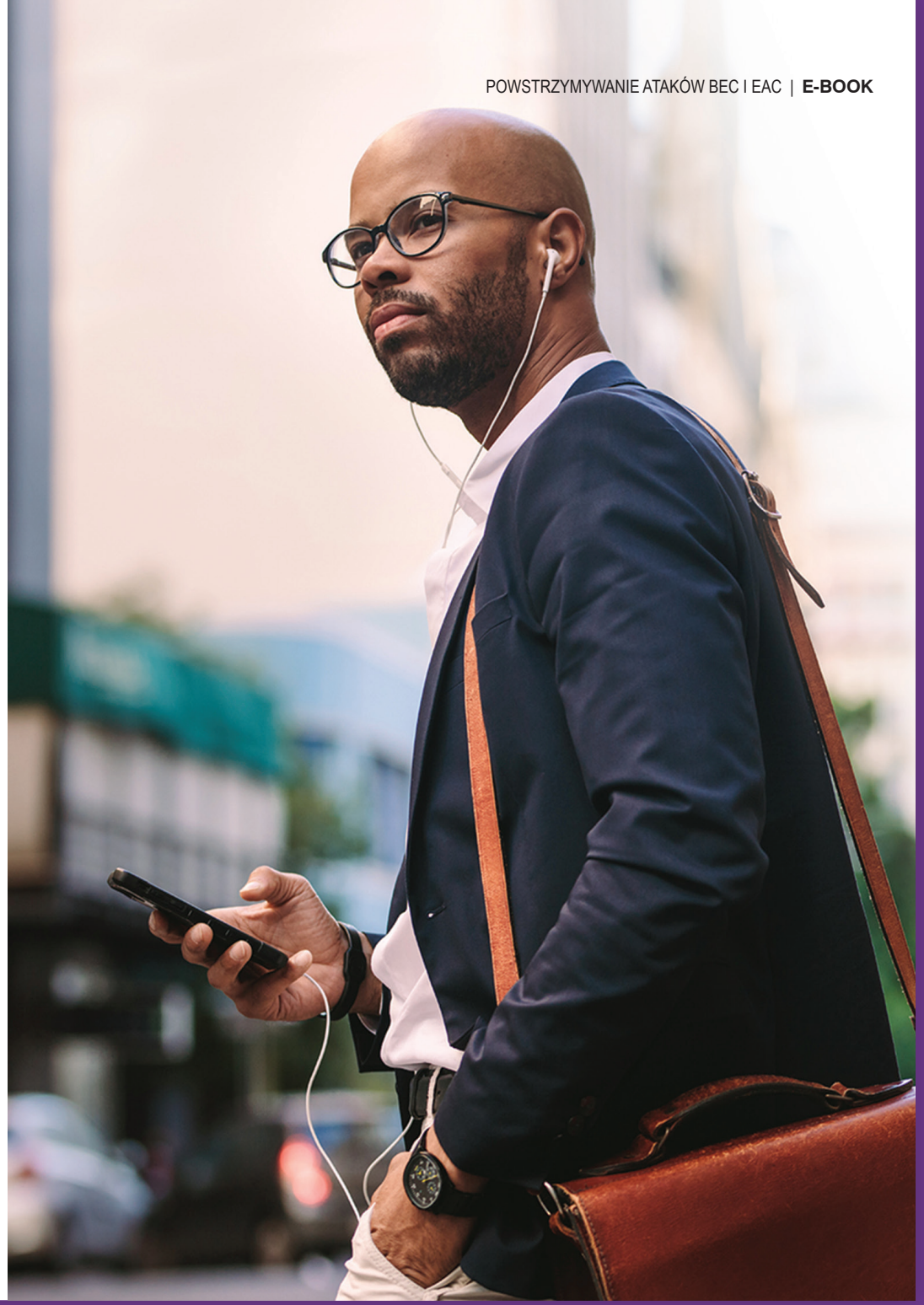
proofpoint.



2020

Powstrzymywanie ataków BEC i EAC

Przewodnik nowoczesnego CISO dotyczący ochrony użytkowników za pomocą rozwiązań Proofpoint zapewniających bezpieczeństwo poczty e-mail

Wysyłanie fałszywych biznesowych wiadomości (BEC) i naruszanie bezpieczeństwa konta e-maila (EAC) są złożonymi problemami wymagającymi wielopoziomowych zabezpieczeń. Cyberprzestępcy znają wiele metod nakłaniania użytkowników, które wykorzystują zaufanie oraz dostęp użytkowników do kluczowych danych, systemów i zasobów.

Aby osiągnąć sukces, przestępcy muszą znaleźć tylko jedną skuteczną metodę. Dlatego musisz zablokować wszystkie, a nie tylko wybrane metody.

Poniżej przedstawiamy, w jaki sposób narzędzie Proofpoint zapewniające bezpieczeństwo poczty e-mail zabezpieczy Twoich użytkowników przed atakami BEC i EAC – i dlaczego jest to jedyne narzędzie, które naprawdę rozwiązuje narastające problemy.

Wprowadzenie

Przeciętny atak zapewnia przestępcom zysk netto na poziomie ok.

130 000 USD.

Ataki BEC i EAC są szybko narastającymi problemami, na które nie ma łatwego rozwiązania.

A to dlatego, że każdy atak BEC i EAC jest inny. Mimo że wszystkie tego typu ataki rozgrywają się na podobnych zasadach, każdy atak jest tak wyjątkowy jak osoby, w które jest wymierzony, a także ich cechy charakteru oraz relacje oparte na zaufaniu, które wykorzystują przestępcy.

Rozpoczynają się od pozornie zwykłej prośby zawartej w wiadomości e-mail od szefa, współpracownika lub partnera biznesowego. „Przelej pieniądze na to konto." „Wyślij płatność tutaj." „Dołącz pliki pracowników".

Definicja BEC i EAC

Prośby wysyłane w ramach ataków BEC i EAC pochodzą jednak od innych osób, niż nam się to wydaje. Są to oszuści stosujący adres e-mail, który wygląda jak znany adres – lub w niektórych przypadkach jak konto e-mailowe osoby, pod którą podszywa się nadawca.

Według FBI ataki BEC i EAC sprawiły, że od 2016 r. firmy na całym świecie poniosły straty (rzeczywiste i potencjalne) w wysokości ponad **26 mld USD**.[1] Przeciętny atak przynosi przestępcy kwotę netto na poziomie niemal **130 000 USD**.[2]

Gartner przewiduje, że ilość ataków BEC będzie się zwiększać dwukrotnie rok do roku, powodując do 2023 r. rzeczywiste straty warte **5 mld USD**.[3]

Ataki EAC, zwane także przejęciem konta e-mailowego, są często powiązane z BEC, ponieważ zainfekowane konta e-mailowe są coraz częściej stosowane w oszustwach typu BEC. (EAC jest także podstawą innego rodzaju ataków cybernetycznych). FBI zaczęło je śledzić w 2017 roku.

Coraz większe żniwo

W czasach infrastruktury opartej na chmurze ataki EAC stają się coraz bardziej powszechne. Najnowsze badanie Proofpoint na temat zagrożeń wykazało, że 40% organizacji stosujących chmurę miało przynajmniej jedno zainfekowane konto.

A nawet jeśli organizacjom uda się odeprzeć ataki BEC, cyberprzestępcy mogą wykorzystać ich zaufane domeny, aby przeprowadzić ataki wymierzone w partnerów biznesowych i klientów. Te ataki mogą nadwyrężyć relacje biznesowe i zniszczyć reputację szanowanych marek.

Aby zatrzymać ataki BEC i EAC, potrzebne są wielopoziomowe zabezpieczenia, które blokują każdą taktykę stosowaną przez przestępców – a nie tylko niektóre z nich.

Poniżej przedstawiamy, w jaki sposób narzędzie Proofpoint zapewniające bezpieczeństwo poczty e-mail ochroni Twoich użytkowników przed atakami BEC i EAC – i dlaczego jest to jedyne narzędzie, które naprawdę rozwiązuje narastające problemy.

[1] **FBI. „Business Email Compromise: The $26 Billion Scam." (Wysyłanie fałszywych biznesowych wiadomości: oszustwo na 26 miliardów USD) Wrzesień 2019.**

[2] **Darla Mercado (CNBC). „New online financial scam costs victims $130K per attack." (Nowe internetowe oszustwo finansowe sprawia, że przy każdym ataku ofiary tracą 130 tys. USD) Luty 2018.**

[3] **Gartner Research. „Protecting Against Business Email Compromise Phishing." (Ochrona przed fałszywymi biznesowymi wiadomościami) Marzec 2020.**

Dlaczego tak trudno zatrzymać ataki BEC i EAC

BEC i EAC koncentrują się na **ludzkich słabościach**, a nie na **niedoskonałościach technicznych**

Ataki BEC trudno jest wykryć, ponieważ nie wykorzystują złośliwego oprogramowania ani złośliwych URL, które mogą zostać zanalizowane przez standardowe zabezpieczenia cybernetyczne. W atakach BEC przestępcy podają się za inną osobę lub wykorzystują inne techniki inżynierii społecznej, aby nakłonić ludzi do działania w imieniu przestępcy. Przykładami takich działań jest wysyłanie poufnych informacji, przelewów pieniężnych, przekierowywanie listy płac i nie tylko.

Ze względu na ukierunkowany charakter i zastosowanie inżynierii społecznej, manualne analizowanie i usuwanie tych ataków jest trudne i czasochłonne.

Ataki BEC wykorzystują wiele różnych technik podszywania się pod inne podmioty, na przykład:

- **Fałszowanie domen.** Przestępca fałszuje adres nadawcy (pole „WIADOMOŚĆ OD” lub „ścieżka zwrotna” w e-mailu), wykorzystując zaufaną domenę. Odbiorca widzi sfałszowany adres, a nie rzeczywistą domenę nadawcy.
- **Domeny przypominające inne domeny.** Aby przedostać się przez środki przeciwdziałające fałszowaniu domen, przestępcy często rejestrują domeny, które przypominają domeny, pod które próbują się podszyć. W nazwie takich domen może na przykład znajdować się cyfra „0” zamiast litery „O” („tw0jafirma.com”).
- **Fałszowanie wyświetlanej nazwy.** Nadawcy e-maili mogą w łatwy sposób zmienić wyświetlaną nazwę. Wiele klientów mobilnej poczty elektronicznej przedstawia domyślnie wyłącznie wyświetlaną nazwę, szczególnie na urządzeniach mobilnych, co sprawia, że jest to prosta, ale skuteczna technika. Większość ataków BEC łączy fałszowanie wyświetlanej nazwy z innymi rodzajami fałszowania.

Takie ataki są skuteczne, ponieważ nadużycie domeny stanowi skomplikowany problem. Zatrzymywanie fałszowania domen jest wystarczająco trudne – a przewidywanie każdej potencjalnej domeny przypominającej inne domeny jest jeszcze trudniejsze. Ten problem staje się jeszcze bardziej zawiły, jeśli uwzględni się każdą domenę partnera zewnętrznego, którą przestępcy mogą wykorzystać w ataku BEC, aby nadużyć zaufanie Twoich użytkowników.

W EAC przestępca zdobywa kontrolę nad prawidłowym kontem e-mail, umożliwiając przeprowadzenie podobnych ataków. Ale w tych przypadkach przestępca nie próbuje tylko podać się za kogoś innego ze względów praktycznych – przestępca jest tą osobą.

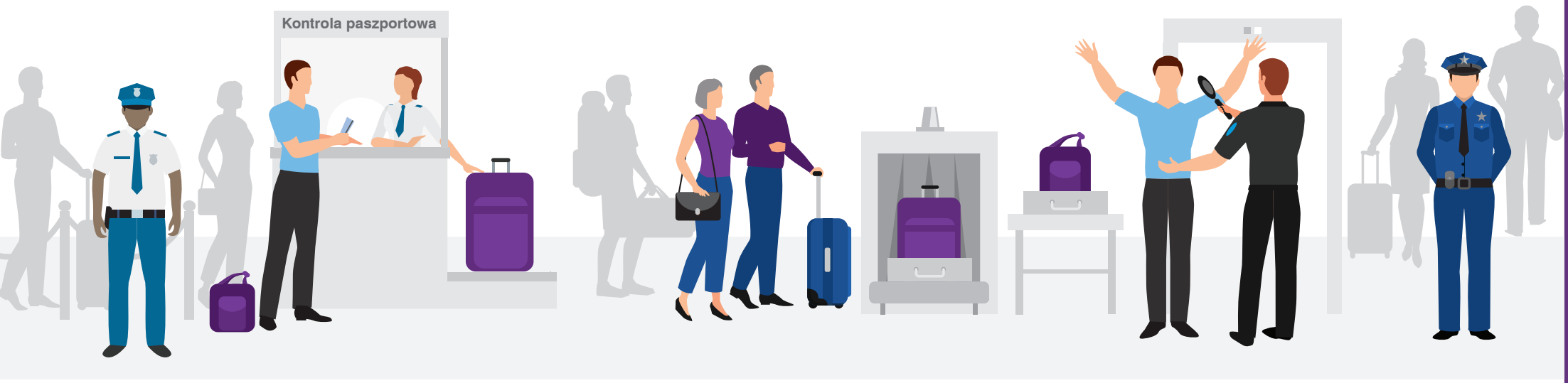
Ponieważ ataki BEC i EAC wykorzystują ludzkie słabości, a nie niedoskonałości techniczne, do obrony przed nimi potrzebne są środki zabezpieczające nastawione na użytkowników, które mogą powstrzymać, wykryć i reagować na wiele różnych technik BEC i EAC.

Porównanie do podróży samolotem

Zastanów się, w jaki sposób lotniska zarządzają zmieniającymi się i rozległymi potencjalnymi problemami w zakresie bezpieczeństwa. Większość lotnisk przyjmuje wielostronne podejście do tej kwestii, a na każdy element składa się dużo kontroli i procedur.

- **Kontrola paszportowa.** Polega na sprawdzaniu paszportów (lub prawa jazdy) oraz kart pokładowych, aby zapewnić, że pasażerowie 1) są osobami, za które się podają i 2) mają uprawnienia do wejścia na pokład.
- **Skanowanie.** Obejmuje skanowanie bagażu i pasażerów, aby zapewnić, że żadne niebezpieczne elementy nie przedostaną się na pokład – oraz że pokładu nie opuści żaden przedmiot, który powinien tam pozostać.
- **Pracownicy obsługi lotniska.** Wyszkoleni pod kątem wykrywania i zgłaszania podejrzanych cech i zachowań.
- **Bezpieczeństwo na lotnisku.** Zespół bezpieczeństwa z uprawnieniami i środkami służącymi do fizycznego zatrzymania niebezpiecznych osób i oddzielenia ich od osób, które mogłyby skrzywdzić.
- **Egzekwowanie prawa.** Organy posiadające wiedzę o zewnętrznych działaniach, które mogą zagrażać podróżującym, np. kradzież tożsamości, sfałszowane paszporty i skoordynowane działania przestępcze. Pomagają utworzyć listy zakazów lotu, ostrzegają zespół bezpieczeństwa lotniska o potencjalnych zagrożeniach i umożliwiają złapanie wielu przestępców, zanim wejdą na lotnisko.

Proofpoint ma podobne podejście w zakresie zabezpieczania wiadomości e-mail. W taki sposób nasze rozwiązanie w zakresie bezpieczeństwa poczty e-mail zabezpiecza każdą drogę, którą może wybrać przestępca, żeby przeprowadzić atak BEC/EAC.



Uwierzytelnianie (kontrola paszportowa)

Jedną z pierwszych czynności dotyczących bezpieczeństwa, jakie muszą wykonać osoby podróżujące do innych krajów to kontrola dokumentów tożsamości i kart pokładowych. To jeden z najważniejszych kroków, jakie może wykonać zespół bezpieczeństwa na lotnisku w celu zapewnienia, że podróżujący jest osobą, za którą się podaje oraz że ma uprawnienia do wejścia na pokład.

Wiele ataków BEC wykorzystuje fałszowanie domen e-mail. Przestępca w nielegalny sposób wykorzystuje zaufaną domenę, aby podać się za osobę, której można zaufać. Oszust fałszuje adres e-mail osoby, za którą się podaje, aby odbiorcy – nawet ci, którzy wiedzą, że należy sprawdzić ścieżkę zwrotną w nagłówku e-mail – nie mogli wykryć różnicy.

Dlatego bardzo ważne jest zastosowanie struktury uwierzytelniania e-maili takiej jak DMARC (Domain-based Message Authentication, Reporting and Conformance). Dzięki DMARC można zabezpieczyć domenę e-mailową przed oszustami, którzy chcą wykorzystać ją do wysyłania spamu, ataków phishingowych i BEC.

Nasze narzędzie do uwierzytelniania e-maili zapewnia widoczność, narzędzia i usługi służące do uwierzytelniania prawidłowych e-maili oraz blokowania fałszywych wiadomości, zanim dostaną się do skrzynki odbiorczej.

Pomożemy Ci:

- Wyświetlić wszystkie zagrożenia przychodzące – takie jak ataki polegające na fałszowaniu wyświetlanej nazwy i fałszowaniu domen przypominających inne domeny – oraz blokowanie ich przy bramie Proofpoint.
- Szybko i poufnie wymusić uwierzytelnianie DMARC w celu blokowania fałszywych e-maili, które fałszują zaufane domeny.
- Automatycznie zidentyfikować i oznaczyć domeny przypominające inne domeny, które są zarejestrowane przez strony trzecie i których nie możesz kontrolować.

Brama e-mail (skanowanie)

Na lotniskach skanowanie pasażerów i bagażu może być często bardzo irytujące. Ale są to ważne procesy zapewniające bezpieczeństwo innych pasażerów. Dzięki prawidłowemu skanowaniu lotniska można zapewnić, że na pokład nie przedostanie się nic niebezpiecznego.

Bramy e-mail odgrywają podobną rolę w zakresie bezpieczeństwa cybernetycznego. Większość bram skanuje e-maile, poszukując złośliwego oprogramowania i niebezpiecznych linków URL. Ta warstwa bezpieczeństwa jest ważna, aby zatrzymać przejęcie konta podczas ataku EAC. Ale BEC i EAC polegają także na inżynierii społecznej, a nie tylko na złośliwym oprogramowaniu i złośliwych linkach. Dlatego często wiadomość nie zawiera żadnego załącznika ani adresu URL, które można poddać analizie.

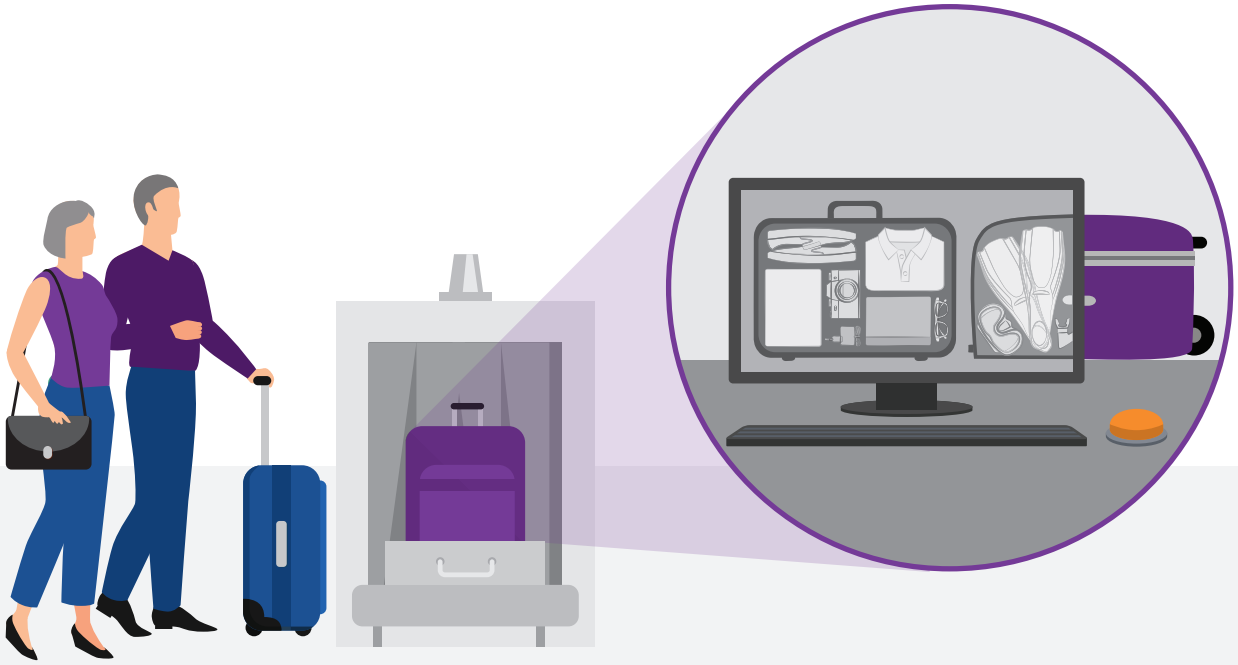
Aby zatrzymać ataki BEC i EAC, bramy e-mail muszą być bardziej zaawansowane i analizować treść oraz kontekst każdego wysłanego e-maila.

Nasze rozwiązanie zapewniające bezpieczeństwo poczty e-mail wykrywa złośliwe URL i załączniki, które mogą prowadzić do zainfekowanych kont. Skanujemy także wiadomości przychodzące w poszukiwaniu znaków inżynierii społecznej i oszustw. Nasza dynamiczna klasyfikacja analizuje e-maile i zarządza e-mailami na podstawie kilku czynników, takich jak m. in.:

- treść e-maila,
- reputacja nadawcy (na podstawie adresu IP w nagłówku e-maila).

Zwykle uwzględniamy kilka czynników. Czy wiadomość pochodzi od zaufanego nadawcy – i czy nadawca ma dobrą reputację? Czy wiadomość zawiera podejrzany temat? Czy nadawca i odbiorca mieli już kontakt e-mailowy? Czy treść e-maila wygląda podejrzanie?

Każdej wiadomości przypisujemy wynik na podstawie poziomu ryzyka. Potem możesz zdecydować, co zrobić z wiadomością zgodnie z uzyskanym wynikiem: zezwolić na otrzymanie wiadomości, zablokować lub przekierować wiadomość do folderu kwarantanny.



Szkolenie na temat bezpieczeństwa (pracownicy obsługi lotniska)

Skanery ciała na lotniskach, wykrywanie chemikaliów, rozpoznawanie twarzy i inne udoskonalenia technologiczne ułatwiły podróżowanie samolotem. Ale do tych wszystkich metod potrzebni są dobrze wyszkoleni pracownicy, którzy będą obsługiwać maszyny, interpretować wyniki i wiedzieć, co z nimi zrobić.

Jeśli chodzi o bezpieczeństwo cybernetyczne, rola ludzi jest jeszcze bardziej istotna, szczególnie w przypadku ataków BEC i EAC. A to dlatego, że te ataki są ukierunkowane na ludzi i wykorzystują ludzkie słabości. Poza tym ataki te są bezskuteczne, jeśli nikt się na nie nie nabierze.

Dzięki szkoleniu na temat bezpieczeństwa pomożemy ci zapewnić, że Twoi użytkownicy staną się silną ostatnią linią obrony. Osiągniemy to przez:

- uczenie użytkowników, jak rozpoznawać, odrzucać i zgłaszać podejrzane wiadomości,
- ujawnianie słabości użytkowników, pokazywanie, którzy użytkownicy są najbardziej podatni na taktyki BEC/EAC, na które najbardziej mogą się nabrać,
- dostosowanie szkoleń do osób, które ich potrzebują, na podstawie słabości użytkowników, sposobu, w jaki ataki są w nich wymierzane oraz ich praw dostępu do kluczowych danych, systemów i zasobów.

Nasze moduły szkoleń na temat bezpieczeństwa są uzupełnione kompleksowymi i aktualnymi danymi na temat zagrożeń, więc odzwierciedlają najnowsze rzeczywiste ataki i techniki. Poza tym zgłaszanie prób BEC/EAC jest łatwe za pomocą naszego przycisku PhishAlarm dla użytkowników Microsoft Outlook i PhishAlarm Analyzer dla zespołu bezpieczeństwa. Obydwa narzędzia są częścią systemu zgłaszania podejrzanych e-maili, który ułatwia zgłaszanie ataków BEC/EAC i naprawianie szkód.

Reakcja na zagrożenia (bezpieczeństwo na lotnisku)

Nawet w przypadku użycia najbardziej zaawansowanych narzędzi i zatrudnieniu najlepiej wyszkolonych pracowników, zawsze coś może pójść nie tak. Dlatego każde lotnisko musi mieć lokalny zespół ochrony. Ci uzbrojeni oficerowie pomagają ograniczać sytuacje wysokiego ryzyka, aresztują każdego, kto stanowi zagrożenie oraz zatrzymują lub usuwają takie osoby z lotniska.

Nasze funkcje automatycznego reagowania na zagrożenia odgrywają podobną rolę w walce z BEC i EAC, koordynując i automatyzując kluczowe części procesu reagowania na incydenty. Oto przykłady działań, które można ustawić jako wykonywane automatycznie, jeśli w skrzynce odbiorczej użytkownika została rozpoznana próba ataku BEC lub EAC:

- wyciąganie e-maili phishingowych zawierających adresy URL, które stały się niebezpieczne po dostarczeniu – łącznie ze wszelkimi kopiami, które zostały przekazane innym użytkownikom,
- usuwanie niepożądanych wiadomości z kont wewnętrznych, które zostały zainfekowane,
- poddawanie kwarantannie e-maili zgłoszonych przez użytkowników jako potencjalnie wysłane przez oszustów,
- wymuszanie zresetowania hasła,
- zawieszanie zainfekowanych kont,
- odwołanie dowolnej aktywnej sesji użytkownika,
- wymuszanie uwierzytelniania opartego na ryzyku.

Pomożemy Ci szybko zatrzymać i usunąć zagrożenia BEC i EAC, aby uniknąć najgorszych efektów udanego ataku.

Obrona konta w chmurze (egzekwowanie prawa)

Czasami, aby zatrzymać zagrożenia związane z podróżą samolotem potrzebne są informacje wykraczające poza granice lotniska. W tym zakresie dużą rolę odgrywają zewnętrzne organy egzekwowania prawa. Lokalna policja, FBI, ministerstwa spraw wewnętrznych i inne agencje mogą zatrzymać zagrożenia i ostrzec pracowników lotniska o działaniach przestępczych, które miały miejsce poza lotniskiem i które mogłyby naruszyć bezpieczeństwo podróżujących.

Tak samo jest w przypadku ataków EAC. W ataku EAC cyberprzestępca przejmuje kontrolę nad kontem prawidłowego użytkownika. A ponieważ konto jest prawdziwe, nawet najlepiej wyszkoleni użytkownicy i najbardziej zaawansowane bramy e-mail mogą mieć trudności w rozpoznaniu takiego działania jako zagrożenia, zakładając, że organizacja w ogóle skanuje wiadomości wewnętrzne.

Nasze bezpieczeństwo w chmurze jest jak policja dla ataków EAC. Wykrywa przypadki naruszenia bezpieczeństwa konta e-mail opartego na chmurze, ostrzega Twój zespół ochrony i podejmuje kroki w celu naprawienia konta, zanim przestępca będzie mieć możliwość jego nadużycia.

Możemy użyć najnowszych informacji na temat zagrożeń i dokładnych danych kryminalistycznych, aby zestawić zagrożenia zewnętrzne, zachowanie konta i kontekst użytkownika. W ten sposób łączymy ze sobą:

- aktywność na koncie – nietypowe operacje, takie jak dodawanie wielu kopii ukrytych w e-mailach lub ustawianie zasad dotyczących przekierowania kalendarzy,
- kontekst – nietypowe logowania z miejsc zbyt odległych, aby mogły pochodzić od jednego użytkownika lub z nowych urządzeń, przez nieznane sieci i o nietypowych porach,
- informacje o zagrożeniach – kampanie ataków wymierzone w określone stanowiska lub grupy za pomocą metod spójnych z zaobserwowaną aktywnością na koncie użytkownika.

Jeśli coś wygląda nie tak, stosowane są środki kontrolne oparte na ryzyku, np. zawieszenie konta, proszenie użytkownika, aby zalogował się ponownie lub wysłanie prośby o uwierzytelnianie wieloskładnikowe.

Łączenie wszystkich elementów

Narzędzie Proofpoint do zabezpieczania poczty e-mail uwzględnia wszystkie taktyki przestępców i zabezpiecza wszystkie nośniki zagrożeń, w tym e-mail firmowy, prywatne konto internetowe, aplikacje w chmurze dla użytkowników końcowych. Nasze zintegrowane, kompleksowe rozwiązanie:

- ogranicza ryzyko BEZ i EAC, chroniąc przed wieloma różnymi taktykami przestępców,
- zapewnia wgląd we wszystkie wiadomości wysłane za pomocą Twojej domeny, w tym zaufanych nadawców zewnętrznych oraz ryzyko pochodzące od zainfekowanych kont w aplikacjach w chmurze,
- zatrzymuje fałszywe e-maile i fałszywe stosowanie zaufanych domen oraz wykrywa zainfekowane konta w chmurze oraz phishing,
- identyfikuje Twoich najczęściej atakowanych użytkowników, pracowników atakowanych w ramach wyłudzenia danych logowania oraz fałszywe e-maile, a także osoby podatne na kradzież danych logowania,
- umożliwia zastosowanie mechanizmów adaptacyjnych, takich jak izolowanie przeglądarki i szkolenie na temat bezpieczeństwa dla Twoich najczęściej atakowanych użytkowników, czyli Very Attacked People™,
- szkoli użytkowników końcowych, aby stali się bardziej odporni na ataki BEC i EAC.

Dzięki dokładnemu wglądowi w te wszystkie dane możesz lepiej zrozumieć zagrożenie, poinformować zarząd i partnerów biznesowych o ryzyku oraz priorytetowo podejść do kwestii ograniczania ryzyka. Sprawiamy, że już nie musisz zarządzać rozwiązaniami pochodzących od różnych dostawców. Dzięki temu kompleksowemu podejściu możesz zoptymalizować zasoby tak, aby poprawić bezpieczeństwo i skuteczność operacji.

Dowiedz się więcej o tym, w jaki sposób wieloskładnikowe podejście Proofpoint nastawione na użytkowników pomaga zatrzymać zagrożenia BEC i EAC na https://www.proofpoint.com/us/solutions/bec-and-eac-protection

DOWIEDZ SIĘ WIĘCEJ

Więcej informacji dostępnych na **proofpoint.com**.

INFORMACJE O PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) jest wiodącą firmą zajmującą się bezpieczeństwem cybernetycznym, która chroni największe aktywa i największe zagrożenia każdej organizacji, czyli ludzi. Dzięki zintegrowanemu zestawowi rozwiązań opartych na chmurze Proofpoint pomaga firmom na całym świecie w zatrzymywaniu ukierunkowanych zagrożeń, zabezpiecza ich dane i sprawia, że ich użytkownicy stają się bardziej odporni na ataki cybernetyczne. Wiodące organizacje o różnych rozmiarach, w tym ponad połowa firm z listy Fortune 1000, polegają na rozwiązaniach Proofpoint dotyczących bezpieczeństwa i zgodności ukierunkowanych na ludzi, które ograniczają najważniejsze zagrożenia związane z e-mailami, chmurą, mediami społecznościowymi i siecią. Więcej informacji można znaleźć na **www.proofpoint.com**.

proofpoint.

0501-002-01-01 06/20