiadać na złośliwe wiadomości, rozprzestrzeniając ataki dalej w obrębie swojej firmy lub nawet na zewnątrz. Chociaż bezwzględne liczby mogą wydawać się niewielkie, to potencjalna skala ataków jest znacząca. Hakerzy potrzebują tylko jednego kliknięcia lub odpowiedzi, aby atak się powiódł. Wystarczy 16 minut, aby użytkownicy kliknęli na złośliwy link, dlatego szybkie zbadanie sprawy i usunięcie skutków ataku jest kluczowe dla zapewnienia bezpieczeństwa organizacji.



Złośliwe e-maile pozostają w skrzynkach użytkowników przez 83 godziny, zanim zostaną usunięte.

Usuwanie skutków ataków może być procesem długotrwałym i czasochłonnym. Analitycy firmy Barracuda ustalili, że od momentu, w którym atak trafia do skrzynek użytkowników, do momentu wykrycia go przez zespół bezpieczeństwa lub zgłoszenia przez użytkowników i ostatecznego usunięcia, mija średnio trzy i pół dnia, czyli nieco ponad 83 godziny. Czas ten można znacznie skrócić dzięki ukierunkowanym szkoleniom z zakresu bezpieczeństwa, które poprawią dokładność zgłoszeń od użytkowników, oraz wdrożeniu zautomatyzowanych narzędzi naprawczych, które mogą automatycznie identyfikować i usuwać ataki, uwalniając czas pracowników działu bezpieczeństwa.

Wiele zespołów ds. bezpieczeństwa wykorzystuje również informacje o zagrożeniach, pochodzące z rozwiązanych incydentów, do aktualizacji polityk bezpieczeństwa i zapobiegania przyszłym atakom. Na przykład, 29% organizacji regularnie aktualizuje swoje listy blokowania, aby blokować wiadomości od określonych nadawców lub z określonych regionów geograficznych. Jednak tylko 5% organizacji będzie aktualizować swoje zabezpieczenia internetowe, aby zablokować dostęp do złośliwych witryn dla całej organizacji. Ten niewielki odsetek wynika z braku integracji pomiędzy reagowaniem na incydenty a bezpieczeństwem sieciowym w większości organizacji.



Jak chronić się przed zagrożeniami po dostarczeniu wiadomości e-mail

- **Wyszkol swoich użytkowników, aby zwiększyć dokładność i liczbę zgłaszanych ataków.** Wyedukowany użytkownik poczty elektronicznej może zapobiec niszczącym skutkom udanego ataku na pocztę elektroniczną. Ciągłe szkolenie w zakresie świadomości bezpieczeństwa zwiększy prawdopodobieństwo, że użytkownicy będą zgłaszać potencjalne zagrożenia do swojego zespołu IT, zamiast odpowiadać, klikać lub przesyłać je dalej. Szkolenia dla użytkowników końcowych powinny być częste, tak aby najlepsze praktyki bezpieczeństwa zostały na stałe wdrożone, a dokładność zgłaszanych zagrożeń chroniła dział IT przed poświęcaniem zbyt dużej ilości czasu na badanie niezłośliwej poczty śmieciowej.

- **Polegaj na społeczności jako źródle potencjalnych zagrożeń.** Dzielenie się danymi o zagrożeniach to skuteczny sposób zapobiegania zagrożeniom, które ewoluują i narażają na szwank dane i użytkowników. Powiązane, a czasami identyczne zagrożenia związane z wiadomościami e-mail mogą dotyczyć więcej niż jednej organizacji, ponieważ hakerzy często wykorzystują te same techniki ataków na wiele celów. Wykorzystanie danych wywiadowczych gromadzonych przez inne organizacje jest skutecznym podejściem do pokonywania ataków na dużą skalę, zamiast korzystania wyłącznie z danych o zagrożeniach zebranych przez indywidualną sieć organizacji. Upewnij

się, że twoje rozwiązanie reagowania na incydenty może uzyskać dostęp i wykorzystać współdzielone dane o zagrożeniach w celu skutecznego wyszukiwania zagrożeń i ostrzegania o potencjalnych incydentach.

- **Wykorzystaj narzędzia do wyszukiwania zagrożeń w celu szybszego badania ataków.** Odkrywanie potencjalnych zagrożeń, jak również identyfikacja zakresu ataku i wszystkich dotkniętych użytkowników może zająć godziny, jeśli nie dni. Organizacje powinny wdrożyć narzędzia do wyszukiwania zagrożeń, które dają im wgląd w pocztę po jej dostarczeniu. Narzędzia te mogą być wykorzystywane do identyfikacji anomalii w już dostarczonej poczcie, szybkiego wyszukiwania zaatakowanych użytkowników i sprawdzania, czy weszli oni w interakcję ze złośliwymi wiadomościami.

- **Automatyzuj działania zaradcze tam, gdzie to możliwe.** Zautomatyzowane systemy reagowania na incydenty mogą znacznie skrócić czas potrzebny na zidentyfikowanie podejrzanych wiadomości e-mail, usunięcie ich ze skrzynek wszystkich użytkowników, których dotyczą oraz zautomatyzowanie procesów, które wzmocnią obronę przed przyszłymi zagrożeniami. Wdrażając zautomatyzowane przepływy pracy, klienci firmy Barracuda skrócili czas reakcji nawet o 95%, skracając czas rozprzestrzeniania się zagrożenia i uwalniając swoje zespoły IT, które mogą skupić się na innych zadaniach związanych z bezpieczeństwem.

- **Wykorzystaj punkty integracji.** Organizacje muszą nie tylko zautomatyzować swoje przepływy pracy, ale także zintegrować reagowanie na incydenty z zabezpieczeniami poczty elektronicznej i stron internetowych, aby zapobiec dalszym atakom. Dane zebrane podczas reagowania na incydenty mogą być również wykorzystane do automatycznych działań naprawczych i pomocy w identyfikacji powiązanych zagrożeń.