Sichere E-Mail und Datenaustausch

mit Mail-Gateways wie von SEPPmail

CAIRO

secure • digital • IT-infrastructures

Der Schutzbedarf nach einer wirklich sicheren Kommunikation und Datenaustausch zwischen Sender und Empfänger - über verschiedene Organisationen hinweg - ist sehr hoch.

Die letzte gesetzliche Änderung war die Einführung der e-Rechnung Anfang 2025, die sowohl auf die E-Mail-Archivierung, aber auch auf den sicheren Austausch der Rechnungen, die Anforderungen nochmal erhöht. Einen wirklichen Schutz bietet nur ein Verschlüssungsverfahren, das aber auch für die Anwender und die IT zu managen ist.

Mail-Gateways

Die Aufwendungen für eine Verschlüsselung sind sowohl auf der Benutzerseite als auch auf der IT-Seite erheblich, da zum einen die IT eine PKI-Infrastruktur bereitstellen muss, als auch die 2 Benutzer mit den privaten & öffentlichen Schlüsseln umzugehen lernen müssen, inkl. deren Nutzung in den E-Mail-Clients. Beides führt dazu, dass gerade im KMU-Segment, die eigentliche E-Mail-Verschlüsselung **nicht** genutzt wird.

Eine professionelle Mail-Gateway Lösung wie von SEPPmail mit einer eingebauten/angeschlossenen PKI-Infrastruktur und einer Zertifikatsverwaltung löst alle diese Herausforderungen.

SEPPmail ist ein deutscher Hersteller und Dank dem von SEPPmail selbst entwickelten GINA-Verfahren ist es den Nutzern möglich, E-Mails verschlüsselt an Empfänger zu übermitteln, die gar keine Verschlüsselungssoftware einsetzen und keinen Schlüssel besitzen.

Die GINA-Spontanverschlüsselung verschlüsselt nach den neusten und sicheren Public-Key-Standards und benötigt keine Softwareinstallation – weder beim Sender noch beim Empfänger.

Die E-Mails können im gewohnten E-Mail-Programm empfangen werden und werden durch **einmalige** Eingabe eines Passworts (via SMS oder Telefon übermittelt) entschlüsselt. Faktisch wird der Key darüber freigeschaltet.

Der Vorteil eines Mail-Gateways ist, dass man alle anderen Schutzmechanismen (Firewall, M365 EOL, Defender) nahe am Sender bzw. Empfänger weiter nutzen kann, da es selbst erstmal per se keine E2E Verschlüsslung durchführt, die die Mails dann unsichtbar für die anderen Schutzmechanismen machen würden.

SEPPmail kann man – je nach Wunsch – aber auch als E2E konfigurieren.

Sie können das Mail-Gateway selbst oder in Ihrer Cloud oder in der Hersteller-Cloud betreiben.

Unsere Beratung, Kauf, Implementierung & Service

CAIRO berät Sie bei der Produktauswahl von Mail-Gateways wie SEPPmail, NoSpamProxy oder Hornetsecurity.

Unsere Spezialisten nehmen Ihre Anforderungen und Ihre bestehenden Mail-Systeme auf, wählen die passenden kostengünstigen Hersteller aus und integrieren diese in Ihre Landschaft und den Betrieb.

Alle Aspekte rund um Mail-Systeme sind Teil unseres Beratungs-Portfolios für moderne Infrastrukturen bis Security- und Compliance-Prüfungen, über das Schwachstellen-Management & Security Awareness Trainings bis zum sicheren IT-Betrieb.

CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).

CAIRO
secure · digital · IT-infrastructures

Tel.: +49 (0)621 86 75 10 Mail: info@cairo.ag Web: www.cairo.ag