Technisch- Organisatorische Maßnahmen zum sicheren E-Mail Versand

E-Mail ist nach wie vor das wichtigste Kommunikationsmittel Geschäftsverkehr, auch wenn Messenger und andere Kommunikationskanäle immer stärker genutzt werden. Wie aber Geschäftsgeheimnisse und personenbezogene Daten in E-Mails wirksam geschützt werden können, ist oft noch ein Buch mit sieben Siegeln.

Frage

Bei der Übermittlung personenbezogener per E-Mail Daten müssen gemäß Art. 32 DSGVO technische und organisatorische Maßnahmen getroffen werden, um ein angemessenes Schutzniveau zu erreichen. Ähnliches gilt für Geschäftsgeheimnisse. Werden diese beim Versand nicht angemessen geschützt, so verlieren sie den Status eines Geschäftsgeheimnisses nach §2 Nr. 1 b) des Gesetzes zum Schutz von Geschäftsgeheimnissen. Die große Frage ist aber, was ist jeweils angemessen, und wie erreicht man einen angemessenen Schutz?

Analyse

Bisher wurden im Bereich Datenschutz E-Mails oft mit Postkarten verglichen, die einfach von allen gelesen werden können, die auf sie zugreifen können. Dieser Vergleich trifft nicht mehr zu, seit von den Datenschutzbehörden erwartet wird, dass Firmen ihre Mailserver mit TLS Verschlüsselung ausstatten. Damit sind E-Mails zumindest auf dem Transportweg sicher geschützt. In einer kürzlich veröffentlichten Arbeitshilfe hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) dazu jetzt festgestellt, dass, in Abhängigkeit von den damit verbundenen Risiken, eine Transportverschlüsselung ausreichend ist. Alternativ können natürlich die Daten vor dem Versand auch sicher verschlüsselt werden und der Schlüssel über einen zweiten und sicheren Kanal zwischen Sender und Empfänger ausgetauscht werden.

Für **Empfänger** ergibt sich zumindest die Pflicht, ihre Mailserver so zu konfigurieren, dass sie eine TLS Verschlüsselung nach dem Stand der Technik unterstützen. Bei dem Empfang von besonders sensiblen Informationen müssen auch Maßnahmen implementiert werden, die sicherstellen, dass Nachrichten auch bei dem gewünschten Empfänger ankommen. Spätestens bei dem Versand von Berufsgeheimnissen, die dem §203 StGB unterliegen, ist zuletzt eine Ende-zu-Ende Verschlüsselung erforderlich.

Für **Versender** von E-Mails ergeben sich ähnliche Pflichten. So muss auch bei dem Versand von personenbezogenen Daten mit „normalem Risiko“ sichergestellt werden, dass die E-Mail nur verschickt wird, wenn der Empfänger auch TLS Verschlüsselung anwendet. Bei hohen Risiken sollte über die technische Maßnahmen sichergestellt werden, dass die E-Mail auch bei dem gewünschten Empfänger ankommt und ein Abfangen durch einen Angreifer wirksam unterbunden wird.

Maßnahmen

Um den sicheren und den gesetzlichen Vorgaben entsprechenden Versand von E-Mails sicherzustellen, sind - in Abhängigkeit von der Art der ausgetauschten Informationen - eine

Reihe von technischen und organisatorischen Maßnahmen umzusetzen. Bei der Umsetzung der technischen Maßnahmen soll man sich dabei an den Technischen Richtlinien des BSI TR 02102-2 und TR 03108-1 orientieren

Grundlegende Maßnahmen

Für den Versand auch von personenbezogenen Daten per E-Mail müssen folgende technischen und organisatorischen Maßnahmen umgesetzt werden:

- Richtlinie zum Versand von E-Mails mit personenbezogenen Daten oder Geschäftsgeheimnissen
- Sichere Transportverschlüsselung mit TLS/STARTTLS
- Perfect Forward Secrecy
- Zwingende TLS Verschlüsselung beim Versand

Maßnahmen für E-Mail Nachrichten mit hohem Risiko

Sollten personenbezogene Daten verschickt werden, die ein hohes Risiko für die Betroffenen beinhalten, sind zusätzliche technische Maßnahmen erforderlich. Hohe Risiken können beispielweise bei dem Versand von besonderen personenbezogenen Daten wie Informationen zu sexueller Orientierung und Gesundheitsdaten oder Daten zu besonders schützenswerten Personengruppen wie Kindern auftreten. Hier sind technische Maßnahmen wie

- DANE
- DNSSEC
- DKIM
- Verwendung offizieller statt selbst-signierter Zertifikate auf den Mailservern
- Verschlüsselungstools zum sicheren Versand von Dateien

in Betracht zu ziehen.

Maßnahmen für E-Mail Nachrichten mit geheim zu haltenden Inhalten

In erster Line betrifft dies Nachrichten mit Privatgeheimnissen bzw. Berufsgeheimnissen nach §203 StGB. Also Daten aus der Tätigkeit von Ärzten, Anwälten, Personal- oder Betriebsräten etc. Hier ist eine Ende-zu-Ende Verschlüsselung als verpflichtend anzusehen, z.B. mittels

- S/Mime
- PGP
- sicheren Dateiverschlüsselungstools

Nächste Schritte

Die Umsetzung der Maßnahmen wie beispielsweise einer Email-Verschlüsselung hat immer auch Auswirkungen auf andere Prozesse, wie Archivierung oder die Hinterlegung von Schlüsseln. Um herauszufinden, welche Maßnahmen für Sie angemessen sind, bietet Ihnen die Süd IT an in einem Workshop Ihre Anforderungen zu erfassen und Lösungen zu skizzieren. Gerne unterstützen wir Sie auch bei der Umsetzung dieser Maßnahmen, die von einer sicheren Konfiguration vorhandener Infrastruktur über Einführung von Perimeter-Verschlüsselung bis hin zur kompletten Auslagerung der E-Mailserver reichen kann.

Resümee

Zwingend umzusetzen sind immer die angegebenen grundlegenden Maßnahmen. Welche der weiterführenden Maßnahmen jeweils umgesetzt werden müssen, hängt stark von der Art der ausgetauschten Informationen sowie der technischen Infrastruktur ab. Die Süd IT unterstützt Sie bei Bedarf gerne bei der Planung und Umsetzung sowohl der organisatorischen wie technischen Maßnahmen.

Weiterführende Informationen

1. DSGVO
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
2. Gesetz zum Schutz von Geschäftsgeheimnissen
   http://www.gesetze-im-internet.de/geschgehg/
3. Orientierungshilfe E-Mail Verschlüsselung
   https://www.datenschutzkonferenz-online.de/media/oh/20200526_orientierungshilfe_e_mail_verschluesselung.pdf
4. Kryptographische Verfahren: Empfehlungen und Schlüssellängen
   https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
5. BSI Richtlinien für den sicheren E-Mail-Transport
   https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03108/index_htm.html
6. StGB § 203 Verletzung von Privatgeheimnissen
   https://www.gesetze-im-internet.de/stgb/__203.html

Kontakt

Falls Sie noch Fragen zu dem Thema haben freue ich mich auf Ihre Kontaktaufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de

Lead-Auditor ISO/IEC 27001, ISO 22301, kritische Infrastrukturen gemäß §8a BSIG
Lead-Auditor & Fachexperte IT-Sicherheitskatalog
VdS-zertifizierter Berater für Cyber-Security,
Datenschutzbeauftragter IHK