Leistungsbeschreibung
htp Net Business MailScan

1. Allgemeines

Der Leistungsumfang von htp Net Business MailScan ergibt sich aus dem Auftrag und dieser Leistungsbeschreibung.

2. Leistungsmerkmale

htp stellt dem Kunden mit diesem Service ein Mailrelay für ein- und ausgehende E-Mails für registrierte IP- und Domainadressen des Kunden zur Verfügung. Der Service umfasst die Funktionen „Virenschutz“ und/oder „Spamschutz“ für eingehende E-Mails. Die Kosten für diesen Service richten sich nach der Anzahl der E-Mail-Benutzer auf Seite des Kunden. Für die Zustellung der eingehenden E-Mails und dem Versand ausgehender E-Mails benötigt der Kunde einen eigenen Mailserver, der nicht Bestandteil dieser Leistung ist.

2.1. Schnittstellen

Der Service htp Net Business MailScan wird von htp so bereitgestellt, dass eingehende E-Mails auf Port TCP-25 über das SMTP Protokoll angenommen und ausgehende E-Mails an den Zielmailserver auf Port TCP-25 über das SMTP Protokoll ausgeliefert werden.

2.2. Relayschutz / Mailweiterleitung / Adressüberprüfung

Ausgehender Mailverkehr:
Der Service htp Net Business MailScan nimmt E-Mails mit jeglichen Zieldomains nur von der IP Adresse des kundeneigenen Mailservers an. Diese E-Mails werden an den für die Zieldomain laut DNS zuständigen Mailserver im Internet ausgeliefert.

Eingehender Mailverkehr:
Der Service htp Net Business MailScan nimmt aus dem Internet eingehende E-Mails nur für die vom Kunden beauftragten E-Mail-Domains entgegen. Eingehende E-Mails aus dem Internet mit unbekannten Zieldomains werden abgelehnt.
Zur Vermeidung von „Backscatter-Mails“ erfolgt bei der E-Mail Annahme durch den htp Net Business MailScan Service eine Gültigkeitsprüfung des E-Mail Empfängers. Dabei wird während der Annahme über eine zusätzliche SMTP Verbindung zum Mailserver des Kunden die Existenz des E-Mail-Empfängers geprüft. Sollte der Mailserver des Kunden dabei mit einer Fehlermeldung („user unknown“) antworten, wird die einzuliefernde E-Mail vom htp Net Business MailScan Service sofort abgelehnt. Sollte der SMTP Dienst des Kunden zur Adressüberprüfung temporär nicht zur Verfügung stehen, so werden alle E-Mails angenommen und zwischengespeichert.

Der Kunde teilt htp bei Beauftragung mit dem Formular „htp Net Business MailScan - Technische Anlage zur Konfiguration“ die IP-Adresse der eigenen Mailserver und die eigenen Domains mit.

2.3. Sessionparameter

Für alle ein- und ausgehende E-Mails, die an den htp Net Business MailScan Service übergeben werden, gelten folgende Bedingungen:

Maximale Anzahl von SMTP-Verbindungen eines Mailservers je 5 Minuten	200
Maximale Anzahl gleichzeitiger SMTP-Verbindungen eines Mailservers	5
Maximale Anzahl von E-Mails je Verbindung	10
Maximale Anzahl von Empfängern je E-Mail	500
Maximale Größe einer E-Mail	20 GByte
Maximale Größe eines E-Mail Headers	32 KByte

E-Mails, die diese Bedingungen nicht erfüllen werden nicht angenommen.

2.4. Queueing

Ein- und ausgehende E-Mails die nicht an den Zielmailserver übermittelt werden können, werden 5 Tage zwischengespeichert. Innerhalb dieser Zeit wird ca. alle 27 Minuten ein erneuter Zustellversuch unternommen. Nach 4 Stunden erhält der Absender der E-Mail einen Hinweis per E-Mail, dass die E-Mail bisher nicht zugestellt werden konnte. Nach 5 Tagen wird die E-Mail mit einem entsprechenden Hinweis an den Absender zurückgesendet.

2.5. Virenschutz

Die Leistung Virenschutz steht nur zur Verfügung, wenn Sie vom Kunden explizit beauftragt wurde.
htp untersucht bei jeder eingehenden E-Mail den Textteil (body) und die Anhänge hinsichtlich Viren und bösartiger Skripte. Virenfreie E-Mails werden unverzüglich an den Mailserver des Kunden zugestellt. Bei infizierten E-Mails wird der vom Virus betroffene Teil der E-Mail unwiderruflich gelöscht. Die E-Mail wird dann ohne den Virusteil zugestellt.
Auf jegliche Veränderung der E-Mail durch den Virenscannvorgang wird der Empfänger der E-Mail hingewiesen. htp fügt hier automatisiert eine entsprechende Nachricht an den Textteil der E-Mail an.
Inhalte von Archiven (z.B. zip) werden rekursiv bis zu einer Tiefe von 10 Stufen dekomprimiert und analysiert.
Der Kunde beauftragt mit dem Formular „htp Net Business MailScan - Technische Anlage zur Konfiguration“ ob Kennwort geschützte Archive blockiert oder durchgelassen werden sollen.

Eine verschlüsselte E-Mail kann aus technischen Gründen nicht auf Viren überprüft werden. Sie wird daher unverändert zugestellt. htp gewährleistet mit dem Einsatz des Virenscanners keinen hundertprozentigen Schutz vor Viren aus dem Internet.

2.6. Spamschutz

Die Leistung Spamschutz steht nur zur Verfügung, wenn Sie vom Kunden explizit beauftragt wurde.
htp bewertet an Hand definierter Kriterien jede eingehende E-Mail hinsichtlich ihrer Spam-Wahrscheinlichkeit. E-Mails, die nicht als Spam bewertet werden, werden unverändert an den Mailserver des Kunden weitergeleitet. E-Mails, die als Spam erkannt werden, werden im E-Mail-Header mit folgender Zeile markiert: „X-Spam-detected-by-htp" Diese Markierung kann z.B. durch den Mailserver des Kunden ausgewertet werden.

Weiterhin wird eine Spam nach einer der folgenden Reaktionsverfahren behandelt:

a) Markierung im Subject
   Das Subject/Betreff der Spam erhält das Prefix „[Spam detected]". Die E-Mail wird dann sofort an den Mailserver des Kunden weitergeleitet.
b) Zwischenspeicherung im Quarantäneverzeichnis inkl. Empfängerreport
   Alle Spams werden empfängerbezogen in einem zentralen Quarantäneverzeichnis gespeichert. Der Empfänger erhält bis zu zweimal täglich einen Report, aus denen Absender und Thema der Spam hervorgehen. Der Empfänger kann sich über einen Link im Report gezielt Spams zustellen lassen. Der Report wird nur dann erstellt, wenn im Quarantäneverzeichnis Spams für den Empfänger vorliegen.
   Die Spams werden im Quarantäneverzeichnis bei Nichtabruf nach 14 Tage gelöscht. Der Kunde kann mit einem Administratorzugang per Web in das Quarantäneverzeichnis einsehen.

Bei der Spam-Erkennung stehen dem Kunden zwei unterschiedliche Empfindlichkeitsstufen (Sensibilitäten) zur Verfügung. Optional kann der Kunde die Funktion „Greylisting" beauftragen. Beim Greylisting gilt eine Sperrzeit von 1 Minute nach dem ersten Zustellversuch (greylisting period) und eine Cache-Zeit von 36 Tagen (greylisting TTL). Der Kunde wird darauf aufmerksam gemacht, dass es durch die Funktion „Greylisting" zu Verzögerungen beim E-Mail-Empfang kommen kann.

Der Kunde erhält die Möglichkeit via Webfrontend bis zu 500 persönliche Black- und Whitelisteintragungen für bestimmte E-Mail-Absender vorzunehmen. E-Mails von Absender die auf der Whitelist enthalten sind werden immer unverändert zugestellt; E-Mails von Absendern, die auf der Blacklist enthalten sind, werden als Spam behandelt.

Für die Administration per Web wird seitens des Kunden ein aktueller Webbrowser mit JAVA Unterstützung benötigt.

Der Kunde teilt htp bei Beauftragung mit dem Formular „htp Net Business MailScan - Technische Anlage zur Konfiguration" die gewünschte Sensibilität des Spam-Filters, das Reaktionsverfahren und weitere Optionen mit.

Die Zugangsdaten für die webbasierte Administration der Quarantänequeue und der Black-/Whitelists erhält der Kunde mit seiner Auftragsbestätigung.

2.7 Monatsberichte

htp stellt Anfang eines Monats dem Kunden per E-Mail ein pdf-Dokument bereit, aus dem eine Zusammenfassung der Mailaktivitäten hervorgeht.

Der Kunde teilt htp bei Beauftragung mit dem Formular „htp Net Business MailScan - Technische Anlage zur Konfiguration" eine E-Mail-Adresse für den Empfang der Monatsberichte mit.

2.8. Softwarepflege

htp führt die für die Erbringung der Leistung erforderlichen Softwareupdates für das Betriebssystem, den Spam-Filter und den Virenscanner durch. Die Virensignaturen des Virenscanners werden mehrmals täglich aktualisiert. htp ist für die Nachhaltung der Lizenzen verantwortlich.

3. Pflichten des Kunden

3.1. DNS Eintrag

Der Kunde muss dafür Sorge tragen, dass der erforderliche MX-Eintrag in der Zonendatei seiner Domain im DNS vorgenommen wird.

3.2. Domainnamen und Mailserver

Der Kunde nennt htp den Domainnamen der E-Mailadressen, für den diese Leistung gelten soll und die statische IP Adresse des kundeneigenen Mailservers, an der die eingehenden E-Mails weitergeleitet werden.

3.3. Endnutzerzahl

Der Kunde teilt htp bei Beauftragung der Leistung die Zahl der Endnutzer, die diese Leistung in Anspruch nehmen, mit. Sollte sich innerhalb der Vertragslaufzeit die Endnutzerzahl ändern, so ist der Kunde verpflichtet, dieses gegenüber htp schriftlich binnen zwei Wochen anzuzeigen.

4. Verfügbarkeit

htp stellt diese Leistung mit einer Verfügbarkeit von 99,9% im Jahresdurchschnitt bereit. htp behält sich das Recht vor, technische Änderungen oder Wartungsarbeiten an ihrem Netz vorzunehmen. Diese bleiben bei der Berechnung der Verfügbarkeit unberücksichtigt. htp wird dabei die Belange des Kunden berücksichtigen und Wartungsarbeiten grundsätzlich in einem außerhalb der üblichen Arbeitszeit liegenden Zeitfenster von 4:00 bis 07:00 Uhr durchführen. htp behält sich vor, diese Wartungszeiten nach angemessener Ankündigung aufgrund technischer oder betrieblicher Erfordernisse zu ändern.

5. Service Level Agreement (SLA)

Störungen werden von htp unverzüglich im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten und den nachfolgenden Bedingungen beseitigt. Für die Entgegennahme von Störungsmeldungen und technischen Fragen hat htp die Servicerufnummer 0800-4877587 (htp plus) eingerichtet. Hinsichtlich der Servicebereitschaft, der Reaktions- und der Entstörzeit gelten folgende Zeiten:

Hotline: 0800-4877587 (htp plus) Montag bis Samstag von 08:00 Uhr bis 22:00 Uhr

Störungsannahme:	werktags inkl. samstags von 08:00 Uhr bis 22:00 Uhr

	werktags (außer samstags), 8 - 18 Uhr
Reaktionszeit	1 Stunde
Entstörzeit	4 Stunden

Reaktionszeit ist der Zeitraum ab Eingang der Störungsmeldung, innerhalb der htp den Kunden telefonisch über mögliche Fehlerursachen und die voraussichtliche Ausfalldauer unterrichtet. Die Reaktion gilt bei Nichterreichbarkeit des Kunden mit dem Anrufversuch als erfolgt. Nach Ablauf der Reaktionszeit beginnt die Entstörzeit, innerhalb der htp die Leistung wieder herzustellen hat. Nach Beseitigung der Störung erhält der Kunde eine telefonische Abschlussmeldung oder eine Abschlussmeldung von einem Techniker vor Ort. Die Störung gilt bei Nichterreichbarkeit des Kunden mit dem Anrufversuch als beseitigt.

6. Haftungsausschluss

htp haftet in dem Fall, dass Teile von E-Mails fälschlicher Weise als Virus erkannt und entfernt wurden, nur im Rahmen der Allgemeinen Geschäftsbedingungen der htp GmbH für die Erbringung von Telefon- und Internetdienstleistungen.