

Herausforderungen cloud-basierter Mail-Infrastrukturen

Immer mehr Unternehmen verabschieden sich davon, den Groupware-Server im eigenen Rechenzentrum zu verwalten. Der Trend geht klar zur Kommunikationslösung aus dem Netz. In dieser Konstellation wird der Groupware-Server in der Cloud betrieben. Oder Firmen richten eine hybride Umgebung ein, die eine Kombination der on premise und in der Cloud laufenden Systeme erfordert. Cloud-Lösungen wie Microsoft 365 bieten viele Vorteile wie garantierte Verfügbarkeit und fortwährende Aktualität.

Doch welchen Herausforderungen stehen Sie als Entscheider gegenüber, wenn Ihr Unternehmen die E-Mail-Anwendung in der Cloud hostet? Was ist dran an der Angst vor Kontrollverlust, beispielsweise durch Hackerangriffe oder auch den Zugriff durch Regierungseinrichtungen? Um eine sichere E-Mail-Kommunikation gewährleisten zu können, gibt es bei der Einführung von Microsoft 365 so einige Punkte zu beachten. Im Whitepaper zeigen wir, wie Sie mögliche Schwierigkeiten aus der Welt schaffen.

1 VERTRAULICHKEIT UND DATENSCHUTZ

Wer sich mit E-Mail beschäftigt, der kommt nicht um die DSGVO herum. Die EU-weite Grundverordnung zum Datenschutz ist für die E-Mail-Kommunikation relevant, da sie den Schutz personenbezogener Daten vorschreibt und im Fall von Verstößen erhebliche Bussgelder vorsieht. Über E-Mail werden bis dato sehr viele Personendaten versendet. Als adäquate Schutzmassnahme für diese Daten nennt die DSGVO Verschlüsselung.

Natürlich sind Verschlüsselung und Datenschutz keine cloud-spezifischen Themen. Auch beim Betrieb einer On-Premise-Infrastruktur gibt es gute Gründe, E-Mails nicht im Klartext zu versenden. Neben DSGVO-Compliance ist das beispielsweise der Schutz von geistigem Eigentum und Geschäftsgeheimnissen.



Verschärft die Cloud-Infrastruktur das Thema? Es wäre zu einseitig, on premise als per se sicher und die Cloud als grundsätzlich unsicher zu sehen. Aber wenn die Cloud als Speicher aller E-Mails des Unternehmens fungiert, macht das den Datenschutz nicht einfacher. Verschlüsselung ist also in jedem Fall angebracht.

Wie ist es also um die Verschlüsselung der Kommunikation in Microsoft 365 bestellt?

2 DATENHOHEIT UND KONTROLLE

Natürlich bietet Microsoft 365 mit Microsoft Azure Information Protection (AIP) eine eigene Verschlüsselungstechnologie, um E-Mails und weitere Inhalte wie Dokumente zu schützen.

Die Nutzung der Microsoft-eigenen Verschlüsselung bringt jedoch eine andere Problematik mit sich, und zwar die der Datenhoheit und Kontrolle. Es ist ein bisschen so, wie jemandem eine verschlossene Geldkassette zur Aufbewahrung zu geben und den Schlüssel mit Klebestreifen darunter zu kleben: dann hätte man die Geldkassette gar nicht erst abschliessen zu brauchen.

Microsoft hat höchstwahrscheinlich kein Interesse daran, Kundeninformationen zu entschlüsseln und zu nutzen. Als amerikanisches Unternehmen fällt der Konzern allerdings unter den CLOUD Act von 2018. Dabei handelt es sich um eine Verschärfung des USA PATRIOT Act von 2001. Vormalig unklare Sachverhalte wurden konkretisiert und der CLOUD Act verschafft US-Behörden jetzt auch Zugriff auf Daten, die auf Servern von US-Unternehmen im Ausland gespeichert sind, und das sogar rückwirkend.

Um die Hoheit über ihre Daten in Microsoft 365 zu behalten, sollten Unternehmen auf eine Verschlüsselung setzen, bei der das Schlüsselmaterial nicht in der Kontrolle des Providers liegt.

3 NUTZERFREUNDLICHKEIT UND AUTOMATISIERUNG VON VERSCHLÜSSELUNG

Verschlüsselung ist kein einfaches Thema. Entscheidend für die erfolgreiche Umsetzung ist die Akzeptanz auf Seiten der Nutzer, für die wiederum die Nutzerfreundlichkeit der Verschlüsselungslösung wichtig ist.

Die Verschlüsselung, zum Beispiel mit ein paar S/MIME-Zertifikaten, selbst in die Hand zu nehmen, ist daher keine gute Alternative. Das funktioniert höchstens bei kleinen Firmen mit technisch sehr versierten Mitarbeitern.

Damit Verschlüsselung nicht am Widerstand oder auch mangelnden technischen Wissen der Mitarbeiter scheitert und diese sich auf ihre eigentlichen Tätigkeiten konzentrieren können, sollte die Verwaltung von Schlüsseln und Zertifikaten sowie die Registrierung der Nutzer immer automatisiert und möglichst im Hintergrund ablaufen.



4 BEDÜRFNISSE VON KOMMUNIKATIONSPARTNERN

Verschlüsselung ist nie einseitig. Wenn Kommunikationspartner nicht in die Überlegungen miteinbezogen werden, ist das ganze Unterfangen zum Scheitern verurteilt.

Es gibt nur sehr wenige Unternehmen, die genug Macht haben, um ihre Verschlüsselung bei allen Kommunikationspartnern – wie Lieferanten, Partnern, Geschäfts- und Privatkunden – «durchzudrücken». Selbst Microsoft hat es trotz wirklich starker Verbreitung seiner Lösungen (noch) nicht geschafft, Azure Information Protection zum allgemeingültigen und alleinigen Standard zu machen.

In der Realität existieren neben Microsofts proprietärer Verschlüsselung weitere Standards, die verbreitet sind und weltweit genutzt werden: S/MIME und (Open)PGP. Und gerade KMU und auch die meisten Privatanwender nutzen gar keine Verschlüsselung, verfügen also weder über Technologie noch über Know-how, um verschlüsselte E-Mails auch nur lesen zu können.

Daher besteht eine weitere Herausforderung bei der Nutzung von Microsoft 365 darin, diese Vielfalt von Verschlüsselungsstandards in der Realität abzubilden und Kommunikationspartnern mehr als Microsofts AIP anzubieten – nämlich genau das, was diese bereits verwenden. Oder – falls sie gar nichts haben – etwas anzubieten, damit verschlüsselte Mails nicht ungelesen bleiben.

5 MIGRATION VON KLARTEXT-ALTLASTEN

Eine weitere Herausforderung bei der Migration zu Microsoft 365 sind «Klartext-Altlasten», denn die meisten Unternehmen haben über Jahre Tausende von unverschlüsselten Nachrichten auf den Servern in der On-Premise-Infrastruktur angesammelt. Selbst wenn Unternehmen sich für eine zusätzliche Verschlüsselungslösung entscheiden, bevor sie ihre E-Mail-Infrastruktur in die Cloud verlagern, gilt die Verschlüsselung in der Regel nur für neue E-Mails. Was passiert dann mit den vielen Klartext-E-Mails? Müssen Unternehmen sich damit abfinden, dass diese Altlasten mit zahlreichen Unternehmensinformationen zukünftig unverschlüsselt in der Cloud lagern und angreifbar sind?



Sichere und nutzerfreundliche E-Mail-Kommunikation in Microsoft 365

Unternehmen haben also einige Herausforderungen zu meistern, wenn sie die Hoheit über ihre Daten behalten und internen Nutzern wie Kommunikationspartnern eine automatisierte und nutzerfreundliche Lösung für sichere E-Mail-Kommunikation bieten wollen. Eine integrierte E-Mail-Verschlüsselungslösung bringt die Datenhoheit zurück ins Unternehmen und ermöglicht automatisiertes sowie anwenderfreundliches Verschlüsseln aller E-Mails. Dabei können Unternehmen Microsoft 365 exakt auf ihre Belange ausrichten, indem sie das Programm um eine integrierte Lösung wie **totemomail**® erweitern.

Mit **totemomail**® wird die Kommunikation innerhalb des Unternehmens mit S/MIME (oder wahlweise auch Microsoft AIP) abgesichert. So wird Microsoft 365 zum sicheren E-Mail-Speicher in der Cloud. Dabei übernimmt **totemomail**® das Schlüssel- und Zertifikatsmanagement, damit die Mitarbeiter den Kopf für anderes freihaben.

Für die sichere Kommunikation nach aussen stehen S/MIME, OpenPGP, TLS und Microsoft AIP zur Verfügung. Falls Empfänger diese Technologien nicht unterstützen, bietet die Lösung mit WebMail und Registered Envelope zwei alternative Methoden, mit denen sie verschlüsselte E-Mails lesen können, ohne über entsprechende Infrastruktur oder technisches Know-how zu verfügen.

EINE LÖSUNG FÜR BESTANDSDATEN IM KLARTEXT

Das **totemomail**® Verschlüsselungs- und Migrations-Tool verschlüsselt bestehende Postfächer und Ordner eines Nutzers mit dessen internen Zertifikat in der On-Premise-Lösung. Dies kann im laufenden Betrieb geschehen, ohne dass der Nutzer dadurch beeinträchtigt wird. Anschliessend werden die nun verschlüsselten Inhalte mit den Microsoft-Migrationstools zu Microsoft 365 migriert.

KONTAKT

Wir freuen uns auf Ihre Kontaktaufnahme, um Ihre ganz speziellen Anforderungen im Zusammenhang mit Office 365 zu besprechen.

Sales Team

sales@totemo.com

+41 44 914 99 00

