Anlage ANH003/22

zur Beantwortung 1 des Fragenkataloges von Torben Berndt zur Sitzung des Ortsrates Barmke am 22.02.2022

Verschlüsseln von E-Mails

Spätestens seitdem die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten ist, gilt es, besonders vorsichtig mit sensiblen Daten umzugehen. Die E-Mail-Kommunikation ist dabei keine Ausnahme.

Bestimmte E-Mails zu verschlüsseln, ist aber schon länger Pflicht: Schon das Bundesdatenschutzgesetz, der Vorgänger der DSGVO, verpflichtete Unternehmen dazu. Doch in Deutschland taten das 2016 laut einer Studie von „Deutschland sicher im Netz“ (DsiN) nur 16 Prozent der befragten Unternehmen.

Nachfolgend geht es daher um folgende Fragestellung:

- Wann ist es nötig, eine E-Mail zu verschlüsseln und wie mache ich das?

Grundsätzlich sollten Sie sich immer bewusst sein, welche Informationen Ihre E-Mail enthält. Vergleichen Sie einfach Ihre E-Mail- Kommunikation mit der Kommunikation, die vor 30 Jahren durchaus üblich war. Belanglose Urlaubsgrüße haben Sie per Postkarte (unverschlüsselt) verschickt. Liebesbriefe wurden schon kuvertiert (verschlüsselt), damit der Postbote nicht mitlesen konnte. Und im Geschäftsbereich haben Sie dick und fett „persönlich“ auf den Briefumschlag geschrieben, um sicherzugehen, dass auch nur der Empfänger den Inhalt liest und nicht der Mitarbeiter der Poststelle.

Das gleiche Prinzip gilt auch bei der E-Mail-Kommunikation. Enthält Ihre E-Mail personenbezogene Daten, muss die E-Mail verschlüsselt werden. Da der Begriff „Personenbezogene Daten“ sehr weitreichend ist, stellen sich jetzt einige von Ihnen die Frage, ob man überhaupt noch per E-Mail kommunizieren sollte.

Die Antwort ist eindeutig „Ja, selbstverständlich!“. Denn jede E-Mail wird von unseren Systemen automatisch verschlüsselt. Es handelt sich hierbei um eine sog. Transportverschlüsselung. Die E-Mail wird durch einen verschlüsselten Tunnel geschickt, so dass Dritte während des Transportes diese E-Mail nicht lesen können. Auf den einzelnen Servern während des Transportweges sind sie aber nach wie vor in Klartext gespeichert, so dass ein nicht autorisierter Zugriff durch Dritte möglich ist. Unterstützt der Empfänger die Verschlüsselungsmethode nicht, ist ein Versand nicht möglich. Sie würden in diesem Fall eine Unzustellbar-Nachricht erhalten.

Um es mit der Postkarte vergleichbar zu machen. Die Postkarte ist mit einer Zaubertinte geschrieben. Diese wird erst sichtbar, wenn die Postkarte in ihrem Briefkasten liegt. Jeder, der nun Zugriff (legal oder illegal) auf den Briefkasten hat, kann die Postkarte lesen. Der Postbote während der Zugstellung selbst aber nicht.

Diese Verschlüsselungsmethode reicht bei den meisten E-Mails aus. Enthält ihre E-Mail aber hochsensible Daten (Beispiel Geschäftsbrief, Vermerk persönlich) besteht von vielen

Datenschutzbeauftragten die dringende Empfehlung, zusätzlich den eigentlichen Inhalt zu verschlüsseln. Hier spricht man von der sog. Inhaltsverschlüsselung.

Diese Verschlüsselungsmethode sollte u. a. dann angebracht werden, wenn es sich um personenbezogene Daten der folgenden Kategorien handelt:

- sexuelle Orientierung,
- ethnische Herkunft,
- politische Meinung,
- biometrische Daten,
- religiöse Überzeugung,
- Informationen über den Gesundheitszustand.

Bei der Inhaltsverschlüsselung werden der Inhalt der E-Mail und etwaige Anlagen verschlüsselt. Die Entschlüsselung kann nur vom direkten Empfänger durchgeführt werden. Der Zugang für den Briefkasten reicht hier also nicht mehr aus.

Diese Verschlüsselung ist jedoch etwas unbequem und erfordert zusätzlich manuelle Schritte. Eine vollkommende Automatisierung ist hierfür technisch zurzeit nicht umsetzbar, da es verschiedene Standards gibt.