DSGVO-konforme E-Mail-Kommunikation in der Cloud

SEPPmail Secure E-Mail-Gateway für Microsoft 365

In vielen Unternehmen ist Microsoft 365 (MS365), die cloud-basierte Version des Office-Anwendungspaketes, nicht mehr wegzudenken. Ein Großteil der Nutzer setzt sich jedoch nicht gründlich damit auseinander, ob die offerierten Sicherheitsvorkehrungen genügen – und das, obwohl Microsoft mit seinen Anwendungen zu einem der beliebtesten Ziele von Cyberkriminellen gehört. So bietet MS365 selbst etwa keine umfangreiche datenschutzkonforme Verschlüsselung nach internationalen Standards für den E-Mail-Versand an. Mit den Lösungen von SEPPmail hingegen erhalten Betriebe eine professionelle Ergänzung für die zertifikatsbasierte Signatur und Verschlüsselung in der MS365-Cloud.

Autor: Günter Esch, Geschäftsführer der SEPPmail – Deutschland GmbH

Gerade für Firmen, die ihre E-Mail-Server als Online-Exchange in der Cloud betreiben, ist es wichtig, geeignete Schutzmaßnahmen zu treffen. Denn bei dem Einsatz von E-Mail-Verschlüsselungslösungen sollten Hacker zu keinem Zeitpunkt in der Lage sein, entsprechende Schlüssel abzugreifen. Auch eine Spontanverschlüsselung ist nur bedingt sicher, wenn es lediglich einen einzigen Unternehmensschlüssel gibt. Entwendet ein Angreifer diesen, ist sogleich die gesamte Unternehmenskommunikation gefährdet. Hinzu kommt, dass eine E-Mail-Signatur über Zertifikate möglich sein sollte. SEPPmail hat sich auf diese Anforderungen spezialisiert und bietet sein Secure E-Mail-Gateway zum Schutz vor Angriffen und der Kompromittierung sensibler Daten auch für Kunden an, die ihre E-Mail-Infrastruktur in MS365 nutzen. Das Gateway lässt sich problemlos in den MS365-Mailstrom integrieren und in der Verantwortung des Kunden betreiben. Exchange Online bleibt hierbei unverändert die zentrale Stelle für den E-Mail-Verkehr, und Sicherheitsfeatures wie Anti-Virus oder Anti-Spam finden weiterhin Verwendung.

E-Mail-Verschlüsselung

SEPPmail unterstützt alle gängigen Standards wie S/MIME, OpenPGP, Domainverschlüsselung und TLS. Verfügt der Empfänger über eigenes Schlüsselmaterial, kommt beim E-Mail-Versand die jeweils beste Methode automatisch zum Einsatz. Der private Schlüssel liegt hierbei ununterbrochen in der Infrastruktur des Kunden. Die patentierte GINA-Technologie erlaubt zudem die verschlüsselte Spontankommunikation mit Adressaten, die selbst keine Verschlüsselungslösung verwenden. Das Verfahren benötigt weder beim Absender noch beim Empfänger eine zusätzliche Softwareinstallation. Alle E-Mails lassen sich wie gewohnt empfangen und werden nach einer kurzen Passworteingabe entschlüsselt. Hier gibt es allerdings nicht nur einen übergreifenden Unternehmensschlüssel, sondern jeder Empfänger besitzt einen eigenen Schlüssel. So wird auch bei MS365 ein sicherer, vertraulicher und unkomplizierter Informationsaustausch gewährleistet.

Zertifikatsbasierte E-Mail-Signatur

Um die Identität des Unterzeichners nachzuweisen, beherrscht die SEPPmail-Appliance außerdem die RFC-konforme Signatur über Zertifikate. Dadurch lässt sich belegen, dass E-Mails vom entsprechenden Absender stammen und auf dem Versandweg nicht verändert wurden. Bei Erstversand beantragt die SEPPmail-Appliance vollautomatisiert ein Zertifikat bei einer der akkreditierten Zertifizierungsstellen, den sogenannten Certificate Authorities. Im Anschluss wird die E-Mail im Namen des Benutzers signiert und derart dessen Herkunft und Integrität bekräftigt.

Large File Transfer

Zu guter Letzt erweitert SEPPmail MS365 um die Funktion des vollintegrierten Large File Transfer (LFT), dank dem sich auch übergroße Dateien verschlüsselt versenden lassen. Hierfür gibt es ein Extra-Add-In für den Outlook-Client.

Teaser:

Wo bewahren Sie Ihren Bankfachschlüssel auf?

Banken bieten Ihnen die Möglichkeit, schützenswerte Gegenstände sicher in einem Bankfach zu hinterlegen. Die Bank Ihres Vertrauens kann ihr Schließfach jedoch zu keinem Zeitpunkt öffnen, da nur Sie den passenden Schlüssel besitzen. Exakt so sollte es auch beim Schutz Ihrer E-Mail-Kommunikation sein.

E-Mails in der Cloud sicher versenden

SEPPmail Secure E-Mail-Gateway für Microsoft 365

In vielen Unternehmen ist Microsoft 365 (M365), die cloud-basierte Version des Office-Anwendungspaketes, nicht mehr wegzudenken. Ein Großteil der Nutzer macht sich jedoch keine Gedanken darüber, ob die offerierten Sicherheitsvorkehrungen ausreichen – und das, obwohl Microsoft mit seinen Anwendungen zu einem der beliebtesten Ziele von Cyberkriminellen zählt. Zum Schutz vor Angriffen und der Kompromittierung Ihrer Daten bietet SEPPmail seine Lösungen zur E-Mail-Verschlüsselung und zertifikatsbasierten Signatur auch für M365 an – und die Schlüssel bleiben jederzeit nur bei Ihnen!

Datenschutzkonforme E-Mail-Kommunikation

Gerade für Firmen, die ihre E-Mail-Server als Online-Exchange in der Cloud betreiben, ist es wichtig, geeignete Datenschutzmaßnahmen zu treffen. So gilt es, bei dem Einsatz von E-Mail-Verschlüsselungslösungen darauf zu achten, dass Cyberkriminelle zu keinem Zeitpunkt entsprechende Schlüssel abgreifen können. Auch eine Spontanverschlüsselung, bei der es lediglich einen einzigen Unternehmensschlüssel gibt, ist nur bedingt sicher. Entwendet ein Angreifer den Schlüssel, ist sofort die gesamte Unternehmenskommunikation gefährdet. Hinzu kommt, dass eine E-Mail-Signatur über Zertifikate möglich sein sollte. Mit dem Secure E-Mail-Gateway erfüllt SEPPmail genau diese Anforderungen. Das Gateway lässt sich problemlos in den M365-Mailstrom integrieren und dabei in Ihrer Verantwortung betreiben. Exchange Online bleibt hierbei unverändert die zentrale Stelle für den E-Mail-Verkehr, und Sicherheitsfeatures wie Anti-Virus oder Anti-Spam finden weiterhin Verwendung.

E-Mail-Verschlüsselung

SEPPmail unterstützt alle gängigen Standards wie S/MIME, OpenPGP, Domainverschlüsselung und TLS. Verfügt der Empfänger über eigenes Schlüsselmaterial, kommt beim E-Mail-Versand die jeweils beste Methode automatisch zum Einsatz. Der private Schlüssel liegt hierbei ununterbrochen in der Infrastruktur des Kunden. Die patentierte GINA-Technologie erlaubt zudem die verschlüsselte Spontankommunikation mit Adressaten, die selbst keine Verschlüsselungslösung verwenden. Alle E-Mails lassen sich wie gewohnt empfangen und werden nach einer kurzen Passworteingabe entschlüsselt. Hier gibt es allerdings nicht nur einen übergreifenden Unternehmensschlüssel, sondern jeder Empfänger besitzt einen eigenen Schlüssel.

Zertifikatsbasierte E-Mail-Signatur

Um die Identität des Unterzeichners nachzuweisen, beherrscht die SEPPmail-Appliance außerdem die RFC-konforme Signatur über Zertifikate. Dadurch lässt sich belegen, dass E-Mails vom entsprechenden Absender stammen und auf dem Versandweg nicht verändert wurden.

Bei Erstversand beantragt die SEPPmail-Appliance vollautomatisiert ein Zertifikat bei einer der akkreditierten Zertifizierungsstellen, den sogenannten Certificate Authorities. Im Anschluss wird die E-Mail im Namen des Benutzers signiert und derart dessen Herkunft und Integrität bekräftigt.