DATENBLATT **Secure Mail Gateway**

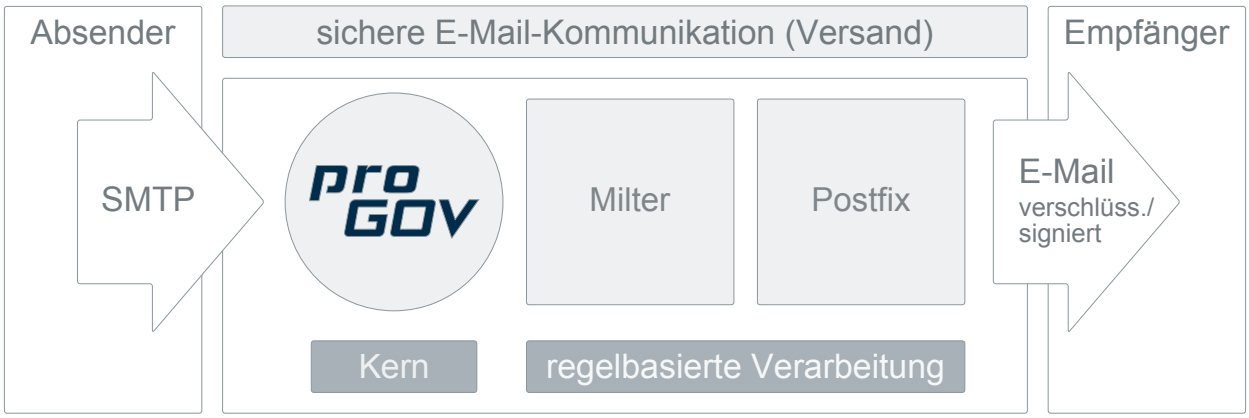
proGOV-Prozess: Sichere E-Mail-Kommunikation

- ✓ Automatisierter Schutz sensibler Daten
- ✓ Verhindert Verstöße gegen die DSGVO
- ✓ Geeignet für Behörden und Unternehmen
- ✓ Integration in marktübliche E-Mail-Systeme
- ✓ Integration in Fachanwendungen

Die Herausforderung

E-Mail ist ein einfacher und erprobter Kommunikationskanal und aus der heutigen Bürokommunikation nicht mehr wegzudenken. Die Tatsache, dass es sich dabei um einen offenen Informationsaustausch, vergleichbar mit einer Postkarte handelt, wird oft vernachlässigt oder verdrängt. Doch nicht erst mit der Wirksamkeit der DSGVO sollte der Schutz, also die Verschlüsselung personenbezogener Daten, eigentlich als Standard gelten. Neben dem Zwang der Gesetzgebung gibt es in Unternehmen aller Branchen und Größenordnungen aber auch in Institutionen des öffentlichen Dienstes schützenwertes Informationsgut, welches besonderer Sorgfalt beim elektronischen Versand bedarf.

Dafür stehen heute zwei sogenannte Public-Key-Verfahren zur Verfügung. Zum einen ist dies S/MIME (Secure/Multipurpose Internet Mail Extensions) und zum anderen PGP (Pretty Good Privacy). Beide Verfahren nutzen standardisierte Algorithmen und Zertifikate sowie öffentliche und private Schlüssel. Auf die Beschreibung der technischen Unterschiede wird an dieser Stelle verzichtet, nicht aber auf einen gravierenden Unterschied beim Nachweis der Authentizität.
Die Anbieter von S/MIME-Zertifikaten sind meist geprüfte Zertifizierungsstelle (CA) oder Vertrauensdienste, die, je nach Klassifizierung, eine Überprüfung der Echtheit einer E-Mail-Adresse und/oder der Identität einer Person bzw. Organisation vornehmen



Vorbetrachtungen

Aus dem Blickwinkel der Informationssicherheit leiten sich die Grundforderungen an den sicheren E-Mail-Austausch aus den normativen Schutzzielen ab. Zur Erfüllung dieser allgemein gültigen Normen leistet Kryptologie einen wesentlichen Beitrag. So dienen Verschlüsselung und Signatur dem Schutz der Integrität, dem Nachweis der Authentizität und der Geheimhaltung von E-Mail-Nachrichten.

und dies als Attribut in das ausgestellte Zertifikat eintragen. Bei PGP-Zertifikaten gibt es dagegen keine zentralen Vertrauensinstanzen. Sie können de facto von jedem im ‚Web of Trust' erzeugt und ausgegeben werden. Das Vertrauen wird von den Benutzern selbst verwaltet. Insbesondere bei der Schaffung von sicheren und vertrauenswürdigen Verwaltungs- und Geschäftsprozessen ist die Anwendung von Zertifikaten ohne vorherige Identitätsüberprüfung nicht angeraten. Verallgemeinert gilt S/MIME = hohe Vertrauensstellung und PGP = niedrige Vertrauensstellung.

DATENBLATT **Secure Mail Gateway**

proGOV-Prozess: Sichere E-Mail-Kommunikation

Lösungsszenario

Die Verantwortung über die Anwendung der kryptographischen Verfahren liegt im Ermessen des Anwenders. Genau an dieser Stelle setzt proGOV als zentrales Secure Mail Gateway an und nimmt innerhalb von geschlossenen Nutzergruppen als regelbasierte Lösung dem einzelnen Anwender diese Entscheidung ab. Es setzt unter anderem Sicherheitsvorgaben der Behörde oder des Unternehmens um, dass zum Beispiel alle ausgehenden E-Mails zu signieren sind und/oder E-Mails mit schützenswertem Inhalt vor Versand immer zu verschlüsseln sind. Geht dies nicht, wird der Versand blockiert und der Absender informiert, um über den weiteren Ablauf entscheiden zu können. Dafür wird proGOV als zentrale Sicherheitskomponente in die Mailkette der bestehenden Infrastruktur einer Organisation integriert. Es arbeitet dann zwischen dem äußerem Mailrelay/Spam- und Virenschutz und internem Mailserver und ergänzt kryptologische Funktionen.

Eine Mail wird dabei von einem beliebigen zuliefernden E-Mail-System erzeugt und via SMTP in proGOV eingeleitet und zur weiteren Behandlung an das integrierte Regelwerk (Milter = Neologismus aus Mail und Filter) übergeben. Die dort hinterlegten Regeln bestimmen nun auf welche Art und Weise (z.B. Signatur oder Signaturprüfung; Ver- oder Entschlüsselung; PGP oder S/MIME) die Mail verarbeitet werden soll. Hierzu werden verschiedenste Marker (Einträge im Header, z .B. Betreff, Absender, Empfänger) und Eigenschaften (Anzahl, Art und Größe der Anhänge) ausgewertet und zugehörige Operationen ausgelöst. Die zur Verschlüsselung oder Signatur notwendigen öffentlichen und privaten Schlüssel werden in der integrierten Zertifikatsverwaltung des proGOV gespeichert und verwaltet oder können aus öffentlichen Verzeichnisdiensten abgerufen werden. Nach erfolgreicher Behandlung verlässt die E-Mail das Regelwerk und wird an die nächste Stelle in der Mailkette weitergeleitet.

Eine besondere Vereinfachung ergibt sich aus der Signaturprüfung bei eingehenden E-Mails. Erkennt proGOV hierbei neue Zertifikate (öffentliche Schlüssel), werden diese automatisch herausgelöst, in einem Verzeichnis gespeichert und können durch einen Administrator dem zentralen Zertifikatsspeicher hinzugefügt werden.

Prozess-Automatisierung

Der Schlüssel zu automatisierten Abläufen und medienbruchfreier Verarbeitung findet sich in der Tatsache, dass generell ein- oder ausgehende E-Mails das integrierte, hierarchisch aufgebaute Regelwerk durchlaufen. Dies ermöglicht weitere automatisierte Prozesse, die von regelbasierter Archivierung bis hin zur direkten Integration in Dritt-Anwendungen reichen.

Implementierung

Reibungslose Prozessabläufe sind ein entscheidender Erfolgsfaktor. Jedoch haben Organisationen individuelle Besonderheiten. Sinnvoll ist es, mögliche Differenzen zwischen standardisierten proGOV IST- und SOLL-Prozessen der Organisation zu ermitteln und direkt mit den daraus resultierenden technischen und infrastrukturellen Maßnahmen zu unterlegen. Bewährt hat sich hierfür ein Infrastrukturworkshop (remote oder vor Ort), der elementare Fragen, wie Portfreischaltungen (Internetzugriff, End-Anwender, Administration, internes Netz), den Umgang mit dem Fully-Qualified Host Name (FQHN - vollqualifizierter Name einer Domain oder numerische IP-Adresse) sowie Mailserver, Mail-Relay und gegebenenfalls Proxyserver abklärt. Auch die Art der zu verwendenden Zertifikate oder Formen der Archivierung müssen abgestimmt werden. Für die Dokumentation und Nachverfolgung ist es hilfreich, ein Übersichtsschema vor und nach der Installation anzufertigen. Damit entsteht für die Implementierung ein kompletter Umsetzungsplan, welcher sämtliche prozessseitigen, infrastrukturellen und technischen Aspekte enthält.

Empfohlene Systemvoraussetzungen:

(virtuelle oder physisch)

- Doppelkern-Prozessor
- Hauptspeicher: 16 GB
- verfügbarer Festplattenplatz: 100 GB
- Speicher Java Virtual Machine: mind. 8 GB
- ISO für Ubuntu 22.04 LTS 64 bit mit deutschem Sprachpaket

Kontakt

procilon GmbH
Leipziger Straße 110
04425 Taucha

+49 342 98 48 78-31
anfrage@procilon.de
www.procilon.de