Attachment in Emails – Useful? Or Unwanted Baggage?

Since its emergence, the email has established itself as a fast and uncomplicated communication medium. Alongside pure text, the email is also suitable for quickly exchanging small files like text documents and images. Although there are now a range of cloud-based services on offer for data exchange, the email is often still the first choice when data like documents and pictures need to be sent quickly to one or more recipients.

However, what seems to be useful in the private environment can turn out to be problematic in email marketing or generally in the communication with customers via email. Especially with transactional emails, which are often urgently awaited by the customer and can to a certain extent contain sensitive data, this can lead to problems.

The associated challenges and the possible consequences are explained in the following:

Attachments as a gateway for malware

Attachments are a popular and common gateway for malware. If criminals are interested in sending Phishing mails, then they will want to deliberately create the impression that the email has been sent from a trustworthy source. Depending on the type of Phishing, this could for example be purportedly the boss, a financial services provider, or an insurance company. This increases the probability and the danger that that these attachments will be opened.

Mostly, the attachments are also manipulated in such a way that they exploit the vulnerabilities of the application (e.g. PDF viewer), the email client, or the operating system to infect the computer of the email recipient. Once under the control of the criminal, the computer can become – unbeknownst to the user – part of a botnet, and then be used to send spam or participate in DDoS attacks. In the same way, criminals can gain access to all data on the computer of the email recipient.

As a result of this grave risk, mailbox providers and spam filters check attachments very carefully. As a consequence, the deliverability of these emails is negatively affected. Email clients warn against or even to a certain extent prevent the loading and execution of attachments. The corresponding consequence would be that recipients would not even receive these emails, or would be unable to read the attachment.

Lack of encryption means lack of data protection

Not every email server in the Internet supports STARTTLS as transport encryption. This procedure for initiating the encryption of a communication by means of Transport Layer Security serves to securely send, forward, and receive encrypted emails. Without the support of STARTTLS, both the content of the email and the associated attachments can be read by third parties. Even with STARTTLS, there is still the danger of "Man-in-the-Middle" (MITM) attacks, through which emails can be intercepted. A higher degree of security can only be achieved through additional protocols like DANE and DNSSEC. However, these are not yet well-established in the market. An additional danger is that the recipient unknowingly retrieves emails from the inbox unencrypted via an unsecured network.

It is not unusual for emails and attachments to contain sensitive content such as payment information or insurance or health data, which should not be read by unauthorized parties. This means that as a sender, it is worth considering what information is to be sent by email and what damage could occur if this information was to fall into the wrong hands. The sender will be held accountable if personal data is made public. In this case, the stipulations in Article 32 ff. GDPR apply. The supervisory authorities and the data subject must be informed of the security leak. The authorities can then impose sanctions against the sender, according to Article 58 GDPR.

For these reasons, email attachments should be avoided in the commercial environment. A recommendable alternative for email attachments is a (deep) link to a downloadable document in the company's own customer portal. There, by means of a secure TLS connection, the customer can see or download his/her own documents. In this way, the user also has the possibility to administer his/her documents centrally, without needing to search through an over-filled email client to find them individually. Regularly logging in to the portal can also create additional customer retention and the possibility to market other offers directly.

Authors: Technical Team
of the Certified Senders Alliance