code_purple
CYBERSECURITY EXPERTS

nanio gmbh | Moosweg 24 | 5606 Dintikon
rhino@codepurple.ch | https://codepurple.ch | +41 79 823 45 30

SPF / DMARC Analyse von .ch und .li Domains

Autor: Thomas Federer
Veröffentlicht am: 4. April 2022

TLDR; Intro / Management Summary

E-Mail wird im Geschäftsleben jeden Tag verwendet. So ist es nicht erstaunlich, dass über 91% aller Cyberangriffe mit einem Phishing-E-Mail beginnen. Als das E-Mail-Protokoll entwickelt wurde, waren die Anforderungen an die Sicherheit ganz anders als heute. Am SMTP-Protokoll hat sich seit 1995 nicht mehr viel verändert. Um die neuen Probleme bezüglich Spam und Missbrauch in den Griff zu bekommen, wurden weitere Technologien wie SPF, DKIM und DMARC entwickelt. Inzwischen sind auch diese Technologien mehrere Jahre alt. Eine Analyse von Codepurple im Februar 2022 aller .ch und .li Domains zeigt auf, dass diese Technologien oft nicht verwendet oder falsch konfiguriert werden, obwohl sie das Potential für einen guten Schutz hätten.

E-Mail

Im heutigen Geschäftsleben sind E-Mails nicht mehr wegzudenken. Nahezu alle Mitarbeitende eines Unternehmens verwenden E-Mail praktisch täglich.

Wann das erste E-Mail versandt wurde, hängt von der Definition ab, was ein E-Mail ist. Die ersten digitalen Meldungen wurden bereits vor über 50 Jahren zwischen Computern ausgetauscht.

E-Mails können heute auf praktisch allen Geräten, welche mit dem Internet verbunden sind, empfangen, versendet und gelesen werden. Oft ist die notwendige Software, ein sogenannter E-Mail-Client, bereits vorinstalliert und muss nur noch konfiguriert werden.

Probleme

Über 91% aller Cyberangriffe beginnen mit einem Phishing-E-Mail[1]. Die einen kommen plump daher und sind für den Laien einfach erkennbar. Die anderen sind professionell umgesetzt und spezifisch für eine bestimmte Person erstellt worden (Spear-Phishing).

Als das E-Mail-Protokoll SMTP[2] (Simple Mail Transfer Protokoll) entwickelt wurde, waren die Sicherheitsanforderungen im Internet ganz anders als heute. So erlaubt das SMTP Protokoll, dass jeder E-Mails im Namen von jeder beliebigen Person versenden kann. Mit Hilfe von Frameworks und Richtlinien können moderne Spamfilter solche gefälschten E-Mails zuverlässig erkennen und als Spam markieren.

Wichtig ist jedoch, dass diese Frameworks und Richtlinien eingesetzt und korrekt konfiguriert werden.

Diese Analyse konzentriert sich auf folgende drei Technologien: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) und DMARC (Domain-based Message Authentication Reporting and Conformance). Jede dieser Technologien funktioniert über Einträge im DNS (Domain Name System). So kann der Domaininhaber die Einstellungen kontrollieren und empfangende Server können diese Informationen lesen. Die Einstellungen im DNS-Server werden als vertrauenswürdig angesehen, da diese nur vom Domain-Inhaber kontrolliert werden können.

Vor zwei Jahren hat das National Cyber Security Center (NCSC) des Bundes bereits eine Analyse gemacht, welche unter https://www.govcert.admin.ch/blog/security-of-the-swiss-domain-landscape-cctld-ch/ frei verfügbar ist. Die Analyse des NCSC beschränkte sich auf die Verwendung der Technologien, aber nicht auf deren Konfigurationen und Einstellungen.

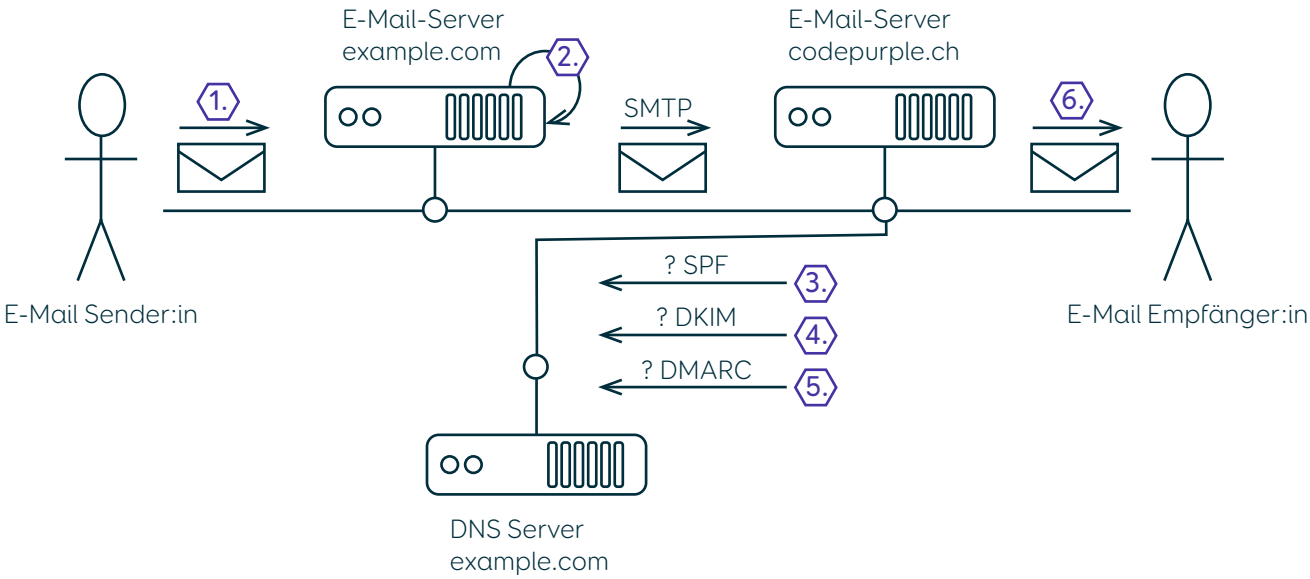
Um zu verstehen, welche Technologie wie und wo ansetzt, gilt es, die Struktur eines E-Mails zu verstehen.

In der folgenden Abbildung wird der Versand eines E-Mails vom Versender bis zum Empfänger vereinfacht dargestellt.

Quellen:
1) https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing
2) https://datatracker.ietf.org/doc/html/rfc2821

code_purple
CYBERSECURITY EXPERTS

nanio gmbh | Moosweg 24 | 5606 Dintikon
rhino@codepurple.ch | https://codepurple.ch | +41 79 823 45 30



Ablauf Versand eines E-Mails

1. Der/Die Sender:in versendet ein E-Mail von test@example.com an rhino@codepurple.ch.

2. Der E-Mail-Server von @example.com errechnet die DKIM Signatur und fügt diese dem E-Mail-Header hinzu.

3. Der E-Mail-Server des/der Empfängers:in @codepurple.ch überprüft beim DNS-Server von example.com mit Hilfe des SPF-Eintrages, ob der versendende Server berechtigt ist.

4. Der E-Mail-Server des/der Empfängers:in @codepurple.ch überprüft mit Hilfe von Daten des DNS-Servers von example.com, ob die DKIM-Signatur valide ist.

5. Der E-Mail-Server des/der Empfängers:in @codepurple.ch überprüft beim DNS-Server von example.com, ob das Alignment gemäss DMARC-Record stimmt.

6. Je nachdem wie erfolgreich die Überprüfungen des Servers waren, wird das E-Mail gelöscht, als Spam markiert oder dem/der Empfänger:in zugestellt.

Ein E-Mail besteht aus einem SMTP-Envelope und den E-Mail-Daten spezifiziert im RFC (Request for Comments) 2822[3)].

Mit dem SMTP-Protokoll kommunizieren E-Mail-Server miteinander. Es ist ein text-basiertes Protokoll, welches ähnlich einem Dialog zwischen zwei Menschen aufgebaut ist. Nachfolgend die vereinfachte Darstellung eines E-Mail-Versandes vom Server @example.com an rhino@codepurple.ch:

E-Mail versenden:

```
Client: Verbindet zum Server
Server: 220 codepurple.ch ESMTP Postfix(Debian/GNU)
Client: HELO example.org
Server: 250 codepurple.ch
Client: MAIL FROM:example@example.com
Server: 250 2.1.0 Ok
Client: RCPT TO:rhino@codepurple.ch
Server: 250 2.1.5 Ok
Client: DATA
Server: 354 End data with <CR><LF>.<CR><LF>
Client: From: example@example.com
        To: Rhino <rhino@codepurple.ch>
        Subject: Password :-)
        Dear Alice,
        I needed a password eight characters long,
        so I picked SnowWhiteandtheSevenDwarves.
        .
Server: 250 2.0.0 Ok: queued as 15B021E282D
Client: QUIT
Server: 221 2.0.0 Bye
```

Quellen:
3) https://datatracker.ietf.org/doc/html/rfc2822

nanio gmbh | Moosweg 24 | 5606 Dintikon
rhino@codepurple.ch | https://codepurple.ch | +41 79 823 45 30

SPF (Sender Policy Framework)

Kurz gesagt: SPF definiert, welche Server (IP-Adressen) im Namen einer Domain E-Mails versenden dürfen. Üblicherweise ist dies der eigene Mail-Server oder die Server eines Newsletter-Services.

Der empfangende Server kann prüfen, ob er das E-Mail von einem Server erhält, der explizit die Erlaubnis hat, E-Mails im Namen der Domain zu versenden.

SPF wurde im April 2014 (vor 8 Jahren) im RFC 7208[4] definiert.

DKIM (DomainKeys Identified Mail)

Kurz gesagt: Der Versender signiert das E-Mail kryptographisch. Der Empfänger kann diese Signatur prüfen.

Der Empfänger kann die kryptographische Signatur prüfen und so verifizieren, ob das E-Mail verändert wurde und ob der Absender das Mail versendet hat. Das E-Mail wird mit dem Private-Key, welcher nur dem Absender bekannt ist, signiert. Der Public-Key für die Validierung der Signatur ist im DNS gespeichert.

DKIM wurde im September 2011 (vor 11 Jahren) im RFC 6376[5] definiert.

DMARC (Domain-based Message Authentication Reporting and Conformance)

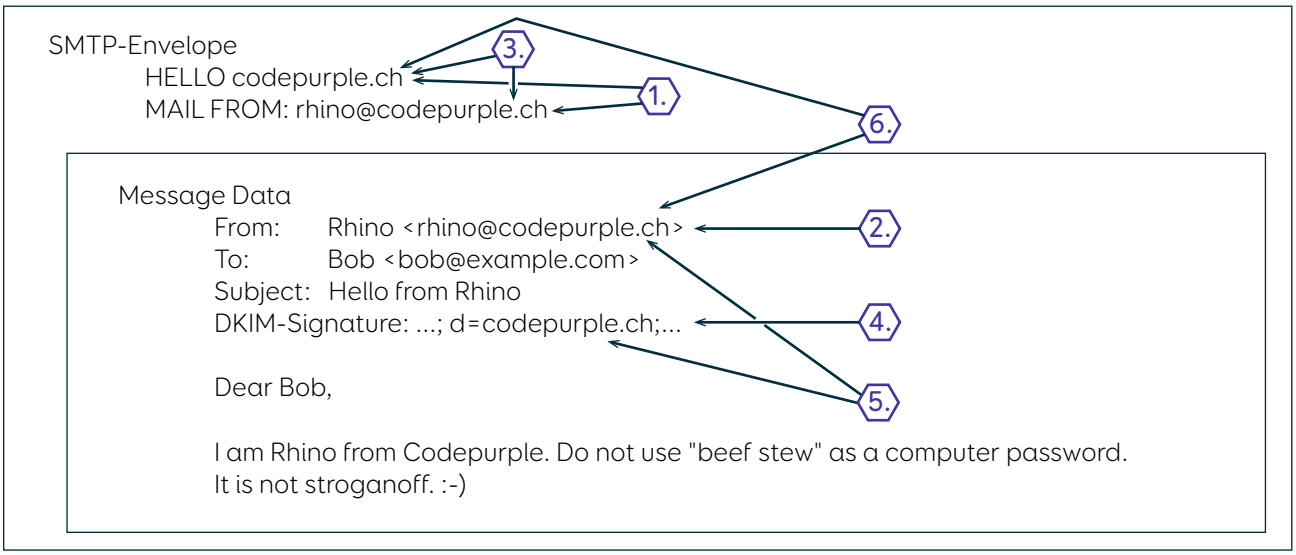
Kurz gesagt: DMARC definiert, das Vorgehen, wenn die SPF oder DKIM Validierung fehlschlagen. Es wird vom empfangenden Server ausgewertet.

DMARC wurde im März 2015 (vor 7 Jahren) im RFC 7489[6] definiert.

DMARC hat ein interessantes Feature: das Reporting. Im DMARC-Record wird spezifiziert, ob das empfangende System DMARC-Reports an eine E-Mail-Adresse senden soll oder nicht. So erhält der Inhaber der Domain einen Einblick, welche Server im Namen der Domain E-Mails versenden.

SPF, DKIM und DMARC

In der folgenden Grafik ist ersichtlich, welche der drei Technologie wo ansetzt:



1. Benutzer:in, der/die die Nachricht übermittelt (nicht sichtbar für den/die Empfänger:in)
2. Benutzer:in, der/die die Nachricht erstellt hat (sichtbar für den/die Empfänger:in)
3. SPF validiert
4. DKIM prüft
5. DMARC DKIM Alignment
6. DMARC SPF Alignment

Quellen:
4) https://datatracker.ietf.org/doc/html/rfc7208
5) https://datatracker.ietf.org/doc/html/rfc6376
6) https://datatracker.ietf.org/doc/html/rfc7489

nanio gmbh | Moosweg 24 | 5606 Dintikon
rhino@codepurple.ch | https://codepurple.ch | +41 79 823 45 30

Analyse

Die Analysen wurden im Februar 2022 durchgeführt. Die Domain-Daten wurden aus dem Zone-File, welches von nic.ch für .ch und .li Domains zur Verfügung gestellt wird, gelesen. Es wurden 2'417'079 .ch und .li Domains analysiert.

Vergleich 2020 / 2022

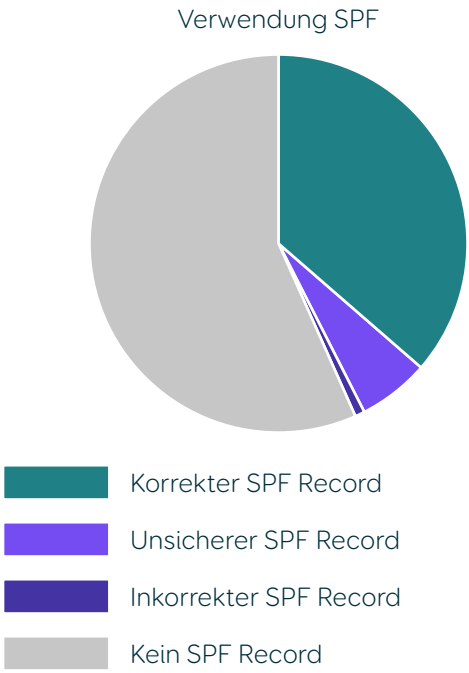
Ein Vergleich der aktuellen Daten mit den Ergebnissen der Analyse des NCSC aus dem Jahr 2020 zeigt, dass sich nicht viel geändert hat. Die Verwendung von SPF ist im Verhältnis leicht gestiegen. Die Verwendung von DMARC ist weiterhin gering.

SPF Review

43% der Domains haben einen SPF-Record. Davon sind 1% fehlerhaft und 14% unsicher eingestellt.

Häufige Fehler:

- Syntax Fehler 24%
- Mehrfacheinträge 40%
- Loops 4%
- Ungültige Referenzen auf andere DNS-Einträge: 30%
- Andere Fehler



Unsichere SPF Einstellungen

Ein SPF-Record mit +all oder ?all erlaubt allen IP-Adressen, ein E-Mail im Namen der Domain zu versenden. Von einer Einstellung mit +all oder ?all ist daher dringend abzuraten. 14% der Domains mit einem SPF-Record haben eine solche Einstellung. Darunter befinden sich unter anderem Gerichte, Anwaltskanzleien und Gemeinden.

Diese Firmen und Institutionen wurden im Vorfeld von Codepurple informiert.

DKIM Review

Eine Analyse zu DKIM kann nicht erstellen werden, da die DKIM DNS-Einträge nicht abgefragt werden können. Zur Überprüfung von DKIM muss ein mit DKIM signiertes E-Mail von der Domain vorhanden sein. Jedes mit DKIM signierte E-Mail, enthält einen Selector, welcher den Namen im DNS definiert, wo der Public-Key gespeichert ist.

Beispiel des DKIM Headers in einem E-Mail:

```
DKIM-Signature: v=1; a=rsa-sha256; d=codepurple.ch; s=example_dkim;...
```

Der Public-Key ist in diesem Beispiel im DNS unter dem Namen example_dkim._domainkey.codepurple.ch gespeichert.

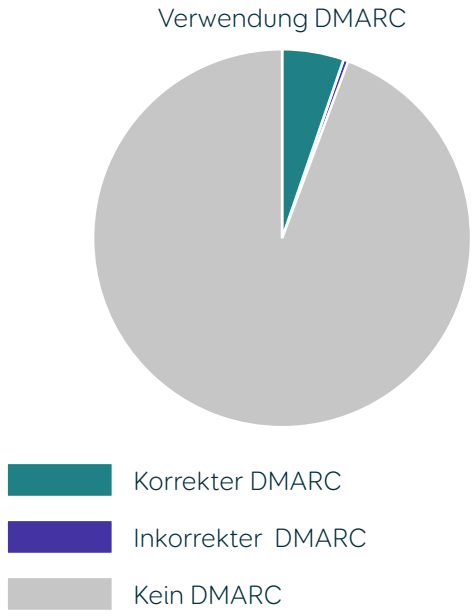
Bei DKIM gilt es weiter zu beachten, dass die Einträge im DNS vorhanden sein können, der versendende

nanio gmbh | Moosweg 24 | 5606 Dintikon
rhino@codepurple.ch | https://codepurple.ch | +41 79 823 45 30

Server jedoch nicht konfiguriert ist und somit die E-Mails nicht mit DKIM signiert werden.

DMARC Review

Von den 1'040'232 Domains mit einem SPF-Record haben 12% der Domains einen DMARC-Record. Davon sind rund 1% fehlerhaft. Die häufigsten Fehler sind Syntaxfehler des Record-Values.



Angriffsvektor über IP-Adressen von Clouddienstleistern

Etwa 27% der SPF-Records verweisen auf IP-Adressen von Clouddienstleistern (Google, Microsoft, Amazon, DigitalOcean, etc.). Oft werden dabei alle IP-Adressen der Clouddienstleister im SPF-Record gesetzt. **Dies eröffnet einen ganz neuen Angriffsvektor**. So kann ein Angreifer einen Server in der Cloud starten und prüfen, ob er eine IP-Adresse zugewiesen bekommen hat, welche im SPF-Record eingetragen ist. Dies kann solange wiederholt werden, bis eine passende IP-Adresse zugewiesen wurde. Das "Suchen" nach einem Server in der Cloud mit einer entsprechenden IP-Adresse erfolgt automatisiert und kostet wenige Dollar. Es lohnt sich, nicht die ganzen IP-Ranges im SPF-Record einzutragen, sondern nur die spezifische, vom Server verwendete IP-Adresse. Dies führt jedoch zu grösseren Aufwendungen in der Administration der SPF-Records.

Fazit

SPF, DKIM und DMARC werden vom empfangenden System ausgewertet. Da diese Systeme vom Empfänger kontrolliert werden, ist davon auszugehen, dass sie richtig konfiguriert sind.

Die Technologien gibt es schon lange. Sie helfen, die Sicherheit im Umgang mit E-Mails zu erhöhen.

Obwohl die Technologien zur Sicherheitsoptimierung vorhanden sind, werden sie in der Praxis selten eingesetzt. Nicht einmal die Hälfte aller Domains nutzen eine der genannten Technologien. Dies kann an fehlendem Wissen oder am Komplexitätsgrad der Technologie liegen. Es zeigte sich, dass die Adaption bei einfacheren Technologien wie SPF höher ist, als bei DMARC oder DKIM, welche eine höhere Komplexität aufweist.

Es lohnt sich regelmässig alle Einträge im DNS-Server zu prüfen und zu aktualisieren. Dies gilt für grosse Unternehmen genauso wie für KMU's. So können alte und nicht mehr benötigte Einträge gelöscht werden und bieten kein unnötiges Angriffspotential.

nanio gmbh | Moosweg 24 | 5606 Dintikon
rhino@codepurple.ch | https://codepurple.ch | +41 79 823 45 30

Codepurple

Codepurple hat sich auf die Cybersecurity-Analyse von Mobilen- und Webanwendungen spezialisiert. Zu unserem Portfolio gehören sowohl Code-Analysen, wie auch Penetration-Tests.

Codepurple erstellt regelmässig Analysen zu Themen rund um Cybersecurity. Bei Erkenntnissen, die für einen grossen Personen- bzw. Firmenkreis von hoher Relevanz sind, publizieren wir diese in unserem Blog. Dazu gehört auch diese Analyse zu den Technologien rund um E-Mail.

Haben Sie Fragen zu Ihrer Domain und den korrekten Einstellungen? Dann kontaktieren Sie uns unverbindlich unter https://codepurple.ch/dnscheck. In einem kurzen Review prüfen wir gerne Ihre Firma oder Organisation.

Referenzen / Quellen

1.) 91% of Cyber Attacks Start with a Phishing Email: Here's How to Protect against Phishing
https://digitalguardian.com/blog/91-percent-cyber-attacks-start-phishing-email-heres-how-protect-against-phishing
Zugegriffen am: 27. März 2022

2.) Simple Mail Transfer Protocol
https://datatracker.ietf.org/doc/html/rfc2821
Zugegriffen am: 27. März 2022

3.) Internet Message Format
https://datatracker.ietf.org/doc/html/rfc2822
Zugegriffen am: 27. März 2022

4.) Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1
https://datatracker.ietf.org/doc/html/rfc7208
Zugegriffen am: 27. März 2022

5.) DomainKeys Identified Mail (DKIM) Signatures
https://datatracker.ietf.org/doc/html/rfc6376
Zugegriffen am: 27. März 2022

6.) Domain-based Message Authentication, Reporting, and Conformance (DMARC)
https://datatracker.ietf.org/doc/html/rfc7489
Zugegriffen am: 27. März 2022