Konfigurieren von sicherem E-Mail-Gateway zur Verwendung von Microsoft Quarantine und Microsoft Quarantine Notification

Inhalt

Einleitung

In diesem Dokument werden die erforderlichen Konfigurationsschritte zur Integration von Cisco Secure Email (CES) mit Microsoft 365 Quarantine beschrieben.

Überblick

In modernen E-Mail-Infrastrukturen werden häufig mehrere Sicherheitsebenen implementiert, was dazu führt, dass E-Mails von verschiedenen Systemen unter Quarantäne gestellt werden. Um die Benutzerumgebung zu optimieren und die Konsistenz der Benachrichtigungen zu verbessern, empfiehlt es sich, die Quarantäneverwaltung auf einer zentralen Plattform zu zentralisieren. In diesem Leitfaden wird erläutert, wie unerwünschte Nachrichten wie Spam und Gymnasium, die von der Cisco CES identifiziert wurden, in die Microsoft 365-Benutzerquarantäne umgeleitet werden.

Voraussetzungen

Stellen Sie zum Abschließen dieser Konfiguration Folgendes sicher:

1. Ein aktiver Tenant im Cisco Secure Email Gateway
2. Ein aktiver Tenant in Microsoft Exchange online.
3. Zugriff auf Microsoft 365 (O365) Services
4. Eine Microsoft 365 Defender-Lizenz (erforderlich, um Quarantänerichtlinien und -benachrichtigungen zu konfigurieren)

Konfigurieren von Microsoft 365 (O365)

Richten Sie zunächst Microsoft 365 ein, um Nachrichten in Quarantäne zu empfangen und zu verwalten.

Quarantäne-Benachrichtigungen in Microsoft Exchange online aktivieren

In der offiziellen Microsoft-Dokumentation finden Sie Informationen zur Konfiguration von Benutzerbenachrichtigungen für Nachrichten in Quarantäne:
Konfiguration der Microsoft Quarantine-Benachrichtigung

Erstellen einer Mailflow-Regel

Konfigurieren Sie nach Aktivierung der Benachrichtigungen eine Regel, die vom Cisco Secure Email Gateway markierte Nachrichten an die von Microsoft gehostete Quarantäne umleitet.

1. Öffnen Sie das Microsoft Exchange-Admin-Center.
2. Gehen Sie im Menü auf der linken Seite zu Mail Flow → Rules.
3. Klicken Sie auf Regel hinzufügen, und wählen Sie dann Neue Regel erstellen aus.
4. Legen Sie folgenden Regelnamen fest: CSE-Quarantäneregeln.
5. Wählen Sie unter Diese Regel anwenden, wenn die Option Nachrichtenkopf aus, und wählen Sie Übereinstimmungen mit Textmustern aus.
6. Geben Sie in den Header-Namen Folgendes ein: X-CSE-Quarantine, und legen Sie den entsprechenden Wert fest: wahr.
7. Wählen Sie unter Folgender Vorgang die Option Nachricht umleiten an aus, und wählen Sie Gehostete Quarantäne aus.
8. Speichern Sie die Konfiguration.
9. Stellen Sie nach dem Speichern sicher, dass die Regel aktiviert ist.

Auf dem Bild sehen Sie, wie die Regel aussieht.

CSE Quarantine

Edit rule conditions Edit rule settings

Status: Disabled

Enable or disable rule

Enabled

Updating the rule status, please wait...

Rule settings

Rule name
CSE Quarantine

Mode
Enforce

Severity
Not specified

Set date range
Specific date range is not set

Senders address
Matching Header

Priority
1

For rule processing errors
Ignore

Rule description

Apply this rule if

'X-CSE-Quarantine' header matches the following patterns: 'true'

Do the following

Deliver the message to the hosted quarantine.

Rule comments

Microsoft-Regel

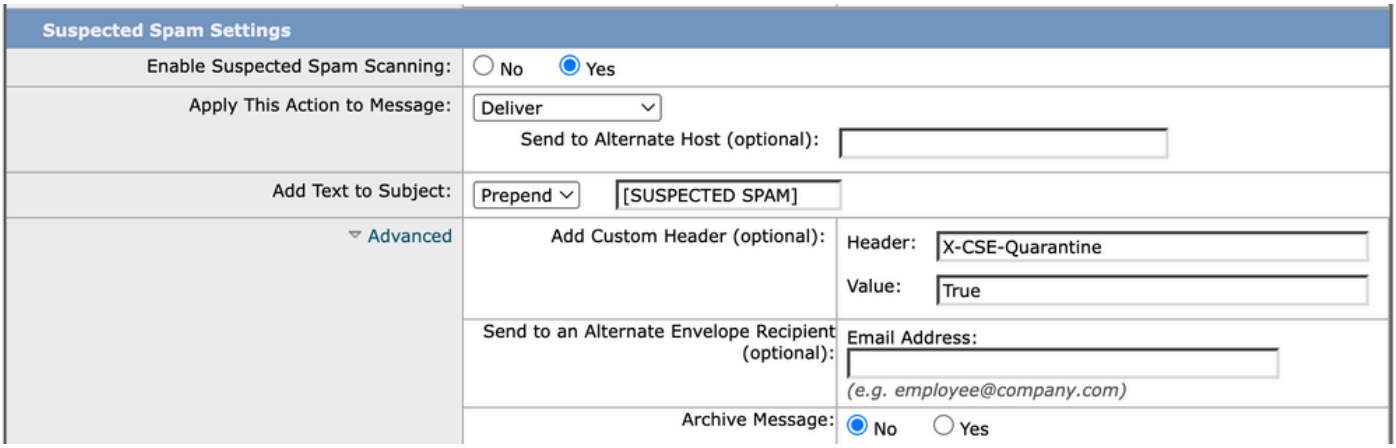
Konfigurieren von Cisco Secure Email

In Cisco CES können Sie einen benutzerdefinierten Header (X-CSE-Quarantine: true) auf alle Nachrichten, die in die Quarantäne von Microsoft umgeleitet werden sollen.

Diese Nachrichten können von jedem Content-Filter oder jeder Engine auf der CES gekennzeichnet werden. In diesem Beispiel wird es für verdächtige Spam-Nachrichten konfiguriert.

1. Öffnen Sie die Cisco Secure Email Management Console.
2. Gehen Sie zu Mail-Policys → Eingehende Mail-Policys.
3. Bearbeiten Sie die Richtlinien, die Sie ändern möchten (wählen Sie z. B. die Standardrichtlinie aus).
4. Klicken Sie auf die Spam-Einstellungen für die ausgewählte Richtlinie.
5. Ändern Sie unter Verdächtiger Spam die Aktion von Quarantäne in Zustellen.
6. Klicken Sie auf Erweitert, und fügen Sie einen benutzerdefinierten Header hinzu:
    - Header-Name: X-CSE-Quarantäne
    - Wert: true (derselbe Wert, der in der Microsoft-Regel verwendet wird)
7. Klicken Sie auf Senden und dann auf Änderungen bestätigen, um die Konfiguration zu übernehmen.

Auf dem Bild sehen Sie, wie die Konfiguration aussieht.



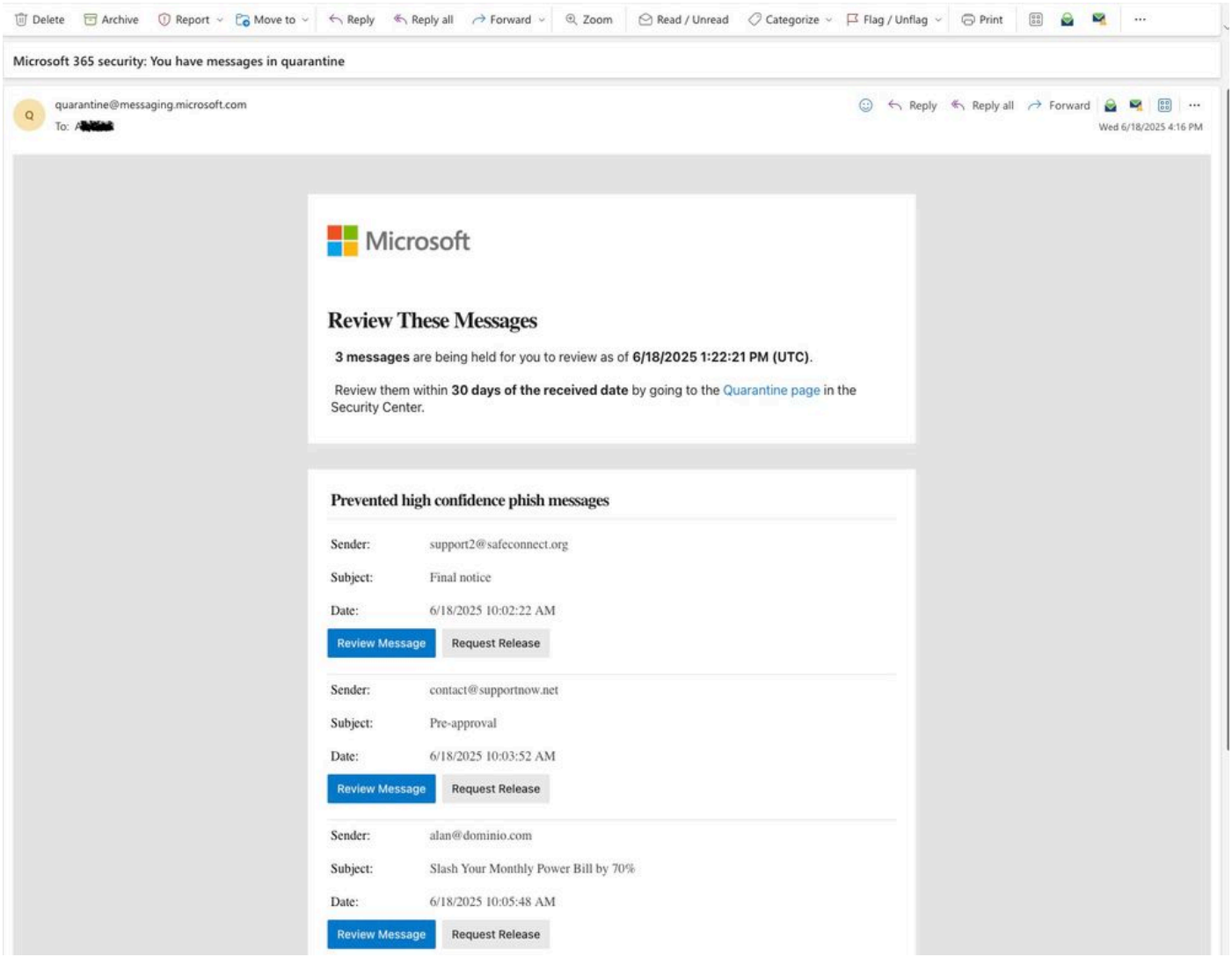
CES-Konfiguration

Überprüfung

Ab diesem Zeitpunkt werden E-Mails, die von der Cisco CES als potenzieller Spam identifiziert

wurden, mit dem benutzerdefinierten Header versehen. Microsoft 365 erkennt dieses Tag und leitet die Nachricht an den Quarantänebereich des Benutzers weiter.

Benutzer, die Quarantänebenachrichtigungen gemäß der Microsoft 365-Konfiguration erhalten.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.