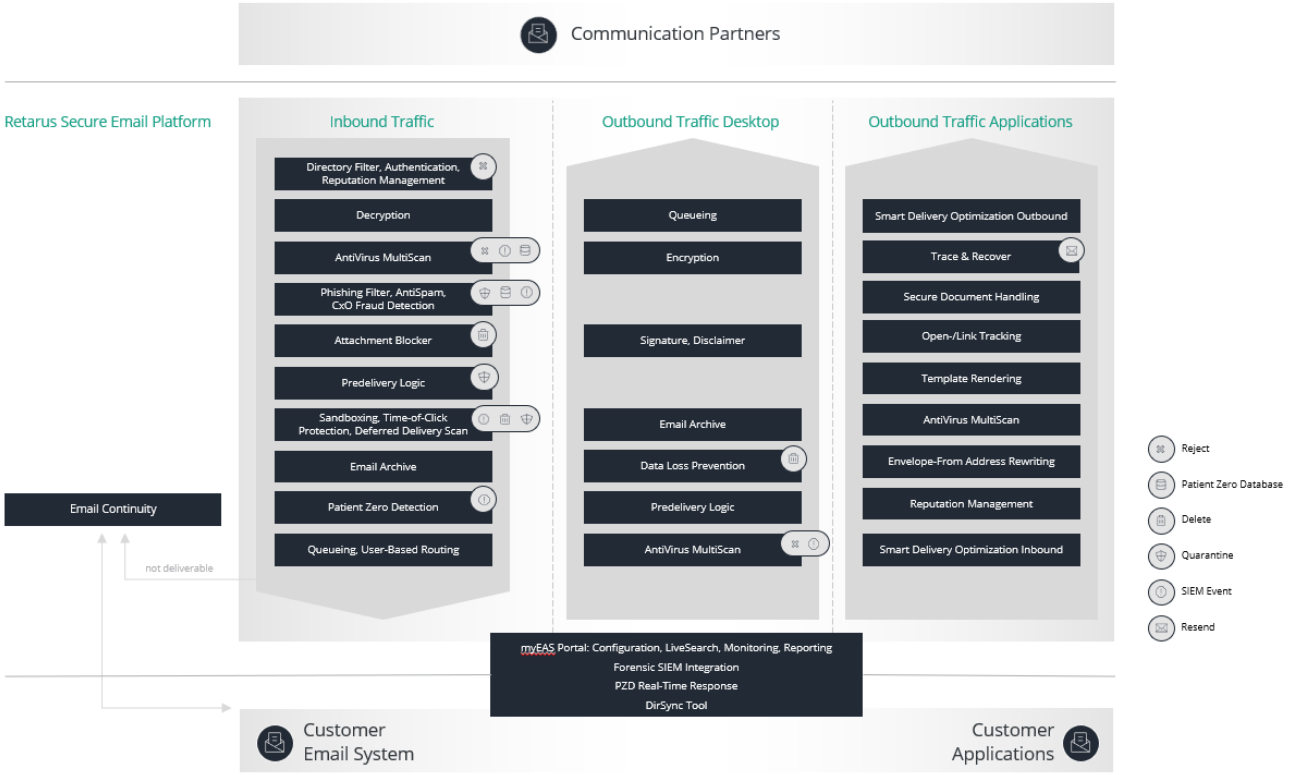
Service-Beschreibung und Mitwirkungspflichten
Retarus Secure Email Platform

Die Retarus Secure Email Platform kombiniert umfassenden Schutz, Advanced Threat Protection, die patentierte Postdelivery Protection-Funktion Patient Zero Detection® und ein durch Predelivery Logic erweitertes Email Routing mit Email Encryption und Email Continuity. Zusätzlich lassen sich mit den Retarus Transactional Email Services Business-Applikationen an die Plattform anbinden.

Der Produktumfang unterteilt sich in die Kategorien Email Cloud Gateway, Email Security, Email Compliance und Email Infrastructure.

Inhalt

Systemarchitektur Retarus Secure Email Platform



Email Cloud Gateway

Das Retarus **Email Cloud Gateway** stellt Funktionalitäten für die Verwaltung und den Schutz des SMTP-Nachrichtenverkehrs zur Verfügung. Der Service kann eigenständig genutzt werden oder durch weitere Module der Retarus Secure Email Platform erweitert werden.

Das Email Cloud Gateway beinhaltet die nachfolgenden Funktionalitäten:

Directory Filter / Inbound Reputation Management

Der Directory Filter weist diejenigen Emails RFC-konform (Reject-Methode) ab, die an Empfänger gerichtet sind, welche im Retarus Enterprise Administration Services Portal (EAS-Portal) nicht konfiguriert sind. Die Konfiguration und Aktualisierung kann entweder manuell durch den Kunden selbst über das EAS-Portal oder automatisiert durch Directory-Synchronisation in einem von Retarus vorgegebenen Format mit Adressbüchern und Verzeichnissen des Kunden erfolgen.

Das Inbound Reputation Management ergänzt den Directory Filter und überprüft die Reputation von Absendern eingehender Emails. Ob ein Absender autorisiert wird, wird anhand der Prüfmechanismen SPF (Sender Policy Framework) und DKIM (DomainKeys Identified Mail) validiert. Klassifizierte Emails, deren Validierung fehlgeschlagen ist, werden gemäß der Kundenkonfiguration im EAS-Portal behandelt bzw. – sofern vom Kunden aktiviert – nach der Vorgabe in der DMARC-Policy (Domain-based Message Authentication, Reporting & Conformance) des Domain-Inhabers (Absender) weiterverarbeitet (Aktionen: None, Quarantine, Reject).

Hinweis: Die Nutzung von DMARC setzt das Routing auf einen dedizierten MX-Record der Retarus voraus.

AntiVirus Multiscan 2-fach

Retarus überprüft Nachrichten beim Empfang und – soweit vereinbart – auch beim Versand auf Virenbefall. Die Überprüfung erfolgt mit zwei Virenscannern verschiedener Anbieter nach Wahl von Retarus. Sobald die Hersteller Updates oder neue Releases bereitstellen, wird Retarus diese unverzüglich zur Virenüberprüfung verwenden. Sofern ein Virenbefall festgestellt wird, löscht Retarus die mit Viren befallenen Nachrichten. Die Adressaten der infizierten Emails und/oder entsprechend hinterlegte Administratoren werden im Rahmen des Quarantäne-Managements informiert.

DHA Protection

Schutz vor DHA-Angriffen (Directory Harvest Attack) für die vom Domain Inhaber gewählte(n) Email-Domain(s). Nachrichten an ungültige Empfänger innerhalb der betroffenen Domain werden abgelehnt. Der Empfang weiterer Nachrichten an ungültige Empfänger wird durch eine Drosselung des identifizierten Senders dieser Nachrichten eingeschränkt.

Backscatter Protection

Schutz vor dem Missbrauch zum Versand automatisch generierten Bounce-Nachrichten (Backscatter). Als Backscatter bezeichnet man die unautorisierte Nutzung einer gültigen Absender-Email-Adresse einer anderen Person für Spam-Kampagnen. In diesem Fall kann es vorkommen, dass die empfangenden Email-Server der Adressaten dieser Nachrichten eine große Anzahl von Zustellungsstatus-Benachrichtigungen (z. B. wenn die Empfängeradresse nicht existiert) an die gültige Email-Adresse der Person senden, die unautorisiert als Absender verwendet wurde. Die Zustellung erfolgt nicht an den eigentlichen Absender.

Die Backscatter Protection erkennt eine erhöhte Anzahl solcher automatisch generierten Nachrichten, filtert diese heraus, verhindert deren Zustellung und isoliert sie in der persönlichen Quarantäne des betroffenen Empfängers. Diese Nachrichten werden in der persönlichen Quarantäne als NDR-Spam markiert hinterlegt.

Email Back-Up / Queuing

Retarus übernimmt bei Unzustellbarkeit der für den Kunden eingehenden Nachrichten eine Zwischenspeicherung von maximal 96 Stunden. Im Fall der endgültigen Unzustellbarkeit erhält der Absender der Nachricht per Email eine Benachrichtigung über die Unzustellbarkeit. Retarus versucht innerhalb dieser 96 Stunden die Zustellung in regelmäßigen kurzen Abständen. Endet die Unzustellbarkeit innerhalb dieses Zeitraumes, werden die eingegangenen Nachrichten paketweise von Retarus weitergeleitet.

Large Email Handling

Entsprechend der vom Kunden definierten Größenbeschränkungen für den Empfang großer Emails werden diese ab der definierten Größe nicht unmittelbar an die Postfächer des Kunden zugestellt, sondern bei Retarus zum Download bereitgestellt. Der Empfänger wird über den Empfang einer solchen – sofern konfiguriert – benachrichtigt. Der Download erfolgt über einen HTTP-Link mit vereinfachter Benutzerauthentifizierung (OneClick-Token-Login).

User-based Routing

Im Rahmen des User-based Routings stellt Retarus Emails für definierte Empfänger beim Kunden innerhalb einer Domain an spezifische Ziel-Server zu.

Email Signature / Disclaimer

Der Kunde hat die Möglichkeit, im Enterprise Administration Services Portal (EAS-Portal) Signaturen oder Disclaimer zu hinterlegen. Retarus hängt den ausgehenden Email-Nachrichten des Kunden die über das EAS-Portal erstellten Signaturen oder Disclaimer an. Bei der Verwendung von Platzhaltern werden diese mit Daten aus der Directory Synchronisation befüllt.

Email Live Search

Mit Email Live Search können alle ein- und ausgehenden Nachrichten in Echtzeit nachverfolgt werden. Es lässt sich für jede Email nachvollziehen, ob und mit welchem Virus sie infiziert war und welche weiteren Filter und Regeln angewendet wurden.

Access Management

Im Retarus Enterprise Administration Services Portal lassen sich Zugriffsrechte für einzelne Administratoren gemäß den Anforderungen des Kunden vergeben, z. B. mit unterschiedlichen Zugriffsrechten für bestimmte Länder, Niederlassungen, Domains oder Abteilungen.

Email Security

Retarus Email Security schützt Email-Infrastrukturen vor Malware wie Viren, Spam, Phishing-Mails, Ransomware und weiteren digitale Bedrohungen. Die mehrstufigen Filtermethoden werden laufend aktualisiert und optimiert. Die Datenverarbeitung erfolgt in Retarus-eigenen Rechenzentren nach den jeweils geltenden Datenschutzregeln.

AntiVirus Multiscan 2-fach

Retarus überprüft Nachrichten beim Empfang und – soweit vereinbart – auch beim Versand auf Virenbefall. Die Überprüfung erfolgt mit zwei Virenscannern verschiedener Anbieter nach Wahl von Retarus. Sobald die Hersteller Updates oder neue Releases bereitstellen, wird Retarus diese unverzüglich zur Virenüberprüfung verwenden. Sofern ein Virenbefall festgestellt wird, löscht Retarus die mit Viren befallenen Nachrichten. Die Adressaten der infizierten Emails und/oder entsprechend hinterlegte Administratoren werden im Rahmen des Quarantäne-Managements informiert.

AntiVirus Multiscan 4-fach

Wie AntiVirus Multiscan 2-fach, jedoch erfolgt die Überprüfung auf Virenbefall mit vier Virenscannern unterschiedlicher Anbieter.

External Sender Visibility Enhancement

External Sender Visibility Enhancement kennzeichnet eingehende Nachrichten, die im Absender eine dem Kunden zugeordnete Absenderdomäne verwenden. Zur Validierung des Absenders wird das Header-Feld MIME-FROM herangezogen. Eingehende Nachrichten werden innerhalb der Retarus-Infrastruktur mit vordefinierten Unicode-Icons (Symbolen) markiert, bevor sie an die Infrastruktur des Kunden übergeben werden. Die Markierung erfolgt im Absenderfeld des „friendly name“.

AntiSpam-Management und Phishing-Filter (Inbound)

Die bei Retarus eingehenden und für den Kunden bestimmten Nachrichten werden durch die von Retarus jeweils eingesetzten Spamfilter untersucht, mit einer SPAM-Wahrscheinlichkeit versehen und nach den kundenindividuell eingestellten Schwellenwerten als „potenzieller Spam“ identifiziert. Die als „potenzieller Spam“ eingestuften Nachrichten werden nicht unmittelbar zugestellt und gemäß der Konfiguration im Quarantäne-Management behandelt. Alternativ können als SPAM erkannte Nachrichten auf Wunsch des Kunden entsprechend gekennzeichnet und zugestellt werden („tag and deliver“). Retarus setzt dabei verschiedene Filter-, Muster-, Erkennungsverfahren und Technologien ein. Der spezielle Phishing-Filter gleicht in eingehenden Emails enthaltene Links mit spezialisierten Quellen für bekannte Phishing-URLs ab. Die Kenntnisnahme und Weiterverarbeitung der quarantinierten bzw. gekennzeichneten Nachrichten obliegen dem Kunden und den von ihm bestimmten Anwendern.

AntiSpam-Management und Phishing-Filter (Outbound)

Vergleichbar mit dem Retarus AntiSpam-Management und Phishing Filter (Inbound) kommt auch im Outbound-Kanal die bekannte Spam-Filter-Technologie von Retarus zum Einsatz. Jeder ausgehenden Email wird dabei eine SPAM-Wahrscheinlichkeit zugewiesen. Bei Überschreitung eines definierbaren Schwellenwerts (standardmäßig 60 Prozent) stehen je nach Konfiguration verschiedene Aktionen zur Verfügung, welche sich auf spezifische Sicherheitsrichtlinien abstimmen lassen. Dazu zählen Ablehnen temporärer Fehler ("Tempfail") oder stilles Verwerfen. Die Möglichkeit zur individuellen Konfiguration erstreckt sich auf alle Hierarchieebenen und können sowohl auf Kunden-, Domain-, Profil- als auch auf Benutzerebene abgestimmt werden. Um die Funktion zu aktivieren, wenden Sie sich bitte an das Retarus Support-Team.

Attachment Blocker

Die Zustellung bestimmter Email-Anhänge (Attachments) kann entsprechend einer vom Kunden getroffenen Konfiguration unterbunden werden. Zu blockierende Attachments lassen sich anhand von Datei-Extensions (z. B. exe, mp3, zip) sowie anhand des jeweiligen MIME-Types bestimmen. Der Dateianhang einer eingehenden Email wird entweder gelöscht und nur der Mail-Body an den Empfänger zugestellt, oder es wird eine Kopie der originalen Email mit Anhang an eine voreingestellte Mailbox (z. B. Administrator) gesendet. Empfänger können mit konfigurierbaren Benachrichtigungen über gelöschte Attachments informiert werden.

Outbound Recipient Restriction

Ausgehende Emails, die von Retarus verarbeitet werden, dürfen standardmäßig bis zu 600 Empfängeradressen haben. Überschreitet eine Email diesen Schwellenwert, weist Retarus sie für die überzähligen Empfänger zurück. Die Form der Benachrichtigung hängt von der Konfiguration Ihres Email-Servers ab. Mit der Funktion *Outbound Recipient Restriction* können Sie die maximale Anzahl von Empfängern für ausgehende Emails individuell (0-600) festlegen. Das Überschreiten des konfigurierten Limits kann je nach Ihren Einstellungen ein Ablehnen der Nachricht, ein temporärer Fehler ("Tempfail") oder ein stilles Verwerfen ausgelöst. Diese Funktion zielt darauf ab, die Aufdeckung von Identitäten ("Identity Exposure") zu verhindern sowie eine effizientere Verwaltung zu ermöglichen. Die Funktion kann auf allen Hierarchieebenen (d.h. Kunde, Domain, Profil, Benutzer) konfiguriert werden. Zur Aktivierung ist die Unterstützung durch das Retarus Support-Team erforderlich.

Outbound Size Restriction

Ausgehende Emails, die von Retarus verarbeitet werden, dürfen standardmäßig eine Größe von bis zu 250 MB (256000 kB) haben. Mit der Funktion *Outbound Size Restriction* können Sie diesen Wert bei Bedarf noch weiter begrenzen. Das Überschreiten des konfigurierten Limits kann je nach Ihren Einstellungen zum Ablehnen, einem temporären Fehler ("Tempfail") oder einer stillen Verwerfung der Nachricht führen. Die Funktion lässt sich auf allen Hierarchieebenen konfigurieren (d.h. Kunde, Domain, Profil, Benutzer). Zur Aktivierung dieses Features ist zunächst die Unterstützung durch das Retarus Support-Team erforderlich.

Deferred Delivery Scan

Im Rahmen von Deferred Delivery Scan (DDS) werden spezifische Dateianhänge einer weitergehenden Analyse mittels zusätzlicher Re-Scan-Vorgänge unterzogen. Durch diese erneuten Scans mit dann aktuelleren Signaturen kann die Zustellung von schädlichen Inhalten, die zum ersten Scan-Zeitpunkt noch nicht erkannt wurden, mit höherer Wahrscheinlichkeit verhindert werden. Sofern ein Virenbefall festgestellt wird, löscht Retarus die entsprechenden Nachrichten und informiert gemäß der Konfiguration im Quarantäne-Management. Da DDS zu einer verzögerten Zustellung der eingehenden Emails führt, gelten ggf. bezüglich Zustellungszeiten vereinbarte Service-Levels insoweit nicht.

Time-of-Click Protection

In Emails enthaltene Links werden automatisiert umgeschrieben (URL-Rewriting). Wenn Empfänger auf entsprechende Links klicken, werden diese auf Phishing-verdächtige Zieladressen überprüft. Ist die Zielseite nicht als Phishing-Seite bekannt, erfolgt eine direkte Weiterleitung. Handelt es sich bei der Zielseite um eine Phishing-Seite, wird eine Sicherheitswarnung angezeigt. Nach Abkündigung des Dienstes können entsprechende Links jedenfalls nicht mehr unmittelbar aufrufbar sein.

CxO Fraud Detection

CxO Fraud Detection verwendet Algorithmen, die „From-Spoofing“ und „Domain-Spoofing“ identifizieren, um gefälschte Absenderadressen (z. B. hochrangiger Vorgesetzter) zu erkennen. Als CxO Fraud eingestufte Nachrichten werden gemäß der Konfiguration im Quarantäne-Management behandelt.

Sandboxing

Beim Sandboxing werden spezifische Dateianhänge einer weitergehenden Analyse unterzogen. Attachments, die potenziell schädliche Inhalte enthalten können, werden in einer virtuellen Maschine ausgeführt und auf ungewöhnliches Verhalten überprüft. Für diese Überprüfung nutzt Retarus die Sandbox-Lösungen eines spezialisierten Drittanbieters. Sofern ein Befall mit schädlichen Inhalten festgestellt wird, werden die entsprechenden Nachrichten gemäß der Konfiguration im Quarantäne-Management behandelt. Da Sandboxing u. a. abhängig von der Dateigröße, dem Dateityp, und der Anzahl der Dateianhänge zu einer verzögerten Zustellung der eingehenden Emails führen kann, gelten ggf. bezüglich Zustellungszeiten vereinbarte Service-Levels insoweit nicht.

Patient Zero Detection®

Patient Zero Detection® erstellt bei Eingang der an die Empfänger des Kunden gerichteten Emails einen digitalen Fingerabdruck („Hash“) aller Dateianhänge und Links. Wenn die von Retarus eingesetzten Virenscanner zu einem späteren Zeitpunkt in einem gleichartigen Attachment oder Link schädliche Inhalte erkennen, lassen sich auch Empfänger bereits zugestellter, potenziell schädlicher Nachrichten frühzeitig identifizieren. Die Administratoren des Kunden und je nach Beauftragung auch direkt die Empfänger dieser Nachrichten werden in einem solchen Falle unverzüglich informiert. Der Kunde wird dadurch in die Lage versetzt, schnellstmöglich Maßnahmen zur Entfernung des Schadcodes aus seiner Infrastruktur oder zur Verhinderung der Ausbreitung von Schadcode zu ergreifen.

Patient Zero Detection® Real-Time Response

Mit Patient Zero Detection® Real-Time Response stellt Retarus eine Software bereit, die der Kunde innerhalb seiner Infrastruktur betreiben kann. Die Software verarbeitet automatisiert Nachrichten, die nach Zustellung in das Empfängerpostfach durch die Patient Zero Detection® als schadhaft identifiziert wurden. Diese können anschließend automatisch aus dem Empfängerpostfach entfernt werden. Voraussetzung für den Betrieb von Patient Zero Detection® Real Time Response ist die Nutzung der „Retarus Forensic SIEM Integration“ sowie die Anbindung an Microsoft Exchange Online oder on-premises. Für Patient Zero Detection® Real-Time Response gelten gesonderte Nutzungsbedingungen, die der Kunde im Falle der Installation bzw. Nutzung der Software zu berücksichtigen und einzuhalten hat. Diese Nutzungsbedingungen sind sowohl im EAS-Portal als auch im Web einsehbar.

Quarantäne-Management

Im Rahmen des Quarantäne-Managements wird dem Kunden ein Email-Security-Report (Digest) zur Verfügung gestellt. Die Zeitpunkte, an denen der Digest jeweils zugestellt werden soll, lassen sich je nach Kundenwunsch einheitlich für alle Anwender oder individuell vom einzelnen Anwender selbst festlegen. Der Digest enthält je nach beauftragten Optionen eine kombinierte Übersicht über Emails, die seitens Retarus aufgrund von Graymail (z. B. Newsletter), Viren, Spam, Phishing, Sandboxing, CxO Fraud, etc. innerhalb der eingestellten Periode für das jeweilige Postfach quarantiniert oder gelöscht wurden. Quarantinierte Nachrichten sind kundenseitig per Klick auf den entsprechenden Eintrag im Digest innerhalb des eingestellten Zeitraums (maximal 30 Tage) abrufbar. Sofern vom Kunden so voreingestellt, können die einzelnen Empfänger via Online-Zugriff auf ihre Quarantäne zugreifen und individuelle Einstellungen festlegen. Administratoren des Kunden können Quarantäne-Einstellungen systemweit im EAS-Portal konfigurieren.

Forensic SIEM Integration

Im Rahmen der Forensic SIEM Integration stellt Retarus eine Schnittstelle zur Verfügung, über die der Kunde Informationen zu Ereignissen und Ergebnissen (Event bzw. Log) abrufen kann, die sich aus der Überprüfung ein- und ausgehender Nachrichten innerhalb der Retarus Email Security ergeben. Diese kann er als zusätzliche Datenquelle in ein bestehendes SIEM-Tool einbinden. Events, die dem Kunden bereitgestellt werden, hängen von den gebuchten Optionen ab und sind verfügbar für:

- AntiVirus Multiscan (inbound und outbound)
- Sandboxing
- CxO Fraud Detection
- Patient Zero Detection®
- Outbound emails, allgemein
- Inbound emails, allgemein

Email Compliance

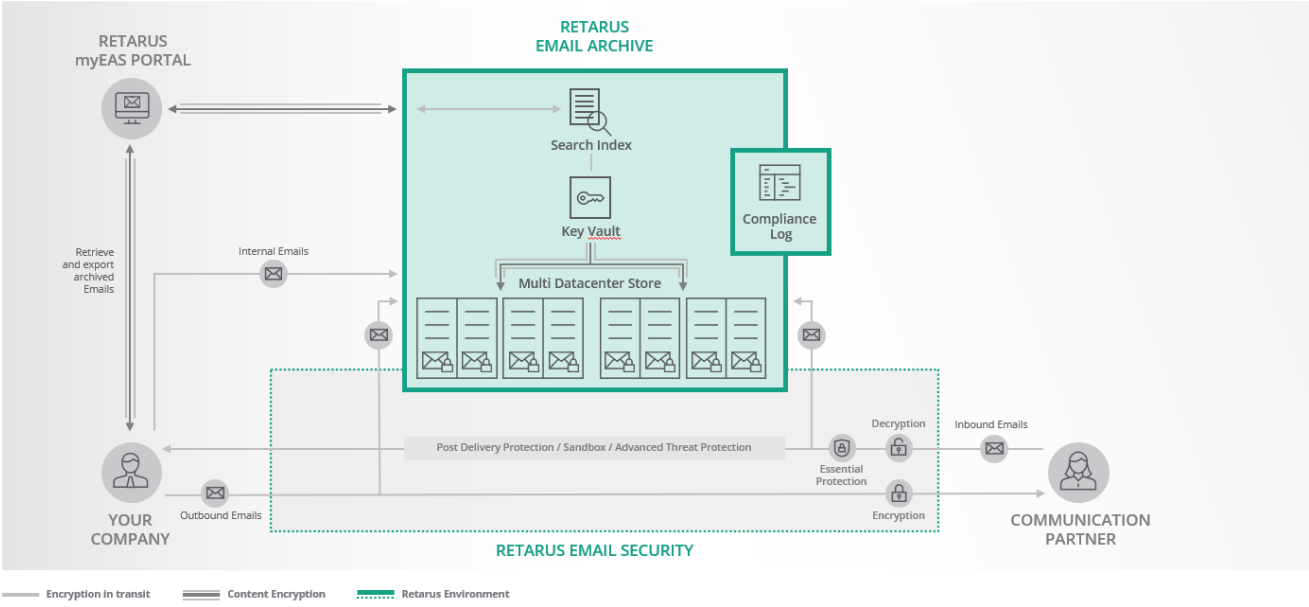
Retarus Email Archive

Das **Retarus Email Archive** speichert ein- und ausgehende Email-Kommunikation automatisch, zuverlässig, und langfristig. Bei Bedarf kann die interne Email-Kommunikation ebenfalls im Retarus Email Archive gespeichert werden.

Nachrichten, die in das Retarus Email Archive übergeben wurden, sind unveränderbar, vor möglichen unberechtigten Zugriffen geschützt und abrufbar. Diese Nachrichten werden während der Laufzeit des Vertrages maximal zehn Jahre gespeichert und am Ende der Laufzeit gesetzeskonform gelöscht, soweit nicht anders vereinbart. Während des Archivierungszeitraums lassen sich archivierte Emails vom Kunden durch verschiedene Filtermöglichkeiten einfach auffinden und erneut zustellen. Wünscht der Kunde vor dem Ablauf des vereinbarten Archivierungszeitraums und der Löschung der Emails den Export des kompletten Archivs, ist dieser vor Ende der Laufzeit von ihm gesondert zu beauftragen.

Der Administrator-Zugriff auf das Email Archive basiert auf dem Vier-Augen-Prinzip. Archivierte Email-Nachrichten und Anhänge lassen sich über leistungsfähige und bei Bedarf, etwa Datenschutzanforderungen granular einschränkbaren Suchfunktionen schnell auffinden.

Es wird automatisch ein vollständiges Zugriffsprotokoll erstellt.



Funktionalitäten:

- Zuverlässige Langzeitspeicherung aller ein- und ausgehenden Emails
- Unveränderliche und sichere Datenspeicherung auf Basis hybrider Verschlüsselung
- Bereitstellung von Tracking-Informationen über EAS Live Search
- Automatische Erstellung eines Zugriffsprotokolls
- Unterstützung bei der Erfüllung von regulatorischen Anforderungen
- Abrufmöglichkeit von Nachrichten inklusive Attachments
- Zugriff nach dem Vier-Augen-Prinzip über das webbasierte Retarus-Verwaltungsportal
- Leistungsstarke Suche mit datenschutzkonformen Einstellungsmöglichkeiten: Auffinden von Emails auf der Grundlage von Absender, Empfänger und Dateitypen in Anhängen, Speicherung der entsprechenden (Meta-)Daten für die Suche nach Betreff, Volltext und Attachment-Namen konfigurierbar

Optionen auf Anfrage

- Archivierung der internen Email-Kommunikation via Journaling (Microsoft Exchange oder M365 Exchange Online)
- Sicherer und bequemer Zugriff für Administratoren des Kunden über Single Sign-on
- Import von Emails aus anderen Archivsystemen (idealerweise im eml-Format)
- Export archivierter Emails auf externe Datenspeicher
- Nutzung kundeneigener (öffentlicher) Schlüssel (privater Schlüssel verbleibt beim Kunden)

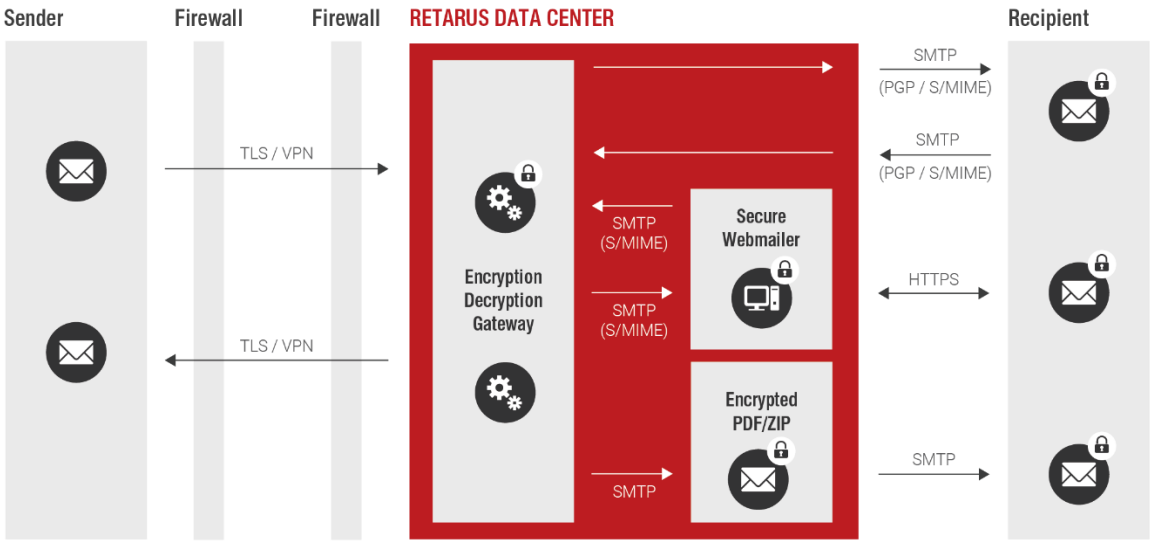
Retarus Email Encryption

Retarus Email Encryption unterstützt Kunden dabei, die Integrität, Authentizität und Vertraulichkeit von Email-Nachrichten zu gewährleisten. Dazu werden Emails entweder automatisiert über vorab abgestimmte Regelwerke oder benutzergesteuert im Retarus-System inklusive eventueller Dateianhänge verschlüsselt und/oder nach Bedarf signiert, bevor diese an den Empfänger versendet werden. Sofern beauftragt, werden ausgehende Nachrichten vor dem Verschlüsseln und eingehende Nachrichten nach dem Entschlüsseln auf Viren geprüft.

Weitere Funktionalitäten:

- Übernahme bestehender Public-Key-Infrastrukturen (PKIs)
- Weiterverwendung bestehender und gültiger S/MIME-Zertifikate
- Unterstützung der Standards OpenPGP, PGP und S/MIME
- Einbindung von kundeneigenen Richtlinien für die Verschlüsselung
- Bereitstellung eines Microsoft Outlook Add-Ins zur Steuerung von Benutzeraktionen für die Verschlüsselung und/oder Signatur von Nachrichten
- Bereitstellung alternativer verschlüsselter Kommunikationswege über den Retarus Secure WebMailer oder den Versand einer verschlüsselten PDF- oder ZIP-Datei
- Optionale Einbindung eines offiziellen Trust Centers (derzeit SwissSign), um S/MIME-Zertifikaten nach dem Industriestandard X.509 zu erstellen
- Automatisierte User-Synchronisierung für die Anlage und Erneuerung von Zertifikaten (auf Anfrage)

Systemarchitektur Retarus Email Encryption



Initialer Email-Encryption-Workshop

Der initiale Email-Encryption-Workshop ist eine notwendige Voraussetzung für die Konfiguration von Retarus Email Encryption. Im Workshop definiert der Kunde gemeinsam mit Retarus kundenspezifische Anforderungen für die Einrichtung. Inhalte können u. a. umfassen:

- Einführung in die Kryptographie
- Vorstellung der etablierten Standards
- Bestandsaufnahme der vorhandenen Infrastruktur
- Analyse der kundenspezifischen Anforderungen und Sicherheitsrichtlinien
- Definition von Workflows und Prozessen, z. B. bezüglich der Verschlüsselung / Signatur oder des Einsammelns öffentlicher Schlüssel
- Festlegung des Layouts und der Inhalte für Email-Benachrichtigungen
- Definition der Verwendung des Secure WebMailers (z. B. die Übermittlung von Zugangsdaten)
- Definition der Verwendung eines verschlüsselten PDF-Dokuments (z. B die Übermittlung des Kennworts)

Auf Basis der Ergebnisse erfolgt die Einrichtung des kundenspezifischen Verschlüsselungsmandanten im Retarus-System basierend auf den Standards S/MIME und PGP oder alternativen Verschlüsselungsmethoden (Secure WebMailer / verschlüsselte PDF- oder ZIP-Datei).

User Synchronization for Encryption (USE)

Die USE ist eine Lösung, zur vereinfachen Verwaltung einzelner Nutzer der Retarus Email Encryption, sowie von Gruppen sowie den zugehörigen S/MIME- oder PGP-Schlüsseln. Die Benutzerfreundlichkeit wird vor allem dadurch verbessert, dass zahlreiche Prozesse automatisiert vorgenommen werden können. Dies betrifft Aktionen wie die Erneuerung, Überprüfung und das Widerrufen von Zertifikaten und Schlüssel. Zudem lassen sich Ablaufdaten leichter überwachen und erforderliche Maßnahmen rechtzeitig einleiten.

- Sicheres Importieren von Benutzern und Zuweisen in vordefinierte Gruppen

- Verwaltung von Richtlinien auf der Grundlage von individuellen Anforderungen und Benutzergruppen
- Automatisierte Erstellung/Widerruf und Synchronisation von S/MIME (SwissSign).
- Unterscheidung zwischen persönlichen und Team-Zertifikaten
- Vollautomatische oder semi-automatische Zertifikatserneuerungen
- Erzeugen und Löschen von PGP-Schlüsseln und Synchronisierung privater Schlüssel der Benutzer
- Import-Möglichkeit von Schlüsseln/Zertifikaten, die über Dritte erstellt/gekauft wurden
- Regeln zur Verwaltung unternehmensspezifischer Verschlüsselungsrichtlinien in einer menschenlesbaren Form.
- Synchronisierung- und S/MIME-Transaktionsreports für Compliance- und Auditing-Zwecke.
- Empfang von Reports per Email oder SFTP- Abholung

Digitale Signatur / Zertifikate

Mit Retarus Email Encryption lassen sich ausgehende Emails bei Bedarf oder automatisiert per Regelwerk mit PGP-Schlüsseln oder S/MIME-Zertifikaten signieren. Bei eingehenden Nachrichten kann der Anwender anhand transparenter Informationen das Prüfergebnis der Signatur einfach erkennen. Neben Standard X.509 S/MIME-Zertifikaten (Email-Zertifikate Class 2) können optional S/MIME-Zertifikate eines Trust Centers (aktuell SwissSign) verwendet werden. Solche werden über die Managed PKI (MPKI) bereitgestellt. Voraussetzung ist, dass der Kunde neben den Bedingungen von Retarus zusätzliche Bedingungen des Trust Centers akzeptiert.

Secure WebMailer

Secure WebMailer ist ein sicheres Web-Portal, über das der Kunde verschlüsselte Emails mit Kommunikationspartnern austauschen kann, die weder S/MIME noch PGP nutzen. Dabei kann über einen Link auf ein persönliches Postfach zugegriffen werden, das für diesen Zweck automatisch im Retarus Secure WebMailer erstellt wurde. Alle Zugriffe sind HTTPS-verschlüsselt. Die Übermittlung der persönlichen Zugangsdaten an die jeweiligen Kommunikationspartner, sowie eine optionale unternehmensspezifische Gestaltung des Secure WebMailers und der Email-Benachrichtigungen werden gemeinsam mit dem Kunden im Rahmen des initialen Email-Encryption-Workshops definiert.

Verschlüsselte PDF- / ZIP-Datei

Retarus bietet die Möglichkeit, vertrauliche Informationen mittels eines kennwortgesicherten PDF-Dokuments oder einer kennwortgesicherten ZIP-Datei zu übermitteln. Hierbei wird der Text der Email inklusive aller Anhänge in eine PDF- oder ZIP-Datei integriert, die verschlüsselt an den Empfänger weitergeleitet wird. Die Übermittlung des Kennworts zum Öffnen des PDF-Dokuments oder der ZIP-Datei und eine optionale Anpassung des verwendeten Templates werden gemeinsam mit dem Kunden im Rahmen des initialen Email-Encryption-Workshops definiert.

Erweiterung für maschinell und/oder applikationsgenerierte Nachrichten (eBusiness-Nutzer)

Der Verarbeitung von maschinell und/oder applikationsgenerierten Nachrichten aus festen Automatismen, Portalanwendungen oder prozessgebundenen Lösungen (z. B. einem Signaturmodul) erfolgt über eine so genannte eBusiness-Lizenz. Dabei wird jeder Absenderadresse einer solchen Anwendung jeweils eine gesonderte eBusiness-Nutzer-Lizenz zugeordnet. Bei der optionalen Verwendung von S/MIME-Zertifikaten verwaltet Retarus im Auftrag des Kunden Class-2-Zertifikate der Kategorie „Silber“.

Data Loss Prevention

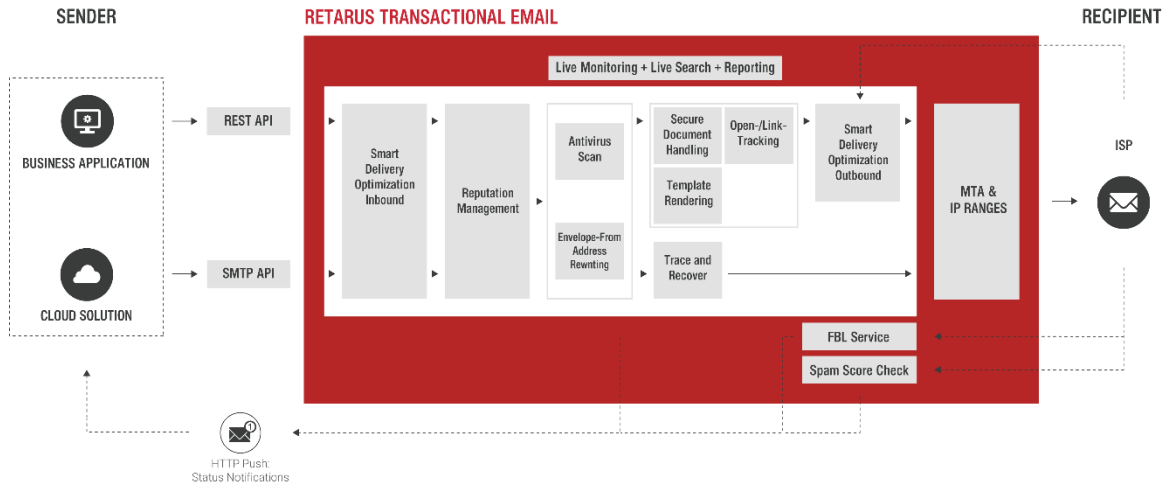
Data Loss Prevention prüft von Anwendern beim Kunden an externe Empfänger adressierte Emails auf im Rahmen der Konfiguration definierte Muster, z. B. Kreditkartennummern oder Bankkontennummern (IBAN). Wenn eine Email solche Muster enthält, wird die Übertragung an externe Empfänger unterbunden. Ferner können bestimmte Mitarbeiter, z. B. ein Administrator oder ein Compliance Officer, über den Versandversuch informiert werden. Die betreffende Email wird der Benachrichtigung als Anhang beigefügt. Optional kann der ursprüngliche Absender ebenfalls informiert werden. Die Prüfung auf solche Muster umfasst den Email-Body. Zusätzlich lässt sich der Versand von Email-Anhängen anhand von Datei-Endungen (z. B. exe, mp3, zip) sowie anhand des jeweiligen MIME-Types unterbinden. Außerdem kann der Kunde über das EAS festlegen, dass Emails nur dann an externe Adressaten versendet werden, wenn eine Kontrollinstanz, z. B. eine Funktionsmailbox, in den Verteiler aufgenommen wird.

Email Infrastructure

Retarus Transactional Email

Mit **Retarus Transactional Email** lassen sich große Email-Volumina direkt aus Geschäftsanwendungen ohne Belastung der eigenen Email-Infrastruktur versenden. Dazu wird die Kundeninfrastruktur über etablierte Schnittstellen an die Retarus Enterprise Cloud angeschlossen. Die Datenverarbeitung erfolgt in Retarus-eigenen Rechenzentren.

Systemarchitektur Retarus Transactional Email



Schnittstellen

SCHNITTSTELLEN	REST (V2)	SMTP
Max. Versandvolumen pro Stunde	Nach Anforderung skalierbar	Nach Anforderung skalierbar
Smart Delivery Optimization	✓	✓
Status-Informationen jeder Email	API-Callback (Webhooks)	API-Callback (Webhooks)
Email Reporting (CSV)	✓	✓
Smart Network Data Services Reporting*	Auf Anfrage	Auf Anfrage
Reputation Management	• Dedizierte IP (optional) • Blacklist-Monitoring • Live-Monitoring • SPF / DKIM • Suppression List • Registered Sender Domain • Feedback Loop Service***** • CSA-zertifiziert***** (EU, CH) • IPv6-/IPv4-Support	• Dedizierte IP (optional) • Blacklist-Monitoring • Live-Monitoring • SPF / DKIM • Suppression List • Registered Sender Domain • Feedback Loop Service* • CSA-zertifiziert* (EU, CH) • IPv6-/IPv4-Support
List Unsubscribe Header Unterstützung	✓	✓
Mandantenfähig (Multi-Domain-Konfiguration)	✓	✓
IP-Whitelisting	✓	✓
Verschlüsselte Anbindung an Retarus Global Delivery Network	✓	✓
Technische Voraussetzungen	HTTPS-API-Client (Job) und empfangender Webservice (Status)	Anwendung mit SMTP-Unterstützung (Job) und empfangender Webservice (Status)
Open Tracking	✓	-
Link Tracking	✓	-
Envelope-From Address Rewriting	✓	✓
Outbound AntiVirus MultiScan	✓	✓
Secure Document Handling	✓	-
Template-Rendering	✓	-
Trace & Recover	-	✓
Spam Score Check	✓	✓
EAS Live Monitoring	✓	✓
EAS Live Search	✓	✓
EAS Reporting	✓	✓
Max. Mailgröße	20 MB	20 MB

***Diese Funktionalitäten erfordern die Nutzung von IPv4-Adressen.

Basiskonfiguration

Die Basiskonfiguration beinhaltet Zugangsdaten bzw. eine registrierte Authentification-IP zu einem API-Endpoint oder zu einem SMTP-Server in einem Retarus-Rechenzentrum. Die Kommunikation erfolgt über eine sichere Verbindung via HTTPS und/oder SMTP Auth Basic via eTLS. Die Einrichtung umfasst eine Senderadresse pro IPv6-Adresse*, Default-Job-Parameter, IP-Routing, SPF-Record und DKIM-Signatur. Der Account wird nach vollständiger Einrichtung der beauftragten Pakete freigeschaltet. Retarus stellt eine Schnittstellenbeschreibung bereit.

*Erläuterung IPv6-Adresse: Die Nutzung nachfolgender Funktionalitäten innerhalb der Services erfordern die Nutzung von IPv4-Adressen:

- Smart Network Data Services Reporting
- Feedback Loop Service
- CSA-zertifizierte IP-Bereiche (Certified Senders Alliance)

Dedicated IP

Einer oder mehreren Senderadressen werden dedizierten IP-Adressen zugeordnet. Hierdurch kann z. B. die Email-Kommunikation aus unterschiedlichen Anwendungen oder von Mutter-/Tochter-Unternehmen getrennt werden. Die Nutzung von dedizierten IP-Adressen (Dedicated IPs) wird ab einem Volumen von 1.000.000 Emails pro Monat empfohlen. Da der Transactional Email Service i.d.R. in einem Rechenzentrumsverbund (Active/Active) genutzt wird, setzt die Nutzung von Dedicated IPs eine Mindestanzahl von zwei dedizierten IP-Adressen voraus. Mit der Einrichtung von dedizierten IP-Adressen, werden dem Kunden für die Dauer der Vertragslaufzeit durch Retarus IP-Adressen zur Nutzung überlassen. Diese werden in das Blacklist-Überwachungssystem von Retarus integriert. Ein Austausch der IP-Adresse durch Retarus ist jederzeit möglich.

Enforced TLS

Auf Ebene der Senderadresse wird während der Basiskonfiguration des Dienstes festgelegt, ob ein hybrides Verschlüsselungsprotokoll für jeden Versand angewandt werden soll. Damit wird eine verschlüsselte Verbindung aufgebaut, wenn der Kunde über die vorgegeben Domäne Emails versendet (enforced TLS). Falls die Empfängerseite keine verschlüsselte Verbindung akzeptiert, wird der Versand abgebrochen.

Envelope-From Address Rewriting

Optional bietet Retarus die Möglichkeit, die Envelope-From-Adresse des Kunden für ausgehende Emails umzuschreiben. Damit lassen sich mögliche Antworten auf ein dediziertes Postfach umleiten. Das Umschreiben von Adressen ist besonders nützlich, wenn es z. B. aus unternehmerischen Richtlinien nicht erlaubt ist, mit der hauseigenen Domain Nachrichten via Internet zu versenden.

Account / Access Token

Ein Account ist als Authentifizierungseinheit definiert (Definition von API-Benutzername/Passwort usw.) und ist bezogen auf ein bestimmtes Rechenzentrum, API-Zugangspunkt. Unter jedem Account können mehrere Domänen verwaltet werden. Sie können auch dieselbe Domain unter mehreren Accounts verwalten.

Smart Delivery Optimization

Retarus steuert den Versand und den Empfang von Emails via Smart Delivery Optimization. Das ermöglicht es, einen möglichst hohen Durchsatz bei ISPs und ESPs aufrecht zu erhalten. Dafür passt Smart Delivery Optimization das Sendeverhalten des Kunden automatisiert an die Rückmeldungen einzelner ISPs und/oder ESPs an. Die optimierte Versandsteuerung kann zu einer Verringerung der vereinbarten Verarbeitungskapazität führen.

Statusinformationen via API-Callback (Webhook)

Retarus stellt Statusinformationen via API-Callback (Webhook) zu Verfügung. Zu neu erzeugten Events wird der Kunde informiert, z. B. über den Zustellungsstatus, Gründe für Unzustellbarkeiten, Blockieren von Emails an Empfänger, die in der Suppression List verzeichnet sind, und Informationen zu Open- und Link-Tracking. Via http-Post lassen sich diese Statusinformationen automatisiert in Geschäftsprozesse und Applikationen integrieren. Damit unterstützt Retarus die Pflege der Stammdaten (Database Hygiene) sowie das aktive Bounce- und Traffic Management des Kunden und fördert somit die Reputation der kundeneigenen Domänen nachhaltig.

Retarus EAS – Live Monitoring

Retarus stellt im EAS-Portal ein Live-Monitoring zur Verfügung, anhand diesem in Real-Time versendete Emails verfolgt werden können. Diese Lösung ermöglicht es, Trendentwicklungen in den Bereichen Zustellung, Soft-/Hard-Bounces und Dropped Messages zu erkennen, um entsprechende Gegenmaßnahmen einleiten zu können.

Retarus EAS Live Search

Retarus stellt im EAS-Portal eine Live Search zur Verfügung. Die Suchfunktion bietet eine transparente Übersicht über alle vom Kunden versendeten Emails. EAS Live Search ermöglicht es, ausgehende Emails anhand von Zeiträumen, Message-IDs sowie Sendern und Empfängern zu suchen und dazu detaillierte Statusinformationen der letzten 45 Tage abzurufen.

Retarus EAS – Reporting

Retarus stellt im EAS-Portal ein Reporting zur Verfügung. Es bietet eine transparente Übersicht aller vom Kunden in den jeweils zurückliegenden 45 Tagen versendeten Emails, die im CSV- oder Excel-Format (XLSX) heruntergeladen werden kann.

Smart Network Data Service – Report (SNDS)

Der Smart Network Data Services (SNDS) Report listet in Form einer CSV-Datei detaillierte Daten zu vom Kunden genutzten IP-Adressen auf. Anhand dieser Daten kann der Kunde deren Reputation bei Microsoft besser nachvollziehen und verbessern. Dieser Service kann nur in Kombination mit einer dedizierten IP-Adresse genutzt werden.

Email Reporting (CSV)

Retarus stellt im Enterprise Administration Services Portal (EAS) einen Versandreport im CSV-Format zur Verfügung. Dem Kunden stehen täglich aktualisierte Reports für insgesamt 180 Tage zum Abruf zur Verfügung. Die Reports erfassen nur Transaktionen, die einen finalen Status aufweisen. Transaktionen, die sich in der Verarbeitung befinden, werden nicht aufgeführt. Reports können in mehrere Teildateien aufgeteilt und komprimiert (z. B. im ZIP-Format) abgerufen werden.

Hinweis: Die Einrichtung eines CSV-Reports bedingt die temporäre Datenspeicherung zum Zweck der Leistungserfüllung. Die gespeicherten Daten enthalten Informationen über die Nachrichtenverarbeitung sowie personenbezogene Daten, z. B. Email-Adressen von Absendern und Empfängern, jedoch keine Inhaltsdaten.

Retarus Spam Score Check

Mit welcher Wahrscheinlichkeit Nachrichten als Spam eingestuft werden, hängt von mehreren Faktoren ab. Auslöser für Spam-Warnungen können ungewöhnliche HTML-Formatierungen oder Tabellenkonstruktionen, übermäßig viele Links oder unseriöse Formulierungen in Betreffzeile und Email-Body sein. Retarus stellt in diesem Zusammenhang den kostenpflichtigen Service „Spam Score Check“ als buchbare Option zu Verfügung. Mit diesem lässt sich vor der Aussendung prüfen, mit welcher Wahrscheinlichkeit eine Email als Spam eingestuft wird. Die Rückführung der Spam Scores erfolgt in einem automatisierten Verfahren, in dem die ermittelten Informationen von Retarus per Email an die zur Verfügung stehende Reply-To-Adresse des Kunden oder via API-Callback an einen bereitstehenden Webservice des Kunden zurückübermittelt. Nach erfolgreicher Übertragung werden alle Informationen zur dieser Sendung gelöscht und nicht archiviert.

Open- und Link-Tracking (optional CNAME)

Open-Tracking gibt die Öffnungsrate von Emails an, Link-Tracking erfasst die Öffnungsrate von in Emails erhaltenen Links. Dazu werden der Email-Body bzw. der Link so verändert, dass sich die Nachrichten auswerten lassen. Um die Wahrscheinlichkeit einer Spam-Klassifizierung zu reduzieren, empfiehlt Retarus, die kostenpflichtige Option CNAME zu buchen. Damit kann der Kunde eine eigene (Sub-) Domain verwenden. Hierbei setzt der Kunde einen A-Record der entsprechenden (Sub-) Domain auf eine Server-Adresse von Retarus. Der Kunde ist verpflichtet, die jeweiligen Email-Empfänger über das Open- und Link-Tracking über ausreichende Datenschutzerklärungen zu informieren und bei diesen gegebenenfalls die vorherige Zustimmung gemäß geltendem Recht einzuholen.

AntiVirus MultiScan

Retarus überprüft Nachrichten beim Versand auf Virenbefall. Dabei kann der Kunde selbst im Vorfeld bestimmen, ob nur die Anhänge einer Nachricht, und/oder der Nachrichtentext (Email-Body) auf Schadsoftware geprüft werden soll. Die Überprüfung erfolgt mit zwei Virenscannern verschiedener Anbieter nach Wahl von Retarus. Sobald diese Anbieter Updates oder neue Releases bereitstellen, wird Retarus diese schnellstmöglich zur Virenüberprüfung verwenden. Sofern ein Virenbefall festgestellt wird, löscht Retarus die entsprechende Nachricht. Statusinformationen über infizierte Emails werden dem Kunden per API-Callback (Webhook) übermittelt.

Secure Document Handling

Mit Secure Document Handling lassen sich Dateianhänge zu versendender Emails verschlüsseln. Zu diesem Zweck werden die Anhänge vor dem Versand in der Retarus-Infrastruktur automatisiert in ein ZIP-Archiv gepackt, das passwortgeschützt verschlüsselt wird. Die Passwörter stellt Retarus den Empfängern der betreffenden Emails separat zu. Um den höchstmöglichen Schutz zu erzielen, ist dieser Service nur in Kombination mit dem Retarus Outbound AntiVirus MultiScan erhältlich.

Trace & Recover

Die Funktion ermöglicht es, Emails, die mittels einer SMTP-Anbindung übertragen werden, als Trace-&-Recover-Nachricht zu kennzeichnen. Alle für Trace & Recover gekennzeichneten Nachrichten werden 45 Tage lang in einem Kurzzeitspeicher abgelegt und sind in die Suchfunktion „Retarus EAS Live Search“ gefunden werden. Für die betroffene Nachricht steht eine Vorschau der ersten 1000 Satzzeichen zur Verfügung. Bevor die Nachricht bei Bedarf erneut versendet wird, kann nur der ursprüngliche Empfänger editiert werden.

Die Zusatzfunktion Trace & Recover setzt die Nutzung von AntiVirus MultiScan voraus und wird, von Retarus, für einen vom Kunden zu bestimmenden technischen Account aktiviert. Trace & Recover kann nicht im Zusammenhang mit Envelope-From Address Rewriting (Outbound) verwendet werden.

Verarbeitungskapazität

Die Berechnungsbasis der Verarbeitungskapazitäten beruht auf der Basiskonfiguration von Transactional Email. Die Messung legt eine Email-Größe von 200 Kilobytes zu Grunde und berücksichtigt Open- und Link-Tracking für einen Zeitraum von einer Stunde.

Eine vertraglich vereinbarte Verarbeitungskapazität auf stündlicher Basis setzt voraus, dass der Kunde alle bei Retarus eingehenden Versandaufträge, wie in dem Beispiel unten aufgeführt, über den Verlauf einer Stunde gleichmäßig verteilt, um den vertraglich vereinbarten Durchsatz darstellen zu können, überprüft Retarus die Verteilung in Fünf-Minuten-Intervallen.

Aufgrund möglicher Sende-Peaks kann die tatsächliche Verarbeitungskapazität das 1,25-Fache der vereinbarten Verarbeitungskapazität betragen. Abhängig von weiteren Funktionen bzw. größeren Emails kann sich die Bandbreite verringern. Abweichungen sind möglich. Für eine Erhöhung der Verarbeitungskapazität ist jeweils eine individuelle Anforderungsprüfung notwendig.

Rechenbeispiel – Verarbeitungskapazität

Im nachfolgenden Beispiel beträgt die vertraglich vereinbarte Verarbeitungskapazität 150.000 Emails/Stunde:

- (150.000 Emails/Stunde) / (12 x Intervall*/Stunde) = 12.500 Emails/Intervall*
- Die Kapazitätserweiterung für Sende-Peaks von 25 % kann den Durchsatz auf ein Maximum von bis zu 15.625 Emails/Intervall* erhöhen.

*Ein Intervall beträgt 5 Minuten.

IP-Whitelisting

Mit der Retarus IP-Whitelisting-Funktion kann der Kunde explizit definieren, welche Applikationen aus seinem Netzwerk via Transactional Email Nachrichten versenden dürfen.

Feedback Loops

Retarus steht mit verschiedenen ISPs (Internet-Service-Providern) über eine Beschwerde-Vereinbarung in Verbindung. Beschwerdeinformationen werden von teilnehmenden ISPs in Form von Feedback-Loops (ARF) an Retarus zurückgemeldet.

Feedback-Loops ist ein vom ISP zur Verfügung gestellter Mechanismus, um Versender darüber zu informieren sobald Nachrichten des Kunden als unerwünscht klassifiziert worden sind. Als in diesem Sinne unerwünscht gelten Emails, die Empfänger als Spam einstufen, z. B. durch einen Klick auf „Dies ist Spam“ im eigenen Postfach).

Beschwerden werden in einem automatisierten Verfahren rückgeführt, in dem die übermittelten Beschwerdeinformationen von Retarus ausgelesen und übermittelt werden – per Email an die zur Verfügung stehende Reply-To-Adresse oder via API-Callback an einen bereitstehenden Webservice des Kunden. Nach erfolgreicher Übertragung werden alle diesbezüglichen Informationen zur Beschwerde gelöscht und nicht archiviert.

Email-Abrechnung

Emails werden je Einheit abgerechnet, wobei eine abrechenbare Einheit 200 Kilobytes beträgt. Emails, die größer als 200 Kilobytes sind, werden entsprechend in mehrere Einheiten zum Zwecke der Abrechnung aufgeteilt.

Beispiel: Eine Email hat eine Größe von 2.403 Kilobytes (ca. 2,4 MB) – dies entspricht 13 Abrechnungseinheiten

Emails werden unabhängig davon in Rechnung gestellt (Identifier: Email-ID), ob die Übertragung erfolgreich war oder nicht (z. B. wenn Emails blockiert oder gebounced wurden).

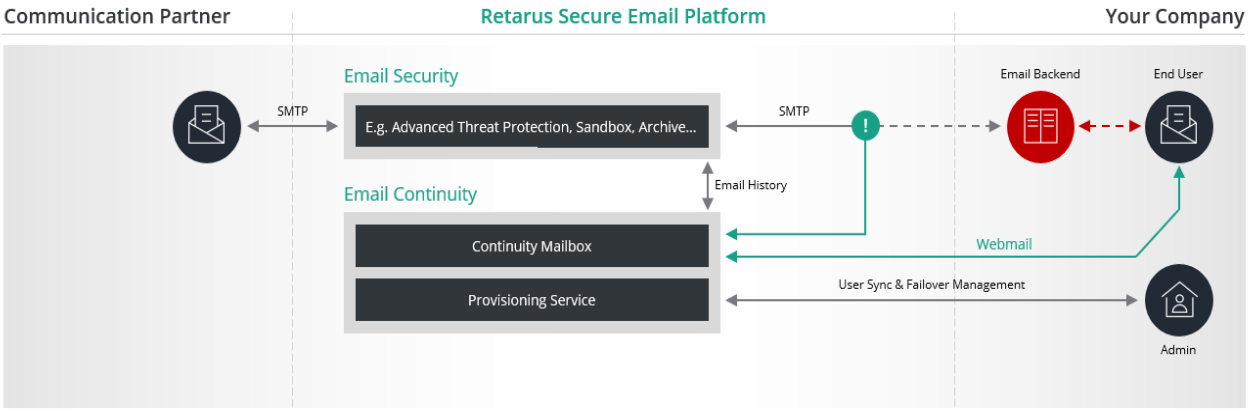
Retarus Email Continuity

Retarus Email Continuity ist eine alternative Email-Plattform zur Aufrechterhaltung der Email-Kommunikation in Katastrophenszenarien (z. B. Malware-Infiltration, Rechenzentrumsausfall, Cloud-Downtime). Bei Bedarf werden auf Anforderung des Kunden der Empfang und der Versand aller ein- und ausgehenden Emails über diese Plattform geroutet.

Weitere Funktionalitäten:

- Enduser-Zugriff auf das Email-Continuity-Postfach via Webmail (HTTPS)
- Interne Adressbuch-Funktionalität zur Darstellung und Suche aller übertragenen Kontaktinformationen innerhalb der betroffenen Kundendomäne
- Administrativer Zugriff auf den Continuity-Service per REST-API für die Verwaltung der Continuity-Mailbox-Benutzer
- Mailbox-Einrichtung über die Retarus Directory-Synchronisation durch die Übermittlung einer CSV-Datei
- Automatisierte Benachrichtigung neu hinzugefügter Continuity-Benutzer
- Passwort-Self-Service über eine Landing-Page (mittels Security Token, die der Kunde verwaltet)
- Rückübertragbarkeit der Emails aus dem Email-Continuity-Postfach (Backsync) in die Produktivsysteme des Kunden
- Optional Zugriff auf alle eingehenden Nachrichten der letzten Tage (Email-Historie bis zu 14 Tage) gemäß der dem Kunden zugeordneten Domänen. Hierfür ist ein Verweis der betreffenden MX-Records des Kunden auf die Retarus-Infrastruktur erforderlich.

Systemarchitektur Retarus Email Continuity



Retarus Predelivery Logic

Retarus Predelivery Logic analysiert Emails bereits zum Zeitpunkt der Interaktion mit der Retarus Enterprise Cloud nach individuellen Regeln, bevor sie an die Kundeninfrastruktur weitergeleitet werden.

Kontrolle, Umleitung oder Anpassung von Emails bis hin zum gesamten Email-Verkehr geschieht auf der Grundlage kundendefinierter Regelwerke, die aus Bedingungen und Aktionen bestehen müssen. Damit lassen sich Emails gezielt z. B. anhand ihres Inhalts, ihrer Sprache oder des Herkunftslandes weiterverarbeiten.

Anbindung an Retarus

Die Anbindung der Systeme des Kunden an die Retarus-Infrastruktur erfolgt in der Regel über das Internetverschlüsselungsprotokoll Transport Layer Security (TLS), um eine gesicherte Übertragung der Daten via SMTP zu gewährleisten. Je nach Beauftragung ist eine Anbindung via opportunistic TLS oder enforced TLS möglich.

Email Security Services können optional über ein Virtual Private Network (VPN) angebunden werden. Voraussetzung für eine Verbindung via VPN ist die gleichzeitige Anbindung an die Retarus-Rechenzentren in München und Frankfurt/Main (RZ DE 1 und RZ DE 2).

Hinweise

Der Schutz vor eingehenden wie ausgehenden Nachrichten mit potenziell schädlichem Charakter nebst eingebetteten Links und Attachments basiert überwiegend auf statistischen und Näherungs-Verfahren. Trotz der Nutzung aller beschriebenen Leistungsmerkmale kann es zu fälschlicherweise abgelehnten, falsch deklarierten oder zur Zustellung von potenziell schädlichen Nachrichten kommen.

Im Übrigen weist Retarus darauf hin, dass das Verfahren des Quarantinierens – abhängig von der Art und Weise der Email-Nutzung und kundenspezifisch vorgenommenen Einstellungen – möglicherweise dazu führt, dass Nachrichten, insbesondere sogenannte „false positives“, nicht oder verspätet zugehen und dem Kunden hieraus ggf. Nachteile entstehen können.

Folgende Service-Optionen setzen AntiVirus MultiScan 4-fach voraus:

- Deferred Delivery Scan
- Sandboxing
- Time-of-Click Protection
- Patient Zero Detection

Soweit nicht ausdrücklich schriftlich anders vereinbart, beschränkt sich die Nutzung von Retarus Email Encryption auf persönlich generierte Unternehmenskommunikation. Die Verarbeitung von maschinell und/oder applikationsgenerierten Nachrichten setzt den Retarus Email Encryption eBusiness-Nutzer zwingend voraus.

Implementierung, Change-Management und Support

Die Implementierung beginnt nach Auftragserteilung und Zusendung des vollständig und korrekt ausgefüllten Setup-Sheets durch den Kunden.

Für Support- und Serviceanfragen sowie Change Requests muss der Kunde Retarus den Kreis autorisierter Personen mitteilen, die solche Anfragen offiziell stellen dürfen. Der technische Ansprechpartner des Kunden für die Implementierung des Services wird dabei grundsätzlich als erster autorisierter Ansprechpartner festgelegt. Dieser kann sodann als Kundenadministrator im Enterprise Administration Portal weitere Support-Kontakte eintragen und somit autorisieren. Kunden-Administratoren können diese Berechtigungen jederzeit ändern, erweitern oder löschen.

Im Kundenauftrag umgesetzte Änderungen am Service und Lösungen für Incidents (inkl. Workarounds) müssen durch den Kunden mindestens in Textform abgenommen werden. Erfolgt innerhalb von zehn Tagen keine Rückmeldung durch den Kunden, wird das jeweilige Kundenticket nach Ablauf dieser Frist automatisch geschlossen und die Änderung / Lösung gilt als abgenommen.

Mitwirkungspflichten

Der Kunde veranlasst unverzüglich die erforderliche Änderung der betreffenden MX-Records.

Der Kunde ist für die von ihm gewählte(n) Email-Domain(s) selbst verantwortlich. Er hat sicherzustellen, dass durch die Verwendung nicht gegen Namens-, Marken- oder sonstige Schutzrechte Dritter verstoßen wird. Retarus ist berechtigt, vom Kunden die sofortige Zuweisung einer neuen Email-Domain zu verlangen, falls der begründete Verdacht einer Rechtsverletzung durch die bisherige Email-Domain besteht.

Soweit nicht ausdrücklich schriftlich anders vereinbart, beschränkt sich die Nutzung der Retarus Secure Email Platform auf normale nutzerbezogene Desktop-Kommunikation. In jedem Fall hat der Kunde sicherzustellen, bekannten Applikationsempfang (Massenempfang) vor der entsprechenden Nutzung der Retarus Secure Email Platform mindestens in Textform zu melden.

Soweit Services auch für den Versand von Emails genutzt werden, ist dies – soweit nicht ausdrücklich schriftlich anders vereinbart – ausschließlich für persönlich generierte Unternehmenskommunikation erlaubt. Der Massenversand von Emails ist außerhalb des Services Transactional Email nicht zulässig. Sollten von Retarus genutzte IP-Adressen aufgrund einer unvorhergesehenen und/oder unsachgemäßen Nutzung der Services zum Email-Versand auf einer Blacklist gelistet werden, oder sollte Retarus deshalb von ähnlichen die Leistungserbringung beeinträchtigenden Maßnahmen betroffen sein, hat der Kunde Retarus sämtliche in diesem Zusammenhang entstandenen Aufwände und Kosten zu ersetzen.

Der Kunde ist sich dessen bewusst, dass die erfolgreiche Nutzung der Retarus-Dienste und die Qualität der Dienstleistungserbringung wesentlich von seiner Mitwirkung abhängt. Der Kunde wird daher das ihm nach Vertragsabschluss zugesandte Implementation-Sheet innerhalb von fünf (5) Werktagen ausgefüllt zurücksenden, insbesondere die in diesem Dokument genannten Mitwirkungspflichten einhalten und erklärt sich damit einverstanden, dass Retarus zum Schutz der stabilen Dienstleistungserbringung und der ISP-Reputation der Parteien dienliche technische Maßnahmen ergreifen darf. Hierbei ist es Retarus ausdrücklich erlaubt, spezifische Email-Aufträge zu verwerfen, das Volumen zu drosseln oder im Extremfall den Zugang zu sperren. Entstehen durch die Nichteinhaltung der Mitwirkungspflichten Aufwände und/oder Kosten, sind diese vom Kunden zu tragen.

Einwilligung

Der Kunde sichert zu, Emails nur an Adressaten zu versenden, die nach den jeweils geltenden gesetzlichen Rahmenbedingungen hierzu ihre ausdrückliche Einwilligung erteilt haben (Opt-In) oder für die ein sonstiger rechtlich anerkannter Erlaubnistatbestand gegeben ist.

Gestaltung der Email

Jede versendete Email muss ein den geltenden rechtlichen Anforderungen entsprechendes, leicht erkennbares Impressum, im Volltext einer jeder Email, enthalten.

Für den Versand von Emails mit Werbeinhalten gilt zudem:

- Der Auftraggeber einer Werbesendung muss klar erkennbar sein.
- In jeder Email ist der Empfänger gesondert auf die Möglichkeit hinzuweisen, die erteilte Einwilligung in die Zusendung von Emails jederzeit zu widerrufen. Der Widerruf / das Abbestellen von Emails (Opt-Out / Unsubscribe) muss dem Empfänger grundsätzlich ohne Weiteres, d. h. ohne die Eingabe von Zugangsdaten (z. B. Login und Passwort) möglich sein.
- In der Kopf- und Betreffzeile der Email darf weder der Absender noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt dann vor, wenn die Kopf- und Betreffzeile absichtlich so gestaltet sind, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.

Technische Konfiguration

- Absenderadressen sind registrierungspflichtig und Bestandteil der Service-Administration. Die Absenderadresse muss in der Lage sein, Emails zu empfangen (valider DNS-MX-Record). Die Absenderdomain muss zudem über einen validen DNS-A-Record verfügen. Rollenbasierende Absenderadressen (z. B. postmaster@) sind nicht erlaubt.
- Der Kunde muss Email-Adressen unverzüglich von den entsprechenden Mailinglisten entfernen, wenn nach dem Beschicken dieser Adressen die Nichtexistenz des Postfachs erkannt wird, spätestens jedoch, wenn drei Hard-Bounces erfolgt sind. Insgesamt darf die Hard-Bounce-Rate pro ISP 1,0 % grundsätzlich nicht übersteigen. Rollenbasierende Empfängeradressen (z. B. postmaster@) werden automatisch verworfen.
- Der Kunde muss Email-Adressen von den entsprechenden Mailinglisten entfernen, wenn der Empfänger die Email als SPAM einstuft (complaint) oder die Einwilligung in den Versand von Emails widerruft.
- Für die in der SMTP-Kommunikation zwischen Email- Servern angegebene „MAIL FROM“-Adresse ist ein SPF-From Record einzutragen, der es SPF-Systemen auf Empfängerseite erlaubt, einen SPF-Test durchzuführen. Der SPF-Record muss mit „-all“ oder „-~all“ enden. Sollten die nötigen Einträge kundenseitig nicht innerhalb von zehn (10) Werktagen erfolgen, wird die erneute Überprüfung nach Aufwand in Rechnung gestellt.
- Das Verfahren DKIM (DomainKeys Identified Mail) ist seitens des Kunden zwingend einzusetzen, d. h. für jede bei Retarus für den Kunden registrierte Absenderdomain hat der Kunde einen entsprechenden DKIM-Schlüssel in seinem DNS zu hinterlegen. Sollten die nötigen Einträge kundenseitig nicht innerhalb von zehn (10) Werktagen erfolgen, wird die erneute Überprüfung nach Aufwand in Rechnung gestellt.
- Jede versendete Email muss einen „List-Unsubscribe"-Header oder einen „List-Help“-Header (siehe RFC 2369) enthalten. Der „List-Unsubscribe“-Header ist für listenbasierte Mailings erforderlich und mit „POST HTTPS“-Link inklusive „One-Click-Unsubscribe“-Funktionalität (RFC 8058) einzufügen. Der angegebene Link muss eine direkte One-Click-Abmeldung mindestens auf Listenebene bewirken. Der Versender darf dem Nutzer eine Bestätigungs-Email für die erfolgte Abmeldung übersenden. Bei nicht-listenbasierten Mailings muss alternativ zum „List-Unsubscribe“-Header der „List-Help“-Header gesetzt werden. Der „List-Help“-Header muss mindestens eine „mailto:“-Adresse oder einen HTTPS-Link enthalten, HTTP-Links sind nicht

zulässig. Sowohl die Verwendung der „mailto:“-Adresse als auch des HTTPS-Links müssen dem Empfänger die Möglichkeit geben, Informationen zu erhalten, aus welchem Grund die Email an ihn versendet wurde und weshalb eine Abmeldung auf Listenebene nicht möglich ist.

- Die Nutzung des „list-unsubscribe-Post“-Header erfordert einen valide URL, die entsprechende POST-Request entgegennehmen und verarbeiten kann.

  Beispiel:

```
List-Unsubscribe:      <mailto:listrequest@example.com?subject=unsubscribe>,
                       <https://example.com/unsubscribe.html?opaque=123456789>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

- Ausnahmen von dieser Verpflichtung können geltend gemacht werden, wenn es aus Gründen der Ausgestaltung des Dienstes und der damit einhergehenden Zusendung automatisierter Emails nicht erforderlich oder möglich ist, eine Abmeldung im vorgenannten Sinne durchzuführen.
- Der Kunde muss eine Abuse-Email-Adresse für das Melden von Missbrauch von Email-Adressen für die Adressaten der Emails einrichten und überwachen. Die Abuse-Email-Adresse kann z. B. als abuse@domain konfiguriert werden.
- Die Übertragung von Emails an den Retarus Transactional Email-Service muss von Seiten des Kunden über eine geschützte Transport Layer Security (TLS) Verbindung, nach dem aktuellen Stand der Technik erfolgen. Retarus setzt ebenfalls beim Versand von Emails an den Adressaten Transport Layer Security (TLS) unter Verwendung von CSA-IP-Adressen ein.
- Retarus ist CSA-zertifiziert (Certified Senders Alliance). Die hier beschriebenen Mitwirkungspflichten entsprechen den aktuellen CSA-Vorgaben. Die CSA kann ihre Anforderungen jederzeit anpassen. Daher verpflichtet sich der Kunde, etwaige Anpassungen mitzutragen. Hierüber werden die Kunden entsprechend von Retarus informiert.