PRIVAZYPLAN®
BRINGT IHREN DATENSCHUTZ AUF KURS.

Verschlüsselung von E-Mails im Falle von besonderen Kategorien „sensibler“ Daten

Verschlüsselung von E-Mails im Falle von besonderen Kategorien „sensibler“ Daten

Die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) in Nordrhein-Westfalen hat eine wichtige Mitteilung publiziert:

Technische Anforderungen an technische und organisatorische Maßnahmen beim E-Mail-Versand

Wie ist die Datenschutz-Grundverordnung (DS-GVO) in Bezug auf den unverschlüsselten Versand von E-Mails zu interpretieren?

E-Mails enthalten zusätzlich zu den Inhaltsdaten (d.h. dem Text der Mail und etwaigen Anhängen) auch Metadaten wie Absender und Empfänger, das Datum und den Betreff.

Sowohl Inhalts- als auch Metadaten können personenbezogene Daten beinhalten. Daher sind bei der datenschutzrechtlichen Beurteilung beide Datenarten zu berücksichtigen.

Nach Art. 32 DS-GVO sind geeignete und angemessene Maßnahmen zu treffen, um die Sicherheit der Verarbeitung personenbezogener Daten und damit auch deren Vertraulichkeit sicherzustellen. Das Bundesdatenschutzgesetz (BDSG) und das Datenschutzgesetz Nordrhein-Westfalen in der jeweils bis zum 24.05.2018 gültigen Fassung stellen vergleichbare Anforderungen. Die in Art. 32 Abs. 1 lit. a) genannten Maßnahmen „Pseudonymisierung“ und „Verschlüsselung“ sind als Beispiele für Standardmaßnahmen zu verstehen, d.h. sofern ihr Einsatz möglich und angemessen ist, sind sie grundsätzlich umzusetzen.

Bei der Übermittlung von E-Mails ist grundsätzlich zwischen einer Verschlüsselung auf Inhaltsebene und einer Verschlüsselung auf Transportebene zu unterscheiden.

Inhaltsebene
Für die Verschlüsselung des Textes einer E-Mail sowie von Anhängen kommen in erster Linie die Standards S/MIME und OpenPGP infrage. Beide Standards unterstützen darüber hinaus digitale Signaturen, um Manipulationen auf dem Übertragungsweg entdecken zu können.

Mit S/MIME und OpenPGP ist eine Ende-zu-Ende-Verschlüsselung möglich, d.h. die Nachricht wird auf dem System des Absenders verschlüsselt und auf dem System des Empfängers entschlüsselt und liegt auf dem Übertragungsweg niemals im Klartext vor.

Die Metadaten werden von der Inhaltsverschlüsselung jedoch nicht erfasst, sie liegen auf den an der Übertragung beteiligten Servern im Klartext vor.

Transportebene
Bei einer Verschlüsselung auf Transportebene werden sowohl Meta- als auch Inhaltsdaten auf der Verbindung zwischen Mail-Client und Server bzw. zwischen verschiedenen Mail-Servern verschlüsselt. Dadurch ist sichergestellt, dass die E-Mail während des Transports über unsichere Netze wie dem Internet von Dritten nicht mitgelesen werden kann. Auf den beteiligten Mail-Servern liegt die E-Mail jedoch im Klartext vor.

Bezüglich der sicheren Implementierung der Transportebene hat das Bundesamt für Sicherheit in der Informationstechnologie die Technische Richtlinie „BSI TR-03108-1: Secure E-Mail Transport“ herausgegeben.

Unter datenschutzrechtlichen Gesichtspunkten ist diese Richtlinie als Stand der Technik zu betrachten, so dass ihre Umsetzung eine notwendige Voraussetzung für die datenschutzkonforme E-Mail-Kommunikation ist.

Fazit
Eine umfassende Absicherung der E-Mail-Kommunikation setzt den Einsatz von sowohl Transport- als auch Inhaltsverschlüsselung voraus.

Bei der Entscheidung, ob eine Ende-zu-Ende-Verschlüsselung erforderlich ist, sind der Schutzbedarf der übertragenen Daten sowie die Angemessenheit der Maßnahme zu berücksichtigen. Sollen Daten mit hohem oder sehr hohem Schutzbedarf, insbesondere die in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien personenbezogener Daten übermittelt werden, ist eine Ende-zu-Ende-Verschlüsselung erforderlich. Da Metadaten einer E-Mail nicht durch Ende-zu-Ende-Verschlüsselung geschützt werden, ist sicherzustellen, dass sie keine Daten mit hohem oder sehr hohem Schutzbedarf enthalten. Insbesondere ist der Betreff neutral zu wählen, beispielsweise „Unser Gespräch am 01.02.“ statt „Ihre Blutwerte“.

Bei der Übermittlung personenbezogener Daten mit normalem Schutzbedarf besteht die Möglichkeit, dass im Einzelfall der Verzicht auf eine Ende-zu-Ende-Verschlüsselung der Inhaltsdaten statthaft ist.
Ein ausdrücklicher Wunsch des Empfängers nach Ende-zu-Ende-Verschlüsselung sollte jedoch in jedem Fall berücksichtigt werden.
Als Mindeststandard ist auch bei der Übermittlung personenbezogener Daten mit normalem Schutzbedarf eine Transportverschlüsselung erforderlich. Dazu ist beim Aufbau einer eigenen E-Mail-Infrastruktur die o.g. BSI-Richtlinie einzuhalten bzw. die Einhaltung der Richtlinie bei der Auswahl des E-Mail-Providers als obligatorisches Kriterium zu berücksichtigen.

In Abhängigkeit von der Art und dem Umfang der per E-Mail versandten Daten kann im Einzelfall die vorherige Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO erforderlich sein.

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestr. 2-4
40213 Düsseldorf
Telefon: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

Quelle: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand/Technische-Anforderungen-an-technische-und-organisatorische-Massnahmen-beim-E-Mail-Versand.html [Hervorhebungen und Hyperlinks durch Nicholas Vollmer]

Es lohnt sich, die obigen Ausführungen mehrmals Wort für Wort zu lesen. Der Inhalt hat es in sich! Möglicherweise wird man bald in NRW (und ggf. auch bundesweit) bald an diesen Maßstäben gemessen. Betroffen ist jeder, der E-Mails zu nicht-privaten Zwecken verschickt und Empfängt: Unternehmen, Verbände, Vereine, Stiftungen, Vermieter, Behörden etc.

Was bedeutet das ganz konkret?

Der externe Datenschutzbeauftragte, Herr Nicholas Vollmer, möchte dies im Folgenden präzisieren und interpretieren.

1.) Anforderungen an die Transportverschlüsselung

Die Aufsichtsbehörde fordert die Auswahl eines sicheren E-Mail-Dienstanbieters gemäß „BSI TR-03108-1: Secure E-Mail Transport“. Dies umfasst zwei wichtige Technologien:

- TLS: https://de.wikipedia.org/wiki/Transport_Layer_Security
- DANE: https://de.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities
  gut erklärt auch hier und hier bei heise

Die diesbezügliche Sicherheit eines E-Mail-Servers kann man hier testen:

- https://ssl-tools.net/mailservers (prüft TLS und DANE)
- https://www.checktls.com/index.html (prüft TLS, aber nicht DANE)

Die Transport-Verschlüsselung ist im Kapitel 11.2.2 im TOM-Guide® beschrieben und wohl wirklich de facto Stand der Technik (nicht zuletzt deswegen, weil die Bayerische Aufsichtsbehörde dies im August 2014 so postuliert hat).

Doch welche Ergebnisse hinsichtlich DANE liefert der Test auf SSL-Tools am 26.03.2018?

- Eine Prüfung aller deutschen Datenschutz-Aufsichtsbehörden hat ergeben, dass zumindest die E-Mail Server in Bayern und Mecklenburg-Vorpommern per DANE geschützt sind.
- Einen DANE-Schutz ist erkennbar bei Mail.de, Freenet.de, Web.de, Gmx.de. Bei vielen anderen Anbietern in Deutschland scheint kein DANE-Schutz vorzuliegen.
- Unklar ist die Sachlage bei Posteo.de (dort gab es einen DANE-Fehler beim Test). Auch der E-Mail Server der Microsoft-Deutschland-Cloud (@onmicrosoft.de) war irgendwie nicht testbar.

Ein Großteil der E-Mails sind somit nicht mittels DANE geschützt. Vom „Stand der Technik“ kann man also nicht unbedingt sprechen.

➔ Jeder Verantwortliche sollte versuchen die DANE-Technologie zu aktivieren. Im Einzelfall kann dies problematisch sein; beispielsweise der Anbieter *DomainFactory* kann dies generell nicht aktivieren. Es bleibt abzuwarten, ob die Aufsichtsbehörden das DANE-Feature aktiv kontrollieren und ggf. bemängeln.

2.) Anforderungen an die Inhaltsverschlüsselung

Für eine Ende-zu-Ende-Verschlüsselungen kommen insbesondere die beiden folgenden Technologien in Frage (siehe u.a. Kapitel 11.2 im TOM-Guide®):

- PGP (siehe auch hier)
  Insbesondere diese drei MS-Windows-Programme stehen zur Auswahl: GPG4Win, gpg4o und p=p.
  Eine Liste (fast) aller Anbieter für (fast) alle Betriebssysteme findet sich hier.
- S/MIME (bitte beachten Sie die Hinweise im Kapitel 11.2.5 im TOM-Guide®)
  Hier werden Zertifikats-Dateien gekauft und auf Servern bzw. Clients installiert.

In Einzelfällen kann es auch reichen, dass man die Informationen separat verschlüsselt und als Datei-Anhang einer E-Mail versendet. Dies ist möglich per:

- ZIP mit Kennwort (siehe hier… ein besonders praktikabler und kompatibler Ansatz)
- PDF mit Kennwort
- MS-Office-Dokumente mit Kennwort

Diese letztgenannten drei Methoden sind aber wohl nicht anwendbar, wenn man massenweise E-Mails mit vielen verschiedenen Personen austauschen will. In allen Fällen müsste man nämlich auf separatem Weg ein individuelles Verschlüsselungs-Passwort vereinbaren.

Die Einrichtung der etablierten Wege per PGP und/oder S/MIME sind mitunter kompliziert und unflexibel. Daher ist es nicht überraschend, dass kaum jemand diese Technologien nutzt. Nichtsdestotrotz wird man sich mit derlei Technologien auseinandersetzen müssen, wenn man die Forderungen der NRW-Datenschutz-Aufsichtsbehörde erfüllen will.

➔ Falls die Wahl auf PGP fällt, so scheint die Software gpg4o empfehlenswert; sie ist sehr einfach zu benutzen und somit sehr viel komfortabler als GPG4Win (innerhalb weniger Minuten ist alles erledigt).

3.) Fazit von Herrn Vollmer (bezüglich des obigen NRW-Schreibens vom März 2018)

Die durch DANE verbesserte Transportverschlüsselung ist technologisch wohl eine große Herausforderung. Viele E-Mail-Dienstanbieter scheinen auf „BSI TR-03108“ nicht vorbereitet zu sein. Es wird sich zeigen, ob dies zu handfesten Problemen mit den Datenschutz-Aufsichtsbehörden führen wird.

Wenn ein Unternehmen aufgrund seines Geschäftsfeldes damit rechnen muss, dass besondere Kategorien „sensibler“ Daten (im Sinne des Artikel 9 DS-GVO) per E-Mail gesendet oder empfangen werden, so muss eine Ende-Zu-Ende-Verschlüsselung angeboten werden.

Vermutlich ist man auf der sicheren Seite, wenn man PGP oder S/Mime anbietet.

Unabhängig von der genutzten Technologie sollte der Verantwortliche auf seiner Internetpräsenz einen Hinweis auf die Ende-zu-Ende Verschlüsselung geben.

Die NRW-Aufsichtsbehörde macht es vor:

Sichere E-Mail:

Wenn Sie sicher sein wollen, dass Ihre E-Mail auf dem Weg zu uns ungelesen bleibt, verschlüsseln Sie Ihre Nachricht. Dazu können Sie unseren öffentlichen **PGP-Schlüssel** verwenden.

Der dazugehörige Fingerprint lautet :

C638 12C7 8854 FBF9 BEB6 3A40 04E3 1A13 6AD6 2811

Kostenlose Programme zur Verschlüsselung finden Sie zum Beispiel unter **GnuPG**.