DKIM Empfehlungen 2018 mit Berücksichtigung des DKIM Crypto Update

1. Problemstellung

DKIM ist eine weit verbreitete Methode, um E-Mails authentifizieren zu können. Doch wenn DKIM nicht richtig eingesetzt wird, ist es nicht wirkungsvoll und kann ein falsches Gefühl von Sicherheit vermitteln. Aus diesem Grund haben wir gängige Best Practices für DKIM zusammengefasst.

2. Technische Maßnahmen

2.1 Länge des Schlüssels

Mit der schnell steigenden Leistungsfähigkeit von Computern können ehemals als sicher geltende RSA Schlüssel mit 512 Bit Länge in kurzer Zeit geknackt werden. Stand heute sollte man mindestens 1024 Bit RSA verwenden. Organisationen wie das amerikanische National Institute of Standards and Technology (NIST) gehen weiter und empfehlen mindestens 2048 Bit. Zu beachten ist hierbei, dass große Schlüssel (üblicherweise ab 4096 Bit) im DNS potentiell Probleme verursachen können, da die Antworten dann nicht mehr in UDP-Paket passen, sondern per TCP beantwortet werden müssen

2.2 Algorithmen

Der DKIM Standard definiert unterstützt lediglich RSA als Algorithmus, modernere Algorithmen werden nicht unterstützt. An diesem Nachteil wird allerdings bereits gearbeitet.

Unter dem Namen "DKIM Crypto Update" verbirgt sich die Initiative den Standard DKIM auf einen aktuellen kryptografischen Stand zu aktualisieren um

eben jenes Problem zu adressieren. Der aktuelle Stand ist im RFC 8301 zu finden.[1]

Die wichtigsten Änderungen betreffen die bereits angesprochene Schlüssellänge. Darüber hinaus wird die Unterstützung von EdDSA als kryptografischer Algorithus neben RSA aufgenommen. EdDSA hat einige Vorteile. Bei gleichem Sicherheitsniveau sind die Schlüssel deutlich kürzer und vermeiden somit die angesprochenen DNS Probleme. Darüber hinaus ist das signieren und verifizieren mit EdDSA weniger Ressourcenintensiv.

Es ist allerdings davon auszugehen, dass heute nicht jeder Empfänger in der Lage ist eine DKIM Signatur mit EdDSA verarbeiten zu können. Daher sollte man, wenn man EdDSA einsetzt, jede E-Mail als Fallback zusätzlich ein zweites Mal über einen anderen Selektor mit RSA signieren.

Eine weitere Neuerung betrifft den verwendeten Hash-Algorithmus. Da SHA-1 nicht mehr als sicher gilt ist ausschließlich SHA-256 zu verwenden.

2.3 Monitoring

Um überwachen zu können, ob die E-Mails bei den Empfängern korrekt verifiziert werden können empfiehlt sich der Einsatz von DMARC. Bei Verwendung einer "none" policy wird die Zustellung der E-Mails durch DMARC nicht beeinflusst, allerdings bekommt man durch das Reporting einen Überblick darüber, ob DKIM wie erwartet funktioniert.

3. Organisatorische Maßnahmen

3.1 Zugriff auf privaten Schlüssel

Die Sicherung und Geheimhaltung des privaten Schlüssels ist essentiell. Falls Unbefugte Zugriff auf den privaten Schlüssel erlangen ist es Ihnen möglich selbst beliebig E-Mails für die zugehörige Domain zu signieren. Der Schlüssel sollte also mit gängigen Methoden (Zugriffsbeschränkungen durch das Betriebssystem, Verschlüsselung der Datenträger,..) abgesichert werden.

[1] https://datatracker.ietf.org/wg/dcrup/about/

3.2 Key rotation

Doch selbst bei aller Vorsicht ist es möglich, dass ein privater Schlüssel kompromittiert wird, bspw. durch einen ehemaligen Mitarbeiter. Daher sollte man unbedingt die Schlüssel regelmäßig rotieren, sprich gegen ein neues Schlüsselpaar austauschen. Mindestens jedes Jahr, besser jedes Quartal oder monatlich. Insbesondere bei kürzeren Intervallen wird klar, dass der Schlüsseltausch automatisiert werden sollte, bspw. über entsprechende Scripte und passende cronjobs. Details zum Ablauf eines Schlüsselaustauschs sind sehr gut im Dokument "M3AAWG DKIM Key Rotation Best Common Practices" [2] beschrieben.

Falls man im Auftrag für jemand anderes E-Mails versendet, zum Beispiel als E-Mail Service Provider sieht man sich beim Schlüsseltausch besonderen Herausforderungen gegenüber, da ein neuer öffentlicher Schlüssel im DNS publiziert werden muss und Änderungen üblicherweise durch den Domainbesitzer und damit den Kunden durchgeführt werden müssen. Lösungen zu diesem Problem sind in unserem Dokument "DKIM leicht gemacht"[3] zu finden.

Autor: Alexander Zeh, Certified Senders Alliance

[2] https://www.m3aawg.org/sites/default/files/document/M3AAWG_DKIM_Key_Rotation_BP-2013-12.pdf

[3] https://certified-senders.org/wp-content/uploads/2017/05/CSA_DKIM_leicht_gemacht.pdf