HORNETSECURITY

FACT SHEET

EMAIL ENCRYPTION

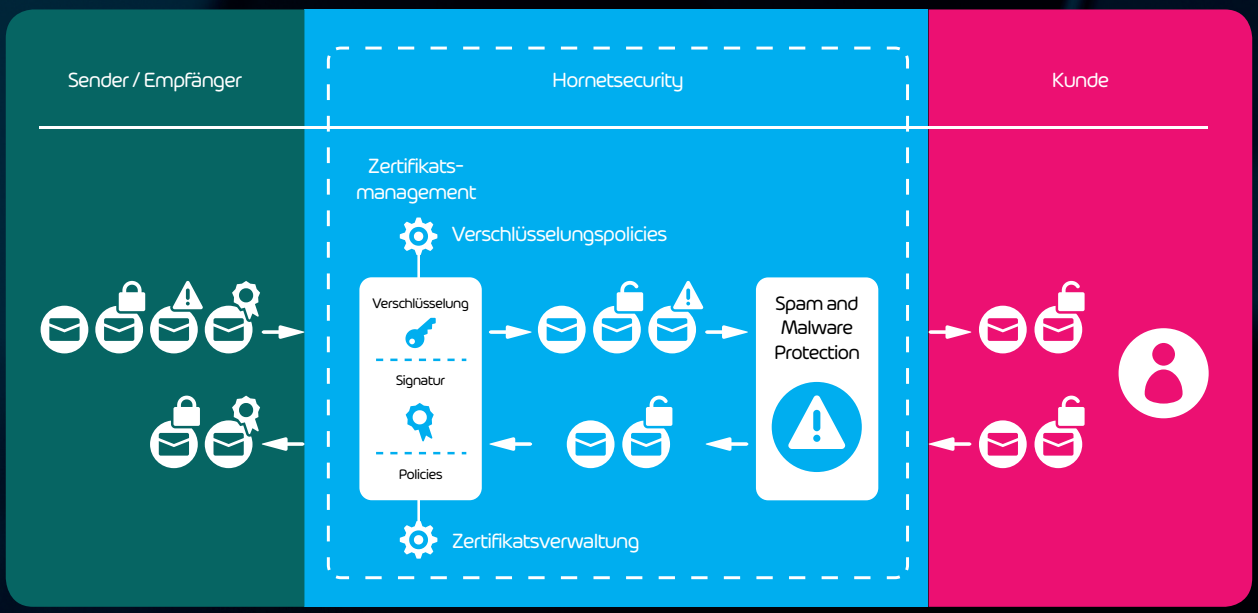
Rundum verschlüsselter Austausch von E-Mails mit Email Encryption
für eine zuverlässig sichere E-Mail-Kommunikation.

Geschäftliche E-Mails enthalten oftmals firmeninterne, persönliche oder andere sensible Inhalte, die bei unzureichendem Schutz während des Transportweges abgefangen und ausgespäht werden könnten.
Mit Email Encryption werden vertrauliche Informationen in der E-Mail-Kommunikation wirksam und sicher verschlüsselt.

Schutz vor:

- **Manipulation von E-Mail Nachrichten**
- **Ausspähung**
- **Abgreifen vertraulicher Informationen**

INTEGRATION VON EMAIL ENCRYPTION IM E-MAIL MANAGEMENT SYSTEM



Email Encryption von Hornetsecurity übernimmt das komplette Zertifikats-Management.

Ver- und Entschlüsselung sowie Signierung erfolgen vollautomatisch und transparent, bei ein- sowie ausgehenden E-Mails. Um die Funktionen und Effizienz von Email Encryption zu garantieren, wird die Buchung und Nutzung von Spam- and Malware Protection vorausgesetzt.

HORNETSECURITY

FACT SHEET

UMFASSENDE FEATURES FÜR DEN **SICHEREN E-MAIL AUSTAUSCH:**

Automatische digitale Signierung & Verschlüsselung ausgehender E-Mails per S/MIME und PGP: Sicherung der E-Mails vor unbefugter Veränderung oder Einsicht durch Dritte während des Transports durch öffentliche Netze.

Automatische Zertifikat-Verwaltung & Schlüsselspeicherung: Hornetsecurity übernimmt die Beschaffung und Installation benötigter Zertifikate. Diese werden in einem zentralen Zertifikatsspeicher vorgehalten.

Persönliche E-Mail-Zertifikate: Hornetsecurity nutzt 2048 Bit codierte Zertifikate einer der größten und seriösesten Certificate Authorities (CA). Bei der Verschlüsselung mit S/MIM erhält jeder Benutzer ein eigenes Zertifikat. Alternativ können auch vom Kunden angelieferte Zertifikate importiert und genutzt werden.

Automatische Entschlüsselung eingehender E-Mail: Liegt der öffentliche Schlüssel des Absenders vor, werden die E-Mails automatisch entschlüsselt und dem Empfänger zugestellt.

Individuelle Einrichtung und Festlegung von Verschlüsselungs-Richtlinien: Im Control Panel wird festlegt, über welche Verschlüsselungsarten man mit Kommunikationspartnern in Kontakt treten möchte: TLS, S/MIME, PGP oder Websafe. Dies ist entweder pauschal oder individuell für einzelne Nutzer, Gruppen oder Domains möglich. Darüber hinaus kann festgelegt werden, wie verfahren werden soll, wenn der Schlüssel eines Empfängers nicht vorliegt.

Testmöglichkeit der Verschlüsselungs-Tauglichkeit: Im Control Panel lässt sich prüfen, über welche Verschlüsselungsoptionen der Kommunikationspartner verfügt. Hierzu wird die E-Mail-Adresse des Empfängers eingegeben, anschließend wird angezeigt, welche Verschlüsselungstechnologie in der Kommunikation mit dieser Adresse eingesetzt werden kann.

Vertrauliche Kommunikation über Websafe: Auch wenn der Kommunikationspartner keine verschlüsselten E-Mails empfangen kann, wird die Verschlüsselung und Vertraulichkeit der E-Mail-Kommunikation mit bestimmten Personen weiterhin gewährleistet.

AUTOMATISCHE VERSCHLÜSSELUNG BEI MINIMALEM VERWALTUNGSAUFWAND:

Handling von Benutzerzertifikaten: Über das Control Panel lassen sich neue Zertifikate für Benutzer anfordern, verlängern oder dauerhaft beziehen (S/MIME Subscription).

Anpassungsfreie Skalierbarkeit: Es ist jederzeit möglich, die Zahl der verschlüsselten E-Mail-Benutzer an die Bedürfnisse des Kunden anzupassen.

Automatische Update: Aufgrund des cloudbasierten Verschlüsselungsservices steht den Unternehmen stets die aktuellste Version des Dienstes zur Verfügung.