Soul4Business Hosted Email Security

Ihr Mailserver war noch nie so sicher und zuverlässig
Konformität mit der kommenden DSGVO

Inhalt

Dieses Dokument enthält folgende Punkte:

- Warum Hosted Email Security?
- Wie funktioniert Hosted Email Security?
- Wie aufwändig ist die Implementierung von Hosted Email Security?
- Technische Details zum Prüfverfahren für Emails
- Geht das auch nachhaltig, umweltschonend und rechtssicher?
- Kontaktdaten und weitere Infos

Warum Hosted Email Security?

Das Thema Security ist eine der größten Herausforderungen für aktuelle EDV-Systeme, und es wird immer wichtiger. Fast täglich hören wir von Problemen wie Hackerangriffen, Erpresser-Trojanern, Malware, Viren, und vielem mehr. Unsere Mailboxen sollten gegen die Flut der täglichen Spamnachrichten geschützt sein, dennoch kommen zu viele unerwünschte Emails durch – oder wichtige Emails landen fälschlicherweise im Spam Ordner. Die versteckten Kosten, die durch die verlorene Zeit entstehen, sind enorm.

Ein weiterer Knackpunkt ist die Zuverlässigkeit der Systeme. Jeder Mailserver kann einmal ausfallen. Jede Internetverbindung garantiert nur ein bestimmtes Maß an Verfügbarkeit. Und jede Kundenanfrage, die nicht durchkommt, kann ein verpasstes Geschäft und im Extremfall einen verlorenen Kunden bedeuten.

Wie funktioniert Hosted Email Security?

14 lastverteilte SMTP-Nodes in ganz Europa sorgen dafür, dass Ihre Emails nicht nur schneller ankommen als bisher, sondern auch einem intensiven Prüfverfahren unterzogen werden. Herkömmliche Mailserver bieten üblicherweise nur ein einziges Virenschutz-Plug-In – bei Soul4Business läuft jede Email zunächst durch eine interne Prüfung, und dann durch drei verschiedene Standard-Virenscannermodule. So gelangen unerwünschte Emails nicht einmal in Ihr Netzwerk – sie werden bereits zuvor abgeblockt.

Die 14 SMTP-Nodes sind zusätzlich durch vier Backupsysteme abgesichert. Dieses umfangreiche Netzwerk speichert auch Ihre Nachrichten, falls Ihr Mailserver nicht verfügbar ist. Selbst beim Teilausfall ganzer Abschnitte des Internets bleiben Sie per Email erreichbar – die Nachrichten werden einfach zugestellt, sobald Ihr Mailserver wieder kontaktiert werden kann.

Durch dieses System ergibt sich auch die Möglichkeit, unser Produkt zur Email Archivierung anzusteuern – beachten Sie dazu das Dokument „Soul4Business Hosted Email Archiving"

Wie aufwändig ist die Implementierung von Hosted Email Security?

Die Inbetriebnahme der Soul4Business Hosted Email Security ist ganz einfach. Sie geben uns lediglich Ihre Emailadressen bekannt und ändern den Mail-Exchange (MX)-Eintrag Ihrer Domain auf den DNS Namen des Soul4Business SMTP-Clusters. Wir sind gerne dabei behilflich.

Die Ersteinrichtung auf unserer Seite erfolgt kostenfrei bei Vertragsabschluss. Sollten im Lauf der Zeit weitere Mailboxen hinzukommen oder gelöscht werden, können Sie diese Änderungen jederzeit auch selbstständig innerhalb unseres Customer Service Bereiches durchführen.

Technische Details zum Prüfverfahren für Emails

Die Verfahren bei der internen Prüfung wurden durch langjährige intensive Beschäftigung mit dem Thema entwickelt und werden aufgrund der sich ständig ändernden technischen Rahmenbedingungen laufend angepasst.

Zur Zeit läuft das Verfahren wie folgt:

Bestimmte Attribute einer Email führen unmittelbar zur Bewertung als Spam und zur Ablehnung der Email. Andere Attribute gelten als schwächere Argumente, diese werden gezählt und summiert, und bilden so eine Bewertung, die üblicherweise als Spam Score bezeichnet wird. Wird ein bestimmter Spam-Score überschritten, wird die E-Mail abgelehnt.

Sollte es vorkommen, dass erwünschte Emails abgelehnt werden, weil etwa der Mailserver des Absenders unsauber definiert ist, kann man diese Empfänger in eine Whitelist eingetragen. Für Emails von Adressen, die auf der Whitelist stehen, wird keine Spam-Prüfung durchgeführt, sehr wohl aber die Virenchecks.

Der Spam-Check beginnt mit der Prüfung des SMTP-Servers auf Korrektheit im Sinne eines Reverse-DNS Eintrags zu seiner IP-Adresse. Dann kontrollieren wir, ob sich die Adresse auf einer Blacklist befindet. Emails von einer IP, die auf einer Blacklist steht, werden natürlich sofort abgelehnt.

Im zweiten Schritt überprüfen wir, ob ein SPF (Sender-Policy-Framework) sowie ein DKIM (DomainKeys-Identified-Mail) Eintrag für diese Domain existieren. Diese Einträge sind zwar nicht zwingend erforderlich, aber üblich, darum erhöhen wir im Falle des Fehlens den Spam-Score. Existieren die Einträge, so werden sie auf Korrektheit geprüft. Schlägt die SPF-Prüfung fehl, so wird die Email ebenfalls sofort abgelehnt – bei derartigen Nachrichten handelt es sich erfahrungsgemäß zu 94,81% um Spam. Fehlerhafte DKIM-Einträge hingegen führen nur zu einer Erhöhung des Spam-Scores.

Im Anschluss daran beginnen unsere Scanner Module damit, die Email auf unerwünschte Werbung (Spam) bzw. Phishing Inhalte zu prüfen. Hier besteht die Möglichkeit, kundenindividuelle Filterregeln zu definieren, welche Sie selbstständig innerhalb des Customer Service Bereiches administrieren können. Dies kann die Treffsicherheit der Prüfung stark erhöhen. Gerne stehen wir Ihnen dabei mit Rat und Tat zur Seite.

Zu guter Letzt erfolgt die Antiviren-Prüfung durch drei verschiedene Virenscanner-module (zur Zeit Kaspersky, F-Secure und ClamAV). Übersteht die E-Mail auch diese Überprüfung positiv, wird sie umgehend an Ihren eigenen Mailserver weitergeleitet, der die abschließende Verteilung in die richtige Mailbox übernimmt.

Geht das auch nachhaltig, umweltschonend und rechtssicher?

Soul4Business hat es sich zum Ziel gesetzt, nicht nur der zuverlässigste, sondern auch der umweltfreundlichste Internet Service Provider zu sein. Wir verwenden möglichst klimaschonende Rechenzentren, darüber hinaus arbeiten wir mit namhaften Umweltschutz Agenturen zusammen, und unterstützen diese in unterschiedlichen Regionen unserer Welt, und kaufen für jeden neuen Kunden 1 ha Regenwald.

Datenschutz wird bei uns ebenfalls „Groß" geschrieben. Wir bemühen uns nicht nur schon jetzt um Konformität mit der kommenden DSGVO, sondern verpflichten uns darüber hinaus, zu weit mehr um dem Schutz Ihrer Daten nachzukommen. Details entnehmen Sie bitte unserer Datenschutz Erklärung welche Sie unter www.soul4business.com/de/Datenschutz-Richtlinie finden.

Kontaktdaten und weitere Infos

Haben Sie noch weitere Fragen? Rufen Sie uns einfach an. Oder schicken Sie uns ein Email – unsere Mailserver sind immer erreichbar.

Soul4Business.Cloud Ltd. Österreich.
Sustainable & Reliable IT Solutions
T. +43.1.537 12 4042
W. soul4business.com
@. info@soul4business.com