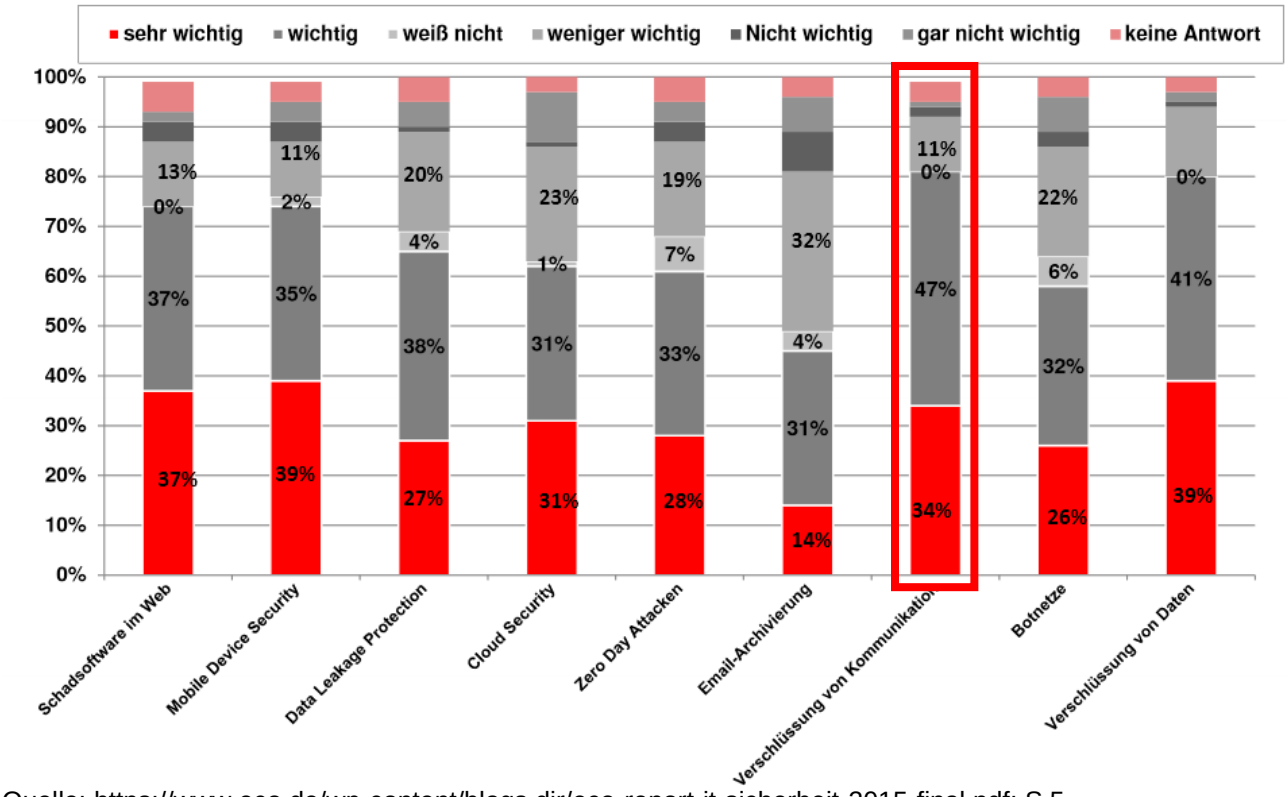
Wie funktioniert ein Verschlüsselungs-Gateway?

von Stefan Cink, Produkt Manager, Net at Work Netzwerksysteme GmbH

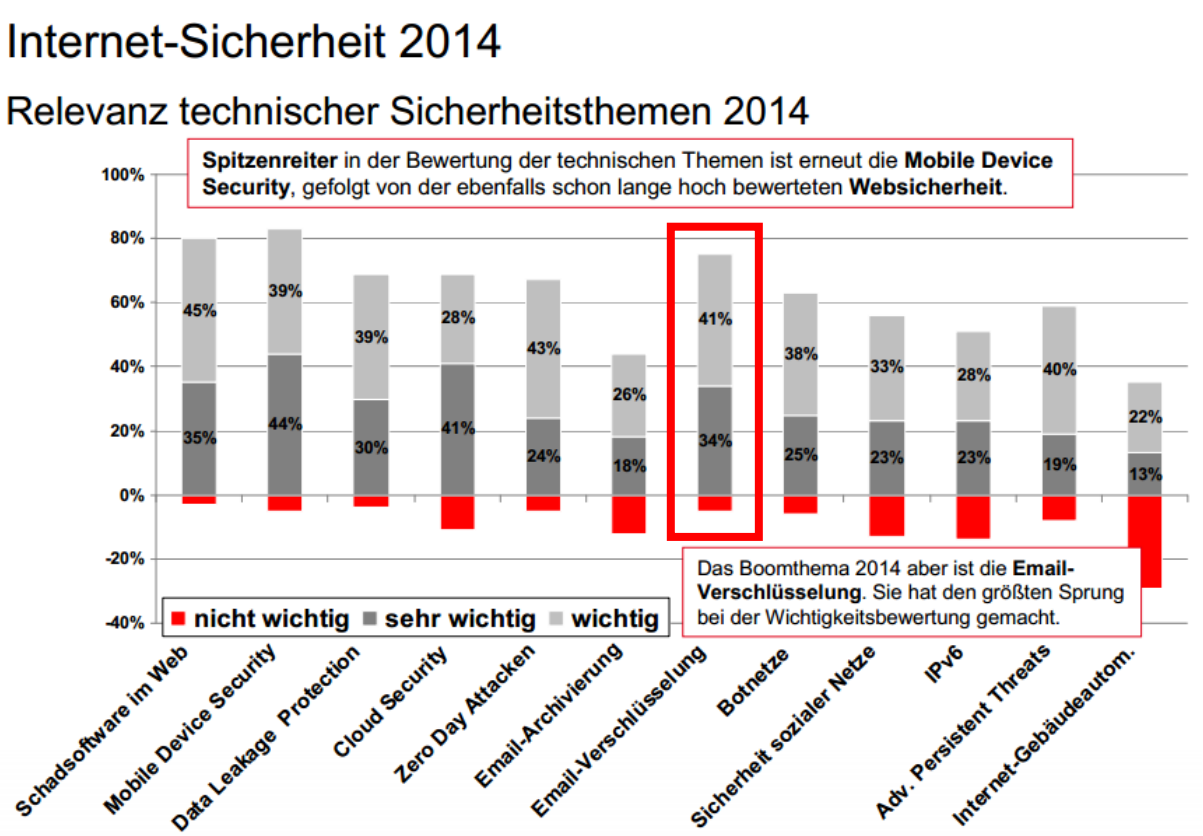
Das Thema "Verschlüsselung von Kommunikation" erfreut sich stark wachsender Beliebtheit. Der Verband der deutschen Internetwirtschaft e. V. (eco) ermittelte in seinem jährlich erscheinenden Report für Internet Sicherheit für das Jahr 2015, dass für 81% der Befragten dieses Thema für sie "wichtig" bis "sehr wichtig" ist. Im Report 2014 war die damit verbundene E-Mail-Verschlüsselung bereits ebenfalls Boomthema.

IT-Sicherheit 2015

Relevanz Sicherheitsthemen 2015



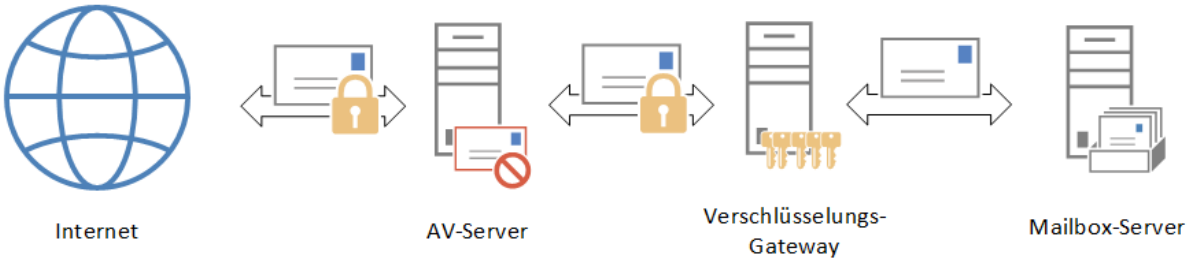
Quelle: https://www.eco.de/wp-content/blogs.dir/eco-report-it-sicherheit-2015-final.pdf; S.5 (Aufgerufen 01.04.2016).



Quelle: https://sicherheit.eco.de/wp-content/blogs.dir/27/files/report-internet-sicherheit-20142.pdf; S. 8 (Aufgerufen 11.02.2015).

In vielen Unternehmen kommen für die E-Mail-Verschlüsselung sogenannte Verschlüsselungs-Gateways zum Einsatz. Der Einsatz eines solchen Gateways erleichtert die Einführung der E-Mail-Verschlüsselung erheblich. Der wesentliche Unterschied zur clientbasierten Verschlüsselung ist zum einen die Verwaltung des Schlüsselmaterials, die nun ausschließlich auf dem Gateway erfolgt. Ein eigens abgesicherter Bereich in einer Datenbank hält sämtliches Schlüsselmaterial vor. Ebenfalls auf dem Gateway erfolgen sämtliche kryptografischen Operationen wie die Verschlüsselung, Entschlüsselung, Signatur und die Prüfung der Signatur. Der Endanwender braucht im Normalfall nicht mehr einzugreifen.

Üblicherweise arbeiten Verschlüsselungs-Gateways als SMTP Host und werden in die vorhandene E-Mail-Kette integriert. Eine beispielhafte Konfiguration könnte wie folgt aussehen:



Ausgehende E-Mails werden von den Benutzern auf dem Mailbox-Server erzeugt und versendet. Der Mailbox-Server sendet die E-Mail anschließend an das Verschlüsselungs-Gateway. Dort wird die E-Mail

abhängig vom verfügbaren Schlüsselmaterial signiert und/oder verschlüsselt. Zuletzt wird sie an den Anti-Virus-Server weitergeleitet, der sie dem E-Mail-Server des Empfängers schließlich zustellt.

Damit das Verschlüsselungs-Gateway ordnungsgemäß funktionieren kann, benötigt es die passenden Schlüssel. Für die Erstellung von Signaturen bedeutet dies, dass für den jeweiligen Absender der passende private Schlüssel im Schlüsselspeicher des Gateways vorhanden sein muss.

Bei der Versorgung mit privaten Schlüsseln gibt es üblicherweise zwei unterschiedliche Herangehensweisen.

1) Der Administrator beantragt die Zertifikate manuell und importiert sie anschließend samt privatem Schlüssel in das Gateway.
2) Das Gateway bezieht die Zertifikate direkt von einer Zertifizierungsstelle. Die Zertifizierungsstelle kann sowohl eine eigene CA, als auch ein öffentliches Trustcenter sein.

Um die ausgehende E-Mail zusätzlich zu verschlüsseln, benötigt das Gateway den öffentlichen Schlüssel des Empfängers im Schlüsselspeicher. Dieser gelangt üblicherweise auf drei Wegen zum Gateway:

1) Der Administrator hat ihn manuell aus dem Internet heruntergeladen und anschließend im Gateway importiert.
2) Das Gateway hat den öffentlichen Schlüssel von einer eingehenden, signierten E-Mail des Kommunikationspartners gelernt.
3) Das Gateway hat den öffentlichen Schlüssel von einem Public-Key-Server im Internet heruntergeladen.

Eingehende E-Mails werden in diesem Szenario zunächst vom Anti-Virus-Server entgegen genommen und auf Malware sowie Spamgehalt geprüft. Ausgenommen von dieser Prüfung sind verschlüsselte E-Mails. Nach der Prüfung werden die E-Mails an das Verschlüsselungs-Gateway weitergeleitet und dort entschlüsselt. Zusätzlich wird die Unversehrtheit und Vertrauenswürdigkeit der Signatur geprüft. Gute Verschlüsselungs-Gateways bieten zusätzlich die Option, die entschlüsselte Nachricht auf Viren und Spamgehalt zu prüfen. Nach der kryptografischen Aufbereitung werden die E-Mails an den Mailbox-Server geschickt und können dort von den Benutzern gelesen werden. Dort kommt die E-Mail bereits in entschlüsselter Form an. Oftmals werden dem Empfänger der E-Mail noch Prüfberichte angehängt, die ihm zeigen, dass die E-Mail ursprünglich verschlüsselt und/oder signiert war.

Der entscheidende Vorteil von Verschlüsselungs-Gateways ist die Zentralisierung der Schlüssel-Administration. Die Benutzer müssen nicht mehr darauf achten, dass der private Schlüssel auf dem Gerät installiert ist, auf dem sie die E-Mail lesen (entschlüsseln) möchten. Besonders beim mobilen Zugriff auf das Postfach birgt dies enorme Herausforderungen und auch Risiken.

Eine weitere Herausforderung sind die öffentlichen Schlüssel der Empfänger, die für die Verschlüsselung benötigt werden. Auch diese müssen auf all den Geräten zur Verfügung stehen, auf dem der Absender die E-Mail verschlüsseln möchte. Zusätzlich müssen die Schlüssel vertrauenswürdig sein. Für S/MIME Zertifikate bedeutet dies, dass sie von einer vertrauenswürdigen Stammzertifizierungsstelle kommen.

Ein Verschlüsselungs-Gateway übernimmt die Verwaltung aller beteiligten Schlüssel und auch der vertrauenswürdigen Zertifizierungsstellen. EBCA-Technologiepartner haben die Zugänge zum öffentlichen Verzeichnisdienst bereits eingebaut und die Root-CAs als vertrauenswürdig vorinstalliert.

Die Einhaltung von Unternehmensregeln kann mit Hilfe eines Verschlüsselungs-Gateways ebenfalls sehr wirksam durchgesetzt werden, indem in der Software Regeln erstellt werden, die für bestimmte Zieldomänen, die Verschlüsselung erzwingen. Aus Versehen unverschlüsselt versendete E-Mails sind dann nicht mehr möglich.

Die Tatsache, dass die E-Mails durch die frühzeitige Entschlüsselung in unverschlüsselter Form in der Mailbox des Benutzers liegen, erfordert allerdings auch entsprechende Schutzmaßnahmen. So sollte zum Beispiel der Zugriff auf den Mailbox-Server grundsätzlich in verschlüsselter Form erfolgen. Für den Zugriff per Web-Schnittstelle bedeutet dies, dass ausschließlich über TLS kommuniziert wird.

Informationen zum Dokument

Version 1.1
01.04.2016

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
D-10115 Berlin

Tel.: +49 30 / 400 54 310
Fax: +49 30 / 400 54 311

info@ebca.de
http://www.ebca.de