Wyobraź sobie dwa scenariusze. W jednym wysyłasz bardzo ważne wiadomości e-mail do potencjalnych klientów, ale nie otrzymujesz od nich odpowiedzi. Później dowiadujesz się, że stało się tak, ponieważ Twój e-mail trafił do folderów spamu i potencjalnie straciłeś możliwości biznesowe. W drugim scenariuszu otrzymujesz telefon od swojego partnera „jakiego rodzaju e-maile wysyłasz”? Ale nie wysyłałeś żadnych e-maili – ktoś się pod Ciebie podszył.

Oba scenariusze są realnymi zagrożeniami. A jeśli korzystasz z usługi poczty e-mail przy użyciu własnej domeny, prawdopodobnie będziesz chciał upewnić się, że konfiguracja jest prawidłowa, aby nie napotkać takich problemów. Dostawcy poczty e-mail powinni mieć skonfigurowane procedury weryfikacji konfiguracji domeny po swojej stronie, ale czasami mogą one zawieść lub dostarczyć fałszywych wyników pozytywnych. Dodatkowo – zawsze warto poszerzać swoją wiedzę. Zanurzmy się więc w kilka technicznych terminów dotyczących konfiguracji poczty e-mail dla domeny niestandardowej: czyli MX, DKIM, SPF i DMARC.

Jak hakerzy mogą wykorzystać domenę bez kluczy do fałszowania wiadomości e-mail

Brak rekordów SPF i DKIM oznacza po prostu, że domena jest narażona na ryzyko ataku hakera. Przede wszystkim, jest to dobry grunt dla hakerów do przekształcania autentycznych wiadomości e-mail w spam, a jednocześnie są one łatwe do podrobienia. Kiedy chcą podszyć się pod twoje e-maile, użyją jednego z darmowych serwerów SMTP online, a następnie zmodyfikują go w pożądany przez siebie sposób w polu ‘FROM’, który go wysyła. Z tego powodu posiadanie odpowiednich rekordów dla swojej domeny jest ze względów bezpieczeństwa i sposobem weryfikacji wiadomości e-mail. Korzystając z podpisu cyfrowego DMARC, hakerzy nie mogą wysyłać wiadomości e-mail w imieniu Twojej domeny, a szyfrowanie nie może zostać sfałszowane, dzięki czemu wiadomości e-mail nie są oznaczane jako spam.

Powiązane z pocztą e-mail rekordy domeny

Zacznijmy od podstaw. Czy kiedykolwiek zadałeś sobie pytanie, kto kieruje Twoim ruchem internetowym? Odpowiedź brzmi: rekordy domen. Informują one Internet o lokalizacji, do której powinien wysyłać ruch internetowy. Najpopularniejsze rekordy to rekordy A, rekordy CNAME, rekordy TXT, rekordy serwerów NS i rekordy MX. Innymi słowy, rekordy nazw domen służą jako książka kontaktowa dla Internetu,

która przechowuje indywidualne adresy. Rozróżnienia opierają się na konwersji języka ludzkiego na język maszynowy znany komputerom w postaci adresów IP. Na przykład, możesz nie zapamiętać numerów osób w swojej książce telefonicznej, ale znasz ich imiona i nazwiska, szukasz tylko imienia i nazwiska, a numer wyskakuje. Tak właśnie działają rekordy domen w Internecie. Dlatego też, gdy wyszukujesz witrynę w przeglądarce, twój gadżet wykorzysta rekordy domeny do identyfikacji adresu IP domeny.

.

Do celów związanych z pocztą e-mail będziemy potrzebować tylko kilku z nich:

- Rekord lub rekordy wskazujące na właściwy adres IP serwera poczty e-mail
- Rekord MX do zdefiniowania domeny, w której przetwarzana jest wiadomość e-mail
- Rekordy TXT do konfiguracji DKIM, SPF i DMARC
- Rekordy SRV ułatwiające konfigurację poczty e-mail

Rekordy A i MX są absolutnie niezbędne, aby podstawowa konfiguracja poczty e-mail działała. Jednak bez DKIM, SPF i DMARC wiele serwerów pocztowych odrzuci Twoje wiadomości. SRV jest opcjonalny, ale zalecany – pomoże użytkownikom końcowym w półautomatycznym konfigurowaniu klientów poczty e-mail.

Rekordy MX i A są absolutnie niezbędne do podstawowej konfiguracji poczty e-mail.

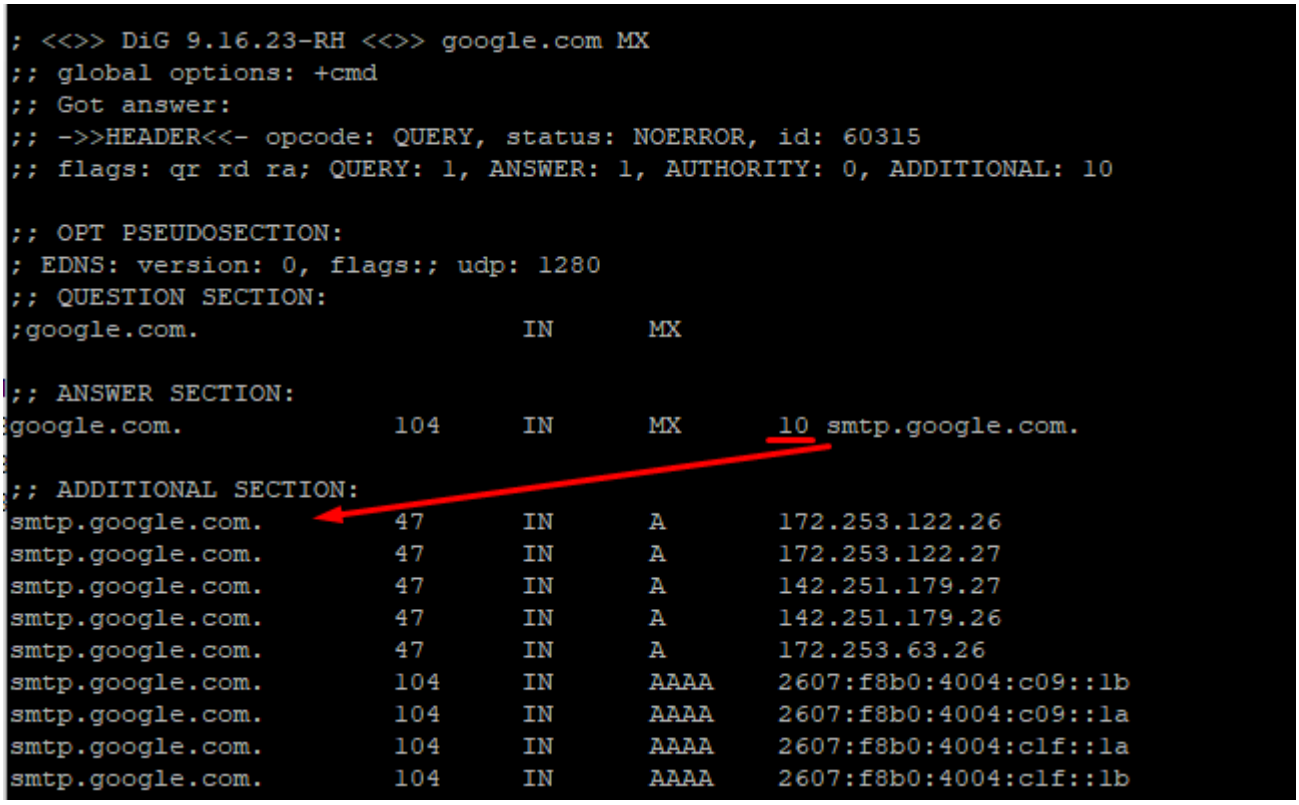
MX i rekordy A – podstawa konfiguracji poczty e-mail

MX jest skrótem od Mail Exchange Record. Jest on odpowiedzialny za identyfikację poszczególnych serwerów, które odbierają wiadomości e-mail dla nazw domen. Innymi słowy, to rekordy MX są ważne w dostarczaniu wiadomości e-mail na Twój adres. Mówiąc wprost, rekordy MX służą do informowania światowych serwerów pocztowych, które akceptują pocztę dla określonej domeny, a także pokazują, gdzie kierowane są wiadomości e-mail wysyłane do domeny. Rekord MX jest zatem wpisem w DNS, który wskazuje serwerowi wysyłającemu, gdzie wysłać wiadomość e-mail.

Jeśli chcesz sprawdzić rekordy MX w systemie Windows, otwórz Wiersz poleceń

systemu Windows. Po uruchomieniu terminala należy wpisać „nslookup” i nacisnąć „Enter”. Zostaniesz poproszony o wpisanie nazwy domeny. W tym momencie rekord MX zostanie wyświetlony po naciśnięciu klawisza „Enter”.

W systemie Linux, w celu identyfikacji, można to osiągnąć za pomocą narzędzia dig z wiersza poleceń systemu Linux. Przykładowy wynik *dig google.com MX* będzie wyglądał następująco:



W obu przypadkach pytamy *Internet* (technicznie: domyślny DNS dostarczony przez dostawcę usług internetowych lub wybrany ręcznie) *jaki jest rekord MX w domenie google.com?*. W rezultacie otrzymujesz nie adres IP, ale raczej nazwę: *smtp.google.com* – ale potem jest dodatkowa sekcja. W tej dodatkowej sekcji znajdują się 4 adresy IPv4, na które faktycznie wskazuje domena *smtp.google.com*. Strzałka na zrzucie ekranu wizualizuje ten pomysł. Zamiast wskazywać na rekord A, rekord MX może wskazywać na rekord CNAME, ale ostatecznie, jeśli podążysz za rekordem CNAME, skończysz z kolejnym rekordem A, który wskazuje na adres IP – czyli to, czego ostatecznie szukamy.

Klucz SPF i jego szczegóły

Spamerzy są wszędzie w Internecie. Mogą oni próbować swoich działań poprzez wysyłanie spamu w imieniu domeny. Aby temu zapobiec, SPF jest używany do nadawania uprawnień do wysyłania wiadomości e-mail tylko dla określonych serwerów. Dlatego SPF jest techniką stosowaną do ochrony domen przed niezweryfikowanymi wiadomościami e-mail, które rzekomo zostały wysłane w ich imieniu. Dodatkowo, dzięki wykorzystaniu SPF, firma może wymienić zweryfikowane i prawidłowe serwery e-mail. Pierwotnie SPF był znany jako „Sender Permitted From”, jednak z czasem zmienił się na „Sender Policy Framework”.

Niemniej jednak, świat był świadkiem ogromnego postępu od czasu SPF, skutkującego ulepszeniami takimi jak DMARC i DKIM, ale SPF nadal odgrywa ważną rolę w określaniu zgodności poczty elektronicznej. W tym przypadku, jednym ze znaczeń rekordu SPF jest to, że zapobiega on fałszerstwom wiadomości e-mail, więc dodając SPF do swojej domeny jesteś chroniony przed ingerencją innych osób w Twoją domenę.

.

Serwer odbierający porównuje rekord domeny SPF z domeną z otrzymanej wiadomości e-mail. Jeśli zauważy jakiekolwiek niedopasowanie i rozbieżności, filtruje je i jednocześnie oznacza jako nieautoryzowane, odrzucając je lub oznaczając jako spam. W przykładzie:

> v=spf1 a mx include:send.sailingbyte.com ip4:188.68.224.153 -all

Całe wyjaśnienie można znaleźć w świetnym narzędziu – mxtoolbox Sailing Byte sample – ale w skrócie ten rekord mówi, jakie rekordy są uwierzytelniane (A, MX, dodatkowa domena i dodatkowy adres IP) i co powinien zrobić serwer docelowy, jeśli wystąpi niezgodność (-all oznacza, że należy go odrzucić). Tak więc, główną informacją jest to, że klucze SPF zawierają listę wszystkich autentycznych adresów IP (lub rekordów domen), które mogą wysyłać wiadomości e-mail w imieniu Twojej domeny.

DKIM i zawarte w nim informacje

Jest to kolejna metoda uwierzytelniania wiadomości e-mail, która pozwala wykrywać niezweryfikowane wiadomości e-mail i pomaga serwerom oznaczać je jako spam lub nieautoryzowane. W rzeczywistości ma ona na celu identyfikację poczty pochodzącej z serwera posiadającego klucz szyfrujący. Aby Domain Keys Identified Mail mógł osiągnąć swój cel, wykorzystuje koncepcję znaną jako Digital Signature affixation przy użyciu kryptografii klucza publicznego.

Kryptografia klucza publicznego wykorzystuje dwa uzupełniające się klucze: jeden klucz nazywany jest *prywatnym* i powinien być zawsze bezpieczny. Jest on używany do podpisywania oryginalnych wiadomości lub odszyfrowywania wiadomości przychodzących, które zostały zaszyfrowane przy użyciu klucza publicznego. Drugi klucz to *publiczny* – jest on używany do weryfikacji podpisu lub do szyfrowania wiadomości, które mogą być odszyfrowane tylko za pomocą klucza prywatnego.

Kiedy serwer nadawcy otrzymuje żądanie wysłania wiadomości e-mail w imieniu użytkownika, używa klucza prywatnego do podpisania wiadomości i dodaje podpis cyfrowy do nagłówków wiadomości e-mail. Informacje w nagłówku zawierały części wartości znacznika, takie jak „d=” w przypadku domeny podpisującej i „b=” dla rzeczywistego podpisu. Teraz, gdy serwer odbierający chce zweryfikować tę wiadomość, może użyć znanego klucza publicznego (który jest przechowywany w rekordzie TXT domeny, więc jest dostępny dla wszystkich), aby zweryfikować podpis cyfrowy zawarty w nagłówkach wiadomości e-mail. Tak więc weryfikując podpis na otrzymanej wiadomości e-mail, mogą potwierdzić autentyczność wiadomości e-mail jako ważnie wysłanej od nadawcy lub określonej domeny. Dodatkowo jest to dowód na to, że treść wiadomości e-mail nie została naruszona, ponieważ podpis został dołączony. W związku z tym DKIM umożliwia zatwierdzenie wiadomości za pomocą podpisu i zapewnia platformę dla organizacji wysyłającej do udostępniania informacji o tym, które wiadomości e-mail są autentyczne lub zgodne z prawem.

Nie wyróżnia jednak nadużyć ani ich nie ujawnia. Znaczenie DKIM na poziomie organizacyjnym polega na stworzeniu podstawy do domagania się odpowiedzialności za wiadomości e-mail wysyłane przez użytkowników. Jeśli jednak masz złośliwych użytkowników, którzy używają Twojego serwera pocztowego do wysyłania uwierzytelnionych wiadomości e-mail do wielu odbiorców, powinieneś być w stanie zidentyfikować takich użytkowników albo poprzez użycie odpowiednich rekordów DMARC (opisanych poniżej), albo poprzez dostosowanie ustawień i limitów

dla wiadomości wychodzących (co jest poza zakresem tego artykułu).

Co to jest DMARC?

A do czego służy rekord DMARC?

Do niedawna rekord DMARC nie był zbyt szeroko stosowany, ale coraz więcej serwerów pocztowych wymaga jego obecności, aby faktycznie dostarczać wiadomości e-mail, a nie je blokować. DMARC jest rodzajem informacji raportującej: więc jeśli serwer pocztowy otrzyma sfałszowaną wiadomość e-mail, może wysłać automatyczny raport do postmastera (właściciela domeny lub wyznaczonego administratora serwera pocztowego) mówiący „uważaj, są spamerzy próbujący użyć twojej domeny” lub „uważaj, niektórzy z twoich użytkowników wysyłają wiadomości spamowe”. Z jednej strony warto więc mieć taką pocztę. Z drugiej strony, może się z tym wiązać wiele informacji technicznych, a w rekordzie DMARC na pewno NIE powinien znajdować się Twój prywatny adres – ponieważ rekordy DMARC są dostępne przez Internet bez żadnych zabezpieczeń. Przykład DMARC wyglądałby następująco:

```
v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com
```

.

Z tego powodu możesz chcieć zautomatyzować niektóre z tych raportów. Może przepływ automatyzacji N8N DMARC byłby dobrą rzeczą do wypróbowania?

SRV i inne rekordy do automatyzacji konfiguracji poczty e-mail

Rekordy SRV lub rekordy zasobów lokalizacji usług (DNS SRV) odgrywają kluczową rolę w automatyzacji procesu konfiguracji poczty e-mail. Te wpisy DNS dostarczają informacji o usługach dostępnych w domenie i określają, jak do nich dotrzeć. Na przykład, podczas konfigurowania serwera SMTP do wysyłania wiadomości e-mail, administrator może wykorzystać rekordy SRV do automatycznego wykrywania odpowiednich serwerów pocztowych bez ręcznego określania adresów IP lub portów. Przykładem takiego rekordu SRV może być:

_smtp._tcp.example.com IN SRV 10 5 443 smtpserver1.example.com

co wskazuje, że istnieje usługa SMTP dostępna na porcie TCP 443 w `smtpserver1.example.com`. Podobnie, w przypadku odbierania wiadomości e-mail za pośrednictwem protokołów IMAP lub POP3, można zdefiniować odpowiednie rekordy SRV w celu usprawnienia procesu konfiguracji. Taka automatyzacja nie tylko zmniejsza liczbę błędów konfiguracji, ale także zwiększa skalowalność i łatwość konserwacji w dużych infrastrukturach poczty e-mail. Dla działu IT jest to bardzo wygodne, ponieważ użytkownicy końcowi (używający na przykład Thunderbirda, którego zdecydowanie polecam) automatycznie wykryją ustawienia serwera – a użytkownicy muszą jedynie podać adres e-mail i hasło.

.

Oprócz usług SMTP, rekordy SRV są równie korzystne do konfigurowania innych usług związanych z pocztą, takich jak przesyłanie (dla bezpiecznych zgłoszeń), zarządzanie (dla zadań administracyjnych) i mechanizmy uwierzytelniania, takie jak OAuth2 lub SASL. Przykładowo, administrator może zdefiniować *_submission._tcp.example.com IN SRV 10 5 587 smtpserver2.example.net*, aby określić serwer do bezpiecznego przesyłania wiadomości e-mail przez TLS na porcie 587. Takie podejście zapewnia, że wszystkie klienty poczty e-mail i serwery w domenie mogą automatycznie wykrywać i łączyć się z odpowiednimi usługami, zwiększając niezawodność i wygodę użytkownika. Co więcej, wykorzystując rekordy SRV w połączeniu z DNSSEC (Domain Name System Security Extensions), organizacje mogą dodać dodatkową warstwę zabezpieczeń do swojej infrastruktury pocztowej, chroniąc przed atakami typu man-in-the-middle i zapewniając, że tylko autoryzowani klienci mają dostęp do serwerów poczty e-mail.

.

Podobnie można skonfigurować rekord autodiscover. Należy utworzyć rekord DNS (zazwyczaj CNAME lub rekord A) wskazujący na usługę dostawcy poczty e-mail. Pozwala to klientom poczty e-mail, takim jak Microsoft Outlook, automatycznie zlokalizować ustawienia niezbędne do połączenia się z serwerem poczty.

Podsumowanie – jak konfiguracja domeny wpływa na działalność firmy

Ważne jest, aby częściej korzystać z SPF i DKIM, zwłaszcza jeśli jesteś organizacją, która wysyła komercyjne dane transakcyjne za pośrednictwem poczty. Posiadanie SPF i DKIM ma kluczowe znaczenie dla utrzymania dobrych relacji z klientami. Dzięki temu mogą oni postrzegać Cię jako poważnego partnera biznesowego, który chroni ich przed stratami i niedogodnościami spowodowanymi przez spoofing i oszustów. Poszczególni menedżerowie i administratorzy poczty mogą mieć własne zasady i przepisy. Jeśli jednak jesteś poważną organizacją ze standardowymi protokołami e-mail, SPF i DKIM są integralną częścią twoich operacji biznesowych. Zrozumienie bezpieczeństwa i autentyczności systemów jest częścią zrozumienia potrzeb nazwy domeny i wszystkiego, co domeny zawierają. Możesz polegać na Sailing Byte, aby uzyskać więcej pomocy nie tylko w zabezpieczaniu domeny, ale także wszystkiego, co dotyczy systemów domenowych.