10 Jahre sichere E-Mail

VOM VORREITER ZUM STANDARD

ober österreich

Zur Person

Vorstellung

Ing. Joachim Minichshofer

Land Oberösterreich
Abteilung Informationstechnologie
Leiter Referat "Security & Linux"

Aufgabenbereich (u.a.):
Technische und organisatorische Sicherheit

Ausgangssituation

E-Mailverschlüsselung beim Land OÖ vor SEPPmail-Rollout

Jede/r Mitarbeiter/in des Landes OÖ kann seit Einführung des elektronischen Dienstausweises (eDA) E-Mails verschlüsseln.

Diese Vorgangsweise hat jedoch einige **Nachteile**:

- Bei Verlust des eDAs sind alle verschlüsselten E-Mails in der Mailbox unlesbar. (Verlust der Daten)
- Für offizielle Postfächer ist die Verschlüsselung nicht möglich.
- Vertretungen sind hier nicht vorgesehen.
- Das Gegenüber muss ein Zertifikat haben. Dies ist vielfach nicht der Fall.

E-Mailverschlüsselung war zu diesem Zeitpunkt zwar möglich, aber nicht verbreitet im Einsatz.

Regulierung führte zu Innovation

Regulierung führte zu Innovation

Anforderung aus Kinder- und Jugendhilfe

Im Jahr 2014 kam es zu einer Änderung im Oö. Kinder- und Jugendhilfe-gesetz und damit zu einer Anforderung für E-Mail-Verschlüsselung aus diesem Bereich:

"§15 (8) Die Bezirksverwaltungsbehörden und die Landesregierung haben Datensicherheitsmaßnahmen zu treffen. Jedenfalls sind alle Datenverwendungen zu protokollieren. **Sensible Daten dürfen nur verschlüsselt übermittelt werden.**"

Oö. Kinder- und Jugendhilfegesetz 2014 - Oö. KJHG 2014

Diese Änderung im Oö. Kinder- und Jugendhilfegesetz führte dazu, dass das Land Oberösterreich nach einer E-Mail-Verschlüsselungslösung suchte, welche die vorher angeführten Nachteile der bereits im Einsatz befindlichen Lösung aufhob und breit eingesetzt werden konnte.

Regulierung führte zu Innovation

Weitere rechtliche Anforderungen

Neben dem Oö. Kinder- und Jugendhilfegesetz sehen wir weitere für uns wichtige Richtlinien und Normen, welche E-Mail-Verschlüsselung fordern oder Nahe legen:

- DSGVO spricht bei der Sicherheit der Verarbeitung "unter Berücksichtigung des Stands der Technik" von Verschlüsselung (Artikel 32) und unter "Verarbeitung" wird auch die "Offenlegung durch Übermittlung" verstanden
- Die Handreichung zum "Stand der Technik" (Teletrust, 2023) beschäftigt sich im Punkt "3.2.7" mit der Verschlüsselung von E-Mails.
- ISO 27001:2022
- NIS2-Richtlinie

E-Mail verschlüsseln

Vorgaben für Benutzer:innen

In den landesinternen Richtlinien für Informationssicherheit ist definiert:

Jedenfalls streng vertrauliche Inhalte dürfen Sie per E-Mail nur verschlüsselt versenden. Beachten Sie dazu das Merkblatt „E-Mail-Verschlüsselung“.

Beispiele:

Gesundheitsdaten, „strafrechtsbezogene Daten“, Verschlusssachen

Im Merkblatt ist die E-Mail-Verschlüsselung (Ende-zu-Ende) beschrieben und darüber hinaus – der Vollständigkeit halber - auch noch alternative Übertragungswege (wie elektronische Zustellung).

Vorgangsweise seitens Benutzer:innen

Um sicherzugehen, dass nur Sender und Empfänger die E-Mail lesen können, muss diese verschlüsselt werden. Hierfür ist seitens der Benutzer:in der Outlook-Button „Verschlüsseln“ zu betätigen.

Das Mail wird dann verschlüsselt übermittelt. Dies übernimmt der SEPPmail Secure Mailgateway.

Nur im Fall von E-Mails an neue Empfänger, die keine Verschlüsselungssoftware einsetzen und keinen Schlüssel besitzen, kommt noch etwas auf den Absender der E-Mail zu. Dazu später mehr...

Empfang von verschlüsselten E-Mails

Die Entschlüsselung von E-Mails übernimmt ebenfalls der SEPPmail Secure Mailgateway.

Beim Empfänger kommt die E-Mail immer unverschlüsselt an. Ein Kennzeichen im Betreff zeigt beim Land OÖ dem Benutzer an, dass es sich um eine verschlüsselte E-Mail handelt.

Die E-Mail kann ohne Probleme weiterverarbeitet werden (z.B. als Eingangsstück im elektronischen Akt).

Domain-Verschlüsselung

Domain-Verschlüsselung

Bei der Domain-Verschlüsselung (Ende zu Ende) handelt es sich um eine Verschlüsselung zwischen zwei SEPPmail Securemail-Gateways.

So wird der gesamte E-Mail-Verkehr zwischen zwei Organisationen ohne Zutun im Vergleich zu TLS gesichert.

Derzeit existieren bereits über 13.000 E-Mail-Domänen (.at: 1676, .de: 4999,.ch: 3002, .com: 1529, ...) , bei denen diese Art der Verschlüsselung wirksam wird.

Beim Land Oberösterreich haben wir in den letzten 3 Monaten mit 851 Domänen domain-verschlüsselte E-Mails benutzt.

GINA

GINA

Versand an neue Empfänger

Dank dem sogenannten GINA-Verfahren ist es möglich, E-Mails verschlüsselt an Empfänger zu übermitteln, die keine Verschlüsselungssoftware einsetzen und keinen Schlüssel besitzen.

Das GINA-Verfahren benötigt keine Softwareinstallation – weder beim Sender noch beim Empfänger.

Die E-Mails können im gewohnten E-Mail-Programm empfangen werden und werden durch Eingabe eines Passworts entschlüsselt.

Sollte ein Empfänger noch nie verschlüsselte E-Mails vom Land OÖ erhalten haben und ist auch keine Domainverschlüsselung möglich, muss der Sender das Passwort dem Empfänger (auf einem anderen Weg) übermitteln.

Versand an neue Empfänger

Der Vorteil des Versands von verschlüsselten E-Mails unabhängig, ob das Secure-Mail-Gateway bereits ein SMIME-Zertifikat für den Empfänger gesammelt hat, überwiegt bei weitem den Aufwand einer einmaligen Mitteilung des Initial-Kennworts.

GINA

GINA

Erfahrungen mit GINA-Empfänger

- Bürger oder kleine Organisation (wie Vereine) nehmen es einfach hin, dass sie vertrauliche Informationen über diesen Weg nun erhalten.
- Hier wird auch der Rückkanal, welchen der Secure Mail Gateway bietet genutzt um sicher zuzustellen.
- Größere Organisationen mit den häufig verschlüsselte E-Mails ausgetauscht werden, melden sich mit der Frage nach Alternative.
- Hier können wir sie nur an ihre eigenen Mail-Verantwortlichen verweisen. GINA kommt ja nur dann zur Anwendung, wenn keine andere Verschlüsselungsmöglichkeit bekannt ist.
- Der Empfänger hat auch die Möglichkeit nachträglich SMIME-Zertifikate über das Secure Mail Gateway einzuspielen. Ein signiertes Mail würde auch reichen.
- Beim Land OÖ haben wir auf unserer Homepage einen Bereich zum Thema E-Mailverschlüsselung geschaffen, wo alle notwendigen Informationen bereitgestellt werden.

Resüme

Resüme

- Der Betrieb der SEPPmail Appliances funktioniert "unauffällig" mit minimalem Personaleinsatz.
- SEPPmail basiert auf anerkannten Technologien (wie S/MIME) und ist im E-Mail-Strom eingebunden
- Herstellerunabhängigkeit wegen Standard (Wechsel mit auf anderes Produkt möglich)
- Compliance mit Regulatorien gegeben

Noch Fragen?