Verschlüsselung von Emails

Grundlagen:

Unterschied Signatur und Verschlüsselung:

- Die Signatur dient dem Nachweis, dass die Nachricht auf dem Weg zum Empfänger nicht manipuliert wurde. Allerdings ist eine signierte Mail nicht verschlüsselt, d.h. die Nachricht wird nach wie vor im Klartext versendet
- Beim Einsatz der Email-Verschlüsselung wird sichergestellt, dass nur der Absender und der Empfänger Zugang zu den Inhalten der verschlüsselten Nachricht haben.
- Beide Verfahren können kombiniert eingesetzt werden
- Beim hier verwendeten Verfahren gibt es zwei Komponenten, einen sogenannten privaten Schlüssel und einen öffentlichen Schlüssel.
- Darum ist zu beachten, dass beim Einsatz der Verschlüsselung jeder Teilnehmer die Voraussetzungen für den Einsatz zu schaffen hat, d.h. sowohl **Sender** als auch **Empfänger** benötigen ein entsprechendes Zertifikat.
- Hat Ihr Unternehmen ein Zertifikat, der Korrespondenzpartner aber nicht, funktionieren nur folgende Wege:
  - Sie können eine verschlüsselte Mail vom Korrespondenzpartner empfangen, ihm aber keine senden
  - Sie können dem Korrespondenzpartner eine signierte Mail schicken, er aber keine an Sie

Wir können folgende Möglichkeiten der Implementierung anbieten:

Variante 1: Reddoxx und Gateway-Zertifikat:

- es wird ein sogenanntes Gateway-Zertifikat angeschafft, das auf der Appliance installiert wird
- Gateway-Ansatz beim Versand: Emails werden unverschlüsselt aus Outlook gesendet und liegen unverschlüsselt im Postausgang-Ordner; Emails werden dann erst auf dem Weg durch die Reddoxx verschlüsselt und zugestellt
- Gateway-Ansatz beim Empfang: Emails werden verschlüsselt durch Reddoxx empfangen, in der Reddoxx entschlüsselt, unverschlüsselt archiviert und unverschlüsselt an Mail-Server zugestellt; liegen somit auch unverschlüsselt im Posteingang

Variante 2: Reddoxx und per-User-Zertifikat

- Es wird ein Zertifikat für jede Email-Adresse bzw. jeden Benutzer erworben, der Email-Signatur und Verschlüsselung benutzen möchte; all diese Zertifikate werden auf der Appliance installiert
- Die Vorteile des Gateway-Ansatzes beim Versand und Empfang gelten genauso wie beim Einsatz eines Gateway-Zertifikats

Variante 3: lokaler Einsatz und per-User-Zertifikate

- Es wird ein Zertifikat für jede Email-Adresse bzw. jeden Benutzer erworben, der Email-Signatur und Verschlüsselung benutzen möchte; die Zertifikate werden nicht in der Appliance hinterlegt, sondern im lokalen Outlook
- Der Gateway-Gedanke findet keine Anwendung. Nachteile:
  1. die Emails werden lokal signiert, verschlüsselt oder entschlüsselt.
  2. Im Posteingang/Postausgang liegen die verschlüsselten Nachrichten und müssen bei jedem Öffnen wieder entschlüsselt werden
  3. Es kann zu Problemen beim Postfachzugriff von Dritten (Sekretariat) kommen
  4. Mobile Geräte können die Nachrichten u.U. nicht entschlüsseln

Gateway- oder per-User-Zertifikat beim Einsatz einer Appliance?

Gateway- oder Personenzertifikate werden immer für eine konkrete E-Mail Adresse ausgestellt. Eigentlich benötigt somit jeder Anwender sein eigenes persönliches Zertifikat.
Eine Besonderheit stellen Gateway-Zertifikate bzw. Domain-Zertifikate dar, die z.B. auf die Adresse gateway@vte-teichmann.de ausgestellt werden. Diese Gateway-Zertifikate können für die Signatur aller E-Mails einer E-Mail Domäne (z.B. vte-teichmann.de) verwendet werden. Obwohl der Einsatz von Gateway-Zertifikaten international standardisiert ist, können einige E-Mail Clients diese nicht richtig verarbeiten (z.B. Webmailer) und erklären die damit erstellten Signaturen für ungültig. Manche E-Mail Clients können auf Basis von Gateway-Zertifikaten auch nicht verschlüsseln. Beispielsweise melden Outlook Express und Windows Live Mail Signaturen auf Basis eines Gateway-Zertifikates als ungültig. Microsoft Outlook stellt die Signatur als gültig dar, kann auf Basis eines Gateway-Zertifikates aber dennoch nicht verschlüsseln. Beim Einsatz einer Reddoxx-Appliance ist dies allerdings möglich.

Stand 15.6.2016