> Mechanizmy weryfikacji nadawcy wiadomości _

28 października 2021 | Marcin Dudek(../../../../author/marcin-dudek/), Michał Praszmo(../../../../author/michal-praszmo/) | #bezpieczeństwo(../../../../tag/bezpieczenstwo/), #dns(../../../../tag/dns/), #poczta(../../../../tag/poczta/)

> W serwisie https://bezpiecznapoczta.cert.pl(https://bezpiecznapoczta.cert.pl) można zweryfikować poprawność implementacji mechanizmów weryfikacji nadawcy poczty w Państwa domenie.

W tym roku mija 50. rocznica przesłania pierwszej wiadomości email. Na początku lat 70., gdy projektowane były stojące za tym mechanizmy, niestety mało kto myślał o bezpieczeństwie informacji, a kluczowymi kwestiami były stabiloność i prostota.

Skrzynka pocztowa obecnie jest centrum życia większości z nas, wykorzystywana zarówno w sferze biznesowej, jak i prywatnej. Wraz ze zwiększonym wykorzystaniem pojawiła się potrzeba na zapewnienie lepszego poziomu bezpieczeństwa zarówno samej skrzynki, treści wiadomości, jak i mechanizmów jej przesyłania. W tym artykule skupiamy się na tym ostatnim, bo okazuje się, że mimo upłynięcia 50 lat, podszywanie się pod nadawcę wiadomości jest nadal jedną z podstawowych technik wykorzystywaną przy atakach socjotechnicznych.

Przykładowo, w czerwcu 2021 r. została wykorzystana błędna konfiguracja mechanizów SPF oraz DMARC dla domeny `sej.pl`, w wyniku czego na skrzynki sejmowe zostały dostarczone maile phishingowe, wykorzystujące jej podobieństwo do domeny `sejm.pl`.

Źródło:
https://twitter.com/radekfogiel/status/1404752636868534279(https://twitter.com/radekfogiel/status/1404752636868534279)

Przez lata powstawały kolejne standardy i mechanizmy, które miały spowodować, że będzie to trudniejsze. Niestety liczba możliwości ich konfiguracji oraz ich wariantów doprowadziła do tego, że bardzo często są nieużywane albo skonfigurowane niepoprawnie.

W artykule postaramy się wytłumaczyć działanie trzech podstawowych mechanizmów mających na celu weryfikację nadawcy wiadomości: SPF, DKIM i DMARC, oraz spróbujemy obalić kilka powstałych mitów z nimi związanych.

SPF (Sender Policy Framework) – RFC7208(https://tools.ietf.org/html/rfc7208)

Mechanizm ten pozwala właścicielowi domeny zdefiniować adresy IP serwerów uprawnionych do wysyłki maili w imieniu tej domeny. Sprawdzenie odbywa się na podstawie domeny obecnej w polu `MAIL FROM` wg. RFC5321 – `RFC5321.MailFrom`, znane też jako `Envelope-Sender`. Należy jednak pamiętać, że zawartość pola `MAIL FROM` może nigdy nie pojawić się w nagłówku widocznym w klientach pocztowych takich jak MS Outlook czy Thunderbird.

Uwaga!

SPF samodzielnie nie sprawdza pola *From* wyświetlanego w klientach pocztowych – `RFC5322.From`, a jedynie `RFC5321.MailFrom`. SPF może przejść sprawdzenia poprawnie, nawet gdy pole *From* jest fałszywe. **W prostych słowach, SPF nie chroni przed popularnym w atakach spoofingiem wyświetlanego adresu mailowego.** Wyjątkiem od tego jest dodatkowe poprawne skonfigurowanie mechanizmu DMARC.

Implementacja techniczna SPF

SPF jest definiowany w rekordzie TXT domeny która ma być chroniona. Serwer pocztowy, który otrzymuje wiadomość, wysyła zapytanie o rekord SPF dla domeny z pola `MAIL FROM` (`RFC5321.MailFrom`), a następnie go analizuje.

O rekord TXT możemy odpytać np. narzędziem *dig* i przefiltrować narzędziem *grep* pod kątem rekordu SPF. Poniżej przykład takiego zapytania dla domeny `nask.pl` :

```
dig txt nask.pl | grep 'v=spf1'
```

W odpowiedzi otrzymamy rekord SPF. W kolejnym podrozdziale zostaną opisane poszczególne jego składowe.

```
nask.pl. 600 IN TXT "v=spf1 include:_spf.nask.pl include:_spf2.nask.pl
ip4:195.187.245.33/24 ip4:193.59.201.32/27 ip4:193.59.201.64/27
ip4:193.59.201.238/32 ip4:195.187.242.0/24 ip4:193.59.204.167/32
ip4:194.181.0.106 ip4:194.181.0.102 ip4:195.187.6.28 -all"
```

Serwer pocztowy, który otrzymał wiadomość, sprawdza czy adres IP, z którego wiadomość została nadana, zawiera się na ostatecznej (po rozwiązaniu wszystkich składowych) liście dozwolonych adresów IP w rekordzie SPF. Jeśli nie, to zależnie od konfiguracji serwera pocztowego (lub konfiguracji mechanizmu DMARC(link do nagłowka w tekscie)), wiadomość może zostać odrzucona albo przeniesiona do spamu.

Uwaga!

Zachowanie serwera pocztowego, do którego dotarła wiadomość niepoprawna według mechanizmu SPF, zależy od jego konfiguracji. Możliwe jest, że mimo błędnej weryfikacji SPF, wiadomość dotrze do adresata.

Struktura rekordu SPF

Rekord SPF zaczyna się od stałego fragmentu `v=spf1` i składa się z dyrektyw opisujących oczekiwane zachowanie. W każdej regule kwalifikator określa co powinno się stać w sytuacji, gdy dopasuje się do hosta próbującego przekazać wiadomość.

Dostępne kwalifikatory to:

Kwalifikator	Nazwa	Opis
-	Fail	Odrzuć
~	Softfail	Rekomenduj odrzucenie
+	Pass	Akceptuj
?	Neutral	Nic nie sugeruj (Neutralne)

Jeśli dana dyrektywa nie posiada kwalifikatora, to przyjmowana jest wartość domyślna `Pass(+)`

Typy dyrektyw (ang. *mechanisms*) opisane są w piątym rozdziale RFC(https://datatracker.ietf.org/doc/html/rfc7208#section-5). Każda z nich pozwala na określenie warunków, które powinny się spełnić, żeby całe sprawdzenie przebiegło pomyślnie.

- `include:_spf.nask.pl` - dyrektywa dopasuje się **tylko** jeśli rekord SPF podanej domeny zwróci wynik `Pass(+)`. W prostych słowach, rekord SPF dla podanej domeny (w przykładzie "_spf.nask.pl") jest również uwzględniany w sprawdzeniach.
- `a:google.com` - domena jest rozwiązywana i jej rekord A jest porównywany z IP nadawcy. Gdy użyte jest samo `a`, sprawdzany jest rekord A domeny, dla której aktualnie weryfikowana jest polityka.
- `mx:google.com` - rekordy A dla rekordów MX podanej domeny dodawane są jako IP uprawnione do wysyłki. Gdy użyte jest samo `mx` sprawdzany jest rekord MX domeny, dla której aktualnie weryfikowana jest polityka.
- `ip4:195.187.245.33/24` - adres IPv4 lub zakres adresacji, który ma zostać porównany z IP nadawcy.
- `ip6:2001:db8::cd30` - adres IPv6 lub zakres adresacji, który ma zostać porównany z IP nadawcy.
- `exists:<domena>` - pozwala na dynamiczne skonstruowanie nazw domen za pomocą makr(https://datatracker.ietf.org/doc/html/rfc7208#section-7). Dopasowuje się w przypadku, gdy odpowiedź DNS zwróci przynamniej jeden rekord A.
- `all` - dyrektywa dopasowująca się do każdego adresu, zazwyczaj jest ustawiana na końcu rekordu SPF jako wartość domyślna z kwantyfikatorem `Fail(-)` – odrzuć, jeśli nie pasuje do poprzednich dyrektyw.

W sytuacji, gdy nie dopasuje się żadna dyrektywa, to domyślnie zwracanym wynikiem jest "neutral". Tak skonstruowany rekord nie podnosi jednak poziomu bezpieczeństwa w przypadku prób podszywania się. Dlatego sugerowanym rozwiązaniem jest umieszczenie zawsze na końcu rekordu dyrektywy `-all` (Fail) lub `~all` (Softfail).

> **Uwaga!**
>
> W wielu miejscach RFC znajdziemy informacje o tym, że jakieś zachowanie serwera pocztowego jest rekomendowane, a nie wymagane. Trzeba pamiętać, że różne serwery pocztowe odbiorcy mogą różnie interpretować otrzymany rekord SPF. Np. wiele serwerów traktuje `-all` oraz `~all` tak samo.

Ograniczenia dla reguł SPF: Maksymalna długość rekordu to 255 znaków i maksymalnie 10 rozwiązań domen (rozwiązania występują przy tagach: `a`, `mx`, `ptr`, `include`, `exists`), wliczając w to rozwiązania rekursywne.

DKIM (DomainKeys Identified Mail) – RFC6376(https://tools.ietf.org/html/rfc6376)

Jest to kolejny mechanizm, który ma za zadanie utrudnić podszywanie się pod nadawcę wiadomości email, ale także ingerowanie w jej treść. Daje możliwość wzbogacenia wiadomości o podpis kryptograficzny z body, nagłówka From, czy innych wybranych pól. Serwer odbiorcy może zweryfikować autentyczność wiadomości wykorzystując kryptografię asymetryczną oraz klucz publiczny odczytany z odpowiedniego rekordu DNS sprawdzanej domeny.

Podpis jest dodawany do nagłówka wiadomości jako pole `DKIM-Signature`, na przykład:

```
DKIM-Signature:
v=1; a=rsa-sha256; c=relaxed/relaxed; d=ncas.us-cert.gov; s=15q3; i=@ncas.us-cert.gov; h=
Content-Type:x-subscriber:X-Accountcode:Errors-To:MIME-Version:
Message-ID:X-ReportingKey:Subject:Date:To:Reply-To:From; bh=bqWW
VsSFeYnMUseujsFFol8xU8ZRNz18EBcFtuxI91c=; b=hjQjcCOi/CzTr1STuUnN
digjN5gW2Wr81UR2CBKpwUV8MqYNlZV76YuGdX+T ...
```

Opis ważnych pól które mogą wystąpić w takich nagłówkach:

- `d=` - domena, którą należy odpytać o klucz publiczny do odszyfrowania podpisu
- `s=` - selector wskazujący, który z opublikowanych kluczy publicznych ma być użyty
- `h=` - jakie pola nagłówka zostały podpisane i mają zostać sprawdzone
- `bh=` - hash treści wiadomości
- `a=` - algorytm, który został użyty do wyliczenia hasha (podpisu)
- `b=` - zaszyfrowany podpis (hash wyliczony przez wysyłającego)

Klucz publiczny jest umieszczany w rekordzie TXT subdomeny zbudowanej z pól Selectora i Domeny nagłówka `DKIM-Signature`. Np. `15q3._domainkey.ncas.us-cert.gov` Gdzie `15q3` jest wartośćią pola `s`, `ncas.us-cert.gov` wartością pola `d`, a `_domainkey` stałe.

Po pobraniu klucza publicznego, pole `b` jest odszyfrowywane i otrzymany hash jest używany do weryfikacji zgodności podpisu. Odbywa się to poprzez wyliczenie nowego hasha z aktualnego body oraz nagłówków i porównaniu go z otrzymanym.

> **Uwaga!**
>
> DKIM sam w sobie nie ma mechanizmów sugerowania co zrobić z wiadomością z niezgodnym podpisem, mimo że niektóre serwery pocztowe mogą to na różne sposoby interpretować. Aby świadomie wskazać co zrobić z taką wiadomością potrzebny jest mechanizm DMARC.

DMARC (Domain-based Message Authentication, Reporting & Conformance) – RFC7489(https://tools.ietf.org/html/rfc7489)

Dopełniającym dwa opisane wcześniej mechanizmy jest DMARC. Stanowi on zestaw reguł budowanych na bazie SPF i DKIM pozwalających zdecydować czy wiadomość faktycznie przyszła od wysyłającego za którego się podaje. Jako centralny punkt odniesienia bierze pole `RFC5322.From` (widoczone w klientach pocztowych). Posiada też możliwość raportowania wykrytych nieprawidłowości.

DMARC opiera się na dwóch kategoriach sprawdzeń:

- Dla SPF - Czy dla otrzymanej wiadomości reguła SPF przeszła sprawdzenia **ORAZ** czy `RFC5321.MailFrom` zgadza się z `RFC5322.From` (czy pole sprawdzane przez SPF zgadza się z

tym wyświetlanym w klientach). Dla ustawienia *relax* dowolne z pól może być subddomeną, dla *strict* domeny muszą być dokładnie takie same.
- Dla DKIM - Czy otrzymana wiadomość jest poprawnie podpisana wg. DKIM **ORAZ** czy wartość w polu `d=` nagłówka DKIM zgadza się z `RFC5322.From`. Dla ustawienia *relax* dowolne z pól może być subddomeną, dla *strict* domeny muszą być dokładnie takie same.

Dowolne z dwóch kategorii sprawdzeń (SPF **LUB** DKIM) musi się zakończyć sukcesem, żeby sprawdzenie DMARC zostało uznane za sukces. Dobrze obrazuje to następujące równanie logiczne:

```
DMARC authentication pass =
(SPF authentication pass AND SPF identifier alignment)
OR
(DKIM authentication pass AND DKIM identifier alignment)
```

Implementacja techniczna DMARC

W momencie, gdy przychodzi email, serwer odbiorcy bierze domenę z nagłówka `RFC5322.From`, a następnie sprawdza rekord TXT dla subdomeny `_dmarc` tej domeny. Np. w przypadku, gdy email przychodzi z domeny `wydzial.przykladowauczelnia.edu.pl`, odpytana zostanie domena `_dmarc.wydzial.przykladowauczelnia.edu.pl`.

Jeśli nie ma tam poprawnego rekordu, znajdowany jest **Public Suffix**, w którym znajduje się badana domena. **Public Suffix** to taka domena, w której wiele niezależnych organizacji może zarejestrować własną subdomenę. W tym przypadku jest to domena `edu.pl`. Następnie serwer odbiorcy sprawdza rekord DMARC domeny bezpośrednio poniżej **Public Suffix**, czyli w tym przypadku `przykladowauczelnia.edu.pl` - więc kolejne zapytanie o rekord TXT zostanie wykonane do domeny `_dmarc.przykladowauczelnia.edu.pl`.

Dzięki temu wystarczy skonfigurować rekord DMARC na domenie bezpośrednio poniżej **Public Suffix** (będzie to ta domena, którą organizacja zakupiła od rejestratora domen).

W rekordzie DMARC umieszczony jest wpis definiujący reguły dopasowania, tzn. co zrobić z wiadomością, gdy nie zostanie spełnione któreś ze sprawdzeń, oraz gdzie wysyłać raporty.

Podobnie jak przy SPF możemy o ten rekord odpytać np. przy użyciu narzędzia *dig*:

```
dig +short txt _dmarc.google.com
```

W odpowiedzi otrzymamy rekord DMARC:

```
"v=DMARC1; p=reject; rua=mailto:mailauth-reports@google.com"
```

Opis ważnych pól, które możemy spotkać w takich rekordach:

- `v=` - wersja protokołu, obecnie musi być `DMARC1`
- `rua=` - lista adresów, na które mają przyjść raporty ze sprawdzeń, opisana w formacie `mailto:<adres email>`. W przykładzie `mailauth-reports@google.com`
- `adkim=` - ustawienia restrykcyjności dla sprawdzeń dopasowania DKIM – `r` (relaxed) lub `s` (strict). W *relaxed* porównywane są tylko domeny narzędne (dopuszczalne są subdomeny).

Domyślnie *relaxed*.

- `aspf=` - ustawienia restrykcyjności dla sprawdzeń dopasowania SPF – `r` (relaxed) lub `s` (strict). W *relaxed* porównywane są tylko domeny narzędne (dopuszczalne są subdomeny). Domyślnie *relaxed*.
- `p=` (polityka) - co ma się stać z wiadomością która nie przejdzie sprawdzeń, możliwe opcje:

Opcja dla `p=`	Opis
none	nie są podejmowane żadne akcje, tylko raportowanie
quarantine	wiadomość powinna zostać przeniesiona do spamu
reject	wiadomość powinna być odrzucona

Rekomendujemy ustawienie polityki `quarantine` lub `reject`, aby zalecić serwerowi odbiorcy by potraktował niepoprawnie zweryfikowaną wiadomość jako spam (`quarantine`) lub ją odrzucił (`reject`).

Więcej możliwych pól można znaleźć w standardzie opisującym mechanizm DMARC. (https://datatracker.ietf.org/doc/html/rfc7489#section-6.3)

Uwaga!

Ustawienia DMARC są jedynie wskazówką dla serwera pocztowego odbierającego wiadomość, nie są obligatoryjne. Jednak większość serwerów weźmie je pod uwagę.

Uwaga!

Mechanizm DMARC powinien być implementowany stopniowo, z początkowymi ustawieniami reakcji na `none`, ale z włączonymi raportami. Na bazie analizy otrzymywanych raportów z sytuacji gdzie sprawdzenie się nie powiodło należy poprawiać konfiguracje usług wysyłających maile. Nagłe włączenie DMARC z ustawieniem `quarantine` lub `reject` może spowodować, że ważne procesy biznesowe, o których nie pomyśleliśmy, np. newsletter u zewnętrznego dostawcy, mogą przestać działać.

Ustawienia dla domen niesłużących do wysyłki poczty

Warto zaznaczyć, że nawet jeśli nie planujemy używać danej domeny do wysyłania maili, to i tak warto dla niej skonfigurować rekordy SPF oraz DMARC. Ktoś może podszywać się pod naszą domenę, mimo że nie mamy w niej żadnej skrzynki pocztowej. Prosta reguła SPF w postaci `v=spf1 -all` oraz DMARC w postaci `v=DMARC1; p=reject; adkim=s; aspf=s;` znacznie to utrudni.

Podsumowanie

Mimo że podstawowe założenia działania poczty są proste, to dodatkowe mechanizmy bezpieczeństwa jak SPF, DKIM czy DMARC mogą przysporzyć kłopotu. W szczególności gdy musimy poprawnie skonfigurować nasz serwer pocztowy albo rozstrzygnąć, czy dana wiadomość została faktycznie wysłana z adresu, za który się podaje.

W kolejnym artykule opiszemy coś, z czym spotykamy się na co dzień. Na przykładzie konkretnego maila i jego nagłówków pokażemy, jak sprawdzić, skąd przyszła wiadomość email i jaki jest jej faktyczny nadawca.

CERT Polska to zespół działający w strukturach NASK - Państwowego Instytutu Badawczego, powołany w 1996 roku do reagowania na incydenty bezpieczeństwa komputerowego. Realizuje zadania CSIRT NASK,

CERT Polska w social mediach

Facebook(https://www.facebook.com/CERT.Polska/)

X(https://x.com/CERT_P

Kontakt

ul. Kolska 12, 01-045 Warszawa
ePUAP: /NASK-Instytut/SkrytkaESP
e-Doręczenia: AE:PL-60057-61611-BCEGR-11

e-mail: info@cert.pl(mailto:info@cert.pl)
Zgłaszanie incydentów: incydent.cert.pl(https://incydent.cert.pl/)
cert@cert.pl(mailto:cert@cert.pl)

jednego z trzech takich zespołów działających na poziomie krajowym w ramach krajowego systemu cyberbezpieczeństwa.

olska)

LinkedIn(https://www.linkedin.com/showcase/cert-polska)

GitHub(https://github.com/CERT-Polska)

Współfinansowane przez instrument Unii Europejskiej „Łącząc Europę”