Dedizierte Mailserver

AGNITAS
e-mail & marketing automation

Dedizierte Mailserver – alles unter eigener Kontrolle

Auf Wunsch betreiben wir für Sie einen dedizierten Mailserver zum E-Mail-Versand. Die betriebsbereit konfigurierte Hardware wird von AGNITAS bereitgestellt und im Highend-Rechenzentrum gehostet. Durch den guten Ruf der AGNITAS profitieren Sie vom Whitelisting und somit von einer vorteilhaften Behandlung durch Spam-Filter.

Definition

Unter einem dedizierten Mail-Server (auch: SMTP-Server) versteht man einen Mail-Server, der Ihnen von AGNITAS zur exklusiven Nutzung zur Verfügung gestellt und betrieben wird.

Vorteile dedizierter Mailserver

Postfach-Anbieter überwachen beim eingehenden E-Mail-Verkehr auch die Reputation der IP-Adressen von Versand-Servern. Einen dedizierten Mailserver zu besitzen, bedeutet, dass Sie keine Störfaktoren oder eventuelle negative Einflüsse anderer Versender auf die Reputation der IP-Adresse dieses Servers haben. Dies beeinflusst die Zustellung, da die Reputation mit darüber entscheidet, ob Ihre E-Mails im Posteingang ankommen oder nicht.

Damit dieser Vorteil nicht zum Nachteil wird, falls ein Server ausfällt oder man auf eine Blacklist gelangt, hat AGNITAS verschiedene Schutzlevels eingerichtet:

Level 1 – Standard

Ein virtualisierter, dedizierter Server

Das Level1 ist das Basisangebot für dedizierte Mailserver. Es umfasst Bereitstellung, Administration und Überwachung der Server sowie einige Schutzvorkehrungen. Grundsätzlich empfehlen wir mindestens zwei Server, um durch technische Redundanzen Ausfallsicherheit zu erhalten.

Folgende Leistungen durch AGNITAS sind enthalten:

- ➜ Hosting und Betrieb der/s Mailserver/s
- ➜ Administration der Hard- und Software
- ➜ Tägliches Backup der Maildateien und des gesamten Betriebssystems
- ➜ Automatisierte Überwachung der Serverdienste (z.B. Mail Transfer Agent)
- ➜ Zustellungs-optimierende Konfiguration des Bounce-Management-Regelwerks (mehr in separatem Factsheet)
  - Laufende Pflege des Regelwerks für den Umgang mit Status-Rückmeldungen (z.B. Bounce Codes) durch empfangende Mailserver
  - Nutzung sogenannter Feedback-Loops großer Provider zur Spam-Reduzierung (Empfänger wird im EMM abgemeldet, wenn er im Postfach auf Spam klickt)
- ➜ Whitelisting der Server bei CSA, Signal Spam und Telekom
- ➜ Überwachung von ca. 100 Blacklists auf Server-Einträge und ggf. Delisting-Anträge für betroffene Server

Level 2 – inkl. Top10-Überwachung und Reporting

Ein virtualisierter, dedizierter Server

Das Level 2 ergänzt das vorherige Paket. Durch automatische Reports werden Sie zudem schnell auf Auffälligkeiten und Probleme hingewiesen.

Folgende Leistungen durch AGNITAS sind enthalten:

- ➜ Alle Leistungen des Level 1
- ➜ Tägliche E-Mail-Reports im CSV-Format mit Kennzahlen für Hardbounces, Softbounces und Annahmebestätigungen im Verhältnis zur Versandmenge für die Top10-Mailbox-Provider (auf Basis deren Top Level Domains, z.B. „.de“): AON, AOL, Bluewin, Freenet, GMail, GMX, Hotmail, T-Online, web.de, Yahoo
- ➜ Definition von Schwellwerten für die 3 Kennzahlen, ab denen eine Alarm-Mail an den Kunden versendet wird
- ➜ Kontakt-Historie am Empfänger mit Überprüfung von Bounce-Ursachen

Level 3 – Das Rundum-Sorglos-Paket

Ein virtualisierter, dedizierter Server

Das Level 3 bietet den maximalen Service und enthält alle Leistungen der vorherigen Pakete. Sie brauchen selbst nicht aktiv zu werden, AGNITAS geht Auffälligkeiten und Problemen nach.

Folgende Leistungen durch AGNITAS sind enthalten:

- ➜ Alle Leistungen des Level 2
- ➜ Proaktive Überwachung der E-Mails an die Top10-Mailbox-Provider hinsichtlich der Quoten für Hardbounces, Softbounces und Annahmebestätigungen auf Basis der Versandmenge
- ➜ Ursachenforschung bei außergewöhnlichen Abweichungen und Kommunikation mit dem Mailbox-Provider

Level-unabhängige EMM-Features

Darüber hinaus bietet Ihnen der EMM verschiedene Analysen und Statistiken, mit denen Sie selbst die Bounce-Entwicklung und Ursachen nachvollziehen können:

- ➜ Bounce-Statistik am Mailing (Hard- & Soft-Bounces) mit Analyse der Bounce-Gründe
- ➜ Top-Domain-Auswertung auch für Bounces am Mailing
- ➜ Automatischer Report mit Auswertung der Top-Bounce-Domains als PDF und CSV

Hosting im Highend-Rechenzentrum

Selbstverständlich stehen alle dedizierten Server in einem Highend-Rechenzentrum, das durch zahlreiche Vorkehrungen die Erreichbarkeit und Ausfallsicherheit sowie den Schutz der Server vor Fremdzugriff sicherstellt.

Wir bieten diesen Service für die Produkte EMM SaaS, EMM Inhouse* und EMM Xpress an.

* Bei EMM Inhouse wird das Bounce-Management-Regelwerk mit jedem Software Update aktualisiert.

Details zum Rechenzentrum

Energieversorgung:

- ≥ 99,999 % p. a. Verfügbarkeit für Energieversorgung
- AlwaysOn-Technologie für redundante USV-Versorgung von A- und B-Feed
- Notstrom über Netzersatzanlage mit Kraftstoffvorrat für mindestens 72 Stunden unter Volllast
- Während des Betriebes auffüllbare Kraftstofftanks (Nachbetankung vor Erreichen des Minimalfüllstandes gesichert durch 24/7-Liefervertrag)
- 100 % Nutzung regenerativer Energie

Klimatisierung:

- ≥ 99,999 % p. a. Verfügbarkeit für Klimatisierung
- Trennung von Kalt- und Warmbereich durch Warmgangeinhausung und Warmluftseparierung über doppelte Decke

Brandschutz:

- Flächendeckende Brandmeldeanlage und Brand-Frühesterkennung mit direkter Aufschaltung zur örtlichen Feuerwehr
- Zonengenaue Löschung mittels Stickstoff-Inertisierung (N2) und anschließende zeitlich unbeschränkte Sauerstoffabsenkung
- Einsatz von nichtbrennbaren oder nur schwer entflammbaren Materialien
- Bauliche Maßnahmen nach Feuerwiderstandsklasse F90

Sicherheit:

- Videoüberwachung mit Archivierung
- 24/7 Sicherheitsdienst vor Ort
- Biometrische Zutrittskontrolle mit 24/7-Zutritt über Transponderkarte
- Raum-in-Raum-Konzept trennt IT-Flächen von Außenwänden
- Perimeterschutz mit Sicherheitszaun und Vereinzelungsschleusen
- Rack-Überwachung mit leistungsfähigen Monitoring-Systemen
- Separate Cages innerhalb des Rechenzentrums mit eigener Absicherung, Zugangs- und Einbruchmeldesystem verfügbar

Zertifizierungen und Testierung:

- ISO/IEC 27001: Informationssicherheitsmanagementsystem
- ISO 27001: Zertifizierung auf der Basis von IT-Grundschutz
- ISO/IEC 20000-1: Servicemanagementsystem
- ISO 9001: Qualitätsmanagementsystem
- EN 50600: Bau und Betrieb sicherer Rechenzentren
- VdS 3406: Objektspezifisches Sicherheitsmanagementsystem
- PCI DSS: Payment Card Industry Data Security Standard
- ISAE 3402 Typ II: Internes Kontrollsystem auf der Basis von COBIT 5