DKIM leicht gemacht

Wie DKIM funktioniert

Kurz gesagt ermöglicht *DomainKeys Identified Mail* (DKIM) dem empfangenden E-Mail Server den Absender einer E-Mail zu authentifizieren. Der sendende E-Mail Server versieht jede gesendete E-Mail mit einer digitalen Signatur. Diese Signaturen werden kryptographisch mithilfe eines so genannten privaten Schlüssels erstellt. Die digitale Signatur ist Teil des E-Mail Headers, welchen der Endnutzer normalerweise nicht zu sehen bekommt. Der empfangende E-Mail Server allerdings validiert diese Signaturen mit Hilfe des zugehörigen öffentlichen Schlüssels, welcher im *Domain Name System* (DNS) veröffentlicht wird, so dass der empfangende E-Mail Server ihn von dort beziehen kann.

Im Grunde benötigt DKIM zwei Komponenten um korrekt zu funktionieren:

- Ausgehende E-Mails werden vom sendenden E-Mail Server mit dem privaten Schlüssel signiert
- Der zugehörige öffentliche Schlüssel wird im DNS veröffentlicht

Das Problem? E-Mail Server werden von Service Providern verwaltet, DNS wird intern verwaltet

In der Praxis verwenden viele Firmen (Marken) die Werkzeuge und Versandserver eines *E-Mail Service Providers* (ESP). Das ist im Grunde eine sehr gute Idee, denn ESPs haben sowohl das nötige Wissen und auch die Mittel um Newsletter und Transaktionsemails auf professionelle Weise zu versenden. Es bringt allerdings auch kleinere Schwierigkeiten mit sich. In vielen Fällen behalten die Marken die Kontrolle über die DNS Einstellungen. Nehmen wir also an ein ESP generiert das Schlüsselpaar aus einem privaten und einem zugehörigen öffentlichen Schlüssel. Der ESP setzt den erzeugten privaten Schlüssel im versendenden E-Mail Server ein, um alle ausgehenden E-Mails zu signieren und stellt der internen IT-Abteilung der Marke den zugehörigen öffentlichen Schlüssel zur Verfügung, damit diese ihn im DNS veröffentlichen können. Das wäre an sich kein wirkliches Problem, wenn das Einrichten von DKIM eine einmalige Sache wäre. Aus Sicherheitsgründen sollten DKIM Schlüssel allerdings mindestens alle 6 Monate

geändert (rotiert) werden. Damit verringert man das Risiko kompromittierter Schlüssel, da Schlüssel geknackt oder gestohlen werden könnten. Um bei dieser Schlüsselrotation einen sauberen und fehlerfreien Übergang zu erreichen werden üblicherweise 3 Schlüsselpaare parallel eingesetzt. Das erste Schlüsselpaar ist das inzwischen abgelaufene, das zweite Schlüsselpaar ist das aktuell genutzte und das dritte Schlüsselpaar ist jenes, welches als nächstes gültig sein wird. Damit hat man einen nicht zu unterschätzenden und andauernden Aufwand um dafür zu sorgen, dass ausgehende E-Mails ordentlich signiert sind.

Wäre es als Marke nicht genial, wenn man diese Arbeit dem ESP überlassen könnte? Und wäre es für ESPs nicht perfekt seinen Kunden den Service anzubieten sich komplett um DKIM zu kümmern, ohne dass die interne IT-Abteilung der Marke etwas tun muss?

Verzweifelt nicht, denn die Rettung ist nah

Die gute Nachricht ist, es gibt bereits gut funktionierende Lösungen für dieses Problem:

- (Sub)domain Delegation:

  Die Marke kann eine Subdomain oder Domain an den ESP delegieren und somit die Kontrolle an den ESP übergeben. Der ESP kann dann den öffentlichen Schlüssel selbst im DNS publizieren. Der Nachteil dieser Lösung: Markeninhaber mögen selten die Idee, die Kontrolle über ihre Domain einer dritten Partei zu übergeben. Mit einer Subdomain Delegation ist es möglich die Kontrolle nur über eine bestimmte Subdomain (z.b. news.example.org statt example.org) zu übergeben. Das resultiert dann aber zumeist in „nicht so hübsch aussehenden" Absenderadressen, wie z.b. info@news.example.org anstelle von news@example.org.

- Canonical Name Record (CNAME):

  Ein CNAME Record definiert im DNS einen Domain Namen als Alias für einen anderen Domain Namen. Eine Marke setzt also lediglich einmal CNAME Records für DKIM im DNS, die einem empfangenden E-Mail Server mitteilen, dass er den öffentlichen Schlüssel an einer anderen Stelle beziehen kann, nämlich im DNS des ESP.

Beispiel:

key1._domainkey.brand_domain.org → key1.brandname.esp_domain.com wobei sich unter "key1.brandname.esp_domain.com" der eigentliche öffentliche Schlüssel befindet.

In diesem Fall setzt die Marke in ihren DNS lediglich die Information wo der öffentliche Schlüssel zu finden ist, im DNS des ESPs. Der ESP kann sich dann um die eigentliche Verwaltung der Schlüssel und die Rotation der Schlüssel kümmern.

Fazit

Subdomain Delegation ist eine gute Möglichkeit um dem ESP die Kontrolle im Bezug auf E-Mail Authentifizierung zu übergeben. Falls es allerdings Bedenken geben sollte auch nur über einen Teil der Domain die Kontrolle zu verlieren, oder falls die Marketingabteilung wert auf „schön aussehende" Absenderadressen legt, dann sind CNAME Records das Mittel der Wahl.

Autoren: Technik Team der Certified Senders Alliance