

E-Mail-Sicherheit mit Postini - Kurzreferenzkarte

Grundlegende Hinweise:

Alle Domänen hinzufügen

Fügen Sie alle Domänen und Subdomänen dem Dienst hinzu. Erstellen Sie für die Domänen, die die gleichen Benutzerlisten nutzen, Alias-Domänen. Aktualisieren Sie Ihre MX-Datensätze für jede Domäne und jede Alias-Domäne.

SMTP-Traffic auf Port 25 einschränken

Nachdem Sie alle Ihre Domänen hinzugefügt haben, schränken Sie den SMTP-Traffic an der Firewall so ein, dass nur noch Verbindungen aus dem Postini IP-Range zugelassen werden. Damit verhindern Sie, dass Spammer Ihren Server auf Port 25 direkt ansprechen.

„Blatant Spam Blocking“ aktivieren

„Blatant Spam Blocking“ minimiert die Anzahl der offensichtlichen Spams in Ihren Benutzerquarantänen.

Benutzer und Mailing-Listen hinzufügen

Fügen Sie alle Benutzer bzw. Alias-Benutzer und Mailing-Listen hinzu. Sie können automatisierte Methoden wie „Directory Sync“, „SMTP Autorcreate“ oder „SmartCreate“ verwenden. Nachdem Sie alle Ihre Benutzer hinzugefügt haben, können Sie durch Aktivieren von „Non-Account Bouncing“ E-Mails an ungültige Adressen blocken.

Virenschutz einrichten

Aktivieren Sie für Ihre Domänen „Non-Account Virus Blocking“, so dass mit Viren infizierte E-Mails an nicht-registrierte Benutzer automatisch gelöscht werden. Konfigurieren Sie außerdem den „Attachment Manager“, um E-Mails mit angehängten, ausführbaren Dateien, die versteckte Viren enthalten können, zu blockieren oder in den Quarantäneordner zu verschieben.

„Connection Manager“-Blockierung aktivieren

Sobald der „Connection Manager“ Angriffe registriert, schützt er automatisch Ihren Server. Sie können auch bestimmte IP-Adressen oder -Ranges blocken und vertrauenswürdige Server festlegen, die nicht als Angreifer geblockt werden.

Benachrichtigungen (Alarmer) konfigurieren

Konfigurieren Sie Ihre „Delivery Manager“- und „Spooling Manager“-Administratorenalarmer, um wichtige Mail-Server-Ereignisse nachzuverfolgen.

Disaster-Recovery einrichten

Wenn Sie die optionale E-Mail-Spooling-Funktion haben, richten Sie den „Spool Manager“ für die Disaster-Recovery ein.

Einen Notfallplan erstellen

Entwickeln Sie für Probleme in Bezug auf den Strom eingehender E-Mails einen Notfallplan und machen Sie sich mit Ihren Support-Optionen und Problemlösungsverfahren vertraut.

IP-Ranges des Dienstes

System	IP-Range	CIDR-Bereich	IP-/Subnetzmaske
200, 201	207.126.144.0 – 207.126.159.255	207.126.144.0/20	207.126.144.0 Maske: 255.255.240.0
5, 6, 7, 8	64.18.0.0 – 64.18.15.255	64.18.0.0/20	64.18.0.0 Maske: 255.255.240.0

Technischer Support - Ressourcen

[[Partner-Support-Information und Ressourcen können hier hinzugefügt werden.](#)]

Während eines Spam-Outbreaks

Ab und an kann es im Internet zu einem Spam-Outbreak kommen. Der Dienst blockiert fast alle Spams. Wenn jedoch Spammer Massen-E-Mails mit neuen Angriffsmethoden versenden, können vorübergehend Spams in Ihren Posteingang gelangen.

Sie können versichert sein, dass Postini sich umgehend um das Problem kümmert und die Filter zum Schutz vor Angriffen aktualisiert. Den Spam-Outbreak-Status können Sie auf der Support-Seite einsehen.

Spam-Problem für einen Benutzer lösen

Wenn Sie feststellen, dass eine Spam-Mail an einen bestimmten Benutzer gesendet wurde, befolgen Sie bitte die folgenden Schritte zur Lösung des Problems:

Wurde die Mailadresse dem Dienst hinzugefügt?

Suchen Sie nach der Mailadresse des Benutzers in der Administrationskonsole.

Falls Sie sie nicht finden, wurde die E-Mail ohne Filterung zugestellt. Fügen Sie die Benutzeradresse hinzu und beachten Sie Folgendes:

- ◆ Wenn die Adresse einem bereits registrierten Benutzer zugeordnet ist, fügen Sie einen Alias-Benutzer hinzu.
- ◆ Falls der Dienst die Adresse über die Alias-Domäne erkennen kann, erstellen Sie eine Alias-Domäne für die Domäne des Benutzers.
- ◆ Wenn die Adresse eine Verteilerliste sein kann, vgl. nachstehende Verteilerlistenlösung.

Wurde die Mail an eine Mailing- oder Verteilerliste anstatt an einen einzelnen Benutzer gesendet?

Stellen Sie im Mailheader die Empfängeradresse fest und suchen Sie diese Adresse in der Administrationskonsole. Wenn Sie die Adresse dort nicht finden, müssen Sie sie der Mailing-Liste hinzufügen. Da Mailing-Listen in der Regel Adressen von firmenexternen Kontakten enthalten, fügen Sie die Liste nicht als Benutzer hinzu. Fügen Sie sie als Alias des verantwortlichen Besitzers hinzu, damit die Quarantäne-Übersicht und die Passwortnachrichten an den Besitzer der Mailing-Liste anstatt an die gesamte Mailing-Liste gesendet werden.

Wurde die E-Mail direkt an Ihren Mailserver gesendet, ohne zuvor den Dienst zu durchlaufen?

Bitte bedenken Sie, dass Spammer DNS-Standards zur Auswahl von MX-Datensätzen nicht einhalten. Um zu verhindern, dass die E-Mail-Schutzdienstfilter umgangen werden, richten Sie Ihren E-Mail-Server bzw. die Firewall so ein, dass nur E-Mails aus dem IP-Range des Dienstes zugelassen werden (vgl. Rückseite).

War die Absenderadresse in der Liste „Genehmigte Absender“?

Wenn der Sender oder die Domäne des Senders auf der Liste „Genehmigte Absender“ (d. h. die persönliche Liste des Benutzers oder eine für das Unternehmen des Benutzers definierte Liste) steht, wird die E-Mail ungeachtet ihres Spam-Inhalts zugestellt. Dies trifft auch zu, wenn der Spammer die Absenderadresse so manipuliert hat, dass sie einem genehmigten Absender entspricht. (Spoofing)

Überprüfen Sie die Absenderlisten auf Benutzer- und Unternehmensebene und löschen sie alle großen und bekannten Domänen, die oft von Spammern manipuliert werden.

Haben Benutzer Ihre eigenen Adressen oder Domänen als eine genehmigte Mailing-Liste hinzugefügt?

- ◆ Wenn ja, werden sämtliche an den Benutzer gerichtete Spam-Mails ungeachtet der Spam-Einstellungen dem Benutzer zugestellt.
- ◆ Entfernen Sie in der Administrationskonsole die Adresse oder Domäne des Benutzers aus den Listen „genehmigte Absender“ und „genehmigte Empfänger“ des Benutzers.

Hat ein Benutzer innerhalb Ihres Unternehmens die E-Mail versendet?

E-Mails, die unter den Benutzern des gleichen Servers ausgetauscht werden, werden nicht durch den Dienst geprüft – es sei denn, Sie haben Ihren Server so konfiguriert, dass auch innerhalb einer Domäne gefiltert wird. Prüfen Sie im Mailheader, ob jemand innerhalb Ihrer Firma die E-Mail versendet hat.

Wurde die E-Mail aus der Quarantäne zugestellt?

Der Benutzer oder ein Administrator können die E-Mail aus dem Quarantäne-Ordner zugestellt haben.