„Kommunikation zwischen Versicherern und Rechtsanwälten einfach so per E-Mail? Eine riskante Angelegenheit!“

Auf Sicherheits- und Datenschutzfragen bei der E-Mail-Kommunikation angesprochen, gehen Versicherer und Anwälte gerne davon aus, dass doch alles in Ordnung sei, da E-Mails ja heutzutage standardmäßig verschlüsselt seien. Doch was ist hier ggf. verschlüsselt und wie sicher und datenschutzkonform ist der Austausch per E-Mail tatsächlich?

Richtig ist zwar, dass E-Mails auf ihrem Weg zum Empfänger in der Regel verschlüsselt werden. Allerdings ist Verschlüsselung nicht gleich Verschlüsselung. Bei der Standard-Verschlüsselung handelt es sich (nur) um eine Transportverschlüsselung (TLS). Dabei werden E-Mails jeweils auf dem Weg vom Client-Rechner des Absenders zum E-Mail-Server des Absenders, dann von dort zum E-Mail-Server des Empfängers und schließlich zum Client-Rechner des Empfängers verschlüsselt. **Auf den Client-Rechnern und insbesondere auf den Mailservern ruhen die E-Mails hingegen unverschlüsselt.**

Risiken in Bezug auf Vertraulichkeit und Integrität der übermittelten Nachrichten bestehen daher hinsichtlich der auf Mailservern gespeicherten Daten, z. B. wegen der ungehinderten Kenntnisnahme durch Mitarbeiter des Providers. Oftmals werden Empfänger und Absender die beteiligten Provider nicht einmal kennen; sie wissen also gar nicht, wo sich „ihre“ Post befindet. Und wer mag garantieren, dass beim Transport **nur Mailserver in Deutschland oder wenigstens in Europa beteiligt sind**? Auch können sich unbefugte Dritte mit einfachen Mitteln als Empfänger-Server ausgeben und – unbemerkt – E-Mails mitlesen („Man-in-the-Middle“).

Hoffnung alleine ist keine Risikobehandlung!

Risiken im Allgemeinen und speziell bei der Datenübermittlung – das muss man ehrlicherweise sagen – können nie gänzlich ausgeschlossen werden. Diese Erwartung hatte auch

der Gesetzgeber bei der DS-GVO nicht. Die sich stellende Frage lautet daher, in welchem Maße können und dürfen Datenschutzrisiken noch akzeptiert werden.

Der ganz wesentliche Faktor bei der Bestimmung von Risiken für die Rechte und Freiheiten betroffener Personen ist die Brisanz der übermittelten Daten. Der Inhalt von E-Mail-Kommunikation zwischen Versicherern und Anwälten kann – Verzeihung! – banal sein, weshalb in diesen Fällen von einem „normalen" Risiko ausgegangen werden kann, so dass die oben beschriebene, obligatorische Transportverschlüsselung ausreichend sein kann.

Oftmals wird die Kommunikation aber auch sensible Daten enthalten, bei denen in Fällen der unbefugten Kenntnisnahme, Manipulation, Weitergabe usw. massive Schäden bei betroffenen Personen zu besorgen sind. Gegenstand der Kommunikation können z. B. besondere Kategorien von Daten, wie Gesundheitsdaten, sein, strafrechtlich relevante Informationen oder Daten, die einem Berufsgeheimnis unterliegen usw. Hier ist von einem hohen Risikopotential auszugehen, so dass eine bloße Transportverschlüsselung den Anforderungen keineswegs genügt.

Nun ist es sicher nicht praktikabel (und zudem fehlerträchtig), jede beabsichtigte Übermittlung auf potentielle Risiken zu untersuchen und darauf basierend den evtl. (gerade noch) ausreichenden Übermittlungsweg zu wählen. Vielmehr läuft es darauf hinaus, bei der Kommunikation zwischen Versicherern und Anwälten grundsätzlich von einem potentiell hohen Risiko ausgehen zu müssen, womit die bloße Transportverschlüsselung als Standard ausscheidet und allenfalls in klaren Ausnahmefällen zur Verfügung steht.

Mögliche Folgen nicht ausreichend gesicherter Kommunikation

Art. 32 DS-GVO verpflichtet Verantwortliche, unter Berücksichtigung des Stands der Technik, des Risikos und anderer Faktoren angemessene technische und organisatorische Maßnahmen zu treffen. Anders gesagt: werden diese Maßnahmen unterlassen, liegt ein massiver Verstoß gegen die DS-GVO vor.

Dabei ist einmal natürlich **jede einzelne**, technisch nicht ausreichend gesicherte E-Mail als Datenschutzverletzung zu sehen.

Viel schwerer dürfte aber wiegen, wenn Verantwortliche organisatorisch nicht für angemessene Maßnahmen sorgen, also – auf einer Risikoanalyse basierend – unternehmensintern nachweislich konkrete und korrekte Vorgaben machen, wie zu kommunizieren ist. Die Datenschutzverletzung kann also bereits in einem „Laissez-faire" bestehen, welches indiziert, dass ein Datenschutzverstoß „billigend in Kauf" genommen wird, wobei es sich dann sogar um einen **vorsätzlichen Verstoß** handelt.

Diesem Vorwurf sehen sich ggf. die innerbetrieblich für die Organisation des Datenschutzes verantwortlichen Personen gegenüber, was **zur persönlichen Haftung auch der Geschäftsleitung** einer Kapitalgesellschaft führen kann. Dass ein solches Risiko bei Vorsatz nicht von einer Haftpflichtversicherung abgefedert wird, braucht hier sicher nicht erläutert zu werden.

Die DS-GVO fordert ein effektives Management von Datenschutz und Datensicherheit, was im Übrigen auch die **Kontrolle seiner Umsetzung** beinhaltet. Wegsehen oder Dulden von nicht datenschutzkonformer Kommunikation sind unentschuldbar. Vielmehr tut die Geschäftsleitung gut daran, wenigstens stichprobenartig zu überprüfen, ob ihre Vorgaben, soweit sie diese pflichtgemäß gemacht hat, auch eingehalten werden – und dies auch zu dokumentieren; denn sonst drohen hier **die nächsten Verstöße** – gegen Art. 32 Abs. 4 DS-GVO und die Nachweispflicht.

Der Vollständigkeit halber soll nicht unerwähnt bleiben, dass Vorstehendes nicht nur für das Versenden von Nachrichten, sondern entsprechend auch gilt für das Bereitstellen eines Empfangskanals („Schicken Sie es mir doch bitte einfach per E-Mail!“).

Was sind die Konsequenzen und wer muss sie tragen?

Ein „Organisationsverschulden“ trifft die Managementebene des Unternehmens; aber können sich **Sachbearbeiter oder sonstige Mitarbeiter** deswegen zurücklehnen? Bereits die allgemeine Treuepflicht eines Arbeitnehmers verpflichtet dazu, sich aktiv dafür einzusetzen, dass der Arbeitgeber keinen Schaden erleidet. Erst recht geraten Mitarbeiter ins Visier, wenn sie sich über Datenschutzvorgaben hinwegsetzen. Ungeachtet der Frage der datenschutzrechtlichen Verantwortlichkeit liegt hierin eine Verletzung des Arbeitsvertrages mit den entsprechenden Folgen (Abmahnung, Kündigung, Schadenersatz).

Droht bei einer Datenschutzverletzung etwa „nur“ ein Bußgeld? … Mitnichten!

Eine Datenschutzverletzung zieht den berüchtigten Rattenschwanz hinter sich her. Beispielsweise führt bereits eine einzelne, an einen falschen Empfänger versandte E-Mail grundsätzlich zur **Meldepflicht gegenüber der Aufsichtsbehörde** und möglicherweise auch zur Pflicht, **die betroffenen Personen hierüber zu informieren**. 10.000 E-Mails, deren Versand als Datenschutzverletzung einzustufen ist, potenzieren evident diese Verpflichtungen.

Erhält die Aufsichtsbehörde (so oder anders) von Verletzungshandlungen Kenntnis, quittiert sie dies mit „verhältnismäßigen, wirksamen und abschreckenden“ Bußgeldern, die im Zusammenhang mit nicht angemessenen technischen und organisatorischen Maßnahmen bis zu 10.000.000 Euro oder 2 % des letztjährigen Jahresumsatzes betragen können.

Nach dem aktuellen **Bußgeldkonzept der Datenschutzaufsichtsbehörden** beträgt ein Tagessatz eines Großunternehmens mit 3 Milliarden Euro Umsatz mithin über 8 Mio. Euro, wobei bereits ein leichter formeller Verstoß mit dem Faktor 2 zu Buche schlagen kann, also mit über 16 Mio. Euro – ohne dass in diesem Beispiel zusätzlich erhöhende Faktoren, wie Vorsatz, berücksichtigt werden.

Davon unabhängig können Datenschutzverstöße selbstverständlich auch noch **Schadenersatzansprüche** von Seiten betroffener Personen zur Folge haben.

Vor diesem Hintergrund dürfte sowohl für die Geschäftsleitung als auch für Mitarbeiter auch nur eine geringe, anteilige Haftung nicht erstrebenswert sein.

Fazit

Die Kommunikation zwischen Versicherern und Anwälten bedarf eines höheren Sicherheitsstandards als ihn die einfache (transportverschlüsselte) E-Mail zu bieten vermag. Wer diese Erkenntnis ignoriert, setzt sich einem beträchtlichen Risiko wegen potentieller Datenschutzverletzungen aus.

Kommen die genannten Übermittlungswege mithin nicht in Betracht, verbleiben nur **alternative Übermittlungsmethoden bzw. Kommunikationskanäle** – also weg von der E-Mail.

In Betracht kommen hier Webservices bzw. GDV-Branchennetz-Services von spezialisierten Dienstleistern, wobei Datenverbindungen nach dort bzw. von dort ebenfalls verschlüsselt sind. Auf dem Server ruhende Daten sind dabei in der Regel zwar ebenfalls nicht verschlüsselt, weil dann die Funktionalitäten des Systems nicht oder jedenfalls nicht vollständig in Anspruch genommen werden könnten.

Allerdings ist bei einem datenschutzkonform arbeitenden Dienstleister klar definiert, wo konkret die Daten sich befinden und (namentlich) welche Administratoren theoretisch Kenntnis von Inhalten erlangen könnten. Mit dem Dienstleister können über einen Vertrag zur Auftragsverarbeitung konkrete technische und organisatorische Maßnahmen vereinbart werden, und Anwälte haben die Möglichkeit, den Dienstleister über eine Vereinbarung zur beruflichen Verschwiegenheit berufsrechtskonform einzubinden.

Um das Thema zu vertiefen, stehe ich Ihnen gerne zu einem Gespräch zur Verfügung:

Tel.: 0681 / 950 82 80
E-Mail: dbm@e-consult.de
LinkedIn: https://www.linkedin.com/in/dominik-bach-michaelis-414392155