0800 400 510 1

AKTUELLE INFORMATION
E-MAILS - VERSCHLÜSSELN ODER DOCH NICHT?

Datenschutz - Nr. 2/2020

Datenschutz

Wir entlasten Führungskräfte und schützen Mitarbeiter. Seit 1997.

E-Mails - Verschlüsseln oder doch nicht verschlüsseln?

Täglich werden global eine Vielzahl von E-Mails über das Internet verschickt. Hierzu finden die unterschiedlichsten E-Mail-Programme von verschiedenen Anbietern Verwendung. Diese nutzen für den Versand der Nachricht wiederum diverse Knotenpunkte im Web. Da das Internet nicht generell verschlüsselt ist, kann die E-Mail dann möglicherweise mitgelesen werden. Für Unternehmen ist es naheliegend, dass sie diese Dateien verschlüsseln. Zumal dies im Rahmen der DSGVO auch teilweise gefordert wird.
Immer mehr Unternehmen stehen daher vor der Wahl ob E-Mails verschlüsselt werden oder nicht. Kommt es aufgrund vielfältiger Faktoren zu einer Bejahung, folgt schon die nächste Frage, nämlich nach dem „Wie soll ich das nur umsetzen?".

Was sind die gesetzlichen Grundlagen?

In dem Art. 5 Abs. 1 lit. f DSGVO werden explizit **geeignete technische und organisatorische Maßnahmen** gefordert, welche personenbezogene Daten angemessen sichern, sowie vor unberechtigter oder unbefugter Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung, oder unbeabsichtigter Schädigung schützen. Des Weiteren finden wir im Art. 32 Abs. 1 Satz 1 DSGVO den Hinweis auf „geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten"; sowie im Art. 32 Abs 1 lit. a DSGVO die „Verschlüsselung von Daten". Auch finden wir im Art. 32 Abs. 1 Satz 1 DSGVO den Verweis auf die „Orientierung am Stand der Technik".

Muss ich nun alle meine Mails verschlüsseln?

Hier ein definitives **Nein**. Für personenbezogene Daten, die per E-Mail versendet werden, gibt es keine speziellen Vorgaben, insbesondere keine unbedingte Pflicht zur Verschlüsselung. Ob der Versender eine E-Mail verschlüsseln muss, hängt zunächst vom Schutzbedarf der übertragenen Daten ab. Wie zuvor beschrieben, ist der Art. 32 DSGVO maßgeblich für die Bewertung, ob eine Verschlüsselung benötigt wird.

Leistungsangebot Datenschutz

- Externer Datenschutzbeauftragter gemäß DSGVO
- Sicher zum Verarbeitungsverzeichnis
- Betroffenenrechte & Mitteilungspflichten steuern
- Webseiten rechtskonform gestalten
- Audits & Bestandsaufnahmen durchführen
- Informationspflichten praktikabel umsetzen
- Auftragsverarbeitungen transparent und sicher

WIE KÖNNEN WIR IHNEN HELFEN?

FKC CONSULT GmbH
Eschenburgstr. 5
23568 Lübeck
www.fkc-gmbh.de

datenschutzberatung@fkc-gmbh.de

0800 400 510 1

AKTUELLE INFORMATION
E-MAILS - VERSCHLÜSSELN ODER DOCH NICHT?

Datenschutz - Nr. 2/2020

Datenschutz

Somit muss ein angemessenes Schutzniveau gewährleistet werden. Soweit ein Bestandteil der Kommunikation kein Austausch sensibler Informationen ist, es z.B. nur um eine rein organisatorische Abstimmung geht, kann auf eine Verschlüsselung durchaus verzichtet werden. Die Grenze zur „Angemessenheit“ ist aber schnell und nicht immer trennscharf überschritten. Dann sind Maßnahmen der Verschlüsselung zu ergreifen.

Welche Verschlüsselungen gibt es?

Grundsätzlich unterscheidet man zwei Arten der E-Mail-Verschlüsselung: die Punkt-zu-Punkt- beziehungsweise Transportverschlüsselung und die End-to-End-Verschlüsselung:

- **Transportverschlüsselung**

Bei der **Transportverschlüsselung** wird zwischen dem E-Mail-Programm und dem Server eine Verbindung aufgebaut und diese z.B. gemäß dem weit verbreiteten Protokoll **"Transport Layer Security" (TLS)** (frühere Bezeichnung SSL, Secure Socket Layer-Verschlüsselung) verschlüsselt. Alle Daten, im Austausch zwischen den beiden Kommunikationspartnern, sind dann während des Versands verschlüsselt. Beim weiteren Versand über unterschiedliche Knotenpunkte im Web zum Empfänger erfolgt die Weiterleitung über diverse Punkte und ist dazwischen nicht zwingend verschlüsselt. Die E-Mail liegt dann sowohl beim E-Mail-Anbieter als auch an den Knotenpunkten des Versands unverschlüsselt vor.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, dass eine TLS-Verschlüsselung erst ab der Version 1.2 zuverlässig ist. Die richtige Konfiguration ist daher unerlässlich. Oftmals ist der Haken bei „Optional TLS“ gesetzt. So erfolgt die Verschlüsselung dann aber nur, wenn dies möglich ist. Ansonsten wird die E-Mail unverschlüsselt übermittelt. Daher sollte unbedingt auf „Mandatory TLS“ gestellt sein. Im Zweifelsfall wird die E-Mail dann nicht versendet und informiert Sie darüber. Mit einem Secure E-Mail-Gateway setzen Sie TLS flächendeckend um. Da hier verschiedene Verschlüsselungsverfahren möglich sind, stellt das Gateway eine verschlüsselte Kommunikation sicher.

Vorsicht ist bei Austausch des Servers, Anpassung der Konfiguration, Ablauf der Gültigkeit und Nichtanerkennung der Gegenstelle geboten, denn dies kann dazu führen, dass bisher sichere TLS-Zertifikate wieder unsicher sind.

0800 400 510 1

AKTUELLE INFORMATION
E-MAILS - VERSCHLÜSSELN ODER DOCH NICHT?

Datenschutz - Nr. 2/2020

Datenschutz

- **End-to-End-Verschlüsselung**

Im Unterschied zur Transportverschlüsselung werden bei der **End-to-End-Verschlüsselung** nicht die einzelnen Abschnitte im Versandkanal verschlüsselt, sondern jede einzelne E-Mail selbst. Das Lesen ist dann nur dem Sender und Empfänger möglich, wenn diese über den erforderlichen Schlüssel verfügen. Weder können die E-Mail-Anbieter die E-Mail lesen, noch haben mögliche Angreifer die Möglichkeit, diese E-Mails unterwegs zu manipulieren. **Damit erfüllt nur diese Technik die drei Ziele der Verschlüsselung im Internet: Vertraulichkeit, Authentizität, Integrität.**

Einer unverschlüsselten Kommunikation ist daher die Transportverschlüsselung zu bevorzugen. **Doch gerade bei sensiblen oder persönlichen Inhalten empfiehlt es sich, den Einsatz einer End-to-End-Verschlüsselung.** Bislang gestaltete sich der Einsatz dieser Kryptografie Technik noch als mühselig. Der Benutzer musste bei der End-to-End Verschlüsselung selbst aktiv werden, um die Technologie nutzen zu können. Allerdings ist dies unter anderem mit einem vom BSI entwickelten Protokoll richtungsweisend vereinfacht und so Usern zugänglicher gemacht worden. Bei der End-to-End-Verschlüsselung ist das Standardprotokoll OpenPGP für die PGP Verschlüsselung sowie das Protokoll S/MIME gebräuchlich. Verbreitet sind auch die RMS (Microsoft Rights Management Services). Diese sind für die Azure Cloud und für den On-Premises-Einsatz geeignet.

Man unterscheidet zwischen **asymmetrisch und symmetrisch** bei den **Verschlüsselungsverfahren**. Ein Austausch des Schlüssels zum Verschlüsseln und Entschlüsseln der Nachrichten ist bei beiden Kommunikationspartnern erforderlich. Unterschiede findet man hierbei, wie viele Schlüssel erzeugt werden und welche öffentlich weitergegeben werden.

Bei dem **symmetrischen Verschlüsselungsverfahren** wird für **beide Kommunikationspartner derselbe Schlüssel** eingesetzt, um eine E-Mail zu verschlüsseln und zu entschlüsseln. Dieser **muss vor der Kommunikation** auf einem **sicheren Weg** zwischen **beiden Partnern ausgetauscht** und von beiden **geheim gehalten werden.** Nachteilig ist es, dass diese Art der Verschlüsselung von Nachrichten innerhalb großer und offener Nutzergruppen, wie dies beim E-Mail-Verkehr der Fall ist, wegen der problematischen Schlüsselverteilung nicht geeignet ist. Vorteilhaft ist es, dass auch große Datenmengen schnell ver- und entschlüsselt werden können.

Bei dem **asymmetrischen Verschlüsselungsverfahren** wird ein Schlüsselpaar **aus öffentlichem und privatem Schlüssel** erzeugt. Die meisten E-Mail-Programme bzw. deren Plugins unterstützen dies. Der **private Schlüssel** wird nur von dessen Eigentümer verwendet und **geheim** gehalten. Der **dazugehörige öffentliche Schlüssel** wird allen **möglichen Kommunikationspartnern zur Verfügung** gestellt. Vergleichbar ist der öffentliche Schlüssel hierbei mit einem herkömmlichen geöffneten Vorhängeschloss, welches von jedermann ver-

0800 400 510 1

AKTUELLE INFORMATION
E-MAILS - VERSCHLÜSSELN ODER DOCH NICHT?

Datenschutz - Nr. 2/2020

Datenschutz

schlossen werden kann, sich aber nur vom Besitzer des dazugehörigen privaten und geheimen Schlüssels wieder öffnen lässt. Für eine sichere Übermittlung wird die Nachricht mit dem öffentlichen Schlüssel des Empfängers vom Absender verschlossen. Das Öffnen ist nur mit dem privaten Schlüssel möglich.

Hilfe zur E-Mail-Verschlüsselung

- Muss die Mail überhaupt verschlüsselt werden? Denkbar ist als Alternative auch das Versenden einer Datei mit Passwortschutz mit separatem Kommunikationskanal für das Passwort.
- Für welche E-Mails möchten Sie Transport- (Punkt-zu-Punkt-) und/oder Inhaltsverschlüsselungen (End-to-End-Verschlüsselungen) nutzen:
  Mit Punkt-zu-Punkt-Verschlüsselungen sind die Metadaten wie am Kontakt beteiligte E-Mail-Adressen, Betreffzeilen u.Ä. geschützt.
  Mit End-to-End-Verschlüsselungen sind die Inhalte und Anhänge Ihrer E-Mails geschützt.
- Überlegen Sie, ob die Standardisierung von Verschlüsselungsverfahren für Ihr Unternehmen sinnvoll ist.
- Nutzen Sie einen zuverlässigen Webclient:
  Bietet der Webclient eine SSL-verschlüsselte HTTPS-Verbindung und die Möglichkeit einer Transportverschlüsselung?
  Ist der Webclient mit der von Ihnen favorisierten Inhaltsverschlüsselungssoftware kompatibel?
  Ist eine Verschlüsselung eines ganzen E-Mail-Postfachs sinnvoll?
  Achten Sie darauf, dass US-Anbieter amerikanischem Recht unterstellt sind (Stichpunkt NSA-Affäre).
- Sind alle E-Mails mit besonders sensiblen oder personenbezogenen Informationen, die nach DSGVO verpflichtend zu verschlüsseln sind, auch verschlüsselt?
- Sind besonders sensible Daten mit Passwörtern verschlüsselt und gehen diese Ihren Kontakten auf anderem Kommunikationsweg zu?
- Existiert ein firmeninterner Leitfaden zur E-Mail-Verschlüsselung?
- Existieren Schulungen und Fortbildungen für Ihre Mitarbeiter?
- Ist ein externer IT-Dienstleister beteiligt, welcher sich um eine möglichst sichere und wirksame Verschlüsselung kümmert?
- Löschung ohne Zustimmung

Wie Sie sehen, ist das Thema rund um die Verschlüsselung von E-Mails nicht so einfach zu beantworten. Können wir Ihnen daher bei der Umsetzung behilflich sein? Gerne sind unsere erfahrenen Berater für Sie da, um mit Ihnen eine datenschutzkonforme Umsetzung zu planen und zu begleiten!

datenschutzberatung@fkc-gmbh.de