Leistungsbeschreibung
Spamfilterservice

1. Hornetsecurity filtert eingehende E-Mails des Auftraggebers auf schädlichen Inhalt (z.B. Viren), unerwünschte Werbung (z.B. Spam) und legitime Werbung (z.B. Newsletter) auf seinen eigenen IT-Systemen. E-Mails an den Auftraggeber werden dazu durch Umstellung der MX-Records für die zu filternden Domains des Auftraggebers auf die Server von Hornetsecurity geleitet. Für die Umstellung des MX-Records ist Hornetsecurity nicht verantwortlich.
2. Die Spamerkennungsrate liegt bei mindestens 99,9% im Monatsdurchschnitt, bezogen auf die Zahl aller E-Mails, die die Systeme von Hornetsecurity für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen. Voraussetzung ist die direkte Zustellung eingehender E-Mails per SMTP auf die Systeme von Hornetsecurity durch Umstellung der MX-Records der Domains des Auftraggebers.
3. Die Virenerkennungsrate liegt im Jahresdurchschnitt bei mind. 99,99%, bezogen auf die Zahl aller E-Mails, die die Systeme von Hornetsecurity für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen.
4. Die Falsch-Positiv-Rate liegt unter 0,00015 im Monatsdurchschnitt, bezogen auf die Zahl aller Clean-E-Mails, die die Systeme von Hornetsecurity für Domains des Auftraggebers im gemessenen Zeitabschnitt erreichen. Ausgenommen sind solche E-Mails, die durch falsch konfigurierte Server (nicht RFC-Konform), über verifizierte Open Relays oder mangelhaft eingerichtete Mailclients versendet wurden.
5. Die Verfügbarkeit im Mailverkehr per SMTP beträgt 99,99% im Jahresmittel. Voraussetzung ist die direkte Zustellung eingehender E-Mails per SMTP auf die Systeme von Hornetsecurity durch Umstellung des MX-Records. Geplante Wartungsarbeiten werden nicht berücksichtigt, diese werden soweit es möglich ist am Wochenende nachts ausgeführt (MEZ).
6. Soweit der Auftraggeber es wünscht werden auch ausgehende E-Mails gefiltert.
7. Empfangene E-Mails werden:
   a. Geblockt (zurückgewiesen), soweit sie noch während der Aufnahme der Datenverbindung mit den Servern von Hornetsecurity mit hoher Sicherheit als unerwünscht erkannt werden,
   b. Wahlweise In Quarantäne gestellt oder mit einer Markierung im Betreff zugestellt, sofern sie nach vollständiger Annahme der E-Mail durch die Server von Hornetsecurity als unerwünscht erkannt werden,
   c. Zugestellt oder zur Abholung bereitgestellt, sofern sie als erwünschte E-Mail erkannt werden.
   d. Die Zustellzeiten liegen typisch im Durchschnitt bei unter 30 Sekunden, der maximale durchschnittliche Wert liegt bei 3 Minuten.
8. E-Mails in Quarantäne werden drei Monate zur Einsicht durch autorisierte Benutzer des Auftraggebers gespeichert. Auf Wunsch des Auftraggebers werden Benutzer über neue E-Mails in der Quarantäne informiert (in der Regel einmal täglich).
9. Auf E-Mails in der Quarantäne können autorisierte Benutzer aus dem Internet zugreifen. Autorisierte Benutzer können interaktiv die Zustellung von E-Mails in Quarantäne auf die Systeme des Auftraggebers veranlassen.
10. Autorisierte Nutzer können persönliche White- und Blacklists pflegen. Die Konfiguration kann über verschiedene Wege erfolgen, z.B. Hornetsecurity Control Panel,

Quarantäne Report, oder das Hornetsecurity Outlook Add-In.

11. Soweit Eingriffe durch den Auftraggeber in die Filterstufen erfolgen (z.B. Einrichten von speziellen White- oder Blacklists), können Qualität und Erkennungsraten der Filterstufen nicht gewährleistet werden.
12. Autorisierte Nutzer des Auftraggebers (z.B. Support-Mitarbeiter und Administratoren) können über das Hornetsecurity Control Panel den kompletten Mailverlauf des Auftraggebers überblicken. Im Live-Monitor können zusätzlich auch alle geblockten (abgewiesenen) E-Mails der vergangenen 7 Tage nachverfolgt werden.
13. Optional werden ein- und ausgehende E-Mails entsprechend eingestellter Richtlinien gefiltert (Content und Compliance-Filter). Je nach Einstellung werden E-Mails, die den Richtlinien nicht entsprechen:
    a. mit einer entsprechenden Fehlermeldung zurückgewiesen (eingehend),
    b. ohne Anhang zugestellt und mit Anhang in eine Quarantäne gestellt, aus der sie von Administratoren dem Empfänger zugestellt werden können (eingehend),
    c. mit einer entsprechenden Fehlermeldung zurückgewiesen (ausgehend).
14. Die Richtlinien zur Content- und Compliance- Filterung können von dazu autorisierten Benutzern des Auftraggebers im Hornetsecurity Control Panel eingestellt werden.
15. E-Mails werden über einen per TLS verschlüsselten Kanal übertragen, soweit die Gegenseite die Übertragung per TLS unterstützt. Weitere Verschlüsselungsverfahren können optional über den Hornetsecurity Encryption Service genutzt werden.
16. Der Inhalt zugestellter E-Mails wird nur gespeichert, wenn der optionale Hornetsecurity Continuity Service oder der Hornetsecurity Archiv Service zusätzlich genutzt wird.
17. Hornetsecurity kann neben den bereits bestehenden Methoden und Verfahren zur Erkennung von Viren weitere AV-Engines von Antivirus Spezialisten optional hinzuschalten.
18. Hornetsecurity stellt den Support autorisierter Benutzer sicher, soweit es die Systeme von Hornetsecurity betrifft. Der Support von Systemen des Auftraggebers ist nicht Bestandteil dieses Vertrags.