

RAPORT **BEZPIECZEŃSTWA** **E-MAIL** **2021**

Kompleksowa analiza zabezpieczeń e-mail najpopularniejszych w Polsce stron WWW z branży e-Commerce, fintech, portali rezerwacyjnych i firm kurierskich.

SŁOWO DO CZYTELNIKÓW

Szanowni Państwo,

od lat e-maile angażują użytkowników i współtworzą wizerunek firm. Skuteczna komunikacja e-mail decyduje o sukcesie każdego e-biznesu. Odpowiada ona bowiem za sprawną komunikację z klientami, za dostarczanie im spersonalizowanych ofert produktowych czy potwierdzeń zrealizowanych transakcji.

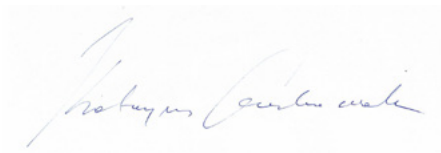
Na przestrzeni ostatnich lat trendy dotyczące komunikacji e-mail zmieniały się. Kluczowym zagadnieniem, któremu ostatnimi czasy globalne firmy poświęcają najwięcej uwagi, jest bezpieczeństwo poczty. Ważna jest ciągła aktualizacja wiedzy oraz ustawiczne dzielenie się doświadczeniami w tym obszarze. Bez względu na wielkość, każda firma powinna wiedzieć, jak bezpiecznie, a co za tym idzie skutecznie, posługiwać się komunikacją e-mail – zarówno tą marketingową, jak i transakcyjną.

Dlatego też składamy na Wasze ręce kompendium wiedzy o zabezpieczeniach komunikacji e-mail połączone z wynikami analizy tego obszaru wśród najpopularniejszych firm w Polsce.

Życzę interesującej lektury,

Katarzyna Garbaciak

Managing Director w EmailLabs



SPIS TREŚCI:

Wstęp: Bezpieczeństwo - najważniejszy trend w komunikacji e-mail na 2021 r.

I Zagrożenia związane z masową wysyłką e-maili marketingowych i transakcyjnych

- 1.1 Które branże są najbardziej narażone na ataki hakerskie?
- 1.2. Rodzaje ataków hakerskich oraz prawdopodobieństwo ich wystąpienia
 - Rodzaje ataków e-mailowych
- 1.3. Najważniejsze ataki cyberprzestępców w 2019 roku

II Nie bądź dinozaurem, poznaj najważniejsze zabezpieczenia – czyli rzecz o SPF, DKIM i DMARC

- 2.1 Dlaczego to takie ważne?
- 2.2. Dostępne zabezpieczenia
 - SPF
 - DKIM
 - DMARC
 - S/MIME

III Wspieranie zabezpieczeń przez polskich i zagranicznych providerów pocztowych

- 3.1 Które zabezpieczenia wspierają najpopularniejsi polscy providerzy pocztowi?
- 3.2. Które zabezpieczenia wspierają najpopularniejsi zagraniczni providerzy pocztowi?

IV Analiza zabezpieczeń komunikacji e-mail top serwisów WWW w Polsce wg kategorii

- 4.1 Jak należy analizować dane?
- 4.2. Wyniki badań:
 - E-commerce
 - Sektor fintech
 - Systemy rezerwacyjne
 - Firmy kurierskie
- 4.3. Ujęcie globalne: wyniki dla najpopularniejszych serwisów WWW w Polsce
- 4.4. Podsumowanie

V Co Twoja firma może zrobić już teraz?

VI Dodatek dla programistów

VII O EmailLabs

BEZPIECZEŃSTWO –

NAJWAŻNIEJSZY TREND W KOMUNIKACJI E-MAIL NA 2021 R.

E-mail jest – i wszystko na to wskazuje, że w przyszłych latach będzie niezmiennie, najpopularniejszym kanałem komunikacji marek z użytkownikami.

Każdego roku rośnie liczba zakładanych skrzynek e-mailowych, w rekordowym tempie wzrasta więc liczba wysyłanych e-maili. W 2020 roku każdego dnia wysyłano ponad 306 miliardów wiadomości e-mail¹, tj. o 13 mld więcej niż w 2019 roku². Podobną tendencję wzrostową notowaliśmy, porównując lata 2018 i 2019. Tak duża skala wysyłanych wiadomości e-mail sprawiła, że ten kanał komunikacji stał się również jednym z najbardziej podatnych na działania cyberprzestępców. Tylko w 2020 roku system Kaspersky Lab udaremnił ponad 727 milionów prób ataków internetowych³, m.in. z wykorzystaniem kanału e-mailowego – to 1,5 raza więcej niż w 2019 roku.

Choć metody cyberprzestępców ewoluują, straty z tytułu ataków były, są i będą stałym

elementem obecności w Internecie. Większość osób odpowiedzialnych za bezpieczeństwo uważa, że jeżeli użytkownik kliknął w załącznik i zainfekował swój komputer, ponosi on bezpośrednią odpowiedzialność za swoje działanie. W końcu przecież „mógł nie klikać”. Niestety wciąż niewiele firm buduje swoje strategie bezpieczeństwa wokół założenia: „Zastanówmy się, co zrobić, by użytkownikowi nie stała się krzywda, nawet jeśli kliknie”. Takie zaklinanie rzeczywistości nie prowadzi do dobrych efektów, podobnie jak apele, na przykład banków: „Nie odpowiadajcie na żadne prośby o loginy i hasła, żaden bank nigdy nie wyśle Wam takiej prośby”.

Tymczasem wielu ekspertów zajmujących się cyberbezpieczeństwem twierdzi, że banki nie stosują pełnych zabezpieczeń, narażając tym samym swoich klientów

...to na firmach wysyłających e-maile spoczywa odpowiedzialność za zabezpieczenie tych, którzy nie potrafią sami o swoje bezpieczeństwo zadbać.



¹ <https://www.dotpay.pl/blog/praktyczny-poradnik-ecommerce/wykorzystanie-e-mail-marketingu-do-promocji-e-sklepu-co-warto-wiedziec>

² Daily number of e-mails worldwide 2024 | Statista.

³ Dane Kaspersky Lab <https://www.facebook.com/watch/?v=612351026135077>, <https://www.facebook.com/watch/?v=3230063277120225>

na działania oszustów podszywających się pod „e-mail z banku”. Powód? Bardzo przyziemny – brak wytypowania tego typu zadań jako priorytetowe lub zwyczajnie... ignorowanie sprawy, zgodnie ze stwierdzeniem: „Przecież w 100% zabezpieczyć się nie można, więc czemu to ma służyć?”. Jednak myślenie zero-jedynkowe nie pomaga. Pomiędzy bielą i czernią jest jeszcze

sporo odcieni szarości. Warto więc zacząć od wykonania pierwszego kroku, tym bardziej, że globalni dostawcy infrastruktury wysyłkowej, jak i providerzy pocztowi – globalni i lokalni – mówią jednym głosem: bezpieczeństwo poczty będzie nie tyle trendem, ile wymogiem dla wysyłek e-mailowych w ciągu najbliższych kilku lat.

O RAPORCIE



W Polsce bezpieczeństwo komunikacji pozostaje tematem zapomnianym. Zapobieganie ewentualnym problemom niestety przegrywa z „gaszeniem pożarów”. Tymczasem wdrożenie zabezpieczeń ma realny wpływ na dobrą dostarczalność e-mailową. Na szczęście świadomość w zakresie bezpieczeństwa komunikacji e-mail ewoluuje w dobrą stronę i – jak zapowiadają providerzy pocztowi wraz z globalnymi dostawcami infrastruktury do wysyłki e-mail – najbliższe lata przyniosą pozytywne zmiany w tym zakresie. Już teraz zapraszamy do zapoznania się z informacjami, w jaki sposób sklepy e-Commerce, systemy rezerwacyjne, fintechy oraz firmy kurierskie w Polsce

zabezpieczają się przed podszywaniem się pod ich domeny wysyłkowe. A także – co jeszcze mogą zrobić, aby wpisywać się w najnowsze trendy związane z bezpieczeństwem komunikacji.

AUTORZY:
zespół



ROZDZIAŁ I

ZAGROŻENIA

związane z masową wysyłką e-maili marketingowych
i transakcyjnych



KTÓRE BRANŻE SĄ NAJBARDZIEJ NARAŻONE NA ATAKI HAKERSKIE?

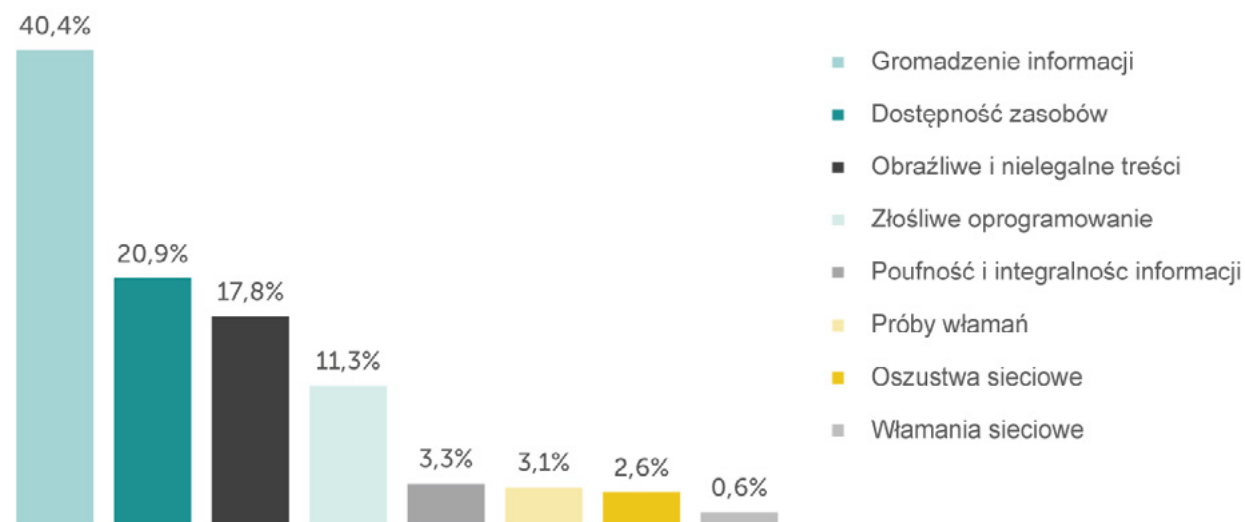
Myślenie, że tylko wąska grupa firm jest narażona na ataki cybersprzestępców, jest błędne. Każda, nawet mała firma, może paść ofiarą phishingu czy spoofingu.

Najczęściej ofiarami przestępstw internetowych stają się:

- instytucje finansowe, w tym banki,
- administracja publiczna,
- telekomy,
- e-Commerce,
- kurierzy,
- usługi abonamentowe (prąd, gaz, woda, telefon, Internet, telewizja).

RODZAJE ATAKÓW HAKERSKICH ORAZ PRAWDOPODOBIENSTWO ICH WYSTĄPIENIA

Badanie CERT Orange Polska 2019 wykazało, że działania niebezpieczne dla skrzynek e-mail mają różne oblicza. Od przesyłania nielegalnych treści, aż do włamań i ataków DDoS. Okazuje się, że oszustwa czają się na każdym kroku, a nasza świadomość na ich temat wciąż nie jest tak duża, jak powinna.



Rysunek 1 Rozkład procentowy kategorii incydentów obsługiwanych przez CERT Orange Polska w 2019 roku.

RODZAJE ATAKÓW E-MAILOWYCH

W tej części warto zadać sobie pytanie, dlaczego hakerzy chcą wysyłać e-maile, podając się za jakąś firmę i jakie metody do tego wykorzystują?

Najpopularniejszą z nich jest **PHISHING**. To nic innego jak próba podszycia się pod znaną markę / firmę w celu wyłudzenia danych od użytkowników lub nakłonienia ich do wykonania innej, niekorzystnej dla nich akcji. Zazwyczaj atak taki dokonuje się poprzez wysyłkę wiadomości e-mail twardząco podobnych do tych, które otrzymujemy od znanych marek, często wysyłanych z tej samej lub twardząco podobnej domeny. Phisherzy najczęściej próbują wykraść hasła użytkowników (np. logujące do konta bankowego) lub nakłonić odbiorców do pobrania złośliwego oprogramowania. Jak podaje raport CERT⁴, aż 40,4% wszystkich incydentów naruszających cyberbezpieczeństwo stanowiły phishing oraz skanowanie portów.



SPOOFING e-maili to nic innego jak wysyłanie wiadomości, których dane nagłówkowe (głównie dotyczące nazwy i adresu e-mail nadawcy) zostały zmodyfikowane tak, aby wyglądały na pochodzące z innego źródła (najczęściej znanej firmy). Zazwyczaj wykorzystywany jest do rozsyłania SPAMU oraz przy próbach wyłudzenia poufnych danych, ale również do głoszenia fake newsów w imieniu firmy. Bardziej złośliwe odmiany spoofingu mogą powodować poważne problemy, a niekiedy stanowić prawdziwe zagrożenie bezpieczeństwa.

W jakim celu hakerzy dopuszczają się przestępstw z wykorzystaniem e-maili?

W branży e-Commerce najczęściej wykradane są dane logowania do sklepu, numery telefonów, adresy oraz dane kart bankowych. W bankach najpopularniejsze jest przejmowanie danych logowania do konta osobistego, wykradanie pieniędzy z karty płatniczej i bezprawne „czyszczenie” kont ofiar ze środków finansowych. Natomiast w branży telekomunikacyjnej największym niebezpieczeństwem są fakszywe

faktury. To jednak nie koniec zagrożeń. Wszystkie usługi, które wymagają od użytkownika podpięcia swojej karty kredytowej, mogą być wymarzone dla hakerów. Dlaczego? Otóż przejmując konto w serwisie, szybko i prosto mogą przejść oni także dane karty płatniczej.

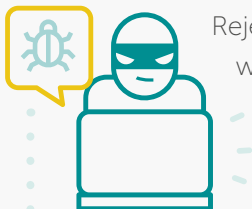
Konsekwencje phishingu i spoofingu, które ponoszą firmy, to najczęściej negatywny PR, utrata reputacji i zaufania klientów, a w konsekwencji... spadek przychodów. Niedawno czytaliśmy o Metro Banku, jednym z największych banków w Wielkiej Brytanii, który do tej pory zmagają się ze skutkami spoofingu. Polegał on na rozestaniu fake newsa o ich zbliżającym się upadku. Po tym jak klienci banku otrzymali informację o negatywnej kondycji finansowej instytucji z zachętą do opróżnienia środków na swoim koncie, przedstawiciele firmy musieli stłumić powstałą panikę. Pomimo podjętych kroków, wskutek ataku cena ich akcji spadła o 11%. A doniesienia o nowym ataku pojawiają się każdego dnia.

⁴ Badania CERT Orange Polska 2019.

NAJWAŻNIEJSZE ATAKI CYBERPRZESTĘPCÓW W 2019 ROKU⁵

Irańscy hakerzy podejrzani o DNS hijacking

Firma FireEye ujawniła globalną kampanię prowadzoną przez irańskich hakerów, których zadaniem było przekierowanie ruchu z firm na całym świecie za pośrednictwem swoich serwerów. Rejestrowali przy tym poświadczenia firm na wypadek planowanych przyszłych ataków.



Milion laptopów ASUS zainfekowanych złośliwym oprogramowaniem

W marcu Kaspersky opublikował informację o zainfekowaniu złośliwym oprogramowaniem około miliona użytkowników sprzętu Asus. Jak się okazało, wraz z pobraniem nowej aktualizacji laptopów dostarczonej przez producenta, użytkownicy instalowali złośliwy kod.



styczeń
2019

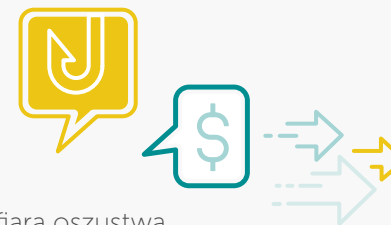
luty
2019

marzec
2019

kwiecień
2019

Polska Grupa Zbrojeniowa ofiara phishingu na 4 mln zł

Polska Grupa Zbrojeniowa padła ofiarą oszustwa kampanii phishingowej. Oszuści podszywali się pod czeskiego dostawcę broni i nakłaniali do opłacenia rzekomych dostaw. Przestępcom udało się wyłudzić 4 mln złotych.



Wyciek danych z Facebooka

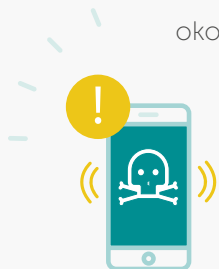
Dane aplikacji Facebooka gromadzone przez inne firmy zewnętrzne wyciekły. Wśród 540 milionów rekordów znajdowały się komentarze, polubienia, reakcje, nazwy kont, identyfikatory i inne dane.



⁵ Badania CERT Orange Polska 2019

WhatsApp zhakowany przez Pegasus

Malware Pegasus przejął kontrolę nad urządzeniami około 1400 użytkowników WhatsApp z całego świata. Oprogramowanie wykorzystало lukę w obsłudze połączeń wideo. Umożliwiło to zainfekowanie smartfona złośliwym oprogramowaniem i rozpoczęcie inwigilacji.



maj
2019



Atak na urządzenia IoT

Złośliwe oprogramowanie Silex ma na celu niszczenie pamięci urządzenia IoT, usunięcie konfiguracji sieci, złamanie zapory sieciowej, a w rezultacie zatrzymanie działania urządzenia.

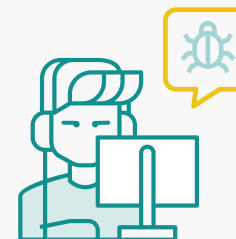
czerwiec
2019

Luka w zabezpieczeniach kart Visa

W wyniku przeprowadzonych badań bezpieczeństwa wykazano lukę w zabezpieczeniach kart Visa. Dzięki manipulowaniu danymi wymienianymi podczas płatności możliwa jest płatność zbliżeniowa przekraczająca określony limit pieniężny.



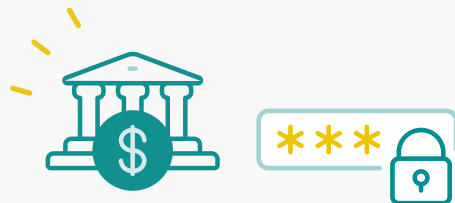
lipiec
2019



Użytkownicy Fortnite zainfekowani ransomwarem Syrk

Gracze w Fortnite zostali narażeni na zainstalowanie złośliwego programu, podszywającego się pod pakiet modyfikacji. Celem ataku było zaszyfrowanie plików użytkownika i zażądanie zapłaty okupu w zamian za odzyskanie danych.

sierpień
2019



Kampania phishingowa na PKO BP

Klienci banku PKO BP zostali ofiarami phishingu. Tym razem oszuści rozsyłali maile z treścią dotyczącą wykrytego nieautoryzowanego logowania i w ten sposób nakłaniali do podania danych logowania na fałszywej stronie internetowej. W rezultacie klienci mogli utracić pieniądze i dostęp do konta.



Klinika dziecięca „Budzik” zainfekowana ransomware

Zainfekowanie ransomware było wynikiem udanej kampanii phishingowej skierowanej na skrzynki pocztowe dziecięcej kliniki. Był to klasyczny przypadek maili z żądaniem zapłaty za fakturę. W wyniku ataku systemy komputerowe placówki zostały zaszyfrowane, co skutecznie zablokowało pracę kliniki.

wrzesień
2019

Ransomware atakujący systemy Linux

Tysiące serwerów internetowych zostało zainfekowanych, a ich pliki zaszyfrowane przez nową odmianę oprogramowania ransomware o nazwie LiLocked. Według badań ransomware atakuje wyłącznie systemy oparte na systemach Linux.

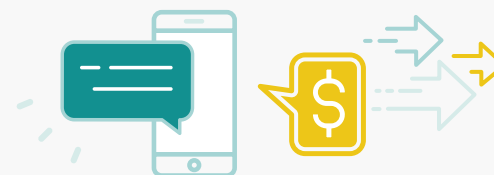
październik
2019



listopad
2019

Fałszywe SMS-y od Biedronki i Rossmanna

Przestępcy próbowali nakłonić klientów sklepów Biedronka i Rossmann do wypełnienia ankiety na fałszywej stronie, na której można było rzekomo wziąć udział w loterii i wygrać iPhone'a. Wypełnienie ankiety skutkowało obciążeniem karty płatniczej na kwotę 75 EUR.



grudzień
2019



Artur Pajkert

Head of Marketing, cyberfolks.pl

Od 2001 roku dzieli się wiedzą i poradami w sprawach e-marketingu i hostingu, jako menedżer, autor publikacji, prelegent, bloger i wykładowca.

Ataki na użytkowników poczty

Komunikacja mailowa często jest pełna odnośników, przycisków i wezwań do akcji. Mocno opiera się tym samym na zaufaniu użytkownika. Zaufaniu dotyczącym tego, że jest on pewien, iż – kiedy wykona akcję, do której próbujesz go skłonić – nie narazi się na żadne niebezpieczeństwo.

Żeby uniemożliwić potencjalnym atakującym wykorzystanie Twojej domeny i łatwe wystanie maila w Twojej własnej domenie, warto jest stosować podstawowe mechanizmy zabezpieczające, takie jak choćby SPF czy DKIM. Żaden

z tych mechanizmów nie chroni jednak przed użyciem nazwy, która jest łudząco podobna do Twojej! Wielu marketerów nie zdaje sobie sprawy z takich zagrożeń, jak cybersquatting i typosquatting.

Oto, na czym polegają:

Cybersquatting

Cybersquatting polega na czyhaniu na wolną nazwę domenową łudząco podobną do Twojej, a różniącą się jedynie końcówką. Przykład: masz domenę TwojaNazwaFirmy.pl, a ktoś rejestruje wolną TwojaNazwaFirmy.com.pl. Przeciętnemu odbiorcy trudno będzie dostrzec różnicę. Tymczasem domena z końcówką .com.pl pozostaje w pełnej dyspozycji atakującego, który może nawet mieć certyfikat SSL, aby zmniejszyć ewentualne podejrzenia.

Typosquatting

Ten atak polega na wykorzystaniu łudząco podobnej nazwy domeny, w której zamieniono

tylko jedną literę, jeden znak – na taki, który jest blisko tego właściwego na klawiaturze. Przykład: onat.pl – onet.pl. W takim przypadku łatwo jest zatem spreparować linki i zbudować stronę o łudząco podobnej zawartości.

Atak homofonetyczny

Atak homofonetyczny rzadziej jest przeprowadzany poprzez e-mail. Polega na rejestracji domeny o nazwie, która brzmi bardzo podobnie do Twojej, choć zapis jest zupełnie inny.

Atak homograficzny

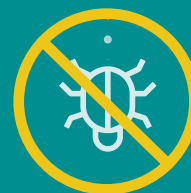
Atak homograficzny to już coś, co zdecydowanie trzeba brać pod uwagę w kontekście komunikacji mailowej. Chodzi o nazwy domowe, które są zapisane tak, że wyglądają łudząco podobnie do tych rzeczywistych, mimo że opierają się o inne znaki. Przykład: Onet.pl – Onet.pl (różnica w pierwszych znakach: cyfra zero i wielka litera o).

ROZDZIAŁ II

NIE BĄDŹ

DINOZAUREM,

poznaj najważniejsze zabezpieczenia –
czyli rzecz o SPF, DKIM, DMARC i S/MIME



DLACZEGO TO TAKIE WAŻNE?

Jeśli jesteś właścicielem domeny to doskonale zdajesz sobie sprawę z tego, że to właśnie ona reprezentuje Twoją markę w najlepszy możliwy sposób. Jest doskonale znana Twoim klientom i właśnie z tej domeny klienci spodziewają się komunikacji od Ciebie. Co zatem jeśli pewnego dnia ktoś wyśle z Twojej domeny treści podobne do tych, które zazwyczaj wysyłasz, tyle że z prośbą o podanie wrażliwych danych lub dokonanie płatności? Warto zapoznać się z zabezpieczeniami, które mogą ustrzec Twoją markę przed wizerunkową katastrofą.

**SPF i DKIM to dziś nie
nice to have
*a must have.***



Bartosz Gajewski

Manager ds. dostarczalności i wsparcia klienta

DOSTĘPNE ZABEZPIECZENIA

Dzięki zabezpieczeniu wiadomości firmy chronią swoich odbiorców przed próbami wyłudzenia ważnych danych osobowych, zabezpieczają renomę swojej firmy przed niepotrzebnymi skandalami, spowodowanymi wysyłką podrobionych wiadomości z ich domeny, oraz zwiększają dostarczalność swoich wiadomości e-mail.



Podstawą bezpiecznej komunikacji jest uwierzytelnienie domeny za pomocą SPF, DKIM i DMARC. Z kolejnych stron dowiesz się, za co odpowiada każde z tych zabezpieczeń i dlaczego są tak istotne.

Ciekawe jest to, że konfiguracja SPF i DKIM w znaczący sposób wpływa nie tylko na bezpieczeństwo, ale i na samą dostarczalność e-maili na globalne skrzynki. „Trudno dziś wyobrazić sobie zadowalającą dostarczalność wiadomości do Gmaila bez poprawnie skonfigurowanych SPF i DKIM” – mówi Bartosz Gajewski, ekspert odpowiedzialny za wdrożenia banków i fintechów w EmailLabs, i dodaje: „To dziś nie coś *nice to have*, a *must have*. W ostatnim czasie odnotowujemy sporo zgłoszeń dotyczących problemów z dostarczalnością do Gmaila wśród marek niedbających o najważniejsze uwierzytelnienia. To wyraźny trend i sądzę, że nakreśli on wymagania spoczywające na nadawcach w najbliższym czasie”.

SPF

SPF jest podstawowym i absolutnie minimalnym zabezpieczeniem. Pozwala wskazać, które adresy IP mogą wysyłać e-maile z danej domeny.

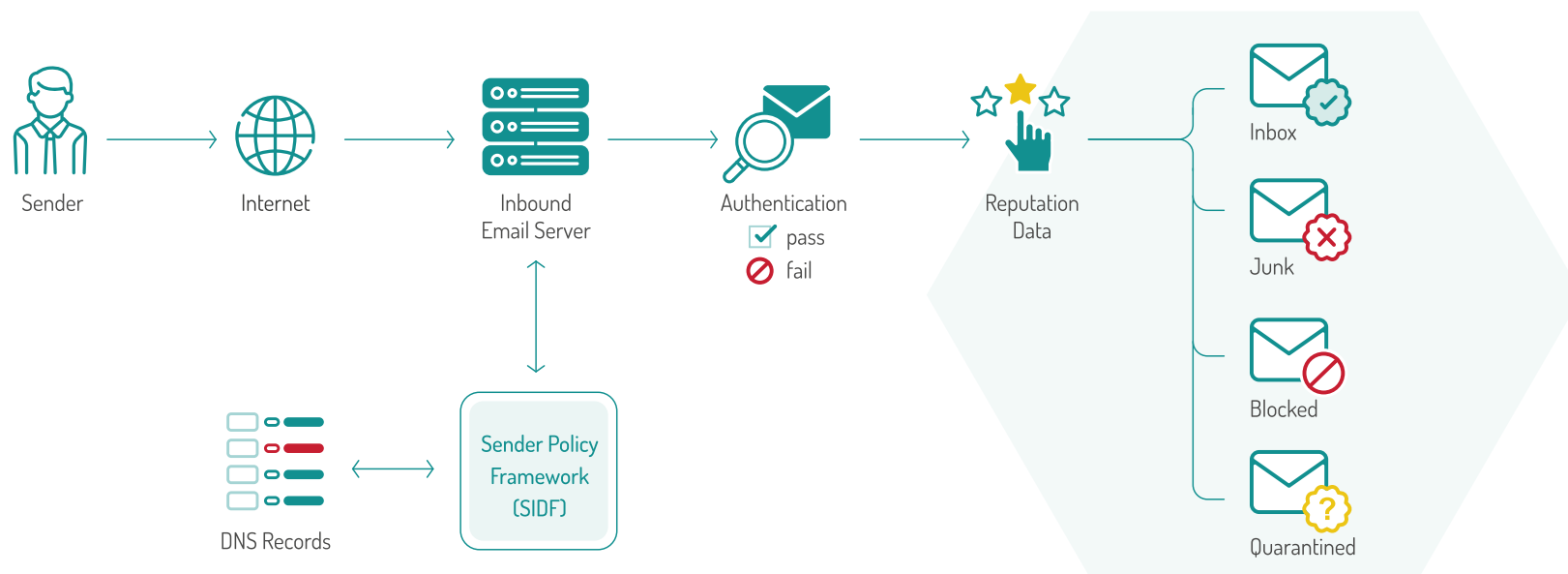
SPF, czyli Sender Policy Framework, to system zabezpieczający serwery SMTP, mający chronić przed nadawcami podszywającymi się pod domeny, do których używania nie mają prawa. System ten oparty jest o stosowny wpis w rekordach DNS danej domeny. Jeżeli IP nadawcy nie jest uwzględnione w rekordzie TXT domeny,

wiadomość otrzymuje odpowiednie oznaczenie lub zostaje odrzucona przez serwer SMTP odbiorcy.

Wiadomości, które mają ustawiony SPF, są pozytywnie odbierane przy wstępnej weryfikacji wiadomości przez serwer SMTP. Innymi słowy serwer ma pewność, że nadawca jest upoważniony do wysyłki tej wiadomości. Kiedy zajdzie poprawna autoryzacja, wiadomość jest dodatkowo poprawnie sformatowana, a IP, z którego wysyłany jest e-mail, posiada wysoką reputację

– ryzyko trafienia do folderu SPAM znacznie spada. Warto wiedzieć, że opisywany standard jest już powszechnie stosowany zarówno przez polskich, jak i zagranicznych providerów, dlatego ustawienie SPF jest dziś obowiązkiem.

Niestety SPF można w prosty sposób oszukać, dlatego nie jest on wystarczającym zabezpieczeniem, a wdrożenie kolejnych certyfikatów jest niezbędne do zapewnienia odpowiedniej ochrony.



DKIM

DKIM to dodatkowe zabezpieczenie, które zostało wprowadzone w odpowiedzi na problemy związane z SPF. DKIM wskazuje, czy wiadomość z danej domeny została rzeczywiście wysłana przez prawdziwego nadawcę.

DKIM, czyli Domain Keys Identified Mail

powstał po to, aby osoba, która otrzymuje wiadomość e-mail, miała pewność, że jego nadawcą jest właściciel adresu, np. example@domena.pl, a nie ktoś, kto się pod niego podsywa.

Jak działa DKIM?

Nadawca, przez odpowiednio skonfigurowany serwer SMTP, umieszcza w nagłówkach zaszyfrowane informacje na temat wiadomości e-mail. Używany jest do tego asynchroniczny klucz szyfrujący.

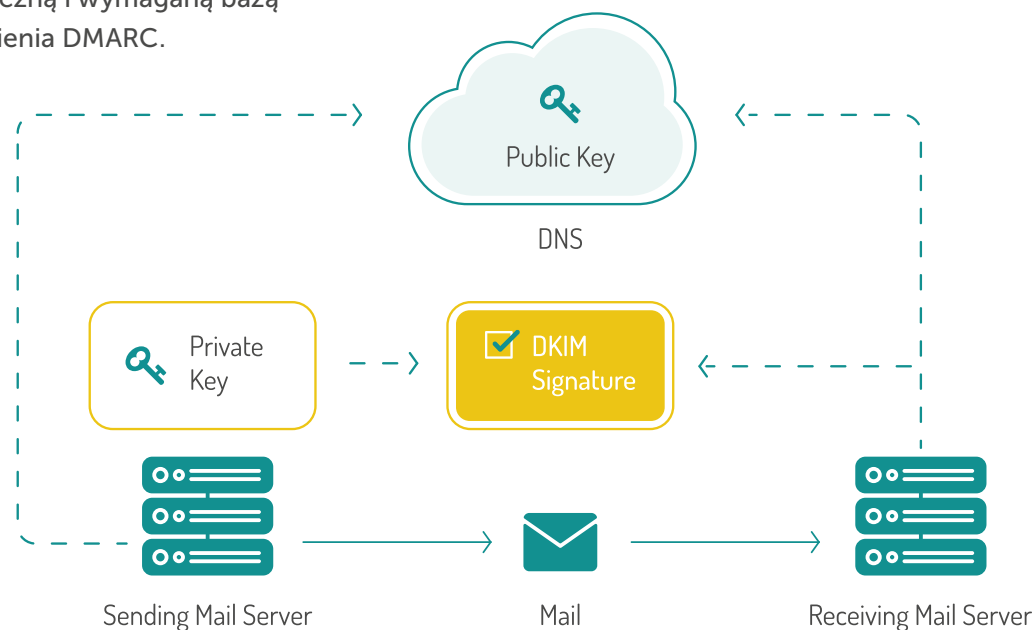
Odbiorca, widząc takie zaszyfrowane informacje, pobiera informacje na temat klucza do rozszyfrowania tych danych z rekordu DNS domeny nadawcy. Jeśli dane zostaną prawidłowo rozszyfrowane, to odbiorca może mieć pewność, że wiadomość rzeczywiście pochodzi od właściciela adresu.

Dlaczego warto mieć DKIM?

Wraz z rosnącą ilością cyberprzestępstw w obrębie e-maili i rozsyłanego SPAMU, providerzy skrzynek pocztowych zaczynają wymagać sygnatury DKIM, aby w ogóle dopuszczać wiadomości do skrzynek odbiorczych. Brak sygnatury DKIM może spowodować, że nawet najbardziej wartościowe treści od zaufanych nadawców trafią do SPAMU lub zostaną zablokowane przez providera już na poziomie serwera.

Sygnatura DKIM jest dziś dodatkowym czynnikiem, który zmniejsza ryzyko podszycia się pod Twoją firmę lub zakwalifikowania Twoich wiadomości jako SPAM, a już niedługo stanie się standardem i niezbędnym minimum.

DKIM jest konieczną i wymaganą bazą dla uwierzytelnienia DMARC.



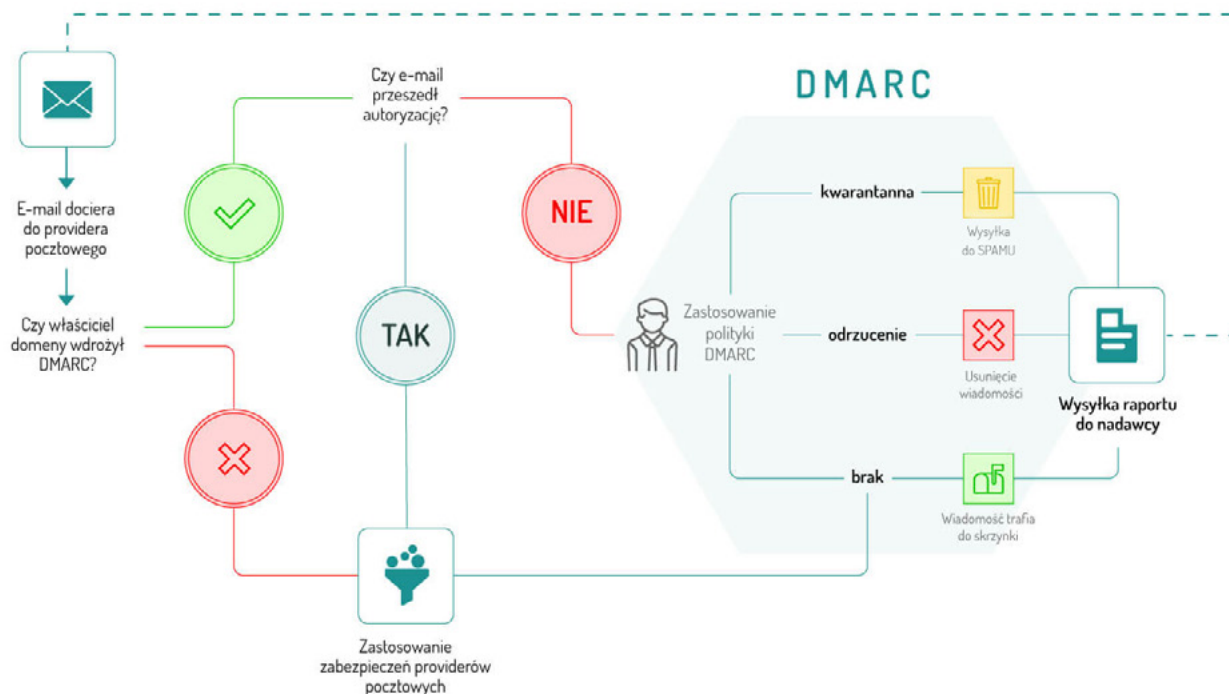
DMARC

DMARC to najbardziej zaawansowany mechanizm ochrony poczty. Prawidłowe ustawienie DMARC gwarantuje, że nikt nie będzie mógł podszyć się pod daną domenę. Jeśli więc z serwera, który nie należy do domeny nadawcy, zostanie wysłany do klienta e-mail „udający”, że został nadany np. przez bank, wówczas „prawdziwy” serwer tego nadawcy może zasignalizować serwerowi odbiorcy e-maila: „Nie pozwalam, żeby moi użytkownicy wysyłali wiadomości, które nie przejdą weryfikacji; jeśli dotrą one do ciebie, odrzuć je”.

DMARC, czyli Domain-based Message Authentication, Reporting & Conformance to metoda standaryzująca mechanizmy kontroli za pomocą rekordów SPF oraz kluczy DKIM, które mają zapewnić o wiarygodności e-maila. DMARC to światowy standard, wspierany przez liderów: Google, AOL, Microsoft czy Yahoo!.

Jak działa DMARC?

Najprościej ujmując DMARC to dopełnienie SPF oraz DKIM o możliwość narzucania Twojej polityki bezpieczeństwa u odbiorcy wiadomości. Możesz zdecydować, że jeżeli polityka DMARC nie będzie spełniona (SPF i DKIM okażą się niepoprawne), wiadomość taka będzie poddana kwarantannie, odrzucona przez serwer, ale co najważniejsze – informacja o takim incydencie zostanie do Ciebie przekazana w formie odpowiedniego raportu.



”

Aby DMARC zadziałał, należy umieścić w swojej domenie nadawcy nagłówkowego specjalne wpisy, które narzucają odpowiednie polityki postępowania z tymi wiadomościami, które nie przejdą pomyślnie testu DMARC. To bardzo korzystne rozwiązanie, gdyż umożliwia prawowitemu nadawcy zadziałać błyskawicznie, gdy tylko otrzyma informację o nieprawidłowym wyniku testu. Jeśli ktokolwiek będzie usiłował podszyć się pod właściciela domeny, będzie czas, aby ostrzec odbiorców tej wiadomości.

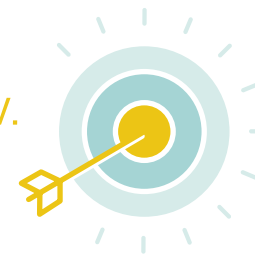


Marcin Kujawski

Dyrektor IT w EmailLabs

Niestety technologie te zostały w Polsce nieco zaniedbane. Wielu operatorów pocztowych nie wprowadziło jeszcze DMARC do swojej infrastruktury, przez co skrzynki u lokalnych operatorów są **mniej odporne na phishing niż u operatorów zachodnich**. A warto to zrobić. Według raportu Return Path tylko 83% poprawnych wiadomości e-mail dociera do odbiorców. Tymczasem DMARC może spowodować, że serwery pocztowe lepiej ocenią wiadomość, bo będą mogły potwierdzić wiarygodność nadawcy.

... tylko 83% poprawnych
wiadomości e-mail
dociera do odbiorców.



Certyfikat S/MIME,

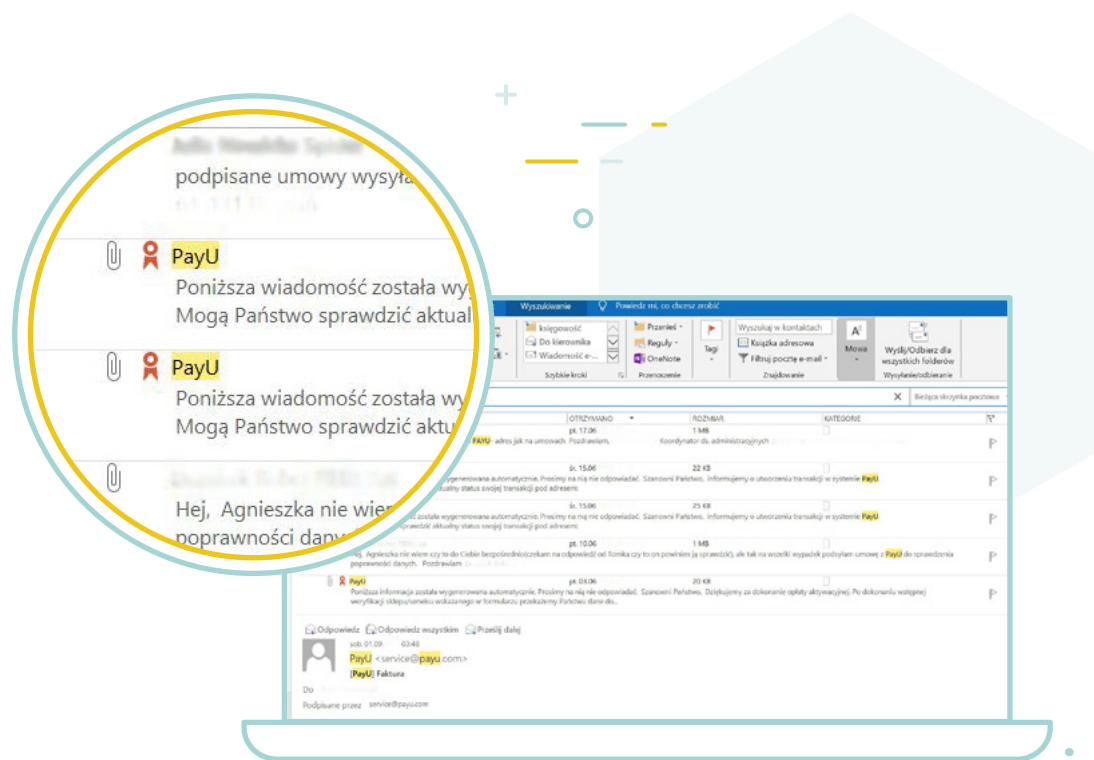
czyli wiadomość podpisana cyfrowo

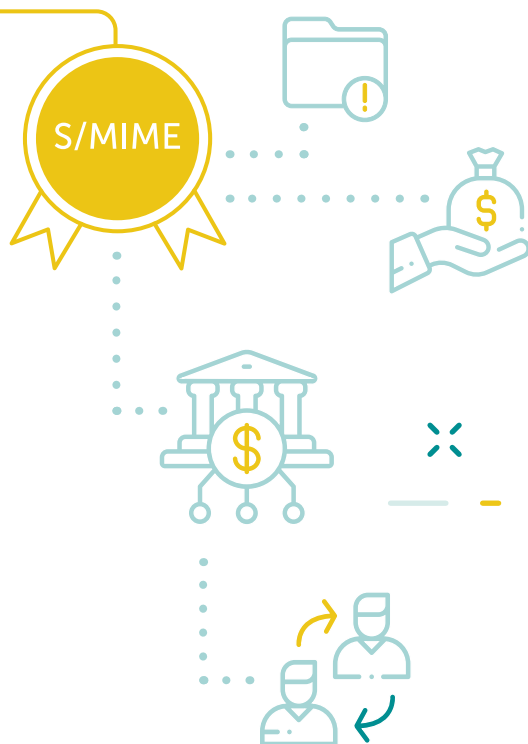
W przypadku e-maili transakcyjnych coraz częstsze zastosowanie, zwłaszcza w branży fintech, zyskuje w Polsce certyfikat S/MIME. Kto najczęściej korzysta z tego rozwiązania poza branżą fintech? Przede wszystkim ci nadawcy, którzy są odpowiedzialni za prowadzenie biznesów, gdzie w wiadomościach e-mail przesyłane są dane szczególnie wrażliwe.

Certyfikat S/MIME daje pewność, że nikt nieuprawniony nie podejrzał wiadomości, a jeśli tak się stało i zmienił wiadomość, odbiorca zostanie o tym poinformowany.

Cyfrowy podpis wiadomości to najlepsza ochrona dla użytkowników programów desktopowych: Microsoft Outlook, Mozilla Thunderbird, czy Apple Mail, ale nie tylko. Jest wspierany również przez Gmail. Warto zwrócić uwagę na to, że ten wykorzystywany szczególnie do ochrony e-maili transakcyjnych certyfikat jest

wydawany przez specjalny urząd certyfikujący i wymaga przekazania dowodu tożsamości oraz świadectwa zatrudnienia w danej firmie. Innymi słowy, nie ma możliwości, aby ktoś spoza firmy zdobył taki certyfikat dla adresów e-mail w Twojej domenie. Wiadomości podpisane kluczem





Najważniejsze zalety certyfikatu S/MIME:

- wyraźny znak graficzny w skrzynce odbiorczej – wiadomości firmy są wyróżnione,
- znak graficzny po otwarciu wiadomości,
- wiadomości podpisane cyfrowo danymi Twojej firmy,
- najlepsze zabezpieczenie dla użytkowników programów desktopowych.

Kto powinien wdrożyć S/MIME?

Cyfrowy podpis wiadomości jest najczęściej wykorzystywany przez firmy, które nadają e-maile przetwarzające dane wrażliwe – są nimi najczęściej banki, fintechy, platformy B2B. Ale nie tylko. S/MIME bywa wykorzystywany w przypadku wiadomości transakcyjnych także w innych branżach, np. w e-Commerce lub w przypadku poczty firmowej.

„Cieszę się faktem, że grupa klientów zainteresowana certyfikatem S/MIME sukcesywnie rośnie. Na pewno świadomość jest o wiele większa niż jeszcze kilka lat temu. Dziś trudno wyobrazić sobie fintech czy bank lub firmę pożyczkową, które nadają wiadomości transakcyjne bez cyfrowego podpisu. Podpisywanie wiadomości certyfikatem S/MIME wymaga odpowiedniego przygotowania od strony technicznej (albo sprawdzonego partnera, doświadczonego w wysyłkach opatrzonych tym certyfikatem). Jeśli tego zabraknie, to w przypadku dużych wolumenów procedowanie wysyłki e-maili może się nieco wydłużyć”.



Marcin Kujawski
Dyrektor IT w EmailLabs



ROZDZIAŁ III

WSPIERANIE

ZABEZPIECZEŃ

przez polskich i zagranicznych providerów pocztowych



Dostawcy poczty elektronicznej muszą zapewniać bezpieczeństwo swoim użytkownikom. Robią to poprzez uwzględnianie zewnętrznych mechanizmów antyphishingowych oraz rozwój swoich wewnętrznych systemów. Przeanalizowaliśmy, które globalne zabezpieczenia honorują providerzy polscy i zagraniczni.

KTÓRE ZABEZPIECZENIA WSPIERAJĄ NAJPOPULARNIEJSI POLSCY PROVIDERZY POCZTOWI?

	Onet	Interia	WP	o2
TLS	✓	✓	✓	✓
SPF	✓	✓	✓	✓
DKIM	✓	✓	✓	✓
DMARC	✓	✗	✓	✓
S/MIME	✗	✗	✗	✗

KTÓRE ZABEZPIECZENIA WSPIERAJĄ NAJPOPULARNIEJSI ZAGRANICZNI PROVIDERZY POCZTOWI?

	Gmail	Yahoo	Outlook.com (dawniej Hotmail)
TLS	✓	✓	✓
SPF	✓	✓	✓
DKIM	✓	✓	✓
DMARC	✓	✓	✓
S/MIME	✓	✗	✓



ROZDZIAŁ IV

ANALIZA

ZABEZPIECZEŃ

komunikacji e-mail top serwisów WWW w Polsce wg branży



WPROWADZENIE

Jak powstawał raport?

Przebadaliśmy ponad 7 tysięcy najpopularniejszych stron WWW w Polsce – **zbiorczo i w podziale na kategorie: e-Commerce, fintech, systemy rezerwacyjne oraz firmy kurierskie**. Dlaczego akurat te 4 kategorie? Gdy przyjrzeć się skrzynce pocztowej przeciętnego Kowalskiego, okazuje się, że e-maile z tych właśnie sektorów stanowią zdecydowaną większość wszystkich odbieranych wiadomości.

Wśród **eCommerce** przeanalizowaliśmy najważniejsze sklepy internetowe z różnych branż, porównywarki cenowe i platformy handlowe online.

W przypadku **fintechów** wzięliśmy pod lupę rozwiązania najpopularniejsze nad Wisłą: od firm udzielających pożyczek, sprzedających ubezpieczenia, przez bramki płatności, serwisy crowdfundingowe, po podmioty odpowiedzialne za cyberbezpieczeństwo, w tym za bezpieczny obieg dokumentów B2B. Wśród nich spora część biznesów to start-upy, będące na początku swojej drogi i nierzadko poszukujące inwestorów. Nie braliśmy pod uwagę banków.

W grupie **systemów rezerwacyjnych** znalazły się strony, na których można zakupić bilety – lotnicze, na koncert, autobus, czy do kina, a także dokonać rezerwacji.

W raporcie ujęliśmy także wszystkie najpopularniejsze **firmy kurierskie** działające na polskim rynku.



JAK NALEŻY ANALIZOWAĆ DANE

Prezentacja i analiza danych wymaga zastosowania określeń typowych dla SPF i DMARC. Poniżej tłumaczymy najważniejsze z nich.

SPF

W przypadku SPF kluczowe są oznaczenia czterech rekordów:

no SPF: brak konfiguracji SPF;

?all (neutral): oznacza brak instrukcji dla serwera odbiorczego, co ma zrobić z wiadomością w przypadku braku autoryzacji; wszystkie wiadomości powinny trafić do skrzynki odbiorczej;

~all (soft fail): jeśli wiadomość nie będzie pochodzić od upoważnionego nadawcy, zostanie wysłana, ale niektóre systemy pocztowe mogą oznaczyć ją jako SPAM;

–all (fail): jeśli kontrola SPF nie powiedzie się, większość systemów pocztowych oznaczy wiadomość przychodzącą jako SPAM.

DKIM

Badanie DKIM zostało przeprowadzone z uwzględnieniem selektorów najpopularniejszych systemów wysyłkowych wraz z domyślnym selektorem „default”.

DMARC

DMARC – jak należy rozumieć poniższe oznaczenia?

Jednym z elementów tego protokołu jest polityka oznaczana jako „p=...”. Informuje ona serwer odbierający, co zrobić z wiadomościami e-mail, które nie przeszły testu DMARC. Stosowane są trzy polityki: none, quarantine i reject:

polityka „p=none” (czyli nic): mówi odbiorcom wiadomości e-mail o wysłaniu raportów DMARC, nie instruuje ich jednak, jak obsługiwać komunikaty e-mail, które nie przejdą kontroli DMARC. W praktyce e-mail dochodzi do skrzynki odbiorczej adresata;

polityka „p=quarantine” (kwarantanna): ta polityka DMARC instruuje odbiorców wiadomości e-mail, aby umieszczali wiadomości e-mail, które nie przeszły kontroli DMARC, w folderze SPAM;

polityka „p=reject” (odrzuć): oprócz wysłania raportów DMARC, ta polityka całkowicie odrzuca wiadomości e-mail, które nie przejdą kontroli DMARC.

Określenie „empty” oznacza brakujący albo nieprawidłowy rekord.



WYNIKI BADAŃ: E-COMMERCE

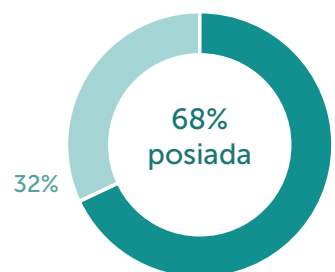


Prawidłowo wdrożonymi uwierzytelnieniami SPF oraz DMARC nie może pochwalić się aż 31% najpopularniejszych w Polsce przedstawicieli branży e-Commerce.

Ponad 80% e-sklepów nie posiada prawidłowego DMARC. Wśród pozostałych 18% zdecydowana większość, bo 62% reprezentantów tej grupy, stosuje politykę „p=none”.

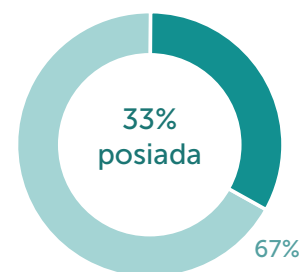
19% spośród przedstawicieli e-Commerce ze skonfigurowanym DMARC stosuje najbardziej restrykcyjną politykę „p=reject”. Polityka „p=quarantine” wykorzystywana jest także przez 19% serwisów z tej grupy. Najbezpieczniejsze rozwiązania najchętniej wdrażają zagraniczne sklepy i platformy online.

SPF – e-Commerce



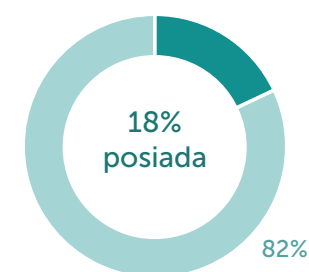
■ posiada ■ nie posiada

DKIM – e-Commerce



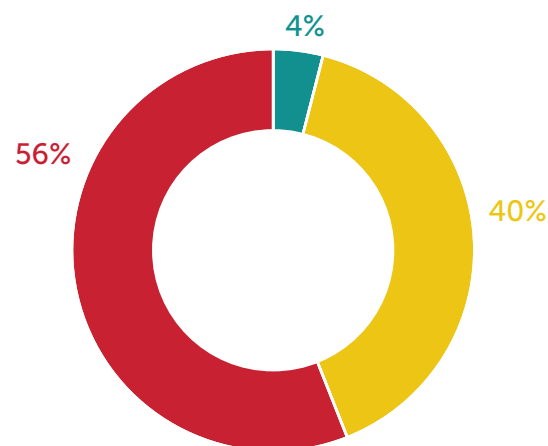
■ posiada ■ nie posiada (lub błędny)

DMARC – e-Commerce



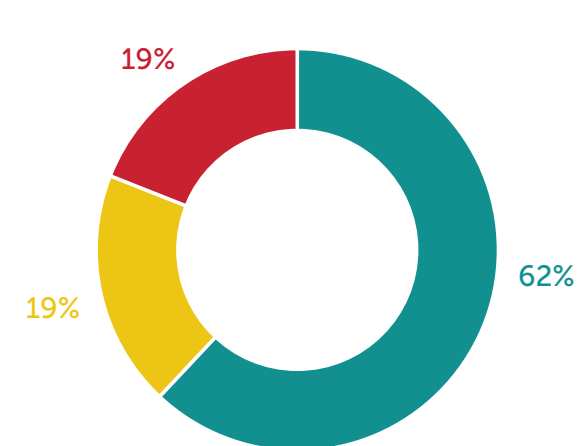
■ posiada ■ nie posiada

Polityka SPF – e-Commerce



■ neutral: brak instrukcji co zrobić z wiadomością
■ soft fail: e-mail na niektórych skrzynkach trafia do SPAMU
■ fail: e-mail na większości skrzynek trafia do SPAMU

Polityka DMARC – e-Commerce



■ p=none: e-mail dochodzi do skrzynki odbiorczej
■ p=quarantine: e-mail trafia do SPAMU
■ p=reject: e-mail nie dochodzi do skrzynki odbiorczej

WYNIKI BADAŃ: SEKTOR FINTECH

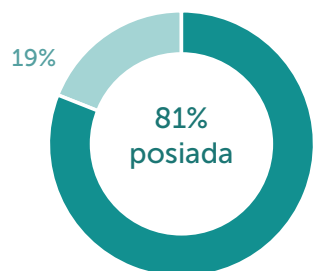


Okolo 11% najpopularniejszych fintechów w naszym kraju, firm zmieniających oblicze nowoczesnych technologii, konkurujących z tradycyjnymi sposobami prowadzenia usług finansowych, nie posiada prawidłowo wdrożonego zarówno SPF, jak i DMARC.

72% przedstawicieli tej grupy nie posiada prawidłowego DMARC. Wśród pozostałych 28%, aż 71% reprezentantów tej grupy stosuje politykę „p=none” i nie instruuje odbiorców wiadomości, jak obsługiwać komunikaty e-mail, które nie przejdą kontroli DMARC. W rezultacie e-mail dochodzi do skrzynki odbiorczej adresata, który może z powodzeniem kliknąć wiadomość i wywołać fałszywą stronę WWW.

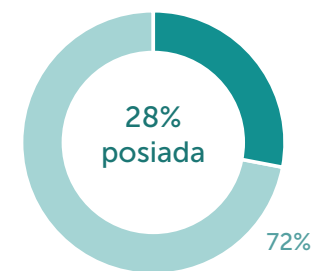
Tylko 11% spośród firm fintech ze skonfigurowanym DMARC stosuje najbardziej restrykcyjną politykę „p=reject”. Są wśród nich przede wszystkim polskie rozwiązania.

SPF – sektor fintech



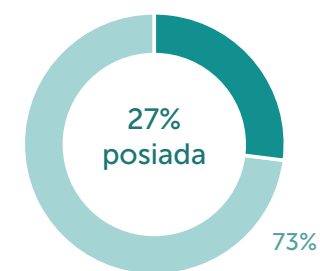
■ posiada ■ nie posiada

DKIM – sektor fintech



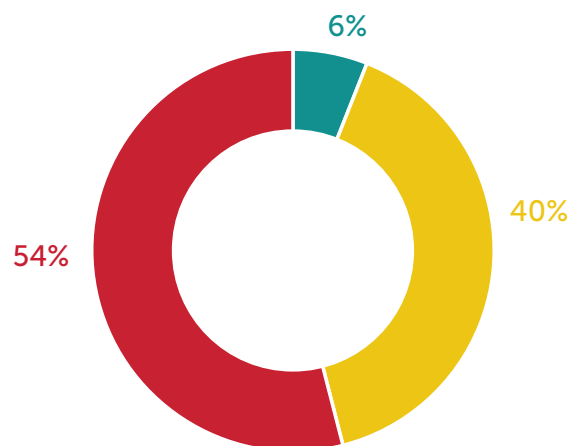
■ posiada ■ nie posiada (lub błędny)

DMARC – sektor fintech



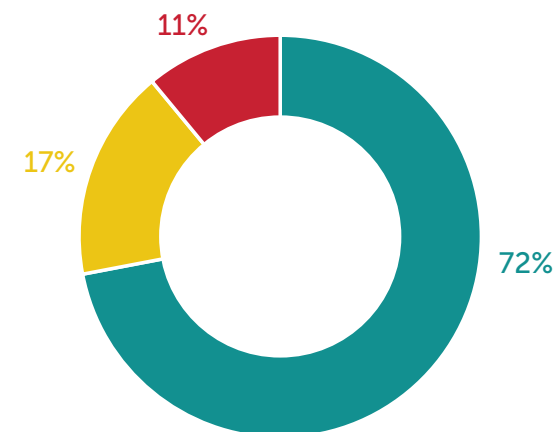
■ posiada ■ nie posiada

Polityka SPF – sektor fintech



■ neutral: brak instrukcji co zrobić z wiadomością
■ soft fail: e-mail na niektórych skrzynkach trafia do SPAMU
■ fail: e-mail na większości skrzynek trafia do SPAMU

Polityka DMARC – sektor fintech



■ p=none: e-mail dochodzi do skrzynki odbiorczej
■ p=quarantine: e-mail trafia do SPAMU
■ p=reject: e-mail nie dochodzi do skrzynki odbiorczej

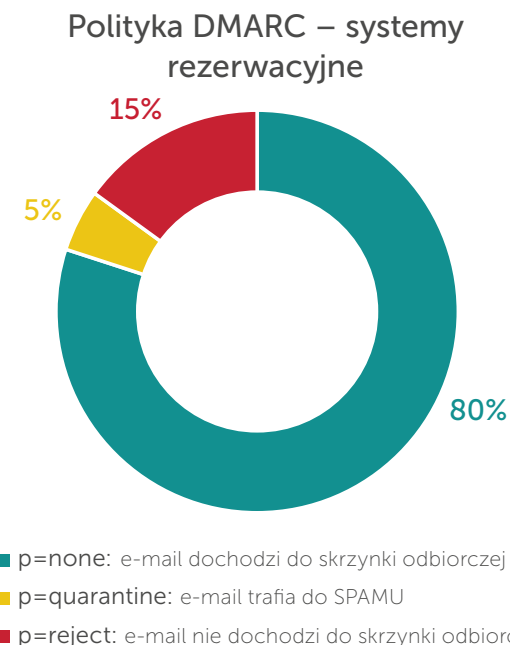
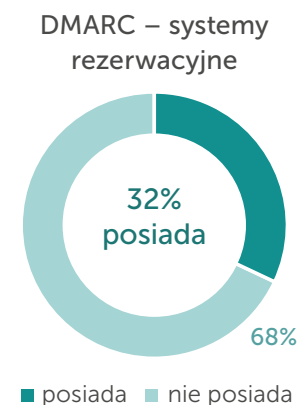
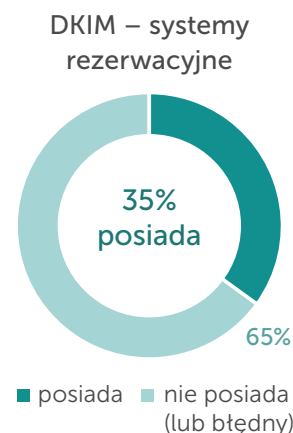
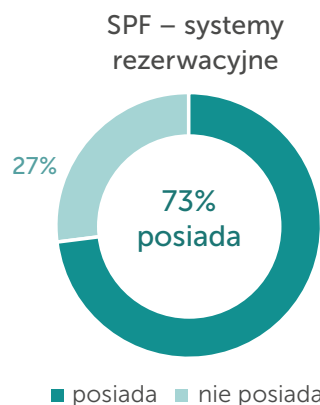
WYNIKI BADAŃ: SYSTEMY REZERWACYJNE



26% systemów rezerwacyjnych, z których w Polsce korzystamy najczęściej, nie posiada prawidłowo wdrożonych uwierzytelnień SPF oraz DMARC.

Okolo 68% systemów, w których kupujemy m.in. bilety na pociąg, samolot, czy do kina, nie posiada prawidłowego DMARC. Wśród pozostałych 32%, aż 80% reprezentantów tej grupy stosuje politykę „p=none” i nie instruuje odbiorców wiadomości, jak obsługiwać komunikaty e-mail, które nie przejdą kontroli DMARC.

Tylko 15% spośród systemów ze skonfigurowanym DMARC stosuje najbardziej restrykcyjną politykę „p=reject”. Odrzuca ona całkowicie korespondencję, która nie przejdzie kontroli DMARC. Najlepiej pod tym względem prezentują się serwisy zagraniczne.



■ **neutral**: brak instrukcji co zrobić z wiadomością
 ■ **soft fail**: e-mail na niektórych skrzynkach trafia do SPAMU
 ■ **fail**: e-mail na większości skrzynek trafia do SPAMU

■ **p=none**: e-mail dochodzi do skrzynki odbiorczej
 ■ **p=quarantine**: e-mail trafia do SPAMU
 ■ **p=reject**: e-mail nie dochodzi do skrzynki odbiorczej



WYNIKI BADAŃ:

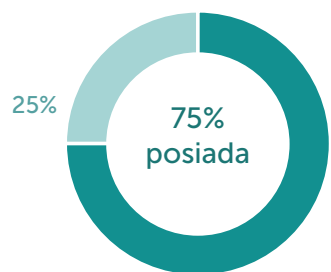
FIRMY KURIERSKIE

Firmy kurierskie, które poddaliśmy badaniu, dzielą się na te, którym zabezpieczenia przed podszywaniem się pod domenę są kompletnie obce i takie, które najpewniej odrobiły zadanie domowe i wdrożyły wszystkie uwierzytelnienia.

25% firm w tej grupie nie posiada prawidłowo wdrożonego zarówno SPF, jak i DMARC. Z DMARC nie korzysta 67% podmiotów. Wśród pozostałych 33%, aż 75% przedstawicieli tej grupy stosuje politykę „p=reject”.

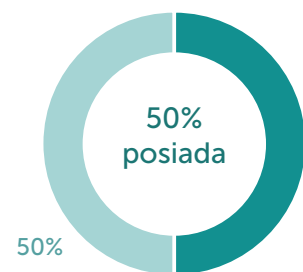
Zwraca uwagę fakt, iż aż połowa najpopularniejszych w Polsce firm doręczających przesyłki, posiada wdrożony DKIM, co jest dobrym wynikiem.

SPF – firmy kurierskie



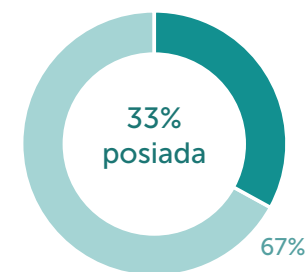
■ posiada ■ nie posiada

DKIM – firmy kurierskie



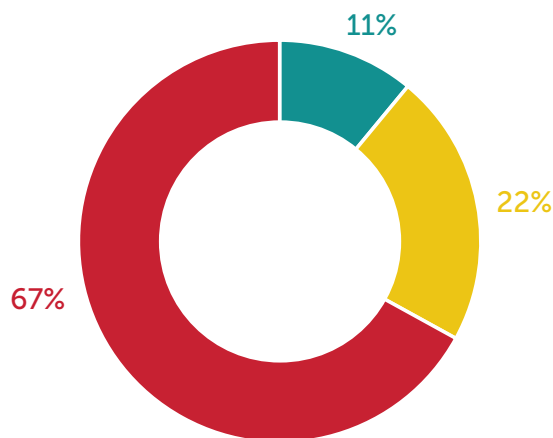
■ posiada ■ nie posiada (lub błędny)

DMARC – firmy kurierskie



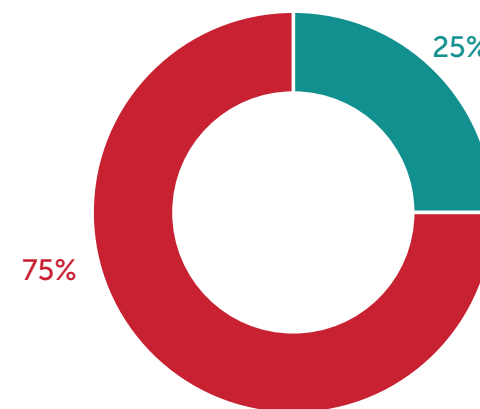
■ posiada ■ nie posiada

Polityka SPF – firmy kurierskie



■ neutral: brak instrukcji co zrobić z wiadomością
■ soft fail: e-mail na niektórych skrzynkach trafia do SPAMU
■ fail: e-mail na większości skrzynek trafia do SPAMU

Polityka DMARC – firmy kurierskie



■ p=none: e-mail dochodzi do skrzynki odbiorczej
■ p=quarantine: e-mail trafia do SPAMU
■ p=reject: e-mail nie dochodzi do skrzynki odbiorczej

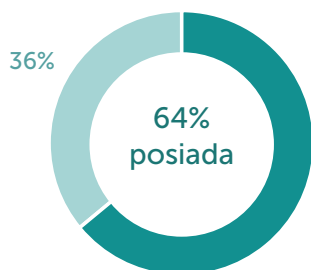
UJĘCIE GLOBALNE: WYNIKI DLA NAJPOPULARNIEJSZYCH SERWISÓW WWW W POLSCE

Z analizy ogólnego zestawienia przygotowanego dla ponad 7 tysięcy najpopularniejszych w Polsce stron WWW wynika, iż ponad 28% serwisów nie posiada poprawnie skonfigurowanego zarówno SPF, jak i DMARC. 64% najchętniej odwiedzanych serwisów WWW korzysta z SPF, a co trzeci posiada uwierzytelnienie DKIM. 21% korzysta z DMARC, z najpopularniejszą polityką „p=none”, stanowiącą ponad 60%.

Z jednej strony obserwujemy spory udział serwisów, które nie dbają o żadne zabezpieczenia komunikacji i są to w większości polskie rozwiązania. Z drugiej – z racji dość licznej reprezentacji globalnych stron WWW, w tym mediów społecznościowych, których założyciele do bezpieczeństwa przykładają najwyższą wagę – utrzymuje się przyzwoita średnia.

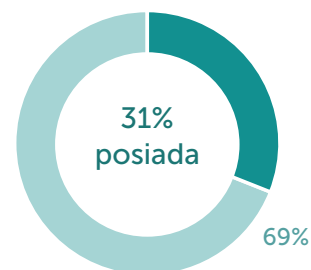
Warto mieć na uwadze, że w grupie roboczej pracującej nad rozwojem standardu, jakim jest DMARC, znaleźli się właśnie przedstawiciele m.in. Facebooka, Google czy PayPala, którzy przodują na naszej liście najpopularniejszych serwisów.

SPF – najpopularniejsze strony w Polsce



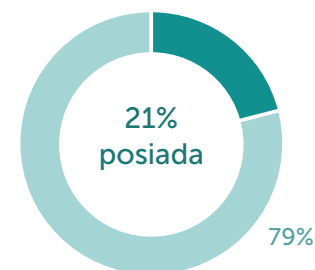
■ posiada ■ nie posiada

DKIM – najpopularniejsze strony w Polsce



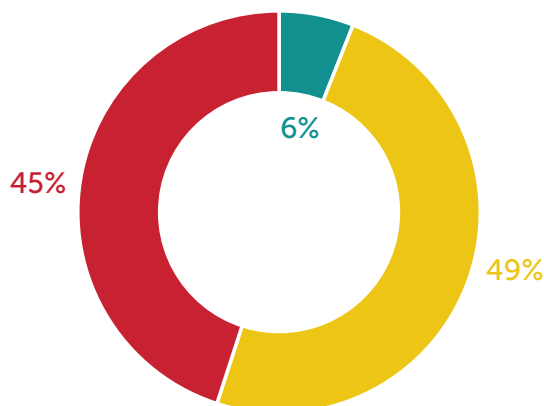
■ posiada ■ nie posiada (lub błędny)

DMARC – najpopularniejsze strony w Polsce



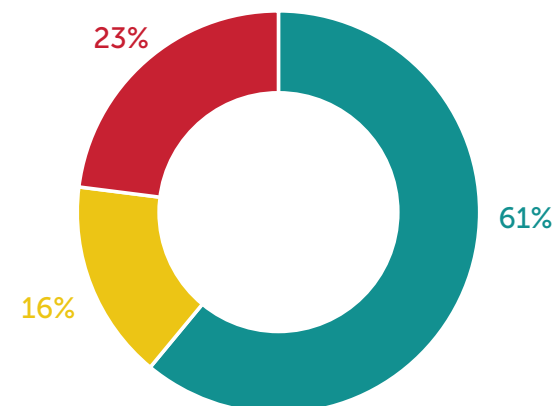
■ posiada ■ nie posiada

Polityka SPF – najpopularniejsze strony w Polsce



■ neutral: brak instrukcji co zrobić z wiadomością
■ soft fail: e-mail na niektórych skrzynkach trafia do SPAMU
■ fail: e-mail na większości skrzynek trafia do SPAMU

Polityka DMARC – najpopularniejsze strony w Polsce



■ p=none: e-mail dochodzi do skrzynki odbiorczej
■ p=quarantine: e-mail trafia do SPAMU
■ p=reject: e-mail nie dochodzi do skrzynki odbiorczej

PODSUMOWANIE

Myśląc o tym, która grupa serwisów online będzie najlepiej zabezpieczona pod kątem SPF, DKIM i DMARC, trochę podświadomie chcemy, aby były to podmioty, które zazwyczaj przetwarzają najbardziej wrażliwe dane. Nasze badania to potwierdzają. Wiele rozwiązań z branży fintech to jeszcze start-upy, powstałe w dużej mierze 2–3 lata temu.

Od nich zazwyczaj wymaga się więcej, ale i wymagają one dużo również od siebie, bo wiele z nich szuka inwestorów, a wypełnienie wszystkich najważniejszych zaleceń dotyczących bezpieczeństwa, zwłaszcza w branży finansowej, to po prostu podstawa zaufania do biznesu. Poza tym lubią być (i są) na bieżąco z najnowszymi rozwiązaniami.

Zaskakuje to, jak mocno rozwiązania e-Commerce pozostają w tyle. Niemal jedna trzecia z nich nie posiada ani SPF, o DMARC nie wspominając. A przecież ofiarami ataków phishingowych i spoofingowych bardzo często padają także sklepy internetowe. Większość najpopularniejszych serwisów w tej branży powstała kilka czy nawet kilkanaście lat temu. Koncentrują się

one raczej na komunikacji marketingowej, wiadomości transakcyjne często są tematem zapomnianym. Bywa też tak, że odpowiada za nie po prostu inna część biznesu, inny dział.

Nierzadko słyszy się, że „Są one wysyłane z (jakiegoś) systemu. Nie wiem, kto za nie odpowiada. To pytanie do IT”. Firmy dbające o profesjonalną obsługę e-maili transakcyjnych, jeśli konfiguruje SPF i DKIM, to raczej w trosce o lepszą dostarczalność. DMARC i bezpieczeństwo pozostają trochę zaniedbanym obszarem komunikacji e-mail. Tymczasem jeśli firmie przydarzy się incydent związany z phishingiem, na pewno poniesie ona spore koszty.



Łączna liczba ataków phishingowych dynamicznie rośnie i wszystko wskazuje na to, że z końcem roku 2021 **możemy odnotować nawet dwukrotny wzrost ataków w stosunku do roku 2020**. Wiele się mówi o tym, w jaki sposób to końcowy użytkownik powinien zabezpieczyć się przed zagrożeniem, wskazując na konieczność sprawdzenia adresów online w nieznanym wiadomościach e-mail, unikania podawania danych uwierzytelniających, jeśli użytkownik nie jest pewien, czy dana strona jest bezpieczna. Poświęca się też sporo miejsca tematyce używania bezpiecznych połączeń, dobrych praktyk korzystania z Wi-Fi, itp.

Wciąż jednak za mało uwagi przykładamy do tego, co firmy mogą zrobić, aby chronić swoich użytkowników. A zabezpieczenia, jakie mogą wdrożyć, w tym choćby DKIM czy DMARC, są rozwiązaniami zaskakująco łatwymi w implementacji. Może nie eliminują w 100% problemu, ale z pewnością istotnie minimalizują zagrożenia związane z atakami phishingowymi.

Jakub Szczęsny, Antyweb

Im bardziej znana marka, tym poważniejsze konsekwencje. Natomiast wdrożenie SPF i polityki „p=reject” daje możliwość zablokowania wiadomości e-mail i ostrzeżenia użytkowników, zanim nastąpi eskalacja problemów i – co istotne – nie kosztuje wiele pracy. Dziś wyraźnie widać, jak podmioty, które odczuły wcześniej konsekwencje działań cyberprzestępców, zaostrzyły wymagania w obszarze bezpieczeństwa i w ostatnim czasie mocno ograniczyły możliwość podszycia się pod ich domeny (jak niektóre firmy kurierskie). Są jednak i takie, które zadania nie odrobiły i wolą odpowiedzialność przerzucić na użytkowników ich serwisów.

Podsumowując wyniki badania – ciągle niewiele biznesów online, zwłaszcza naszych rodzimych, dba o bezpieczeństwo komunikacji e-mail. Mamy od kogo się uczyć i na kim wzorować. Jak pokazuje przypadek DMARC, najbardziej świadome serwisy WWW same tworzą i rozwijają standardy bezpieczeństwa.

SPF, DKIM, DMARC... – oczywiście nie ma idealnego rozwiązania, zawsze przecież ktoś może kupić domenę łudząco podobną do naszej i z niej wysyłać fałszywą korespondencję. Jednak taki atak ma mniejszą siłę rażenia – po serii komunikatów prasowych wielu użytkowników poczty dokładniej przygląda się otrzymanym wiadomościom e-mail. Nie zapominajmy, że biznes nie stoi w miejscu i nie przygląda się biernie eskalacji skutków działań cyberprzestępców. Incydenty związane z bezpieczeństwem poczty miały również pozytywny wpływ na zmiany dokonane przez wiele firm w tym obszarze.

Wierzymy, że dzięki raportom, takim jak nasz, coraz więcej firm, zwłaszcza polskich, zdecyduje się na wdrożenie choćby SPF i indywidualnego DKIM. Eksperti EmailLabs już szósty rok wspierają biznesy online w konfiguracji tych zabezpieczeń.

Chcących dowiedzieć się więcej na ten temat, zapraszamy do kontaktu.



Katarzyna Garbaciak
Managing Director, EmailLabs

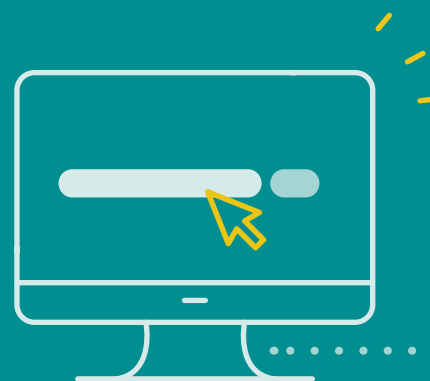


ROZDZIAŁ V

CO TWOJA

FIRMA

może zrobić już teraz?





Chcesz przekonać się, czy Twój serwis WWW spełnia wymogi bezpieczeństwa komunikacji e-mail? To naprawdę proste i nie trzeba pracować w IT, aby się o tym przekonać.

1.

Wejdź na jeden z serwisów podających ustawienia związane z daną domeną, np. MXTOOLBOX. W wyszukiwarce wpisz nazwę Twojej domeny i sprawdź wyniki.

SuperTool Beta7

mojadomena.pl

MX Lookup

2.

Jeśli interesuje Cię konkretny parametr i chcesz sprawdzić rekordy SPF czy politykę DMARC, zmień filtrowanie, wybierając: „SPF Record Lookup”, „DKIM Lookup” bądź „DMARC Lookup”.

Test	Result	
DMARC Record Published	No DMARC Record found	More Info
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	More Info
DNS Record Published	DNS Record found	

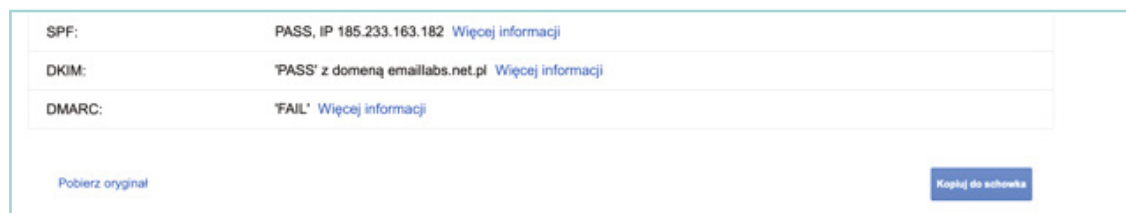
3.

W kolejnym kroku wyślij testowy e-mail z Twojej domeny na swój adres, np. w Gmailu. Po jego otrzymaniu wejdź w opcję „Pokaż oryginał”.



4.

W szczegółach wiadomości sprawdzisz poziom zabezpieczenia Twojej komunikacji e-mail.



Nie masz ustawionego SPF i DKIM? Zgłoś się do osób odpowiedzialnych za zarządzanie serwerami SMTP, opiekującymi się DNS czy ogólnie domenami w Twojej firmie. Być może dział bezpieczeństwa będzie dobrym adresatem. Możesz też skorzystać z know-how firmy dostarczającej e-mail API i serwery SMTP, która niejako w pakiecie oferuje standardy komunikacji e-mailowej i na pewno podpowie, jak ustawić wymagane parametry.

ROZDZIAŁ VI

DODATEK

dla programistów



PRZYKŁADOWY WPIS SPF

`domena.pl IN TXT „v=spf1 mx a ptr ip4:127.0.0.1/24 a:mailer.domena.com.pl
include:another.domena.org ~all”`

domena.pl IN TXT – część określająca domenę oraz rodzaj wpisu w DNS

v=spf1 – część deklarująca wpis jako SPF

mx – pozwalaj serwerom określonym jako mx na wysyłanie wiadomości

a – pozwalaj na wysyłkę danemu adresowi IP

ptr – pozwalaj na wysyłkę wszystkim domenom kończącym się na domena.pl

ip4:127.0.0.1/24 – pozwalaj adresom IP z danego zakresu na wysyłkę wiadomości

a:mailer.domena.com.pl – pozwalaj na wysyłkę wiadomości z podanych serwerów

include:another.domena.org – pozwalaj na wysyłkę wiadomości z podanych domen

~all lub ?all lub –all – określenie rodzaju restrikcji wobec podanego wpisu np.:

– jeżeli nie spełnia podanych warunków wpisu, odrzuć pocztę,

~ jeżeli nie spełnia warunków, nie odrzucaj wiadomości, ale zaznacz wiadomość,

? neutralne, błędna autoryzacja nie ma wpływu na wysyłkę.

Pamiętaj!

**Błędna konfiguracja SPF uniemożliwi skuteczne
dostarczenie wiadomości Twojej firmy!**



PRZYKŁADOWY WPIS DKIM

Zasada działania DKIM jest dosyć prosta. Generowana jest para kluczy: prywatny i publiczny. Ten pierwszy zostanie wykorzystany do wygenerowania sumy kontrolnej, która umieszczana jest wewnątrz nagłówka wiadomości e-mail, natomiast publiczny klucz musi zostać umieszczony w rekordzie DNS pod odpowiednim adresem, w formacie:

selektor_domainkey.domena.pl

Selektor – ciąg znaków umożliwiający posiadanie wielu kluczy dla jednej domeny.

_domainkey – stały ciąg znaków, który będzie odpytywany przez serwer odbiorcy.

Domena/subdomena – musi być taka sama jak ta, która będzie wykorzystywana w polu „from” wiadomości e-mail.

Oto, jak powinien wyglądać wpis w DNS:

selektor._domainkey.domena.pl descriptive text „v=DKIM1; g=*; k=rsa; p=MIGfMA0GCSqGS1b3DQEBAQ.....”

Serwer odbiorcy, badając nagłówki wiadomości, natrafia na następujący zapis:

DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; d=domena.pl; s=selektor; t=1439834102; bh=JiUlKHkzkmhZO5hdosgTv3gDmKk=; h=Date:Subject:From:To:List-Unsubscribe; b=Fgq2lwXyRJUdcQ8m8iZD.....

Dzięki wpisowi w DNS serwer odbiorcy może ocenić, czy wiadomość została nadana przez serwer deklarowany w polu „from”. Sprawdzanie wiadomości odbywa się na zasadzie porównania sumy kontrolnej dodanej do wiadomości oraz sumy wygenerowanej przez serwer odbiorcy na podstawie klucza publicznego umieszczonego w DNS. Jeżeli klucze się zgadzają, wiadomość dostarczana jest do skrzynki odbiorczej.

Jak każda technologia, DKIM może również zostać złamany, chociażby przez wyciek klucza prywatnego. Możliwe jest także rozszyfrowanie klucza prywatnego w przypadku wykorzystania zbyt słabego szyfrowania.

Praktyki, które musisz znać:

- w celu zabezpieczenia swoich wiadomości w jak najwyższym stopniu, używaj złożonego szyfrowania, np. rsa-sha256;
- co jakiś czas odśwież klucz publiczny oraz prywatny;
- jeżeli to możliwe, używaj kilku selektorów na przemian.

ROZDZIAŁ VII

O EMAILLABS





EmailLabs™

**Wysyłaj skutecznie
powiadomienia ze strony
i potwierdzenia zamówień
dzięki bezpiecznemu API
i SMTP w chmurze!**

W kilka minut podłącz swój sklep
lub aplikację i zyskaj najlepszą
dostarczalność na rynku.

CO NAS WYRÓŻNIA?



BEZPIECZEŃSTWO WYSYŁEK

W EmailLabs dbamy o standaryzację wysyłki e-mail. W standardzie zapewniamy szyfrowanie TLS, zabezpieczenie wiadomości SPF oraz DKIM. Wspieramy naszych klientów w konfiguracji DMARC oraz certyfikatu S/MIME. Obsługujemy e-maile transakcyjne banków i branży fintech.



UNIKALNE NA POLSKIM RYNKU KNOW-HOW

Spełniamy standardy globalnych i lokalnych providerów e-mailowych. Dzięki know-how zbudowanemu w oparciu o wdrożenia największych klientów z branży e-Commerce czy fintech, posiadamy empiryczną wiedzę dotyczącą zasad, jakimi kierują się providerzy pocztowi.



NAJLEPSZA DOSTARCZALNOŚĆ E-MAIL

Dzięki infrastrukturze autoryzowanej u polskich i zagranicznych providerów i odpowiednim jej przygotowaniu, Twoje e-maile transakcyjne zawsze trafiają do skrzynki głównej. Posiadamy praktyczną wiedzę w zakresie budowania i utrzymywania jak najlepszej reputacji nadawcy.



SZCZEGÓŁOWA ANALITYKA E-MAIL

Panel analityczny pozwala na sprawdzenie wszystkich statusów e-maili, w tym Feedback Loop czy Spambounce i to w czasie rzeczywistym. Umożliwia on sprawdzenie logów każdego pojedynczego e-maila wraz z dokładnymi komunikatami zwracanymi przez providerów.



EMAILLABS – EKSPERCI W ZAKRESIE DOSTARCZALNOŚCI E-MAILI

SZYBKA INTEGRACJA PO API LUB SMTP

Posiadamy gotowe połączenie z wieloma systemami, dzięki czemu integracja z EmailLabs może zająć dosłownie kilka minut.

BEZPIECZEŃSTWO

W EmailLabs Twoje dane są bezpieczne. Uwzględniamy indywidualne zapisy prawne. Nasza usługa, jak i serwerownie zapasowe, realizowane są w pełni na obszarze EOG.

SKALOWALNOŚĆ

Obsługujemy najbardziej świadome fintechy oraz banki. Dzięki skalowalnej infrastrukturze możemy dopasować zasoby do wolumenów, jakie wysyłasz.

SKONTAKTUJ SIĘ Z NAMI:



Paula Przeglęta
Key Account Manager
☎ +48 515 866 398
✉ sales@emaillabs.pl

WEJDŹ NA
www.emaillabs.pl
I PRZETESTUJ BEZPIECZNĄ
WYSYŁKĘ E-MAIL!



ŹRÓDŁA:

1. <https://www.dotpay.pl/blog/praktyczny-poradnik-ecommerce/wykorzystanie-e-mail-marketingu-do-promocji-e-sklepu-co-warto-wiedziec>
2. Daily number of e-mails worldwide 2024 | Statista.
3. Dane Kaspersky Lab, <https://www.facebook.com/watch/?v=612351026135077>, <https://www.facebook.com/watch/?v=3230063277120225>
4. Badania CERT Orange Polska 2019.
5. Cashless/Fintech Poland, Mapa Polskiego Fintechu 2019.
6. Return Path, Authenticating Email with DMARC, SPF and DKIM.
7. Google, Gmail. Managing S/MIME Certificates.
8. Alexa, Amazon Top Sites.
9. www.egospodarka.pl, Spam i phishing.
10. www.barracuda.com, E-mail spoofing.



