DANE as Basis for Secure Data Transmission of Emails

DANE and DNSSEC make sure that your email safely gets to the right recipient

Once you've ruined your reputation, life gets a lot simpler. This might be the case for private individuals, but it's a different story in business. Mail-order retailers, service providers, and the banking industry are profoundly dependent on their good reputation, and are therefore also intent on maintaining and optimizing it on the Internet. If their customers become the victims of a "Man in the Middle" attack, this good reputation can go down the drain in a matter of moments. In a "Man in the Middle" attack, the attacker manages to get between the customer and the business, and impersonates the business. Such an attack is also possible in the other direction, targeting the business as a supposedly trusted customer.

Here's an example to demonstrate: Let's assume you're an online retailer and you send automated transaction emails such as invoices and order confirmations. Now these are forwarded into the wrong hands through a "Man in the Middle" attack. The customer never receives the invoice and you are none the wiser about what's going on. Of course, you don't get your money, given that the customer never got the invoice. What do you do? You send a reminder. A reminder without a prior invoice just annoys the customer and leads to a loss of trust, a disaster from the marketing perspective.

But it could get worse: In a successful attack, sensitive customer data – such as address, bank account details, or shopping habits – can end up in unauthorized hands. For insurance companies, medical companies, credit institutes, or dating platforms this is particularly serious, because in these cases extremely sensitive customer data is involved.

Painful consequences

The protection of your customer data is not only of the highest priority for you, but also for the email service provider that is sending on your behalf. Article 33 of the European General Data Protection Regulation (GDPR) stipulates what happens in the case of a breach involving personal data: In this case, the data controller (here, the company doing the marketing) must inform the data subjects (customers whose data has been breached) – as well as the supervisory authorities in the European Member State where

your activities are based – of the data breach, according to the requirements of Article 34 GDPR.

In this case, it's not only your reputation that is in danger, you also face the threat of financial consequences. If responsibility for the data breach is found to lie with the data controller or a data processor contracted by the data controller (in this case the email service provider), then in the case of a breach of personal data as set out in Article 58 GDPR, the supervisory authority can exercise powers of investigation and redress, and impose sanctions against those responsible. In the worst case, this can even result in a definitive ban on the processing of such data, which concretely means a ban on business activities. In addition, periodic penalty payments can be imposed. Alongside these or alternatively there is the threat of heavy fines of up to 20 million Euro or 4% of annual turnover, as spelled out in Article 83 GDPR. A recent example: The British data protection authority (ICO) fined British Airways the equivalent of 205 million Euro, in the wake of unknown parties fraudulently gaining access to customer data from the airline carrier.

The fact is, it is not enough to secure your own servers in the best possible way. Because a "Man in the Middle" attack exploits the vulnerabilities of the transport of an email from point A to point B. To fulfill the requirements of Art. 5 Para 1 (f) GDPR to ensure appropriate security for personal data, you should be protecting sensitive customer data by means of DNSSEC and DANE.

What are DNSSEC and DANE?

DANE (DNS-based Authentication of Named Entities) is a validation process that secures the establishment of an encrypted connection between a client and a server. By comparing certificates (TLSA Record), communication partners using DANE close the conceptual weakness of SSL/TLS, through which a third party can present itself as "the right server" and can convince the client to transfer its data to the wrong "right" one. The prerequisite for using DANE is DNSSEC (Domain Name System Security Extensions), which makes sure that the validation features transmitted via the DNS are verifiable. Because here also, attackers can smuggle false information into the DNS and lead the client to the wrong resource.

And this is how it works:

What does typical email transport with DANE look like? Supposing that you, as an online retailer, send an email to a customer with an account at example.com, it would look like this:

- Your mail server determines which mail server is responsible for the receiver domain. IN the process, it also checks whether the receiver domain's DNS server offers DNSSEC.
- If the DNS server offers DNSSEC, then your mail server checks whether there is a TLSA Record for the receiver domain.
- Then your mail server establishes a connection to the receiver domain's mail server. If the latter does not offer STARTTLS for encrypting the connection, your mail server immediately terminates the connection, because this looks suspiciously like it could be a Downgrade Attack.
- If the destination server offers STARTTLS, then your mail server begins a TLS-encrypted connection. In doing so, it compares the checksum of the destination server's certificate with the TLSA information that it has obtained via DNSSEC.
- If the checksums correspond, the destination server is verified. If the checksums do not match, a DANE-activated client will immediately abort, because this looks suspiciously like it could be a "Man in the Middle" attack. Traditional clients would at this point cluelessly continue to transmit, and would send data to an untrustworthy destination.

So far, so good. So that DANE works with DNSSEC, both DANE and DNSSEC must be configured on the online retailer's mail server. In the case that an email service provider is used for sending emails, the email platform must be upgraded so that DNS requests also check for DNSSEC functionality and use its capabilities for verification.

The foundations have been around a long time. "DNSSEC is a mature and stable procedure that's been around for years," according to Patrick Koetter (Leader of the Competence Groups "Anti-Abuse" and "Email" at eco – Association of the Internet Industry). "Practical experience on large ISP platforms and and measurements show that the concerns of some administrators are simply not in line with the facts."

If you consider the financial consequences and the loss of reputation that a Downgrade Attack or "Man in the Middle" attack result in, the once-off expense for the activation of

DANE and DNSSEC is well worth it. They represent the only automated and cost-effective possibility for a truly secure data transmission between email servers.
Read more about related technologies and dive deeper into the topic in a workshop at the CSA Summit 2020.