SIBA Swiss Insurance Brokers Association

Basel, 26. September 2023

Mailverschlüsselung

In Sachen Verschlüsselung kann man generell folgendes festhalten:

Die weit verbreitete TLS-Verschlüsselung (Transport Layer Security) ist u.a.. für die Übermittlung von besonders schützenswerten Personendaten (bspw. Gesundheitsdaten) oder anderen heiklen Informationen grundsätzlich nicht ausreichend, da sie die E-Mail nur während dem Transport verschlüsselt. In diesen Fällen braucht es eine Verschlüsselung des Mailinhalts, so dass er auch im Postfach nur mit dem Entschlüsselungs-Schlüssel lesbar ist.

Weit verbreitete Standards für die Inhaltsverschlüsselung sind:

- S/MIME ist ein Standard für die Verschlüsselung und die digitale Signatur von E-Mail-Nachrichten. Es ist dafür gedacht, die Vertraulichkeit und Integrität von Nachrichten zu gewährleisten und die Authentizität des Absenders zu bestätigen.
- PGP oder GPG sind beliebte Alternativen zu S/MIME für die E-Mail-Verschlüsselung und digitale Signaturen. Diese Standards ermöglicht Benutzern, ihre E-Mails zu verschlüsseln und zu signieren, um die Vertraulichkeit und Authentizität zu gewährleisten.
- End-to-End-Verschlüsselungs-E-Mail-Dienste: Es gibt auch E-Mail-Dienste, die eine eingebaute End-to-End-Verschlüsselung bieten, wie ProtonMail oder Incamail.
- Übermittlung via Portale: Man kann auch mit einem Übermittlungsdienst/Portal arbeiten (bspw. eigenes Kundenportal), in welchem man die Daten zum Download anbietet. Indem man den Kunden Logindaten vergibt oder die Links zu den Dateien wiederum verschlüsselt, kann man sicherstellen, dass nur berechtigte Personen auf das Kundenportal zugreifen.

Es gibt keinen allgemein gültigen Inhaltsverschlüsselungsstandard, der in sämtlichen Mailpostfächern integriert ist. Der Schlüsselaustausch mit dem Empfänger ist nicht immer möglich (insbesondere mit Privatpersonen), da die entsprechenden Zertifikate nicht implementiert sind. Deshalb sollte darauf geachtet werden, eine Variante zu wählen, welche einerseits für die Kunden einfach handhabbar ist und andererseits für den Broker eine hohe Sicherheit bietet.

Wird gar keine der oben dargestellten Varianten verwendet und nur mit TLS gearbeitet, sollte von den Kunden bspw. via Mandatsvereinbarung eine Einwilligung eingeholt werden, dass besonders schützenswerte Personendaten auch unverschlüsselt versendet werden dürfen.

Swiss Insurance Brokers Association
Arnold Böcklin-Strasse 41
CH-4051 Basel
Telefon +41 58 590 46 78
info@siba.ch
www.siba.ch