2020 Kompleksowy przewodnik po strategii bezpieczeństwa e-maili

Powstrzymywanie złośliwego oprogramowania, phishingu i oszustw e-mailowych dzięki podejściu nastawionemu na ludzi

STRESZCZENIE

E-mail jest najważniejszym narzędziem biznesowym każdej organizacji – a obecnie także najpopularniejszą drogą rozprzestrzeniania złośliwego oprogramowania.[1] Stał się żyznym gruntem dla najbardziej szkodliwych zagrożeń cybernetycznych i wszelkiego rodzaju oszustw[2] oraz kanałem, który jest najczęściej stosowany przez cyberprzestępców do atakowania ich ofiar. Za pomocą e-maili cyberprzestępcy nakłaniają użytkowników do kliknięcia na niebezpieczny link, co powoduje udostępnienie danych uwierzytelniających a nawet sprawia, że odbiorcy sami nieświadomie są sprawcami ataków (takich jak przelewanie pieniędzy lub wysyłanie poufnych plików).

Zagrożenia uległy zmianie. Mimo to znaczna część sektora bezpieczeństwa cybernetycznego nadal stosuje stare modele zagrożeń, starając się wprowadzić drobne ulepszenia do starych strategii, które z dnia na dzień stają się coraz mniej skuteczne.

Czas na nowe podejście. We współczesnym świecie zagrożeń skuteczny program bezpieczeństwa cybernetycznego koncentruje się przede wszystkim na ludziach.

Pomiar, wykrywanie i zgłaszanie zagrożenia użytkowników

Pierwszym krokiem ochrony użytkowników jest ustalenie, którzy użytkownicy są najbardziej narażeni na ataki. Mimo że każda organizacja może inaczej mierzyć różne czynniki ryzyka, wszystkie sposoby pomiaru powinny uwzględniać podatność, ataki i przywileje.

Podatność to sposób określenia użytkowników, którzy są najbardziej podatni na atak. Analiza ataku może wykryć, kto w Twojej organizacji jest celem ataku, jak poważna jest sytuacja i przez kogo prowadzony jest atak. Przywilej może pomóc określić, jak bardzo szkodliwy dla organizacji byłby skuteczny atak.

Użytkowników, którzy stanowią większe od przeciętnego ryzyko określone na podstawie dowolnego połączenia tych czynników, nazywamy VAP – czyli Very Attacked People™. Należy ich szybko rozpoznać, aby zespół ds. bezpieczeństwa mógł zastosować zebrane informacje i zgłosić je innym osobom w organizacji, jeśli to konieczne.

[1] Raport Verizon. „2019 Data Breach Investigations Report." (Raport Verizon z dochodzeń w sprawie naruszania danych w 2019 roku.) Lipiec 2019.
[2] Proofpoint. „Human Factor Report 2019." (Raport o czynnikach ludzkich w 2019 roku.) Wrzesień 2019.

Podatność: w jaki sposób użytkownicy pracują i na co klikają

Ocena podatności związana z tym, jak ludzie pracują zaczyna się od ustalenia, jakie stosują narzędzia, platformy i aplikacje. Może to obejmować określenie stosowanych aplikacji w chmurze oraz ustalenie, czy używane urządzenia są bezpieczne.

Drugą częścią pomiaru podatności jest rozpoznanie stopnia podatności użytkowników na phishing i inne cyberataki.

Szkolenie na temat bezpieczeństwa może pomóc w rozpoznaniu, którzy użytkownicy są w najmniejszym stopniu przygotowani na rozpoznanie i zgłaszanie zagrożeń cybernetycznych oraz na opieranie się im. Ogólnie, użytkownicy, którzy uzyskają słaby wynik w ćwiczeniach szkoleniowych lub nie ukończą tych ćwiczeń, są bardziej podatni na zagrożenia niż osoby, które osiągnęły wysokie wyniki.

Ale prawdziwy test odporności użytkowników polega na określeniu, jak radzą sobie z rzeczywistymi atakami. Symulowane ataki, szczególnie te, które przypominają rzeczywiście stosowanie techniki, mogą pomóc w rozpoznaniu osób podatnych na zagrożenia oraz taktyk, które działają na użytkowników.

Ataki: w jaki sposób użytkownicy są atakowani

Każdy cyberatak może być szkodliwy. Ale niektóre ataki są bardziej niebezpieczne, ukierunkowane lub zaawansowane niż inne. Dlatego pomiar tego aspektu ryzyka może być trudniejszy niż się to wydaje.

Niewybredne zagrożenia „produktowe” mogą być bardziej powszechne niż inne rodzaje zagrożeń. Ale można je dobrze rozpoznać i łatwiej zablokować.

Inne zagrożenia mogą pojawić się tylko w kilku atakach. Mogą jednak stanowić poważniejsze zagrożenie ze względu na ich stopień zaawansowania lub ludzi, w których są wymierzone.

Znajomość różnicy pomiędzy rodzajami ataków odgrywa istotną rolę w rozpoznaniu użytkowników, którzy są narażeni na duże ryzyko. Obszerna wiedza o zagrożeniach i terminowe uzyskiwanie danych są kluczowymi czynnikami w rozpoznaniu, kto i w jakim stopniu jest ofiarą ataku.

Przywilej: do czego użytkownicy mają dostęp

Pomiar przywilejów użytkowników rozpoczyna się od ustalenia wszystkich potencjalnie cennych elementów, do których mają dostęp: danych, uprawnień finansowych, kluczowych stosunków i nie tylko.

Pozycja użytkownika w strukturze organizacji również odgrywa rolę w ustalaniu przywilejów. Ale to nie jedyny czynnik – często nawet nie jest najważniejszy.

Asystent administratora może stanowić bardziej atrakcyjny cel ataku niż menedżer średniego poziomu, jeśli chodzi o szpiegowanie firm, ponieważ asystent ma dostęp do kalendarza dyrektora generalnego. Podobnie, pielęgniarka w szpitalu posiadająca dostęp do danych pacjenta może być bardziej przydatnym celem dla złodziei tożsamości niż dyrektor finansowy.

Ograniczanie ryzyka

Rozpoznanie osób VAP ma istotne znaczenie, jeśli chodzi o bezpieczeństwo e-maili. Ale to tylko pierwszy krok. Dzięki podejściu nastawionemu na ludzi wszyscy mogą być chronieni, ponieważ sposób ochrony odpowiada poziomowi ryzyka, na które narażone są poszczególne osoby.

Podstawowa warstwa: bezpieczeństwo dla każdego

Ponieważ ataki e-mailowe mogą mieć wiele różnych form, potrzebujesz obrony, która zatrzyma całą gamę zagrożeń e-mailowanych, a nie tylko niektóre z nich. Oto najważniejsze kroki, które trzeba wykonać, aby ochronić e-maile przed współczesnymi zagrożeniami:

- Zatrzymaj załączniki ze złośliwym oprogramowaniem i złośliwe URL, zanim dotrą do skrzynek odbiorczych użytkowników.
- Zapobiegaj atakom niezwiązanym ze złośliwym oprogramowaniem, takim jak włamania do firmowych kont e-mailowych (BEC) i innym oszustwom, także takim, które pochodzą z zainfekowanych kont e-mail w Twojej organizacji.
- Zabezpiecz przeglądanie Internetu i osobistej poczty elektronicznej za pomocą izolacji poczty internetowej i osobistej.
- Spraw, aby użytkownicy stali się bardziej odporni za pomocą szkolenia na temat bezpieczeństwa.
- Ochroń dane przed naruszeniami i zagrożeniami wewnętrznymi.

Warstwa VAP: regulowane środki kontroli dla osób o większych potrzebach

Skuteczna strategia zabezpieczania e-maili ochrania wszystkich użytkowników. Ale ochrona nastawiona na ludzi rozpoznaje, że niektórzy użytkownicy, czyli Twoi VAP, potrzebują dodatkowej warstwy bezpieczeństwa i dodatkowych środków kontroli. Takie osoby VAP mogą być bardziej podatne na to, że staną się ofiarami ataków. Mogą być także częściej celem ataków. Mogą mieć wysokie przywileje użytkowników w zakresie poufnych danych i systemów. Lub mogą charakteryzować się dowolnym połączeniem tych trzech cech, co powoduje wyższe ogólne ryzyko.

Poniżej znajdują się ważne środki kontrolne dla użytkowników zidentyfikowanych jako VAP:

- Ukierunkowane szkolenie na temat bezpieczeństwa
- Regulowane środki ochronne oparte na ryzyku, na przykład uwierzytelnianie o wyższym poziomie, izolacja sieci i URL.
- Ochrona przed zainfekowaniem (przejęciem) dla kont opartych na chmurze.

Reakcja: podejmowanie skutecznych działań, gdy dojdzie do ataku

Gdy atak stanie się skuteczny, prędkość, z jaką możesz powstrzymać i naprawić szkody może stanowić istotną różnicę pomiędzy krótkotrwałym incydentem a długotrwałym ograniczeniem.

W wielu organizacjach reakcja na incydenty jest wolnym, pracochłonnym procesem. Pod tym względem przydatna może okazać się automatyzacja.

Skuteczne procesy reakcji automatyzują pracochłonne zadania, takie jak powiązanie i analizowanie powiadomień bezpieczeństwa, weryfikacja wskaźników infekcji (IOC) i gromadzenie danych kryminalistycznych. Automatyzacja może także pomóc w działaniach naprawczych, takich jak aktualizacja zapory sieciowej i list zablokowanych wiadomości e-mail przez wyciąganie złośliwych wiadomości e-mail ze skrzynek pocztowych i ograniczanie dostępu do konta zainfekowanych użytkowników.

W przypadku strategicznego zastosowania automatyzacja przyspiesza czas reakcji na incydenty i odciąża członków zespołu ds. bezpieczeństwa, aby mogli skupić się na działaniach, które są najlepiej wykonywane przez ludzi.

Rezultat

Obecnie e-mail jest najważniejszym narzędziem biznesowym – i ulubionym kanałem ataków stosowanym przez cyberprzestępców. Mimo że ataki e-mailowe mogą mieć wiele różnych postaci, zróżnicowane źródła i unikalne cele – mają jeden wspólny element: ludzi.

Ataki e-mailowe polegają na skłonieniu odbiorców do zrobienia czegoś, czego nie powinni robić: otworzenia złośliwego załącznika, kliknięcia na niebezpieczny adres URL, wysłania poufnych informacji lub przelania pieniędzy na fałszywe konto. Dlatego zabezpieczenie e-maila wymaga podejścia nastawionego na ludzi.

Dzięki odpowiedniej strategii, odpowiednim narzędziom, danym i szkoleniu organizacje mogą zarządzać ryzykiem związanym z e-mailem i zabezpieczyć swój najważniejszy kanał komunikacji biznesowej.

WPROWADZENIE

E-mail jest zdecydowanie najczęstszym kanałem ataków

Codziennie na całym świecie bitwa o dane korporacyjne toczy się na jednej z najbardziej znanych i głównych przestrzeni współczesnej pracy: w skrzynce odbiorczej.

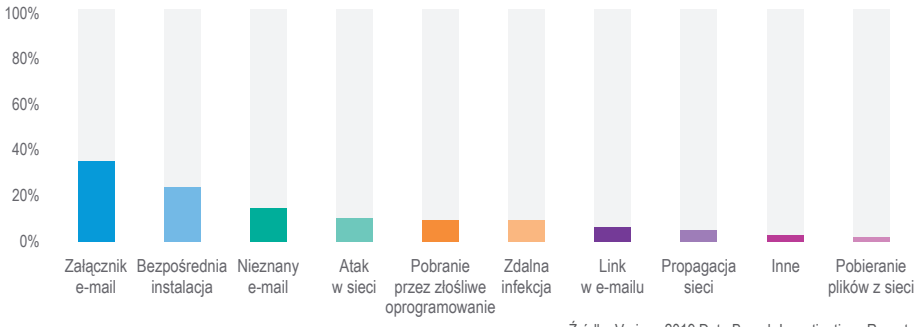
E-mail, będący najpopularniejszym kanałem rozsyłania złośliwego oprogramowania[3] oraz żyznym gruntem dla wszelkiego rodzaju oszustw,[4] jest narzędziem, którego cyberprzestępcy najczęściej używają do atakowania swoich ofiar. Za pomocą e-maili cyberprzestępcy nakłaniają użytkowników do kliknięcia na niebezpieczny link, co powoduje udostępnienie danych uwierzytelniających a nawet sprawia, że odbiorcy sami bezpośrednio wykonują polecenia (takie jak przelewanie pieniędzy lub wysyłanie poufnych plików).

Nie trudno zrozumieć, dlaczego przestępcy wolą stosować e-mail. E-mail opiera się na kilkudziesięcioletniej architekturze, która nie została zaprojektowana pod kątem zachowania bezpieczeństwa. E-mail jest uniwersalny. W odróżnieniu od sprzętu komputerowego i infrastruktury komputerowej, ataki e-mailowe wykorzystują luki w zabezpieczeniach, których nie da się naprawić – a mianowicie ludzi.

Co roku wiele organizacji wydaje miliardy na narzędzia zapewniające bezpieczeństwo w celu wzmocnienia granic sieci, wykrycia włamań do sieci i zabezpieczenia punktów końcowych. Ale dzisiejsze ataki rozszyfrowują ludzką naturę, a nie tylko technologię. A e-mail to najprostszy sposób, aby dotrzeć do ludzi.

Czas na nowe podejście. Dzisiejszy świat zagrożeń wymaga nowego sposobu myślenia i nowej strategii – takiej, która skupia się na ochronie ludzi, a nie infrastruktury.

Najważniejsze źródła złośliwego oprogramowania



Źródło: Verizon 2019 Data Breach Investigations Report

Potraktuj ten przewodnik jako punkt początkowy. Oto, czego się dowiesz:

- Dlaczego e-mail powinien być najważniejszym priorytetem bezpieczeństwa.
- Co sprawia, że tak trudno go zabezpieczyć.
- Dlaczego bezpieczeństwo nastawione na ludzi jest bardziej skuteczne – i bardziej opłacalne – niż podejścia nastawione na granice, które nie dotrzymują kroku dzisiejszym zagrożeniom nastawionym na ludzi.

KILKA FAKTÓW

94%

cybernetycznych zagrożeń zewnętrznych zaczyna się od e-maila.[5]

27%

zewnętrznych ataków powodujących naruszenie bezpieczeństwa firmy zostało wykonanych za pomocą skradzionych danych uwierzytelniających, często uzyskanych za pomocą prostego e-maila phishingowego.[6]

26 mld USD

Straty z powodu oszustw dotyczących fałszywych biznesowych wiadomości e-mail (BEC) i infekcji kont e-mailowych (EAC) osiągnęły wartość 26 mld USD; są to potencjalne straty na całym świecie.[7]

90%

rozpoznanych instancji złośliwego oprogramowania dociera do użytkownika przez e-mail.[8]

47 ataków dotyczących fałszerstwa e-mail

Organizacje będące celem ataków w samym pierwszym kwartale 2019 stały się ofiarami średnio 47 ataków dotyczących fałszerstwa e-mail.[9]

3X +

Mediana kwoty w dolarach skradzionej w ramach ataków związanych z wysyłaniem fałszywych biznesowych wiadomości e-mail (BEC) wyniosła 24 439 USD, czyli ponad trzy razy więcej niż mediana kwoty naruszenia danych.[10]

3 Raport Verizon. *„2019 Data Breach Investigations Report."* Lipiec 2019.
4 Proofpoint. *„Human Factor Report 2019."* Wrzesień 2019.
5 Raport Verizon. *„2019 Data Breach Investigations Report."* Lipiec 2019
6 Badanie Forrester. *„The Forrester Wave Enterprise Email Security, Q2 2019."* Maj 2019.
7 FBI. *„Business Email Compromise: the $26 billion scam."* Wrzesień 2019.
8 Raport Verizon. *„2019 Data Breach Investigations Report."* Lipiec 2019
9 Proofpoint. *„Proofpoint Quarterly Threat Report Q1 2019."* Maj 2019.
10 Raport Verizon. *„2019 Data Breach Investigations Report."* Lipiec 2019

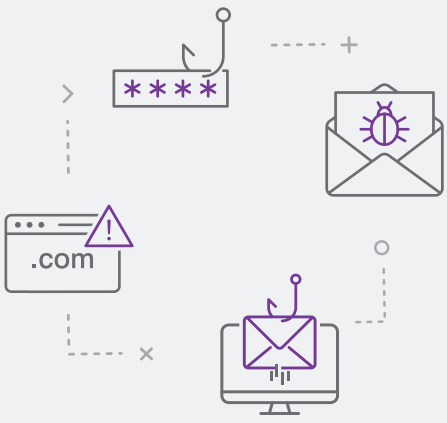
Ataki e-mailowe rozwijają się szybciej niż metody obrony

Zabezpieczenie e-maili odgrywa kluczową rolę w ochronie firmy. Ale jest to także trudne wyzwanie,

ponieważ zagrożenia e-mailowe są bardzo liczne i mają szeroką skalę. Techniki ataków nieustannie się zmieniają. Ludzka natura – słaby punkt w każdej organizacji – jest nieustannym celem ataków.

Nic dziwnego, że rozwiązania opracowane do zwalczania ataków sprzed zaledwie dwóch lub trzech lat mają trudności w nadążaniu za zmianami.

Narzędzia do ataków e-mailowych



Oto kilka sposobów, które stosują cyberprzestępcy do przeprowadzania ataków za pomocą e-maila.

Złośliwe oprogramowanie: złośliwy kod, który infekuje komputery i serwery. Może zostać dostarczone jako załącznik w postaci pliku, złośliwy link URL lub plik wtórnie pobrany przez złośliwe oprogramowanie, które już było zainstalowane na zainfekowanych systemach.

Phishing: złośliwe wiadomości e-mail mające na celu nakłonienie odbiorców do wykonania czynności pożądanej przez przestępcę. Może to obejmować podanie danych poświadczających do konta, wysłanie poufnych informacji lub nawet wykonanie przelewu (patrz „Oszustwo e-mailowe" poniżej).

Oszustwo e-mailowe: rodzaj phishingu mający na celu nakłonienie odbiorców do przelania pieniędzy lub wysłania poufnych informacji do przestępcy. Oszustwo e-mailowe zwykle nie jest związane ze złośliwym oprogramowaniem. Polega raczej na inżynierii społecznej mającej na celu nakłonienie ofiary do wykonania ataku w imieniu przestępcy. W takich atakach zwykle wykorzystywane są zwodniczo wyświetlane nazwy, spoofing domen lub domeny przypominające inne domeny, aby skłonić odbiorców do zaufania nadawcy.

Wewnętrzny phishing: phishing stosujący zainfekowane konto e-mail w celu atakowania użytkowników na tej samej domenie e-mail, zwykle innych pracowników firmy. Taki rodzaj phishingu jest skuteczny, ponieważ większość organizacji nie spodziewa się zagrożeń pochodzących z ich własnej domeny. Poza tym odbiorcy zakładają, że można zaufać wiadomości otrzymanej od innych pracowników.

Phishing oparty na osobistej poczcie internetowej: ataki wymierzone w użytkowników za pośrednictwem ich osobistych kont poczty internetowej. Wiele osób korzysta ze swojej osobistej poczty e-mail w trakcie pracy, narażając swojego pracodawcę na zagrożenia pochodzące z tego często nieoczekiwanego źródła.

Dlaczego potrzebujesz podejścia nastawionego na ludzi

Głównym celem cyberataków nie jest już infrastruktura lecz ludzie. Ta zmiana sprawiła, że stare podejście do bezpieczeństwa cyfrowego oparte na granicach sieci jest całkowicie przestarzałe – jeśli w ogóle kiedykolwiek działało.

A to dlatego, że nie ma już granicy, której trzeba bronić. Ludzie są mobilni, korzystają z danych firmowych z każdego miejsca i na wszystkich rodzajach urządzeń, sieci i platform poza tradycyjną siecią firmową.

Powszechne wdrożenie chmury tylko przyspieszyło rozwój tego trendu. Nawet jeśli Twoja infrastruktura w chmurze jest bezpieczna, ludzie, którzy z niej korzystają są tylko ludźmi.

Dlatego skuteczne bezpieczeństwo cybernetyczne koncentruje się najpierw na ludziach.

Model VAP (podatność, ataki, przywilej – „Vulnerability, Attack, Privilege")

Ludzie są wyjątkowi, podobnie jak wyjątkowa jest ich wartość dla cyberprzestępców i ryzyko dla pracodawców. Mają różne nawyki cyfrowe i słabe punkty. Są celem ataków cyberprzestępców na różne sposoby i z różnym stopniem intensywności. Mają także wyjątkowe kontakty profesjonalne i uprzywilejowany dostęp do danych w sieci i w chmurze.

Łącznie te wszystkie czynniki tworzą ogólne ryzyko użytkownika, które nazywamy indeksem VAP (pomiar podatności, ataków i przywilejów).

Podatność

Podatność użytkowników związana jest z ich cyfrowym zachowaniem – jak pracują i na co klikają. Mogą otwierać e-mail służbowy z niezarządzanych urządzeń osobistych. Mogą stosować nośniki danych oparte na chmurze i instalować zewnętrzne dodatki na aplikacjach w chmurze. Mogą być także szczególnie podatni na taktyki przestępców dotyczące phishingu e-mailowego.

Ataki

Współczesne cyberataki są bezlitosne, przybierają wiele różnych postaci i nieustannie się zmieniają. Ważne jest, aby zrozumieć, nie tylko kto w Twojej organizacji jest ofiarą ataku, ale w jaki sposób i kto tego dokonuje oraz czy atak jest częścią większej kampanii. Na przykład użytkownik, który jest celem kilku bardzo zaawansowanych zagrożeń może stanowić większe ryzyko niż ktoś, kto jest ofiarą szerokiej, masowej kampanii ataków.

Przywilej

Przywilej mierzy wszystkie potencjalnie wartościowe elementy, do których pracownicy mają dostęp, na przykład dane, uprawnienia finansowe, kluczowe stosunki i nie tylko. Pomiar tego aspektu ryzyka jest istotny, ponieważ odzwierciedla potencjalną korzyść dla przestępców – oraz szkody dla organizacji, jeśli bezpieczeństwo zostanie naruszone.

Pomiar, wykrywanie i zgłaszanie zagrożenia użytkowników

Pierwszym krokiem ochrony użytkowników jest ustalenie, którzy użytkownicy są najbardziej narażeni na ataki. Mimo że każda organizacja może inaczej mierzyć różne czynniki ryzyka, wszystkie sposoby pomiaru powinny uwzględniać podatność, ataki i przywileje.

Podatność to sposób określenia użytkowników, którzy są najbardziej podatni na atak. Analiza ataku może wykryć kto w Twojej organizacji jest celem ataku, jako poważna jest sytuacja i przez kogo wykonywany jest atak. Przywilej może pomóc określić, jak bardzo szkodliwy dla organizacji byłby skuteczny atak.

Użytkowników, którzy stanowią większe od przeciętnego ryzyko ustalone na podstawie dowolnego połączenia tych czynników, nazywamy VAP. Należy ich szybko rozpoznać, aby zespół ds. bezpieczeństwa mógł zastosować zebrane informacje i zgłosić je innym osobom w organizacji, jeśli to konieczne.

Ten poziom widoczności we wszystkich trzech obszarach jest ważny dla bezpieczeństwa nastawionego na ludzi. Bez niego organizacje nie mogą dowiedzieć się, kto potrzebuje dodatkowej warstwy bezpieczeństwa lub jak najlepiej chronić takie osoby.

Podatność: w jaki sposób użytkownicy pracują i na co klikają

Pomiar podatności nie jest łatwym zadaniem, jeśli stosuje się tradycyjne narzędzia bezpieczeństwa nastawione na technologię. Ale za pomocą podejścia nastawionego na ludzi możesz zmierzyć: jak użytkownicy pracują i na co klikają.

Ich sposób pracy obejmuje narzędzia, systemy i platformy, które wykorzystują do wykonania pracy. To, na co klikają jest odzwierciedleniem ich wiedzy o bezpieczeństwie oraz skłonności do nabrania się na taktyki ataków.

W jaki sposób pracują Twoi użytkownicy

Ocena podatności związana z tym, jak ludzie pracują zaczyna się od ustalenia, jakie stosują narzędzia, platformy i aplikacje. Obejmuje to następujące elementy:

- jakie aplikacje w chmurze stosują,
- ile i jakie urządzenia stosują do otwierania e-maili,
- informacje, czy te urządzenia są bezpieczne,
- informacje, czy użytkownik stosuje dobrą higienę cyfrową,
- informacje, czy użytkownik konsekwentnie stosuje uwierzytelnianie wieloskładnikowe.

Im bardziej szczegółowe są Twoje dane, tym lepiej.

Na co klikają Twoi użytkownicy

Drugą częścią pomiaru podatności jest rozpoznanie stopnia podatności użytkowników na phishing i inne cyberataki.

Szkolenie na temat bezpieczeństwa, istotna część każdej skutecznej strategii bezpieczeństwa, może pomóc w rozpoznaniu, którzy użytkownicy są w najmniejszym stopniu przygotowani na rozpoznanie i zgłaszanie zagrożeń cybernetycznych oraz na opieranie się im. Ogólnie, użytkownicy, którzy uzyskają słaby wynik w ćwiczeniach szkoleniowych lub nie ukończą tych ćwiczeń, są bardziej podatni na zagrożenia niż osoby, które osiągnęły wysokie wyniki.

Ale prawdziwy test odporności użytkowników polega na określeniu, jak radzą sobie z rzeczywistymi atakami.

Symulacje phishingowe będące rodzajem wpuszczenia przestępców do środka i sprawdzenia, kto otworzy złośliwy plik lub przeleje pieniądze przestępcy (oczywiście nie jest to idealne zachowanie) są najlepszym sposobem zmierzenia tego aspektu podatności.

Symulowane ataki, szczególnie te, które przypominają rzeczywiście stosowanie techniki, mogą pomóc w rozpoznaniu, kto jest podatny na zagrożenia i na jakie taktyki. Ktoś, kto otwiera symulowany e-mail phishingowy i otwiera załącznik może być najbardziej podatny. Użytkownik, który zignoruje takiego e-maila, ma nieco niższą ocenę, a użytkownik, który zgłosi e-mail zespołowi ds. bezpieczeństwa lub administratorowi e-maila zostanie uznany za najmniej podatnego.

Ataki: w jaki sposób użytkownicy są atakowani

Każdy cyberatak może być szkodliwy. Ale niektóre ataki są bardziej niebezpieczne, ukierunkowane lub zaawansowane niż inne. Dlatego pomiar tego aspektu ryzyka może być trudniejszy niż się to wydaje.

Niewybredne zagrożenia „produktowe” mogą być bardziej powszechne niż inne rodzaje zagrożeń. Ale można je dobrze rozpoznać i łatwiej zablokować.

Inne zagrożenia mogą pojawić się tylko w kilku atakach. Mogą jednak stanowić poważniejsze zagrożenie ze względu na ich stopień zaawansowania lub ludzi, w których są wymierzone.

Znajomość różnicy pomiędzy rodzajami ataków odgrywa istotną rolę w rozpoznaniu użytkowników, którzy są narażeni na duże ryzyko. Obszerna wiedza o zagrożeniach i terminowe uzyskiwanie danych są kluczowymi czynnikami w rozpoznaniu, kto i w jakim stopniu jest ofiarą ataku.

Do czynników, które należy szczególnie uwzględnić w ocenie każdego użytkownika należą:

- stopień zaawansowania cyberprzestępcy,
- skala i ukierunkowanie ataków,
- rodzaj ataku,
- ogólna liczba ataków.

Należy zawsze uwzględnić te czynniki w kontekście działów, grup lub oddziałów, do których należy dany użytkownik.

Na przykład, niektórzy użytkownicy mogą być uznawani za nienarażonych na ryzyko na podstawie liczby lub rodzaju złośliwych e-maili, które wysyłane są do nich bezpośrednio. W rzeczywistości jednak mogą stanowić większe ryzyko, ponieważ pracują w często atakowanych działach i dlatego istnieje większe prawdopodobieństwo, że w przyszłości staną się głównym celem ataku.

Przywilej: do czego użytkownicy mają dostęp

Pomiar przywilejów użytkowników rozpoczyna się od ustalenia wszystkich potencjalnie cennych elementów, do których mają dostęp: danych, uprawnień finansowych, kluczowych stosunków i nie tylko.

Użytkownicy posiadający na przykład dostęp do ważnych systemów lub zastrzeżonej własności intelektualnej mogą potrzebować dodatkowej ochrony, nawet jeśli nie są szczególnie podatni lub nie są jeszcze brani pod uwagę przez atakujących.

Pozycja użytkownika w strukturze organizacji również odgrywa rolę w ustalaniu przywilejów. Ale to nie jedyny czynnik – często nawet nie jest najważniejszy.

Asystent administratora może stanowić bardziej atrakcyjny cel ataku niż menedżer średniego poziomu, jeśli chodzi o szpiegowanie firm, ponieważ asystent ma dostęp do kalendarza dyrektora generalnego. Podobnie, pielęgniarka w szpitalu posiadająca dostęp do danych pacjenta może być bardziej przydatnym celem dla złodziei tożsamości niż dyrektor finansowy.

Dla przestępców wartościowym celem ataku będzie każda osoba, która posłuży jako środek do osiągnięcie ich celu.

NAJNOWSZE OSZUSTWA BEC I EAC

Oto popularne ofiary ostatnich ataków BEC i EAC.

Barbara Corcoran, gospodyni programu „Shark Tank”:

400 000 USD

Rząd Portoryko:

4 mln USD

Nikkei America:

29 mln USD

Red Kite Community Housing:

1,2 mln USD

Manor (Texas) Independent School District:

2,3 mln USD

Toyota Boshoku:

37 mln USD

Cabarrus County, N.C.:

2,5 mln USD

Ocala, Fla.:

750 000 USD

Rijksmuseum Twenthe (muzeum):

3,1 mln USD

Wiem, kim są moi VAP – co teraz? Bezpieczeństwo nastawione na ludzi w akcji

Rozpoznanie osób VAP ma istotne znaczenie, jeśli chodzi o bezpieczeństwo e-maili. Ale to tylko pierwszy krok. Dzięki podejściu nastawionemu na ludzi wszyscy mogą być chronieni, ponieważ sposób ochrony odpowiada poziomowi ryzyka, na które narażone są poszczególne osoby.

Podstawowa warstwa: bezpieczeństwo dla każdego

Bezpieczeństwo e-maili zaczyna się od solidnej ochrony dla każdego użytkownika Ponieważ ataki e-mailowe mogą mieć wiele różnych form, potrzebujesz obrony, która zatrzyma całą gamę zagrożeń e-mailowanych, a nie tylko niektóre z nich. Oto najważniejsze kroki, które trzeba wykonać, aby ochronić e-maile przed współczesnymi zagrożeniami:

Zatrzymaj załączniki ze złośliwym oprogramowaniem i złośliwe URL, zanim dotrą do skrzynek odbiorczych użytkowników.

Większość cyberataków polega na skłonieniu ofiary do wykonania konkretnego działania – w wielu przypadkach jest to np. otworzenie załącznika lub kliknięcie na link. Ale te uruchomione przez ludzi ataki nie będą skuteczne, jeśli ofiara, w którą wymierzony jest atak nigdy nie zobaczy wiadomości.

Dlatego właśnie potrzebna jest bezpieczna brama e-mail. Dzięki zatrzymywaniu zagrożeń dotyczących złośliwego oprogramowania zanim trafią do skrzynki odbiorczej użytkownika brama może chronić organizacje przed wieloma różnymi złośliwymi zagrożeniami, w tym przed ransomware, trojanami związanymi z bankowością online, trojanami ze zdalnym dostępem, złodziejami informacji, programami do ściągania plików, botnetami i nie tylko.

Zatrzymaj zagrożenia dotyczące oszustw, nie tylko te związane ze złośliwym oprogramowaniem

Zatrzymywanie zagrożeń dotyczących złośliwego oprogramowania jest bardzo ważne, ale niektóre najbardziej szkodliwe ataki e-mail w ogóle nie są oparte na złośliwym oprogramowaniu. Polegają raczej na inżynierii społecznej.

Do przykładów należy wysyłanie fałszywych biznesowych wiadomości e-mail (BEC), rodzaj fałszerstwa dotyczącego przelewu pieniężnego. Według FBI od 2016 roku działania typu BEC doprowadziły do ponad 26 mld USD potencjalnych strat. Organ ścigania twierdzi, że ataki BEC zgłoszono we wszystkich 50 stanach USA oraz w 177 krajach, a do fałszywych przelewów doszło w przynajmniej 140 krajach.[11]

W BEC i innych atakach niezwiązanych ze złośliwym oprogramowaniem oszust za pomocą sfałszowanego, zainfekowanego lub wyglądającego jak inne konta e-mail podaje się za kogoś, komu odbiorca może zaufać. Stosując fałszywą tożsamość, przestępcy proszą ofiarę, aby wykonała konkretne działanie w ich imieniu – na przykład przelała pieniądze do zagranicznego banku, wysłała poufne pliki itp.

Zagrożenia dotyczące oszustw są złożonym problemem o wielu obliczach. Aby je zatrzymać, potrzebna jest wielowarstwowa obrona, która zabezpieczy e-maile przychodzące, wychodzące i wewnętrzne oraz będzie działać w całościowy, spójny sposób.

Oprócz szkolenia użytkowników i innych środków kontroli opisanych w niniejszej sekcji warto uwzględnić poniższe kluczowe elementy obrony e-maila przed oszustami.

[11] FBI. *„Business Email Compromise: the $26 Billion Scam.”* Wrzesień 2019.

DMARC

Zastosuj uwierzytelnianie e-maili DMARC. DMARC to ogólna polityka internetowa, która potwierdza, że nadawca e-maila jest tym, za kogo się podaje, i że jest upoważniony do wysyłania wiadomości w imieniu organizacji.

Dzięki DMARC otrzymasz dane o wszystkich wiadomościach, które są wysyłane za pomocą Twojej domeny e-mailowej, w tym od zaufanych nadawców zewnętrznych, takich jak Marketo, Salesforce lub SurveyMonkey. Za pomocą tych danych możesz upoważnić wszystkich prawidłowych nadawców próbujących wysłać e-mail w Twoim imieniu oraz zablokować każdego, kto stosuje Twoją zaufaną domenę do kradzieży pieniędzy lub wyrządzenia szkód Twojej marce.

Dynamiczna klasyfikacja

Mimo że DMARC może pomóc w zatrzymaniu zagrożeń fałszujących Twoją domenę, przestępcy stosują inne techniki w celu oszukania użytkowników. Dlatego kolejnym ważnym elementem zatrzymywania zagrożeń niezwiązanych ze złośliwym oprogramowaniem jest dynamiczna analiza i klasyfikacja treści e-maili. Ten aspekt bezpieczeństwa e-maili polega na parsowaniu treści e-maila, a nie tylko jego źródła. Dlatego potrzebujesz narzędzia do zabezpieczania e-maili, które może wyszukać widoczne znaki oszustwa i zablokować lub w dalszym ciągu analizować wszystko, co wygląda niebezpiecznie. Dynamiczna klasyfikacja analizuje e-maile i zarządza e-mailami na podstawie kilku czynników, takich jak m. in.:

- treść e-maila, nagłówek i adres IP,
- reputacja nadawcy,
- relacja pomiędzy nadawcą a odbiorcą.

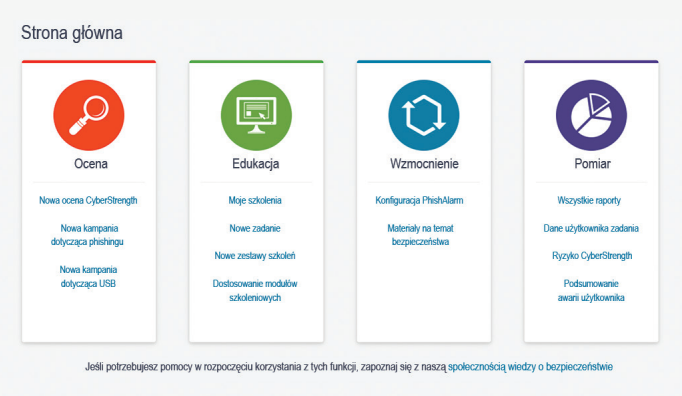
Wewnętrzna obrona e-maila

W niektórych przypadkach przestępcy w ogóle nie starają się ukryć swojego e-maila – przejmują po prostu prawidłowe konto. Strategia infekcji kont e-mailowych (EAC) może być stosowana w wielu różnych atakach, ale jest to szczególnie silna taktyka oszustów. A to dlatego, że:

- Większość organizacji nie poddaje e-maili wewnętrznych takiej samej analizie i środkom kontrolnym, jak w przypadku e-maila zewnętrznego.
- Większość użytkowników z natury ufa wiadomościom e-mail otrzymanym od osób, które zna.
- Przestępcy, którzy przejmują kontrolę nad kontem mają dostęp do źródła informacji o zainfekowanym użytkowniku – wiedzą, z kim koresponduje, o czym rozmawia, a nawet jaki ma styl pisania. Te szczegóły sprawiają, że sposób, w jaki przestępcy podszywają się pod inne osoby jest bardzo przekonujący.

Spraw, aby użytkownicy stali się bardziej odporni za pomocą szkolenia na temat bezpieczeństwa

Przestępcy stali się bezwzględnie skuteczni w wykorzystywaniu ludzkiej natury dzięki przekonującym technikom fałszowania, przykuwającym uwagę tematom i trudnym do powstrzymania wezwaniom do działania. Jak omawiamy w naszym raporcie **2019 Human Factor** na najskuteczniejsze e-maile phishingowe kliknięto 1,6 razy, co oznacza, że na niektóre e-maile kliknęli nie tylko odbiorcy, lecz również inne osoby, do których przekierowano wiadomość.[12]



Ochroń dane przed naruszeniem i zagrożeniami wewnętrznymi

Brak obrony e-mail może zatrzymać każde zagrożenie. Nawet wśród najlepiej wyszkolonych pracowników niektórzy użytkownicy mogą paść ofiarami ataków inżynierii społecznej.

Dlatego każda strategia obrony e-maila powinna obejmować narzędzia do zapobiegania utracie danych (DLP), w tym szyfrowanie. Nawet jeśli coś pójdzie nie tak, szybka odpowiedź i DLP zapewniają, że atak nie rozprzestrzeni się, a przestępcy nie zdobędą najbardziej poufnych danych.

DLP jest także przydatną obroną przed zagrożeniami wewnętrznymi. Nikt nie chce uznawać swoich współpracowników za potencjalnych wrogów bezpieczeństwa. Ale zagrożenia wewnętrzne – w tym pochodzące od pracowników, którzy są nieuważni, padli ofiarami przestępstwa lub zostali zainfekowani – spowodowały średnio 8,76 mln USD szkód w 2018 r.[13]

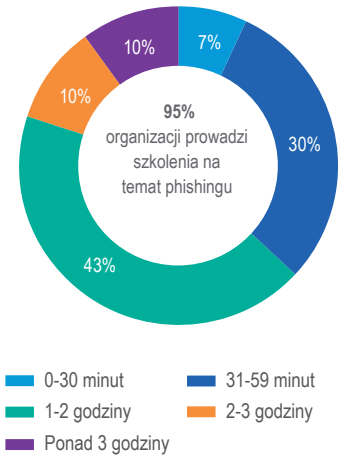
Niezależnie od tego, czy dane wydostają się z Twojego środowiska przez zewnętrzne naruszenie bezpieczeństwa lub atak wewnętrznych, DLP pomoże zachować ich bezpieczeństwo.

[12] Proofpoint. *„The Human Factor 2019."* Wrzesień 2019.
[13] Ponemon Institute. *„2018 Cost of Insider Threats: Global."* Kwiecień 2018.

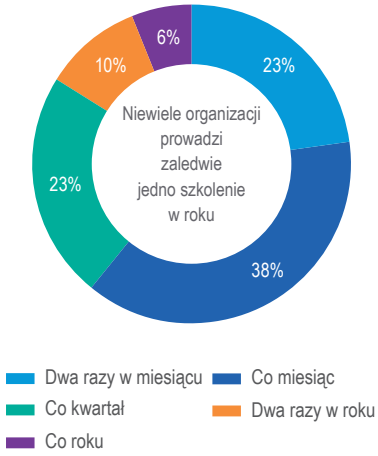
OSTRZEŻONE I UZBROJONE

Oto, w jaki sposób organizacje wdrażają programy szkoleniowe na temat bezpieczeństwa.

Czas przeznaczony na szkolenia na temat bezpieczeństwa każdego roku



Częstotliwość szkoleń na temat bezpieczeństwa



Warstwa regulowana: środki kontrolne dla VAP

Skuteczna strategia zabezpieczania e-maili ochrania wszystkich użytkowników. Ale ochrona nastawiona na ludzi rozpoznaje, że niektórzy użytkownicy, czyli Twoi VAP, potrzebują dodatkowej warstwy bezpieczeństwa i dodatkowych środków kontroli. Takie osoby VAP mogą być bardziej podatne na ataki, częściej mogą być celami ataków, mieć duże przywileje użytkowników związane z poufnymi danymi i systemami – lub mogą charakteryzować się dowolnym połączeniem tych trzech cech.

Ukierunkowane szkolenie na temat bezpieczeństwa

Szkolenie na temat bezpieczeństwa w całej firmie jest przydatne w celu odkrycia luk bezpieczeństwa i ograniczenia skali ataków wymierzonych w ludzi. Ukierunkowane szkolenie nie tylko ujawnia oczywiste luki, lecz może być także przydatnym środkiem zapobiegawczym dla wszystkich VAP, nie tylko dla tych, którzy mają wysoką podatność na zagrożenie.

Użytkownicy zidentyfikowani jako VAP na przykład ze względu na ich profil ataków mogą wziąć udział w szkoleniu na temat dokładnie tych zagrożeń, które są w nich wymierzone. Natomiast użytkownicy z wysokimi przywilejami mogą otrzymać dodatkowe szkolenie związane z kampaniami ataków wymierzonych w dane, do których mają dostęp.

Regulowane zabezpieczenie oparte na ryzyku

Stosowanie najsurowszych środków kontroli bezpieczeństwa dla wszystkich użytkowników przez cały czas nie jest praktycznym rozwiązaniem dla większości organizacji. Mogłoby to mieć nawet skutki odwrotne od zamierzonych. Zbyt surowe środki kontrolne mogą ograniczyć produktywność użytkowników i mogą powodować, że użytkownicy będą stosować obejścia zabezpieczeń, aby tylko wykonać swoją pracę.

Ale czasami ta dodatkowa warstwa bezpieczeństwa jest konieczna. Pracownik mający bezpośredni kontakt z obsługą klienta może być szczególnie narażony na atak, który krąży w Twojej branży. Osoba zajmująca się badaniami może być celem szczególnie wyrafinowanego ataku Lub dyrektor generalny ze względu na charakter swojej pracy może mieć dostęp do poufnych danych organizacji.

W niektórych przypadkach można zwiększyć wymagania uwierzytelniania. W innych przypadkach konieczne może być zastosowanie izolacji sieciowej dla wszelkich adresów URL, na które użytkownik klika w e-mailu.

Niezależnie od tego, jaką przyjmują postać, najważniejszym elementem regulowanych zabezpieczeń jest aktualny wgląd w czynniki ryzyka związane z VAP oraz stosowanie środków kontroli, które są proporcjonalne do tych rodzajów ryzyka.

Ochrona kont opartych na chmurze

Infekcja kont e-mailowych (EAC), szczególnie dla kont opartych na chmurze, szybko staje się preferowaną metodą ataków. Dla cyberprzestępcy zainfekowane konto jest praktycznie licencją na kradzież.

Zainfekowane konto e-mail może zostać użyte na wiele różnych złośliwych sposobów. Po zdobyciu kontroli nad odpowiednim kontem intruz może przemieszczać się do innych miejsc w firmie, kraść dane lub oszukiwać Twoich partnerów biznesowych i klientów. Dlatego ochrona kont pocztowych, szczególnie opartych na chmurze, odgrywa tak dużą rolę.

Sytuacja, w której dochodzi do infekcji: w jaki sposób przestępcy przejmują konta oparte na chmurze

Podczas infekcji kont e-mailowych konto e-mailowe nie tylko *wydaje się* być nieprawidłowe – to prawdziwy problem. Oto kilka przykładów, w jaki przestępcy mogą zdobyć kontrolę nad Twoim kontem użytkownika.

Ataki przy użyciu siły. Przestępca, zwykle za pomocą zautomatyzowanego skryptu, próbuje kombinacji nazwy użytkownika/hasła na wielu różnych kontach, aż jedno zadziała.

Ataki metodą powtórzenia naruszenia. Wiele osób stosuje to samo hasło dla wielu kont, co nie jest dobrą praktyką. Jeśli jedno z tych haseł zostanie ujawnione w niepowiązanym wycieku danych, wszystkie inne konta z tą samą nazwą użytkownika (często jest to adres e-mail) i z tym samym hasłem będą zagrożone.

Phishing. Staromodny phishing danych logowania pozostaje skutecznym sposobem pozyskania hasła ofiary. Bez dodatkowych środków kontroli, takich jak uwierzytelnianie wieloskładnikowe (MFA), utracone dane logowania mogą prowadzić do naruszenia bezpieczeństwa kont.

Reakcja: podejmowanie skutecznych działań, gdy dojdzie do ataku

Nie da się uniknąć incydentów dotyczących bezpieczeństwa. Ale nie muszą mieć katastrofalnych skutków.

Gdy atak stanie się skuteczny, prędkość, z jaką możesz powstrzymać i naprawić szkody może stanowić istotną różnicę pomiędzy krótkotrwałym incydentem a długotrwałym ograniczeniem. Dlatego energiczna struktura reakcji odgrywa kluczową rolę w każdej strategii bezpieczeństwa nastawionej na ludzi.

W wielu organizacjach reakcja na incydenty jest wolnym, pracochłonnym procesem obejmującym:

- badanie i weryfikowanie incydentu,
- ograniczenie zagrożenia,
- określenie przyczyny i zakresu,
- usuwanie zainfekowanych systemów.

Wszystkie te kroki są niezbędnymi składowymi skutecznej reakcji. Ale osoby zajmujące się bezpieczeństwem dobrze wiedzą, że ręczne wykonywanie tych procesów nie jest skalowalne. Pod tym względem przydatna może okazać się automatyzacja.

Skuteczne procesy reakcji automatyzują pracochłonne zadania, takie jak powiązanie i analizowanie powiadomień bezpieczeństwa, weryfikacja wskaźników infekcji (IOC) i gromadzenie danych kryminalistycznych. Automatyzacja może także pomóc w działaniach naprawczych, takich jak aktualizacja zapory sieciowej i list zablokowanych wiadomości e-mail przez wyciąganie złośliwych wiadomości e-mail ze skrzynek pocztowych i ograniczanie dostępu do konta zainfekowanych użytkowników.

W przypadku strategicznego zastosowania automatyzacja przyspiesza czas reakcji na incydenty i odciąża członków zespołu ds. bezpieczeństwa, aby mogli skupić się na działaniach, które są najlepiej wykonywane przez ludzi – zrozumienie, ustalanie priorytetów i reagowanie na prawdziwe zagrożenia.

Lista kontrolna: na co należy zwrócić uwagę w rozwiązaniu zapewniającym bezpieczeństwo

Branża cyberbezpieczeństwa powoli dochodzi do wniosku, że współczesne ataki wymierzone są w ludzi, a nie w technologię. Ale bezpieczeństwo nastawione na ludzi to więcej niż tylko hasło marketingowe. To całkowicie nowy sposób postrzegania zagrożeń i metod ich powstrzymywania.

Poniżej znajduje się lista kontrolna z kwestiami, o które warto zapytać w kontekście rozwiązań bezpieczeństwa nastawionych na ludzi.

Skuteczne bezpieczeństwo e-maili dla wszystkich użytkowników

Najlepszy sposób na zapobieganie atakom e-mail to zatrzymanie ich, zanim jeszcze dotrą do skrzynki odbiorczej. Szukaj rozwiązania, które może rozpoznać i zablokować szeroki zakres ataków i taktyk, w tym:

- ataki oparte na złośliwym oprogramowaniu, które wykorzystują załączniki i URL,
- ataki inne niż złośliwe oprogramowanie, np. BEC,
- EAC i narzędzia przejmujące konta w chmurze.

Ludzie odgrywają największą rolę w dzisiejszych atakach e-mailowych. Dlatego szkolenie na temat bezpieczeństwa powinno być kluczowym elementem Twojej strategii bezpieczeństwa e-maili. Upewnij się, że Twój program szkoleniowy charakteryzuje się następującymi cechami:

- szkolenie oparte na sprawdzonych metodach i rzeczywistych atakach,
- symulacje phishingowe oparte na rzeczywistych kampaniach, aby szkolić użytkowników na zagrożeniach, z którymi mogą najprawdopodobniej się spotkać,
- ukierunkowane dodatkowe szkolenie dla użytkowników, którzy mają poważne luki w zabezpieczeniach.

Aby zabezpieczyć dane, które zostały ukradzione, przypadkowo udostępnione lub w złośliwy sposób narażone na niebezpieczeństwo przez pracownika wewnętrznego, niezmiernie ważne jest szyfrowanie i inne środki DLP. Skuteczne DLP może:

- analizować szczegółowo treść e-maili i, jeśli to konieczne, zapobiegać wysłaniu części wychodzących wiadomości i podobnych treści,
- identyfikować i chronić wszystkie standardowe formy ograniczonej treści, takie jak PCI, HIPAA, FINRA i inne regulowane materiały,
- automatycznie zmieniać trasę e-maili, szyfrować lub odrzucać e-maile, które naruszają zasady bezpieczeństwa i inne zasady oraz powiadamiać odpowiednie osoby w Twojej organizacji,

Regulowane środki kontrolne dla VAP

Użytkownicy o wysokim ryzyku – na podstawie podatności, profilu ataku i przywileju – wymagają dodatkowych środków kontroli bezpieczeństwa. Rozwiązanie zapewniające bezpieczeństwo e-maili nastawione na ludzi pomaga rozpoznać takie osoby VAP i ochronić je za pomocą dodatkowych warstw zabezpieczeń. Postaraj się znaleźć rozwiązanie, które:

- dostarczy przydatne dane dotyczące Twoich VAP zebrane przez kompleksową, aktualną analizę zagrożeń oraz dokładny wgląd w profil ryzyka użytkowników,
- oferuje narzędzia do raportowania, które ułatwiają ujawnienie podatności, profilu ataków i przywilejów użytkowników oraz komunikowanie o nich, a także zapewniają porównania pomiędzy działami i innymi branżami,
- automatycznie reagują na zmieniające się profile ryzyka użytkowników za pomocą uwierzytelniania o podwyższonym poziomie, ograniczonych przywilejów, izolacji URL i nie tylko.

Szybka, skuteczna reakcja, gdy dojdzie do ataku

Automatyzowanie kluczowych części procesu reagowania na incydenty może pomóc w usprawnieniu krytycznych pracochłonnych zadań i odciążyć osoby odpowiedzialne za reakcje, aby były gotowe do zadań o wyższym poziomie trudności. Postaraj się znaleźć narzędzia do automatycznej reakcji, które:

- weryfikują zagrożenia, identyfikują zainfekowanych użytkowników i gromadzą dane kryminalistyczne oraz kontekst dotyczący tych użytkowników,
- uzupełniają powiadomienia o zagrożeniu danych o propozycje rozwiązań
- ograniczają i naprawiają zagrożenia oraz stosują ponowne uwierzytelnianie kont w środowisku, w chmurze i lokalnie.

Dowiedz się więcej

Aby dowiedzieć się więcej o tym, jak możesz zastosować podejście do bezpieczeństwa e-maili nastawione na ludzi, wejdź na **www.proofpoint.com/us/products/email-protection/email-security-and-protection**.

DOWIEDZ SIĘ WIĘCEJ

Więcej informacji znajduje się 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.

0301-001-01-01 03/20