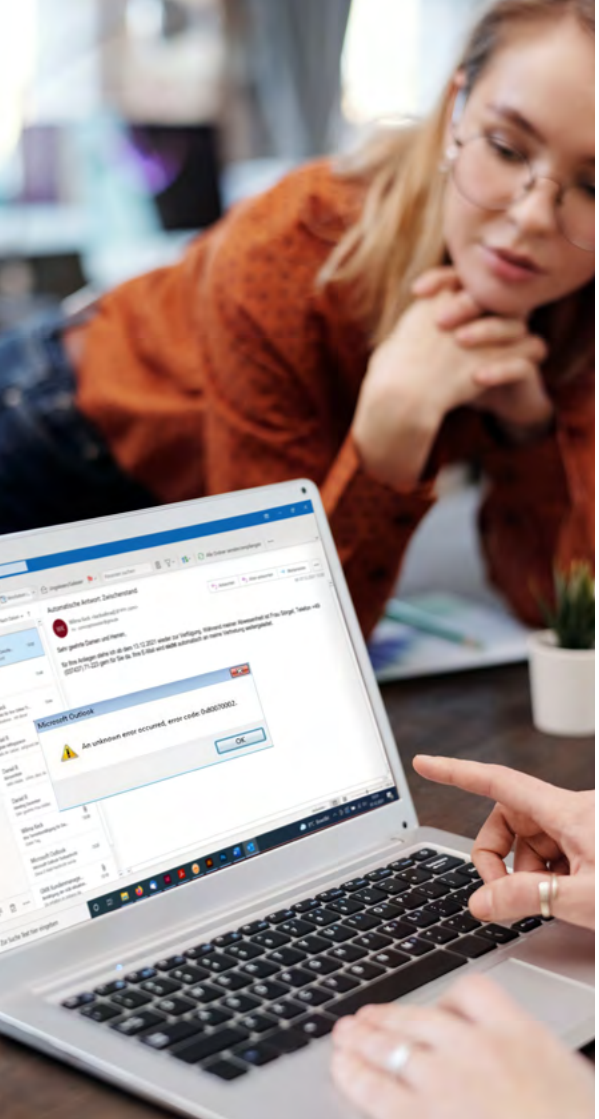

Datenschutz-
Kopfzerbrechen
beim
E-Mail-Versand?
Die Lösung:
comcrypto MXG



Vereinfachung von Prozessen für die E-Mail-Übertragung

Im Geschäftsalltag ist E-Mail weiterhin branchenübergreifend ein relevanter und stetig wachsender Kommunikationskanal. Die Umsetzung von Schutzmaßnahmen wie verschlüsselter E-Mail-Übertragung bedingt oft einen enormen finanziellen und vor allem organisatorischen Aufwand. Die Prozesse zum datenschutzkonformen E-Mail-Versand sind oft sehr komplex, schulungsbedürftig und nur schwer zu überwachen bzw. nachzuweisen.

Bei uns bekommen Sie eine **neue Kategorie der sicheren E-Mail-Übertragung**. Mehrere Verschlüsselungs-Technologien werden miteinander verknüpft und automatisiert angewendet. Wir nennen das **„adaptive Verschlüsselung“**.

Das bedeutet, dass die **Prozesse zur sicheren E-Mail-Übertragung** deutlich einfacher und sogar **automatisiert umgesetzt** werden können. Schutzziele aus gesetzlichen Pflichten (z.B. Datenschutz), aber auch aus dem eigenen Schutzbedarf heraus, werden mit erheblich weniger Aufwand erreicht.

Aufsichtsbehörden definieren mehrere angemessene Sicherheitslevel

Seit Mai 2020 gibt es klare Vorgaben der Landes-Datenschutzaufsichtsbehörden (aktualisiert im Juni 2021), welche technischen Maßnahmen eine angemessene Risikominderung bewirken, jeweils abhängig vom vorliegenden Datenschutz-Risiko für die Betroffenen.

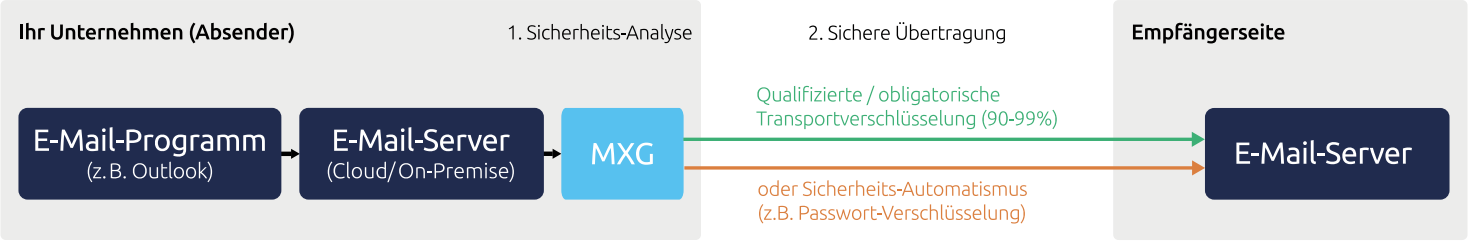
Fallgruppen	Anforderungen
E-Mail-Nachrichten mit **„normalen Risiken“**	Obligatorische Transportverschlüsselung („Mandatory TLS“, „erzwungenes TLS“) oder Inhaltsverschlüsselung
E-Mail-Nachrichten mit **„hohen Risiken“**	Qualifizierte Transportverschlüsselung („Verified TLS“, „TLS mit Zertifikatsprüfung“) oder Inhaltsverschlüsselung
Besonderheit für **Berufsgeheimnisträger**	„haben […] die Höhe des jeweiligen Risikos besonders zu prüfen“ Berufsgeheimnis ist ein **Indiz für hohes Risiko**

Daraus folgt:

1) Standard-TLS („opportunistic“ TLS) ist **keine ausreichende Absicherung** für den Versand von personenbezogenen Daten.

2) Inhaltsverschlüsselung ist zur Einhaltung der Vorgaben **nicht zwingend erforderlich.**

Comcrypto MXG – das E-Mail-Gateway für sichere ausgehende Übertragung



Die Besonderheit des **comcrypto MXG**: Erstmals werden Transport- und Inhaltsverschlüsselung **adaptiv miteinander verknüpft** und können so **automatisiert eingesetzt** weden. Neben den traditionellen Verschlüsselungsverfahren steht dabei auch die qualifizierte Transportverschlüsselung (geeignet für personenbezogene Daten mit hohen Risiken) zur Verfügung. Mit comcrypto MXG gelingt es automatisiert,

- ✔ zu identifizieren, mit welchen E-Mail-Empfängern die qualifizierte Transportverschlüsselung möglich ist (bei ca. 90% der ausgehenden E-Mails möglich),
- ✔ in diesen Fällen die ausgehende E-Mail sicher und sofort lesbar als „normale E-Mail“ zuzustellen (enorme Arbeitsersparnis), sowie
- ✔ für die restlichen Fälle einen geeigneten Sicherheits-Automatismus anzuwenden.

Passende Automatismen für verschiedene Prozesse (einige Beispiele)

Sensibler Datenaustausch, „hohe Risiken“

Wenn qualifiziertes TLS verfügbar ist, erfolgt die Zustellung als normale E-Mail mit sicherem Transport (in ca. 90% der Fälle).

Wenn qualifiziertes TLS nicht verfügbar ist, erfolgt eine automatische Verschlüsselung mit Passwort und die E-Mail wird mit passwortgeschütztem Anhang übertragen, zzgl. einer Information an den Absender.

Mindestsicherheit für Kommunikation mit „normalen Risiken“

Wenn obligatorische (oder qualifizierte) Transportverschlüsselung verfügbar ist, dann erfolgt die Zustellung als normale E-Mail mit ausreichend sicherem Transport (in ca. 99% der Fälle).

Wenn kein oder nur sehr schwaches TLS verfügbar ist, kommt es zum vorübergehenden Stopp der E-Mail und einer Rückfrage an den Absender.

Kommunikation ohne sensible Inhalte

Zustellung als normale E-Mail, auch bei Sicherheitseinschränkungen.

Der Absender erhält optional einen Hinweis, wenn ein unsicherer E-Mail-Transportweg vorliegt.

Kundenstimmen

„Die comcrypto-Technologie **durchlief erfolgreich unsere strenge Datenschutzprüfung**. Seit wir MXG im Einsatz haben, höre ich keine Klagen mehr aus der IT."
Uwe Sablotny, Geschäftsführer
Sparkasse Factoring GmbH

„Die Hinweise der MXG-Lösung sensibilisieren unsere Mitarbeiter und schaffen **automatisch mehr Bewusstsein für das Thema der Sicherheit** beim E-Mail-Versand, ohne dass wir einen Schulungsaufwand damit haben. Die Mitarbeiter werden davon **entlastet, sich vor jeder E-Mail Gedanken über die Sicherheit machen zu müssen**."
Matthias Schüring, Geschäftsführer
dia-systems GmbH (IT-Tochtergesellschaft der **Diakonie Mark-Ruhr gGmbH**)

„**Auch unter überdurchschnittlicher Last läuft das MXG noch entspannt** und sorgt automatisch ohne Aufwand für zuverlässige Sicherheit im E-Mail-Versand."
Marco Rauschmann, IT-Coordinator
Munich Security Conference (Stiftung Münchner Sicherheitskonferenz gGmbH)

„Ich habe in meinen verschiedenen beruflichen Stationen schon einige IT-Projekte mitgemacht. **Ich habe es selten erlebt, dass alles so problemlos läuft.**"
Stephan Poltermann, Administrator
Wohnungsbaugenossenschaft Zukunft eG

Branchenübergreifender Einsatz des MXG E-Mail-Gateways

comcrypto GmbH | Brückenstraße 4 | 09111 Chemnitz | +49 (0) 371 256206 - 00 | info@comcrypto.de