Entscheidungshilfe zur Wahl eines Verschlüsselungsverfahrens mit dm

Weitere Informationen zur E-Mail-Verschlüsselung bei dm finden Sie unter <https://www.dm.at/e-mail-signatur-456882>

Verfahren	Prinzip	Vorteile	Voraussetzungen
S/MIME (von dm bevorzugt)	<p>E-Mails werden auf Basis des Industriestandards S/MIME verschlüsselt.</p> <p>dm benötigt dazu für die beteiligten E-Mail-Adressen des Partnerunternehmens jeweils ein S/MIME-Zertifikat. Der Versand von E-Mails an diese Adressen wird anschließend automatisch verschlüsselt.</p> <p>dm sendet mit jeder E-Mail das dazugehörige S/MIME-Zertifikat in Form einer digitalen Signatur mit, hiermit können E-Mails an den dm-Empfänger verschlüsselt zurückgesendet werden.</p>	<p>S/MIME ist bei der E-Mail-Verschlüsselung im Unternehmensumfeld am weitesten verbreitet und wird von nahezu allen gängigen E-Mail-Programmen (zB Microsoft Outlook, Mozilla Thunderbird, Lotus Notes, Apple Mail) ohne weitere Zusatzsoftware und Kosten unterstützt.</p> <p>S/MIME-Zertifikate können entweder von kommerziellen Zertifizierungsstellen beschafft oder kostenfrei selbst ausgestellt werden.</p>	<p>Die Anwender müssen daran denken bei schützenswerten E-Mails vor dem Versand die Verschlüsselung zu aktivieren.</p> <p>Für jedes an der Kommunikation beteiligte Postfach muss ein S/MIME-Zertifikat bestellt oder erzeugt werden und lokal im E-Mail-Programm des Anwenders eingerichtet werden. Beim Wechsel von Ansprechpartnern oder Änderung von E-Mail-Adressen muss der Prozess wiederholt werden, wodurch sich ohne Automatisierung ein dauerhafter Pflegeaufwand ergibt.</p> <p>Wenn parallel mit einem Smartphone oder Tablet auf das E-Mail-Postfach zugegriffen werden soll, muss S/MIME auf diesen Geräten ebenfalls eingerichtet werden, um die verschlüsselten E-Mails auch dort lesen zu können.</p>
PGP	<p>E-Mails werden einzeln auf Basis des Internetstandards PGP verschlüsselt.</p> <p>Analog zu S/MIME müssen dm für die an der Kommunikation beteiligten E-Mail-Adressen des Partnerunternehmens PGP-Schlüssel zur Verfügung gestellt werden. Im Gegenzug erhält der Partner PGP-Schlüssel für dm-E-Mail-Adressen.</p>	<p>PGP-Schlüssel können kostenlos selbst erstellt werden. Das Verfahren ist kompatibel zu OpenPGP, Autocrypt und pEp.</p>	<p>In der Regel muss zusätzliche Software zur Unterstützung von PGP installiert werden wie zB Enigmail oder Gpg4win.</p> <p>Die obigen Voraussetzungen des Verfahrens S/MIME gelten gleichermaßen für die Nutzung von PGP.</p>

<p>S/MIME mit Domain-Zertifikaten oder PGP mit Domain-Schlüsseln</p> <p>(von dm bevorzugt)</p>	<p>Das Prinzip ist analog zu S/MIME und PGP, allerdings wird nur ein Zertifikat bzw Schlüssel verwendet, welches für die Verschlüsselung aller E-Mail-Adressen einer Domain genutzt wird. Dieses Verfahren wird hauptsächlich auf E-Mail-Verschlüsselung-Gateways eingesetzt.</p>	<p>Mit einem S/MIME-Domain-Zertifikat oder PGP-Domain-Schlüssel können E-Mails an alle E-Mail-Adressen einer Domain verschlüsselt werden (zB an *@dm.de). Der Wechsel von Ansprechpartnern oder die Änderung von E-Mail-Adressen lösen daher keinen zusätzlichen Aufwand aus. Soweit eine Gateway-Lösung verwendet wird, entsteht für die Anwender kein weiterer Aufwand, die Verschlüsselung erfolgt transparent durch das Gateway.</p>	<p>Es wird eine Gateway-Lösung zur Verschlüsselung von E-Mails benötigt, da E-Mail-Programme in der Regel keine domainweiten Zertifikate akzeptieren. Soweit solch ein Gateway noch nicht vorhanden ist, entstehen bei der Anschaffung Einrichtungsaufwände und Lizenzkosten.</p>
<p>TLS-Transportverschlüsselung</p>	<p>Zwischen den E-Mail-Gateways des Partnerunternehmens und dm wird eine verschlüsselte Verbindung aufgebaut, über welche dann die E-Mails gesichert übertragen werden.</p>	<p>Die Verschlüsselung muss nur einmalig eingerichtet werden und umfasst automatisch alle zwischen dem Partnerunternehmen und dm übertragenen E-Mails. Hierdurch kann die Verschlüsselung einer schützenswerten E-Mail auch nicht vergessen werden. Für die Anwender entsteht kein weiterer Aufwand, die Verschlüsselung erfolgt transparent durch die E-Mail-Gateways.</p>	<p>Da bei einer Transportverschlüsselung nur die Verbindung bis zum nächsten Server verschlüsselt wird wo die E-Mail wieder gelesen werden kann, muss dieser nächste Server exklusiv dem Partnerunternehmen zur Verfügung stehen. Dies schließt den Betrieb der E-Mail-Gateways durch Shared Hosting Provider bzw Hosted Email Security Services aus. Alle beteiligten E-Mail-Server müssen außerdem jederzeit über gültige Zertifikate einer allgemein anerkannten Zertifizierungsstelle verfügen.</p>
<p>Anhangbasierte Verschlüsselung</p>	<p>Die E-Mail wird als passwortgeschützter Anhang versendet, angehängt an eine Träger-E-Mail. Dieses Verfahren wird immer dann verwendet, wenn schützenswerte Daten per E-Mail übertragen werden sollen und kein anderes sicheres Verfahren zur Verfügung steht.</p>	<p>Es sind keinerlei besondere Software oder Kenntnisse notwendig um die verschlüsselte E-Mail zu öffnen.</p>	<p>Zum Öffnen der E-Mail muss jedes Mal ein persönlich festgelegtes Passwort eingegeben werden, die E-Mail kann anschließend jedoch auch im Klartext im eigenen E-Mail-Programm abgespeichert werden. Der Anwender muss über ein zuverlässiges Passwort-Management verfügen, da ohne Kenntnis des eigenen Passworts die entsprechend verschlüsselten E-Mails von dm nicht mehr gelesen werden können.</p>