certification 2021

MORGENSTERN

Prüfbericht

comcrypto MXG

DATENSCHUTZ-ready

Geprüfte Software

zur Umsetzung der Vorgaben der

EU-DSGVO

PRIVACY CERTIFICATION

DATENSCHUTZ-ready

by MORGENSTERN

MORGENSTERN consecom GmbH | Hohe Straße 8 | 09112 Chemnitz | Germany

MORGENSTERN

Datenschutzbegutachtung von comcrypto MXG

MORGENSTERN consecom GmbH
Hohe Straße 8
09112 Chemnitz

25.08.2021
Dr. Knut Karnapp
Aktenzeichen: CON400/20

Inhalt

I. Prüfgegenstand

Prüfgegenstand ist das E-Mail-Gateway „comcrypto MXG“ (nachfolgend „comcrypto“).

comcrypto soll automatisiert den E-Mail-Versand über verschiedene Verschlüsselungsarten datenschutzkonform ausgestalten. Eine E-Mail-Verschlüsselung kann als Transportverschlüsselung und Ende-zu-Ende-Verschlüsselung (Inhaltsverschlüsselung) ausgestaltet werden.

Im Folgenden werden zunächst die technischen Rahmenbedingungen beschrieben, die für eine Begutachtung von comcrypto durch MORGENSTERN als Mindestvoraussetzung zugrunde gelegt werden. Im Anschluss erfolgt jeweils eine Auseinandersetzung mit und Bewertung der technischen Umsetzung durch comcrypto. Abschließend wird eine datenschutzrechtliche Bewertung vorgenommen.

II. Technische Begutachtung

1. Transportverschlüsselung

Bei einer Transportverschlüsselung werden E-Mails auf dem Transportweg verschlüsselt. Die Verbindung zwischen den kommunizierenden E-Mail-Servern wird mithilfe eines Algorithmus verschlüsselt und kann nur mit dem passenden Schlüssel entschlüsselt werden. Der E-Mail-Inhalt bleibt unverschlüsselt und könnte bei einem erfolgreichen Angriff auf den Transportweg oder auf den Empfangsserver gelesen werden.

Eine Transportverschlüsselung reduziert somit die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß.

1.1. Technische Mindestvoraussetzung

Grundsätzlich kann zwischen drei Stufen von Transportverschlüsselung unterschieden werden.

Bei der opportunistischen (einfachen) Transportverschlüsselung wird mittels STARTTLS als Einstellung am E-Mail-Server zwischen den am Sendevorgang beteiligten E-Mail-Servern eine Verschlüsselung ausgehandelt. Diese Verschlüsselungsart wird nur aktiviert, wenn STARTTLS auf beiden E-Mail-Servern aktiviert ist. Falls beim Empfänger-Server STARTTLS nicht aktiviert ist, findet auch keine Transportverschlüsselung statt. Eine Zertifikatsprüfung findet ebenso nicht statt. Diese Übertragungsart eignet sich nicht für die Übertragung personenbezogener Daten.

Die obligatorische Transportverschlüsselung erfolgt unter Anwendung von Schlüsselprotokollen gemäß dem Standard TLS 1.2 oder 1.3. Dabei kommen Verschlüsselungsalgorithmen nach der technischen Richtlinie des BSI „TR-02102-2“ zum Einsatz. Diese Übertragungsart eignet sich für die Übertragung von Daten mit normalem Schutzbedarf. Ist das STARTTLS beim Empfängerserver nicht oder nur in einer veralteten Version (z. B. TLS 1.0) verfügbar, wird der E-Mail-Versand gestoppt.

Auf der obligatorischen Transportverschlüsselung aufbauend ist eine qualifizierte Transportverschlüsselung möglich. Dabei werden einschränkend nur solche Algorithmen nach BSI TR-02102-2 eingesetzt, die auch über eine Perfect Forward Secrecy (PFS) als besondere Eigenschaft der Schlüsselprotokolle verfügen. Zusätzlich ist bei der qualifizierten Transportverschlüsselung ein von einer unabhängigen Zertifizierungsstelle validiertes, gültiges TLS-Zertifikat auf Empfängerseite erforderlich, das vom sendenden System geprüft wird.

1.1.1. Transportweg vom eigenen E-Mail-Server zu comcrypto

Der Transportweg vom Absender-E-Mail-Server zu comcrypto sollte mittels einer qualifizierten Transportverschlüsselung möglich sein.

1.1.2. Transportweg von comcrypto zum Empfangsserver

Der Transportweg von comcrypto zum E-Mail-Server des Empfängers einer E-Mail sollte differenziert nach Schutzniveau des jeweiligen Nachrichteninhalts abgestuft verschlüsselt werden können. Sowohl eine obligatorische Transportverschlüsselung als auch eine qualifizierte Transportverschlüsselung sollten aktivierbar sein.

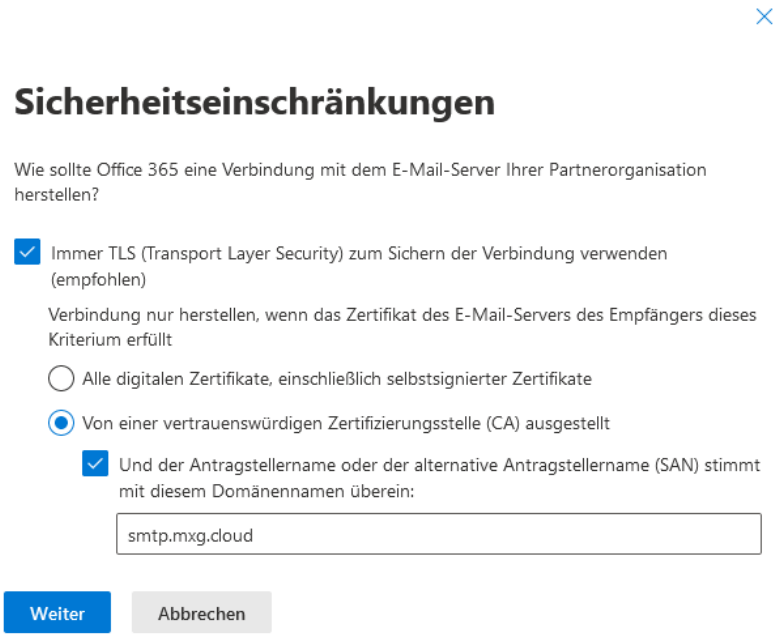
Darüber hinaus sollte der Absender eine Mitteilung über das Ergebnis der Zertifikatsprüfung auf Empfängerseite erhalten, sodass der Absender bei Fehlen eines entsprechenden TLS-Zertifikats die Möglichkeit hat, den Sendevorgang abzubrechen und die E-Mail separat inhaltsverschlüsselt zu versenden. Alternativ sollte eine automatische Inhaltsverschlüsselung (s. II. 2., II. 5.) möglich sein.

Mindestvoraussetzungen

- Qualifizierte Transportverschlüsselung auf dem Transportweg zwischen Absender-E-Mail-Server und comcrypto-Server
- Mindestens obligatorische Transportverschlüsselung auf dem Transportweg vom comcrypto-Server zum Empfänger-E-Mail-Server
- Möglichkeit der Aktivierung einer qualifizierten Transportverschlüsselung
- Information des Absenders, wenn der Empfänger über kein gültiges TLS-Zertifikat verfügt

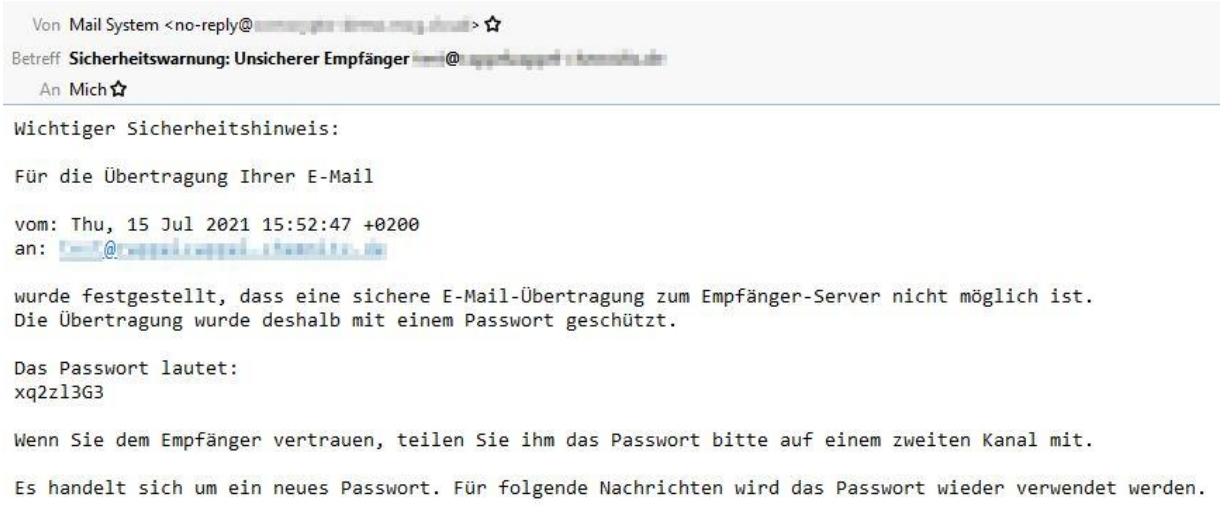
1.2. Umsetzung bei comcrypto

Die Sicherung des Transports vom E-Mail-Absender zu comcrypto geschieht durch geeignete Einstellungen im E-Mail-System des Absenders, z.B. für Exchange:



Der Transport von comcrypto zum Empfänger-System erfolgt in mehreren Schritten. Zunächst wird ein Secure DNS Lookup durchgeführt. Hierbei soll die IP-Adresse des Empfänger-Systems fälschungssicher im DNS (Domain Name System) abgerufen werden, um die Übertragung an falsche IP-Adressen auszuschließen.

Darüber hinaus kommt TLS in den Protokollversionen 1.2 bzw. 1.3 zum Einsatz. Comcrypto unterstützt alle Transportverschlüsselungsmöglichkeiten inklusive der qualifizierten Transportverschlüsselung. Sollte auf einem Empfänger-Server kein entsprechendes Zertifikat vorhanden sein oder eine Verifikation fehlschlagen, kann ein E-Mail-Versand automatisch abgebrochen und eine Inhaltsverschlüsselung erzwungen werden.



Von Mail System <no-reply@ >
Betreff **Sicherheitswarnung: Unsicherer Empfänger**
An Mich

```
Wichtiger Sicherheitshinweis:

Für die Übertragung Ihrer E-Mail

vom: Thu, 15 Jul 2021 15:52:47 +0200
an:

wurde festgestellt, dass eine sichere E-Mail-Übertragung zum Empfänger-Server nicht möglich ist.
Die Übertragung wurde deshalb mit einem Passwort geschützt.

Das Passwort lautet:
xq2zl3G3

Wenn Sie dem Empfänger vertrauen, teilen Sie ihm das Passwort bitte auf einem zweiten Kanal mit.

Es handelt sich um ein neues Passwort. Für folgende Nachrichten wird das Passwort wieder verwendet werden.
```

1.3. Bewertung

Die von comcrypto unterstützten Transportverschlüsselungsmöglichkeiten erfüllen die technischen Mindestvoraussetzungen.

2. Inhaltsverschlüsselung

Bei einer Inhaltsverschlüsselung wird der versandte Inhalt einer E-Mail codiert, das heißt auch die ruhenden Daten beim Empfänger.

2.1. Technische Mindestvoraussetzung

Comcrypto sollte mit einer Inhaltsverschlüsselung, die bereits auf dem Ausgangsserver (z.B. mittels Sophos SPX, SEPPmail GINA, Cryptshare) oder auf dem ausgehenden E-Mail-Client (S/MIME, PGP/MIME/inline) eingesetzt wird, kompatibel sein, um bei Bedarf einen inhaltsverschlüsselten Transport von E-Mails an comcrypto und dann an den Empfänger zu ermöglichen. Die bereits inhaltsverschlüsselte Nachricht sollte transportverschlüsselt an den Empfänger weitergeleitet werden können. Dadurch soll erreicht werden, dass durch die erfolgte Inhaltsverschlüsselung die Nachricht zugestellt wird, auch wenn die Transportverschlüsselung auf Empfängerseite nicht gewährleistet werden kann. Das Risiko wäre in diesem Fall durch die vorab bereits erfolgte Verschlüsselung des Inhalts der Nachricht ausreichend gemindert.

Daneben sollte comcrypto eine eigene Inhaltsverschlüsselung der über comcrypto transportierten E-Mails vornehmen können.

Mindestvoraussetzungen

- Kompatibilität von comcrypto mit vorhandener Inhaltsverschlüsselung des Kunden
- Möglichkeit der Inhaltsverschlüsselung mit comcrypto

2.2. Umsetzung bei comcrypto

Comcrypto bietet die Möglichkeit, eine originäre Inhaltsverschlüsselung regelbasiert einzubinden. Der Empfänger erhält bei Einbindung einer Inhaltsverschlüsselung eine E-Mail mit verschlüsseltem Anhang.

Gesicherte Nachricht von [redacted]

Vollansicht schließen

Von: [redacted]

15.07.2021 um 15:57 Uhr

HTML SecuredData Mehr Speicherplatz für Anhänge

Guten Tag,

diese Nachricht von [redacted] wurde vom E-Mail-System des Absenders durch ein Passwort geschützt.

Um Ihre Nachricht zu lesen, öffnen Sie bitte die angehängte Datei SecuredData.html in Ihrem Browser und geben Sie Ihr Passwort ein.

Hinweise:

Wenn dies Ihre erste verschlüsselte Nachricht vom Absender ist, dann erfahren Sie Ihr Passwort direkt von ihm auf einem zweiten Weg.

Die Verschlüsselung erfolgte, weil

a) Der Absender den Inhalt als besonders vertraulich eingeschätzt und diesen Schutz veranlasst hat.

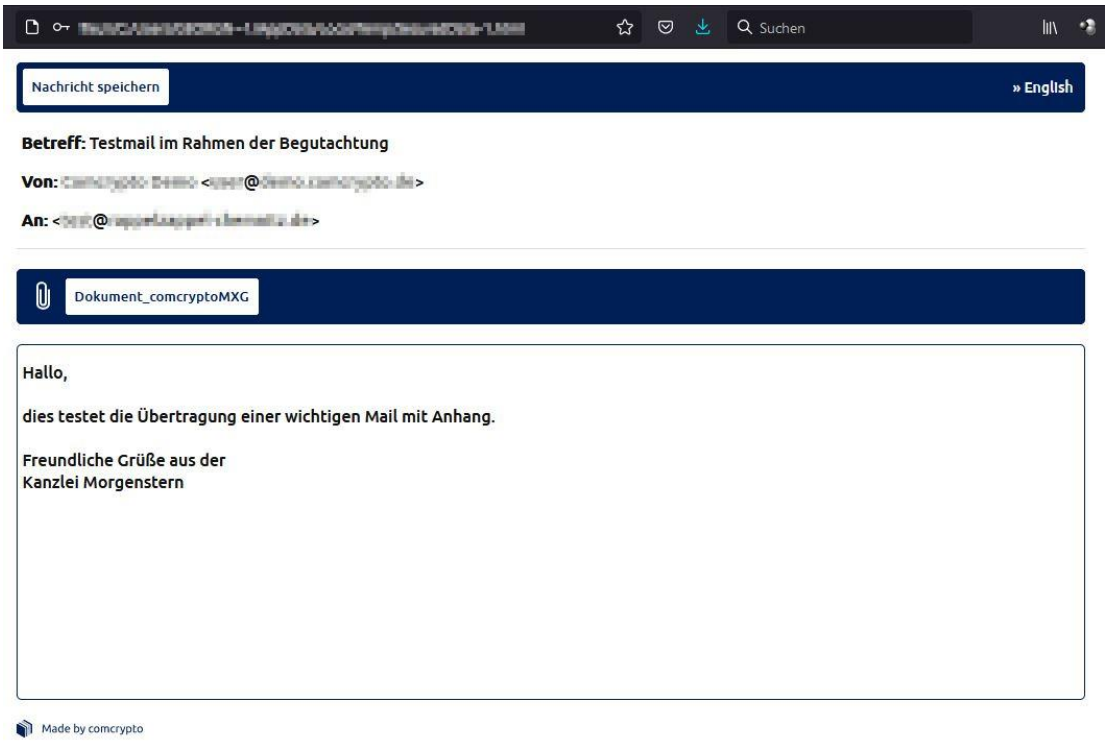
Oder

b) Ein Problem in der TLS-Konfiguration Ihres E-Mail-Servers festgestellt wurde. Bitte benachrichtigen Sie in diesem Fall Ihren Administrator. Er kann durch Weiterleiten dieser Mail an help@comcrypto.de eine genaue Statusanalyse dazu anfordern.

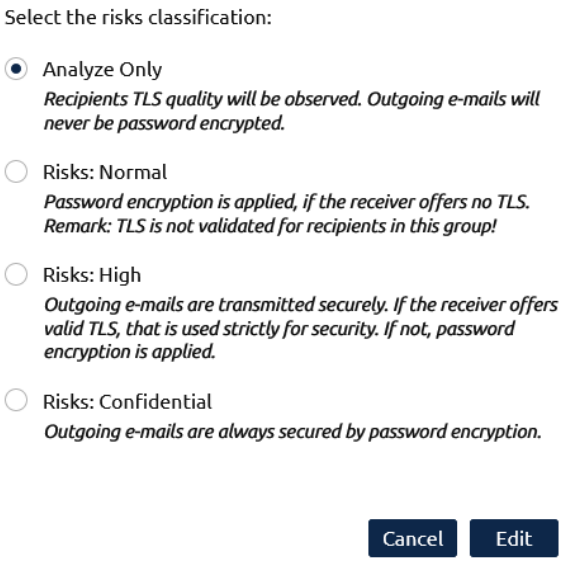
Freundliche Grüße

[redacted]

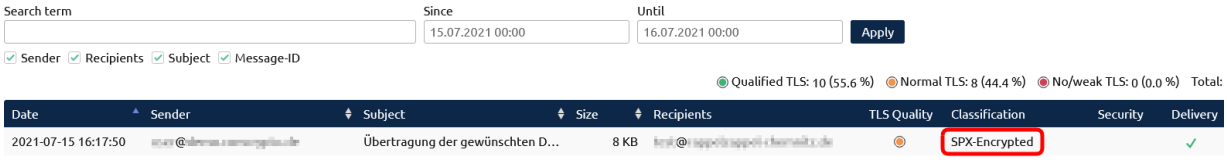
Das Öffnen des Dateianhangs, die Eingabe des Passworts und das Lesen der entschlüsselten E-Mail erfolgen im Browser des Empfängers.



Der Kunde kann dabei auswählen, in welchen Risikoszenarien eine Inhaltsverschlüsselung erzwungen wird.



Zusätzlich kann der Kunde beim Einsatz von comcrypto auch auf eigene Inhaltsverschlüsselungssysteme zurückgreifen, die von comcrypto erkannt und als bestehende Risikominderung berücksichtigt werden.



2.3. Bewertung

Die technischen Mindestvoraussetzungen zur Inhaltsverschlüsselung werden von comcrypto erfüllt. Die Ausgestaltung der Anwendungsszenarien und Konfigurationsmöglichkeiten werden im Detail unter II. 5. überprüft.

3. Protokollierung

3.1. Technische Mindestvoraussetzung

Es muss nachvollziehbar protokolliert werden, welche Sicherheitsmaßnahmen beim jeweiligen E-Mail-Versand eingesetzt wurden. Das dient der revisionssicheren Nachvollziehbarkeit und Überprüfbarkeit der vorgenommenen Verschlüsselungsmaßnahmen.

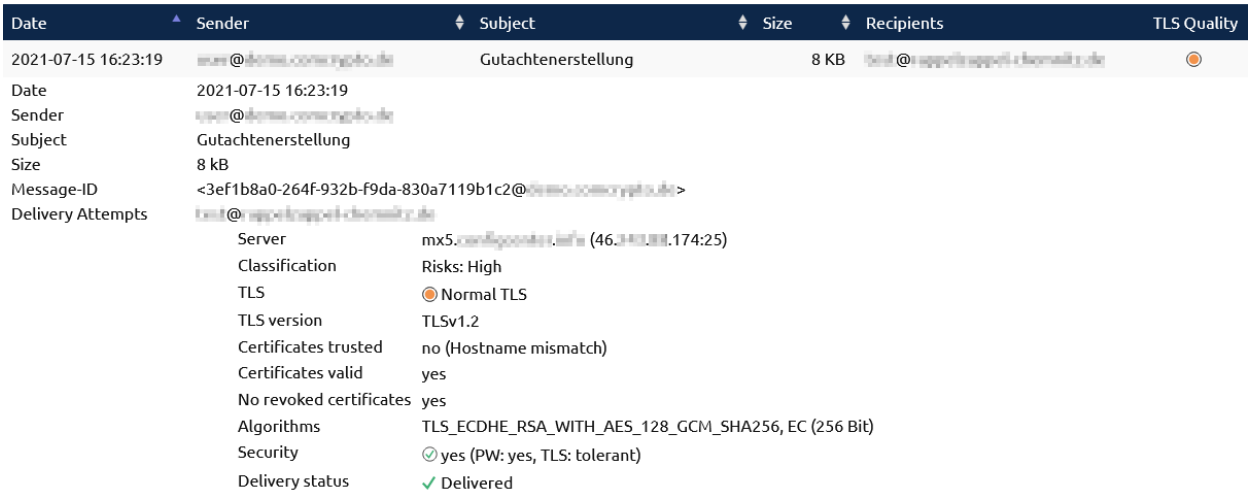
Mindestvoraussetzungen

- Nachvollziehbare und revisionssichere Protokollierung der beim E-Mail-Versand eingesetzten Sicherheitsmaßnahmen

3.2. Umsetzung bei comcrypto

Folgende Informationen zu versendeten E-Mails werden von comcrypto protokolliert und können im Benutzer-Interface eingesehen werden:

- Datum und Uhrzeit
- Absender
- Betreff (optional)
- Größe
- Empfänger
- Angewandter TLS-Standard
- Angewandte Risikoklasse
- Ergebnis der Zertifikatsprüfung
- Angewandter Algorithmus
- Erfüllung der Sicherheitsregeln
- Zustellungsstatus



Date	Sender	Subject	Size	Recipients	TLS Quality
2021-07-15 16:23:19	[redacted]	Gutachtenerstellung	8 KB	[redacted]	

Date	2021-07-15 16:23:19
Sender	[redacted]
Subject	Gutachtenerstellung
Size	8 kB
Message-ID	<3ef1b8a0-264f-932b-f9da-830a7119b1c2@[redacted]>
Delivery Attempts	[redacted]

Server	mx5.[redacted] (46.[redacted].174:25)
Classification	Risks: High
TLS	Normal TLS
TLS version	TLSv1.2
Certificates trusted	no (Hostname mismatch)
Certificates valid	yes
No revoked certificates	yes
Algorithms	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, EC (256 Bit)
Security	yes (PW: yes, TLS: tolerant)
Delivery status	✓ Delivered

3.3. Bewertung

Die von comcrypto umgesetzte Protokollierung der angewandten Sicherheitsmaßnahmen erfüllt die technische Mindestvoraussetzung.

4. Datenaufbewahrung

4.1. Technische Mindestvoraussetzung

Die Datenaufbewahrung bei comcrypto als „Zwischenstation“ darf nur solange erfolgen, wie sie technisch für die Zustellung notwendig ist.

Außerdem muss die Serverinfrastruktur, auf der comcrypto ausgeführt wird, technisch ausreichend gegen etwaige Angriffe Dritter abgesichert sein.

Mindestvoraussetzungen

- Datenaufbewahrung bei comcrypto erfolgt nur so lange wie erforderlich
- Ausreichende technische und organisatorische Maßnahmen

4.2. Umsetzung bei comcrypto

Die E-Mails werden auf den comcrypto-Servern unverzüglich nach erfolgreicher Zustellung an den Empfänger gelöscht.

Über diesen Zeitpunkt hinaus werden nur Protokoll- bzw. Metadaten der versendeten E-Mails zu Dokumentationszwecken gespeichert. Eine Löschung kann auf Anfrage des Kunden vorgenommen werden.

Comcrypto trifft umfangreiche technische und organisatorische Maßnahmen zur Absicherung gegen etwaige Angriffe Dritter. Die einzelnen Maßnahmen können der beigefügten Liste der technischen und organisatorischen Maßnahmen entnommen werden.

An dieser Stelle hervorzuheben sind zunächst die technischen Maßnahmen zur Verhinderung, dass Datenverarbeitungssysteme von Unbefugten genutzt werden könnten (Ziff. 1.2 der Anlage), sowie zur Gewährleistung, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Ziff. 2.1 der Anlage).

Darüber hinaus trifft comcrypto eine Vielzahl technischer und organisatorischer Maßnahmen, die die Verfügbarkeit der Serverinfrastruktur gewährleisten sollen und im Falle eines Systemausfalls eine rasche Wiederherstellbarkeit ermöglichen (Ziff. 3.1 und 3.2 der Anlage).

4.3. Bewertung

Der umfangreiche Einsatz von Verschlüsselungsmaßnahmen durch comcrypto bei den Datenverarbeitungen führt zu einem hohen Sicherheitsniveau der ruhenden Daten und der Daten auf dem Transportweg. Die Zugangskontrollmaßnahmen entsprechen dem Stand der Technik und verhindern eine unbefugte Nutzung der Datenverarbeitungssysteme, sodass die Serverinfrastruktur ausreichend gegen etwaige Angriffe Dritter abgesichert ist.

Die Serverinfrastruktur ist auch durch die umfangreichen technischen Maßnahmen zur Gewährleistung der Verfügbarkeit der Serverinfrastruktur und damit der Verfügbarkeit der von comcrypto angebotenen Dienste geschützt. Sämtliche Maßnahmen nach aktuellem Stand der

Technik, die in einem Rechenzentrum vorgehalten werden sollten, werden durch comcrypto getroffen.

5. Konfigurationsmöglichkeiten und Usability

5.1. Technische Mindestvoraussetzung

Das E-Mail-Gateway comcrypto sollte Datenschutz durch Technikgestaltung gemäß Art. 25 DS-GVO gewährleisten können. Dafür muss comcrypto individuelle Konfigurationsmöglichkeiten bereithalten, um ein dem Einsatzzweck angemessenes Datenschutzniveau herstellen zu können. Die Standardeinstellungen sollten bereits ein grundsätzlich angemessenes Datenschutzniveau schaffen.

Je nach Schutzniveau der zu übermittelnden Nachrichten muss es möglich sein, den entsprechenden Verschlüsselungsstandard anwenden zu können. Ein „Laien-Nutzer", das heißt nicht nur ein IT-Administrator, sollte in der Lage sein, im Benutzer-Interface das automatische Anwenden von Regeln, die beim E-Mail-Versand eingesetzt werden, einzustellen.

Mindestvoraussetzungen

- Datenschutzfreundliche Einstellungen im Standard
- Nutzerfreundliche Konfigurationsmöglichkeiten

5.2. Umsetzung bei comcrypto

Im Benutzer-Interface stellt comcrypto verschiedene Optionen zur Individualisierung des Sicherheitsverhaltens zur Verfügung.

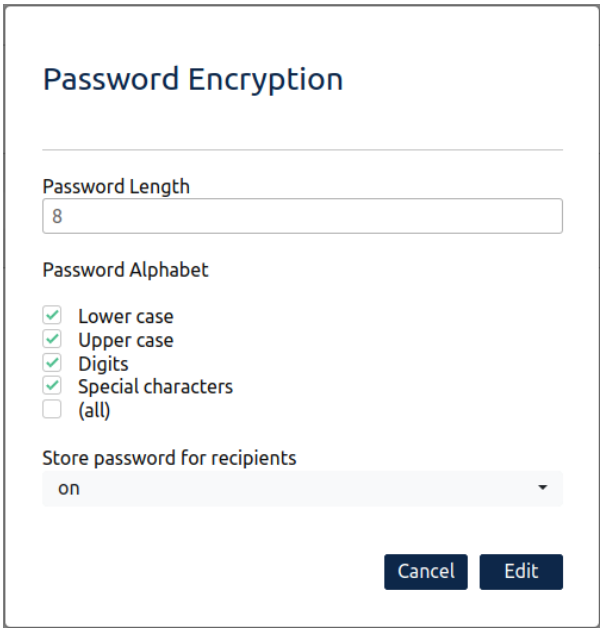
Zunächst ist es möglich, jeder Empfängerdomain eine von vier Risiko-Klassen zuzuordnen: „Analyze Only", „Risks: normal", „Risks: high" und „Risks: confidential". Je nach Risiko-Klasse einer Domain lässt sich einstellen, wann eine Inhaltsverschlüsselung eingesetzt werden soll:

Classification effects	
Analyze Only	Recipients TLS quality will be analyzed. Outgoing e-mails will never be password encrypted.
Risks: Normal	Password encryption is applied, if the receiver does not offer *'normal' TLS encryption.*
Risks: High	Password encryption is applied, if the receiver does not offer *'qualified' TLS encryption.*
Risks: Confidential	Outgoing e-mails are always secured by password encryption.

Hierfür wird die Transportverschlüsselung, die für den Transportweg verwendet werden kann, anhand des Zertifikats, der verfügbaren TLS-Protokollversionen und der verfügbaren Algorithmen beim Empfangsserver analysiert.

Darauf aufbauend können Sicherheitsregeln erstellt werden, nach denen sich entschieden wird ab welchem Risiko eine Inhaltsverschlüsselung erzwungen wird. Denkbar ist eine automatische Inhaltsverschlüsselung für den Fall, dass beim Empfänger kein gültiges TLS-Zertifikat, das für eine wirksame Transportverschlüsselung erforderlich wäre, vorhanden ist.

Darüber hinaus kann das jeweilige Verfahren zur Inhaltsverschlüsselung, das von comcrypto erkannt werden soll, ausgewählt werden. Diesbezüglich lassen sich die Regeln zur Passworterstellung und -speicherung auf Seiten der Absenderdomain für einen Empfänger speichern.



Daneben kann der Einsatz einer Inhaltsverschlüsselung von jedem Absender direkt mithilfe von sogenannten „E-Mail-Markern“ erzwungen werden. Durch einen Zusatz in der Betreffzeile könnten somit bestehende Sicherheitsregeln umgangen werden, um eine Inhaltsverschlüsselung dort zu erzwingen, wo anhand der Sicherheitsregeln noch keine Inhaltsverschlüsselung notwendig ist. Diese Einstellungsmöglichkeit ist optional.

Marker

To effect the usage of password encryption for a specific mail, users can type the following markers in front of their mail subject.

This will overrule the automatic decision due to the recipient's domain classification. The marker will be deleted before sending the mail.

Marker	Description
##!	The mail will be encrypted with the recipient's default password. If the recipient has no password yet, a password will be created. In both cases, the sender will be notified.
##+	The mail will be encrypted with a new password. The new password will overwrite the recipient's default password for later re-usage and the sender will be notified.
##=password	The mail will be encrypted with a custom password. The custom password will overwrite the recipient's default password for later re-usage. Type the custom password instead of 'password' in the marker.

5.3. Bewertung

Die Konfigurationsmöglichkeiten von comcrypto sind angemessen differenziert, um einzelfallbezogen ein angemessenes Datenschutzniveau gewährleisten zu können. Das Benutzer-Interface ist so ausgestaltet, dass auch ein „Laien-Nutzer“ diese Einstellungsmöglichkeiten vornehmen kann.

III. Rechtliche Begutachtung

1. Prüfungsumfang / Scope

Die Voraussetzungen für eine Begutachtung durch MORGENSTERN in datenschutzrechtlicher Hinsicht richten sich im Wesentlichen nach den Vorschriften der Datenschutz-Grundverordnung (nachfolgend „DS-GVO“) und des Bundesdatenschutzgesetzes (nachfolgend „BDSG“).

Diese Prüfung umfasst daher ausschließlich die Fälle, in denen bei der Übermittlung einer E-Mail personenbezogene Daten gemäß Art. 4 Nr. 1 oder Nr. 9 DS-GVO (z. B. Anschrift, Name, E-Mail-Adresse, Telefonnummer, Beruf, Gesundheitsdaten etc.) übermittelt werden. Personenbezogene Daten (nachfolgend auch „Daten“) können sich im Betreff einer E-Mail, im Empfängerfeld, im Textfeld oder im Anhang oder auch an sonstigen Stellen befinden. Aber auch die Umstände der Kommunikation können als personenbezogene Daten zu werten sein, wenn diese sich auf natürliche Personen beziehen lassen.[1]

Nicht Gegenstand dieser rechtlichen Prüfung sind spezielle Vorschriften für Daten, die der Geheimhaltung unterliegen, wie beispielsweise bei einer Verarbeitung durch Berufsgeheimnisträger (z. B. Rechtsanwälte, Steuerberater). Aus den anwendbaren Vorschriften können sich erhöhte Anforderungen an die zu ergreifenden Schutzmaßnahmen ergeben, die von einem Verantwortlichen dann zusätzlich zu den Regelungen der DS-GVO zu beachten sind. Gemäß Erwägungsgrund 75 der DS-GVO können bei der Verarbeitung von personenbezogenen Daten, die einem Berufsgeheimnis unterliegen, durch einen Verlust der Vertraulichkeit außerdem Risiken für die Rechte und Freiheiten der betroffenen Person auftreten. Das Vorliegen eines Berufsgeheimnisses ist also ein Indiz für ein hohes Risiko, das sich auch in der Wahl von angemessenen Maßnahmen wiederfinden muss.[2]

Was den „Adressatenkreis“ angeht, ist Mindestvoraussetzung der Begutachtung in rechtlicher Hinsicht nicht nur, dass comcrypto selbst die den Anbieter treffenden Pflichten einhält, sondern, dass ein nachweisbarer datenschutzkonformer Einsatz für Verantwortliche möglich ist. Gleichwohl wird ausdrücklich darauf hingewiesen, dass jeder Verantwortliche selbst die Einhaltung der datenschutzrechtlichen Anforderungen gewährleisten muss und diese auch bei Einsatz von Drittdiensten nach außen verantwortet.

So sind oft weitere Maßnahmen (z. B. Virenschutzprogramme) sowie die Nutzung mobiler Endgeräte (z.B. Smartphones und Tablets) zu berücksichtigen, die hier nicht beleuchtet werden können. Betrachtet werden sollen demnach nur die von comcrypto angebotenen Verschlüsselungsverfahren und nicht die Verarbeitungen und Prozesse, die bei einem Verantwortlichen vor- oder nachgelagert geschehen.

Grundsätzlich erfolgen die Bewertungen bezüglich comcrypto ausgehend von den datenschutzrechtlichen Pflichten, die einen Verantwortlichen treffen. Im Hinblick auf den Anbieter (comcrypto GmbH) und damit den Auftragsverarbeiter der einsetzenden verantwortlichen Stellen können die Voraussetzungen nur im Hinblick auf die Pflichten nach Art. 32 DS-GVO betrachtet werden.

---

[1] Orientierungshilfe der Datenschutzkonferenz „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“, Stand: 16. Juni 2021.
[2] Siehe Fußn. 1.

Der Nachweis über die datenschutzkonforme Verschlüsselung beim Verantwortlichen ist zwar noch nicht allein durch Einsatz eines „zertifizierten“ E-Mail-Gateways erbracht. Es trägt aber maßgeblich zur Erfüllung der Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO, insbesondere zum Nachweis der Pflicht zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) sowie des Art. 28 Abs. 1 DS-GVO, bei.

Im ersten Schritt ist daher die zutreffende Einordnung der datenschutzrechtlichen Rolle der comcrypto GmbH als Auftragsverarbeiterin gemäß Art. 28 DS-GVO und die Einhaltung der hiermit einhergehenden datenschutzrechtlichen Pflichten zu betrachten.

Kern der Prüfung stellen dann Art. 5 Abs. 1 f), 32 und 25 DS-GVO dar. Daneben sollen noch die einzelnen Datenschutzgrundsätze des Art. 5 Abs. 1 DS-GVO nebst der hiermit einhergehenden Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) beleuchtet werden.

2. Auftragsverarbeitung nach Art. 28 DS-GVO

2.1. Gesetzliche Anforderungen

Erfolgt eine Verarbeitung personenbezogener Daten im Auftrag eines Dritten, müssen verantwortliche Stellen und der sog. Auftragsverarbeiter bestimmte Vorgaben beachten, die sich aus Art. 28 DS-GVO ergeben.

Die comcrypto GmbH stellt im Ergebnis wohl einen Auftragsverarbeiter im Sinne des Art. 28 DS-GVO dar.

Die Verarbeitungstätigkeit mit comcrypto beschränkt sich anders als bei E-Mail-Providern, nicht ausschließlich auf die Übermittlung der Nachricht.[3]

Die Verschlüsselung von Daten, die per E-Mail übermittelt werden, sei es nur auf dem Transportweg oder im ruhenden Zustand, stellt als solche eine Verarbeitung von personenbezogenen Daten dar, die auf Weisung und im Auftrag des Verantwortlichen erfolgt.

Gemäß Art. 28 Abs. 1 DS-GVO dürfen Verantwortliche daher nur solche Anbieter einsetzen, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet ist. Ferner haben der Verantwortliche und der Auftragsverarbeiter vor Beginn der Tätigkeit einen Vertrag zur Auftragsverarbeitung abzuschließen, der inhaltlich den Anforderungen des Art. 28 Abs. 3 DS-GVO genügt.

Mindestvoraussetzungen

- Bereitstellung eines Auftragsverarbeitungsvertrages gemäß Art. 28 Abs. 3 DS-GVO
- Angemessene technische und organisatorische Maßnahmen gemäß Art. 28 Abs. 1, 32 DS-GVO sowie Bereitstellung einer Beschreibung dieser Maßnahmen für die Kunden

[3] Vgl. Arbeitspapier 169 (WP 169) der Artikel-29-Gruppe, wonach Anbieter von Telekommunikationsdiensten, worunter auch E-Mail-Anbieter zu fassen sind, nur in Bezug auf Verkehrs- und Rechnungsdaten und nicht auf die übermittelten Daten verantwortlich sind.

2.2. Umsetzung bei comcrypto und Bewertung

Vor der Inanspruchnahme von comcrypto wird dem Auftraggeber der Abschluss eines Vertrags zur Auftragsverarbeitung angeboten. Dieser Vertrag genügt inhaltlich auch den Anforderungen des Art. 28 Abs. 3 DS-GVO und enthält alle Pflichtangaben.

Dem Auftragsverarbeitungsvertrag ist zudem immer eine Beschreibung der technischen und organisatorischen Maßnahmen von comcrypto beigefügt, sodass ein Verantwortlicher überprüfen kann, ob die Anforderungen des Art. 28 Abs. 1, 32 DS-GVO in Bezug auf das Schutzniveau der Daten und des Risikos beim Verantwortlichen erfüllt sind.

3. Datenschutzgrundsätze Art. 5 DS-GVO

3.1. Gesetzliche Anforderungen

Die einzelnen Anforderungen an die Verarbeitung von personenbezogenen Daten leiten sich aus den grundlegenden Datenschutzgrundsätzen ab, die in Art. 5 Abs. 1 DS-GVO geregelt sind:

- **Rechtmäßigkeit** (rechtmäßige Datenverarbeitung aufgrund einer Rechtsgrundlage)
- **Verarbeitung nach Treu und Glauben** (faire Verarbeitung)
- **Transparenz** (Vorhersehbarkeit und Nachvollziehbarkeit der Verarbeitung)
- **Zweckbindung** (Zwecke für die Verarbeitung müssen festgelegt werden)
- **Datenminimierung** (Beschränkung der Daten auf das notwendige Maß)
- **Richtigkeit** (Daten sollen korrekt und auf dem aktuellen Stand gehalten werden)
- **Speicherbegrenzung** (Daten sollen nach Zweckerreichung nur noch im absolut notwendigen Umfang gespeichert werden)
- **Integrität und Vertraulichkeit** (Schutz vor geplanten Zugriffen und ungeplanten Beeinträchtigungen)

Die Datenschutzgrundsätze gehen eng mit der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO einher, wonach der Verantwortliche die Einhaltung der Grundsätze nachweisen können muss. Mit der Rechenschaftspflicht hat der Gesetzgeber eine eher abstrakte Pflicht eingeführt, deren Einhaltung im Gesetz nicht eindeutig beschrieben ist. Die Rechenschaftspflicht lässt sich durch die Dokumentation sämtlicher Prozesse und Umsetzungen erfüllen.

Mindestvoraussetzungen

- Erleichterung des Nachweises der Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DS-GVO beim Kunden zur Erfüllung der Rechenschaftspflicht

3.2. Umsetzung bei comcrypto und Bewertung

Der Einsatz von comcrypto ist hilfreich, um als Verantwortlicher nachweisen zu können, dass der Schutz der E-Mail-Kommunikation im Einklang mit dem Datensparsamkeits- und den Speicherbegrenzungsgrundsatz erfolgt.

Wie oben beschrieben (Ziffer I. 4.2) werden die E-Mails auf den comcrypto-Servern unverzüglich nach erfolgreicher Zustellung an den Empfänger gelöscht. Über diesen Zeitpunkt hinaus werden nur Protokoll- bzw. Metadaten der versendeten E-Mails zu Dokumentationszwecken gespeichert. Eine Löschung kann dabei immer auf Anfrage des Verantwortlichen vorgenommen werden.

Ferner ermöglicht die Protokollierung durch comcrypto den Nachweis, dass ausreichende Sicherheitsmaßnahmen beim E-Mail-Versand getroffen wurden und gewährleistet damit die revisionssichere Nachvollziehbarkeit und Überprüfbarkeit der vorgenommenen Verschlüsselungsmaßnahmen im Sinne der Rechenschaftspflicht und des Grundsatzes der Integrität und Vertraulichkeit (vgl. Ziffer I. 3.2).
Die einzelnen protokollierten und einsehbaren Informationen (Ziffer I. 3.2) sind auch erforderlich, um die Zwecke einer sicheren Verschlüsselung und Nachweisbarkeit dieser zu erfüllen. Darüber hinausgehende Informationen werden nicht protokolliert, sodass Verantwortlichen betreffend die Protokolldaten eine transparente und dem Zweck angemessene Datenverarbeitung ermöglicht wird (Art. 5 Abs. 1 a) und b) DS-GVO).

4. Technische und organisatorische Maßnahmen nach Art. 5 Abs. 1 f), 32 DS-GVO

4.1. Gesetzliche Anforderungen

Nach dem Grundsatz der Integrität und Vertraulichkeit in Art. 5 Abs. 1 f) DS-GVO sind Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Verantwortliche sowie Auftragsverarbeiter haben dafür gemäß Art. 32 DS-GVO unter Berücksichtigung

- des Stands der Technik,
- der Implementierungskosten und
- der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dabei schließen diese Maßnahmen gegebenenfalls ausdrücklich auch die Verschlüsselung personenbezogener Daten ein (Art. 32 Abs. 1 a) DS-GVO).

Bei der Auswahl der Maßnahmen ist also bereits gesetzlich vorgesehen, dass es keinen „allgemeinen für alle geltenden Standard“ gibt, sondern eine Balance zwischen dem Schutzniveau, dem Stand der Technik und dem konkreten Risiko zu finden ist.

Eine einheitliche Definition des Begriffs „Stand der Technik“ gibt es nicht und kann mit Blick auf die technischen Fortentwicklungen, die sich im ständigen Wandel befinden, auch kaum sinnvoll

bestimmt werden. Allerdings darf man als Verantwortlicher davon ausgehen, dass behördliche Vorgaben zu konkreten technischen Maßnahmen dem Stand der Technik entsprechen.

Für den E-Mail-Versand und insbesondere den Verschlüsselungsverfahren kann man aktuell daher die Standards der technischen Richtlinie des BSI „TR-02102-2" (vgl. dazu Ziffer I. 1.1) sowie der Landesdatenschutzbehörden als den „Stand der Technik" ansehen.

Die Verschlüsselung beim Versand von E-Mails soll vor allem vor der unbefugten Einsichtnahme und / oder Kenntnisnahme der personenbezogenen Daten durch Dritte schützen und ganz konkret die Erfolgswahrscheinlichkeit passiver Abhörmaßnahmen Dritter auf dem Transportweg auf ein geringfügiges Maß reduzieren. Um auch gegen Dritte zu bestehen, die aktiv in den Netzverkehr eingreifen, muss sie in qualifizierter Weise durchgeführt und durch Maßnahmen zur kryptografischen Absicherung der Angaben der Empfänger über die zur Entgegennahme der Nachrichten berechtigten Geräte flankiert werden.[4]

Dabei ist in Bezug auf den datenschutzrechtlich Verantwortlichen wie folgt zwischen der comcrypto GmbH als Auftragsverarbeiterin und dem jeweiligen Verantwortlichen als Auftraggeber zu unterschieden.

4.1.1. TOM bei comcrypto

Da Verantwortliche ausdrücklich nur solche Auftragsverarbeiter einsetzen dürfen, die ausreichende TOM getroffen haben (Art. 28 Abs. 1 DS-GVO), gehören zu den wesentlichen Rahmenbedingungen für eine Begutachtung, dass der Anbieter comcrypto hinreichende Garantien hierfür erbringt, sowohl was die angebotenen Verschlüsselungsverfahren als solche angeht als auch die Gewährleistung der Sicherheit der Daten des Verantwortlichen, die von comcrypto empfangen werden. Nach Art. 32 DS-GVO müssen mithin ausdrücklich auch Auftragsverarbeiter geeignete und angemessene TOM ergreifen.

4.1.2. TOM beim Verantwortlichen

Soweit es um die durch den Verantwortlichen zur treffenden TOM geht, beschränkt sich diese Prüfung auf die verschlüsselte Übertragung als technische Maßnahme. Maßgeblich ist für die Begutachtung daher, welche Anforderungen an einen Verantwortlichen zu stellen sind, wenn es um die Verschlüsselung des E-Mails-Verkehrs geht, um hierauf aufbauend bewerten zu können, ob comcrypto diesen Anforderungen gerecht wird.

Die Verschlüsselung wird als eine mögliche technische Maßnahme ausdrücklich gemäß Art. 32 Abs. 1 a) DS-GVO vorgesehen. Eine generelle gesetzliche Pflicht zur Verschlüsselung jeglichen E-Mail-Verkehrs gibt es grundsätzlich zwar nicht. Die Datenschutzkonferenz (nachfolgend „DSK") hat aber in einer Orientierungshilfe („Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail", Stand: Juni 2021) die technischen Anforderungen dazu formuliert, wie personenbezogene Daten per E-Mail datenschutzkonform übermittelt werden können und hierbei im Ergebnis festgestellt, dass personenbezogene Daten per E-Mail zwingend verschlüsselt zu übertragen sind.

Beschlüsse der DSK gelten zwar nur für öffentliche Stellen. Private Unternehmen sollten sich allerdings auch im Regelfall an den Vorgaben der DSK orientieren, jedenfalls solange nicht

[4] DSK Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail" (Stand: 16. Juni 2021.), dort unter 2., Seite 2.

ausdrücklich anderweitige Anforderungen für private Unternehmen der Landesaufsichtsbehörden erfolgen.

Bei den konkret zu wählenden Verschlüsselungsverfahren ist nach der DSK zwischen „normalen Risiken“ und „hohen Risiken“ für die betroffenen Personen zu unterschieden. Darüber hinaus werden von der DSK die Anforderungen an solche personenbezogenen Daten beleuchtet, die dem Berufsgeheimnis nach §203 StGB unterliegen.

E-Mail-Nachrichten, die personenbezogene Daten mit einem „normalen Risiko“ beinhalten, sind mindestens mit einer obligatorischen Transportverschlüsselung zu versenden.

Sobald die Inhalte mit einem „hohen Risiko“ für die Betroffenen einhergehen, sollte mindestens eine qualifizierte Transportverschlüsselung (oder Inhaltsverschlüsselung) eingesetzt werden. Vor dem Hintergrund des aufwändigen Verfahrens bei der Inhaltsverschlüsselung, ist die qualifizierte Transportverschlüsselung immer grundsätzlich einmal das vorzugswürdige und rechtlich grundsätzlich auch angemessene Verfahren für Daten mit einem hohen Risiko.

Enthält die E-Mail Inhalte, die einem Berufsgeheimnis unterliegen, soll nach der DSK eine Inhaltsverschlüsselung verwendet werden.

Die einfache Standard-Transportverschlüsselung bietet bei der Übermittlung von personenbezogenen Daten laut der DSK keine ausreichende Sicherheit.

Von „normalen Risiken“ geht die DSK aus, wenn der Bruch der Vertraulichkeit ein Risiko für die Rechte und Freiheiten der betroffenen Person darstellt. Hinsichtlich der Schutzanforderungen ist von der nächsten Qualifikationsstufe zu sprechen, wenn mit dem Vertraulichkeitsbruch ein hohes Risiko einhergeht.

Für ein hohes Risiko kann es z.B. schon ausreichen, wenn der E-Mail-Inhalt schützenswerte Personengruppen (z.B. Beschäftigte oder Kinder) oder sensible personenbezogenen Daten (z.B. Gesundheitsdaten, Religion) betrifft. Aber auch der Versand besonders umfangreicher Daten kann zu einem hohen Risiko führen.

Indiz für ein hohes Risiko kann ferner die Verarbeitung von Daten sein, die dem Berufsgeheimnis unterliegen (vgl. Erwägungsgrund 75 der DS-GVO).

Es ist im Rahmen geschäftlicher Korrespondenz oder der Kommunikation von Behörden kaum ein Fall denkbar, in dem keinerlei personenbezogene Daten beim E-Mail-Versand verarbeitet werden. Zudem wird man als Unternehmen relativ oft die Grenze des „hohen Risikos“ erreichen können.

Wichtig ist zudem, dass Verantwortliche als Sender für den sicheren Kommunikationsverkehr verantwortlich sind. Allerdings stellt die DSK auch fest, dass Personen, die gezielt personenbezogene Daten per E-Mail entgegennehmen, die Voraussetzungen für den sicheren Empfang schaffen müssen.

Die DSK stellt demgegenüber wiederum ausdrücklich fest, dass ein anderer Kommunikationskanal als der E-Mail-Versand gewählt werden muss, wenn eine sichere Übermittlung per E-Mail nicht erfüllt werden kann. Ein Verantwortlicher sollte dazu also überhaupt erkennen können, ob ein eingesetztes und aktiviertes Verschlüsselungsverfahren „Erfolg“ hat. Das Fehlen der Voraussetzungen für eine obligatorische oder qualifizierte Transportverschlüsselung (z.B. kein STARTTLS oder mit TLS-Zertifikatsfehler) entbindet den

Verantwortlichen also nicht per se nicht von der Pflicht zur Verschlüsselung bzw. sicheren Datenübermittlung.
Aus dem Fehlen der Voraussetzungen für bestimmte Verschlüsselungsverfahren bei dem Empfänger kann auch nicht ohne Weiteres von einem Einverständnis des Empfängers in die ungesicherte Übermittlung ausgegangen werden.

Hieraus ist als Mindestvoraussetzung der Begutachtung damit auch in datenschutzrechtlicher Hinsicht von comcrypto zu erwarten, dass mindestens eine obligatorische sowie eine qualifizierte Transportverschlüsselung möglich ist.

Da ein hohes Risiko schnell anzunehmen ist, sollte die qualifizierte Transportverschlüsselung als „Standardverschlüsselung" herangezogen werden können.

Da diese beiden Verfahren aber nur dann funktionieren, wenn die Empfänger-Server die technischen Voraussetzungen erfüllen (Ziffer I. 2.2, 2.3), sollten Verantwortliche zudem eine Information darüber erhalten, wenn die Voraussetzungen beim Empfänger nicht erfüllt sind, um dann entscheiden zu können, wie weiter verfahren werden soll (z.B. Wahl der Inhaltsverschlüsselung oder eines anderen sicheren Kommunikationskanals).

Mindestvoraussetzungen

- Obligatorische und qualifizierte Transportverschlüsselung
- Information des Absenders, wenn der Empfänger über kein TLS-Zertifikat verfügt
- Ggfs. Inhaltsverschlüsselung

4.2. Umsetzung bei comcrypto und Bewertung

4.2.1. TOM bei comcrypto

Wie unter Ziffer I. 4.2, 4.3 beschrieben, trifft comcrypto umfangreiche technische und organisatorische Maßnahmen. Die einzelnen Maßnahmen können der beigefügten Beschreibung der technischen und organisatorischen Maßnahmen entnommen werden.

4.2.2. TOM beim Verantwortlichen

Comcrypto bietet sowohl eine obligatorische als auch eine qualifizierte Transportverschlüsselung an, die auch den Anforderungen der Richtlinien des BSI entsprechen (vgl. Ziffer I. 1.2, 1.3).

Sollte auf einem Empfänger-Server kein entsprechendes Zertifikat vorhanden sein oder eine Verifikation fehlschlagen, kann ein E-Mail-Versand außerdem automatisch abgebrochen und eine Inhaltsverschlüsselung erzwungen werden, worüber der Verantwortliche auch informiert wird (vgl. Ziffer I. 2.2, 2.3).

5. Privacy by design und by default nach Art. 25 DS-GVO

5.1. Gesetzliche Anforderungen

5.1.1. Datenschutz durch Technikgestaltung / Privacy by design, Art. 25 Abs. 1 DS-GVO

Art. 25 Abs. 1 DS-GVO regelt den Grundsatz „Datenschutz durch Technikgestaltung". Hiernach hat der Verantwortliche bereits zum Zeitpunkt der Festlegung der Mittel zur Datenverarbeitung als auch bei der eigentlichen Verarbeitung geeignete TOM (z.B. Pseudonymisierung) zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen. Auch hier sind, wie im Rahmen von Art. 32 DS-GVO, der Stand der Technik, die

Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken zu berücksichtigen.

Datenschutz soll demnach bereits in der Konzeptions- und Entwicklungsphase berücksichtigt werden. Soweit ein Verantwortlicher, wie beim Einsatz von Drittanbieter-Produkten auf diese Phase keinen bis kaum Einfluss hat, trifft den Verantwortlichen „nur“ noch die Pflicht, eine Prüfung der Vorgaben und entsprechend eine angemessene Auswahl eines Dienstleisters zu treffen. Eine unmittelbare „Pflicht“ für die einzelnen Anbieter, diese Voraussetzungen zu erfüllen besteht zwar nicht. Gleichwohl soll auch die Erfüllung der Anforderungen des Art. 25 Abs. 1 DS-GVO Mindestvoraussetzung sein.

5.1.2. Datenschutz durch datenschutzfreundliche Voreinstellungen / Privacy by default, Art. 25 Abs. 2 DS-GVO

Der Grundsatz des Datenschutzes durch datenschutzfreundliche Voreinstellungen nach Art. 25 Abs. 2 DS-GVO verpflichtet einen Verantwortlichen, geeignete TOM zu treffen, die sicherstellen, dass durch Voreinstellungen nur solche personenbezogenen Daten verarbeitet werden, die für den konkreten Verarbeitungszweck erforderlich sind. Das gilt sowohl hinsichtlich der Datenmenge, dem Verarbeitungsumfang, der Speicherfrist als auch der Zugänglichkeit.

Die Standardeinstellungen bei comcrypto sollten als Mindestvoraussetzung der Begutachtung also bereits ein grundsätzlich angemessenes Datenschutzniveau schaffen.

Mindestvoraussetzungen

- Benutzerfreundliche und differenzierte Konfigurationsmöglichkeiten zur Gewährleistung des Datenminimierungsgrundsatzes
- Auslieferung im Standard weist bereits die datenschutzfreundlichsten Einstellungen und eine auf das erforderliche Maß begrenzte Protokollierung auf

5.2. Umsetzung bei comcrypto

Wie unter Ziffer I. 5.2, 5.3 näher beschrieben, stellt comcrypto im Benutzer-Interface verschiedene Optionen und angemessen differenzierte Konfigurationsmöglichkeiten zur Individualisierung des Sicherheitsverhaltens zur Verfügung. Es ist möglich, jeder Empfängerdomain verschiedenen Risiko-Klassen zuzuordnen und dementsprechend je nach Risiko-Klasse einer Domain einzustellen, wann eine Inhaltsverschlüsselung eingesetzt werden soll.

Standardmäßig werden die E-Mails auf den comcrypto-Servern, die dort zum Zwecke der verschlüsselten Übertragung „zwischengelagert" werden, außerdem im Sinne des Datenminimierungsgrundsatzes und des Art. 25 Abs. 2 DS-GVO unverzüglich nach erfolgreicher Zustellung an den Empfänger gelöscht.

Es werden ferner bereits standardmäßig nur diejenigen Informationen protokolliert, die zwingend zur Durchführung und Dokumentation der Verschlüsselung erforderlich sind.

Weiterhin lässt sich auch der Datenschutzbeauftragte in eine geplante Einführung von comcrypto einbeziehen, da Kunden die Möglichkeit einer kostenfreien Test-Installation ermöglicht wird, um das E-Mail-Gateway vor dem Einsatz prüfen zu können.

6. Notwendigkeit einer Datenschutzfolgenabschätzung nach Art. 35 DS-GVO

Nach Art. 35 Abs. 1 Satz 1 DS-GVO müssen Verantwortliche eine Datenschutz-Folgenabschätzung durchführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. Dabei ist die Durchführung insbesondere erforderlich bei der umfangreichen Verarbeitung sensibler personenbezogener Daten (Art. 9 Abs. 1 DS-GVO).

Durch die naturgemäß große Menge an Daten, die, wenn auch nicht für lange Zeit, über comcrypto-Server laufen, verarbeitet comcrypto zwingend umfangreich Daten, und zwar Inhaltsdaten (Textinhalte und gegebenenfalls Anlagen) und Metadaten (z. B. Absender, Datum, Betreff).

Im Kern gestaltet comcrypto die Datenverarbeitung grundsätzlich sicherer. Die Verarbeitung im Zusammenhang mit dem E-Mail-Versand als solchen führt also wohl nicht schon zu hohen Risiken für die Betroffenen. Es sollte jedoch nicht außer Acht gelassen werden, dass Verantwortliche im Einzelfall je nach Sensibilität und Umfang der Verarbeitung zur Durchführung einer Datenschutz-Folgenabschätzung gezwungen sein können, wenn comcrypto eingeführt werden soll.

Letztlich muss jedes Unternehmen eine eigene Einzelfallprüfung vornehmen. Hierbei wird unter anderem auch eine Rolle spielen, ob comcrypto auf den eigenen Servern des Verantwortlichen oder in der Cloud-Variante des Anbieters verwendet wird. Es kann nicht pauschal beurteilt werden, ob der Einsatz von comcrypto für verantwortliche Stellen generell die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung auslöst.

IV. Ergebnis

Im Ergebnis bietet comcrypto mit seinen technischen Einstellungen und Konfigurationsmöglichkeiten ein Produkt, mit dem den Kunden eine datenschutzkonforme Verschlüsselung des E-Mail-Verkehrs gelingen kann. Die rechtlichen und technischen Mindestvoraussetzungen von MORGENSTERN für die Datenschutzbegutachtung sind erfüllt und gehen zum Teil auch darüber hinaus.

Mit der im Standard vorgesehenen obligatorischen Transportverschlüsselung bietet comcrypto das erforderliche Mindestmaß an Sicherheit bei der E-Mail-Kommunikation, ohne den „normalen" Kommunikationsfluss durch aufwendige Passworteingaben zu hemmen. Zugleich lässt sich comcrypto in nutzerfreundlicher Art und Weise an die Gegebenheiten des Kunden betreffend Schutzniveau des Inhalts sowie faktische Lage beim Empfänger individuell anpassen.

Comcrypto erhält von MORGENSTERN daher das Prädikat „Datenschutz-ready".

Chemnitz, 25/08/2021

Dr. Knut Karnapp

Rechtsanwalt | Attorney-at-law