21.07.2021

Leistungsbeschreibung
Email Encryption

1. Der Hornetsecurity Email Encryption ist eine Erweiterung des Hornetsecurity Spam and Malware Protection und setzt die Nutzung des Spamfilterservice voraus.
2. Hornetsecurity verschlüsselt und signiert ausgehende E-Mails und entschlüsselt eingehende E-Mails des Auftraggebers auf seinen eigenen IT-Systemen entsprechend den eingestellten Richtlinien.
3. Ausgehende E-Mails werden per S/MIME signiert, sofern die dazu nötigen privaten Schlüssel im Zertifikatsspeicher vorliegen und im Control Panel im Bereich S/MIME Users die Signierung für den Benutzer aktiviert wurde.
4. Die Richtlinien zur Verschlüsselung ausgehender E-Mails können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.
5. Je nach Einstellung der Richtlinien werden ausgehende E-Mails:
   a) mit dem öffentlichen Schlüssel des Empfängers per S/MIME oder PGP verschlüsselt übertragen,
   b) nicht verschlüsselt aber über einen per TLS verschlüsselten Kanal übertragen,
   c) im geschützten Hornetsecurity Websafe für den Empfänger bereitgestellt,
   d) unverschlüsselt übertragen.
6. Die Policies können durch autorisierte Benutzer z.B. im Hornetsecurity Control Panel gesetzt werden. Die Verschlüsselung einer Mail kann zusätzlich durch den Benutzer beim Versand über einen Betreff-Zusatz („Tag“) oder das Hornetsecurity Outlook Add-In sichergestellt werden.
7. Sofern die Richtlinie zwingend die verschlüsselte Übertragung vorsieht, aber der dazu nötige öffentliche Schlüssel des Empfängers nicht im Zertifikatsspeicher vorliegt und die ggf. eingestellte Übertragung per TLS vom empfangenden Server nicht unterstützt wird, werden ausgehende E-Mails an diesen Empfänger zurückgewiesen und nicht übertragen.
8. Eingehende, per S/MIME oder PGP verschlüsselte E-Mails werden automatisch entschlüsselt, sofern der dazu nötige private Schlüssel des Empfängers im Zertifikatsspeicher vorliegt.
9. Öffentliche Schlüssel werden automatisch aus Signaturen eingehender E-Mails extrahiert und im Zertifikatsspeicher hinterlegt.
10. S/MIME-Zertifikate für Benutzer des Auftraggebers können im Rahmen der S/MIME User Subscription per Control Panel bestellt werden. Alternativ können PGP Keys für die Benutzer des Auftraggebers generiert oder vorhandene S/MIME Zertifikate und PGP Keys vom Hornetsecurity Support im Zertifikatsspeicher abgelegt werden. Für die Nutzung von Zertifikaten und Keys erhebt Hornetsecurity eine jährliche Gebühr pro Zertifikat und Key des Benutzers gemäß der aktuellen Preisliste. Diese Subscription verlängert sich automatisch sofern sie nicht 3 Monate vor Ablauf deaktiviert wird und inkludiert die automatische Neubestellung von Zertifikaten und Keys bei Bedarf.
11. Hornetsecurity stellt die Geheimhaltung der im Zertifikatsspeicher gespeicherten privaten Schlüssel des Auftraggebers sicher. Die Pflicht zur Geheimhaltung besteht auch nach Ende dieses Vertrags fort.
12. Über den Websafe können Kommunikationspartner verschlüsselte E-Mails sicher via https abrufen, sofern der Auftraggeber den Websafe in seinen Verschlüsselungsrichtlinien aktiviert hat. Hierfür erhält der Absender der Nachricht eine PIN, die er dem Empfänger zur initialen Authentifizierung und / oder zum Passwortreset zur Verfügung stellt. Im

Rahmen des Websafe 2.0 (ab Sommer 2021) bietet Hornetsecurity für den Login von Kommunikationspartnern am Websafe die Option, die PIN über einen weiteren Kanal auf mobile Endgeräte des Kommunikationspartners zu senden. Hornetsecurity behält sich vor, die Verwendung des SMS-Gateways bei Verdacht auf missbräuchliche Nutzung zu deaktivieren.

13. Hornetsecurity unterstützt den verschlüsselten Versand nach EDIFACT-Standard. Die hierfür notwendigen S/MIME-Zertifikate mit RSASSA-PSS Hashverfahren werden hierfür vom Auftraggeber für den Import bereitgestellt.
14. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Vertragsbestandteil.
15. Hornetsecurity ermöglicht optional eine Anbindung der E-Mail-Infrastruktur des Kunden an den E-Mail made in Germany (EmiG) – Verbund und realisiert hierfür die Mailserver-seitige Umsetzung, die für die Erfüllung der Anforderungen an eine durchgehende Transportverschlüsselung von E-Mails im EmiG-Verbund notwendig sind.
    a. Hornetsecurity stellt sicher, dass eine als EmiG gekennzeichnete Nachricht nicht über andere, potenziell unsichere Kanäle zugestellt wird.
    b. Die durchgängig verschlüsselte Datenübertragung zwischen den Mail Transfer Agents (MTAs) hierfür wird sichergestellt mittels STARTTLS-Erweiterung gemäß RFC 3207.
    c. Die TLS1.2-Verbindung wird durch Hornetsecurity eingehend (TLS-Client) wie ausgehend (TLS-Server) realisiert.
    d. Hornetsecurity stellt sicher, dass EmiG-Kommunikation nur unter Verwendung Perfect Forward Secrecy (PFS)-fähiger Schlüsselaustauschverfahren basierend auf dem Diffie-Hellmann-Verfahren aufgebaut wird.
    e. Bei Schlüsselneuverhandlungen für Mailkommunikation innerhalb des EmiG-Verbundes verwendet Hornetsecurity secure renegotiation gemäß RFC 5746.
    f. Jeder Zertifikats- / Verschlüsselungsfehler beim STARTTLS-Aufbau wird genauso behandelt, als sei gar keine SMTP-Verbindung aufgebaut worden: Die Mail wird in eine Mail-Queue zurückgestellt, aus der weitere Zustellversuche unternommen werden. Bei dauerhaftem Fehlschlagen der Zustellung wird eine Bounce-Nachricht an den Sender geschickt.
    g. Hornetsecurity überprüft anhand der innerhalb des EmiG-Verbunds annoncierten Zertifikatsfingerprints die Identität und EmiG-Verbund-Zugehörigkeit der Kommunikationspartner der Nutzer des Kunden:
    h. Der per MX-Lookup ermittelte Hostname eines Mailservers wird mit dem im Host-Zertifikat hinterlegten Namen abgeglichen.
    i. Es wird überprüft, ob der Fingerprint des vom Mailserver des Kommunikationspartners verwendeten Zertifikats dem über EmiG annoncierten Fingerprints entspricht.
    j. Schlägt diese Validierung fehl, wird die E-Mail-Kommunikation mit diesem Mailserver unterbrochen, die Mail wird nicht weitergeleitet.
    k. Die Zertifikatsprüfung wird gemäß PKIX einschließlich der Sperrprüfung der Server- und Sub-CA-Zertifikate durchgeführt.
    l. Die per https vom EmiG-Verbund bidirektional zur Verfügung zu stellenden JSON-MX-Infrastrukturlisten werden durch Hornetsecurity gemäß der EmiG-Vorgaben für den Kunden vollautomatisch generiert und gepflegt.
    m. Hornetsecurity annonciert die notwendigen Informationen, die der Kunde dem EmiG-Verbund mitzuteilen

hat, über die von EmiG vorgegebenen Verfahren (MX-Infrastruktur-Listen).

n. Die Authentifikation des sendenden Mailservers als Server eines EmiG-Teilnehmers wird mittels dynamischem Abgleich mit den bei EmiG registrierten IPs durchgeführt.

o. Hornetsecurity bietet dem Kunden verschiedene Möglichkeiten der Darstellung, ob eine Nachricht gemäß den Vorgaben des EmiG-Verbunds versendet oder empfangen wurde.

   i. Im Control Panel wird dem Nutzer dargestellt, ob eine Mailkommunikation gesichert über den EmiG-Verbund stattfand.

   ii. Unter Verwendung eines Outlook-Addins kann der Nutzer den EmiG-Status seiner Nachrichten und Kommunikationspartner in Outlook einsehen (Feature ist in Vorbereitung).

16. Fair Use Limits (Einschränkungen zur angemessenen Nutzung)

a. Die Bandbreite, der Speicherplatz, die Infrastruktur und die Ressourcen, die für die Nutzung der Software erforderlich sind und die wir in diesem Zusammenhang zur Verfügung stellen, werden von allen unseren Kunden gemeinsam genutzt. Daher haben wir das Recht, Maßnahmen zu ergreifen, um sicherzustellen, dass alle Kunden die Lösung angemessen und fair nutzen, so dass eine solche Nutzung die normale Serviceleistung für andere Kunden nicht beeinträchtigt oder verhindert.

b. Wir haben uns dazu entschlossen, keine Richtwerte vorab festzulegen, die eine exzessive oder unangemessene Nutzung bestimmen, da wir nach unserem Ermessen entscheiden können, unsere normalen Service-Levels aufrechtzuerhalten, indem wir anderen Nutzern reservierte Ressourcen, die zu diesem Zeitpunkt nicht genutzt werden, neu zuweisen oder Ressourcen anderweitig skalieren. Sie verstehen, dass wir, wenn wir uns entscheiden, unsere Richtlinie zur angemessen Nutzung nicht aktiv durchsetzen, nicht davon ausgehen, dass wir auf unser Recht, dies zu tun, verzichtet haben, noch haben wir zugestimmt, dass Sie unsere Dienste weiterhin auf demselben Niveau nutzen, wie Sie es zu einem bestimmten Zeitpunkt tun.

c. Um unsere Dienste nutzen zu können, müssen Sie abrechenbare Einheiten erwerben. Die Anzahl der abrechenbaren Einheiten, die Sie benötigen, hängt von einer Reihe von Kriterien ab, wie z. B. der Größe Ihres Unternehmens, der Anzahl der Nutzer und der Speichergröße der jeweiligen Datenquellen. Sie können die Anzahl der abrechenbaren Einheiten, die Sie benötigen, anhand unserer Leitfäden, die wir auf unserer Webseite für Gebühren und Abrechnungen hochgeladen haben, oder durch die Unterstützung unseres Vertriebsteams ermitteln.

d. Unabhängig von der Anzahl der abrechenbaren Einheiten, die Sie erworben haben, müssen Sie unsere Dienstleistungen zweckmäßig nutzen, und zwar in einer Weise, die es nicht erforderlich macht, dass wir unverhältnismäßig viele Ressourcen zuweisen müssen. Um dies festzustellen, werden wir Ihre Nutzung unserer Ressourcen und Ihren Speicherbedarf mit dem eines durchschnittlichen Kunden vergleichen. Den Durchschnittskunden ermitteln wir, indem wir die 5% höchsten und die 5% niedrigsten Kunden der jeweiligen Ressource unberücksichtigt lassen und den Mittelwert über alle unsere aktiven Kunden bilden.

e. Spezifische Merkmale, die sich auf die Branche beziehen, in der Sie tätig sind, werden bei der Feststellung, ob die Nutzung als angemessen angesehen wird, nicht berücksichtigt.

f. Wenn wir nach vernünftigem Ermessen und in gutem Glauben davon ausgehen, dass die Nutzung unserer Lösung durch Sie nicht sinnvoll ist oder gegen diese Richtlinie verstößt, werden wir nach eigenem Ermessen eine der folgenden Maßnahmen ergreifen
   i. Ihnen erlauben, unsere Lösungen weiterhin zu nutzen, jedoch vorbehaltlich unter der Bezahlung zusätzlicher Gebühren und der Einhaltung von Bedingungen, die wir unter den gegebenen Umständen für angemessen halten.
   ii. Sie zu informieren, dass Ihr Konto innerhalb eines nach unserem Ermessen angemessenen Zeitrahmens gekündigt wird. Während dieses Zeitraums werden die Backups ausgesetzt.

g. Wenn wir von unserem Recht Gebrauch machen, Ihr Konto wie oben beschrieben zu kündigen:
   i. werden Ihre Sicherungsdaten am Ende des von uns in der diesbezüglichen Benachrichtigung festgelegten Zeitrahmens gelöscht, ungeachtet anderslautender Bestimmungen in den Allgemeinen Geschäftsbedingungen.
   ii. erhalten Sie eine Rückerstattung der im Voraus gezahlten Gebühren für die verbleibenden Tage Ihres Abonnementzeitraums.