E-MAIL ENCRYPTION GATEWAY

SICHERER E-MAIL VERKEHR

E-MAIL – EIN ZENTRALES EINGANGSTOR FÜR CYBER-KRIMINELLE

Täglich werden bis zu 269 Milliarden E-Mails weltweit versendet.[1] Somit stellt die E-Mail-Kommunikation immer noch eines der wichtigsten Kommunikationswege im geschäftlichen Umfeld dar. Dabei ist die E-Mail-Kommunikation für Unternehmen weiterhin eine große Schwachstelle, welche Angreifer nutzen um Unternehmensdaten als „Man-in-the-middle“ abzugreifen. Sind die E-Mails unverschlüsselt, können Angreifer den Mailverkehr nicht nur mitlesen, sondern auch manipulieren. Kritisch wird es, wenn es sich um sensible bzw. vertrauliche Daten handelt.

Mit dem E-Mail Encryption Gateway (kurz EEGW) bietet die Telekom die Lösung, um sich vor Lausch-Attacken und E-Mail-Manipulationen zu schützen. Das EEGW stellt die Ver- und Entschlüsselung von E-Mails mittels hochsicheren Verschlüsselungsstandards sicher und lässt sich als Gateway einfach in bestehende Kunden-Infrastrukturen integrieren. Die „Security as a Service“-Lösung wird in hochsicheren deutschen Rechenzentren gehostet und gewährleistet damit die Umsetzung der Anforderungen der EU-DSGVO
(EU- Datenschutzgrundverordnung).

[1] vgl. Radicati Group (2017). Verfügbar unter: https://de.statista.com/statistik/daten/studie/252278/umfrage/prognose-zur-zahl-der-taeglich-versendeter-e-mails-weltweit/

FAKTEN
BEDROHUNGSLAGE DER DATENSICHERHEIT

WARUM IST DATENSICHERHEIT SO WICHTIG?

Datensicherheit ist heute ein sehr bedeutender Bestandteil von Unternehmen. Mit der EU-Datenschutzgrundverordnung gewinnt diese noch mehr an Bedeutung. Unternehmen verpflichten sich personenbezogene Daten zu schützen. Folgen können nicht nur Daten- und Reputationsverlust des Unternehmens, sondern auch hohe Bußgelder sein.

Damit es erst gar nicht so weit kommt, müssen personenbezogene Daten geschützt sein.
Mit dem EEGW wird eine erhöhte Sicherheitsanforderung an den E-Mail Verkehr garantiert. E-Mails sind somit auch außerhalb des firmeneigenen Netzwerkes geschützt.

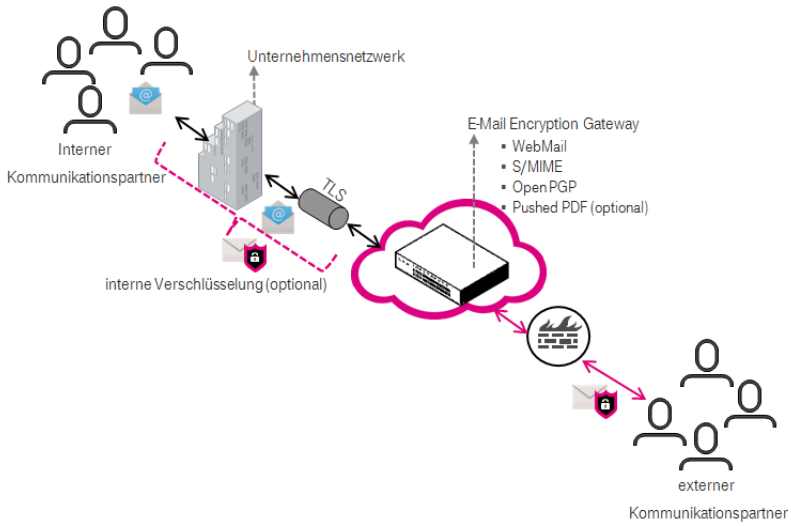
E-MAIL ENCRYPTION GATEWAY
DIE LÖSUNG

Das E-Mail Encryption Gateway schützt den E-Mail Verkehr auch außerhalb des Firmennetzwerkes. Mittels entsprechender Verschlüsselungstechnologie sind E- Mails vor Cyber-Kriminellen geschützt. Durch die in redundanten Rechenzentren aufgebaute EEGW-Plattform garantiert die Telekom eine monatlich durchschnittliche Verfügbarkeit von 99,20%.

DIE VORTEILE IM ÜBERBLICK:

- Keine Installation von Hardware oder Software erforderlich
- Keine Installation dedizierter E-Mail-Clients oder Plug-ins
- Betriebskosten und Administrationsaufwand auf ein Minimum reduziert
- Verfügbarkeit von 99,20%
- Service rund um die Uhr (24/7)
- einfache Bedienung für den Nutzer
- Automatische und zentrale Verwaltung von Zertifikaten und Schlüsseln
- Automatisches Einsammeln von S/MIME Zertifikaten und PGP-Schlüsseln
- Redundante Plattform erzeugt hohe Ausfallsicherheiten
- Lizenzierung anhand der Anzahl von E-Mail Adressen

WAS PASSIERT MIT DEN E- MAILS?



Die E-Mail wird vom internen Kommunikationspartner verschickt. Je nach Kriterium, wird die E-Mail am E-Mail Encryption Gateway (EEGW) verschlüsselt. Das EEGW erstellt dabei für den internen Kommunikationspartner ein selfsigned Open PGP Schlüsselpaar und S/MIME Zertifikat . Vom EEGW wird geprüft, ob der externe Kommunikationspartner bereits mit seinem Zertifikat/Schlüssel bekannt ist, um ihm die E-Mail entsprechend seiner Verschlüsselungstechnologie verschlüsselt zuzusenden. Ist er noch nicht bekannt, wird ihm eine Benachrichtigungsmail zur Authentifizierung versendet. Nutzt der externe Kommunikationspartner weder Open PGP noch S/MIME, stellt das WebMail Interface eine sichere Alternative dar, wodurch er dennoch verschlüsselte E-Mails lesen kann.

KOMMUNIKATION MIT EXTERNEN KOMMUNIKATIONSPARTNER

Beim Versenden einer E-Mail an einen externen Kommunikationspartner wird durch das EEGW geprüft, ob für diesen bereits ein Nutzerprofil in der Datenbank existiert.

E-MAIL WIRD VOM INTERNEN KOMMUNIKATIONSPARTNER VERSENDET

… was passiert mit dieser E-Mail wenn der externe Kommunikationspartner dem EEGW noch nicht bekannt ist oder dieser kein S/MIME oder Open PGP hat?

Sofern der externe Kommunikationspartner bisher noch nicht mit dem EEGW kommuniziert hat, erhält er eine Benachrichtigungsmail. Hierbei hat er zwei Möglichkeiten, um Zugriff auf die original E-Mail zu bekommen.

Der externe Kommunikationspartner benutzt S/MIME oder Open PGP Verschlüsselung. Hierbei antwortet er auf die Benachrichtigungsmail mittels einer durch sein Zertifikat signierten E-Mail bzw. hängt seinen PGP Schlüssel an. Nach Prüfung auf Gültigkeit der EEGW wird für ihn ein Nutzerprofil angelegt und die E-Mail zugesendet. Er gilt nun als „bekannt" für das EEGW und erhält alle weiteren E-Mails direkt in sein Postfach.

Der externe Kommunikationspartner benutzt keine E-Mail-Verschlüsselungstechnologie. Hierbei kann der externe Empfänger nach einer Registrierung über eine SSL gesicherte Webschnittstelle (=WebMail Interface) Zugriff auf die E-Mail bekommen oder wahlweise (optionale Leistung) sich die E-Mail als verschlüsseltes PDF zuschicken lassen (=Pushed PDF).

WELCHE VERSCHLÜSSELUNGSTECHNOLOGIEN WERDEN UNTERSTÜTZT?

- S/MIME
- Open PGP

Die Art der Verschlüsselung richtet sich danach, welches Verfahren für den externen Kommunikationspartner des Kunden im EEGW hinterlegt worden ist.

NACH WELCHEN KRITERIEN WIRD VERSCHLÜSSELT?

- Header (z.B. Vertraulichkeit: Persönlich / Privat / Vertraulich)
- Schlüsselwörter im Betreff
- Empfängerdomäne
- Absenderdomäne

DAS KEY MANAGEMENT DES EEGW UNTERSTÜTZT FÜR DAS VER-/ENTSCHLÜSSELN VON E-MAILS FOLGENDE STANDARDS:

- Asymmetrische Verschlüsselung: RSA, DSA, El Gamal
- Symmetrische Verschlüsselung: RC2, RC4, DES, 3DES, Blowfish, Twofish, Cast5, AES, AES192, AES256, IDEA, Safer-SK128
- Hash: MD2, MD5, MDC2, SHA, SHA–1, SHA–256, SHA–384, SHA–512, RipeMD160, Tiger, Haval

KONTAKT
T-Systems International GmbH
E-Mail: security-info@t-systems.com

HERAUSGEBER
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main