Leistungsbeschreibung Secure Mail Services für AppAgile

1 Leistungsumfang Secure Mail Services

Mit Secure Mail Services bietet T-Systems International GmbH (im folgenden „T-Systems“) einen erweiterten Schutz für die eingehenden und ausgehenden E-Mails. Darunter zählen im wesentlichen zwei Sicherheitseigenschaften: Viren- und Spamschutz.

Die Leistungen werden als zentraler Service im Zusammenhang mit der AppAgile Plattform angeboten.

1.1 Virenschutz

Je nach gewähltem Profil werden die ein- und ausgehenden E-Mails nach unerwünschter Software (Viren, Würmer, Trojaner, etc.) untersucht. Die T-Systems setzt für diese Überprüfung mindestens zwei unterschiedliche Viren-Scanner von marktführenden Herstellern ein.

GEFILTERTE INHALTE

Der Virenscanner scannt die E-Mails und deren Dateianhänge auf Viren, Würmer und Trojaner und filtert diese aus. Weiterhin können Archive in gängigen Formaten bearbeitet werden. Eine Prüfung verschlüsselter oder anderweitig zugriffsgeschützter E-Mails, kann nicht durchgeführt werden. E-Mails mit erkannten Viren werden aus sicherheitstechnischen Gründen nicht zugestellt, sondern werden mit entsprechender Fehlermeldung abgewiesen. Somit können virenbefallene E-Mails das Netz des Kunden nicht erreichen und bewahren das Kundennetz vor Schaden.

AKTUALISIERUNG DER VIRENSIGNATUR

Die Aktualisierung der Virensignaturen im System der T-Systems erfolgt stündlich. T-Systems übernimmt keine Gewährleistung für die Entdeckung sämtlicher Schadprogramme, da deren Erkennung auf der zeitnahen Aktualisierung der Virensignaturen nach Bekanntwerden der Schädlinge beim Hersteller der Antivirensoftware basiert.

1.2 Spamschutz

T-Systems verwendet unterschiedliche Verfahren, um eine E-Mail als Spam zu identifizieren. Darunter zählen Methoden, die auf „Recurrent Pattern Detection“ basieren. Ziel ist es den Empfang von unerwünschten Massenmails zu reduzieren bzw. diese mittels bestimmter Merkmale zu erkennen und kenntlich zu machen.

- Alle durchlaufenden Mails werden auf Spam-Verdacht überprüft und gekennzeichnet. Die Kennzeichnung erfolgt in der Betreffzeile der E-Mail.
- Die E-Mails erhalten desweiteren eine extra Headerzeile, in der ihre Spamwahrscheinlichkeit vermerkt ist und auf die im Mailclient gefiltert werden kann.
- E-Mails werden nicht weiter verändert und weitergeleitet.
- E-Mails werden nur RFC-Konform gelöscht.
- E-Mails werden nur RFC-Konform geblockt.

E-Mails werden zu dem Zeitpunkt, an dem sie den betreffenden Server bei T-Systems erreichen, aufgrund typischer Merkmale ggf. als Spam erkannt. Trotz aller Vorsichtsmaßnahmen kann es im Einzelfall vorkommen, dass E-Mails versehentlich als Spam erkannt werden. Der Kunde hat daher regelmäßig im Posteingang zu überprüfen, ob ggf. als Spam-Mail gekennzeichnete E-Mail tatsächlich Spam-Mail war. T-Systems haftet insofern nicht für verlorene Daten.

QUARANTÄNE FUNKTION

Der Quarantäne-Modus ermöglicht die automatische Filterung der Spam-Mails in der Mailplattform, so dass Info-Dienste wie z.B. Blackberry nicht mit diesen belastet werden. Die als Spam erkannten E-Mails werden, soweit konfiguriert, in entsprechenden Postfächern vorgehalten. Die genaue Anleitung über die Funktionsweise wird im Mailbox-Handbuch dargestellt.

Zusätzliche Informationen:

- Der Zugriff zum Quarantänepostfach erfolgt über eine gesicherte Verbindung (https).
- Einmal täglich wird eine Zusammenfassung neuer in die Quarantänepostfach eingelieferter Mails persönlich zugestellt. Aus dieser Mail heraus sind weitere Aktionen möglich.
- Die Quarantänemailbox befindet sich auf den Servern der T-Systems

Durch die regelmäßige Zusendung eines Spamreports behält der Benutzer täglich den Überblick über Eingänge in seine persönliche Quarantänemailbox. Aus dieser Mail heraus ist es auch möglich, sich Mails zuzustellen oder zu löschen, ohne sich an der Quarantänebox anmelden zu müssen.

1.3 Individuelle Einstellung durch den Endbenutzer

Mit Beauftragung erhält der Kunde Zugriffsdaten für das Administrations-Portal und kann die Filterung von Junk-E-Mails individuell konfigurieren. Webgestützte Verwaltungswerkzeuge erleichtern einzelnen Usern die Konfiguration von individuellen Black- und White-Listen vorzunehmen. Durch diese Funktionen erhält der Endbenutzer mehr Verantwortung, kann seine Privatsphäre besser schützen und selbst entscheiden, welche E-Mails als Spam betrachtet werden. 3.1. Black- und Whitelisten

Für jede Domain, aber auch einzelne E-Mailadressen können spezifische Black-Listen konfiguriert werden. Diese verhindern E-Mail-Missbrauch und dienen der Vorbeugung gegen DOS-Angriffe. Ebenso individuell zu konfigurierende White-Listen dagegen sorgen dafür, dass „False-Positives“ reduziert werden und verhindern die versehentliche Klassifizierung wichtiger E-Mails als unerwünschte Post.

RBL (REALTIME BLACK LISTS)

E-Mails von Servern, die auf RBL's gelistet sind, können in der Betreffzeile gekennzeichnet oder geblockt werden, aktivierbar über das webgestützte Verwaltungswerkzeug.

FORCED TLS

Um das Risiko zu minimieren, dass E-Mails mit bestimmten Kommunikationspartnern auf dem Übertragungsweg nicht mitgelesen werden, ist es möglich zu bzw. von bestimmten Domänen E-Mails nur mit Hilfe eines mit TLS gesicherten Kanals zu übertragen. Eine Übertragung der E-Mails in Klarschrift zu den gewünschten Kommunikationspartnern wird dann nicht mehr akzeptiert. Hierbei werden nur die vom BSI empfohlenen Cipher verwendet.

ATTACHMENT BLOCKING

E-Mails mit bestimmten Anhängen können grundsätzlich abgelehnt werden.

SPAM-KENNZEICHNUNG

Die Kennzeichnung einer Spam in der Betreffzeile kann individuell durch den Kundenadministrator angepasst werden.

SPAM-BLOCKING

Der Kundenadministrator kann für bestimmte Domains oder E-Mailadressen die Zustellung von Spams blockieren.

1.4 Verfügbare Profile

T-Systems bietet vier unterschiedliche Profile an:

- Profil 1: Nur die eingehenden E-Mails werden überprüft.
- Profil 2: Ein- und ausgehende E-Mails werden überprüft.
- Profil 3: Eingehende E-Mails werden überprüft inkl. Quarantäne Funktionalitäten.
- Profil 4: Ein und ausgehende E-Mails werden überprüft inkl. Quarantänefunktionalitäten.

Über die angebotenen Profile wird die Möglichkeiten eröffnet, die Secure Mail Service nach individuellen Anforderungen auszuwählen.

1.5 Bereitstellungsprozess

Nach Beauftragung erhält der Kundenadministrator eine E-Mail mit Zugangsdaten zum Administrations-Portal sowie weitere Informationen, die für die Einrichtung des Service notwendig sind.

1.6 Reporting (nur in Verbindung mit Quarantäne Funktion)

Über ein Webportal erhält der Kunde jederzeit Zugriff auf seine Reportingdaten. Des weiteren wird ein monatlicher Report als Servicebericht in PDF zur Verfügung gestellt. Dieser umfasst:

- Anzahl der E-Mails, die geprüft wurden,
- Anzahl der E-Mails, die als Spam gekennzeichnet wurden,
- Anzahl der E-Mails, die über Greylisting abgewiesen wurden,
- Anzahl der E-Mails, die Viren enthielten.

Die Reports werden ausschließlich an berechtigte Personen des Kunden ausgehändigt. Der Berechtigungs-kreis ist vom Auftraggeber bekannt zu geben.

1.7 Archivierung der Daten

Logdateien werden 30 Tage ab dem Zeitpunkt des Entstehens vorgehalten. Sobald sich die gesetzlichen Vorgaben ändern, wird die Archivierungsdauer der Logdateien entsprechend angepasst.

1.8 Kundenservice

Das User Help Desk ist telefonisch unter +49 180 5242 510 erreichbar und steht 24x7 zur Verfügung.

1.9 Verfügbarkeit und Wartung

VERFÜGBARKEIT

T-Systems gewährleistet pro Jahr eine Verfügbarkeit von 99,98% für den Service, sowie eine Verfügbarkeit von 99,5% für das Administrations-Portal.

WARTUNGSFENSTER

Zu Wartungszwecken – insbesondere für Änderungen und Aktualisierungen der Server-Konfiguration – können die Leistungen außer Betrieb genommen werden (Wartungsfenster). Die T-Systems wird die Kunden rechtzeitig, bevor ein Wartungsfenster in Anspruch genommen wird, darüber informieren. Die Zeiten der Wartungsfenster fließen nicht in die Berechnung einer Verfügbarkeit ein.

2 Mitwirkungspflichten

Der Kunde stellt notwendige Informationen termingerecht und vollständig zur Verfügung. Die Verantwortung für den rechtskonformen Umgang der Lösung in Bezug auf den End-User eines E-Mail-Postfaches obliegt dem Kunden.

2.1 Secure Mail Services (Recipient Check)

Der Kunde stellt T-Systems aktuelle Listen, mit E-Mailadressen der zu schützenden Postfächer zur Verfügung, die in das System importiert werden können.

Ein automatisierter Abgleich ist möglich und kann vom Kunden selbst durchgeführt werden. Hierzu stellt T-Systems entsprechende Scripts zur Verfügung, die in die Kundeninfrastruktur eingearbeitet werden können.

Der Kunde darf bei Nutzung des Outbound-Service vorsätzlich keine Spams oder mit Viren befallene Mails über Secure Mail Services versenden. T-Systems behält sich vor vom Kunden versendete Spams oder mit Viren befallene Mails zu blocken. Der Kunde hat dafür Sorge zu tragen, dass nicht Mails von Dritten den Outbound-Service nutzen.

2.2 Änderung des MX-Records

Vorgesehene MX-Records, an die die E-Mails weitergeleitet werden müssen, damit der Spamschutz für den Kunden aktiviert werden, lauten z. Zt.

- MX10 Secure101.t-systems.com
- MX20 Secure201.t-systems.com
- MX50 Secure501.t-systems.com

Diese Änderung führt der Kunde aus oder veranlasst es bei seinem Service Provider. Weitere MX-Records dürfen nicht eingetragen sein. Weitere MX-Records können zur Verschlechterung des Secure Mail Services führen und somit die Spam- und Viruserkennung negativ beeinflussen.

Bei technischen Änderungen/Erneuerungen kann eine Änderung der MX-Records notwendig werden. T-Systems wird den Kunden rechtzeitig über entsprechende Änderung informieren. Die notwendige Änderung der MX-Record führt der Kunde aus, oder veranlasst sie bei seinem Service Provider.

3 Datenschutz

Die T-Systems International GmbH betreibt im Rahmen des Betriebs in Rechenzentren Datenverarbeitung im Auftrag. Um den Service erbringen zu können sind E-Mail-Inhalte und dazugehörige Verkehrsdaten durch den Leistungserbringer einsehbar und damit verarbeitbar bzw. kann ein Zugriff auf personenbezogene Daten des Auftraggebers/Kunden dabei nicht ausgeschlossen werden. Gemäß § 11 Bundesdatenschutzgesetz (BDSG) ist jeweils der Auftraggeber für die Einhaltung der Vorschriften des BDSG und anderer bereichsspezifischer Regelungen zum Datenschutz verantwortlich, wenn personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt werden. Zu diesem Zweck kann der Auftraggeber/Kunde mit der T-Systems eine Vereinbarung abschließen.

4 Vertragslaufzeit

Die Mindestvertragslaufzeit entspricht der Laufzeit des Vertrages über die AppAgile Plattform.