# Ochrona poczty e-mail dla Office 365

## nie działa poprawnie?
## Oto sposób jak to naprawić.


Liczba naruszeń bezpieczeństwa danych ustawicznie się zwiększa.
Sieci i zasoby firmowe są stale zagrożone atakiem.
Malware nieustannie mutuje i namnaża się.
Ransomware staje się powoli przykrą codziennością.

**Co jest wspólnym mianownikiem tych trendów? Poczta elektroniczna**

VadeSecure
Predictive Email Defense

# Spis treści

# WPROWADZENIE

**93% włamań sieciowych wiąże się z atakiem typu phishing lub spear phishing.**

Zasadniczo, obszar zabezpieczeń większości organizacji, dbających o własne bezpieczeństwo pozostaje stosunkowo szczelny. Dostępu do sieci strzegą zapory, serwery są regularnie aktualizowane, a poszczególne urządzenia chronione przed wykorzystaniem przez niepowołane osoby. Niestety, poważną luką w tym systemie zabezpieczeń pozostaje poczta elektroniczna.

**E-mail pozostaje głównym źródłem problemów, które spędzają sen z powiek osobom odpowiedzialnym za cyberbezpieczeństwo.**

Co więcej, hakerzy wykorzystają pocztę e-mail aby dotrzeć do najsłabszego ogniwa bezpieczeństwa każdej organizacji: jej pracowników.

Jeżeli sądzisz, że Twoja firma jest chroniona przed atakami za pośrednictwem poczty ponieważ korzystacie z Office 365 z pakietami zabezpieczającymi skrzynki e-mail, takimi jak EOP, Proofpoint, McAfee bądź Barracuda, proponujemy byś raz jeszcze rozważył ten temat. Wszystkie z wymienionych powyżej narzędzi nie uchronią Twojej organizacji przed atakami typu zero-day czy spear phisingiem.

**Według badań przeprowadzonych w 2016 roku przez Vanson Bourn, 84% organizacji przyznało, że w 2015 roku padło ofiarą ataków typu spear phishing. Jednocześnie 71% z nich potwierdziło, że stosuje już pewne sposoby ochrony poczty elektronicznej.**

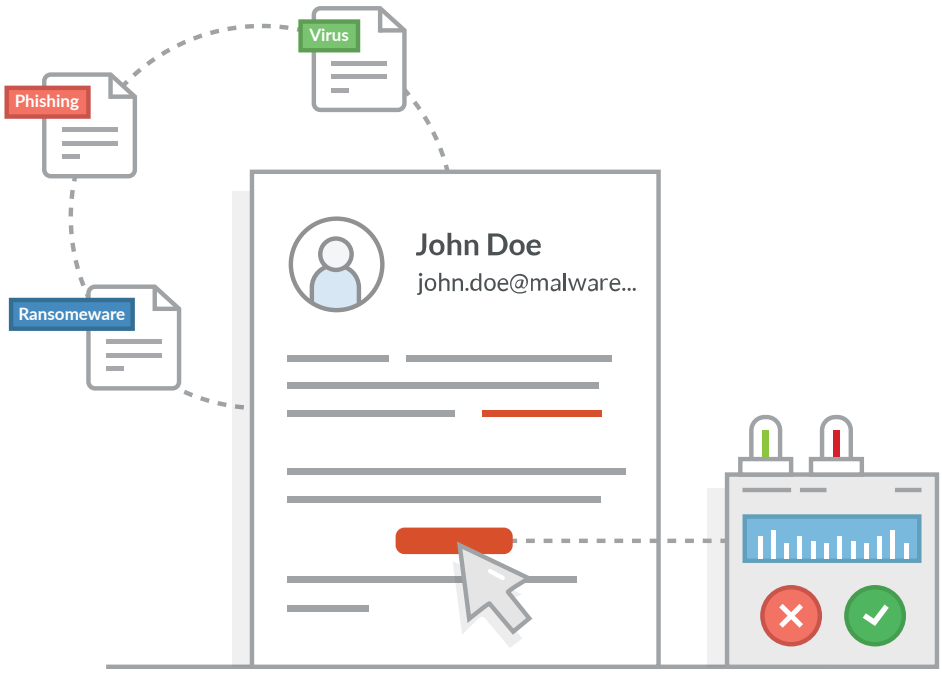
## Ochrona poczty email wymaga zmian.

Problem jest dwojaki:

1. **Technologia:** Większość „systemów bezpieczeństwa” poczty elektronicznej to nic innego niż górnolotnie reklamowane filtry antyspamowe. Zostały stworzone z myślą o zablokowaniu znanych ataków ze strony masowo wysyłanych wiadomości. Struktura takich filtrów nie pozwala na sprawne wykrywanie ataków zero-day bądź powstrzymywania prób phishingu.

2. **Ludzie:** Większość pracowników odpowiada na dobrze napisane maile phishingowe bądź klika w zamieszczone w nich odnośniki. Pomimo odbytych szkoleń bezpieczeństwa 20-30% odbiorców otwiera standardowe wiadomości phishingowe, zaś 12-20% klika znajdujące się w nich odnośniki. Te i tak już wysokie wyniki są niemalże dwukrotnie wyższe w przypadku ataków typu spear phishing.

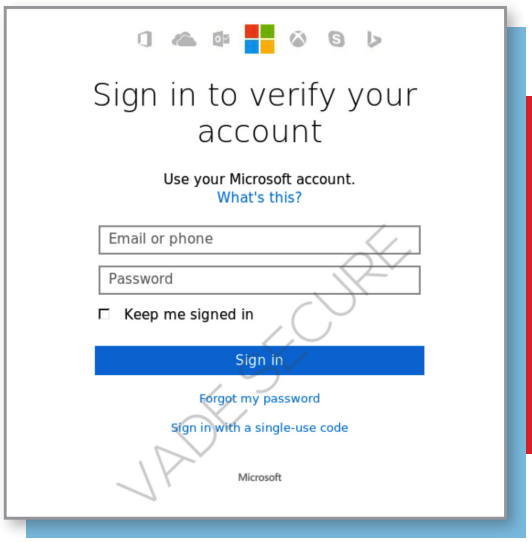
**W dalszej części tekstu opiszemy sedno tego problemu oraz objaśnimy jak sprawnie i szybko wyeliminować luki w systemie ochrony Office 365.**




1. Szacunki zostały zaczerpnięte z dokumentu Verizon's 2016 Data Breaches Report oraz z opublikowanego w sierpniu 2016 roku badania przeprowadzonego na Friedrich-Alexander University, które to wyniki dobrze pokrywają się z wynikami uzyskanymi przez inne, analogiczne, badania.

# PHISHING

Phishing to technika hakerska polegająca na wysyłaniu łudząco prawdziwych wiadomości do potencjalnych ofiar. Jej nazwa pochodzi od angielskiego słowa „fishing" (łowienie ryb), w którym pierwsza litera została zastąpiona literami „ph", jako odniesienie do prekursorów hakingu z lat 60 i 70tych - tzw. „phreakerów" (ang. „phone freaks" czyli „telefonicznych świrów"). Praktycznie każdy użytkownik internetu miał do czynienia z atakiem phishingowym. Ataki tego typu polegają na masowym wysyłaniu wiadomości pod fałszywym pretekstem, z prośbą o podanie haseł lub innych danych dostępu. Mogą też zawierać linki do szkodliwego oprogramowania lub samo oprogramowanie w postaci załącznika.




Zajęci pracownicy w pośpiechu nie dostrzegą, że ten ekran logowania jest próbą phishingu. W momencie gdy wpiszą swoje dane, o bezpieczeństwie sieci będzie można zapomnieć.

Wiele stron phishingowych wygląda identycznie jak prawdziwe strony, pod które się podszywają. Często jedyną różnicą jest niewielka i łatwa do przeoczenia zmiana w adresie. Po kliknięciu na link do takiej strony, odwiedzający ją użytkownicy mogą zostać łatwo przekonani do podania swoich danych hakerowi. Nawet strony znajdujące się na czarnych listach potrafią obejść takie zabezpieczenie korzystając ze strony pośredniczącej. W takiej sytuacji, odnośnik przenosi użytkownika do strony nieuwzględnionej przez filtry, której jedynym zadaniem jest przekierowanie na stronę służącą do przeprowadzenia ataku.

Programy typu malware, chociaż lepiej blokowane przez filtry, wciąż stanowią poważne zagrożenie. Odkryte niedawno programy zero-day malware mogą z łatwością ominąć zabezpieczenia, zwłaszcza, jeśli zostały ukryte w plikach takich jak dokumenty PDF lub Office. W ten właśnie sposób dokonano wielu najnowszych ataków typu ransomware.

## Pomimo braku konkretnego adresata, średnio aż 20% użytkowników otwiera każdy załączony w takim mailu plik lub link.[2]

Jak zobaczymy za chwilę, wszystkie te ataki mogą być znacznie groźniejsze, jeżeli zostaną dokładnie dopasowane do ofiary jako atak spear phishingowy.

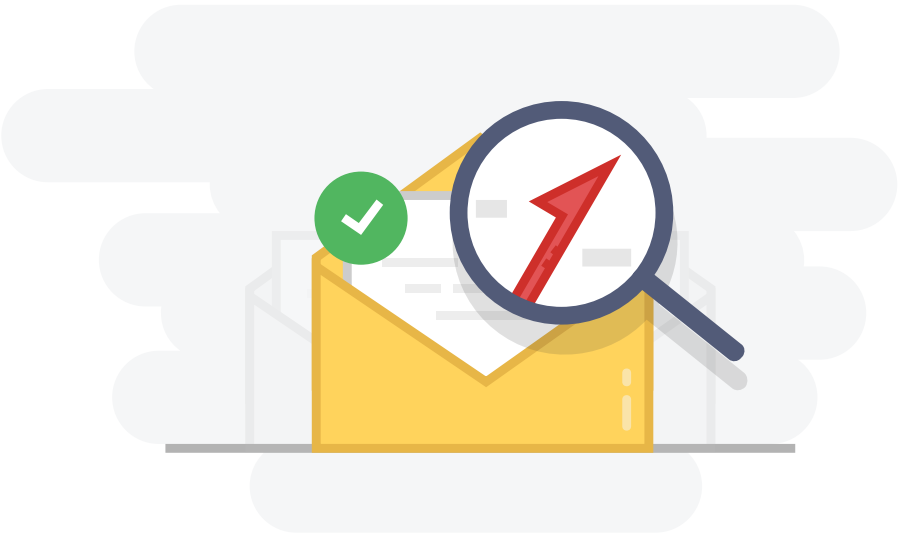
2. Ibid.

# SPEAR PHISHING

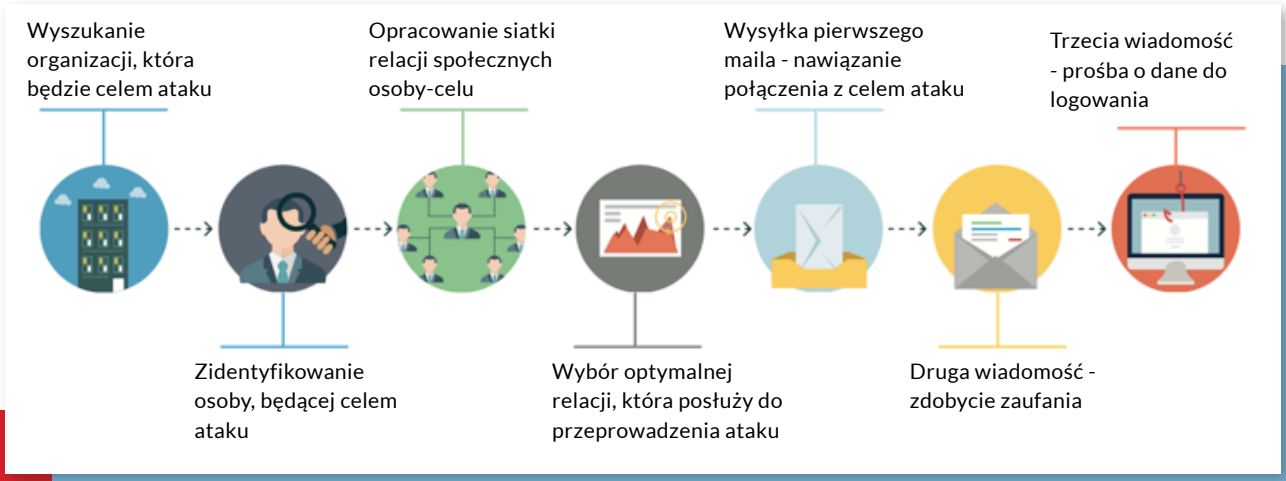
Spear phishing stanowi rozszerzoną wersję phishingu, wymierzoną w konkretnych pracowników. Celem jest zwykle uzyskanie nieuprawnionego dostępu do sieci, danych i aplikacji. W odróżnieniu od masowego charakteru phishingu, często polegającego na wysyłaniu setek tysięcy wiadomości do losowych odbiorców w ciągu kilku godzin, spear phishing jest podejściem znacznie bardziej metodycznym i wymierzonym w pojedynczego odbiorcę. Początkowy e-mail często nie zawiera żadnych odnośników ani załączników. Zwykle jest to wiadomość mająca skłonić odbiorcę do nawiązania kontaktu i przekonania go, że nadawca jest faktycznie osobą, za którą się podaje. Po zdobyciu zaufania ofiary, haker wysyła monit o podanie danych dostępowych bądź wiadomość z groźnym odnośnikiem lub załącznikiem.

**Dopasowanie treści maila spear phishingowego do konkretnego adresata, a także brak łatwych do zidentyfikowania, uwzględnionych w blacklistach adresów URL lub załączników zawierających malware, sprawiają, że wiadomości takie nie są zatrzymywane przez standardowe filtry.[3]**

Aby zademonstrować atak typu spear phishing, przyjrzyjmy się fikcyjnej firmie Bezpieczna Sp. z o.o., zatrudniającej 10 000 pracowników w pięciu placówkach w różnych miastach. Firma daje także zatrudnienie ponad 500 osobom na stanowiskach administracyjnych. Celem hakerów jest zdobycie dostępu do bazy danych firmy, zawierającej setki tysięcy danych pracowników. Wśród danych znajdują się wrażliwe dane osobiste, takie jak np. numery PESEL i numery kont bankowych, które mogą zostać odsprzedane złodziejom tożsamości.



2. Ibid.




Atak spear phishingowy rozpoczyna się od wyszukania organizacji oraz konkretnej osoby w jej strukturze, które mają być jego celem. Kolejnymi etapami są określenie siatki osób, z którymi kontaktuje się pracownik - cel ataku oraz wybór najbardziej optymalnej relacji, która posłuży jako płaszczyzna ataku. Wykorzystując konkretną relację, atakujący będzie podszywał się pod wybraną osobę, wysyłając kolejne maile z spreparowanego wcześniej konta, próbując zdobyć zaufanie swojego celu.

Powyższy rysunek ukazuje typowy atak spear phishingowy. Pierwszym krokiem hakera jest zdobycie informacji o firmie Bezpieczna Sp. z o.o. i opracowanie najskuteczniej metody ataku. Po sporządzeniu listy kierowników i członków zarządu figurujących w dziale „Nasz zespół" na firmowej stronie internetowej, atakujący przygotowują sieć znajomości wewnątrz firmy w oparciu o serwisy społecznościowe jak Facebook czy LinkedIn. Po zdobyciu informacji o tym, kto zna kogo w organizacji, hakerzy są gotowi do przeprowadzenia ataku.

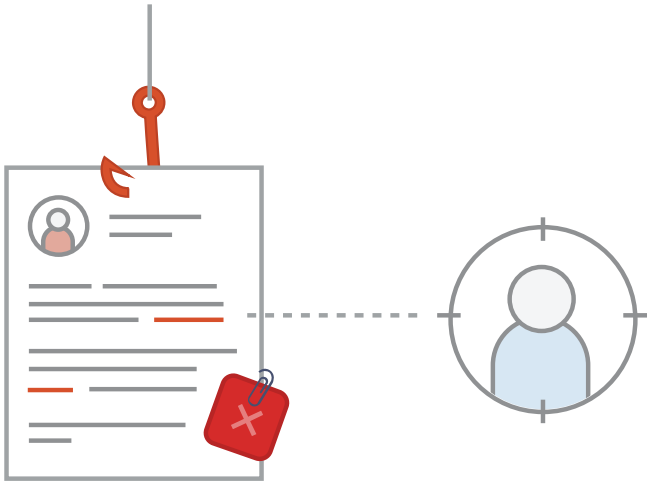
Aby zdobyć jego zaufanie, wysyłają do niego e-mail, w którym udając Kowalskiego, pytają o to, jak spędza urlop (uzyskawszy wcześniej tę informację za pośrednictwem zdjęć i postów z Facebooka). Nowak odpowiada na pytanie i pierwszy etap ataku kończy się powodzeniem. Haker skutecznie podszył się pod osobę zatrudnioną w Bezpieczna Sp. z o.o. i zaczyna zdobywać zaufanie wcielając się w autentycznego pracownika. Następnie Nowak opowiada mu jak przyjemnie spędza urlop w gronie rodzinny. Haker kontynuuje rozmowę o wakacjach, poruszając też wątki służbowe, w których wykorzystuje informacje zdobyte w trakcie pierwszego etapu rekonesansu (np. wspomina imiona i nazwiska autentycznych pracowników firmy).

Dlaczego oszust nie został wykryty? Czyżby Jan Kowalski nie posiadał firmowego adresu, po którym można by było ustalić nadawcę? Nic bardziej mylnego. Firma Bezpieczna Sp. z.o.o pozwala jednak pracownikom na używanie osobistych urządzeń mobilnych w ramach polityki Bring Your Own Device (BYOD) do wzajemnej komunikacji mailowej. W tym przypadku, haker, sprawdzając konto Kowalskiego na portalu LinkedIn wie, że używa on adresu jankowalski1@gmail.com. Tworzy zatem adres jankowalski.1@gmail.com. Nowak nie zauważa tej drobnej, acz istotnej różnicy, co pozwala na kontynuowanie ataku.

Z serwisu LinkedIn hakerzy wiedzą, że w zespole Nowaka od niedawna pracuje Janina Wiśniewska. Udający Jana Kowalskiego haker wysyła do Nowaka list z dokumentem w formacie PDF, opisanym jako „kwestionariusze danych osobowych nowego pracownika", w których ukryty jest malware, zapisujący wprowadzane dane. Jeżeli Michał Nowak otworzy załącznik, program potajemnie zainstaluje się na jego komputerze i prześle dane logowania hakerowi, który w ten sposób uzyska dostęp do firmowej sieci.

Podszywający się Jana Kowalskiego haker może również wysłać do Nowaka wiadomość typu „Cześć Michał, nie ma mnie w biurze, ale muszę pilnie zadzwonić do banku i upewnić się, czy składki ubezpieczeniowe Janiny zostały właściwie opłacone. Nie pamiętam danych logowania do nowej bazy danych pracowników. Możesz mi pomóc?" Jeżeli pan Kowalski wyśle żądane dane, haker może zalogować się do bazy danych jak każdy upoważniony pracownik. W jednym i drugim przypadku haker uzyskuje dane logowania, dające dostęp do wewnętrznej sieci firmy Bezpieczna Sp. z o.o. Mając taki dostęp, może uzyskać dane osobiste wszystkich pracowników.

Powyżej opisaliśmy przykład sytuacji, który wydarzył się w dziale kadr ale równie dobrze mógłby zaistnieć w dziale finansów, marketingu, IT bądź jakimkolwiek innym. Większość pracowników upublicznia w sieci wystarczająco dużo informacji o sobie, by umożliwić oszustom wykorzystanie tych danych do podszycia się pod nich i uzyskania wiadomości zastrzeżonych wyłącznie dla upoważnionych pracowników.



# SPEAR PHISING I JEGO WPŁYW NA BIZNES

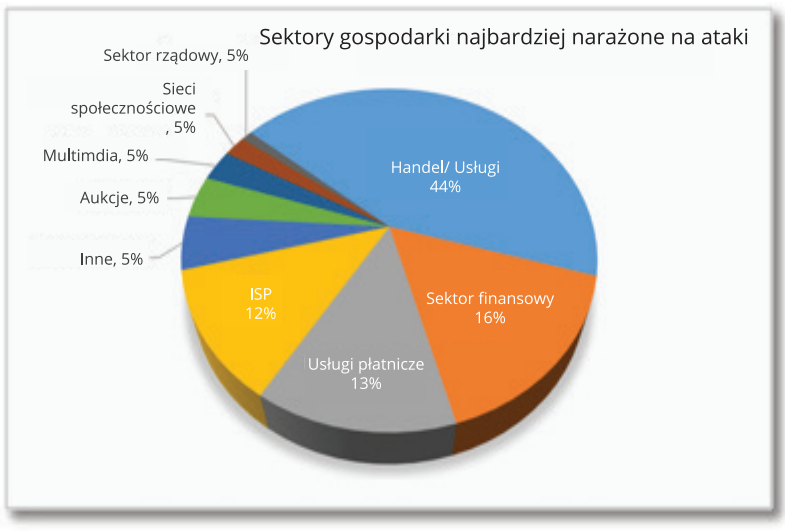
Jaki jest faktyczny wpływ takich incydentów na firmy? Ich skala może być różna, ale zwykle jest proporcjonalna do kompetencji atakującego i rozmiaru faktycznego celu. Zastanów się nad finansowymi konsekwencjami włamania do Twojej firmy. Co haker może zrobić z uzyskanymi danymi?

**Przykład: Sony Pictures**

Za przykład niech posłuży przypadek Sony Pictures z 2014 roku. Reputacja koncernu mocno ucierpiała, kiedy upublicznione zostały prywatne e-maile członków zarządu, w których niepochlebnie wyrażali się o znanych osobach. Studio straciło też kontrolę nad procesem wydawniczym filmów, które nie będąc jeszcze wydane, trafiły w ręce piratów, przez co legalne wydania musiały zostać skierowane na rynek jak najszybciej. Skutkiem były milionowe straty. Ucierpiała też renoma koncernu Sony, co zmniejszyło jej wartość w oczach inwestorów i ograniczyło możliwości biznesowe w Hollywood. Konkurencja otrzymała zaś wgląd w wewnętrzne działanie studia. Dodatkowo, koncern musiał wydać 8 milionów dolarów na odszkodowania dla pracowników, którzy musieli chronić swoją tożsamość przed kradzieżą zapoczątkowaną przez ten incydent.

Ataki typu spear phishing często stanowią pierwszy etap większej kampanii hakerskiej. Po uzyskaniu dostępu, hakerzy mogą, bowiem dokonać wielkich szkód wykradając dane klientów, własność intelektualną i prywatne listy, a nawet usuwając kluczowe dane bądź szyfrując je oprogramowaniem ransomware.

Firmy, które padły ofiarą takiego ataku, ryzykują dodatkową utratę reputacji, spadek wartości rynkowej i konkurencyjności, procesy sądowe oraz trudności ze spełnieniem norm bezpieczeństwa. Nie należy też zapominać, że dla osób wysoko postawionych w hierarchii takich organizacji wszystko to może oznaczać poważne problemy w karierze zawodowej.




Ataki w różnych branżach, II kwartał 2016.

(Źródło: APWG Global Phishing Raport z II kw. 2016)

4. Brandom, Russell, "Sony Pictures will pay up to $8 million to settle hack lawsuit with employees." The Verge, October 20, 2015.

## Ryzyko w różnych branżach

**Usługi finansowe:** Przedsiębiorstwa finansowe muszą ograniczać ryzyko ataku typu spear phishing mogącego doprowadzić do kradzieży informacji handlowych, danych osobistych, numerów kart kredytowych i rachunków bankowych itp. Skuteczne ataki mogą wiązać się ze stratami finansowymi, konsekwencjami prawnymi oraz odpowiedzialnością karną.

**Handel:** Jak pokazało kilka zakrojonych na szeroką skalę i przeprowadzonych niedawno ataków hakerskich, handlowcy są narażeni na ryzyko wycieku danych klientów, w tym danych o kartach kredytowych. To z kolei naraża ich na kary ze strony instytucji nadzoru oraz konieczność wypłacania odszkodowania klientom. Dodatkowym kosztem takich ataków jest utrata zaufania i spadek wartości marki, często budowanej wysokim kosztem przez długie lata. Handlowcy również mogą stać się ofiarami ataków spear phishingowych, w wyniku których wykradzione zostaną informacje o kartach kredytowych, wykorzystywanych następnie do przeprowadzenia transakcji finansowych. Prowadzone obecnie dochodzenia dowodzą istnienia dużych operacji polegających na kradzieży towarów ze sklepów e-commerce i wywożenia ich za granicę w ilościach hurtowych.

**Firmy wytwarzające własność intelektualną:** Ataki typu spear phishing są szczególnie groźne dla firm z branż np. farmaceutycznej lub technologicznej, w których informacje cyfrowe mają znaczną wartość inwestycyjną. Ataki tego rodzaju mogą sprawić, że własność intelektualna, której opracowanie kosztowało długie lata i miliony złotych może nagle znaleźć się w rękach konkurencji.

**Przemysł i obronność:** Strategiczne zakłady przemysłowe i przedsiębiorstwa z branży zbrojeniowej są bardzo cennym celem dla wywiadowców państwowych i prywatnych. Firmy zbrojeniowe są częstym obiektem ataku ze strony elektronicznego wywiadu obcych państw. Przedsiębiorstwa takie są w istocie stroną w niewypowiedzianej cyfrowej wojnie, która, choć niewidzialna i relatywnie nieznana, ma bardzo intensywny przebieg. Firmy biorące w niej udział starają się wyciszać przypadki skutecznych ataków, więc można założyć, że w tej branży łamanie zabezpieczeń zdarza się częściej niż sugerowałyby to oficjalne dane. Koszt działań obcych wywiadów jest trudny do oszacowania, ale poważne przypadki szpiegostwa mogą zagrażać bezpieczeństwu narodowemu i możliwościom zabezpieczenia przyszłych kontraktów z zakresu obronności.

**Ochrona zdrowia:** Organizacje, których funkcjonowanie określa legislacja, chroniąca prywatność danych i bezpieczeństwo informacji medycznych muszą trzymać się sztywnych i złożonych wytycznych zgodnych z obowiązującym prawem (compliance). Wycieki danych wiążą się w ich przypadku z poważnymi konsekwencjami finansowymi i prawnymi. Istotna jest również utrata reputacji związana z wyciekiem wrażliwych danych osobowych, przechowywanych przez służbę zdrowia. Kilku dużych ubezpieczycieli przekonało się niedawno, jak wysokie mogą być koszty związane z ochroną przed kradzieżą tożsamości dziesiątków milionów ubezpieczonych osób, których nazwiska, adresy i numery polis wyciekły na zewnątrz.

5. APWG Global Phishing Raport z II kw. 2016)

# DLACZEGO TAK WIELE ORGANIZACJI JEST WRAŻLIWYCH NA ZAGROŻENIA ZE STRONY POCZTY ELEKTRONICZNEJ?

Problem polega na tym, że standardowe systemy filtrowania wiadomości, stworzone dla Office 365, takie jak EOP, Proof point, McAfee i Barracuda NIE są w stanie przechwycić wiadomości będącej próbą ataku typu spear phishingowego.

Architektura tych systemów bezpieczeństwa (podobnie jak wielu innych systemów ochrony poczty e-mail) została stworzona z myślą o zwalczaniu spamu. Z tego powodu, ich działanie koncentruje się na wiadomościach wysyłanych masowo i polega na blokowaniu podejrzanych e-maili oraz tych z dołączonymi załącznikami, które zawierają malware lub adresy URL do stron phishingowych.

Systemy te, choć bardzo skuteczne w procesie filtrowania spamu, nie są dobrą metodą obrony przed atakami typu spear phishing. Dobrze skonstruowany mail tej kategorii, z racji nierozpoznawalnego, złośliwego kodu, ominie wszystkie standardowe filtry spamowe.

**Standardowa ochrona poczty e-mail skutecznie blokuje masowy spam ...**

Systemy bezpieczeństwa poczty, mające swoje korzenie w zabezpieczeniach antyspamowych, sprawdzają się w przypadku masowych kampanii phishingowych. Następuje to co prawda z opóźnieniem, dopiero gdy pierwsze kilkadziesiąt tysięcy maili z nowym typem phishingu zostanie rozesłanych i ewentualnie rozpoznanych przez niniejsze systemy jako zagrożenie i wpisane w ich reguły filtrujące. (Rzecz jasna, jest to mała pociecha dla firm, których pracownicy zdążyli już otrzymać jedną z wiadomości wysłanych na początku kampanii...)

**...lecz w żaden sposób nie zabezpiecza przed wyszukanymi atakami spear phishingowymi...**

Ochrona poczty e-mail oparta o model sygnatury jest całkowicie nieskuteczna w zetknięciu z współczesnymi zagrożeniami: wysublimowanymi i precyzyjnie zaadresowanymi atakami spear phishingowymi czy malware typu zero-day.

Współczesne organizacje zamiast kolejnego filtru antyspamowego, potrzebują więc dopasowanego do powyższych zagrożeń narzędzia, które zabezpieczą przed nimi skrzynki e-mailowe.

# DLACZEGO MICROSOFT EXCHANGE ONLINE PROTECTION (EOP) POZOSTAJE NIESKUTECZNE?

Wspomnieliśmy wcześniej, że EOP jest względnie skutecznym środkiem ochrony przed znanymi zagrożeniami. Z drugiej strony, można z całą pewnością stwierdzić, iż pozostaje całkowicie bezradny w kontekście nieznanych niebezpieczeństw, niezależnie czy mowa o kodzie zero-day ukrytym w pliku excel czy ataku spear phishingowym, mającym na celu pełną kompromitację poczty e-mail organizacji.

Oto czego nie zapewnia EOP z perspektywy bezpieczeństwa poczty e-mail:

- Brak możliwości rozpoznawania nowych i rozwijających się zagrożeń, których sygnatura nie jest jeszcze znana.
- Brak możliwości bezpiecznego analizowania wszystkich załączników, takich jak pliki .zip.
- Brak możliwości bezpiecznego analizowania odnośników URL w czasie rzeczywistym, pozwalającej na blokowanie ukrytych przekierowań.
- Brak sprawnego wykrywania spoofingu.
- Brak systemu powiadomień dla administratorów i użytkowników w przypadku wykrycia próby ataku phishingowego.

W mniejszym lub większym stopniu, praktycznie każdy system „bezpieczeństwa" poczty, taki jak McAfee, Barracuda czy Proofpoint oparty jest na technologii filtrowania spamu i ma podobną wadę, którą jest niemożność identyfikacji nieznanych zagrożeń, takich jak ataki spear phishingowe bądź nieznane, złośliwe oprogramowanie, ukryte w dołączonym do maila, niewzbudzającym podejrzliwości pliku.

Choć część z tych producentów twierdzi, że ich oprogramowanie zawiera podstawowe moduły analityczne, zdolne wykrywać bardziej zaawansowane zagrożenia poczty e-mail, w rzeczywistości są one w stanie wykrywać prymitywne próby oszustw, jak np. różniące się domeny w polach 'Od:' i 'Odpowiedz:'. Analizy tego typu należą do absolutnie podstawowych i mogą być z łatwością ominięte przez niezbyt zaawansowanych hakerów.

6. EOP nie uwzględnia również niektórych przydatnych narzędzi, takich jak klasyfikacja graymail (poczty o niskim priorytecie) czy anulowanie subskrypcji jednym kliknięciem

# Zestawienie producentów

| | Proofpoint Essential | McAfee | Vade Secure | Barracuda | EOP |
|---|---|---|---|---|---|
| **Znane zagrożenia** | | | | | |
| **Podstawowa ochrona oparta o sygnaturę znanych zagrożeń** | √ | √ | √ | √ | √ |
| Spam ujęty na blackliście | √ | √ | √ | √ | √ |
| Malware ujęty na blackliście | √ | √ | √ | √ | √ |
| Phishing ujęty na blackliście | √ | √ | √ | √ | √ |
| **Nieznane zagrożenia** | | | | | |
| **Wykrywanie Zero-Day Malware/Phishingu/Spamu** | | | | | |
| Heurystyka i machine learning w zakresie podstawowym | √ | | √ | | |
| Complex Reputational Analysis | √ | | √ | | |
| Zaawansowana analiza za pomocą sztucznej inteligencji | | | √ | | |
| **Antyphishing i ochrona** | | | | | |
| Eksploracja URL w czasie rzeczywistym | | | √ | | |
| Ochrona przed przekierowaniem URL | √ | | √ | √ | |
| Kwerenda poufnych danych | | | √ | | |
| Dokładne wykrycia spoofingu | √ | | √ | | |
| Wykrywanie niejednakowych adresów nadawcy | | | √ | | |
| Uwierzytelnianie DKIM nadawcy | √ | √ | √ | √ | √ |
| Uwierzytelnianie SPF nadawcy | √ | √ | √ | √ | √ |
| **Komfort użytkowania** | | | | | |
| Klasyfikacja niskopriorytetowych maili | √ | | √ | | |
| Anulowanie subskrypcji jednym kliknięciem | √ | | √ | | |
| Zaawansowane anulowanie subskrypcji | | | √ | | |
| Archiwizacja | √ | √ | | √ | |
| Retencja SMTP | √ | √ | √ | √ | √ |
| **Wdrożenie** | | | | | |
| Cloud / SaaS | √ | √ | √ | √ | √ |
| On premise | √ | √ | √ | √ | |
| Instalacja w 30 min. | | | √ | | |
| Kompatybilność Exchange | √ | √ | √ | √ | √ |
| Kompatybilność z Office 365 | √ | √ | √ | √ | √ |
| Kompatybilność z Google Apps | √ | √ | √ | √ | |
| Zimbra (Zimlet) | | | √ | | |
| cPanel Plugin | | | √ | | |

# COŚ WIĘCEJ NIŻ OCHRONA NA PODSTAWIE SYGNATURY

Kilka lat temu Vade Secure uznało, że standardowe systemy filtrujące wiadomości, które opierają się na modelu rozpoznania sygnatury przypominają niekończącą się grę w kotka i myszkę. Ich miejsce powinny zająć elastyczne metody zabezpieczeń, mogące rozpoznać nowe zagrożenia w oparciu o cechy wcześniejszych wzorców. W skrócie, konieczne stało się opracowanie sztucznej inteligencji wyszkolonej do wykrywania najnowszych zagrożeń, określanych jako zero-day threats.

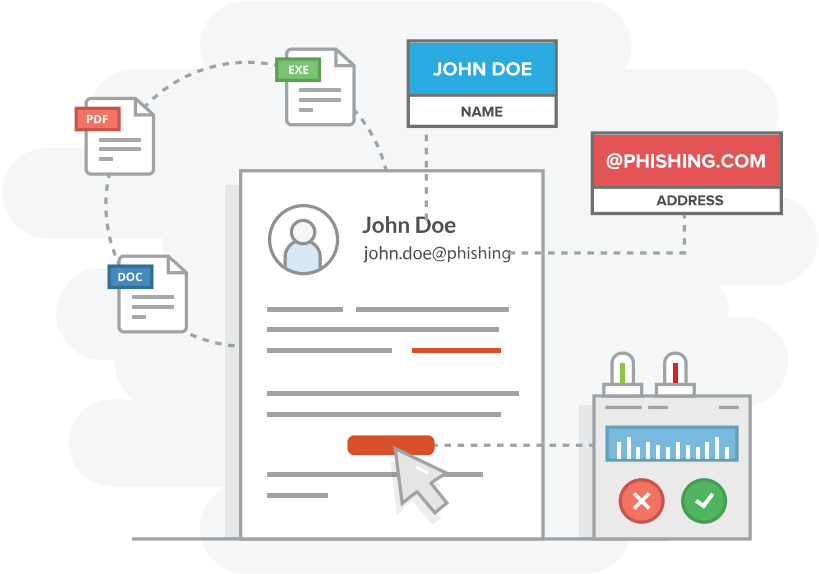
Każdego dnia Vade Secure przetwarza miliardy wiadomości e-mail. Posiadamy znaczącą przewagę rynkową w Europie (np. 90% wiadomości e-mail we Francji jest filtrowane przez nasze filtry) i coraz bardziej zaznaczamy swoją obecność w Ameryce Północnej oraz innych krajach na świecie.

Dzięki temu, mamy dostęp do bardzo szerokiego zbioru danych, na podstawie którego nasz model sztucznej inteligencji może uczyć się rozpoznawania i analizowania szkodliwych wiadomości, stron phishingowych i różnych wariacji malware. Aktualnie nasz system może skutecznie rozpoznawać ukierunkowane ataki typu spear phishing, kwerendy danych wrażliwych i programy typu zero-day malware ukryte w plikach executable oraz dokumentach PDF, Office i wielu innych.

Z każdym dniem system machine learning Vade Secure staje się bardziej efektywny i złożony. Nowe reguły działania oraz informacje dotyczące pojawiających się zagrożeń są stale gromadzone w aktualizowanych gatewayach i transferowane globalnie przez działające nieprzerwanie 24/7 centra oceny zagrożeń Vade Secure.

## Sztuczna inteligencja oraz tradycyjne filtry

System SI Vade Secure wspierany jest przez dodatkowe zabezpieczenia, takie jak tradycyjne filtry antyspamowe, działające w oparciu o sygnatury oraz zaawansowaną blacklistę (określoną przez jednego z naszych największych klientów mianem „jak dotąd najlepszej").



## Rozwiązanie Vade Secure

Pełna ochrona poczty elektronicznej Vade Secure to filtrowanie spamu, klasyfikacja wiadomości graymail i najbardziej niezawodne rozwiązanie zabezpieczające e-mail dostępne na rynku.

**Filtrowanie wstępne:** wiadomości oraz załączone do nich pliki są analizowane pod kątem znanych sygnatur phishing i malware. Pozwala to szybko zablokować napływ spamu i masowe ataki.

**Ochrona przed malware:**

- nasz program sprawdza kod zawarty we wszystkich plikach, także w dokumentach PDF, Office i innych.

**Bezpieczna analiza adresów URL:** wszystkie adresy URL są sprawdzane, aby wykryć te, które prowadzą bezpośrednio do złośliwego oprogramowania, stron phishingowych bądź innych niebezpiecznych witryn. W odróżnieniu od większości podobnych narzędzi, Vade Secure sprawdza adres, do którego kieruje odnośnik URL w chwili, gdy wiadomość trafia do systemu oraz ponownie, kiedy użytkownik uruchomi go przez kliknięcie.

**Sztuczna inteligencja:** wszystkie pozostałe informacje są analizowane pod kątem nieznanego malware i nowych strategii phishingowych oraz ataków typu zero-day, które mogłyby ominąć filtry. Reguły bezpieczeństwa, na których oparte jest nasze oprogramowanie, są aktualizowane i rozwijane na podstawie miliardów wiadomości analizowanych codziennie.

- **Weryfikacja tożsamości:** nasz system Identity MatchTM korzysta z wielu subtelnych technicznych i behawioralnych kryteriów, aby ustalić, czy nadawca wiadomości jest faktycznie osobą, za którą się podaje.
- **Weryfikacja domeny:** domena nadawcy jest dodatkowo sprawdzana w celu potwierdzenia jej autentyczności.
- **Analiza treści:** Vade Secure dokonuje kompleksowej analizy każdej wiadomości e-mail, szukając prób kradzieży informacji osobowych. Sztuczna inteligencja ostrzega użytkownika, jeżeli w mailu znajduje się prośba o podanie danych osobowych bądź danych dostępu.

**Dane wywiadowcze:** Vade Secure to działające 24/7 centrum rozpoznawania zagrożeń, w którym zatrudnieni są specjaliści z dziedziny bezpieczeństwa poczty elektronicznej. Ich zadaniem jest ciągła analiza nadchodzących wiadomości, pozwalająca na wykrywanie nowych, ciekawych z perspektywy badawczej zagrożeń.

**Kontrolowanie spamu:** Vade Secure przechwytuje 99,99% spamu, czyli zapewnia niemalże zerową możliwość przepuszczenia fałszywej wiadomości (<0,00001%).

**Zarządzanie reklamami/wiadomościami graymail:** Zapewnij swoim klientom możliwość kategoryzacji wiadomości reklamowych i automatycznego anulowania subskrypcji za pomocą jednego kliknięcia.

## Opcje wdrożenia:

Wdrożenie Vade Secure jest proste. Program może zostać dodany do istniejącego pakietu Office 365 w czasie krótszym niż 10 minut, jako system działający równolegle do istniejących rozwiązań typu EOP lub Barracuda, bądź je zastępujący.

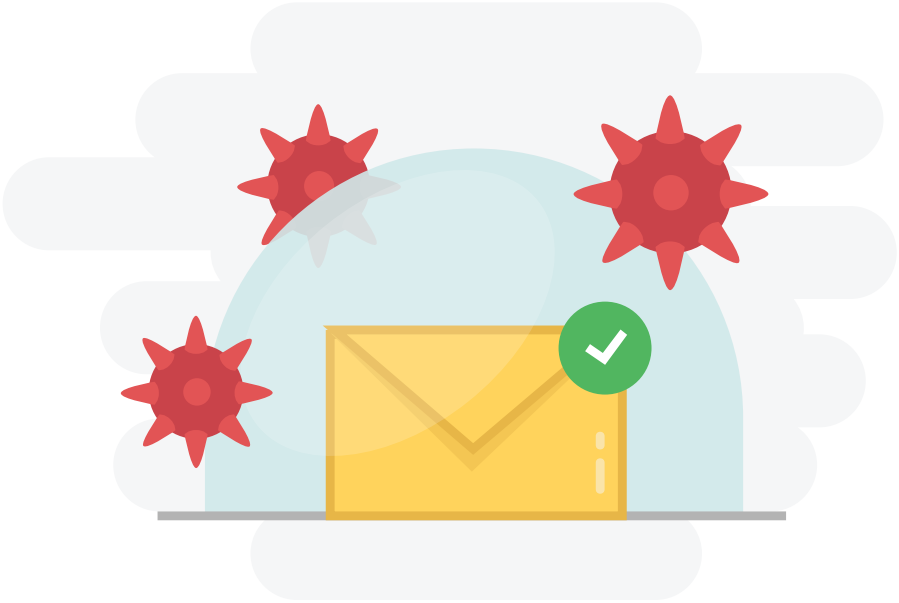
Zatrzymywanie spamu, filtrowanie wstępne i wykrywanie malware są w pełni dostępne od chwili zakończenia instalacji. System nie musi uczyć się rozpoznawania tych zagrożeń. Wykrywanie ataków typu spear phishing początkowo ma skuteczność na poziomie 90%, optymalną sprawność uzyskując po ok. 2 tygodniach od instalacji, kiedy system dostosuje się o zwyczajów i stylów korespondencji stosowanych w danej firmie.

Dostępne są również dodatkowe wtyczki dla korporacyjnych usług Gmail i Zimbra. Vade Secure dostępny jest jako usługa w chmurze bądź jako gateway ulokowany na maszynie wirtualnej

# PODSUMOWANIE

Ochrona przed phishingiem, a zwłaszcza przed spear phishingiem jest ciągłym procesem. Każdego dnia w skrzynkach odbiorczych pracowników firm na całym świecie pojawiają się nowe wersje tego zagrożenia. Środki przeciwdziałania muszą być wydajne, a jednocześnie elastyczne. Sztuczna inteligencja oraz specjalistyczna ochrona poczty odgrywają krytyczną rolę w zapewnieniu cyberbezpieczeństwa organizacji.

Nawet jedna wiadomość, która przedrze się przez system zabezpieczeń skrzynki mailowej może doprowadzić do ogromnych strat



# O Vade Secure

Vade Secure jest światowym liderem w dziedzinie oprogramowania antyphishingowego, oferującym zestaw narzędzi do ochrony przed phishingiem, malware i spamem. Firma zabezpiecza obecnie setki milionów skrzynek pocztowych na całym świecie. Szeroki zakres działania Vade Secure umożliwia uzyskanie wyjątkowo dokładnych informacji o naturze szkodliwych wiadomości e-mail. Zdobyta w ten sposób wiedza pozwala firmie dostarczać zaawansowanych rozwiązań do ochrony poczty elektronicznej, skutecznie zabezpieczając ją przed wszelkimi zagrożeniami czy atakami zero-day. Vade Secure jest również liderem w dziedzinie filtrowania spamu, dostarczając narzędzia ułatwiające zarządzanie wiadomościami graymail, co przekłada się na zwiększenie produktywności. Rozwiązania oferowane przez Vade Secure są dopasowywane do potrzeb rynku ISP, OEM, firm z branży hostingowej oraz enterprise.

**Więcej informacji o rozwiązaniu Vade Secure można znaleźć na oficjalnej stronie www.vadesecure.com**

**Dystrybutor na terenie Polski: Ectacom Sp z o.o., ul. Dominikańska 21B, 02-738 Warszawa, +48 501 295 580, kontakt@ectacom.pl, www.ectacom.pl**