E-Mail Sicherheit

Es geht um Ihren guten Ruf!

Lockout für Spammer, Phisher, Datensauger

In dieser Anleitung erfahren Sie,

- Warum Firmen zu wenig für sichere E-Mail Korrespondenz tun
- Wann unsichere Mails gegen den Datenschutz verstoßen
- Wie Sie mit 3 Schritten die Vertraulichkeit, Integrität und Authentizität Ihrer Mails stärken
- Wie Sie die Schwachstellen Ihrer E-Mail-Systeme erkennen – und anschließend beheben

Autor: Manfred Engel

4ads.de

Inhalt

„Sicherer E-Mail Versand und -Empfang“ beschränkt sich bei vielen Unternehmen und Privatpersonen leider darauf,

a) die E-Mails über eine SSL/TLS verschlüsselte Schnittstelle abzurufen und zu versenden, sowie
b) den Spamfilter fleißig zu trainieren, damit die Spam-Erkennungsrate besser wird.

Doch das ist im geschäftlichen Bereich viel zu wenig, denn:

Firmen sollten sichere Mails senden

In der Mail-Kommunikation mit Kunden muss für die Sicherheit der Kundendaten gesorgt sein. **Es im Eigeninteresse der Unternehmen, dass Kundendaten (Anschrift, E-Mail-Adresse, Bankdaten …) nicht in die falschen Hände gelangen.**

Es reicht definitiv nicht aus, dass die Kundendaten in einer gut abgesicherten Datenbank gespeichert werden. Auch der Kommunikationsweg, d.h. die Übermittlung Ihrer E-Mail Nachrichten an Ihre Kunden sollte genauso gut abgesichert sein wie Ihre Datenbank.

Sowohl im Bundesdatenschutzgesetz wie auch in der DSGVO wird empfohlen, E-Mails mit personenbezogenen Daten zu verschlüsseln. **Es besteht jedoch keine Pflicht.** Doch andererseits stufen manche Landes-Datenschutzbeauftragte eine fehlende Verschlüsselung von E-Mails mit sensiblen persönlichen Daten sogar als Straftat nach § 203 STGB ein.

In der Praxis bereitet die erwünschte Ende-zu-Ende-Verschlüsselung von E-Mails oft Probleme, denn dies ist erst nach Austausch von Schlüsseln zwischen Sender und Empfänger möglich. Je nach Mailprogramm funktioniert diese Art der Verschlüsselung mal besser und mal schlechter. **Solange der Empfänger die Ende-zu-Ende-Verschlüsselung nicht unterstützt,**

bleibt sie wirkungslos. 100% Vertraulichkeit von E-Mails ist kaum möglich. Bzw. nur dann, wenn der komplette Inhalt verschlüsselt wird. Dies ist – siehe oben - zumindest im Massengeschäft schwer erreichbar. Unternehmen behelfen sich derzeit damit, dass vertrauliche Kundenpost nicht per Mail verschickt, sondern im Kundenkonto ablgegt wird. Per E-Mail erfolgt dann der Hinweis, dass ein neues Dokument im Kundenkonto hinterlegt wurde.

Doch neben der **VERTRAULICHKEIT** von E-Mails gibt es noch die Faktoren „Integrität“ und „Authentizität“. Diese Umsetzung dieser beiden Faktoren ist nicht auf die Ausstattung der Mail-Empfänger angewiesen.

INTEGRITÄT bedeutet, dass eine Mail unverändert beim Empfänger ankommt. Genau so, wie sie vom Absender verfasst wurde.

AUTHENTIZITÄT bedeutet, dass sicher ist, dass der angegebene Absender die Mail tatsächlich geschrieben hat (und nicht ein krimineller „Phisher“).

Zur Gewährleistung von Integrität und Authentizität Ihrer E-Mails gibt es einen Mechanismus, den Sie für Ihr Unternehmen einsetzen können:

SPF, DKIM DMARC: für integre, authentische Mails

Es geht um 3 Einträge im DNS Record (Domain Name System Eintrag) Ihrer Seite, die m.E. auch Laien vornehmen können.

1. SPF

Der SPF (Sender Policy Framework) Eintrag nennt die IP-Adressen, über die Ihre Mails verschickt werden dürfen.

Die zulässigen IPs werden im SPF-Record Ihrer Domain hinterlegt & können von den Empfänger-Servern abgerufen werden.

SPF ist eine zusätzliche Absender-Angabe. Vergleichbar mit einem Brief, der außen auf dem Umschlag PLUS innen eine Absenderangabe hat. Falls die Absenderangaben nicht

übereinstimmen, ist die Echtheit des Briefes/der Mail zweifelhaft.

SPF stärkt die Authentizität Ihrer Mails, ist aber nicht fälschungssicher. Sie sollten SPF einsetzen, doch die Schutzwirkung nicht überbewerten.

SPF-Anleitung:
Ein SPF-Eintrag folgt immer dieser Form:
„v=spf1 **Quellen** **Qualifikator**“

Der SPF von 4ads.de lautet zum Beispiel:
„v=spf1 include:mailbox.org -all“

„Quellen“ sind die Mailserver bzw. die IPs, die Ihre Mails verschicken dürfen. Bei 4ads.de dürfen Mails ausschließlich über die Mailserver von mailbox.org verschickt werden. Mails von anderen Servern mit dem Absender „4ads.de“ verstoßen gegen die SPF-Policy.

Falls 4ads.de zusätzlich auch noch Mails über Ionos verschicken würde, müsste der SPF-Eintrag wie folgt lauten:

„v=spf1 include:mailbox.org include:_spf.perfora.net include:_spf.kundenserver.de -all“

„Qualifikator“ ist die Art, wie empfangende Server mit Mails umgehen sollen, die gegen die SPF-Policy verstoßen.

„-all“ bedeutet „Hardfail“ bzw. dass ungültige Mails nicht zugestellt werden.
„~all“ bedeutet „Softfail“ bzw. dass ungültige Mails in den Spam-Ordner verschoben werden.

So gehen Sie vor:
1.) Erkundigen Sie sich bei Ihrem Mailprovider, über welche Server Ihre Mails verschickt werden sollen, und wie der SPF-Eintrag lauten muss.
2.) Fügen Sie dem DNS Ihrer Domain einen neuen „TXT“ – Eintrag in der oben beschriebenen Form hinzu.
3.) Prüfen Sie mit diesem Tool, ob der SPF-Eintrag korrekt angelegt wurde:
https://www.spf-record.de/spf-lookup

Eine ausführliche, brauchbare Anleitung zur Erstellung eines SPF-Records finden Sie z.B. bei Google: https://support.google.com/a/answer/10683907?hl=de

2. DKIM

DomainKeys Identified Mail (DKIM) ergänzt SPF. Durch DKIM wird dem Header Ihrer E-Mails eine fälschungssichere Signatur hinzugefügt.

Im DKIM-Eintrag wird der öffentliche Schlüssel für Ihre ausgehenden Mails hinterlegt, und der versendende Mailserver generiert daraus sowie aus einem Hash-Wert, der aus dem Mail-Inhalt berechnet wird, den privaten Schlüssel.

Der empfangende Mailserver kann anhand der DKIM-Signatur prüfen, a) ob die Mail über Ihren Server verschickt wurde, und b) ob sie auf dem Transportweg verändert wurde. Denn falls die Mail inhaltlich verändert wurde, wird die DKIM-Signatur ungültig. Kurz: **DKIM ist sehr fälschungssicher,** gewährleistet die Integrität und stärkt die Authentizität Ihrer Mails.

DKIM-Anleitung:
Für DKIM müssen Sie einen öffentlichen und einen privaten Signierschlüssel generieren. Viele Provider nehmen Ihnen diese Arbeit ab und liefern Ihnen den öffentlichen Schlüssel, damit sie ihn ins DNS eintragen können. Alternativ können Sie z.B. hier die DKIM-Schlüssel generieren: https://easydmarc.com/tools/dkim-record-generator

Der DKIM-Eintrag hat, genau wie der SPF-Eintrag, den Typ „TXT“.
Den Hostnamen tragen Sie in der Form „selektor._domainkey.domain“ ein. Anstatt „selektor“ tragen Sie eine frei wählbare Bezeichnung ein, anstatt „domain“ tragen Sie den Namen Ihrer Domain ein.

Ein Hostname im DKIM-Record für 4ads.de würde z.B. lauten:
MXZZo144._domainkey.4ads.de
(der Mittelteil bleibt fix)

Das Feld „Wert“ sieht so aus:

v=DKIM1;k=rsa;p=MIGfM.....IDAQAB

v=DKIM1 ist die DKIM-Version.
k=rsa ist der Verschlüsselungsmechanismus („rsa“ ist der häufigste Mechanismus)
p= MIGfM.....IDAQAB ist der Base64-kodierte öffentliche Signierschlüssel.**So gehen Sie vor:**
1.) Erkundigen Sie sich bei Ihrem Mailprovider, ob ausgehende Mails automatisch DKIM-signiert werden**. Falls nein, wechseln Sie den Provider.** (T-Online und Ionos bieten z.B. keine DKIM-Signierung ausgehender Mails an).
2.) Fügen Sie dem DNS Ihrer Domain einen neuen „TXT“ – Eintrag in der oben beschriebenen Form hinzu.
3.) Prüfen Sie mit diesem Tool, ob der DKIM-Eintrag korrekt angelegt wurde:
https://dmarcian.com/dkim-inspector/

Verzichten Sie in keinem Fall auf DKIM. Verzichten Sie lieber auf Ihren jetzigen Mailprovider, falls dieser kein DKIM anbietet. Zusätzliche Anleitung: https://support.google.com/a/answer/174124?hl=de

3. DMARC

DMARC (Domain-based Message Authentication Reporting and Conformance) verbindet SPF und DKIM.

Der DMARC-Eintrag gibt an, was mit Mails passieren soll, die gegen SPF und/oder DKIM verstoßen. Die Optionen lauten: a) nichts, b) Quarantäne, c) Ablehnung.

Meist BEGINNT man mit der Anweisung, dass bei Verstößen - nichts - passieren soll (außer dass Sie benachrichtigt werden). Link zur #Anleitung: Siehe unten, „DMARC-Anleitung“.

Für die DMARC-Policy legen Sie einen weiteren „TXT“-Eintrag an, der für 4ads.de so aussieht:

Hostname: _dmarc.4ads.de
Wert: v=DMARC1; p=reject; sp=reject; pct=100; rua=mailto:dmarc@4ads.de; ri=86400;

Erläuterung:
v=DMARC1 ist die DMARC Protokollversion
p=reject ist die Anweisung, dass alle Mails, die

gegen die SPF- oder die DKIM-Policy verstoßen, abgewiesen werden. Möglich wäre auch p=quarantine (Quarantäne-Richtlinie) oder p=none (Beobachtungsmodus).

sp=reject ist die gleiche Anweisung wie p=reject, doch mit „sp“ bezieht sie sich auf die Subdomains.

pct=100 bedeutet, dass 100% = alle Mails den DMARC-Prüfprozess durchlaufen müssen. Es sind auch geringere Werte, z.B. pct=50 oder pct=10 möglich.

rua=mailto://email-adresse//; ri=86400 bedeutet, dass alle 86400 Sekunden (=täglich) ein Report an die genannte E-Mail-Adresse verschickt wird.

Eine brauchbare Anleitung zu DMARC finden Sie hier: https://support.google.com/a/answer/10032473?hl=de
DMARC-Checker: https://www.dmarcanalyzer.com/de/dmarc-de/dmarc-record-check/

Mit SPF-DKIM-DMARC haben Sie ein mächtiges Reputations-Werkzeug an der Hand.

1. Richtig konfiguriert, setzen Sie Ihre Mails dadurch automatisch auf die „Whitelist“ der empfangenden Server. **Sie authentifizieren sich, weisen sich als seriöser Sender aus.**
   Kurz: Ihre Mails werden dank SPF-DKIM-DMARC nicht im Spam landen.
2. Durch DKIM **erreichen Sie Mail-Integrität.** Es ist nahezu unmöglich, Ihre Mails auf dem Transportweg zu verändern. Ihre Mails kommen genau so beim Empfänger an, wie Sie sie geschrieben haben. Falls auf dem Transportweg irgend etwas an Ihrer Mail verändert wird, passt der einzigartige DKIM-Schlüssel nicht mehr, mit dem Ihre Mail beim Abschicken signiert wurde. Folge: Der empfangende Server wird diese Mail abweisen.
3. Mit SPF-DKIM-DMARC **stärken Sie Ihre Reputation.** Insbesondere wenn Sie die

DMARC-Policy „p=reject“ wählen, wird es Spammern unmöglich gemacht, Ihre Domain als Absenderadresse z.B. für Pharma-, Sex- oder Drogenwerbung oder für Phishing-Attacken zu missbrauchen.

4. **Sie tun etwas für die Umwelt.** Spambekämpfung = Energie + CO2-Emissionen sparen. Vergl. Sie meinen **Kurzbeitrag!**
5. **Achtung:** Falls Sie einen Newsletter versenden, sollten Sie diesen nicht über Ihre Hauptdomain verschicken. Newsletter werden häufig weitergeleitet. Z.B. weil ein Newsletter-Empfänger Ihren Newsletter so interessant findet, dass er ihn an andere Personen weiterleitet. Durch die Weiterleitung wird der Inhalt der Mail u.U. verändert, und die DKIM-Signatur stimmt nicht mehr.
   Um zu vermeiden, dass Ihre Newsletter deshalb zurückgewiesen werden, brauchen Sie eine eigene Newsletter-Domain **mit softeren SPF-DKIM-DMARC-Policies** als bei Ihrer Haupt-Domain!

4. Extra: BIMI

BIMI ist in diesem Zusammenhang kein Brokkoli, sondern steht für „Brand Indicators for Message Identification“.

Unternehmen, die

1. SPF richtig implementieren
2. DMARC richtig implementieren
3. Ein Logo im SVG-Format besitzen

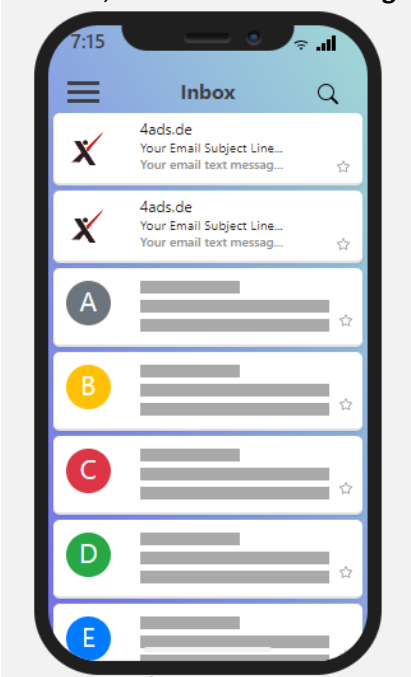
… sind <u>prinzipiell</u> BIMI-fit.

Das bedeutet: Wenn ein BIMI-fittes Unternehmen eine Mail verschickt, wird im Postfach des Empfängers neben der Mail das Logo des Unternehmens angezeigt. Zum einen ist das ein visueller „Echtheitsnachweis“ Ihrer Mail, zum anderen stärken Sie dadurch Ihre Marke und Ihre Reputation. **Nicht zu vergessen der werbliche „Wiedererkennungs-Effekt“.**

Auch BIMI wird mit Hilfe eines DNS-Eintrags realisiert, der bei 4ads.de so aussieht:

v=BIMI1;l=https://4ads.de/bil-der/img/4adsgooglewerbung.svg; a=;

Ergebnis: Wenn eine Mail von 4ads in Ihrem Postfach landet, **sehen Sie das 4ads-Logo:**



Ist Ihre Seite BIMI-fit? Der Bimi-Check zeigts: https://bimigroup.org/bimi-generator/

Aktuell gibt es am „BIMI“-Konzept allerdings noch <u>zwei Haken:</u>

1. Nur wenige Mail-Provider unterstützen das „BIMI“-Konzept, nämlich AOL, YAHOO, NETSCAPE, GMAIL.
   Bei COMCAST und SEZNAM laufen Pilotversuche. Microsoft hat angekündigt, BIMI nicht zu unterstützen.
2. Für 100%ige BIMI-Compliance braucht man zusätzlich eine **Zertifizierung durch Digicert**. Die Kosten hierfür belaufen sich bei der 1. Domain auf ca. 2.000,- USD, für jede weitere Domain auf ca. 500,- USD.
3. **In Kombination (keine flächendeckende Unterstützung + hohe Zertifizierungskosten) ist dieses Konzept derzeit aus meiner Sicht zu teuer.**
4. Allerdings kann es trotzdem sinnvoll sein, seine Domain „BIMI-fit“ zu machen. Denn „BIMI-Fit“ bedeutet: Fehlerfreie Implementierung von SPF, DMARC & Co.!

DANE, MTA-STS, TLS-RPT: Server-Shakehands für mehr Mail-Sicherheit

Wenn eine Mail gesendet wird, baut der sendende Server eine Verbindung zum empfangenden Server auf. Dabei wird (beim STARTTLS-Verfahren) entweder zunächst unverschlüsselt beim empfangenden Server nachgefragt, ob dieser eine verschlüsselte Verbindung anbietet.

Falls der empfangende Server bejaht, wird die verschlüsselte Verbindung aufgebaut, und die Mail wird übermittelt. Verneint der empfangende Server, wird die Mail unverschlüsselt übertragen.

Dieses STARTTLS-Verfahren hat eine große Schwäche: ein Hacker kann sich in die anfangs unverschlüsselte Verbindung einklinken, und erzwingen, dass die Mail unverschlüsselt übertragen wird ... d.h. der Hacker kann „mitlesen“, was in der Mail steht.

Beim etwas sichereren SSL/TLS-Verfahren wird von Anfang an eine verschlüsselte Verbindung erzwungen. Die größte Schwachstelle von TLS liegt bei den Zertifizierungsstellen.

Beide Server vertrauen darauf, dass das von einer Zertifizierungsstelle ausgestellte SSL/TLS Zertifikat wirklich sicher ist. Falls eines der Zertifikate korrumpiert ist ... kann ein Hacker auch bei SSL/TLS den Inhalt der Mail „mitlesen“.

Hier schaffen die beiden Zusatzverfahren „DANE“ und „MTA-STS“ Abhilfe:

DANE

Bei **DANE** (DNS-Based Authentication of Named Entities) werden SSL/TLS-Zertifikate mit DNS-Einträgen verknüpft. Dadurch können sendender und empfangender Server das Zertifikat **- unabhängig von der Zertifizierungsstelle -** überprüfen.

Nachteil: DANE setzt zwingend voraus, dass die DNS Einträge mittels „DNSSEC“ (vgl. nachfolgendes Kapitel) vor Manipulation geschützt sind.

Leider ist DNSSEC nur gering verbreitet, und damit auch DANE. **Zahlen:** Top-Level-Domains (also .com, .de, .eu ...) nutzen derzeit zu 91% DNSSEC. AABER: Auf der Ebene der Second-Level-Domains (also meine-domain.de, deine-domain.de) sind in Deutschland gerade mal 1,5% der Domains durch DNSSEC geschützt. **Zahlen-Quelle:** Artikel auf Heise Online vom März 2022).

20 Doch es gibt inwzischen einige Mailprovider, die DANE einsetzen. Mails zwischen GMX-Adressen und Posteo.de-Adressen sind z.B. DANE-gesichert, da beide Provider DANE implementiert haben. Schwieriger wird's, wenn man Mailadressen der eigenen Domain nutzen möchte.

Ob Ihre Domain DANE kann, zeigt der DANE Validator:
https://dane.sys4.de/

Falls Ihre Domain kein DNSSEC und damit kein DANE kann, oder falls die Postfächer Ihrer E-Mail-Empfänger DANE nicht unterstützen, **dann können (und sollten) Sie MTA-STS verwenden,**

um „Man-in-the-Middle“ Angriffe bzw. das Mitlesen Ihrer E-Mails zu verhindern:

MTA-STS

Eine Alternative zu DANE - und völlig unabhängig von DNSSEC - ist das MTA-STS-Verfahren (Mail Transfer Agent – Strict Transport Security).

Bei MTA-STS Einfach wird bei einer ersten Mail-Verbindung zu einem neuen Server der Fingerprint des Zertifikats in einer lokalen Datenbank als zukünftige Referenz gespeichert.

Bei jedem weiteren Verbindungsaufbau zu diesem Server wird das Zertifikat gegen diesen lokalen Fingerprint geprüft.

Somit ist auch MTA-STS eine von den Zertifizierungsstellen unabhängige (und damit nur schwer zu überlistende) Überprüfung.

MTA-STS ist jedoch etwas schwächer als DANE, denn falls beim ersten Verbindungsaufbau das SSL/TLS-Zertifikat bereits korrumpiert ist, kann ein Hacker nicht nur bei diesem Mailaustausch,

sondern auch bei allen künftigen Mails „mitlesen“.

Trotzdem bewerte ich MTA-STS als enormen Sicherheitsgewinn für den E-Mail Verkehr.

So implementieren Sie MTA-STS:

A)
1.) Sie brauchen zwingend eine SSL-gesicherte Subdomain in exakt folgender Form:
mta-sts.meine-domain.de
(bitte ersetzen Sie „meine-domain.de“ durch den Namen Ihrer Domain)

2.) Im Webspace dieser Domain legen Sie folgendes Verzeichnis an:
.well-known
(bitte beachten Sie den Punkt vor „well-known“)

3.) Sie erstellen eine .txt-Datei mit dem Namen
mta-sts.txt

4.) In diese Datei schreiben Sie folgende Zeilen:
version: STSv1
mode: testing
mx: *.mailbox.org
mx: mxext1.mailbox.org
mx: mxext2.mailbox.org
mx: mxext3.mailbox.org
max_age: 604800
(bitte ersetzen Sie die 4 mx-Einträge durch die Einträge Ihrer eigenen Domain).

5.) Laden Sie die Datei mta-sts.txt in das „well-known-Verzeichnis“ Ihrer Subdomain hoch.

Ob Sie alles richtig gemacht haben, können Sie anschließend feststellen, indem Sie https://mta-sts.meine-domain.de/.well-known/mta-sts.txt aufrufen.

B)
Nun brauchen Sie noch 2 DNS-Einträge (TXT-Einträge).
Mit dem ersten Eintrag dokumentieren Sie, dass

Sie MTA-STS praktizieren.
Hostname: _mta-sts
Wert: v=STSv1; id=12235678;
(Beim Wert können Sie der ID eine beliebige, max. 32stellige alphanumerische Kombination zuweisen).

Mit dem zweiten Eintrag **(=TLS-RPT)** initialisieren Sie das Reporting.
Hostname: _smtp._tls
Wert: v=TLSRPTv1; rua=mailto:mtare-ports@meine-domain.de

Fertig.

DNSSEC & CAA: für Mail- und Serversicherheit

DNSSEC

Im September 2014 kam heraus, dass E-Mails, die über Yahoo!-, Hotmail- und Gmail-Server

verschickt werden sollten, stattdessen über nicht autorisierte Mail-Server geroutet wurden. Die Hacker nutzten damals eine Schwachstelle im DNS aus: DNS akzeptiert **– ohne Prüfung –** (gefälschte) Antworten der Gegenseite.

Aus diesem Grund wurde DNSSEC entwickelt (Domain Name System Security Extensions). Mit DNSSEC wird die Kette „First Level Domain" – „Second Level Domain" – „Subdomain" überprüft, z.B. um betrügerische Mail-Umleitungen durch Hacker zu verhindern.

Also: Wenn ein DNS-Resolver nach www.4ads.de sucht, wird zuerst bei den „de"-Nameservern nachgeschaut, und dort werden dann die für „4ads" zurückgegebenen Einträge überprüft. Anschließend wird bei „4ads" nachgeschaut, welche Einträge für die „www" Subdomain zurückgegeben werden.

Kurz: DNSSEC ist zwar leider kaum verbreitet in Deutschland (nur 1,5% der Webseiten setzen es ein). Zum Teil liegt das an den Providern, die dieses Feature nicht bereitstellen. Fehlendes

DNSSEC wäre für mich zwar noch kein Grund, den Provider zu wechseln.
ABER, UMGEKEHRT: Wenn Ihr Provider DNSSEC anbietet, sollten sie es nutzen. In der Regel sind es 1-2 Mausklicks sowie eine geringe monatliche Gebühr, die ein weiteres Stück Sicherheit schaffen.

CAA

Ein kleiner, letzter Punkt zu mehr Sicherheit im E-Mail Verkehr, und ein allerletztes Kürzel:

CAA (Certificate Authority Authorization)

Mit CAA können Sie festlegen, welche Zertifizierungsstellen berechtigt sind, SSL/TLS-Zertifikate für Ihre Domain auszustellen.

Also, wenn Sie Ihre SSL/TLS-Zertifikate z.B. regelmäßig über GlobalSign oder DigiCert oder ... beziehen, können Sie dies mit Hilfe eines DNS-Eintrags dokumentieren.

Warum sollten Sie das tun?

Weil Sie damit verhindern, dass (von anderen Zertifizierungsstellen) missbräuchlich Zertifikate auf Ihre Domain ausgestellt werden.

(Je nach Zertifizierungsstelle) kann sich theoretisch jeder X-Beliebige ein Zertifikat für Ihre Domain ausstellen lassen ... **und seine eigene Seite dann mit Hilfe dieses Zertifikats als Ihre Seite ausgeben – klassisches Phishing-Modell.**

Seit 2017 ist die Ausstellung von SSL/TLS Zertifikaten jedoch so geregelt, dass die Zertifizierungsstelle zuerst nachschauen **muss,** ob sie berechtigt ist, ein Zertifikat auszustellen.

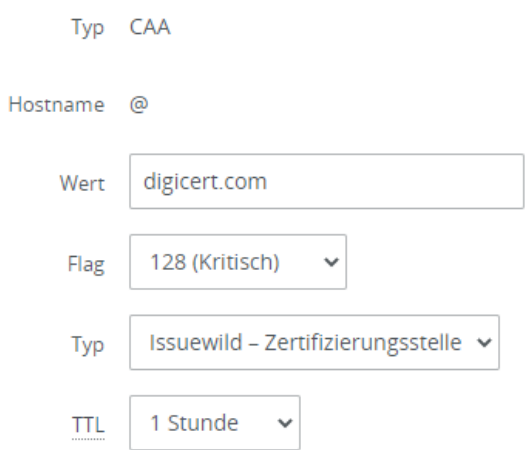
Falls die Berechtigung fehlt, DARF die betreffende Zertifizierungsstelle **kein** Zertifikat für Ihre Seite ausstellen.

Mit anderen Worten: Sie als Domaininhaber legen fest, wer Zertifikate für Ihre Domain ausstellen darf (und Sie verbieten dadurch allen anderen Zertifizierungsstellen, ein Zertifikat für Ihre Seite auszustellen).

Wenn Sie KEINEN CAA Record angelegt haben, kann jede beliebige Zertifizierungsstelle ein SSL/TLS-Zertifikat für Ihre Seite ausstellen. Dadurch steigt die Missbrauchsgefahr!

Den CAA Eintrag fügen Sie ebenfalls der DNS Ihrer Domain hinzu. **Achtung:** Bitte nicht als „TXT“-Eintrag. Für CAA gibts einen eigenen Eintragstyp namens „CAA“.

So sieht der CAA Eintrag für 4ads.de aus:



Im Feld „Wert“ geben Sie den Namen Ihrer Zertifizierungsstelle an (bei 4ads.de ist DigiCert die Zertifizierungsstelle).

Im Feld „Flag“ haben Sie die Wahl zwischen 0 (unkritisch) und 128 (kritisch). „Kritisch“ bedeutet: wenn die Eintragungen im CAA-Record nicht ausgewertet werden können (z.B. weil ich „Donald Duck Enterprises“ als Zertifizierungsstelle angebe), dann darf KEINE Zertifizierungsstelle ein Zertifikat ausstellen.

Im Feld „Typ“ geben Sie an, ob die Zertifizierungsstelle Wildcard-Zertifikate („Issuewild“) oder Einzel-Zertifikate („issue“) ausstellen darf. Wildcard-Zertifikate gelten für Domain und sämtliche Subdomains, Einzelzertifikate gelten nur für die Domain selbst.

Mit all diesen Maßnahmen härten Sie den E-Mail Verkehr. **Bitte, prüfen Sie Ihren (Sicherheits-) Status Quo unter folgender Adresse:**

https://www.hardenize.com/

Fazit

Bis vor ca. 3 Jahren ging ich recht sorglos mit dem Thema E-Mail Sicherheit um. E-Mail Sicherheit **hieß damals für mich:**

1. Regelmäßig die Zugangspasswörter ändern und dabei halbwegs „sichere“ Passwörter verwenden.
2. Virenscanner & Spamfilter fürs Postfach
3. Newsletter etc. nie über die Firmen-Mail bestellen, sondern über eine Freemailer-Adresse, und von dort weiterleiten.
4. Kundenmails und andere kritische Mails lokal speichern und jährlich auf einen Stick oder eine CD auslagern.

Dann stieß ich auf die Seite …

https://haveibeenpwned.com/

… und stellte fest, dass meine (damalige) E-Mail Adresse in der Vergangenheit 6 mal „erwischt“ (pwned) wurde. D.h. konkret wurden entweder

Anbieter (bzw. deren Kundendatenbanken) gehackt, wie z.B. **Dropbox** (2012), **Adobe** (2013) oder **Linkedin** (2016), **bei denen ich ein Kundenkonto habe/hatte**. Oder es wurde im großen Stil Mail-Verkehr mitgelesen, und daraus wurden dann Daten extrahiert.

Zum Glück habe ich auch damals schon häufig meine Passwörter gewechselt. Und ich verwende ein Passwort nie mehrfach. Die einzige spürbare Änderung in den Jahren seit 2012 war die deutliche Zunahme von Spam. Ich gehe davon aus, dass dies auf die „erwischte“ E-Mail-Adresse zurückzuführen ist. Denn die anderen Mail-Adressen hatten in der Zeit nach 2012 +/- genauso viel Spam wie vorher auch.

Seit diesem „AHA-Erlebnis“ befasse ich mich intensiv mit der Thematik „sichere E-Mails“.
Meine Meinung: Besser als „sichere E-Mails“ sind nur „noch sicherere E-Mails“.

Ich würde mich freuen, wenn Ihnen die Themen in dieser PDF Anregungen dafür geben, wie Sie Ihre E-Mails sicherer machen können

Impressum / über den Autor

Ich bin „Google Ads Optimierer der ersten Stunde“. **Seit 2001, über 2 Jahrzehnte.**

Ganz kurz: ich mache so ziemlich alles im Bereich Google Ads.

Mit Ausnahme der ganz einfachen Geschäftsmodelle (= Kunde sucht Produkt **-->** Shop/Anbieter bietet genau dieses Produkt an). Bei diesen Geschäftsmodellen ist KI-gesteuerte Optimierung händischer Optimierung überlegen.

Bei komplexeren Geschäftsmodellen, z.B. Beratergeschäft oder Leadgenerierung für den Vertrieb, ist **meine** händische Ads-Optimierung den Algorithmen überlegen ... **und das macht Spaß**.

Mein Hobby sind Bücher. Lesend und schreibend. Im Lauf der Zeit sind so um die 20 Publikationen entstanden … und die nächste steht kurz bevor:
Ein Buch über Wordpress. **Genauer:** Wie man

Wordpress von Beginn an **planvoll** anlegt, um eine sichere, schnelle, stabile, gut pflegbare, nachhaltige Webseite zu erhalten.

Das Thema **„E-Mail-Sicherheit“** ist ein kleiner Teil dieses Buchs. Hier in der PDF wird das Thema jedoch anders (= z.B. an einigen Stellen ausführlicher) dargestellt als im Buch.

Falls Sie am Thema **„Wordpress“** interessiert sind, folgen Sie mir einfach auf Linkedin:
https://de.linkedin.com/in/engel-4ads

Dann erfahren Sie rechtzeitig den Erscheinungstermin und den Termin für **die kleine 24stündige Rabatt-Aktion** am Anfang.

Und …

falls Sie am Thema **„Google Ads“** interessiert sind, besuchen Sie gerne meine Webseite 😊

Impressum
Manfred Engel
4ads Google Werbung
Am Franzosengraben 13
93533 Wernberg-Köblitz

Kopien und Weitergabe dieses Ratgebers

1. Das Kopieren (in elektronischer und nicht - elektronischer Form) sowie die Weitergabe und Verbreitung dieses Ratgebers ist

- in unveränderter Form* -

ausdrücklich **erlaubt und erwünscht.**

2. Zitate **mit Quellenangabe und Nennung des Autors** sind erlaubt. Copy & Paste-Veröffentlichung ohne Quellenangabe ist verboten.

3. Die Weitergabe und Verbreitung einer **geänderten** elektronischen oder nicht-elektronischen Form dieses Ratgebers ist **ausschließlich nach vorheriger schriftlicher Vereinbarung** mit dem Autor möglich. Ohne vorherige schriftliche Vereinbarung mit dem Autor ist geänderte Weitergabe/Verbreitung des Ratgebers verboten.

*** „in unveränderter Form“ bedeutet:** weder dürfen Inhalte verändert werden, noch dürfen Seiten entfernt oder hinzugefügt werden.