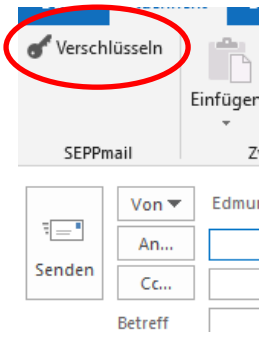
E-Mail Verschlüsselung

Bildungsdirektion Oberösterreich

E-Mails, die über das Internet versandt werden, können grundsätzlich an jedem Knotenpunkt gelesen bzw. auch verändert werden. Daher sind E-Mails mit streng vertraulichem Inhalt zu verschlüsseln.
Solche Inhalte dürfen nur per Post, duale Zustellung / Elektronischem Rechtsverkehr, Boten oder verschlüsseltem E-Mail übermittelt werden.

Verschlüsselte Übertragung von streng vertraulichen/personenbezogenen Inhalten

Um sicherzugehen, dass nur Sender und Empfänger die E-Mail lesen können, muss diese verschlüsselt werden. Zu beachten ist, dass der Betreff und andere Metadaten (To, From,...) auch bei einem verschlüsselten E-Mail im Klartext vorhanden sind. Daher beim Betreff auf unverfängliche Formulierungen achten und keine sensiblen Daten erwähnen.



Sollen streng vertrauliche Inhalte per E-Mail übermittelt werden, dann aktivieren Sie auf jeden Fall den Outlook-Button „Verschlüsseln".

Kann das E-Mail verschlüsselt zugestellt werden, besteht kein weiterer Handlungsbedarf.

Ist für diesen Empfänger noch keine E-Mail-Verschlüsselung möglich, so erhalten Sie per E-Mail ein Kennwort. Das Kennwort teilen Sie dem Empfänger auf einem anderen Weg (z.B. telefonisch, SMS) mit.

Nur so sind Sie sicher, dass der streng vertrauliche Inhalt/personenbezogene Daten auf jeden Fall verschlüsselt übermittelt werden.

Hintergrund-Wissen

Verschlüsselungsverfahren
Für das Verschlüsseln von E-Mails gibt es mehrere Methoden, verwendet wird allerdings fast ausschließlich das Private-Public-Key Verfahren. Zum Verschlüsseln und Entschlüsseln werden dabei verschiedene Schlüssel (Keys) verwendet.
Der zum Verschlüsseln dienende öffentliche Schlüssel (Public Key) kann über beliebige unsichere Kanäle übermittelt werden (Datenträger, E-Mail, Internet etc.).
Zum Entschlüsseln, also Lesen einer Nachricht wird der private Schlüssel (Private Key) verwendet. Dieser verbleibt beim Besitzer und wird niemals an andere übermittelt.

Vorgang bei der Verschlüsselung
Um verschlüsselte E-Mails austauschen zu können, muss jeder Kommunikationspartner ein Schlüsselpaar bestehend aus einem geheimen und einem öffentlichen Schlüssel besitzen. Während der geheime Schlüssel sorgfältig geschützt nur dem Anwender selbst zur Verfügung stehen sollte, ist der öffentliche Schlüssel an alle Kommunikationspartner zu verteilen.

Wenn „Anton" eine verschlüsselte E-Mail an „Beatrice" senden will, nimmt er den öffentlichen Schlüssel von „Beatrice". „Beatrice" kann mit ihrem privaten Schlüssel, den nur sie besitzt, die Nachricht entschlüsseln.

Ebenso im umgekehrten Fall. Wenn „Beatrice" eine verschlüsselte Nachricht an „Anton" senden will, nutzt sie den öffentlichen Schlüssel von „Anton", um die Nachricht zu chiffrieren. Nur „Anton" kann diese E-Mail mit seinem geheimen Schlüssel dechiffrieren und lesen.

Schlüsselgenerierung

Für das Private-Public-Key Verfahren gibt es verschiedene Implementierungen wie PGP (Pretty Good Privacy) oder GNU-PG (GNU Privacy Guard). Beide verwenden dazu X509-Zertifikate. Aber auch diverse E-Mail Clients (wie z.B. Microsoft Outlook) können mit Hilfe eines X509-Zertifikats E-Mails verschlüsseln. Während PGP und GNU-PGP, bei welchen die Schlüssel vom Benutzer generiert werden, vor allem im privaten Bereich verwendet werden, kommen im Unternehmensbereich vor allem X509-Zertifikate zum Einsatz, die von einer CA (Certificate Authority) ausgestellt wurden. Die Partner, mit denen der verschlüsselte E-Mailverkehr durchgeführt werden soll, müssen sich ebenfalls ein geeignetes Zertifikat bei einem Trust-Center ausstellen lassen (z.B. a-trust Verisign, etc.). Die Zertifikate sind im Allgemeinen kostenpflichtig, es gibt jedoch einige Zertifizierungsdiensteanbieter, die diesen Dienst kostenlos anbieten.