TREND MICRO

Email Reputation Services

Administratorhandbuch

Dynamischer Spam-Schutz auf Netzwerkebene

Messaging Security

Datenschutz und Offenlegung persönlicher Daten

Einige Funktionen, die in Trend Micro Produkten zur Verfügung stehen, erfassen und senden Feedback hinsichtlich Produktnutzungs- und Ermittlungsinformationen an Trend Micro. Einige dieser Informationen werden in bestimmten Rechtsordnungen und im Rahmen von bestimmten Vorschriften als persönliche Daten betrachtet. Wenn Sie nicht möchten, dass Trend Micro persönliche Daten erfasst, müssen Sie die entsprechenden Funktionen deaktivieren.

Email Reputation Services erfasst alle von Ihnen über die Konsole bereitgestellten Daten und überträgt sie an die Trend Micro Server. Um die Erfassung von Daten zu deaktivieren, müssen Sie die Registrierung für den Service aufheben.

Die von Trend Micro gesammelten Daten unterliegen den im Trend Micro Datenschutzhinweis angegebenen Bedingungen:

https://www.trendmicro.com/privacy

Dokument-Nr.:ERGM09115/201012

Release-Datum:Mai 2013

Dokumentversion Nr.: 3.00

Geschützt durch U.S. Patent-Nr.: 7,606,214; 7,926,108; 7,814,540

Im Trend Micro™ Email Reputation Services-Administratorhandbuch werden die Hauptfunktionen dieses Diensts vorgestellt. Sie sollten sich das Handbuch vor der Nutzung des Diensts durchlesen.

Detaillierte Informationen zur Verwendung bestimmter Funktionen innerhalb der Software stehen in der Online-Hilfedatei und in der Trend Micro Knowledge Base zur Verfügung.

Trend Micro ist stets bemüht, die Dokumentation zu verbessern. Setzen Sie sich mit uns in Verbindung, wenn Sie Fragen, Kommentare oder Vorschläge zu diesem oder einem anderen Trend Micro Dokument haben: docs@trendmicro.com.

Bewerten Sie diese Dokumentation auf der folgenden Website:

http://www.trendmicro.com/download/documentation/rating.asp

Inhaltsverzeichnis

Vorwort

Kapitel 1: Einführung in Email Reputation Services

Kapitel 2: Gesperrt?

Kapitel 3: Erste Schritte

Kapitel 4: Verwenden der Verwaltungskonsole

Kapitel 5: Hilfe anfordern

Anhang A: Glossar

Stichwortverzeichnis

Vorwort

Willkommen beim Trend Micro ™ Email Reputation Services Administratorhandbuch. In diesem Handbuch werden die wichtigsten Funktionen des Diensts und Konfigurationsanweisungen für Ihre Produktionsumgebung vorgestellt. Lesen Sie sich dieses Handbuch durch, bevor Sie den Dienst konfigurieren.

Dokumentation

Die Trend Micro Email Reputation Services Dokumentation besteht aus folgenden Komponenten:

- Online-Hilfe: Unterstützt Sie bei der Konfiguration aller Funktionen über die Benutzeroberfläche. Sie können auf die Online-Hilfe zugreifen, indem Sie die Webkonsole öffnen und dann auf das Hilfesymbol klicken.
- Administratorhandbuch: unterstützt Sie bei der Planung der Verteilung und der Konfiguration aller Diensteinstellungen.

Zielgruppe

Die Zielgruppe der Email Reputation Services Dokumentation sind IT-Manager und E-Mail-Administratoren in mittleren und großen Unternehmen. Die Dokumentation setzt voraus, dass der Leser über fundierte Kenntnisse im Bereich „E-Mail-Messaging-Netzwerke“ verfügt, einschließlich Details zu folgenden Themen:

- SMTP-Protokoll
- Message Transfer Agents (MTAs)

Hinweis

Sie müssen in der Lage sein, Ihren MTA zur Erstellung einer DNS-Abfrage vom Typ „Liste der bekannten Spam-Quellen“ zu konfigurieren, bevor Sie die Einstellungen für Email Reputation Services ändern.

In der Dokumentation wird nicht davon ausgegangen, dass sich der Leser mit Virenschutz oder Anti-Spam-Technologie auskennt.

Dokumentationskonventionen

Die Dokumentation verwendet die folgenden Konventionen:

TABELLE 1. Dokumentationskonventionen

KONVENTION	BESCHREIBUNG
GROSSSCHRIFT	Akronyme, Abkürzungen und die Namen bestimmter Befehle sowie Tasten auf der Tastatur
Fettdruck	Menüs und Menübefehle, Schaltflächen, Registerkarten und Optionen
Kursivdruck	Verweise auf andere Dokumente
`Schreibmaschinenschrift`	Muster für Befehlszeilen, Programmcode, Internet-Adressen, Dateinamen und Programmanzeigen
Navigation > **Pfad**	Der Navigationspfad zu einem bestimmten Fenster **Datei** > **Speichern** bedeutet beispielsweise, dass Sie in der Benutzeroberfläche im Menü **Datei** auf **Speichern** klicken
 **Hinweis**	Konfigurationshinweise
 **Tipp**	Empfehlungen oder Vorschläge
 **Wichtig**	Informationen zu den erforderlichen oder standardmäßigen Konfigurationseinstellungen und Produktbeschränkungen
 **Warnung!**	Wichtige Aktionen und Konfigurationsoptionen

Kapitel 1

Einführung in Email Reputation Services

Trend Micro Email Reputation Services bietet kostengünstige gehostete Hochleistungssicherheitsdienste, die Unternehmen vor Spam, Viren und unangemessenen Inhalten schützen, bevor diese Ihr Netzwerk erreichen.

Trend Micro Email Reputation Services

Als erste Verteidigungslinie stoppt Trend Micro Email Reputation Services über 80 % der Spam-Nachrichten, bevor diese Ihr Netzwerk überfluten, die Sicherheit des E-Mail-Gateways gefährden und die Systemressourcen überlasten.

Wenn Ihr E-Mail-Server eine Anfangsverbindung eines anderen E-Mail-Servers akzeptiert, zeichnet er die IP-Adresse des Computers auf, der die Verbindung anfordert. Ihr E-Mail-Server fragt dann den zugehörigen DNS-Server ab, der wiederum die Trend Micro Reputation-Datenbank abfragt, um zu ermitteln, ob ein Datensatz für die IP-Adresse des anfordernden Computers vorhanden ist.

Wenn der Host in einer Datenbank aufgelistet wird, empfiehlt Email Reputation Services eine entsprechende Aktion. Sie können Aktionen auch anpassen.

Trend Micro bietet für den Email Reputation Services Dienst zwei Stufen: Standard und Advanced.

Standard-Dienst

Mithilfe dieses Diensts können Sie Spam sperren, indem Sie angeforderte IP-Adressen anhand der Trend Micro Reputation-Datenbank validieren, die vom Trend Micro Smart Protection Network unterstützt wird.

Diese immer größer werdende Datenbank enthält derzeit mehr als 1 Milliarde IP-Adressen mit Reputation-Bewertungen auf Grundlage von Spam-Aktivitäten. Trend Micro Spam-Ermittler überprüfen und aktualisieren diese Bewertungen in regelmäßigen Abständen, um Genauigkeit zu gewährleisten.

Email Reputation Services Standard-Dienst ist ein DNS-Dienst, der auf Einzelabfragen basiert. Der designierte E-Mail-Server stellt eine DNS-Abfrage an den Standard-Reputation-Datenbankserver, sobald er eine E-Mail-Nachricht eines unbekannten Hosts erhält. Wenn der Host in der Standard-Reputation-Datenbank aufgelistet wird, meldet Email Reputation

Services diese E-Mail-Nachricht als Spam. Sie können den MTA (Message Transfer Agent) so einrichten, dass die entsprechende Aktion für diese E-Mail-Nachricht auf Basis der Email Reputation Services Ergebnisse durchgeführt wird.

Hinweis

Trend Micro empfiehlt, den MTA so zu konfigurieren, dass eine E-Mail-Nachricht von einer in der Standard-Reputation-Datenbank enthaltenen IP-Adresse gesperrt wird.

Erweiterter Dienst

Dieser Dienst erkennt und stoppt Spam-Quellen, über die Millionen von Nachrichten versendet werden.

Bei diesem Dienst handelt es sich um eine dynamische Anti-Spam-Echtzeitlösung. Zum Bereitstellen dieses Diensts überwacht das Trend Micro Netzwerk automatisierter Expertensysteme gemeinsam mit Trend Micro Spam-Experten kontinuierlich Netzwerk- und Datenverkehrsmuster und aktualisiert die dynamische Reputation-Datenbank sofort, wenn neue Spam-Quellen auftauchen – häufig innerhalb weniger Minuten nach dem ersten Auftreten von Spam. Die dynamische Reputation-Datenbank wird entsprechend der Zu- oder Abnahme der Spam-Aktivität aktualisiert.

Standardmäßig stellt der erweiterte Dienst eine DNS-Anfrage an die Standard- und dynamische Reputation-Datenbank (eine in Echtzeit dynamisch aktualisierte Datenbank). Diese Datenbanken weisen verschiedene Einträge auf, mit denen Trend Micro eine effiziente und leistungsfähige Datenbank unterhalten kann, die schnell auf hochdynamische Spam-Quellen reagieren kann.

Der erweiterte Email Reputation Services Dienst hat mehr als 80 % der insgesamt eingehenden Verbindungen in Kundennetzwerken blockiert. Die Ergebnisse richten sich nach dem Spam-Anteil in den eingehenden E-Mails. Je mehr Spam empfangen wird, desto höher ist der Prozentsatz der blockierten Verbindungen.

Trend Micro Smart Protection Network

Email Reputation Services wird vom Trend Micro Smart Protection Network unterstützt. Hierbei handelt es sich um ein globales Netzwerk, das von hochqualifizierten Spam-Ermittlern betrieben wird, die die Reputation-Bewertungen von IP-Adressen recherchieren, sammeln, verarbeiten und verteilen. Diese Experten überwachen die Spam-Aktivitäten, erstellen Informationen zu Spam-Quellen, überprüfen die Genauigkeit der Reputation-Bewertungen und arbeiten mit Organisationen zusammen, um sicherzustellen, dass Spammer ordnungsgemäß vom Dienst nachverfolgt werden.

Das Smart Protection Network arbeitet rund um die Uhr, um Verfügbarkeit und schnelle Reaktionszeiten zu gewährleisten und Echtzeitupdates zur sofortigen Verfügbarkeit in der Datenbank bereitzustellen. Dieser Premium-Dienst stellt die wichtigste Komponente bei der Erstellung und Verwaltung einer zuverlässigen Reputation-Datenbank dar.

Trend Micro Bedrohungsanalyse-Team

Als Teil des Smart Protection Network verwaltet das Trend Micro Bedrohungsanalyse-Team die Reputation-Datenbank, um genaue und aktuelle Bewertungen zu garantieren. Jede Bewertung enthält umfangreiche Spam-Verläufe und Spam-Beispiele für vollständige Transparenz bezüglich der Datenbanken. Dieser Dienst ist einzigartig, weil er von allen Personen mit Fragen zu einer zugewiesenen Bewertung vollständig überprüfbar ist.

Reputation-Zuweisung

Die Ermittler des Bedrohungsanalyse-Teams folgen strengen Richtlinien beim Nominieren und Entfernen von IP-Adressen aus den Datenbanken, die Teil der Email Reputation Services Standard-Dienstebene sind. Eine IP-Adresse erhält eine Reputation-Zuweisung, wenn sie:

- Spam gesendet oder das Senden von Spam unterstützt hat (z. B. Anbieten von Diensten für Spammer oder Zulassen, dass entsprechende Ressourcen von Spammern verwendet werden).

- als ungesicherter E-Mail-Server („Open Relay“) fungiert, der zum Senden von Spam verwendet wurde.
- als ungesicherter Port auf einem Computer („Offener Proxy“) fungiert, der zum Senden von Spam verwendet wurde.
- als dynamisch zugewiesene Adresse fungiert, die nicht als E-Mail-Server verwendet werden soll.

Vor der Verarbeitung einer IP-Adresse wird diese vom Smart Protection Network anhand sorgfältiger Richtlinien kategorisiert. Derselbe Ermittler, der die Reputation zugewiesen hat, kann auch alle Anforderungen zum Ändern der zugewiesenen Reputation überprüfen. Es wird alles unternommen, um sicherzustellen, dass der Reputation-Datensatz korrekt ist und dass Änderungen rechtzeitig vorgenommen werden.

Jeder Reputation-Datensatz enthält Beispiele des tatsächlich von der IP-Adresse empfangenen Spams, den Verlauf des Spam-Verhaltens, eine Aufzeichnung der gesamten Korrespondenz bezüglich der Vermittlung, sämtliche Fehlerbehebungen und andere damit zusammenhängende Informationen. Bei dynamisch zugewiesenen IP-Adressen, die vom ISP an die Standard-Reputation-Datenbank übermittelt wurden, enthält der Reputation-Datensatz Übermittlungsdaten und alle Einschränkungen, die vom ISP auferlegt wurden.

Informationen zur Überprüfung der Reputation einer IP-Adresse finden Sie unter *Nach IP-Adressen suchen auf Seite 4-5*.

Zustellungsinfrastruktur

Trend Micro hat weltweit einige der größten IP-Netzwerke und Rechenzentren aufgebaut. Die Trend Micro Netzwerk-DNS- und Datenbankserver sind geografisch in den wichtigsten Einrichtungen weltweit verteilt und überwachen und optimieren das Netzwerk kontinuierlich, um größtmögliche Verfügbarkeit für Email Reputation Services Kunden zu gewährleisten.

Funktionsweise

Die tatsächliche Implementierung von Email Reputation Services enthält eine DNS-Suche pro IP-Adresse. Wenn ein E-Mail-Server die Anfangsverbindung eines anderen E-Mail-Servers akzeptiert, zeichnet er die IP-Adresse des Computers auf, der die Verbindung anfordert. Der empfangende E-Mail-Server fragt dann seinen DNS-Server ab, um festzustellen, ob ein Datensatz für diese IP-Adresse vorhanden ist.

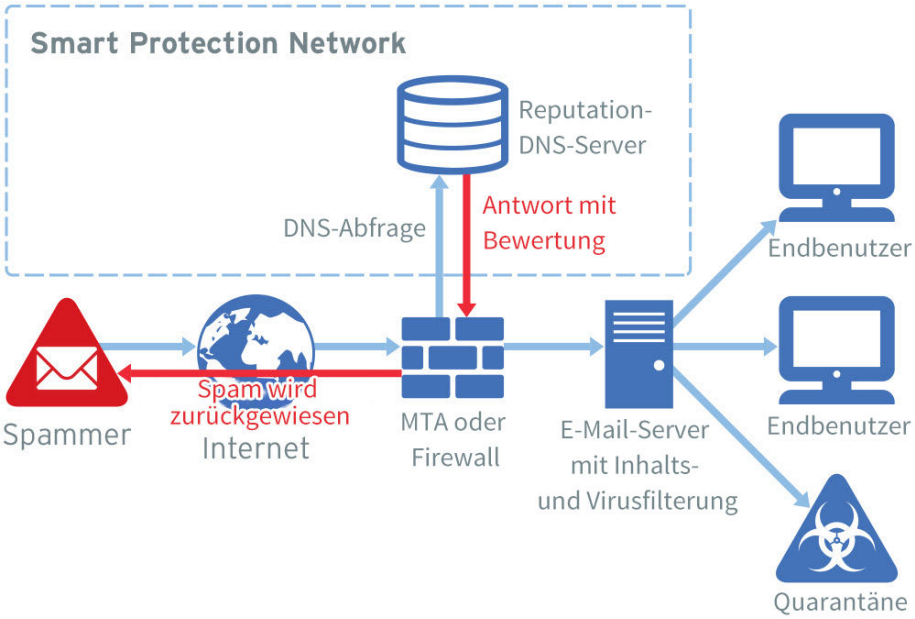

ABBILDUNG 1-1. Smart Protection Network-Workflow

Standard-Edition: Eine einzelne DNS-Abfrage wird an die Standard-Reputation-Datenbank gesendet, die bekannte und dokumentierte Spam-Quellen sowie umfangreiche Listen mit dynamischen IP-Adressen enthält. Eine positive Antwort seitens dieser Datenbank sollte dazu führen, dass der E-Mail-Server einen Fehler vom Typ 550 oder eine Ablehnung der angeforderten Verbindung zurückgibt.

Advanced-Edition: Eine einzelne DNS-Abfrage wird an die Standard- und dynamische Reputation-Datenbank gesendet. Eine positive Antwort seitens der dynamischen Datenbank sollte dazu führen, dass der E-Mail-Server einen Fehler vom Typ 450 oder einen temporären Ausfall der angeforderten Verbindung zurückgibt. Bei den Listen in dieser Datenbank handelt es sich gelegentlich um rechtmäßige E-Mail-Server mit infizierten Hosts, die vorübergehend Spam versenden. Wenn die Verbindungsanforderung von einem rechtmäßigen E-Mail-Server ausgeht, wird sie erneut in die Warteschlange eingereiht und zu einem späteren Zeitpunkt wiederholt. Dies führt bis zum Ablauf der Auflistung zu Verzögerungen bei der E-Mail-Zustellung, die E-Mail wird aber nicht gesperrt.

Abhängig von den Funktionen des E-Mail-Servers stehen Ihnen unter Umständen weitere Optionen für die Verarbeitung von IP-Verbindungen zur Verfügung. Mithilfe bestimmter Optionen kann die Anzahl an Verbindungen gedrosselt oder beschränkt werden, die von einem Internetprotokoll während eines festgelegten Zeitraums akzeptiert werden. Andere Optionen wiederum ermöglichen Ihnen die Einrichtung verschiedener Suchebenen für Nachrichten von fragwürdigen IP-Adressen im Gegensatz zu bekannten IP-Adressen. Das Hauptziel besteht darin, möglichst viele Verbindungen bei der ersten Anfrage zurückzuweisen. Bei diesen zurückgewiesenen Verbindungen handelt es sich um Spam-Nachrichten, die niemals akzeptiert werden und daher nie in der E-Mail-Infrastruktur auftauchen. Indem Sie die Infrastruktur vor unerwünschten Spam-Nachrichten schützen, sorgen Sie dafür, dass wichtige Bandbreiten-, Verarbeitungs- und Speicherressourcen geschont werden.

Verbindungen anstelle von Nachrichten sperren

Kunden sind der Meinung, dass das Hinzufügen von Email Reputation Services zu ihren Anti-Spam-Lösungen enorme Auswirkungen auf die Auslagerung bestehender Filterlösungen hat. Was nur wie ein geringer Anstieg der blockierten Verbindungen erscheinen mag, kann sich in einer drastischen Abnahme der tatsächlichen Nachrichten niederschlagen, die in der jeweiligen E-Mail-Infrastruktur gefiltert werden.

Die Überführung gesperrter Verbindungen in gesperrte Nachrichten erfordert mehr Aufwand, als sich aus einem 1:1-Verhältnis ergeben würde.

Untersuchungen belegen, dass rechtmäßige Quellen durchschnittlich etwas mehr als eine Nachricht pro Verbindung enthalten, während jede Verbindung aus einer Spam-Quelle konservativ gerechnet 1,6 Nachrichten im Durchschnitt enthält.

Es erweist sich als weitaus effizienter, Spam auf der Verbindungsebene zurückzuweisen, als jede Nachricht die vollständige Anti-Spam-Überprüfung durchlaufen zu lassen.

TABELLE 1-1. Anforderungen für Verbindungssperrung und Überprüfung

Anforderungen für das Sperren von Verbindungen	Anforderungen für die Überprüfung aller Nachrichten
Der erste Teil des SMTP-Handshakes	Der vollständige SMTP-Handshake
Eine DNS-Abfrage	Vollständige Nachrichtenanalyse belastet Computer, auf denen Anti-Spam-Lösungen ausgeführt werden

Kapitel 2

Gesperrt?

Wenn Ihre ISP-Adresse gesperrt wurde, Sie aber in keiner der Email Reputation Services-Listen als Administrator der IP-Adresse(n) geführt werden, wenden Sie sich zur Behebung des Problems an den ISP. Trend Micro Email Reputation Services kann keine Probleme bezüglich der gesperrten Listen für Endbenutzer oder diejenigen Benutzer beheben, die nicht direkt für das entsprechende Netzwerk in den gesperrten Listen verantwortlich sind.

Wenn Sie als ISP-Anbieter fungieren und Ihre IP-Adresse oder die IP-Adresse Ihres Abonnenten gesperrt wurde, finden Sie weitere Informationen unter *Schritt 3: Anforderung zum Entfernen senden auf Seite 2-5*.

Hinweis

Trend Micro entfernt IP-Adressen nur auf Anforderung des gültigen Eigentümers des IP-Raums.

Für das Nichtentfernen einer IP-Adresse aus den gesperrten Listen sind verschiedene Gründe denkbar:

- Umstrukturierung des Netzwerks

  Wenn ein ISP, insbesondere ein kleinerer mit einem oder mehreren Netzwerken der Klasse C, seinen IP-Adresspool so umstrukturiert, dass die festen Server und Einwahlserver ihre Plätze tauschen.

- Netzwerkvererbung

  Wenn Sie einen Adresspool geerbt haben, der zuvor gesperrt wurde oder immer noch gesperrt ist.

- Fehler beim Auflisten

  Da IP-Adressen dynamisch sind, wurden bestimmte IP-Adressen unter Umständen fälschlicherweise zu den gesperrten Listen hinzugefügt.

Warum wird Ihre Adresse gesperrt? Mögliche Gründe:

- Wenn sich Ihre IP-Adresse in der DUL-Liste befindet und:
  - Sie einen Standard-Mail-Client verwenden, liegt es wahrscheinlich daran, dass Ihr Mail-Programm so eingerichtet ist, dass es einen anderen Mail-Server als den von Ihrem aktuellen ISP bereitgestellten Server verwendet.
  - Sie einen Mail-Server (SMTP) auf Ihrem Computer verwenden oder Ihre Internetverbindung für verschiedene andere Personen in einem lokalen Netzwerk mit einem Proxy-Server freigeben, liegt es wahrscheinlich daran, dass Ihre Empfänger nicht zwischen der rechtmäßigen E-Mail-Zustellung und dem unbefugten Eindringen eines Spammers in die jeweiligen Geräte unterscheiden können.
- Wenn sich Ihre IP-Adresse in der Liste der bekannten Spam-Quellen befindet, wird Ihre IP-Adresse unter Umständen aus folgenden Gründen gesperrt:
  - Bei der IP-Adresse handelt es sich unter Umständen um eine bekannte Spam-Quelle
  - Die IP-Adresse unterstützt unter Umständen einen Dienst, der Spam sendet
  - Die IP-Adresse verwendet unter Umständen ein Open Relay mit mehreren Hops
  - Die IP-Adresse verwendet unter Umständen einen infizierten Host
- Befindet sich Ihre IP-Adresse in der QIL-Liste, finden auf Ihrem Computer oder Server unter Umständen nicht autorisierte Aktivitäten

statt. Dies kann bedeuten, dass Ihr Computer gehackt oder infiziert wurde.

Schritt 1: IP-Adresse festlegen

Sie können die Befehlskonsole verwenden, um nach Ihrer IP-Adresse zu suchen. Wenn Sie jedoch nicht genau wissen, nach welcher IP-Adresse Sie suchen möchten, überprüfen Sie die unzustellbaren E-Mail-Nachrichten und -Header auf eine Zeile ähnlich der folgenden:

Prozedur

- 550 Dienst nicht verfügbar; Client-Host [127.0.0.2] mithilfe von Trend Micro RBL+ gesperrt.

  Weitere Informationen finden Sie unter https://www.ers.trendmicro.com/reputations/index?ip_address=127.0.0.2

Die zu überprüfende IP-Adresse lautet in diesem Fall 127.0.0.2.

Schritt 2: Status der IP-Adresse überprüfen

Wenn Sie vermuten, dass Ihre IP-Adresse gesperrt wurde, können Sie mithilfe des Suchformulars überprüfen, ob dies zutrifft.

Prozedur

- Wenn die IP-Adresse mithilfe des Formulars in keiner Liste gefunden werden kann, wenden Sie sich an den Administrator oder ISP-Anbieter.
- Wenn die IP-Adresse gesperrt wurde, wird in diesem Formular die Liste angezeigt, in der sich die IP-Adresse befindet. Wenn sich die IP-Adresse in mehr als einer Liste befindet, müssen Sie für jede Liste eine Anforderung zum Entfernen senden. Weitere Informationen finden Sie unter *Schritt 3: Anforderung zum Entfernen senden auf Seite 2-5*.

Hinweis

Stellen Sie sicher, dass Sie die richtigen Kontaktdaten und den richtigen Prozess verwenden, um das Entfernen der IP-Adresse aus einer Liste anzufordern. Wenn Sie die Anfrage an einen ungeeigneten Kontakt senden, kommt es zu Verzögerungen und einer möglichen Nichtverarbeitung der Anfrage.

Schritt 3: Anforderung zum Entfernen senden

Nachdem Sie festgestellt haben, dass die IP-Adresse gesperrt wurde, können Sie für jede Liste eine Anforderung zum Entfernen senden.

Prozedur

1. Überprüfen Sie den Status Ihrer IP-Adresse. Weitere Informationen finden Sie unter *Schritt 1: IP-Adresse festlegen auf Seite 2-4*.
2. Senden Sie eine Anforderung zum Entfernen der IP-Adresse:
   - Senden Sie eine Anforderung an Ihren Administrator oder ISP-Anbieter.
   - Als Administrator oder ISP-Anbieter senden Sie eine Anforderung an Trend Micro:
     a. Klicken Sie auf den Link „Aus der Globalen Blockiert-Liste zu entfernende Anforderung“.
     b. Sie müssen die angeforderten Informationen im Web-Formular angeben.
     c. Klicken Sie auf **Senden**.

Hinweis

Anforderungen zum Entfernen müssen aus einem autorisierten Konto stammen, wie z. B. abuse@(Domänenname) oder postmaster@(Domänenname). Auf diese Weise wird sichergestellt, dass Trend Micro in Kontakt mit dem gültigen Besitzer der IP-Blöcke steht.

Schritt 4: Untersuchung

Nachdem Trend Micro die erforderlichen Informationen erhalten hat, werden die IP-Adressen überwacht, und Trend Micro kommuniziert mit den Eigentümern der IP-Blöcke, um die Gültigkeit der Ansprüche zu ermitteln.

Trend Micro ermittelt die Aktionen, die zur Auflistung geführt haben, sowie die Maßnahmen, die zur Behebung und zur Vermeidung eines erneuten Auftretens dieser Probleme in der Zukunft ergriffen wurden. Gegebenenfalls werden Richtlinien zur Handhabung bei Missbrauch, AUPs (Acceptable Use Policies) und sämtliche in der Benachrichtigung aufgetretenen Probleme angefordert.

Diese Diskussionen werden dokumentiert und untersucht, um mit einer Empfehlung für die Auflistung fortzufahren (Entfernung, Probezeit, Auflistung beibehalten). Es gibt eine Probezeit, in der die IP-Adresse aus der Liste entfernt, aber ohne neue Nominierung wieder aktiviert werden kann, wenn es neue Vorfälle gibt. Die Auflistung wird über einen angemessenen Zeitraum überwacht, um sicherzustellen, dass keine neuen Spam-Aktivitäten auftreten. Wenn am Ende der Probezeit keine neuen Spam-Aktivitäten aufgetreten sind, entfernt Trend Micro die IP-Adresse aus den gesperrten Listen.

Kapitel 3

Erste Schritte

Dieses Kapitel enthält Informationen zu den ersten Schritten mit Trend Micro ™ Email Reputation Services.

Email Reputation Services konfigurieren

Email Reputation Services ist am effektivsten, wenn es die erste Verteidigungslinie in Ihrer Messaging-Infrastruktur darstellt. Trend Micro empfiehlt, alle anderen DNS-Sperrtechniken nach der Aktivierung von Email Reputation Services zu entfernen.

Informationen zum Aktivieren und Konfigurieren von Email Reputation Services finden Sie unter:

- *Konto erstellen auf Seite 3-2*
- *MTA konfigurieren auf Seite 3-5*

Konto erstellen

Erstellen Sie ein Konto, um sich anzumelden. Sie können Email Reputation Services testen (siehe *Testkonto anfordern auf Seite 3-4*) oder den vollständigen Service erwerben. Nach der Anmeldung erhalten Sie eine E-Mail mit Anweisungen zur weiteren Vorgehensweise.

Wenn Sie sich für eine Testversion registrieren, müssen Sie das Anforderungsformular ausfüllen, das für den zu testenden Servicelevel geeignet ist. Bei Erwerb des vollständigen Service stellt Trend Micro Ihnen Anweisungen zum Erstellen eines Kundenkontos bereit. Anschließend erhalten Sie von Trend Micro einen Aktivierungscode per E-Mail.

Mithilfe des Aktivierungscodes können Sie nur auf den Servicelevel zugreifen, bei dem Sie registriert sind (Standard oder Advanced).

Hinweis

Der Aktivierungscode für Email Reputation Services Advanced beinhaltet Zugriff auf Email Reputation Services Standard (eine Unterkomponente).

Es kann bis zu einer Stunde dauern, bis der ausgegebene Aktivierungscode von den Trend Micro Email Reputation Services Systemen erkannt wird.

Wenn Sie kein Konto erstellen, können Sie weiterhin die Reputation einer IP-Adresse abfragen (siehe *Nach IP-Adressen suchen auf Seite 4-5*) oder eine IP-

Adresse für die Globale Genehmigt-Liste (siehe *Globale Genehmigt-Liste auf Seite 4-6*) nominieren. Die Einstellungen für besseren Spam-Schutz können jedoch nicht konfiguriert werden.

Prozedur

1. Öffnen Sie den Browser mithilfe der folgenden URL:

   https://www.ers.trendmicro.com

2. Klicken Sie auf den Link **Registrieren** unterhalb der Anmeldefelder.

   Die Seite **Konto erstellen** wird angezeigt.

3. Stellen Sie die folgenden Informationen bereit:

   - Aktivierungscode

     Hinweis

     Wenn Sie den Service nicht gekauft haben und ihn lediglich testen möchten, klicken Sie auf **Link für einen Testaktivierungscode anfordern**. Weitere Informationen finden Sie unter *Testkonto anfordern auf Seite 3-4*.

   - E-Mail (zweimal)
   - Kennwort (zweimal)
   - Vorname
   - Nachname
   - Firmenname
   - Land/Region
   - Firmentyp

Hinweis

Der Aktivierungscode sollte mit dem Aktivierungscode übereinstimmen, der beim Konfigurieren des MTA für den Zugriff auf Email Reputation Services verwendet wurde. Trend Micro sendet eine E-Mail-Nachricht an die im Formular angegebene Adresse. Diese Nachricht enthält den Benutzernamen, das Kennwort und eine URL, auf die Sie zum Aktivieren des Kontos klicken können.

4. Klicken Sie auf „Registrieren“.

Testkonto anfordern

Wenn Sie den Dienst nicht erworben haben und lediglich testen möchten, können Sie einen Aktivierungscode für die Testversion anfordern.

Nachdem Sie sich für den Testdienst registriert haben, erhalten Sie von Trend Micro eine E-Mail mit dem Aktivierungscode und Anweisungen zur Konfiguration Ihres MTA. Dieser Aktivierungscode ist nur während des Testzeitraums gültig. Sie müssen einen neuen Aktivierungscode anfordern, wenn Sie den Dienst erwerben.

Prozedur

1. Öffnen Sie den Browser mithilfe der folgenden URL:

   https://www.ers.trendmicro.com

2. Klicken Sie auf den Link **Registrieren** unterhalb der Anmeldefelder.

   Die Seite **Konto erstellen** wird angezeigt.

3. Klicken Sie auf den Link **Aktivierungscode für Testversion anfordern**.

   Die Seite **Email Security Advanced Kostenlose 30-tägige Testversion** wird angezeigt.

4. Füllen Sie das Formular aus, um Ihre kostenlose Testversion anzufordern.

5. Kehren Sie zur Seite **Konto erstellen** zurück.

6. Geben Sie den Aktivierungscode der Testversion und die erforderlichen Informationen an, um Ihr Email Reputation Services Konto zu registrieren.

MTA konfigurieren

Der nächste Schritt besteht in der Konfiguration Ihres MTA zum Durchführen der geeigneten DNS-Abfragen für den Typ von Email Reputation Services, den Sie abonniert haben:

- Standard: Verbindungen mit einem Fehlercode der Ebene 550 (Verbindung verweigert) werden zurückgewiesen. Ihr MTA gibt diesen Fehlercode an den Server zurück, der die Verbindung initiiert hat, da die IP-Adresse zu einem bekannten Spammer in der Standard-Reputation-Datenbank gehört.

- Advanced: Nachdem die Standard- und die dynamische Reputation-Datenbank abgefragt wurden, gibt der MTA einen Fehlercode der Ebene 450 (Server vorübergehend nicht verfügbar, versuchen Sie es erneut) für die vorübergehende Ablehnung der Verbindung zurück, wenn sich die IP-Adresse in der dynamischen Reputation-Datenbank befindet.

Rechtmäßige E-Mail-Server mit infizierten Hosts, die vorübergehend Spam-Nachrichten senden, können in der dynamischen Reputation-Datenbank aufgelistet werden. Wenn die Verbindungsanforderung von einem rechtmäßigen E-Mail-Server ausgeht, wird sie erneut in die Warteschlange eingereiht, und die Nachricht wird zu einem späteren Zeitpunkt gesendet. Dieser Vorgang führt bis zum Ablauf der Auflistung zu einer kurzen Verzögerung bei der E-Mail-Zustellung. Die E-Mail wird jedoch nicht dauerhaft gesperrt.

Bestimmte Server verfügen über zusätzliche Optionen zum Verarbeiten fragwürdiger IP-Verbindungen. Zu diesen Optionen gehören die Drosselung und die Weiterleitung von Nachrichten zur detaillierten Überprüfung.

Ausführliche Konfigurations- und Setup-Optionen erhalten Sie in den Produkthandbüchern und/oder beim technischen Support. Weitere Informationen finden Sie unter https://success.trendmicro.com/

Bei der Konsole anmelden

Email Reputation Services ist Teil des Trend Micro Smart Protection Network.

Prozedur

1. Öffnen Sie den Browser mithilfe der folgenden URL:

   https://www.ers.trendmicro.com

2. Geben Sie Ihren Benutzernamen oder Ihre E-Mail und Ihr Kennwort ein.

3. Klicken Sie auf **Anmelden**.

   Das Trend Micro Email Reputation Services Portal wird angezeigt.

Tipp

Trend Micro empfiehlt, das Kennwort nach der ersten Anmeldung zu ändern.

Weitere Informationen finden Sie unter *Kontodaten ändern auf Seite 4-16*.

Kennwort vergessen

Wenn Sie Ihr Kennwort vergessen haben und sich nicht mehr beim Dienst anmelden können, können Sie Ihr Kennwort zurücksetzen.

Prozedur

1. Öffnen Sie den Browser mithilfe der folgenden URL:

   https://www.ers.trendmicro.com

2. Klicken Sie auf den Link **Kennwort vergessen?** unterhalb des Kennwortfelds.
3. Geben Sie Ihre E-Mail ein. Sie erhalten eine E-Mail-Nachricht von Trend Micro.
4. Klicken Sie auf den Link in der E-Mail.

   Der Bildschirm **Kennwort zurücksetzen** wird angezeigt.
5. Geben Sie Ihr neues Kennwort zweimal ein.
6. Klicken Sie auf **Aktualisieren**.

Kapitel 4

Verwenden der Verwaltungskonsole

Melden Sie sich nach der Erstellung des Trend Micro ™ Email Reputation Services Kontos bei der Verwaltungskonsole an und konfigurieren Sie die Einstellungen.

Email Reputation Services-Konsole

Die umfangreiche Karte und das dazugehörige Diagramm auf diesem Bildschirm zeigen Spam-Statistiken, die aus Rechenzentren weltweit zusammengestellt wurden.

Dieses Dashboard bietet folgende Möglichkeiten:

- Anzeigen der globalen Spam-Bedrohungsstatistiken, siehe *Globale Spam-Bedrohungen auf Seite 4-2*.
- Anzeigen Ihrer Netzwerkstatistiken, siehe *Ihr Netzwerk auf Seite 4-3*.

Hinweis

Sie können die Netzwerkstatistiken erst dann über das Dashboard anzeigen, wenn Sie sich angemeldet haben.

- Suchen nach einer IP-Adress-Reputation, siehe *Nach IP-Adressen suchen auf Seite 4-5*.
- Nominieren einer IP-Adresse für die Datenbank der Globale Genehmigt-Liste, siehe *Globale Genehmigt-Liste auf Seite 4-6*.
- Klicken Sie auf den Link zu den globalen Spam-Nachrichten, in denen aktuell wichtige Spam-Angriffe mit Screenshots und Lösungsdetails für Trend Micro Benutzer dargestellt werden.

Globale Spam-Bedrohungen

Auf dieser Registerkarte werden zwei Arten von Statistiken angezeigt:

Prozedur

- Statistiken für globale Spam-Bedrohungen nach Land

  Je dunkler die Farbe, desto höher ist die Spam-Rate eines Landes. Trend Micro berechnet die Spam-Rate anhand der über das Netzwerk geleiteten E-Mail-Nachrichten und anhand der von Email Reputation Services gesperrten Spam-Nachrichten.

Zur Anzeige weiterer Informationen können Sie folgendermaßen vorgehen:

- Wenn Sie den Mauszeiger über ein bestimmtes Land bewegen, wird ein Ballonsymbol mit der aktuellen Statistik angezeigt.
- Verwenden Sie den linken Schieberegler, um die Karte zu vergrößern oder zur näheren Betrachtung zu verkleinern.
- Klicken Sie auf das Start-Symbol, um die ursprüngliche Größe wiederherzustellen.
- Klicken Sie auf die Karte oder die Diagramminformationen und verschieben Sie sie an eine neue Position.

- Ein visuelles Diagramm mit Spam-Daten

  Der Spam-Index zeigt die aktuellen Spam-Trends, die sich aus der Überwachung der Spam-Menge ergeben, die an Email Reputation-Server weltweit gesendet wird.

  Sie können die Spam-Trends filtern, indem Sie auf „Woche“, „Monat“ oder „Jahr“ klicken.

Ihr Netzwerk

Nach der Anmeldung können Sie auf dieser Registerkarte zwei Arten von Statistiken anzeigen:

Prozedur

- Spam-Statistiken für Ihr Netzwerk

  Zur Anzeige der aktuellen Statistiken für Ihr Netzwerk auf der Karte klicken Sie auf das blinkende Globus-Symbol „MY ERS“ für ein bestimmtes Land. Ein Fenster mit dem Namen des Landes wird angezeigt.

  Zur Anzeige weiterer Informationen können Sie folgendermaßen vorgehen:

  - Wenn Sie den Mauszeiger über ein bestimmtes Land bewegen, wird ein Ballonsymbol mit der aktuellen Statistik angezeigt.
  - Verwenden Sie den linken Schieberegler, um die Karte zu vergrößern oder zur näheren Betrachtung zu verkleinern.
  - Klicken Sie auf das Start-Symbol, um die ursprüngliche Größe wiederherzustellen.
  - Klicken Sie auf die Karte oder die Diagramminformationen und verschieben Sie sie an eine neue Position.

- Ein visuelles Diagramm aller E-Mail-Nachrichten, die von Ihrem Netzwerk empfangen und gesperrt wurden

  Email Reputation Services bietet Schutz vor bekannten und unbekannten Spam-Quellen, indem Spam-Nachrichten auf der Ebene der SMTP-Verbindung gesperrt werden. Wenn ein Mail-Server eine Verbindung zu einem MTA herstellt, der mit Email Reputation Services geschützt ist, werden bei der DNS-Auflösung die Email Reputation Services-Listen unter Verwendung der mit dem Konto verknüpften Kriterien abgefragt.

  Wenn Email Reputation Services meldet, dass der E-Mail-Server in einer der Email Reputation Services-Listen aufgeführt wird, wird dieser Verbindungsversuch zur Anzahl der gesperrten Spam-Nachrichten hinzugefügt.

  Sie können die Spam-Trends filtern, indem Sie auf „Tag“, „Woche“ oder „Monat“ klicken.

IP-Reputation

In diesem Abschnitt können Sie folgende Aufgaben durchführen:

- Suchen nach IP-Adressen (siehe *Nach IP-Adressen suchen auf Seite 4-5*)

- Nominieren einer IP-Adresse für die Globale Genehmigt-Liste (siehe *Globale Genehmigt-Liste auf Seite 4-6*)

Nach IP-Adressen suchen

Wenn Sie den Verdacht haben, dass Ihre IP-Adresse von Email Reputation Services gesperrt wird, suchen Sie nach der vollständigen IP-Adresse und ermitteln Sie die Datenbank, in der die Adresse aufgelistet wird.

Hinweis

Dieses Suchtool basiert auf IP-Adressen und verwendet keine Host- oder Domänennamen.

So suchen Sie nach einer IP-Adresse:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Navigieren Sie zu **IP-Reputation** > **Nachschlagen**.

3. Geben Sie die IP-Adresse ein.

4. Klicken Sie auf **Prüfen**.

   Abhängig von den Ergebnissen können Sie eine der folgenden Aktionen ausführen:

   - Befindet sich die IP-Adresse nicht in einer der Email Reputation Services-Datenbanken, stammt die IP-Adresse aus einer seriösen Quelle. Sie können Trend Micro bitten, diese IP-Adresse zur Globale Genehmigt-Liste' hinzuzufügen (siehe *Globale Genehmigt-Liste auf Seite 4-6*).

   - Wenn die IP-Adresse nicht aufgelistet wird, Sie aber der Meinung sind, dass über die Adresse Spam gesendet wird und Sie an der

Integrität der IP-Adresse zweifeln, können Sie die IP-Adresse in Ihrem Netzwerk sperren (siehe *Blockiert Listen auf Seite 4-11*).

- Wenn die Adresse aufgelistet wird, können Sie darum bitten, sie vorübergehend aus der Globalen Blockiert-Liste zu entfernen.

Globale Genehmigt-Liste

Trend Micro unterhält mehrere Datenbanken, bei denen es sich je nach dem jeweiligen Verhalten entweder um genehmigte oder gesperrte IP-Adressen handelt. Eine dieser Datenbanken ist die Globale Genehmigt-Liste. IP-Adressen in dieser Liste stellen IP-Adressen dar, die authentifiziert wurden und bekanntermaßen von zulässigen Absendern stammen. IP-Adressen in dieser Liste sind automatisch zugelassen und durchlaufen das Netzwerk.

Obwohl diese Datenbank von Trend Micro unterhalten wird, können Sie auch Ihre IP-Adresse nominieren und dieser Liste hinzufügen. Trend Micro wird dann eine entsprechende Untersuchung durchführen und feststellen, ob die von Ihnen nominierte IP-Adresse tatsächlich in diese Datenbank aufgenommen werden soll.

So nominieren Sie eine IP-Adresse für die Globale Genehmigt-Liste:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Navigieren Sie zu **IP-Reputation** > **Globale Genehmigt-Liste**.

3. Lesen Sie sich die Beschreibung der Globale Genehmigt-Liste durch. Wenn Sie einverstanden sind, klicken Sie auf **Zur Kenntnis genommen, ich stimme zu.**.

Hinweis

Geben Sie alle erforderlichen Informationen auf den folgenden Registerkarten an, um sicherzustellen, dass Trend Micro eine vollständige Untersuchung durchführen kann. Sie werden unter Umständen zur Eingabe weiterer Informationen aufgefordert, wenn die bereitgestellten Informationen nicht ausreichen.

4. Über die Registerkarte **Mail Transfer Agent**:

   - So fügen Sie einen oder zwei Einträge hinzu:

     a. Geben Sie Folgendes an:

        - IP
        - FQDN
        - E-Mail-Domänenname
        - Firmenname
        - Land/Region
        - Firmentyp

     b. Um einen weiteren Eintrag hinzuzufügen, klicken Sie auf **Land hinzufügen**.

   - So fügen Sie weitere Mail Transfer Agent-Einträge hinzu:

     a. Laden Sie eine CSV-Beispieldatei herunter.

     b. Geben Sie die erforderlichen Informationen ein, und speichern Sie die Datei.

     c. Importieren Sie die Datei auf die Website.

5. Über die Registerkarte **HELO/EHLO-Prüfung**:

   - Geben Sie die Zeichenfolge HELO/EHLO an, um einen oder zwei Einträge hinzuzufügen. Sie können auch auf **Eintrag hinzufügen** klicken, um eine weitere Zeichenfolge hinzuzufügen.

- So fügen Sie weitere HELO-/EHLO-Zeichenfolgeneinträge hinzu:

  a. Laden Sie eine CSV-Beispieldatei herunter.

  b. Geben Sie die erforderlichen Informationen ein, und speichern Sie die Datei.

  c. Importieren Sie die Datei auf die Website.

6. Geben Sie auf der Registerkarte **Kontaktdaten** Ihre E-Mail sowie Ihren Vor- und Nachnamen an.

7. Klicken Sie auf **Nominieren**.

   Trend Micro führt eine Untersuchung durch und legt fest, ob die IP-Adresse zur Globale Genehmigt-Liste hinzugefügt werden kann. Wenn die IP-Adresse die Kriterien zum Hinzufügen zur Globale Genehmigt-Liste nicht erfüllt, können Sie die IP-Adresse dennoch zu Ihren internen zulässigen Listen (*Genehmigt-Listen auf Seite 4-9*) hinzufügen.

Richtlinie verwalten

Im Abschnitt „Richtlinien“ können Sie folgende Aktionen ausführen:

- Erstellen einer Liste mit der Bezeichnung „Zulässige Absender“, um E-Mail-Nachrichten aus bestimmten vertrauenswürdigen Ländern und von bestimmten vertrauenswürdigen IP-Adressen immer zu erhalten.
- Erstellen einer Liste mit der Bezeichnung „Blockierte Absender“', um E-Mail-Nachrichten aus bestimmten Ländern und von bestimmten IP-Adressen immer zu sperren.
- Anpassen der dynamischen Reputation-Einstellungen

Sie können die Listen anhand einzelner IPv4- oder IPv6-IP-Adressen oder nach Land definieren.

Genehmigt-Listen

Mithilfe zulässiger Listen können Nachrichten zulässiger Absender die Filterung auf IP-Ebene umgehen. Die zulässigen Listen werden nicht auf Ihren MTA angewendet. Sie können aber weitere zulässige oder blockierte Absender einrichten oder zusätzliche Filterung bei Ihrem MTA durchführen. Der Nachteil, der sich aus der IP-Filterung ergibt, besteht in den zusätzlichen Ressourcen, die zum Verarbeiten, Filtern und Speichern des höheren Aufkommens von Spam-Nachrichten benötigt werden, die andernfalls blockiert würden.

Bei der Suche nach Standard-Reputation-Diensten (Liste der bekannten Spam-Quellen) lautet die Reihenfolge der Bewertungshierarchie wie folgt:

1. Zulässige IP
2. Gesperrte IP
3. Zulässiges Land
4. Gesperrtes Land

Bei der Suche nach dynamischen Reputation-Diensten (QIL) werden die vom Kunden definierten „gesperrten Richtlinienlisten“ (IP, Land) ignoriert, und nur die zulässigen Listen werden überprüft. Andernfalls entspricht die Reihenfolge der Richtliniensuche (erst IP, dann Land) der Reihenfolge des Standard-Reputation-Diensts (Liste der bekannten Spam-Quellen).

Geben Sie keine überlappenden CIDR-Bereiche in den zulässigen oder gesperrter Listen ein, da die gesperrte Liste unter Umständen Vorrang vor der zulässigen Liste hat.

So fügen Sie die zulässige Liste hinzu:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Klicken Sie auf **Richtlinie** > **Genehmigt-Listen**.

3. Wählen Sie das Land aus und klicken Sie auf **Hinzufügen>**. Der Name des ausgewählten Landes sollte in den rechten Rahmen verschoben werden.

   Warnung!

   Gehen Sie beim Hinzufügen eines Landes umsichtig vor, da unter Umständen auch bekannte Spammer zur zulässigen Liste hinzugefügt werden.

4. Geben Sie die IPv4- oder IPv6-Adresse an und klicken Sie auf „Hinzufügen >“. Die IP-Adresse sollte in den rechten Rahmen verschoben werden.

   Wenn Sie die IP-Adresse angeben, steht Ihnen eine der folgenden Optionen zur Verfügung:

   - IPv4-Standardformat: 123.123.123.123
   - IPv4-IP-Adressbereich in CIDR-Notation: 123.123.123.123/24

     Hinweis

     Vermeiden Sie die Angabe desselben CIDR-Bereichs in den zulässigen und gesperrten Listen, da dies zu unerwarteten Ergebnissen führen kann. Bei Bedarf muss der zulässige CIDR-Bereich kleiner oder gleich dem gesperrten CIDR-Bereich sein.

     Beispiel: Vermeiden Sie die Angabe von 172.31.15.164/30 in der zulässigen Liste und die Angabe von 172.31.15.164/31 in der gesperrten Liste.

   - IPv6-Standardformat:
     - 2001:0db7:85a3:0000:0000:8a2e:0370:7334
     - 2001:db7:85a3:0:0:8a2e:370:7334
     - 2001:db7:85a3::8a2e:370:7334

5. Klicken Sie auf **Speichern**.

Blockiert Listen

Blockiert Listen stoppen Nachrichten von den gesperrten Absendern unter Umgehung der Filterung auf IP-Ebene. Die gesperrten Listen werden nicht auf Ihren MTA angewendet. Sie können aber weitere gesperrte oder zulässige Absender einrichten oder zusätzliche Filterung bei Ihrem MTA durchführen. Der Nachteil, der sich aus der IP-Filterung ergibt, besteht in den zusätzlichen Ressourcen, die zum Verarbeiten, Filtern und Speichern des höheren Aufkommens an Spam-Nachrichten benötigt werden, die andernfalls blockiert würden. Bei Verwendung der gesperrten Listen kann es zu einer insgesamt niedrigeren Spam-Erfassungsrate kommen.

Bei der Suche nach Standard-Reputation-Diensten (Liste der bekannten Spam-Quellen) lautet die Reihenfolge der Bewertungshierarchie wie folgt:

1. Zulässige IP
2. Gesperrte IP
3. Zulässiges Land
4. Gesperrtes Land

Bei der Suche nach dynamischen Reputation-Diensten (QIL) werden die vom Kunden definierten „gesperrten Richtlinienlisten“ (IP, Land) ignoriert, und nur die zulässigen Listen werden überprüft. Andernfalls entspricht die Reihenfolge der Richtliniensuche (erst IP, dann Land) der Reihenfolge des Standard-Reputation-Diensts (Liste der bekannten Spam-Quellen).

So fügen Sie Elemente zur gesperrten Liste hinzu:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Klicken Sie auf **Richtlinie** > **Blockiert Listen**.

3. Wählen Sie das Land aus und klicken Sie auf **Hinzufügen>**. Der Name des ausgewählten Landes sollte in den rechten Rahmen verschoben werden.

4. Geben Sie die IPv4- oder IPv6-Adresse an und klicken Sie auf **Hinzufügen>**. Die IP-Adresse sollte in den rechten Rahmen verschoben werden.

   Wenn Sie die IP-Adresse angeben, steht Ihnen eine der folgenden Optionen zur Verfügung:

   - IPv4-Standardformat: 123.123.123.123
   - IPv4-IP-Adressbereich in CIDR-Notation: 123.123.123.123/24

     Hinweis

     Vermeiden Sie die Angabe desselben CIDR-Bereichs in den zulässigen und gesperrten Listen, da dies zu unerwarteten Ergebnissen führen kann. Bei Bedarf muss der zulässige CIDR-Bereich kleiner oder gleich dem gesperrten CIDR-Bereich sein.

     Beispiel: Vermeiden Sie die Angabe von 172.31.15.164/30 in der zulässigen Liste und die Angabe von 172.31.15.164/31 in der gesperrten Liste.

   - IPv6-Standardformat:
     - 2001:0db7:85a3:0000:0000:8a2e:0370:7334
     - 2001:db7:85a3:0:0:8a2e:370:7334
     - 2001:db7:85a3::8a2e:370:7334

5. Klicken Sie auf **Speichern**.

Reputation-Einstellungen

Sie können die zu aktivierenden Listen aus den Listen auswählen, die die Standard-Reputation-Datenbank bilden. Standardmäßig sind alle Listen aktiviert. Bei der Standardeinstellung handelt es sich um die wirksamste Kombination zur Reduzierung von Spam. Des weiteren erfüllt sie die Anforderungen der meisten Kunden. Sie können auch den Schieberegler der dynamischen Reputation verwenden, um den Grad der Strenge anzugeben,

mit der E-Mail-Verbindungen von Email Reputation Services gesperrt werden sollen.

Warnung!

Wenn Sie bestimmte Listen in der Standarddatenbank deaktivieren, kommt es möglicherweise zu einem Anstieg der Spam-Nachrichten, die auf Ihrem internen E-Mail-Server einer zusätzlichen Inhaltsfilterung unterzogen werden müssen.

Standard Reputation Services-Datenbank

Die Standard Reputation Services enthalten eine Datenbank mit den folgenden Listen:

- Bei der **Liste der bekannten Spam-Quellen** handelt es sich um eine Liste mit IP-Adressen von E-Mail-Servern, die als Spam-Quellen bekannt sind.
- Bei der **Liste der DFÜ-Benutzer (DUL)** handelt es sich um eine Liste dynamisch zugewiesener IP-Adressen oder jenen mit einer Acceptable Use Policy (AUP), die öffentliche E-Mail-Server verbietet. Die meisten Einträge werden in Zusammenarbeit mit dem ISP verwaltet, dem der Netzwerkspeicherplatz gehört. IP-Adressen in dieser Liste sollten E-Mails nicht direkt senden, sondern die E-Mail-Server des zugehörigen ISP verwenden.
- Die **Liste mit neuen Bedrohungen (ETL)** enthält IP-Adressen von E-Mail-Servern, die an aktiven Ransomware-, Malware- oder anderen E-Mail-Bedrohungskampagnen beteiligt sind.

Für den Bereich „Standard“:

- Sie können die Durchsuchung ausgewählter Listen aktivieren oder deaktivieren, indem Sie die Kontrollkästchen verwenden.
  - Aktivieren Sie das Kontrollkästchen, um die Liste zu aktivieren.
  - Deaktivieren Sie das Kontrollkästchen, um die Liste zu deaktivieren. Das Email Reputation Services-System überspringt diese Liste während einer Suchanfrage.

- Klicken Sie auf die Schaltfläche **Speichern**, um neue Einstellungen zu speichern.

Schieberegler für dynamische Reputation

Verwenden Sie den Schieberegler für die dynamische Reputation, um Sperrstufen folgendermaßen festzulegen:

- **Sehr streng**: Wenn Ihr Netzwerk mit Spam überflutet wird, wählen Sie eine strengere Einstellung aus. Mit dieser Einstellung können jedoch auch Verbindungen von berechtigten E-Mail-Absendern gesperrt werden.
- **Weniger streng**: Wenn rechtmäßige E-Mails gesperrt werden, wählen Sie eine weniger strenge Einstellung aus.

Tipp

Trend Micro empfiehlt, Änderungen an den dynamischen Einstellungen vorsichtig und in kleinen Schritten vorzunehmen. Sie können die Einstellungen dann optimieren, indem Sie die erhöhte Menge an empfangenem Spam und empfangenen rechtmäßigen Nachrichten messen und weitere kleine Änderungen vornehmen.

Wenn Sie viele Spam-Nachrichten erhalten und möglichst viele sperren möchten, verwenden Sie die strengste Stufe. Wenn durch diese Einstellung zu viele rechtmäßige Nachrichten gesperrt werden, können Sie die Einstellung um eine Stufe herabsetzen und auf Basis des resultierenden Anteils der empfangenen Spam-Nachrichten bewerten.

Reputation-Einstellungen konfigurieren

So konfigurieren Sie Reputation-Einstellungen:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Navigieren Sie zu **Richtlinie** > **Reputation-Einstellungen**.

3. Aktivieren oder deaktivieren Sie eine der Listen des Reputation-Standarddiensts.

4. Verschieben Sie den Schieberegler unter **Erweiterter Reputation-Dienst** an eine der folgenden Positionen:

   - **Stufe 4**: Die strengste Einstellung. Wenn Email Reputation Services auch nur eine einzige Spam-Nachricht von einer IP-Absenderadresse erkennt, wird die Adresse des Absenders zur dynamischen Reputation-Datenbank hinzugefügt. Wie lange die IP-Adresse in der Datenbank verbleibt, richtet sich danach, ob von Email Reputation Services weitere Spam-Nachrichten dieses Absenders ermittelt werden.

   - **Stufe 3**: Eine weniger strenge Einstellung. Email Reputation Services lässt eine geringe Anzahl an Spam-Nachrichten von Absendern mit einer guten Bewertung zu. Wenn Email Reputation Services jedoch eine Zunahme der Spam-Nachrichten von diesem Absender feststellt und der zulässige Grenzwert überschritten wird, wird der Absender zur dynamischen Reputation-Datenbank hinzugefügt. Wie lange die IP-Adresse in der Datenbank verbleibt, richtet sich danach, ob von Email Reputation Services weitere Spam-Nachrichten dieses Absenders ermittelt werden. Der Zeitraum kann maximal auf den in Stufe 4 geltenden Zeitraum verlängert werden.

   - **Stufe 2**: Eine tolerante Einstellung. Email Reputation Services lässt eine größere Menge an Spam-Nachrichten von Absendern mit einer guten Bewertung zu. Wenn Email Reputation Services jedoch eine Zunahme der Spam-Nachrichten von diesem Absender feststellt und der zulässige Grenzwert überschritten wird, wird der Absender zur dynamischen Reputation-Datenbank hinzugefügt. Der Zeitraum, den die IP-Adresse in der Datenbank verbleibt, ist in der Regel kürzer als der Zeitraum für Stufe 3.

   - **Stufe 1**: Die am wenigsten strenge Einstellung. Email Reputation Services lässt dieselbe Menge an Spam-Nachrichten von Absendern mit einer guten Bewertung wie in Stufe 2 zu. Der Zeitraum, den eine

IP-Adresse in der Datenbank verbleibt, ist in der Regel kürzer als der Zeitraum für Stufe 2.

5. Klicken Sie auf **Speichern**.

Administration

Im Abschnitt „Administration“ können Sie folgende Aufgaben durchführen:

- Ändern des Benutzernamens und Kennworts der Verwaltungskonsole
- Ändern des Aktivierungscodes

Kontodaten ändern

Sie können die E-Mail und das Kennwort der Konto-ID ändern. Zum Schutz Ihres Kennworts empfiehlt Trend Micro, das Kennwort regelmäßig zu ändern. Das Kennwort muss 8 bis 32 alphanumerische Zeichen umfassen.

Konto-ID ändern

So ändern Sie die Konto-ID:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Navigieren Sie zu **Administration** > **Kontodaten**.
3. Klicken Sie auf die Registerkarte **Konto-ID**.
4. Geben Sie die neue Konto-ID zweimal ein.
5. Geben Sie das Kennwort ein.

6. Klicken Sie auf **Aktualisieren**.

Kennwort ändern

So ändern Sie das Kennwort:

Prozedur

1. Öffnen Sie die folgende URL:

   https://www.ers.trendmicro.com

2. Navigieren Sie zu **Administration** > **Kontodaten**.
3. Klicken Sie auf die Registerkarte **Kennwort**.
4. Geben Sie das alte Kennwort einmal und das neue Kennwort zweimal ein.
5. Klicken Sie auf **Aktualisieren**.

Aktivierungscode ändern

Geben Sie zum Aktualisieren, Reaktivieren oder Fortsetzen der Verwendung des Diensts den neuen von Trend Micro erhaltenen Aktivierungscode im Lizenzierungsbildschirm ein. Nach der ordnungsgemäßen Validierung Ihres neuen Aktivierungscodes wird dieser sofort gespeichert und verwendet.

Geben Sie zum Ändern des Aktivierungscodes den neuen Aktivierungscode ein und klicken Sie dann auf **Aktivieren**.

Kapitel 5

Hilfe anfordern

In diesem Kapitel wird beschrieben, wie Sie zusätzliche Hilfe bei auftretenden Problemen erhalten und wie Sie Kontakt mit dem Support aufnehmen.

Häufig gestellte Fragen (FAQs)

Warum wurden Sie auf diese Website verwiesen?

Die meisten Benutzer werden an diese Website verwiesen, nachdem sie eine unzustellbare E-Mail mit dem Hinweis erhalten haben, dass ihre E-Mail zurückgewiesen wurde. Wenn Sie eine E-Mail mit einem Verweis auf Trend Micro Email Reputation Services erhalten haben, liegt dies höchstwahrscheinlich daran, dass die von Ihrem E-Mail-Server verwendete IP-Adresse gesperrt wurde.

Warum wird meine IP-Adresse in der Liste der bekannten Spam-Quellen aufgeführt?

Ihre IP-Adresse wird in der Liste der bekannten Spam-Quellen aufgeführt, da Spam-E-Mails von dieser IP-Adresse empfangen wurden. Nach der Meldung dieses Problems wurden von Ihrem ISP keine Maßnahmen ergriffen.

Warum wird meine IP-Adresse in der DUL aufgeführt?

Ihre IP wird in der DUL aufgelistet, weil sie in rDNS nicht als statisch definiert ist. Wenden Sie sich zur korrekten Definition Ihrer IP-Adresse an Ihren ISP.

Warum wird meine IP-Adresse in der ETL aufgeführt?

Ihre IP-Adresse ist möglicherweise an aktiven Ransomware-, Malware- oder anderen E-Mail-Bedrohungskampagnen beteiligt.

Warum wird meine IP-Adresse in der QIL aufgeführt?

Ihre IP-Adresse wird in der QIL aufgeführt, weil sie kürzlich am Senden von Spam-E-Mails beteiligt war.

Warum erhalte ich eine unzustellbare E-Mail, obwohl die IP-Adresse in keiner der gesperrten Listen enthalten ist?

Unter Umständen haben Sie die lokale IP anstelle der IP des ISP bereitgestellt. Wenden Sie sich an Ihren ISP, um die richtige IP-Adresse anzufordern. Sie können die unzustellbare E-Mail und die Header alternativ auch auf eine Zeile ähnlich der folgenden überprüfen:

Prozedur

- 550 Dienst nicht verfügbar; Client-Host [127.0.0.2] mithilfe von Trend Micro RBL+ gesperrt.

  Weitere Informationen finden Sie unter https://www.ers.trendmicro.com/reputations/index?ip_address=127.0.0.2

Die zu überprüfende IP-Adresse lautet in diesem Fall 127.0.0.2.

Hilfe zur Verwaltungskonsole anfordern

Ausführliche Informationen zum Arbeiten mit der Verwaltungskonsole finden Sie in den Hilfedateien. Sie können auf die Hilfe auf Seitenebene für einen bestimmten Bildschirm zugreifen, indem Sie oben rechts auf dem jeweiligen Bildschirm auf das Hilfesymbol klicken.

Kontaktaufnahme mit Trend Micro

Sie erreichen Ihre Trend Micro Ansprechpartner telefonisch oder per E-Mail:

Adresse	Trend Micro Deutschland GmbH Parkring 29 85748 Garching
Telefon	+49 (0)89 8393 29700
Website	https://www.trendmicro.com
E-Mail	support@trendmicro.com

- Weltweite Support-Büros:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Kontaktaufnahme mit Trend Micro:

  http://www.trendmicro.de/ueber-uns/kontakt/index.html

- Trend Micro Produktdokumentation:

  https://docs.trendmicro.com

Problemlösung beschleunigen

Sie sollten die folgenden Informationen zur Hand haben, um die Problemlösung zu beschleunigen:

- Schritte, um das Problem nachvollziehen zu können
- Informationen zur Appliance und zum Netzwerk
- Marke und Modell des Computers sowie zusätzlich angeschlossene Hardware oder Geräte
- Größe des Arbeitsspeichers und des freien Festplattenspeichers
- Betriebssystem- und Service Pack-Version
- Version des installierten Agents
- Seriennummer oder Aktivierungscode
- Ausführliche Beschreibung der Installationsumgebung
- Genauer Wortlaut eventueller Fehlermeldungen

Support-Portal verwenden

Über das Trend Micro Support-Portal können Sie rund um die Uhr online auf die aktuellsten Informationen über allgemeine und ungewöhnliche Probleme zugreifen.

Prozedur

1. Navigieren Sie zu https://success.trendmicro.com.
2. Wählen Sie unter den verfügbaren Produkten aus oder klicken Sie auf die entsprechende Schaltfläche, um nach Lösungen zu suchen.
3. Mit dem Feld **Support durchsuchen** können Sie nach verfügbaren Lösungen suchen.
4. Falls Sie keine Lösung finden, klicken Sie auf **Support kontaktieren** und wählen Sie den gewünschten Support aus.

Tipp

Um online eine Supportanfrage zu senden, besuchen Sie die folgende URL:

https://success.trendmicro.com/smb-new-request

Das Problem wird von einem Support-Mitarbeiter von Trend Micro untersucht, der innerhalb von 24 Stunden oder weniger auf Ihre Anfrage reagiert.

Verdächtige Inhalte an Trend Micro senden

Es gibt mehrere Optionen, um verdächtige Inhalte an Trend Micro zur weiteren Analyse zu senden.

Email Reputation Services

Fragen Sie die Reputation einer bestimmten IP-Adresse ab, und geben Sie einen Message Transfer Agent zum Hinzufügen zur Liste der allgemein zulässigen Adressen an:

https://www.ers.trendmicro.com/

Informationen zum Senden von Nachrichten an Trend Micro finden Sie im folgenden Knowledge Base-Artikel:

https://success.trendmicro.com/solution/1112106

Anregungen und Kritik

Das Trend Micro Team ist stets bemüht, die Dokumentationen zu verbessern. Bei Fragen, Anmerkungen oder Anregungen zu diesem oder einem anderen Dokument von Trend Micro besuchen Sie diese Website:

https://docs.trendmicro.com/en-us/survey.aspx

Anhang A

Glossar

Dynamische Reputation-Datenbank (QIL)

Bei der dynamischen Reputation-Datenbank oder der IP-Schnellliste (Quick IP List, QIL) handelt es sich um eine hochdynamische Liste, die erweiterte Erkennungstechniken für durch Botnets (Zombie-Netzwerke, SMTP-Malware, Spyware) verursachte Angriffe verwendet. IP-Adressen werden aufgrund der Art der Bedrohung schnell hinzugefügt und entfernt.

Liste der DFÜ-Benutzer (DUL)

Die Liste der DFÜ-Benutzer (DUL) enthält IP-Adressen in dynamischen Bereichen, die von ISPs angegeben werden. Die meisten rechtmäßigen E-Mail-Quellen verfügen über statische IP-Adressen.

Liste mit neuen Bedrohungen (ETL)

Die **Liste mit neuen Bedrohungen (ETL)** enthält IP-Adressen von E-Mail-Servern, die an aktiven Ransomware-, Malware- oder anderen E-Mail-Bedrohungskampagnen beteiligt sind.

Falsch positiv

Ein falsch positives Ereignis tritt auf, wenn ein E-Mail-Absender fälschlicherweise als Spammer bezeichnet wird. Wenn Sie die erweiterte Version von Email Reputation Services abonniert haben, können Sie festlegen, wie streng Email Reputation Services mit Servern umgeht, die versuchen, E-Mail-Verbindungen mit Ihrem Netzwerk herzustellen.

Bei Auswahl einer zu strengen Einstellung könnten Verbindungen von Absendern gesperrt werden, die versuchen, rechtmäßige E-Mail-Nachrichten zuzustellen.

Globale Genehmigt-Liste

Die Globale Genehmigt-Liste enthält rechtmäßige E-Mail-Quellen, die von Email Reputation-Quellen und dem Threat Protection Network erfasst wurden.

HTTP

Bei HTTP (Hypertext Transfer Protocol) handelt es sich um ein Standardprotokoll für die Übertragung von Webseiten (einschließlich Grafiken und Multimedia-Inhalten) von einem Server an einen Client über das Internet.

HTTPS

Hypertext Transfer Protocol mit SSL (Secure Socket Layer). HTTPS ist eine Variante von HTTP, die für sichere Transaktionen verwendet wird.

IP

„Das Internet Protocol (IP) ermöglicht die Übertragung von Datenblöcken, so genannten Datagrammen, von Quellen an Ziele. Bei diesen Quellen und Zielen handelt es sich um Hosts, die anhand von Adressen mit fester Länge identifiziert werden.“ (RFC 791)

Liste der bekannten Spam-Quellen

Die Liste der bekannten Spam-Quellen enthält IP-Adressen, die mit dem Senden von Spam in Zusammenhang stehen.

Liste mit Marketing-Nachrichten (Marketing Message List, MML)

Die Liste mit Marketing-Nachrichten (MML), auch bekannt als Graymail, enthält E-Mail-Quellen, die bekanntermaßen umfangreiche Marketing-Nachrichten senden.

Phishing-Angriff

Phishen oder Phishing ist eine immer häufiger auftretende Betrugsform, bei der Internet-Benutzern durch das Imitieren einer rechtmäßigen Website persönliche Daten entlockt werden sollen.

Ein typisches Beispiel wäre der Fall, in dem ein nichts ahnender Benutzer eine dringend erscheinende (und authentisch aussehende) E-Mail erhält, in der ihm mitgeteilt wird, dass es ein Problem mit seinem Konto gibt, das umgehend behoben werden müsse, da ansonsten das Konto geschlossen werde. Die E-Mail enthält eine URL zu einer täuschend echten Website. Rechtmäßige E-Mails oder Websites können leicht kopiert werden, und es muss nur noch das so genannte Back-End für die zu sammelnden Daten geändert werden.

In der E-Mail wird der Benutzer aufgefordert, sich auf der Website anzumelden und einige Kontodaten zu bestätigen. Persönliche Daten, wie Anmeldenamen, Kennwort, Kreditkartennummer, Sozialversicherungsnummer usw., werden dann an einen Hacker weitergeleitet.

Phishing-Mails lassen sich schnell, billig und in großer Zahl umsetzen. Ein Hacker kann mit Phishing-Mails erhebliche finanzielle Gewinne erzielen. Selbst für einen Computerspezialisten sind Phishing-Angriffe nur schwer zu erkennen. Dem Phish-Schreiber rechtlich beizukommen ist ebenfalls nicht einfach, wenn nicht gar unmöglich.

Melden Sie Trend Micro alle Websites, hinter denen Sie Phishing-Websites vermuten. Weitere Informationen finden Sie unter *Verdächtige Inhalte an Trend Micro senden auf Seite 5-6*.

Ping

Ping ist ein Dienstprogramm, das eine ICMP-Echoanfrage an eine IP-Adresse sendet und auf Antwort wartet. Mit dem Ping-Dienstprogramm kann festgestellt werden, ob der Computer mit der angegebenen IP-Adresse online ist.

SOCKS 4

SOCKS 4 ist ein TCP-Protokoll, das von Proxy-Servern zum Herstellen einer Verbindung zwischen Clients im internen Netzwerk oder LAN und Computern oder Servern außerhalb des LAN verwendet wird. Das SOCKS 4-Protokoll erstellt Verbindungsanfragen, richtet Proxy-Verbindungen ein und leitet Daten auf der Anwendungsschicht des OSI-Modells weiter.

TCP

TCP (Transmission Control Protocol) ist ein verbindungsorientiertes, zuverlässiges End-to-End-Protokoll für eine aus Schichten bestehende Hierarchie von Protokollen zur Unterstützung von Multi-Netzwerk-Anwendungen. TCP verwendet IP-Datagramme für die Adressauflösung. Weitere Informationen finden Sie in der Spezifikation DARPA Internet Program RFC 793.

Stichwortverzeichnis

TREND MICRO INCORPORATED

Trend Micro Deutschland GmbH Zeppelinstraße 1 Hallbergmoos, Bayern 85399 Deutschland

Tel.: +49 (0) 811 88990-700 Fax: +4981188990799

sales@trendmicro.de marketing@trendmicro.de

www.trendmicro.com

Item Code: ERGM09115/201012