htp stellt speziell für Geschäftskunden MailRelay-Service zur Verfügung. Kunden, die eigene E-Mail Server betreiben, können über den htp MailRelay-Service E-Mails aus dem Internet empfangen und E-Mails in Richtung Internet versenden.

Der htp MailRelay-Service ist hochverfügbar und wird von htp mit mehreren Servern in unterschiedlichen Rechenzentren zur Verfügung gestellt.

Nutzen Sie den htp MailRelay-Service für den Empfang und Versand Ihrer E-Mails über das SMTP-Protokoll. Ihr E-Mail-Server liefert stets Ihre ausgehenden E-Mails an die htp MailRelay-Server aus. htp übernimmt die Zustellung im Internet oder speichert temporär die E-Mails bei Nichterreichbarkeit und nimmt automatisch weitere Zustellversuche vor.
Für den E-Mail Empfang können Sie den htp MailRelay-Service für Ihre Domain als ersten Mailserver (Primary MX) oder Fallback Mailserver (Fallback MX) verwenden. E-Mails werden bei Nichterreichbarkeit Ihrer Server zwischengespeichert. Zusätzlich bietet htp Ihnen wertvolle Zusatzdienste zur Reduzierung von SPAM an.

Zur Nutzung des htp MailRelay-Services für ausgehende E-Mails (outbound) müssen Sie als Geschäftskunde der htp über eine htp Internetanbindung mit einer statischen IP Adresse für Ihren E-Mail-Server verfügen.
Zur Nutzung des htp MailRelay-Services für eingehende E-Mails (inbound) müssen Sie zusätzlich die verwendeten E-Mail-Domains über htp registriert haben.

htp bietet Ihnen die MailRelay-Services „Premium“ und „Standard“ zur Auswahl. Wählen Sie den für Ihre Firma optimalen MailRelay-Service aus und beauftragen Sie den Dienst einfach über das Formular „Konfigurationsauftrag htp MailRelay Dienste“. Das Formular bieten wir Ihnen auf unserer Homepage http://www.htp.net im Downloadpool unter der Rubrik „Auftragsformulare“ zum Download an.

Bitte beachten Sie, dass Sie für die Nutzung des htp MailRelay-Service an Ihrer Firewall den Port TCP-25 für die SMTP Verbindungen gemäß folgender Tabelle frei schalten. Verwenden Sie für den E-Mail Versand an Ihrem Mailserver den angegebenen ausgehenden htp MailRelay-Server als „Next Mail Hop“.

	MailRelay Premium	**MailRelay Standard**
Eingehend / Inbound	mxp01.htp-tel.de (212.59.41.8) mxp02.htp-tel.de (212.59.41.9)	mxu01.htp-tel.de (81.14.242.8) mxu02.htp-tel.de (81.14.242.9)
Ausgehend / Outbound	mx03.htp-tel.de (212.59.41.10)	mx04.htp-tel.de (81.14.242.10)

Funktionsübersicht der htp MailRelay Dienste

Funktion	MailRelay Premium	MailRelay Standard
Eingehend / Inbound		
Maximale Größe einer E-Mail	200 MB	50 MB
SMTP Empfänger Check	✔	✘
Greylisting (optional)	✔	✘
Greylisting Sperrzeit	3 Min.	✘
Greylisting Gültigkeitszeit	1 Tag	✘
Greylisting Whitelist-Zeit	95 Tage	✘
Block dynamic IP	✔	✔
SPAM-Analyse	✔	✘
Blocking High-SPAM (optional)	✔	✘
Header Kennzeichnung	✔	✘
E-Mail Caching	✔	✔
Maximale Speicherzeit bei Nichterreichbarkeit	5 Tage	5 Tage
Infomail an den Absender bei Nichterreichbarkeit	4 Std.	4 Std.
Zustellintervall bei Nichterreichbarkeit	30 Min.	30 Min.
Ausgehend / Outbound		
Maximale Größe einer E-Mail	200 MB	50 MB
Limitierung der E-Mail Frequenz je IP-Adresse	✔	✘
Maximale Anzahl der E-Mails je Stunde	500	✘
Maximale Anzahl von E-Mails je Tag	5.000	✘
E-Mail Caching	✔	✔
Maximale Speicherzeit bei Nichterreichbarkeit	5 Tage	5 Tage
Infomail an den Absender bei Nichterreichbarkeit	4 Std.	4 Std.
Zustellintervall bei Nichterreichbarkeit	30 Min.	30 Min.

Erläuterungen

SMTP Empfänger Check
Mit dem SMTP Empfänger Check vermeiden Sie Systemüberlastungen Ihres Mailservers bei SPAM-Attacken. Eingehende E-Mails, für die auf dem Mailserver des Kunden kein gültiger Empfänger existiert, werden bereits am htp MailRelay abgelehnt. Hierzu prüft das htp MailRelay während der Zustellung aus dem Internet die Gültigkeit der Empfänger E-Mail-Adresse, indem das htp MailRelay eine SMTP Verbindung zum Mailserver des Kunden aufbaut und eine SMTP Mailzustellung startet. Hierbei wird die SMTP Session nur bis zur Empfängermitteilung gehalten. Meldet der Mailserver des Kunden keine Fehlermeldung („user unknown“) für den Empfänger, so nimmt das htp MailRelay die E-Mail aus dem Internet an und leitet sie anschließend an den Mailserver des Kunden weiter.
Mit dieser Technik wird sichergestellt, dass jede angenommene E-Mail einem Postfach auf dem Mailserver des Kunden zugestellt werden kann.

Greylisting
Beim Greylisting weist das MailRelay eine E-Mail beim ersten Zustellversuch mit einem temporären Fehler ab. Wenn die E-Mail vom versendenden Mailserver innerhalb der „Greylisting-Gültigkeitszeit“, jedoch nach Ablauf der „Greylisting Sperrzeit“ erneut zugestellt wird, wird Sie sofort akzeptiert und an den Mailserver des Kunden weitergeleitet.
Das MailRelay identifiziert eine E-Mail an Hand der E-Mail-Adressen des Senders und des Empfängers und an Hand der IP-Adresse des absendenden Mailservers. Für eine akzeptierte E-Mail werden diese Parameter vom htp MailRelay in eine Whitelist übernommen, so dass bei einem erneuten E-Mailversand innerhalb der „Greylisting Whitelist-Zeit“ mit gleicher Absender-, Empfängeradresse und gleicher IP-Adresse des Mailservers die E-Mails sofort angenommen werden.
Durch dieses Verfahren werden E-Mail von SPAM-Bots, die keinen zweiten Zustellversuch nach angemessener Zeit vornehmen, nicht angenommen. Die Anzahl der SPAM-Mails wird hierdurch erheblich reduziert. Allerdings kann es je nach Konfiguration des versendenden Mailservers zu Verzögerungen bei der Zustellung kommen. Die Verzögerungen betragen in der Regel 15 Minuten bis maximal eine Stunde.

Block dynamic IP
Mailserver und Mailrelay-Server im Internet besitzen statische IP Adressen. Nur mit einer statischen IP Adresse ist gewährleistet, dass Mailserver nicht nur E-Mails versenden, sondern auch empfangen können. E-Mails von „Mailservern“ mit einer dynamischen IP Adresse ist in der Regel SPAM und wird generell geblockt.

Blocking High-SPAM
Eingehende E-Mails werden auf Wunsch des Kunden automatisch einer ersten SPAM Analyse unterzogen und hinsichtlich ihrer SPAM Wahrscheinlichkeit bewertet. Sollte die Wahrscheinlichkeit sehr hoch sein, so wird die E-Mail vom htp MailRelay nicht angenommen. Die SMTP-Verbindung wird mit einer entsprechenden Fehlermeldung beendet.

Header Kennzeichnung
Eingehende E-Mails werden auf Wunsch des Kunden automatisch einer detaillierten SPAM Analyse inkl. einer Textanalyse unterzogen und hinsichtlich ihrer SPAM Wahrscheinlichkeit bewertet. Die Bewertung wird in den Header der E-Mail wie folgt aufgenommen und kann auf dem Mailsystem des Kunden entsprechend ausgewertet werden.

Headerzeilen der SPAM-Analyse:

kein Spam:

```
X-Spam-Checker-Version: SpamAssassin on mail.htp-tel.de
X-Spam-Level:
X-Spam-Status: No, score=0.0 required=4.0
```

Spam:

```
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin on mail.htp-tel.de
X-Spam-Level: ****
X-Spam-Status: Yes, score=5.0 required=4.0
X-Spam-Report: […]
```

E-Mail Caching
Das htp MailRelay speichert E-Mails bei Nichterreichbarkeit des zuständigen nächsten Mailservers (Next-Hop) und versucht diese zu einem späteren Zeitpunkt erneut zuzustellen. Der nächste Mailserver ist bei eingehenden E-Mails der Mailserver des Kunden, der z.B. auf Grund einer Leitungsstörung oder eines Serverproblems nicht zur Verfügung steht. Bei ausgehenden E-Mails handelt es sich um den für die Empfängerdomain zuständigen Mailserver im Internet.
Die Speicherung erfolgt bei temporären SMTP-Fehlermeldungen des Mailservers (Fehlercode 4xx) oder bei Nichterreichbarkeit. Das htp MailRelay versucht regelmäßig die Zustellung im „Zustellintervall“. Nach einer bestimmten Zeit erhält der Absender eine Infomail, aus welchen Grund die E-Mail noch nicht zugestellt werden konnte. Nach Ablauf der „maximalen Speicherzeit“ sendet das htp MailRelay die E-Mail inkl. einer Fehlermeldung an den Absender zurück.

Limitierung der E-Mail Frequenz
Eine Begrenzung des E-Mail Durchsatzes verhindert, dass unkontrolliert massenhaft E-Mails vom Mailserver des Kunden versendet bzw. empfangen werden können. Sollten sich z.B. im Netz des Kunden mit Schadcode infizierte Rechner befinden, von denen eine SPAM- oder DOS-Attacke initiiert wird, so begrenzt das htp MailRelay den ausgehenden E-Mail-Versand. Das Risiko eines Imageschadens oder eines Blacklisteintrages wird hierdurch minimiert.
Bei einem SPAM-Angriff aus dem Internet auf kundeneigene Domains werden durch die Limitierung die Mailserver des Kunden vor einem Systemausfall durch Überlastung geschützt. Sollte eine wichtige E-Mail durch die Limitierung blockiert werden, so wird in der Regel der versendende Mailserver die Zustellung nach angemessener Zeit erneut vornehmen.
Alle ein- und ausgehenden E-Mails, die den angegebenen maximalen E-Mail Durchsatz überschreiten, werden mit einer temporären Fehlermeldung (Fehlercode 4xx) abgelehnt.