DANE als Grundlage für die sichere Datenübertragung von E-Mails

DANE mit DNSSEC sorgt dafür, dass Ihre E-Mail mit Sicherheit beim Richtigen ankommt

Ist der Ruf erst ruiniert, lebt es sich recht ungeniert. Für Privatpersonen mag das ja vielleicht zumindest teilweise zutreffen. Versandhändler, Dienstleister oder das Bankgewerbe leben aber zum großen Teil von ihrem guten Ruf und sind deshalb auch im Internet darauf bedacht, ihre gute Reputation zu halten bzw. zu optimieren. Werden Kunden aber Opfer einer sogenannten „Man in the Middle" Attacke, ist der gute Ruf ganz schnell futsch. Bei einem „Man in the Middle"-Angriff platziert sich der Angreifer zwischen Kunde und Anbieter und gibt vor, der Anbieter zu sein. Ein solcher Angriff ist auch in der anderen Richtung möglich.

Zur Erläuterung nachfolgend ein Beispiel: Angenommen, Sie sind Online-Versandhändler und verschicken automatisiert Transaktionsmails wie zum Beispiel Rechnungen und Auftragsbestätigungen. Nun werden diese über einen „Man in the Middle" in fremde Hände geleitet. Die Rechnung kommt nie bei Ihrem Kunden an und Sie merken noch nicht einmal etwas davon. Natürlich bekommen Sie auch kein Geld, da der Kunde keine Rechnung bekommen hat. Was geschieht? Sie verschicken eine Mahnung. Eine Mahnung ohne vorherige Rechnung sorgt für Verärgerung und Vertrauensverlust beim Kunden, aus Marketingsicht ein Desaster.

Aber es kann noch schlimmer kommen: Bei einem erfolgreichen Angriff gelangen auch sensible Daten Ihres Kunden wie beispielsweise Adresse, Bankverbindung und Einkaufsgewohnheiten in unberechtigte Hände. Bei Versicherungen, Krankenkassen, Kreditinstituten oder auch Dating-Plattformen wiegt das besonders schwer, denn hier sind hochsensible Kundendaten unterwegs.

Empfindliche Konsequenzen

Der Schutz Ihrer Kundendaten hat nicht nur für Sie, sondern auch für den E-Mail Service Provider, der in Ihrem Auftrag versendet, höchste Priorität. Artikel 33 der europäischen Datenschutzgrundverordnung (DSGVO) sieht vor, was passiert, wenn eine Verletzung personenbezogener Daten erfolgt ist: In diesem Fall muss der Verantwortliche (hier das Marketing treibende Unternehmen) der Aufsichtsbehörde (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit BfDI bzw. Landesdatenschutzbehörden) und

den Betroffenen unter den Voraussetzungen des Artikels 34 DSGVO die Datenverletzung mitteilen.

Dann ist nicht nur Ihre Reputation in Gefahr, es drohen auch finanzielle Konsequenzen. Sofern dem Verantwortlichen bzw. dem ggfls. von ihm beauftragten Auftrags Verarbeiter (in diesem Fall der Email Service Provider) die Verantwortung für die Datenschutzverletzung zugeschrieben werden kann, werden die Aufsichtsbehörden im Falle einer Verletzung personenbezogener Daten gemäß Artikel 58 DSGVO gegenüber dem oder den Verantwortlichen Untersuchungs-, Abhilfe- und Sanktionsbefugnisse geltend machen. Im schlimmsten Fall kann dies sogar ein endgültiges Verbot der Verarbeitung solcher Daten zur Folge haben, was konkret ein Verbot der Geschäftstätigkeit bedeutet. Darüber hinaus können Zwangsgelder verhängt werden. Daneben oder alternativ drohen nach Artikel 83 DSGVO erhebliche Geldbußen bis zu 20 Millionen Euro oder 4% des Gesamtjahresumsatzes. Jüngstes Beispiel: Die britische Datenschutzbehörde (ICO) hat gegen British Airways ein Bußgeld in Höhe von umgerechnet 205 Millionen Euro verhängt, nachdem sich Unbekannte Zugriffe auf die Kundendaten der Fluggesellschaft erschlichen hatten.

Fakt ist: Es reicht nicht aus, den eigenen Server bestmöglich abzusichern. Denn ein Man in the Middle nutzt die Schwachstelle des Transports einer E-Mail von A nach B. Um den Anforderungen von Artikel 5 Absatz 1 f. DSG-VO zu genügen, die angemessene Sicherheit personenbezogener Daten zu gewährleisten, sollten Sie sensible Kundendaten mittels DNSSEC und DANE schützen.

Was sind DNSSEC und DANE?

DANE (DNS-based Authentication of Named Entities) ist ein Prüfverfahren, das den Aufbau einer verschlüsselten Verbindung zwischen einem Client und einem Server absichert. Über einen Zertifikatsabgleich (TLSA Record) schließen DANE nutzende Kommunikationspartner die konzeptionelle Schwäche von SSL/TLS, bei der ein Dritter sich als „der richtige Server“ ausgeben könnte und den Client dazu bringen könnte, seine Daten an den „falschen Richtigen“ zu übertragen. Voraussetzung für den Einsatz von DANE ist DNSSEC (Domain Name System Security Extensions), welches sicherstellt, dass die per DNS übermittelten Prüfmerkmale verifizierbar sind. Denn auch hier könnten Angreifer falsche Angaben ins DNS einschleusen und den Client zum Falschen leiten.

Und so funktioniert es:

Wie sieht nun ein typischer Mailtransport mit DANE aus? Gesetzt den Fall, Sie als Online-Händler senden eine Mail an einen Kunden mit einem Mailkonto bei example.de. Dann sieht das wie folgt aus:

- Ihr Mailserver bestimmt den für die Empfängerdomain zuständigen Mailserver. Dabei prüft er auch, ob der DNS-Server der Empfängerdomain DNSSEC anbietet.
- Bietet der DNS-Server DNSSEC an, prüft ihr Mailserver ob ein TLSA-Record für die Empfängerdomain vorliegt.
- Dann baut ihr Mailserver eine Verbindung zum Mailserver der Empfängerdomain auf. Bietet dieser kein STARTTLS für eine Verschlüsselung der Verbindung an, bricht ihr Mailserver sofort ab, denn der Verdacht einer Downgrade-Attacke steht im Raum.
- Bietet der Zielserver STARTTLS an, beginnt ihr Mailserver eine TLS-verschlüsselte Verbindung. Dabei vergleicht er die Prüfsumme des Zertifikats des Zielservers mit der TLSA-Information, die er per DNSSEC erhalten hatte.
- Stimmen die Summen überein, gilt der Zielserver als verifiziert. Passen die Summen nicht zusammen, bricht ein DANE-aktivierter Client sofort ab, denn es besteht der Verdacht einer „Man in the Middle"-Attacke. Herkömmliche Clients senden jetzt ahnungslos weiter und senden Daten an ein nicht vertrauenswürdiges Ziel.

So weit, so sicher. Damit DANE mit DNSSEC funktioniert, müssen sowohl DANE als auch DNSSEC auf dem Mailserver des Online-Händlers eingerichtet sein. Sofern ein E-Mail-Service-Provider für den Versand genutzt wird, muss die Mailplattform so erweitert werden, dass DNS-Abfragen auch auf DNSSEC-Funktionalität prüfen und dessen Fähigkeiten zur Verifikation nutzen.

Die Grundlagen dafür sind längst gegeben. „DNSSEC ist ein ausgereiftes und seit Jahren stabiles Verfahren", sagt Patrick Koetter (Kompetenzgruppenleiter der Gruppen „Anti-Abuse" und „E-Mail" des eco – Verband der Internetwirtschaft e.V.). „Praktische Erfahrung auf großen ISP-Plattformen und Messungen zeigen, die Bedenken mancher Administratoren sind fachlich nicht haltbar."

Bedenkt man die finanziellen Konsequenzen und den Reputationsverlust, den eine Downgrade-Attacke und/oder „Man in the Middle"-Attacke nach sich ziehen können, lohnt sich der einmalige Aufwand für die Aktivierung von DANE und DNSSEC. Sie stellen die einzige automatisierte und kostengünstige Möglichkeit für eine wirklich sichere Datenübertragung zwischen E-Mailservern dar.

Lesen Sie mehr über verwandte Technologien und tauchen Sie während eines Workshops auf dem CSA Summit 2020 noch tiefer in das Thema ein.