cubewerk

· weil uns IT begeistert! ·

Anwenderhandbuch – securePostfach

Dieses Handbuch steht ausschließlich securePostfach-Kunden während der Vertragslaufzeit zur Verfügung. Eine Veröffentlichung oder Weitergabe dieses Handbuches ist nicht gestattet.

Stand: 15.01.2021

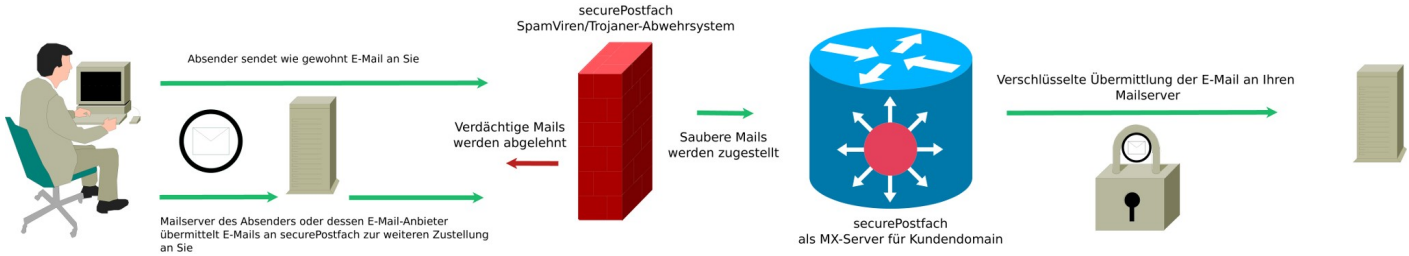
Inhaltsverzeichnis

Produktbeschreibung

securePostfach ist eine sichere - und optional verschlüsselte - cloudbasierte Spam- und Virenschutzlösung zur Absicherung Ihrer eingehenden E-Mails. securePostfach wird durch die cubewerk GmbH in hochverfügbaren deutschen Rechenzentren betrieben. Die Rechenzentren sind geografisch voneinander getrennt um eine höchstmögliche Ausfallsicherheit zu gewährleisten.

securePostfach nimmt ausschließlich als viren- und spamfrei erkannte E-Mails für Sie an. Verdächtige oder

schadhafte E-Mails werden abgelehnt und der Absender darüber informiert. So gelangt eine E-Mail gar nicht erst in Ihren rechtlichen Einflussbereich und Ihre Benutzer sind geschützt.



Voraussetzungen zur Nutzung von securePostfach

Sie benötigen einen eigenen Mailserver welcher per SMTP E-Mails akzeptiert. Typische Mailserver sind Microsoft Exchange, IBM Notes, Zimbra, Kopano, Postfix uvw.

Sie benötigen eine eigene E-Mail-Domäne (der Teil hinter dem @-Zeichen Ihrer E-Mail-Adresse) wie z. B. cubewerk.de. E-Mail Adressen bei FreeMail-Anbietern wie web.de, gmx.de, t-online.de usw. können **nicht** über securePostfach abgesichert werden.

Sie benötigen auf die DNS-Einstellungen Ihrer E-Mail-Domäne Zugriff. In der Regel können diese Einstellungen über Ihren Hosting-Anbieter oder direkt über z. B. 1und1, Strato oder Domainfactory abgeändert werden. Nötig ist, die MX DNS-Einträge (Mail Exchange) auf securePostfach zeigen zu lassen.

Beschreibung der E-Mail-Prüfung & Zustellung

Durch die Änderung der MX-Einträge werden E-Mails an Sie, zuerst an securePostfach zugestellt. Hier erfolgt eine mehrstufige Spam- und Virenprüfung, Inhalts- und Reputationsprüfung sowie weitere Inspektionen der E-Mail bzw. des Absenders auf Auffälligkeiten. Zusätzlich kommen mehrere getrennte und herstellerunabhängige Virenschutzlösungen zur Prüfung zum Einsatz. Dies erfolgt alles während der Absenderserver noch auf die erfolgreiche Quittierung seiner E-Mail-Zustellung wartet. Die komplette Prüfung dauert ~ 5 Sekunden.

Wird die E-Mail durch securePostfach als sauber eingestuft, erhält diese einen digitalen Stempel und es folgt eine Übergabe der E-Mail an Ihren E-Mail Server.

Stuft unser System E-Mails als verdächtig ein, werden diese bereits **beim Zustellversuch** des Absenders abgelehnt. Dieser erhält hierüber umgehend eine Information und kann die E-Mail um den schadhaften Inhalt kürzen oder verdächtige Anhänge entfernen. Ein typischer Angreifer oder Spammer, versucht es selten ein zweites Mal.

securePostfach verzichtet bewusst auf das Annehmen und anschließende Löschen oder Markieren von E-Mails.

Auch besteht keine Möglichkeit, verdächtige E-Mails aus einer sogenannte Quarantäne zu entfernen oder einen Spamverdachts oder Junk-Ordner zu nutzen. Verdächtige Mails werden gar nicht erst angenommen. Dies alles wären Maßnahmen, die den Anwender in der Regel nur Zeit kosten oder fehleranfällig sind. Auch müsste sich der Empfänger eine einmal angenommene E-Mail rechtlich zurechnen lassen – auch wenn er sie nicht zu Gesicht bekommt. Dies wird von vorne herein durch securePostfach ausgeschlossen.

Blockierte Dateianhänge

Da sich sehr häufig in bestimmten Dateianhängen bis dato unbekannte Viren oder Trojaner einnisten, ist eine weitere wichtige Maßnahme zur Schadensbegrenzung das Blockieren von Anhängen mit hohem Schadpotenzial. Das PDF-Format zum sicheren Dokumentenaustausch hat sich als saubere Alternative etabliert. Sollten Sie eine generelle Ausnahme der Dateiblockierung für Ihr Unternehmen wünschen, teilen Sie uns dies bitte per E-Mail mit oder nehmen selbst die Einstellungen im Kundencenter dazu vor.

securePostfach blockiert standardmäßig folgende Dateianhänge mit häufigem Schadinhalt:

(exe|vbs|pif|scr|bat|cmd|com|cpl|doc|xls|xlsx|ppt|pptx|docx|docm|zip|iso|uu|dot|dotm|mht|xz)

Kundencenter

securePostfach-Kunden erhalten mit Auftragserteilung Zugangsdaten für das Kundencenter. Das Kundencenter ist erreichbar unter https://portal.cubewerk.de/index.php

Das Kundencenter bietet neben Vertragsdetails auch die Möglichkeit zur Recherche sowie Definition von White- und Blacklisten sowie die Nachverfolgung von E-Mails.

Lizenzierung und Nutzung

securePostfach wird pro E-Mail-Domäne lizenziert. Bei Bestellung teilen Sie uns mit, für welche E-Mail Domänen Sie securePostfach benötigen. Im Anschluss nennen Sie uns Ihre öffentliche IP-Adresse bzw. den Hostnamen für die Zustellung von E-Mails an Sie und den gewünschten Port.

Nach der Umstellung Ihrer MX-Einträge, werden die E-Mails durch seucrePostfach verarbeitet.

E-Mails an nicht lizenzierte Domänen, werden nicht angenommen.

Einschränkungen

Besitzen Sie eine kostenlose E-Mail-Adresse bei Ihrem Internetanbieter bzw. FreeMail-Anbieter wie t-online.de, web.de gmx.de, freenet.de uvw., kann securePostfach **nicht genutzt** werden.

Konfiguration Mailserver des Kunden

securePostfach prüft bei jeder neuen eingehenden E-Mail gegen Ihren E-Mail Server, ob es die An-Adresse gibt. Dieses Ergebnis wird für 60 Minuten gespeichert. Hierzu erfolgt eine „Testzustellung“ an Ihren Mailserver. Stellen Sie Ihren E-Mail Server zwingend so ein, dass er nur gültige E-Mail-Adressen akzeptiert. (Stichwort CatchAll). Es ist somit Ihnen überlassen, welche E-Mail-Adressen Sie auf Ihrem E-Mail-Server pflegen/hinterlegen und dementsprechend auch annehmen.

securePostfach stellt ausschließlich TLS-verschlüsselt, E-Mails an Ihren E-Mail-Server zu. Bitte stellen Sie durch nötige Firewallregeln sicher, dass ausschließlich die securePostfach-Mailserver eine Verbindung zu Ihrem Mailserver aufbauen können. Der Port ist standardmäßig 25/TCP – kann jedoch beliebig von Ihnen vorgegeben werden.

Bitte hinterlegen Sie zwingend mindestens zwei Mailserver in Ihrem DNS, um eine Ausfallsicherheit zu

gewährleisten. Eine weiterhin direkte - und somit parallele - Zustellung an Ihren Mailserver ist ab diesem Zeitpunkt nicht mehr empfohlen. Hierdurch würde man die securePostfach-Abwehrlösung aushebeln/umgehen.

DNS-Einstellungen für securePostfach:

Hostname	MX-Priorität
mx1.securepostfach.de	10
mx2.securepostfach.de	10
mx3.securepostfach.de	10

Bitte verwenden Sie **nur** Hostnamen als MX-Einträge. IP-Adressen können sich ändern.
Stellen Sie sicher, dass securePostfach ohne Authentifizierung E-Mails an Sie per SMTP übergeben kann.

Sollte ein weiterer Spam- oder Virenfilter auf Ihrem Mailserver aktiv sein oder sonstige Software oder Einstellungen, die eine erneute Überprüfung oder Filterung durchführt, stellen Sie zwingend sicher, dass Sie ungewünschte E-Mails annehmen und verwerfen (discard) oder in Quarantäne verschieben. Eine Ablehnung ist nicht erlaubt. Diese werden sonst von securePostfach an den Absender als unzustellbar zurück geschickt. Dies muss **zwingend** vermieden werden um sog. Backscatter[1] zu vermeiden.

Bitte beachten Sie, dass securePostfach E-Mails bis zu einer Größe von 50MB annimmt. Stellen Sie zwingend sicher, dass auch Ihr Mailserver mindestens 50MB große Mails annimmt. Zur Sicherheit ist empfohlen, wegen unterschiedlicher Rechengrößen (10024/1024 Bytes) bzw. Kodierungen von E-Mails (7bit, 8bit) ~ 20% Größenunterschied einzuplanen. Nehmen Sie somit mindestens Mails mt einer Größe von 70MB an.

IPv4 & IPv6

SecurePostfach spricht aus- und eingehend, neben IPv4, auch IPv6. Durch die Hinterlegung der obigen DNS-Einträge, stehen automatisch beide Protokolle zur Verfügung.

Bitte achten Sie beim Setzen Ihrer Firewallregeln darauf, dass Sie auch für IPv6 Freischaltungen vornehmen, falls Sie dieses Protokoll schon unterstützen.

Verdächtige E-Mails an cubewerk-Helpdesk melden

Sollten Sie dennoch einmal E-Mails erhalten, die unser Filtersystem aus Ihrer Sicht als falsch eingestuft hat, bitten wir Sie, diese E-Mails an uns weiterzuleiten. Einsendungen werden manuell geprüft und verdächtige E-Mails im Anschluss dem securePostfach-Filtersystem angelernt.

Verwenden Sie hierzu die E-Mail-Adresse **spaminput@cubewerk.de**

Bitte leiten Sie E-Mails **ausschließlich** als Anhang weiter.

Microsoft Outlook: E-Mail öffnen -> Weitere - Als Anlage weiterleiten

Kopano WebApp: Rechtsklick auf E-Mail, Senden an

Mozilla Thunderbird: Rechtsklick auf E-Mail -> Weiterleiten als - > Anhang

Nur durch die Weiterleitung als Anhang, ist die E-Mail für unseren Helpdesk verwertbar.

Achtung: Es erfolgt **keine** Rückmeldung/Antwort auf Ihre Einsendungen. E-Mails die durch unser Helpdesk als tatsächlich verdächtig eingestuft werden, werden zukünftig abgelehnt.

Bitte melden Sie keine E-Mails, für welche Sie sich selbst einmal angemeldet haben (Newsletter, Angebote

1 https://de.wikipedia.org/wiki/Backscatter_(E-Mail)

usw.) von tatsächlichen Firmen. Beantragen Sie hier selbstständig gegenüber diesen Firmen, ein Austragen aus deren Newslettern.

Wenn Ihr Mailserver einmal nicht verfügbar ist

Sollte Ihr Mailserver einmal nicht verfügbar sein, lagert securePostfach bis zu 5 Tage Ihre E-Mails ein und versucht in regelmäßigen Abständen automatisch die erneute Zustellung. Konnte innerhalb von 5 Tagen keine Zustellung erfolgen, werden die E-Mails an den Absender zurück gesendet.

Optional kann hier für Sie eine Alarmierung aktiviert werden. Sie erhalten dann eine E-Mail an eine alternative E-Mail Adresse, falls die Zustellung an Sie gerade gestört ist.

Erzwingen der Verschlüsselung

Bei der E-Mail-Zustellung an Sie obliegt es dem Absender, ob er vertrauliche Informationen an Sie per Klartext (wie auf einer Postkarte) verschickt oder verschlüsselt – wie z. B. mit secureTransport.

Mit securePostfach besteht die Möglichkeit für Sie, **pauschal** nur eine ausschließlich verschlüsselte Übermittlung **zu akzeptieren**. Sollte diese scheitern oder dem Versender nicht möglich sein, erfolgt keine Annahme und er erhält darüber eine Benachrichtigung. Diese Option kann auf Wunsch manuell aktiviert werden. Bitte sprechen Sie uns an.

Fehlercodes bei Ablehnung von E-Mails

securePostfach lehnt aus unterschiedlichen Gründen E-Mails ab. Damit Absender hierüber ausreichend informiert werden, enthält jede Ablehnung auf SMTP-Ebene, einen mehrsprachigen Fehlercode sowie einen Verweis auf ausführliche weitere Informationen für Absender.

Details unter: https://www.cubewerk.de/securepostfach-info/

Datenschutz und Datenspeicherung

securePostfach stellt lediglich einen Transportdienst dar. Es erfolgt **keine** dauerhafte Speicherung von E-Mails oder Anhängen außerhalb der temporären Aufbewahrungsfrist, wenn Ihr Mailserver einmal nicht erreichbar ist. E-Mails werden lediglich für die Dauer der Zustellung im Speicher des Transportdienstes vorgehalten, falls Ihr Mailserver temporär die Annahme verweigert.

Zur Erkennung von Missbrauch sowie zur monatlichen Abrechnung werden Log-Dateien über die eingelieferten E-Mails für eine Abrechnungsperiode. Weitere Details zur Datenspeicherung entnehmen Sie bitte der Datenschutzerklärung.

Die Verbindung ggü. securePostfach ist auf Wunsch dauerhaft verschlüsselt möglich. secureTransport weist sich ggü. dem Einlieferer mit einem öffentlichen und gültigen X509-Zertifikat aus. Die verwende Verschlüsselungscipher ist ECDHE-RSA-AES128-GCM-SHA256. Diese kann jedoch auch stärker (je nach Unterstützung der Gegenseite) verhandelt oder gar erzwungen werden.

Für die verschlüsselte endgültige Übertragung der E-Mails an Sie als Empfänger, wird ebenso auf X509-Zertifikatsbasis die Übermittlung durchgeführt. Folgende Ciphers werden von Ihnen akzeptiert:

EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:AES256-SHA:CAMELLIA128-SHA:AES128-SHA

cubewerk

· weil uns IT begeistert! ·

Für Ihre Datenschutzerklärung kann folgende Textergänzung verwendet werden:

„Für den elektronischen Dokumentenaustausch und Parteienverkehr mit Kunden/Partnern kommt eine nach aktuellem Stand der Technik deutsche Lösung zur Spam- und Virenprüfung (securePostfach) zum Einsatz. Diese stellt eine technische und organisatorische Maßnahme (TOM) zur Abwehr von Angriffen gegen die IT-Landschaft per E-Mail dar. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen wir als Verantwortliche hierdurch geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 DSGVO).“

securePostfach Mail-Header

Wurde eine empfangene E-Mail erfolgreich geprüft, setzt securePostfach im E-Mail-Header das Sicherheitsflag ‚X-securePostfach-checked: yes‘ pro E-Mail.

Hierdurch können Sie in Ihrem E-Mail Client bzw. Server, die E-Mails weiter filtern bzw. sehen den Erfolg der Prüfung durch securePostfach.

Wartung und Störung

Als Betreiber sind wir an einer sehr hohen Verfügbarkeit und Servicequalität interessiert. Aus diesem Grund ist securePostfach hochverfügbar konzipiert und ein Ausfall eines Systems garantiert weiterhin einen reibungslosen Betrieb. In seltenen Fällen ist es nötig, dass zur Abwehr von akutem Schaden für unsere Kunden sicherheitsrelevante Updates umgehend eingespielt werden müssen. Dies erfolgt in der Regel nach Ankündigung und kann zu kurzen Unterbrechungen des Dienstes führen.

Missbrauchsvermeidung

Bitte stellen Sie sicher, dass Sie die E-Mail-Adresse abuse@IHRE-DOMAIN annehmen und auswerten. Diese E-Mail-Adresse dient Fremden dazu, auffällige E-Mails von Ihrer Domain zu melden bzw. auf einen Missbrauch Ihrer IT-Landschaft oder einzelnen E-Mail-Konten hinzuweisen. Optional können Sie uns diese E-Mails durch eine automatische Regel weiterleiten. Bitte sprechen Sie uns dazu an.