
Success Story
2
Nutzer
Münchner Sicherheitskonferenz
Passwort
****
Mail
msc
comcrypto

Foto: MSC / Karl-Josef Hildenbrand

Die Münchner Sicherheitskonferenz

Die Münchner Sicherheitskonferenz ist das weltweit führende Forum für Debatten zur internationalen Sicherheitspolitik. Sie bietet eine Plattform für diplomatische Initiativen und Ansätze, um den drängendsten Sicherheitsrisiken der Welt zu begegnen.

Die MSC will Vertrauen fördern und zur friedlichen Beilegung von Konflikten beitragen, indem sie einen **anhaltenden und informellen Dialog innerhalb der internationalen Sicherheitsgemeinschaft ermöglicht**.
Besonders großen Raum haben dabei die informellen Begegnungen zwischen Amtsträgern, um Frieden durch Dialog zu fördern. Bei der Hauptkonferenz im Februar versammeln sich mehr als 450 hochrangige Entscheidungsträger und prominente Meinungsführer aus der ganzen Welt – darunter Staatsoberhäupter, Minister, Führungspersönlichkeiten von internationalen Organisationen und Nichtregierungsorganisationen sowie führende Vertreter aus Wirtschaft, Medien, Forschung und Zivilgesellschaft.

Sichere E-Mail-Übertragung bei der Münchner Sicherheitskonferenz

Marco Rauschmann

Seit 2019 als Koordinator für IT und aktuell als IT-Manager bei der Stiftung Münchner Sicherheitskonferenz gGmbH in München tätig, Fachinformatiker mit jahrzehntelanger Berufserfahrung in international tätigen Großunternehmen wie der Fujitsu TDS und Escada SE.

Aufgrund der politischen Exponiertheit der Konferenz und unserer Teilnehmer legen wir nicht nur besonderen Wert auf die physische Sicherheit, sondern auch auf den **virtuellen Schutz unserer Gäste. Das gilt insbesondere für die Kommunikation**. Schon mehrfach haben Hackergruppen versucht, sich in die E-Mail-Konten unserer Teilnehmer einzuschleichen. In jüngster Zeit etwa war die berüchtigte Gruppe Phosphorous aus dem Iran sehr aktiv und nutzte angebliche E-Mails der MSC für Phishing-Attacken.

Wir waren daher auf der Suche nach einer Lösung, welche die **Sicherheit unserer E-Mail-Übertragungen erhöht. Gleichzeitig durften daraus aber keine komplizierten Prozesse** entstehen, vor allem für unsere Kommunikationspartner, die Teilnehmer der Konferenz.

Im Vorfeld hatten wir im Bedarfsfall bereits mit verschlüsselten E-Mail-Anhängen und auch mit S/MIME gearbeitet. Im internationalen Kontext gestalten sich die damit verknüpften Prozesse aber oft umständlich und schulungsaufwändig.

Zielgerichtete Umsetzung mit comcrypto MXG

Der erste Austausch zwischen der MSC und comcrypto erfolgte nach einer digitalen Veranstaltung zum Thema sichere E-Mail. **Das neuartige Sicherheitskonzept überzeugte durch einfache Prozesse für die User** und gleichzeitig große Flexibilität in der zentralen Konfiguration.

Die MSC startete daraufhin mit einer Pilotphase, um zu analysieren, wo etwaige Herausforderungen liegen und ob das Gateway von comcrypto diese in vollem Umfang bewältigt.

„Im Anschluss an die aufschlussreiche Analysephase haben wir uns gemeinsam mit dem Team von comcrypto **die technischen Workflows überlegt, die bestmöglich zu unseren organisatorischen Prozessen passen**.“, erklärt Marco Rauschmann, IT-Manager der Münchener Sicherheitskonferenz. „Diese Unterstützung direkt durch den Hersteller war sehr hilfreich.“

Bei der MSC werden, besonders im Vorfeld wichtiger Konferenzen, sensible Daten wie die Redemanuskripte der Teilnehmer ausgetauscht, die nicht vorab publik werden sollen. Andererseits geht es aber auch um den Schutz der Konferenzteilnehmer selbst und die **Vermeidung von IT-Sicherheitsrisiken.**

> *„Auch unter überdurchschnittlicher Last läuft das MXG noch entspannt und sorgt automatisch für zuverlässige Sicherheit im E-Mail-Versand.*
>
> *Marco Rauschmann,*
> *Manager IT*

Der Einsatz des E-Mail-Gateways comcrypto MXG führt beim E-Mail-Versand zu einem Sicherheits-Screening aller Empfänger-Server, bei dem **Veränderungen an den E-Mail-Systemen direkt sichtbar werden** und darauf reagiert werden kann. Mit dieser Gewissheit „kann ich meinen IT-Kollegen, z.B. in anderen internationalen Organisationen, dann auch mal einen Tipp geben, wenn was an ihren Mailservern nicht stimmt“, scherzt Rauschmann.

Andererseits werden die Abläufe für die eigenen Mitarbeiter durch das MXG Gateway nicht verändert. **Die Absender versenden normale E-Mails**, in seltenen Ausnahmefällen bekommen sie bei unvorhergesehenen Sicherheits-Risiken eine Rückmeldung. Diese einfache Handhabbarkeit war ein wichtiges Kriterium, da die Mitarbeiterzahlen vor und während der Konferenzen oft wechseln und **keine Schulungsaufwände für die neue Lösung entstehen durften**.

Comcrypto MXG erfüllt diese Anforderungen, dank des Einsatzes der „**Adaptiven Verschlüsselung**“. Der Begriff beschreibt die technische Verknüpfung von Inhalts- und Transportverschlüsselung sowie automatischer Fallback-Mechanismen und deren automatisierte Anwendung, angepasst an das benötigte Schutzniveau der E-Mail.

Marco Rauschmann fasst zusammen: „**Auch unter überdurchschnittlicher Last läuft das MXG noch entspannt und sorgt automatisch für zuverlässige Sicherheit im E-Mail-Versand.**“

Über die comcrypto GmbH

*Die comcrypto GmbH mit Sitz in Chemnitz entwickelt kryptographische Systeme zum Schutz digital übermittelter Daten per E-Mail. Aus einem Forschungsprojekt in Kooperation mit der Technischen Universität Chemnitz gegründet, ging comcrypto 2018, nach mehrjähriger Entwicklung des heute über 20-köpfigen Teams, mit dem **E-Mail-Gateway MXG** an den Markt.*

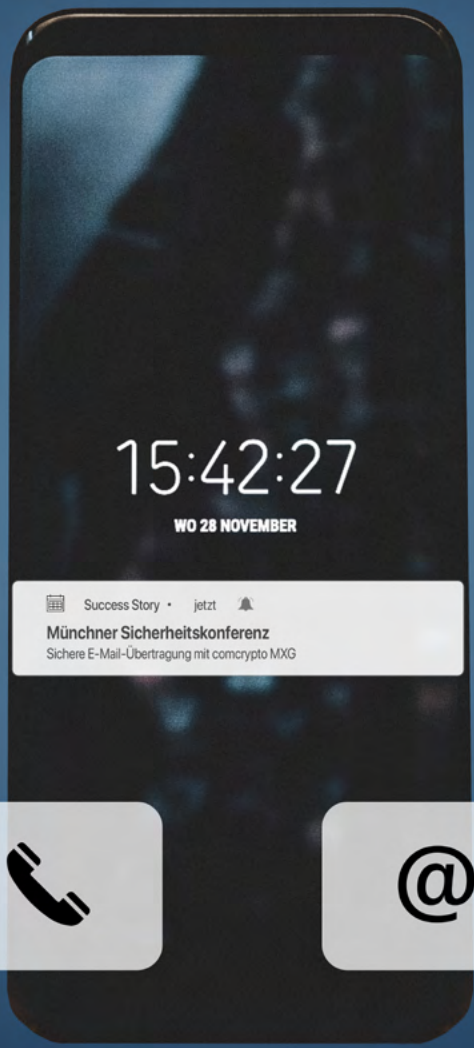
Comcrypto MXG **verknüpft** dabei **bestehende technologische Ansätze** der E-Mail-Verschlüsselung zur sogenannten **adaptiven Verschlüsselung**, angepasst an aktuelle Vorgaben der deutschen Datenschutzaufsichtsbehörden. Die adaptive Verschlüsselung ermöglicht es, ausgehende E-Mails **automatisiert** und stets mit dem für die Übertragung nötigem Sicherheitslevel zu versenden.

Das Unternehmen folgt bei der Entwicklung einer klaren „**Do it yourself**“ – Philosophie. Von der ersten Skizze auf Papier bis zur letzten Zeile Code entstehen alle E-Mail-Lösungen komplett inhouse. Mittels jahrelanger Weiterentwicklung des comcrypto-eigenen Technologie-Stack bis hin zur Betrachtung von Post-Quanten-Kryptographie, besitzt das Unternehmen alle nötigen Kompetenzen, E-Mail-Übertragung heute und in Zukunft sicher und komfortabel zu gestalten.

Comcrypto ist **Mitglied im Cyber-Sicherheitsrat Deutschland e. V.** und hat sich mit der Mitgliedschaft im TeleTrusT - Bundesverband IT-Sicherheit e.V. dem Grundsatz der hochqualitativen und vertrauenswürdigen “**IT Security made in Germany**” verschrieben.

msc

comcrypto



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