

LAND OBERÖSTERREICH SETZT AUF E-MAIL-VERSCHLÜSSELUNG VON SEPPMAIL

Die E-Mail ist im Verwaltungsalltag in Organisationen und Behörden das wichtigste Kommunikationsmittel. Trotzdem wird die E-Mail-Kommunikation oftmals nicht ausreichend geschützt. So gehören laut einer Proofpoint-Studie E-Mails zu den beliebtesten Einfallstoren für Cyberattacken. Hacker nutzen Sicherheitslücken aus, um mit gezielten Angriffen persönliche Daten auszuspähen.

Bei einer unverschlüsselten E-Mail kann sich der Absender nie sicher sein, ob seine Nachricht auch wirklich beim Empfänger ankommt. Denn Cyberkriminelle fangen E-Mails ab, lesen diese mit und manipulieren die Nachricht sogar, indem sie den Inhalt gänzlich verändern. Gesetzliche Anforderungen wie die Europäische Datenschutz-Grundverordnung (EU-DSGVO) sehen die Verschlüsselung von vertraulichen Daten vor. Das Versenden von unverschlüsselten E-Mails mit vertraulichem Inhalt wie besonderen Kategorien von personenbezogenen Daten ist somit nicht zulässig. Dies war u.a. ein Grund, dass das Land Oberösterreich eine neue E-Mail-Verschlüsselungslösung eingeführt hat.

Das Land Oberösterreich geht als öffentliche Verwaltung sorgsam mit vertraulichen Daten um. Es stehen die Punkte Gesetzmäßigkeit, Bürgerfreundlichkeit, Umweltbewusstsein, Wirtschaftlichkeit und Subsidiarität im Mittelpunkt aller Mitarbeiter. Um eine gute Verwaltung zu ermöglichen, muss ein optimaler, sicherer Austausch von wichtigen Daten und Informationen innerhalb der Organisation sowie mit Unternehmen, anderen öffentlichen Stellen und Bürgern stetig gewährleistet sein. Denn ein gutes Vertrauensverhältnis zu den Bürgern ist wichtig, um einen reibungslosen Verwaltungsbetrieb aufrechtzuerhalten.

Ersatz gesucht

Beim Land Oberösterreich war bereits eine Verschlüsselungslösung im Einsatz. Alle Mitarbeiter konnten mittels eines elektronischen Dienstausweises E-Mails verschlüsselt senden und empfangen. Dieses Verfahren brachte jedoch einige Nachteile mit sich. Bei Verlust des elektronischen Dienstausweises waren alle verschlüsselten Nachrichten in der Mailbox unlesbar, es sei denn, sie wurden im Vorfeld zusätzlich unverschlüsselt abgelegt. Des Weiteren bereiteten verschlüsselte E-Mails im Postfach Probleme bei der elektronischen Weiterverwendung. Auch war die Verschlüsselung für Rollenpostfächer nicht möglich, und Vertretungen konnten gar nicht berücksichtigt werden. Zudem musste der Kommunikationspartner über ein Zertifikat verfügen, was aber oftmals nicht der Fall war.

„Aus diesem Grund machten wir uns auf die Suche nach einer neuen Verschlüsselungslösung, die neben dem Versand und Empfang von E-Mails mit gewohnter Anwendung auch die verschlüsselte E-Mail-Kommunikation mit beliebigen Empfängern ermöglicht; selbst wenn diese über kein eigenes Schlüsselmaterial verfügen“, sagt Dipl.-Ing. Roland Krenner, Leiter der Abteilung Informationstechnologie beim Land Oberösterreich. Die Lösung sollte dabei alle gängigen Verschlüsselungsmethoden wie PGP und S/MIME unterstützen.

Evaluierungsphase für eine ganzheitliche Lösung

In der Evaluierungsphase führte das Land Oberösterreich eine Marktanalyse von Verschlüsselungsgateways durch. In diesem Zuge wurde das Projektteam der Abteilung Informationstechnologie des Landes Oberösterreich auf den Verschlüsselungsexperten SEPPmail aufmerksam. Bei einem Besuch der it-sa in Nürnberg informierten sich die Verantwortlichen über die Lösungen des Herstellers. Dabei überzeugten eine ausführliche Präsentation und insbesondere die Lösung im Bereich Secure Messaging. Aufgrund des Alleinstellungsmerkmals der GINA-Technologie zur Unterstützung von Benutzern ohne Secure Mail-Infrastruktur sowie der Abdeckung aller anderen Anforderungspunkte fiel die Entscheidung schließlich auf die Verschlüsselungslösung „Secure E-Mail Gateway“ von SEPPmail.

Implementierung im laufenden Betrieb

Beim Land Oberösterreich ist die E-Mail-Infrastruktur zwischen Empfang, Routing, Versand und Mailstore getrennt; die Integration der SEPPmail-Appliances in den Mailstrom stellte somit kein Problem dar. Zusätzlich existierte bereits ein Lightweight Directory Access Protocol (LDAP)-Verzeichnis, das sämtliche Informationen über beim Land Oberösterreich



existierende E-Mail-Adressen beinhaltet. Der SEPPmail-Outlook-Client nutzt dieses Verzeichnis, um diejenigen E-Mail-Adressen zu ermitteln, die für die Verschlüsselung berechtigt sind. So ist ein Rollout der Verschlüsselung unabhängig von den im E-Mail-Client eingebundenen E-Mail-Adressen, wie die persönliche E-Mail-Adresse bzw. Rollenpostfächer, möglich. Die Abteilung Informationstechnologie des Landes Oberösterreich führte die Implementierung der SEPPmail-Lösung innerhalb von zwei Tagen durch. Bereits am ersten Tag konnten die ersten verschlüsselten E-Mails mittels S/MIME und Domain-Verschlüsselung versendet werden. Das Anbinden der insgesamt 8.000 Accounts der offiziellen Postfächer des Landes sowie der persönlichen Postfächer der Mitarbeiter erfolgte sukzessive und ist inzwischen abgeschlossen.

E-Mail-Verschlüsselung im Arbeitsalltag

Die neue Appliance prüft bei jedem E-Mail-Versand, ob eine Domain-Verschlüsselung möglich ist. Bei verschlüsselten E-Mails wird geprüft, ob eigenes Schlüsselmaterial des Empfängers wie S/MIME oder OpenPGP erfasst ist. Ist dies nicht der Fall, kommt bei verschlüsselten E-Mails die GINA-Technologie zum Einsatz. GINA verschlüsselt die Nachricht und versendet sie als html-Anhang mit einer Träger-E-Mail. Somit ist die E-Mail ausgeliefert und liegt vollständig auf dem Empfängersystem vor. Die Lösung erstellt ein Initialpasswort, das der Absender dem Empfänger über einen zweiten Übertragungsweg, z.B. per SMS oder Telefon, mitteilt. Damit kann der Empfänger die Nachricht samt Anhängen unabhängig vom genutzten E-Mail-Client auf jedem internet-fähigen Gerät öffnen.

„Die SEPPmail-Appliance wählt bei jedem E-Mail-Versand automatisch die jeweils beste Verschlüsselungsmethode aus“, sagt

Dipl.-Ing. Krenner. „Zudem kann der Empfänger im GINA-Webportal auch sofort verschlüsselt antworten – auch wenn er selbst keine Verschlüsselungslösung einsetzt. Für die alltägliche E-Mail-Kommunikation ist dies ein absoluter Mehrwert.“ Die Lösung lässt sich zudem mit Blick auf die verschärfte Gesetzgebung wie z.B. die DSGVO flexibel skalieren.

Skalierung problemlos möglich

Bei Problemen oder Schwierigkeiten bezüglich der E-Mail-Kommunikation steht der SEPPmail-Support via Ticketsystem per E-Mail oder Telefon zur Verfügung. „Unsere Erfahrungen mit dem Support sind allesamt positiv“, erklärt Dipl.-Ing. Krenner. „Der Hersteller reagierte stets professionell. Unsere Anforderungen wurden rasch behandelt. So wurde auf unseren Wunsch hin das SEPPmail-Outlook-Plugin kostenpflichtig erweitert.“ Die SEPPmail-Lösung wurde auch von den Mitarbeitern des Landes Oberösterreich sehr gut aufgenommen.

„Obwohl die gesamte Materie der E-Mail-Verschlüsselung äußerst komplex ist, ist die Anwendung in der Praxis einfach und technisch absolut unauffällig, da es lediglich einen zusätzlichen Button in Outlook gibt“, sagt Dipl.-Ing. Krenner. Nur wenige der externen GINA-User benötigten neben der grundlegenden Einführung noch weitere Einweisungen durch die Verantwortlichen.

Das Land Oberösterreich passt die Lizenzen dem Wachstum entsprechend an. Die Hardware ist ausreichend dimensioniert; falls eine weitere Appliance notwendig wird, ist dies dank des modularen Aufbaus des E-Mail-Systems problemlos möglich. „Da auch bei unseren externen Kommunikationspartnern S/MIME, PGP und Domain-Verschlüsselung immer mehr Verbreitung finden, wird in Zukunft ein großer Teil des E-Mail-Verkehrs auch ohne expliziten Wunsch des Users automatisch verschlüsselt“, so Dipl.-Ing. Krenner.

FAZIT

Heute können beim Land Oberösterreich mehr als 8.000 Personen mit dem Secure E-Mail Gateway von SEPPmail verschlüsselt kommunizieren. Die Implementierung erfolgte im laufenden Verwaltungsbetrieb. Die SEPPmail-Appliance löst die vorhandene Verschlüsselungslösung auf Basis eines elektronischen Dienstausses ab. Jetzt ist sogar die sichere E-Mail-Kommunikation mit Dritten möglich, die selbst nicht verschlüsseln. In der Praxis hat sich die Lösung schnell bewährt, da das Versenden und Empfangen von verschlüsselten E-Mails einfacher denn je ist.

Die Lösung sorgt für umfassende Sicherheit bei der E-Mail-Kommunikation und wählt dabei automatisch die geeignetste Verschlüsselungsmethode aus. Der Schutz von personenbezogenen Daten der Bürger und Mitarbeiter ist somit gegeben. Zudem hilft die Lösung bei der Einhaltung gesetzlicher Vorgaben wie der DSGVO.