Sichere E-Mail-Kommunikation im E-Government

Bei der Kommunikation von Behörden mit Bürgern, anderen Amtsstellen und Partnern aus den verschiedensten Bereichen ist ein sicherer Datenaustausch unabdingbar. Dies vor dem Hintergrund, dass besonders schützenswerte Personendaten vorhanden sind und versendet werden.

Den Beitrag finden Sie auch online
www.netzwoche.ch

Ein wirksamer Schutz der E-Mail-Kommunikation ist für die öffentliche Hand ein Muss. Dies gilt umso mehr, als Cyberangriffe wie Phishing und Datendiebstahl rasant zunehmen. Jüngst zeigte eine Cyberattacke auf die Waadtländer Gemeinde Rolle überdeutlich, welche Folgen solche Vorgänge nicht nur für die Wirtschaft, sondern auch für die öffentliche Hand haben können. Dazu kommt, dass allgemein anerkannte aktuelle Datenschutzstandards sowie gesetzliche Vorgaben immer höhere Anforderungen an den Umgang mit schützenswerten Daten stellen.

E-Mail ist nach wie vor das gebräuchlichste Kommunikationsmittel im Alltag der meisten Behörden. Im Laufe der Zeit sind die unterschiedlichsten technischen Lösungen auf den Markt gekommen, um den E-Mail-Verkehr abzusichern – Verschlüsselung garantiert die Integrität der Inhalte, und mittels elektronischer Signatur wird die Authentizität des Absenders gewährleistet. Dadurch wird die E-Mail-Kommunikation vertrauenswürdig und sicher. Manche Lösungen sind jedoch schwierig zu bedienen und erfordern aufwändige manuelle Arbeitsschritte.

Die ideale E-Mail-Security ist einfach zu bedienen

Dies muss nicht so sein. Drei Schweizer Anbieter für sichere E-Mail-Kommunikation machen es möglich: Die Schweizerische Post (Incamail), Health Info Net (HIN) und Seppmail haben sich zusammengetan und bieten die einheitliche, hochverfügbare Gesamtlösung Swiss Mail Security an, die automatisierte E-Mail-Verschlüsselung und Signierung ermöglicht. Unkompliziert, unabhängig von der technischen Lösung des Kommunikationspartners und in höchster Schweizer Qualität.

Sichere E-Mail-Kommunikation auf Schweizer Art funktioniert wie folgt: Alle E-Mails werden automatisch verschlüsselt und beim Empfänger wieder entschlüsselt. Zwischen Anwendern von Seppmail-Systemen, Incamail und dem im Gesundheitswesen etablierten HIN-Netzwerk ist der E-Mail-Verkehr somit vollautomatisch abgesichert. Die Benutzer und die Schlüssel werden zentral verwaltet und müssen nicht manuell erfasst und aktualisiert werden. Die Lösung arbeitet mit weltweit anerkannten Standards wie OpenPGP, S/MIME und TLS. Wer mit Partnern kommuniziert, die nicht über eine eigene Verschlüsselungslösung verfügen, profitiert von einer patentierten Push-Technologie namens GINA. Diese ermöglicht den Versand verschlüsselter E-Mails an beliebige Empfänger. So ist die gesamte E-Mail-Kommunikation gegen Spam, Phishing-Attacken und Viren geschützt.

Der Autor
Philipp Bachmann, COO und Sales & Channel Manager, Seppmail
bachmann@seppmail.ch

Beim Versand und beim Empfang der E-Mails ändert sich für die Nutzer nichts – Verschlüsselung und Signierung gehen völlig transparent über die Bühne, und man kann die gewohnte E-Mail-Software nutzen, etwa Outlook. Auch die Installation und das Einspielen von Updates sind unkompliziert. Darüber hinaus ermöglicht ein programmierbares Regelwerk die Anpassung an organisationsspezifische Sicherheitsrichtlinien.

Swiss Mail Security lässt sich breits einsetzen

Rund 250 000 Privatpersonen in der Schweiz nehmen bereits am Netzwerk teil und können die automatisch verschlüsselten E-Mails transparent empfangen. Dank der patentierten Push-Technologie GINA sind auch alle anderen Bürger verschlüsselt erreichbar. Und auch über 2100 Schweizer Unternehmen sind mit an Bord und profitieren von automatisch verschlüsseltem und signiertem Datenaustausch – ideal für die Kommunikation mit Steuerbehörden und Wirtschaftsämtern.

Die Lösung ist zudem als sichere Zustellplattform gemäss VeÜ-ZSSV akkreditiert. Dies ermöglicht etwa Anwälten die gesetzeskonforme Entgegennahme von Gerichtseingaben oder den Versand von Gerichtsentscheiden.

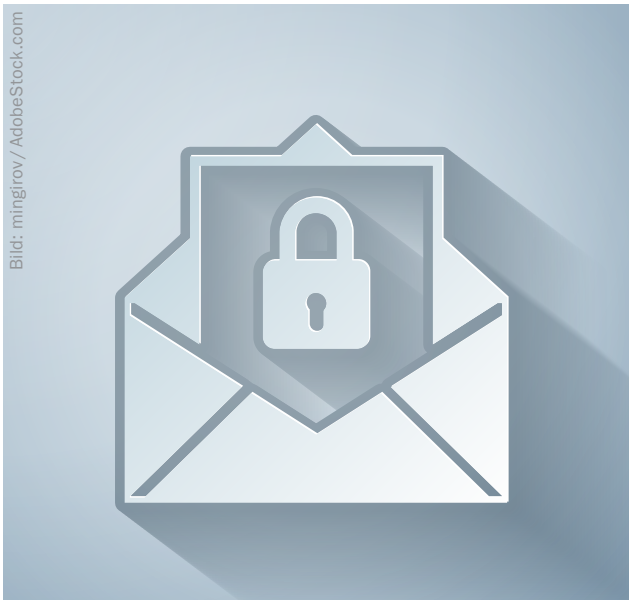

Bild: mingirov / AdobeStock.com