Phishing-Whitelisting und Eindämmung von Fehlalarmen

Kurzreferenz

Version: 2.2

Überarbeitet: Dezember 2024

Inhalt

venza®

Einführung

Dieser Leitfaden enthält Anleitungen zur Erstellung von Whitelists und zur Reduzierung von False Positives in E-Mail-Servern, Firewalls, Spam-Filtern und verschiedenen anderen Tools, um die Sicherheit zu gewährleisten:

- **VENZA Phishing-Kampagnen** werden zu Testzwecken an Empfänger zugestellt.
- **Die VENZA Phishing Compliance Reports** liefern verwertbare Ergebnisse für Abhilfemaßnahmen.

Die Anweisungen sind nach dem Werkzeug oder der Ressource geordnet.

Um eine erfolgreiche Kampagne zu gewährleisten, befolgen Sie die Anweisungen sowohl für den E-Mail-Server als auch für alle zusätzlichen Tools oder Ressourcen, die Ihre Organisation verwendet.

Whitelisting

Whitelisting ist eine Sicherheitspraxis, bei der eine Liste von zugelassenen E-Mail-Adressen, Domänen oder IP-Adressen erstellt wird, die E-Mails an das E-Mail-System eines Unternehmens senden dürfen, ohne dass sie blockiert oder als Spam gekennzeichnet werden.

Abschwächen von Falschmeldungen

Ein False Positive ist ein Fehler, der auftritt, wenn ein System ein Ereignis meldet, z. B. dass eine Zielperson auf eine Phishing-E-Mail geklickt hat, obwohl der Endbenutzer dies nicht tatsächlich getan hat. Sie sind nicht auf einen bestimmten Anbieter oder ein bestimmtes Tool beschränkt und treten bei allen Phishing-Simulationsplattformen auf.

Falschmeldungen werden in der Regel von den Sicherheitsfiltern der E-Mail-Anbieter verursacht. Filter prüfen den Inhalt von E-Mails, bevor sie für den Posteingang des Empfängers freigegeben werden. Für das Phishing-Simulationstool wird dies als Aktion registriert und als solche gemeldet.

Nachdem das Whitelisting erfolgt ist, können in der E-Mail-Verwaltung zusätzliche Regeln und Konfigurationen festgelegt werden, um dieses Problem zu entschärfen, z. B:

- E-Mail-Gateway-Konfiguration

- Server-seitige Regeln
- Aktualisieren von Richtlinien in der E-Mail-Verwaltung

VENZA Whitelisting Informationen

Campaign IP Address

108.163.193.74

Domains

account-profile.com	expedia-us.com	usa-fedex.com
collectionsagency.com	noreply@venzagrc.com	yelprating.com
corporateoffice.biz	hotelreview.today	your-account-login.com
discriminationweb.com	humanresources.center	noreply@venzapeak.com
documentsservice.com	legalactions.org	root@internal.venzapeak.com
employeerewards.site	shipmentnotice.com	

Landing Page URLs

accounts.your-account-login.com	giftcard.your-account-login.com	reviewdocs.your-account-login.com
bdaycard.your-account-login.com	guestpromo.your-account-login.com	rewards.your-account-login.com
benefits.your-account-login.com	invoices.your-account-login.com	services.your-account-login.com
benifits.your-account-login.com	legalactions.your-account-login.com	shipmentnotice.your-account-login.com
collectionsagency.your-account-login.com	linkdin.your-account-login.com	subscription.your-account-login.com
debtcollections.your-account-login.com	newjobs.your-account-login.com	survey.your-account-login.com
directdeposit.your-account-login.com	payroll.your-account-login.com	trynet.your-account-login.com
documentshare.your-account-login.com	phishing.venzagroup.com	verify.your-account-login.com
documents.your-account-login.com	phonebill.your-account-login.com	wiretransfers.your-account-login.com
docusigning.your-account-login.com	promo.your-account-login.com	yelprating.your-account-login.com
email.your-account-login.com	publicadvise.your-account-login.com	

Whitelisting von E-Mail-Anbietern

Google

Whitelisting nach IP-Adresse

1. Melden Sie sich bei der Google Workspace Admin-Plattform an.
2. Navigieren Sie zu *Apps* und dann zu Google Workspace.
3. Wählen Sie *Google Mail* auf der linken Seite aus.
4. Wählen Sie Ihren Bereich aus dem Abschnitt *Organisationseinheit* auf der Seite aus.
5. Blättern Sie zur Registerkarte *Spam, Phishing und Malware* auf der rechten Seite.
6. Blättern Sie auf der Registerkarte *Spam, Phishing und Malware* zu der Einstellung *E-Mail-Zulassungsliste*. Oder geben Sie in das Suchfeld "email allowlist" ein.
7. Geben Sie in das Feld *E-Mail-Zulassungsliste* die IP-Adresse von VENZA (**108.163.193.74**) ein.
8. Klicken Sie unten auf der Seite auf *Speichern.*

Benutzerdefinierten Spam-Filter hinzufügen

1. Melden Sie sich bei der Google Workspace Admin-Plattform an.
2. Navigieren Sie zu *Apps* und dann zu Google Workspace.
3. Wählen Sie *Google Mail* auf der linken Seite aus.
4. Wählen Sie auf der Seite *Einstellungen für Google Mail* die Option *Spam, Phishing und Malware*.
5. Wählen Sie Ihren Bereich aus dem Abschnitt *Organisationseinheit* auf der Seite aus.
6. Blättern Sie zu *Spam* und klicken Sie auf *Konfigurieren* oder *Weitere Regel hinzufügen.*
7. Geben Sie im Feld *Einstellung hinzufügen* einen eindeutigen Namen ein (z. B. VENZA Phishing).
8. Scrollen Sie in der *Kopfzeile Optionen zum Umgehen von Filtern und Warnbannern* nach unten zu *Spamfilter umgehen und Warnungen für Nachrichten von Absendern oder Domänen in ausgewählten Listen ausblenden.*
9. *Wählen Sie* aus diesen Optionen Liste *erstellen oder bearbeiten.*
10. *Adressliste verwalten*, wählen Sie *Adressliste hinzufügen*.
11. Wählen Sie *Bulk-Upload-Adressen*.

a. Geben Sie die Domains der VENZA Phishing-Kampagne ein, jeweils durch ein Komma getrennt, oder kopieren Sie den unten angegebenen Text:
humanresources.center,documentsservice.com,legalactions.org,employeeerewards.site,your-account-login.com,corporateoffice.biz,employeeerewards.site,collectionsagency.co,corporateoffice.biz,employeeerewards.site,account-profile.com,shipmentnotice.com,yelprating.com
b. Klicken Sie auf *Speichern.*

12. Aktivieren Sie auf der ursprünglichen Seite *Einstellungen hinzufügen* die Funktion *Navigieren zu Spam-Filter umgehen und Warnungen für Nachrichten von Absendern oder Domänen in ausgewählten Listen ausblenden*, indem Sie das Kästchen daneben aktivieren.
13. Wählen Sie darunter die Funktion *Vorhandene Liste verwenden* und wählen Sie die soeben erstellte Liste aus.
14. Vergewissern Sie sich, dass das Kästchen markiert ist.

IP-Adressen als eingehende Gateways hinzufügen

1. Melden Sie sich bei der Google Workspace Admin-Plattform an.
2. Navigieren Sie zu *Apps* und dann zu Google Workspace.
3. Wählen Sie *Google Mail* auf der linken Seite aus.
4. Wählen Sie auf der Seite *Einstellungen für Google Mail* die Option *Spam, Phishing und Malware*.
5. Wählen Sie auf der linken Seite Ihre übergeordnete Organisation aus.
6. Führen Sie einen Bildlauf zur *Einstellung für das eingehende Gateway* durch und klicken Sie dann auf *Bearbeiten*.
7. Füllen Sie die Informationen wie folgt aus:
   a. Klicken Sie unter *Gateway IPs* auf Hinzufügen und geben Sie die VENZA IP-Adresse (**108.163.193.74**) ein.
   b. Vergewissern Sie sich, dass das Kästchen neben *Ablehnen aller E-Mails, die nicht von* Gateway-IPs *stammen,* ***nicht*** aktiviert ist.
   c. Aktivieren Sie das Kästchen neben *TLS für Verbindungen von den oben genannten E-Mail-Gateways erforderlich.*
   d. Aktivieren Sie das Kontrollkästchen neben *Nachricht wird als Spam betrachtet, wenn die folgende Kopfzeilen-Regexp übereinstimmt.*
      I. Geben Sie in das Feld für den Textausdruck unten einen Tag ein, der in einer Phishing-Test-E-Mail wahrscheinlich nicht zu finden ist.

II. Dies könnte eine zufällige Zusammenstellung von Buchstaben sein, zum Beispiel: *sduenvgdopajwdkasd*.

e. Aktivieren Sie das Kontrollkästchen neben *Gmail-Spamauswertung bei E-Mails von diesem Gateway deaktivieren; Header-Wert verwenden.*

f. Klicken Sie auf *Speichern.*

Avanan in Google auf die Positivliste setzen

1. Melden Sie sich bei der Google Workspace Admin-Plattform an.
2. Navigieren Sie zu *Apps* und dann zu Google Workspace.
3. Wählen Sie *Google Mail* auf der linken Seite aus.
4. Wählen Sie auf der linken Seite Ihre übergeordnete Organisation aus.
5. Wählen Sie auf der Seite *Einstellungen für Google Mail* die Option *Compliance*.
6. Bewegen Sie den Mauszeiger über die Einstellung *Inhaltskonformität*.
7. Klicken Sie auf die Schaltfläche *Konfigurieren* oder *Weiteres hinzufügen*.
8. Scrollen Sie im Pop-up-Fenster *Einstellung hinzufügen* zum Abschnitt *Inhaltskonformität* und geben Sie eine Beschreibung der Regel ein (z. B. VENZA Phishing).
9. Kreuzen Sie unter Abschnitt Nummer eins das Kästchen neben Inbound an.
10. Füllen Sie unter Abschnitt Nummer zwei die folgenden Angaben aus:
    a. Drop-Down-Menü: Wählen Sie *Wenn alle der folgenden Punkte auf die Nachricht zutreffen*.
        I. Klicken Sie im Popup-Fenster *Ausdrücke* auf *Hinzufügen*.
        II. Wählen Sie im Dropdown-Menü *Übereinstimmungstyp* die Option *Quell-IP liegt innerhalb des folgenden Bereichs*.
        III. Geben Sie die VENZA IP-Adresse (**108.163.193.74**) in das Feld *Übereinstimmungstyp* ein.
11. Füllen Sie unter Punkt drei die folgenden Felder aus:
    a. Drop-Down-Menü: Wählen Sie Nachricht *ändern*
    b. Überschriften: Kontrollkästchen neben *Benutzerdefinierte* Kopfzeilen *hinzufügen*
        I. Klicken Sie im Pop-up-Fenster für *benutzerdefinierte Überschriften* auf *Hinzufügen*.
        II. Geben Sie in das Feld *Header Name* "X-CLOUD-SEC-AV-Info" ein (ohne Anführungszeichen).

III. Geben Sie in das Feld *Wert* "[Portalname],google_mail,inline" ein, wobei Sie "[Portalname]" durch den Namen Ihres Avanan-Portals ersetzen.

12. Klicken Sie auf *Speichern*.
13. Navigieren Sie zur Seite *Einstellungen für Google Mail* und wählen Sie *Compliance.*
14. Bewegen Sie den Mauszeiger über die Einstellung *Inhaltskonformität*.
15. Klicken Sie auf *Bearbeiten*.
16. Blättern Sie im Pop-up-Fenster "*Einstellungen hinzufügen'* zu Abschnitt Nummer zwei.
17. Klicken Sie auf *Bearbeiten* neben der Regel "[Portalname],google_mail,inline" und stellen Sie sicher, dass "[Portalname]" als Avanan-Portalname Ihrer Organisation registriert ist.
18. Füllen Sie die unten stehenden Felder wie folgt aus:
    a. Drop-Down-Menü: Wählen Sie *Metadaten-Übereinstimmung.*
    b. Attribut: Wählen Sie *Source IP.*
    c. Übereinstimmungstyp: Wählen Sie *Quelle liegt nicht innerhalb des folgenden Bereichs*.
        I. Geben Sie im Pop-up-Fenster *Match type* die IP-Adresse von VENZA ein (**108.163.193.74**).
19. Klicken Sie auf *Speichern*.

Microsoft 365

Hinweis: Diese Anweisungen gelten nicht für Mailserver, die Exchange 2010 oder früher sind.

Whitelisting Erweiterte Lieferrichtlinie

1. Melden Sie sich über Ihr Benutzerkonto im Microsoft 365 Admin Center an.
2. Navigieren Sie zu *Admin Center*.
3. Navigieren Sie zu *Sicherheit*.
4. Navigieren Sie unter *Sicherheit* zum Abschnitt *E-Mail & Zusammenarbeit* und wählen Sie *Richtlinien & Regeln*.
5. Navigieren Sie zu *Bedrohungsrichtlinien*.
6. Navigieren Sie zu *Erweiterte* Lieferung
7. Wählen Sie auf der Seite *Erweiterte Zustellung* die Registerkarte *Phishing-Simulation*.
8. Klicken Sie auf *Bearbeiten*.

9. Geben Sie die folgenden Informationen in den Abschnitt *Phishing-Simulation von Dritten bearbeiten* ein.
    a. Geben Sie unter *Domain* die VENZA Phishing-Kampagnen-Domains ein.
    b. Geben Sie unter *Sende-IP* die VENZA IP-Adresse (**108.163.193.74**) ein.
    c. Geben Sie unter *Zuzulassende Simulations-URLs* die URLs der VENZA Phishing-Kampagne ein.

Zusätzliche Bedrohungspolicen Freistellung

1. Melden Sie sich über Ihr Benutzerkonto im Microsoft 365 Admin Center an.
2. Navigieren Sie zu *Admin Center*.
3. Zu *Sicherheit* navigieren
4. Klicken Sie auf *Richtlinien und Regeln* und wählen Sie *Anti-Spam* unter Richtlinienoptionen.
5. Klicken Sie auf *Verbindungsfilterrichtlinie* und wählen Sie *Verbindungsfilter bearbeiten*.
6. Fügen Sie die VENZA IP-Adresse (**108.163.193.74**) in den Abschnitt *Always allow messages from the following IP addresses or address range* ein.
7. Aktivieren Sie die Option *Sichere* Liste *einschalten*.
8. Klicken Sie auf *Speichern*.

Umgehung des Spamfilters

1. Melden Sie sich über Ihr Benutzerkonto im Microsoft 365 Admin Center an.
2. Navigieren Sie zu *Exchange* und dann zu *Mail Flow*.
3. Navigieren Sie von *Mail Flow* zu *Regeln*.
4. Klicken Sie auf die Schaltfläche + *Regel hinzufügen*.
5. Wählen Sie die Option *Spam-Filter umgehen* und erstellen Sie einen Namen für die Regel, wenn Sie dazu aufgefordert werden.
6. Geben Sie die folgenden Optionen ein:
    a. Wählen Sie im Abschnitt *Diese Regel anwenden, wenn... die* Option *Absender*. Wählen Sie dann *IP-Adresse IP-Adresse ist in einem dieser Bereiche oder stimmt genau überein*.
        I. Klicken Sie rechts neben "*Text eingeben*' auf "*Wörter eingeben*', um das Fenster "*IP-Adressbereiche festlegen*' aufzurufen.
        II. VENZA IP-Adresse (**108.163.193.74**) eingeben.

III. Klicken Sie auf *Speichern*.

b. Klicken Sie im Feld *Do the Following...* auf die Schaltfläche + (Plus), um eine neue Regel zu erstellen.
   I. Klicken Sie auf die Option *Eigenschaften der Nachricht ändern*.
   II. Wählen Sie die Option *Spam-Konfidenzniveau (SCL) festlegen*.
   III. Klicken Sie auf die Option *Spam-Konfidenzniveau (SCL)* auf ***"-1" setzen***.
   IV. Klicken Sie auf *Spam-Filterung umgehen*.
   V. Klicken Sie auf *Speichern*.

c. Bleiben Sie im Feld *Do the Following...* und klicken Sie auf die Schaltfläche + (Plus), um eine weitere Regel zu erstellen.
   I. Klicken Sie auf die Option *Eigenschaften der Nachricht ändern*.
   II. Wählen Sie die Option *Nachrichtenkopf festlegen*.
   III. Klicken Sie auf *Wörter eingeben*.
   IV. Geben Sie in das Feld "X-MS-Exchange-Organization-BypassClutter" ein.
   V. Klicken Sie auf *Speichern*.
   VI. Klicken Sie auf "*Enter Words*" und geben Sie unter "*Header Value' und* manuell "True" ein.
   VII. Klicken Sie auf *Speichern.*

7. Vergewissern Sie sich, dass der Status der neuen Regel auf aktiviert gesetzt ist.
   a. Wenn sie deaktiviert ist, klicken Sie auf die neu eingerichtete Regel.
   b. Klicken Sie auf *Aktivieren*.
   c. Klicken Sie im Fenster auf die Schaltfläche *Regeleinstellungen bearbeiten*, um sie als aktiviert zu speichern.

Avanan in Microsoft 365 auf die Positivliste setzen

1. Melden Sie sich über Ihr Benutzerkonto im Microsoft 365 Admin Center an.
2. Navigieren Sie zu *Admin Center*.
3. Navigieren Sie zu *Exchange*.
4. Klicken Sie in der *Navigationsleiste* auf *Mail Flow*.
5. Klicken Sie auf *Regeln*.
6. Klicken Sie auf das *Pluszeichen (+)* am oberen Rand der Seite.
7. Klicken Sie im Dropdown-Menü auf *Neue Regel erstellen*.
8. Geben Sie im Pop-up-Fenster *Neue Regel* einen benutzerdefinierten Namen in das Feld *Name* ein (z. B. VENZA Phishing).

9. Bewegen Sie den Mauszeiger im Dropdown-Menü *Diese Regel anwenden, wenn...* über die Option *Der Absender* und wählen Sie dann *IP-Adresse liegt in einem dieser Bereiche oder entspricht genau der* Auswahl auf der rechten Seite.
10. Geben Sie VENZA IP (**108.163.193.74**) in das Pop-up-Fenster ein.
11. Klicken Sie auf das *Pluszeichen (+)* auf der rechten Seite des Feldes, um die IP-Adresse hinzuzufügen.
12. Drücken Sie *OK*.
13. Wählen Sie aus dem Dropdown-Menü *Do the following...* die Option *Modify the message properties*.
14. Wählen Sie *Nachrichtenkopf* einstellen.
15. Klicken Sie auf die Option *Text eingeben*, die sich neben dem Menü *Folgendes tun...* befindet.
16. Geben Sie "X-CLOUD-SEC-AV-Info" (ohne Anführungszeichen) ein oder kopieren Sie es und fügen Sie es in das Feld des Pop-up-Fensters ein.
17. Drücken Sie *Ok*.
18. Navigieren Sie zur Überschrift *Eigenschaften dieser Regel* und aktivieren Sie das Kontrollkästchen neben *Audit this rule with severity level*.
19. Navigieren Sie zur Überschrift *Wählen Sie einen Modus für diese Regel* und wählen Sie *Durchsetzen.*
20. Aktivieren Sie das Kontrollkästchen neben der Option *Verarbeitung weiterer Regeln stoppen*.
21. Klicken Sie auf *Speichern*.
22. Verschieben Sie die Priorität dieser Regel über die Regel *Avanan - Protect mail flow*.

Advanced Threat Protection Link Ausnahmen

1. Melden Sie sich über Ihr Benutzerkonto im Microsoft 365 Admin Center an.
2. Navigieren Sie zu *Exchange* und dann zu *Mail Flow*.
3. Navigieren Sie von *Mail Flow* zu *Regeln*.
4. Klicken Sie auf die Schaltfläche + *Regel hinzufügen*.
5. Name für Regel erstellen.
6. Geben Sie die folgenden Optionen ein:
   a. Wählen Sie im Abschnitt *Diese Regel anwenden, wenn... die* Option *Absender*. Wählen Sie dann *IP-Adresse ist in einem dieser Bereiche oder stimmt genau überein.*

I. Klicken Sie rechts neben "*Text eingeben'* auf "*Wörter eingeben'*, um das Fenster "*IP-Adressbereiche festlegen'* aufzurufen.
II. VENZA IP-Adresse (**108.163.193.74**) eingeben.
III. Klicken Sie auf *Speichern*.

b. Markieren Sie im Abschnitt *Folgende Schritte ausführen* die Option *Eigenschaften der Nachricht ändern*.
I. Wählen Sie die Option *Nachrichtenkopf festlegen*.
II. Setzen Sie den Nachrichtenkopf auf *X-MS-Exchange-Organization-SkipSafeLinksProcessing*.
III. Setzen Sie den Wert auf "1".

c. Klicken Sie auf *Speichern*.

8. Vergewissern Sie sich, dass der Status der neuen Regel auf aktiviert gesetzt ist.
a. Wenn sie deaktiviert ist, klicken Sie auf die neu eingerichtete Regel.
b. Klicken Sie auf *Aktivieren.*
c. Klicken Sie im Fenster auf die Schaltfläche *Regeleinstellungen bearbeiten*, um sie als aktiviert zu speichern.

Microsoft Exchange (2016, 2019)

Whitelisting nach IP-Adresse

1. Melden Sie sich bei Ihrem Exchange Admin Center-Konto an und navigieren Sie zu *Mail Flow.*
2. Wählen Sie unter *Mailflow* die Option *Regeln*.
3. Klicken Sie auf + *Regel hinzufügen* und wählen Sie dann *Neue Regel erstellen* aus der Dropdown-Liste.
4. Geben Sie der Regel im oberen Textfeld einen eigenen Namen (z. B. VENZA Phishing).
5. Wählen Sie im Abschnitt *Diese Regel anwenden, wenn...* im linken Feld *Absender* und im rechten Feld *IP-Adresse liegt in einem dieser Bereiche oder stimmt genau überein*.
6. Geben Sie im Pop-up-Fenster *IP-Adressbereiche angeben* VENZA IP (**108.163.193.74**) ein.
7. Klicken Sie auf *Speichern.*
8. Markieren Sie im Abschnitt *Do the following* section die Option *Modify the message properties* im linken Feld und *legen Sie* im rechten Feld *eine Nachrichtenüberschrift fest.*

9. Klicken Sie unter den soeben bearbeiteten Feldern im Abschnitt *Do the Following* auf die linke/erste Option *Enter Text*.
10. Geben Sie "X-MS-Exchange-Organization-BypassClutter" (ohne Anführungszeichen) in das Feld ein.
11. Klicken Sie auf Speichern.
12. Klicken Sie unter den soeben bearbeiteten Feldern im Abschnitt *Do the Following* auf die rechte Seite/zweite Option *Enter Text*.
13. Tippen Sie "true" (ohne Anführungszeichen, Groß- und Kleinschreibung beachten)
14. Klicken Sie auf *Speichern.*
15. Klicken Sie auf das Symbol + *(Pluszeichen)* auf der rechten Seite des *Abschnitts Do the Following*...
16. Wählen Sie in den beiden neuen Dropdown-Menüs, die unter *Und* erschienen sind, die Option *Eigenschaften der Nachricht ändern* auf der linken Seite.
17. Wählen Sie im rechten Dropdown-Menü unter *Und* die Option *Spam-Konfidenzniveau (SCL) festlegen*.
18. Wählen Sie im Popup-Fenster *SCL angeben* die Option *Spam-Filterung umgehen*.
19. Klicken Sie auf *Speichern.*
20. Klicken Sie auf *Weiter*, um zur Seite *Regeleinstellungen festlegen* zu gelangen.
21. Lassen Sie alle Optionen/Einstellungen auf der Seite *Regeleinstellungen festlegen* unverändert.
22. Klicken Sie auf *Weiter.*
23. Klicken Sie auf der Seite *Überprüfen und Fertigstellen* auf *Fertigstellen.*

Whitelisting von Spam-Filtern und Firewalls

AppRiver

Whitelisting Spam-Filter

1. Melden Sie sich beim AppRiver Admin Center an.
2. Navigieren Sie zu den *Filtern,* einer auswählbaren Registerkarte oben auf der Seite.
3. Wählen Sie auf der linken Seite der Seite "*Filter'* die Option "*IP-Adressen'.*
4. Klicken Sie auf die Schaltfläche *Hinzufügen* unter der Überschrift *Erlaubte IP-Adressen.*
5. Fügen Sie die VENZA IP (**108.163.193.74**) hinzu.
6. Klicken Sie auf *Speichern.*

Barracuda Essentials

Whitelisting von E-Mail-Sicherheitsdiensten in der Cloud

1. Melden Sie sich bei der Barracuda Cloud Control-Plattform an.
2. Navigieren Sie zu *E-Mail-Sicherheit.*
3. Navigieren Sie unter *E-Mail-Sicherheit* zu den *Einstellungen für eingehende Nachrichten.*
4. Navigieren Sie in den *Einstellungen für eingehende Verbindungen* zu *IP-Adressrichtlinien.*
5. Wählen Sie den Abschnitt *IP-Blocking/Exemption* und geben Sie in der obersten Zeile die VENZA IP-Adresse (**108.163.193.74**) ein.
6. Geben Sie in das Feld *Netzmaske* **255.255.255.255** ein.
7. Wählen Sie im Feld *Richtlinie* die Option *Befreit.*
8. Klicken Sie auf *Hinzufügen,* um den Vorgang abzuschließen.

Whitelisting Email Security Gateway

1. Melden Sie sich beim Barracuda Email Security Gateway Webportal an.
2. Navigieren Sie auf dem Dashboard zur Seite *BLOCK/ACCEPT.*
3. Navigieren Sie auf der Seite *BLOCK/ACCEPT* zu den *IP-Filtern.* .
4. Wählen Sie den Abschnitt *Erlaubte IP/Bereich* und geben Sie in der obersten Zeile die VENZA IP-Adresse (**108.163.193.74**) ein.
5. Geben Sie in das Feld *Netzmaske* **255.255.255.255** ein.

6. Wählen Sie im Feld *Richtlinie* die Option *Befreit*.
7. Klicken Sie auf *Hinzufügen*, um den Vorgang abzuschließen.

Barracuda Advanced Threat Protection Ausnahmeregelung

1. Melden Sie sich beim Barracuda Email Security Gateway Webportal an.
2. Navigieren Sie auf dem Dashboard zur Seite *ATP-Einstellungen*.
3. Geben Sie die VENZA IP-Adresse ein (**108.163.193.74**).
4. Geben Sie in das Feld *Netzmaske* **255.255.255.255** ein.
5. Klicken Sie zum Abschließen auf *Hinzufügen*.

Absenderliste zulassen

1. Melden Sie sich bei der Barracuda Admin-Konsole an.
2. Navigieren Sie zum *Dashboard*.
3. Navigieren Sie zu *Einstellungen.*
4. Navigieren Sie zu *Erlaubte Absender*.
5. Geben Sie die Domainnamen der VENZA Phishing-Kampagne ein.
6. Klicken Sie auf *Speichern*.

Cisco Cloud E-Mail-Sicherheit

Whitelisting nach IP-Adresse

1. Navigieren Sie in der Verwaltungskonsole von Cisco IronPort zur Registerkarte *Mail Policies*.
2. Wählen Sie *HAT Overview* und stellen Sie sicher, *dass InboundMail* lister ausgewählt ist.
3. Klicken Sie auf *WHITELIST*. Wenn Sie *WHITELIST* nicht sehen, erstellen Sie eine Gruppe mit diesem Titel.
4. Klicken Sie auf *Absender hinzufügen* und fügen Sie dann die VENZA IP (**108.163.193.74**) hinzu.
5. Klicken Sie auf *Senden* und dann auf *Änderungen übernehmen*.

Whitelisting Ausbruchsfilter Scannen

1. Navigieren Sie in der Verwaltungskonsole von Cisco IronPort zur Registerkarte *Mail Policies*.
2. Geben Sie unter dem Abschnitt *Message Modification* in der Tabelle *Bypass Domain Scanning* die VENZA IP (**108.163.193.74**) ein.
3. Klicken Sie auf *Senden* und dann auf *Änderungen übernehmen*.

Fortinet FortiGate

Kampagnen-URLs auf die Whitelist setzen

1. Melden Sie sich bei Ihrem Fortinet-Administratorkonto an.
2. Navigieren Sie zu *Sicherheitsprofile* und dann zu *Webfilter*.
3. Erstellen Sie einen neuen Filter, erweitern Sie dann den *Status-URL-Filter*, aktivieren Sie ihn und wählen Sie *Erstellen*.
4. Geben Sie die URLs der VENZA Phishing-Kampagne ein
   a. Alle Kampagnen-URLs müssen einzeln eingegeben werden, ohne https://.
5. Wählen Sie unter Typ die Option *Einfach*.
6. Stellen Sie sicher, dass *Status* aktiviert ist.

Mimecast

Hinzufügen einer Richtlinie für zulässige Absender

HINWEIS: Bearbeiten Sie nicht die Standardrichtlinie Zulässiger Absender. Erstellen Sie für jede Whitelisting- und Falsch-Positiv-Minimierungs-Richtlinie eine neue Richtlinie.

1. Melden Sie sich bei der Mimecast-Verwaltungskonsole an.
2. Wählen Sie in der Symbolleiste *Administration* den Menüpunkt *Gateway / Policies*.
3. Wählen Sie in der Liste der Richtlinien die Option *Erlaubte Absender*.
4. Klicken Sie auf die Schaltfläche *Neue Richtlinie*.
5. Füllen Sie die Felder der Police wie unten beschrieben aus:
   a. **Optionen**
      I. Politik-Erzählung: VENZA Phishing
      II. Richtlinie für zugelassene Absender: Zulässiger Absender

b. **Emails von**
    I. Adressen Basierend auf: Beide
    II. Gilt von: Alle
    III. Speziell: Gilt für alle Absender
c. **Emails an**
    I. Gilt für: Alle
    II. Speziell: Gilt für alle Begünstigten
d. **Gültigkeit**
    I. Aktivieren/Deaktivieren: Aktivieren
    II. Richtlinie als immerwährend festlegen: Immer eingeschaltet
    III. Datumsbereich: Alle Zeiten
    IV. Richtlinie überschreiben: Markiert.
    V. Bidirektional: Nicht angekreuzt.
e. **Quell-IP-Bereiche**
    I. Geben Sie die VENZA IP-Adresse ein (**108.163.193.74/32**).

6. *Speichern* und *Beenden*.

Greylisting

1. Melden Sie sich bei der Mimecast-Verwaltungskonsole an.
2. Wählen Sie in der Symbolleiste *Administration* den Menüpunkt *Gateway / Policies*.
3. Wählen Sie in der Liste der Richtlinien die Option *Greylisting*.
4. Klicken Sie auf die Schaltfläche *Neue Richtlinie*.
5. Füllen Sie die Felder der Police wie unten beschrieben aus:
    a. **Optionen**
        I. Politik-Erzählung: GreyList Umgehung VENZA Phishing
        II. Richtlinie für zugelassene Absender: Keine Maßnahmen ergreifen
    b. **Emails von**
        I. Adressen basierend auf: Die Rücksendeadresse
        II. Gilt von: Alle
        III. Speziell: Gilt für alle Absender
    c. **Emails an**
        I. Gilt für: Alle
        II. Speziell: Gilt für alle Begünstigten

d. **Gültigkeit**
    I. Aktivieren/Deaktivieren: Aktivieren
    II. Richtlinie als immerwährend festlegen: Immer eingeschaltet
    III. Datumsbereich: Alle Zeiten
    IV. Richtlinie überschreiben: Markiert.
    V. Bidirektional: Nicht angekreuzt.

e. **Quell-IP-Bereiche**
    I. Geben Sie die VENZA IP-Adresse ein (**108.163.193.74/32**).

6. *Speichern* und *Beenden*.

DNS-Eingangsauthentifizierung

1. Melden Sie sich bei der Mimecast-Verwaltungskonsole an.
2. Wählen Sie in der Symbolleiste *Administration* den Menüpunkt *Gateway / Policies*.
3. Navigieren Sie im Dropdown-Menü *Definitionen* zur Option *DNS-Authentifizierung - eingehend*.
4. Wählen Sie Neue DNS-Authentifizierung - Eingehende Überprüfungen.
5. Erstellen Sie einen Namen für die *neue DNS-Authentifizierung*
6. Lassen Sie alle Optionen unangekreuzt.
7. Klicken Sie auf *Speichern* und *Beenden.*
8. Navigieren Sie zur Schaltfläche *Verwaltung* in der Symbolleiste und wählen Sie den Menüpunkt *Gateway / Policies*.
9. Wählen Sie in der Liste der Richtlinien die Option *DNS-Authentifizierung - Eingehende* Richtlinie.
10. Klicken Sie auf die Schaltfläche *Neue Richtlinie*.
11. Füllen Sie die Felder der Police wie unten beschrieben aus:
    a. **Optionen**
        I. Politik-Narrativ: VENZA DNS-Autorisierung
        II. Richtlinie für zugelassene Absender: Keine Authentifizierung
    b. **Emails von**
        IV. Adressen Basierend auf: Beide
        I. Gilt von: Alle
        II. Speziell: Gilt für alle Absender

c. **Emails an**
    I. Gilt für: Adressgruppen
    II. Speziell: E-Mail-Sicherheits-Admins
d. **Gültigkeit**
    VI. Aktivieren/Deaktivieren: Aktivieren
    I. Richtlinie als immerwährend festlegen: Immer eingeschaltet
    II. Datumsbereich: Alle Zeiten
    III. Richtlinie außer Kraft setzen: Markiert.
    IV. Bidirektional: Nicht angekreuzt.
e. **Quell-IP-Bereiche**
    I. Geben Sie die VENZA IP-Adresse ein (**108.163.193.74/32**).

12. *Speichern* und *Beenden*.

URL-Umgehungsrichtlinie

1. Melden Sie sich bei der Mimecast-Administrationskonsole an.
2. Wählen Sie in der Symbolleiste *Administration* den Menüpunkt *Gateway / Policies*.
3. Wählen Sie in der Liste der Richtlinien die Option *URL-Schutzumgehung*.
4. Klicken Sie auf die Schaltfläche *Neue Richtlinie*.
5. Füllen Sie die Felder der Police wie unten beschrieben aus:
    a. **Optionen**
        I. Bericht über die Richtlinie: VENZA Phishing-URL-Umgehung
        II. Option auswählen: Keine Maßnahmen ergreifen
    b. **Emails von**
        I. Adressen Basierend auf: Beide
        II. Gilt von: Alle
        III. Speziell: Gilt für alle Absender
    c. **Emails an**
        I. Gilt für: Interne Adressen
        II. Speziell: Gilt für alle internen Begünstigten
    d. **Gültigkeit**
        I. Aktivieren/Deaktivieren: Aktivieren
        II. Richtlinie als immerwährend festlegen: Immer eingeschaltet
        III. Datumsbereich: Alle Zeiten

IV. Richtlinie außer Kraft setzen: Markiert.

V. Bidirektional: Nicht angekreuzt.

e. **Quell-IP-Bereiche**

I. Geben Sie die VENZA IP-Adresse ein (**108.163.193.74/32**).

6. *Speichern* und *Beenden*.

Proofpoint

Safelisting IPs Proofpoint Essentials

1. Melden Sie sich bei Proofpoint Essentials an und navigieren Sie zu *Sicherheitseinstellungen*
2. Navigieren Sie zu *E-Mail* und dann zu *Absenderlisten.*
3. Wählen Sie Liste sicherer Absender.
4. Geben Sie die VENZA IP-Adresse (**108.163.193.74**) in das entsprechende Feld ein.
5. Klicken Sie auf *Speichern*.

Safelisting von Domains in Proofpoint Essentials

1. Melden Sie sich bei Proofpoint Essentials an und navigieren Sie zu *Sicherheitseinstellungen*
2. Navigieren Sie zu *E-Mail* und dann zu *Filterrichtlinien*.
3. Klicken Sie auf der Registerkarte *Eingehend* auf *Neuer Filter.*
4. Erstellen Sie einen eigenen Namen für den Filter (z.B. VENZA Phishing.)
5. Vergewissern Sie sich, dass die *Richtung* auf *Eingehend* eingestellt ist, und klicken Sie dann auf Weiter.
6. Stellen Sie im Abschnitt *Filterlogik* sicher, dass der Bereichsfilter auf <Firma> eingestellt ist.
7. Wählen Sie die folgenden Felder aus den Dropdown-Feldern unter dem Abschnitt *Wenn* aus:
   a. Erstes Dropdown-Feld: Absenderadresse.
   b. Zweites Dropdown-Feld: IS
   c. Drittes Dropdown-Feld: Geben Sie eine der VENZA Phishing-Kampagnen-Domains ein.
8. Wählen Sie im Abschnitt *Do* die Option *Allow* aus dem Dropdown-Menü *Actions*.

9. Beschreiben Sie im Feld *Filterdetails* auf der rechten Seite den Filter, falls erforderlich.
10. Klicken Sie auf *Speichern*.
11. Führen Sie die Schritte 3-10 für jede der VENZA Phishing-Kampagnen-Domänen aus.

Whitelisting in Proofpoint Enterprise

1. Melden Sie sich beim Proofpoint Enterprise Admin-Portal an.
2. Navigieren Sie zu *E-Mail-Schutz.*
3. Wählen Sie unter *Spamschutz* die Option *Organisatorisch sichere Liste*.
4. Klicken Sie auf *Hinzufügen*.
5. Füllen Sie im Popup-Fenster *Proofpoint -Global Safe* die Felder wie unten beschrieben aus:
   a. Filter-Typ: Absender Hostname
   b. Operator: Gleich
   c. Wert: VENZA Phishing-Kampagne Domains eingeben.
6. Klicken Sie auf *Änderungen speichern.*

Whitelisting in Proofpoint URL Defense

1. Melden Sie sich beim Proofpoint Enterprise Admin-Portal an.
2. Navigieren Sie zu *E-Mail-Schutz.*
3. Wählen Sie im Dropdown-Menü *Gezielter Angriffsschutz* die Option *URL-Abwehr.*
4. Klicken Sie auf *URL Rewrite Policies*.
5. Navigieren Sie zum Abschnitt *Ausnahmen* und geben Sie VENZA Phishing Campaign Domains ein.
6. Klicken Sie auf *Änderungen speichern*.

Whitelisting Proofpoint Email Firewall

1. Melden Sie sich beim Proofpoint Enterprise Admin-Portal an.
2. Navigieren Sie zu *E-Mail-Firewall* und wählen Sie dann *Regeln.*
3. Wählen Sie unter *Regeleinstellungen* die Optionsschaltfläche *Ein* für *Aktivieren.*
4. Geben Sie einen benutzerdefinierten Namen für die Regel ein (z. B. VENZA Phishing.)
5. Wählen Sie unter dem Abschnitt *Bedingungen* die Option *Hinzufügen.*
6. Geben Sie jede der VENZA Phishing-Kampagnen-Domains ein.
7. Wählen Sie im Abschnitt *Disposition* die *Zustellmethode Jetzt zustellen.*

8. Klicken Sie auf *Speichern*.

Sophos

Ändern der Zulassen/Blockieren-Liste in Sophos E-Mail

1. Melden Sie sich bei der Sophos E-Mail Appliance (SEA.) an.
2. Navigieren Sie zu *Konfiguration* und dann zu *Richtlinie*.
3. Navigieren Sie in der *Richtlinie* zu *Zulassen-Listen*.
4. Klicken Sie auf die zutreffende Liste, die auf den unten stehenden Informationen basiert, um das Fenster *Listeneditor* zu öffnen und fortzufahren:
   a. Spamfilter außerhalb von SEA: **Registerkarte Absender.**
      I. Geben Sie jede gewünschte Position in das Textfeld Einträge *hinzufügen* ein.
      II. Klicken Sie auf *Hinzufügen.*
      III. Geben Sie jede der VENZA Phishing-Kampagnen-Domains einzeln ein.
   b. Kein Spam-Filter außerhalb der SEA: **Registerkarte Hosts**.
      I. Geben Sie jede gewünschte Position in das Textfeld Einträge *hinzufügen* ein.
      II. Klicken Sie auf *Hinzufügen.*
      III. VENZA IP-Adresse (**108.163.193.74**) eingeben.

Whitelisting in der Sophos XG Firewall

1. Melden Sie sich am Sophos XG Firewall-Portal an.
2. Klicken Sie auf *Web.*
3. Navigieren Sie zu *Ausnahmen.*
4. Klicken Sie auf *Ausnahme hinzufügen*.
5. Erstellen Sie einen Namen (VENZA Phishing) und eine Beschreibung.
6. Aktivieren Sie unter "*Ausgewählte Überprüfungen oder Aktionen überspringen*" jedes Kontrollkästchen für die betreffenden Sophos Produkte.
7. Geben Sie in das Feld *Suchen/Hinzufügen* die VENZA Phishing-Kampagnen-Domains im folgenden Format ein:
   a. ^([A-Za-z0-9.-]*\.)?ABC\.com\.?/

I. Geben Sie in "ABC" den Namen der VENZA Phishing-Kampagne vor der Top-Level-Domain ein.
II. Geben Sie in ".com" die Top-Level-Domain der VENZA Phishing-Kampagnen-Domain ein.

8. Klicken Sie auf *Speichern.*

SonicWall

Whitelisting von IPs in E-Mail-Sicherheitsgeräten

1. Melden Sie sich bei der administrativen SonicWall-Appliance an.
2. Klicken Sie auf *Verwalten*.
3. Navigieren Sie im Abschnitt *Sicherheitsdienste* zu *Anti-Spam*.
4. Navigieren Sie in *Anti-Spam* zu *Adressbuch* und dann zu *Erlaubt*.
5. Klicken Sie auf *Hinzufügen.*
6. Wählen Sie *IPs* aus dem Dropdown-Menü *Listentyp auswählen*.
7. Geben Sie in das Textfeld die VENZA IP-Adresse ein (**108.163.193.74)**
8. Klicken Sie auf *Hinzufügen*.

Whitelisting von IPs in der CFS-Richtlinie von SonicWall

1. Melden Sie sich auf der SonicWall-Verwaltungsseite an.
2. Klicken Sie auf *Policies* und wählen Sie dann *Objects*.
3. Klicken Sie unter *Adressoptionen* auf *Hinzufügen*.
4. Geben Sie in das Textfeld die VENZA IP-Adresse ein (**108.163.193.74)**
5. Navigieren Sie zurück zu *Richtlinien* und wählen Sie dann *Objekte*.
6. Wählen Sie unter *Adressgruppen* die Option Hinzufügen.
7. Geben Sie einen benutzerdefinierten Namen für die *Ausschlussgruppe* an (z.B. VENZA Phishing.)
8. Markieren Sie die zuvor hinzugefügte VENZA IP-Adresse (**108.163.193.74)** und klicken Sie auf den nebenstehenden Pfeil, um die Gruppe in das rechte Feld zu verschieben.
9. Klicken Sie auf *OK.*
9. Melden Sie sich nun bei der administrativen SonicWall-Appliance an.
10. Klicken Sie auf *Verwalten* und navigieren Sie zu *Sicherheitsdienste*.

11. Navigieren Sie in den *Sicherheitsdiensten* zu *Inhaltsfilter.*
12. Klicken Sie auf die Option *Ausgeschlossene Adresse*
13. Wählen Sie die zuvor erstellte *Ausschlussgruppe* (z.B. VENZA Phishing) aus dem Dropdown-Menü aus.
14. Klicken Sie auf *Akzeptieren*.

SpamTitan

Hinzufügen von zulässigen IP-Adressen

1. Melden Sie sich beim SpamTitan Email Security-Portal an.
2. Navigieren Sie zu *System Setup* und dann zu *Mail Relay*.
3. Wählen Sie *IP-Steuerelemente* und klicken Sie auf *Hinzufügen*.
4. Füllen Sie im Popup-Fenster "*Erlaubte IP hinzufügen'* die folgenden Felder aus und befolgen Sie dabei die nachstehenden Schritte:
   a. IP/Netzwerk: VENZA IP-Adresse eingeben (**108.163.193.74)**
   b. Netzmaske: 255.255.255.255 eingeben
   c. Adresstyp: Wählen Sie IPv4
5. Klicken Sie auf *Speichern*.

Unterstützung

Wir unterstützen Sie bei jedem Schritt des Whitelisting und der Entschärfung von Phishing-Fehlalarmen. Wenn Sie auf Probleme stoßen oder Fragen haben, wenden Sie sich bitte an den Support.

Kontaktieren Sie uns

E-Mail

Telefon

Live-Chat

Ticket

Kontaktieren Sie Ihren E-Mail-Dienstanbieter

Wenn Sie technische Schwierigkeiten mit Ihrem E-Mail-System und/oder den oben genannten Tools haben, wenden Sie sich bitte direkt an Ihren E-Mail-Anbieter. Er kann Ihnen zusätzliche Unterstützung und Fehlerbehebung anbieten, die auf Ihre E-Mail-Plattform zugeschnitten sind.

Über VENZA

VENZA ist ein führender Anbieter von Sicherheits- und Datenschutzlösungen, die das Gastgewerbe in die Lage versetzen, Schwachstellen zu minimieren und die Einhaltung von Vorschriften zu gewährleisten. VENZA unterstützt mehr als 2000 Hotels weltweit und schützt Gäste und ihre Daten mit 360-Grad-Transparenz für proaktives Risikomanagement vor Sicherheitsverletzungen. So können sich Hotelmanager auf den Gästeservice konzentrieren und das Vertrauen in ihre Marke stärken.

Besuchen Sie www.VENZAGroup.com für weitere Informationen.

Kontakt

Verkäufe: sales@venzagroup.com

Kundenerfolg: success@venzagroup.com