Compliance Filter

Inhalt

Sprache und Symbole in der Dokumentation....4

Über den Compliance Filter....6

Regelreihenfolge innerhalb aller Services....8

Compliance Filter aktivieren....11

Filterregeln....12

Filterregel für eingehende E-Mails erstellen....13
Filterregel für ausgehende E-Mails erstellen....19
Anzeige von Filterregeln....26
Aktionen in Filterregeln....28
Arten von Filterregeln....31
Filterregel bearbeiten....39
Priorität einer Filterregel ändern....41
Reihenfolge der Filterregeln....43
Filterregel aktivieren....49
Filterregel des Compliance Filters deaktivieren....50
Filterregel des Compliance Filters löschen....51

Verzeichnisse....53

Verzeichnis erstellen....54
Verzeichnis bearbeiten....57
Verzeichnis löschen....59

Reguläre Ausdrücke....61

Erklärung der regulären Ausdrücke....62
Ausnahmen bei regulären Ausdrücken....70
Häufige Anwendungsfälle von regulären Ausdrücken....71

Beispiele für komplexe reguläre Ausdrücke 73

Compliance Filter deaktivieren 75

Index 76

Sprache und Symbole in der Dokumentation

Gender-Erklärung

Aus Gründen der besseren Lesbarkeit wird in dieser Dokumentation die Sprachform des generischen Maskulinums verwendet. Es wird an dieser Stelle darauf hingewiesen, dass die ausschließliche Verwendung der männlichen Form genderunabhängig verstanden werden soll.

Verwendete Symbole

Zur besseren Kenntlichkeit relevanter Schritte innerhalb handlungsanleitender Kapitel werden folgende Symbole verwendet:

SYMBOL	BEDEUTUNG	ERKLÄRUNG
	Voraussetzung	Bedingung, die vor dem nächsten Schritt erfüllt sein muss
	Zwischenresultat	Resultat, welches nach einem Schritt zwischenzeitlich erzielt wird
	Endresultat	Resultat, welches nach der Schrittreihenfolge eines handlungsanleitenden Kapitels erzielt wird

Warn- und Sicherheitshinweise

Die Warn- und Sicherheitshinweise werden eingesetzt, um Benutzer über Restrisiken und Gefahren zu informieren und diese mit einer empfohlenen Vorgehensweise zu vermeiden. Folgende Warn- und Sicherheitshinweise werden in dieser Dokumentation verwendet:

SYMBOL	BEDEUTUNG	ERKLÄRUNG
	HINWEIS	Weiterführende Informationen innerhalb eines bestimmten Absatzes, die für die Ausführung weiterer Schritte relevant sind.

SYMBOL	BEDEUTUNG	ERKLÄRUNG
	TIPP	Hinweis zu Konfigurationsmöglichkeiten.
	WICHTIG	Warnhinweis mit Informationen über Einschränkungen oder wichtige Konfigurationsmöglichkeiten des Services.
	ACHTUNG	Warnhinweis über zusätzliche Kosten, die, abhängig von gebuchten Serviceleistungen, möglicherweise entstehen können.
	WARNUNG	Warnhinweis zum möglichen Verlust von Daten.
	GEFAHR	Sicherheitshinweis zur möglichen System-Infizierung mit einer Malware.

Über den Compliance Filter

Mit dem Compliance Filter können Administratoren auf Kundenebene eigene Filterregeln definieren, um z. B. eingehende E-Mails als **Gültig**, **Spam** oder **Threat** zu kategorisieren (siehe "E-Mail-Kategorien" im Control-Panel-Handbuch). Außerdem können E-Mails abgelehnt, über einen anderen Server umgeleitet oder an andere Empfänger weitergeleitet werden. Für eine Einordnung der Filterregeln des Compliance Filters in die Regelreihenfolge aller unserer Services siehe Regelreihenfolge innerhalb aller Services auf Seite 8.

VORSICHT:

Fehlerhafte Filterregeln beeinträchtigen den E-Mail-Verkehr und können unsere Services außer Kraft setzen.

Der Compliance Filter eignet sich nicht zum Umschreiben von Adressen.

Der Compliance Filter kann sowohl eingehende als auch ausgehende E-Mails prüfen. Nach der Aktivierung des Compliance Filters (siehe Compliance Filter aktivieren auf Seite 11) können Administratoren auf Kundenebene Filterregeln der folgenden Arten definieren:

- **Header**
- **Body**
- **Erweitert**

In den Bedingungen der Filterregeln können reguläre Ausdrücke verwendet werden (siehe Reguläre Ausdrücke auf Seite 61). Für jede Filterregel legen Administratoren auf Kundenebene eine Aktion fest. Diese Aktion wird automatisch auf die E-Mails angewendet, auf die die Filterregel zutrifft. Für weitere Informationen zu den Filterregeln siehe Filterregeln auf Seite 12. Insgesamt können bis zu 1500 Filterregeln pro Kunde definiert werden.

Neben Filterregeln für einzelne Ausdrücke können auch komplexere und präzisere Filterregeln mithilfe von Verzeichnissen erstellt werden, die jeweils bis zu 15000 literale oder bis zu 1000 reguläre Ausdrücke enthalten können (siehe Verzeichnisse auf Seite 53). Administratoren auf Kundenebene können bis zu 250 Verzeichnisse für ihre Hauptdomain erstellen und pflegen.

Insbesondere Verzeichnisse mit regulären Ausdrücken verringern den Aufwand für die Erstellung und die Pflege von Filterregeln erheblich.

Um den Compliance Filter für eine Domain aktivieren und einstellen zu können, muss Spam and Malware Protection (siehe "Spam and Malware Protection" im Control-Panel-Handbuch) für die Domain aktiviert sein. Sobald Spam and Malware Protection deaktiviert wird, wird auch der Compliance Filter deaktiviert und kann nicht mehr eingestellt werden.

Administratoren auf Kundenebene können den Compliance Filter deaktivieren, falls sie ihn nicht mehr verwenden möchten (siehe Compliance Filter deaktivieren auf Seite 75).

Regelreihenfolge innerhalb aller Services

Die Regeln von Spam and Malware Protection (siehe "Spam and Malware Protection" im Control-Panel-Handbuch) haben eine bestimmte Priorität, in der sie abgearbeitet werden. Sobald eine höher priorisierte Regel greift, werden keine Regeln mit niedrigerer Priorität mehr verarbeitet. Hierdurch kann es vorkommen, dass eine E-Mail trotz eines bestehenden Whitelisting-Eintrags für ihre Absenderadresse blockiert wird, weil die IPv4-Adresse des versendenden Servers auf der RBL-Blackliste erfasst worden ist.

Regelreihenfolge (von oben nach unten in absteigender Priorität):

Eingehende E-Mails

1. RBL-Liste (blockieren)
2. Massenspamerkennung (blockieren)
3. Compliance Filter
4. Email Authentication (blockieren)
5. Prüfung auf bösartige Inhalte (quarantinieren)
6. Email Authentication (quarantinieren)
7. Content Control, sofern aktiviert (quarantinieren)
8. benutzerbasiertes Whitelisting (zustellen)
9. benutzerbasiertes Blacklisting (quarantinieren)

10. administratives Whitelisting (zustellen)

> **Hinweis:**
>
> Das administrative Whitelisting ist ein Sonderfall unter den Regeln. Denn Administratoren können bei Whitelist-Einträgen auf der Ebene einer Domain auswählen, welche Filter durch den Eintrag umgangen werden (siehe "Blacklist-Eintrag für eine Domain erstellen" im Control-Panel-Handbuch). Die betroffenen E-Mails überspringen bei ihrer Verarbeitung also die ausgewählten Filter. Dies gilt auch für Filter, die in der Liste vor dem administrativen Whitelisting stehen. Die Position, an der das administrative Whitelisting in der Liste eingeordnet ist, bezieht sich auf die Standardeinstellung von Whitelist-Einträgen auf der Ebene einer Domain. Standardmäßig umgehen die Einträge als einzigen Filter die Spam-Filterung.

11. administratives Blacklisting (quarantinieren)
12. allgemeines Whitelisting (zustellen)
13. allgemeine Spamregeln (quarantinieren)
14. Infomail Filter (quarantinieren)

> **Hinweis:**
>
> Der Compliance Filter (siehe Über den Compliance Filter auf Seite 6) wird vor Content Control (siehe Über Content Control) angewendet. Deshalb können Administratoren mit Regeln des Compliance Filters, die E-Mails als **Gültig** kategorisieren, Ausnahmen für Content Control erstellen.
>
> Für Content Control können hingegen keine Ausnahmen über benutzerdefiniertes Whitelisting und Blacklisting sowie über administratives Blacklisting erstellt werden, da diese Regeln erst nach Content Control angewendet werden. Lediglich über administratives Whitelisting ist es möglich, Content Control zu umgehen.

Ausgehende E-Mails

1. RBL-Liste

2. Compliance Filter
3. Prüfung auf bösartige Inhalte
4. Content Control, sofern aktiviert

Compliance Filter aktivieren

Sie haben Spam and Malware Protection für die Domain aktiviert (siehe "Spam and Malware Protection aktivieren" im Control-Panel-Handbuch), für die Sie den Compliance Filter aktivieren möchten.

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie den Compliance Filter aktivieren, um eigene Regeln zur Filterung von E-Mails erstellen zu können (siehe Filterregeln auf Seite 12).

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie den Compliance Filter aktivieren möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Aktivieren Sie den Schalter **Compliance Filter aktivieren**.

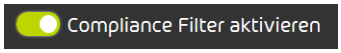

Abbildung 1: Compliance Filter aktivieren

Der Compliance Filter wird aktiviert.

Der Compliance Filter ist aktiviert worden. Sobald Filterregeln erstellt worden sind, kann der Compliance Filter verwendet werden.

Anschließend können Sie Filterregeln (siehe Filterregeln auf Seite 12) und Verzeichnisse (siehe Verzeichnisse auf Seite 53) für den Compliance Filter erstellen.

Filterregeln

Der Compliance Filter prüft E-Mails einer Domain. Im Modul **Compliance Filter** können Administratoren auf Kundenebene Filterregeln für eingehende und ausgehende E-Mails verwalten. Die Administratoren können Filterregeln für eingehende (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13) und ausgehende E-Mails (siehe Filterregel für ausgehende E-Mails erstellen auf Seite 19) erstellen. Die erstellten Filterregeln werden in zwei Tabellen angezeigt (siehe Anzeige von Filterregeln auf Seite 26).

Hinweis:

Für eine Hauptdomain können bis zu 1500 Filterregeln erstellt werden.

Für jede Filterregel können Administratoren auf Kundenebene eine Aktion (siehe Aktionen in Filterregeln auf Seite 28) auswählen. Die Aktion wird durchgeführt, sobald die Filterregel auf eine E-Mail angewendet wird.

Zusätzlich wählen Administratoren auf Kundenebene für jede Filterregel eine Art (siehe Arten von Filterregeln auf Seite 31) aus. Die Art der Filterregel bestimmt, auf welche E-Mails die Filterregel angewendet wird.

Eine mögliche Bedingung für Filterregeln sind die Empfänger, an die eine E-Mail gesendet wird. Falls eine E-Mail an mehrere Empfänger versendet wird und eine Filterregel auf einige dieser Empfänger zutrifft, wird die Aktion nur auf die Zustellung der E-Mail an die Empfänger angewendet, für die die Filterregel gilt. Somit sind verschiedene Aktionen für verschiedene Empfänger derselben E-Mail möglich.

Administratoren auf Kundenebene können bestehende Filterregeln im Nachhinein bearbeiten (siehe Filterregel bearbeiten auf Seite 39). Außerdem können die Administratoren die Priorität der Filterregeln ändern (siehe Priorität einer Filterregel ändern auf Seite 41). Die Priorität spielt eine Rolle dafür, in welcher Reihenfolge die Filterregeln des Compliance Filters abgearbeitet werden. Für weitere Informationen zu der Reihenfolge der Filterregeln des Compliance Filters siehe Reihenfolge der Filterregeln auf Seite 43.

Falls eine Filterregel vorübergehend nicht verwendet werden soll, können Administratoren auf Kundenebene sie deaktivieren (siehe Filterregel des Compliance Filters deaktivieren auf Seite 50). Deaktivierte Filterregeln können später erneut aktiviert werden (siehe Filterregel aktivieren auf Seite 49).

Sobald eine Filterregel nicht mehr benötigt wird, können Administratoren auf Kundenebene die Filterrregel löschen (siehe Filterregel des Compliance Filters löschen auf Seite 51).

Filterregel für eingehende E-Mails erstellen

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11).

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) für eingehende E-Mails erstellen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie die Filterregel erstellen möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.
5. Klicken Sie unter **Regeln für eingehende E-Mails** auf **Regel hinzufügen**.

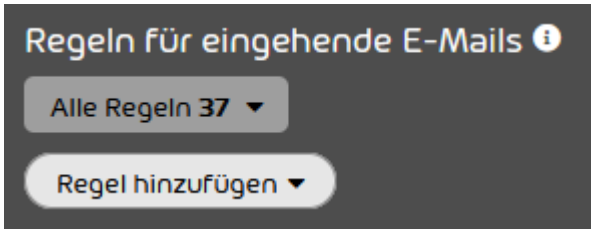

Abbildung 2: Regel hinzufügen

6. Wählen Sie unter **Aktion** aus, was mit den E-Mails geschehen soll, auf die die Filterregel angewendet wird. Sie können aus den folgenden Aktionen wählen:

   - **Ablehnen**
   - **Empfänger ändern**
   - **Umleiten**
   - **BCC hinzufügen**
   - **Als „Gültig “ markieren**
   - **Als „Spam “ markieren**
   - **Als „Threat “ markieren**

   Hinweis:

   Eine Erklärung der Aktionen finden Sie unter Aktionen in Filterregeln auf Seite 28.

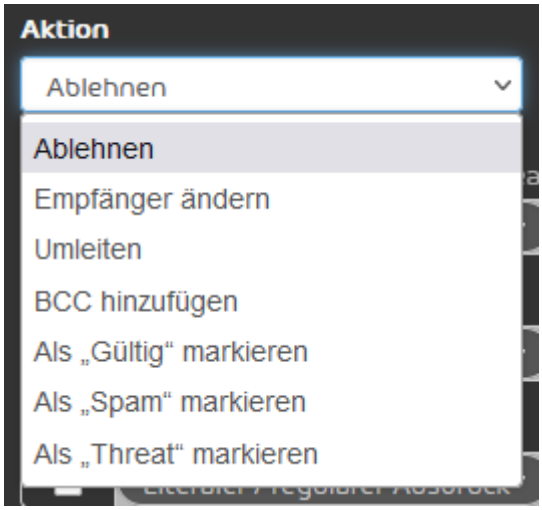

Abbildung 3: Aktion auswählen

Falls für die ausgewählte Aktion zusätzliche Angaben erforderlich sind, erscheint unter dem Drop-down-Menü ein zusätzliches Feld. Für weitere Informationen zu den zusätzlichen Feldern der Aktionen siehe Aktionen in Filterregeln auf Seite 28.

7. Wählen Sie unter **Bedingungen** die Art der Filterregel aus. Sie haben die folgenden Optionen:

   - **Header**: Die Filterregel betrifft alle E-Mails, deren Header einen festgelegten Suchbegriff enthält.
   - **Body**: Die Filterregel betrifft alle E-Mails, deren Body einen festgelegten Suchbegriff enthält.
   - **Erweitert**: Sie können für die E-Mails den Absender, den Empfänger, die IPv4-Adresse und den Hostname festlegen. Sie können auch Suchbegriffe für den Betreff und den Anhang der E-Mails und eine maximale E-Mail-Größe festlegen. Die Filterregel betrifft alle E-Mails mit den festgelegten Merkmalen.

> **Hinweis:**
>
> Die Art der Filterregel bestimmt, auf welche E-Mails die Filterregel angewendet werden soll.

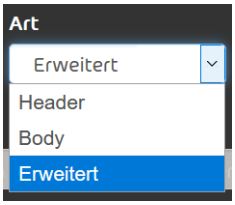

Abbildung 4: Art der Filterregel auswählen

Unter dem Drop-down-Menü werden Felder zur Konfiguration der Filterregel angezeigt. Welche Felder angezeigt werden, hängt von der ausgewählten Art der Filterregel ab.

> **Hinweis:**
>
> Unter Arten von Filterregeln auf Seite 31 finden Sie eine Übersicht und Erklärungen der Felder, die für jede Art von Filterregel verfügbar sind.

8. Falls Sie die Art **Erweitert** ausgewählt haben, folgen Sie den folgenden Schritten:

   a) Wählen Sie unter **Bedingungen** die logische Verknüpfung zwischen den Bedingungen aus, die für die Filterregel gelten soll. Sie haben die folgenden Optionen:

   - **Alle Bedingungen erfüllen**: Alle ausgewählten Bedingungen müssen erfüllt werden, damit die Filterregel auf eine E-Mail angewendet wird. Diese Verknüpfung entspricht einem logischen UND.
   - **Eine beliebige Bedingung erfüllen**: Es reicht, dass eine der ausgewählten Bedingungen erfüllt wird, damit die Filteregel auf eine E-Mail angewendet wird. Diese Verknüpfung entspricht einem logischen ODER.

   b) Setzen Sie ein Häkchen in den Checkboxen der Bedingungen, die für die Filterregel gelten sollen.

➔ Die Eingabefelder der ausgewählten Bedingungen werden freigeschaltet.

   c) Falls das Eingabefeld der ausgewählten Bedingung ein Drop-down-Menü enthält, wählen Sie aus, welche Art von Eingabe Sie machen möchten. Sie haben die folgenden Optionen:

   - **Literaler / regulärer Ausdruck**: Der eingegebene Wert wird das literaler oder regulärer Ausdruck interpretiert.
   - **Im Verzeichnis enthalten**: Der eingegebene Wert wird als Name eines Verzeichnisses (siehe Verzeichnisse auf Seite 53) interpretiert, das in der Bedingung referenziert wird. Die Bedingung wird erfüllt, falls der entsprechende Wert der E-Mail mit einem Eintrag aus dem referenzierten Verzeichnis übereinstimmt.
   - **Nicht im Verzeichnis enthalten**: Der eingegebene Wert wird als Name eines Verzeichnisses (siehe Verzeichnisse auf Seite 53) interpretiert, das in der Bedingung

referenziert wird. Die Bedingung wird erfüllt, falls der entsprechende Wert der E-Mail mit keinem einzigen Eintrag aus dem referenzierten Verzeichnis übereinstimmt.

d) Falls Sie die Bedingung **Absender** oder **Empfänger** ausgewählt haben, wählen Sie aus, auf welches Feld der E-Mail sich der eingegebene Wert beziehen soll. Sie haben die folgenden Optionen:

- **Laut Envelope**: Der eingegebene Wert muss mit der Adresse übereinstimmen, die als Parameter von **MAIL FROM:** (Absenderadresse) oder **RCPT TO:** (Empfängeradresse) während der E-Mail-Übertragung übergeben worden ist.
- **Laut Header**: Der eingegebene Wert muss mit der Adresse übereinstimmen, die im Feld **From** (Absenderadresse) oder **To** im Header der E-Mail angegeben ist.
- **Laut beidem**: Die eingegebene Absenderadresse muss entweder als Parameter von **MAIL FROM:** oder im Feld **From** im Header der E-Mail angegeben sein. Die eingegebene Empfängeradresse muss entweder als Parameter von **RCPT TO:** oder im Feld **To** im Header der E-Mail angegeben sein.

9. Geben Sie je nach der Art der Eingabe einen Suchbegriff, einen Wert oder den Namen eines Verzeichnisses in die Eingabefelder der Bedingungen ein.

> **Hinweis:**
>
> Ein Suchbegriff wird als literaler oder regulärer Ausdruck auch gefunden, falls er von Text umgeben ist.

> **Hinweis:**
>
> Um genauere und vielseitigere Regeln zu definieren, können Sie reguläre Ausdrücke verwenden. Eine Beschreibung des Aufbaus und der Funktionalität von regulären Ausdrücken finden Sie unter Reguläre Ausdrücke auf Seite 61 und Erklärung der regulären Ausdrücke auf Seite 62. Unter Ausnahmen bei regulären Ausdrücken auf Seite 70 finden Sie eine Übersicht nicht unterstützter Zeichen.
>
> Reguläre Ausdrücke können nur in Regeln des Typs **Erweitert** verwendet werden.

> **Hinweis:**
>
> Geben Sie in das Feld **Größer als** die maximale E-Mail-Größe in Megabyte ein.

10. Optional: Geben Sie unter **Beschreibung (optional)** eine Beschreibung der Filterregel ein.

Abbildung 5: Filterregel beschreiben

11. Klicken Sie auf **Hinzufügen**.

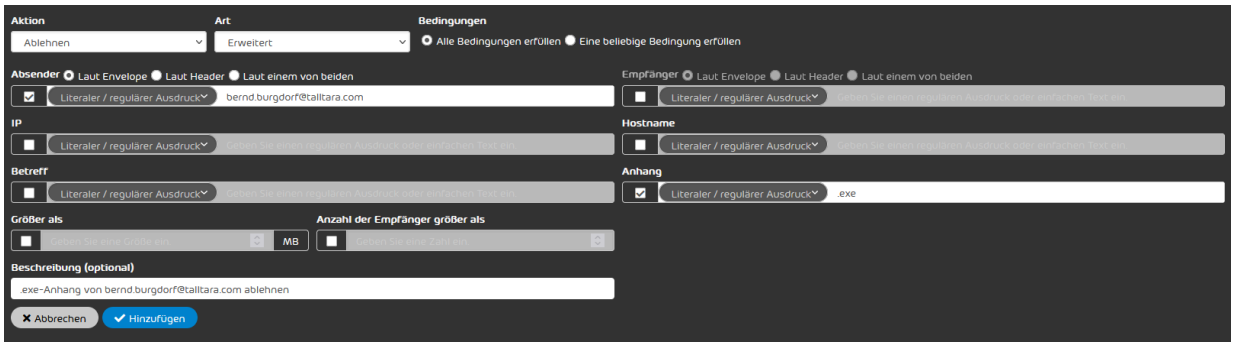

Abbildung 6: Filterregel hinzufügen

Die Filterregel wird zu der Tabelle unter **Regeln für eingehende E-Mails** hinzugefügt (siehe Anzeige von Filterregeln auf Seite 26). Die Filterregel erhält die niedrigste Priorität aller bestehenden Filterregeln und wird an das Ende der Tabelle gesetzt. Die Filterregel wird aktiviert.

Eine Filterregel für eingehende E-Mails ist erstellt worden.

Anschließend können Sie die Filterregel bearbeiten (siehe Filterregel bearbeiten auf Seite 39), die Priorität der Filterregel ändern (siehe Priorität einer Filterregel ändern auf Seite 41), die Filterregel vorübergehend deaktivieren (siehe Filterregel des Compliance Filters deaktivieren auf Seite 50) oder löschen (siehe Filterregel des Compliance Filters löschen auf Seite 51).

Filterregel für ausgehende E-Mails erstellen

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11).

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) für ausgehende E-Mails erstellen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.

2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie die Filterregel erstellen möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.
5. Klicken Sie unter **Regeln für ausgehende E-Mails** auf **Regel hinzufügen**.

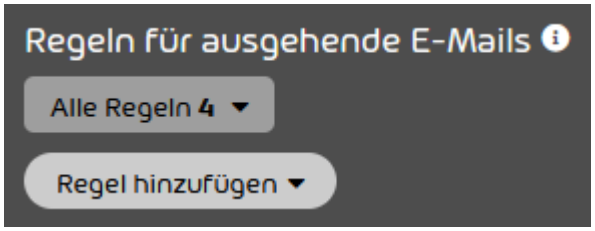

Abbildung 7: Regel hinzufügen

6. Wählen Sie unter **Aktion** aus, was mit den E-Mails geschehen soll, auf die die Filterregel angewendet wird. Sie können aus den folgenden Aktionen wählen:

   - **Ablehnen**
   - **Empfänger ändern**
   - **Umleiten**
   - **BCC hinzufügen**
   - **Absender benachrichtigen**

   Hinweis:

   Eine Erklärung der Aktionen finden Sie unter Aktionen in Filterregeln auf Seite 28.

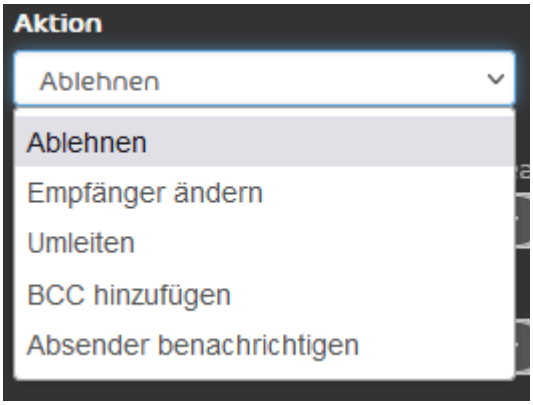

Abbildung 8: Aktion auswählen

Falls für die ausgewählte Aktion zusätzliche Angaben erforderlich sind, erscheint unter dem Drop-down-Menü ein zusätzliches Feld. Für weitere Informationen zu den zusätzlichen Feldern der Aktionen siehe Aktionen in Filterregeln auf Seite 28.

7. Wählen Sie unter **Art** die Art der Filterregel aus. Dies bestimmt die E-Mails, auf die die Filterregel angewendet werden soll. Sie haben die folgenden Optionen:

   - **Header**: Die Filterregel betrifft alle E-Mails, deren Header einen festgelegten Suchbegriff enthält.
   - **Body**: Die Filterregel betrifft alle E-Mails, deren Body einen festgelegten Suchbegriff enthält.
   - **Erweitert**: Sie können für die E-Mails den Absender, den Empfänger, die IPv4-Adresse und den Hostname festlegen. Sie können auch Suchbegriffe für den Betreff und den Anhang der E-Mails und eine maximale E-Mail-Größe festlegen. Die Filterregel betrifft alle E-Mails mit den festgelegten Merkmalen.

   Hinweis:

   Die Art der Filterregel bestimmt, auf welche E-Mails die Filterregel angewendet werden soll.

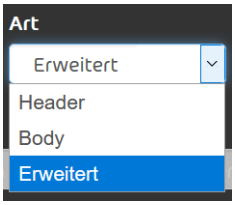

Abbildung 9: Art der Filterregel auswählen

Unter dem Drop-down-Menü werden Felder zur Konfiguration der Filterregel angezeigt. Welche Felder angezeigt werden, hängt von der ausgewählten Art der Filterregel ab.

Hinweis:

Unter Arten von Filterregeln auf Seite 31 finden Sie eine Übersicht und Erklärungen der Felder, die für jede Art von Filterregel verfügbar sind.

8. Falls Sie die Art **Erweitert** ausgewählt haben, folgen Sie den folgenden Schritten:

   a) Wählen Sie unter **Bedingungen** die logische Verknüpfung zwischen den Bedingungen aus, die für die Filterregel gelten soll. Sie haben die folgenden Optionen:

   - **Alle Bedingungen erfüllen**: Alle ausgewählten Bedingungen müssen erfüllt werden, damit die Filterregel auf eine E-Mail angewendet wird. Diese Verknüpfung entspricht einem logischen UND.
   - **Eine beliebige Bedingung erfüllen**: Es reicht, dass eine der ausgewählten Bedingungen erfüllt wird, damit die Filteregel auf eine E-Mail angewendet wird. Diese Verknüpfung entspricht einem logischen ODER.

   b) Setzen Sie ein Häkchen in den Checkboxen der Bedingungen, die für die Filterregel gelten sollen.

➔ Die Eingabefelder der ausgewählten Bedingungen werden freigeschaltet.

   c) Falls das Eingabefeld der ausgewählten Bedingung ein Drop-down-Menü enthält, wählen Sie aus, welche Art von Eingabe Sie machen möchten. Sie haben die folgenden Optionen:

   - **Literaler / regulärer Ausdruck**: Der eingegebene Wert wird das literaler oder regulärer Ausdruck interpretiert.
   - **Im Verzeichnis enthalten**: Der eingegebene Wert wird als Name eines Verzeichnisses (siehe Verzeichnisse auf Seite 53) interpretiert, das in der Bedingung referenziert wird. Die Bedingung wird erfüllt, falls der entsprechende Wert der E-Mail mit einem Eintrag aus dem referenzierten Verzeichnis übereinstimmt.
   - **Nicht im Verzeichnis enthalten**: Der eingegebene Wert wird als Name eines Verzeichnisses (siehe Verzeichnisse auf Seite 53) interpretiert, das in der Bedingung

referenziert wird. Die Bedingung wird erfüllt, falls der entsprechende Wert der E-Mail mit keinem einzigen Eintrag aus dem referenzierten Verzeichnis übereinstimmt.

d) Falls Sie die Bedingung **Absender** oder **Empfänger** ausgewählt haben, wählen Sie aus, auf welches Feld der E-Mail sich der eingegebene Wert beziehen soll. Sie haben die folgenden Optionen:

- **Laut Envelope**: Der eingegebene Wert muss mit der Adresse übereinstimmen, die als Parameter von **MAIL FROM:** (Absenderadresse) oder **RCPT TO:** (Empfängeradresse) während der E-Mail-Übertragung übergeben worden ist.
- **Laut Header**: Der eingegebene Wert muss mit der Adresse übereinstimmen, die im Feld **From** (Absenderadresse) oder **To** im Header der E-Mail angegeben ist.
- **Laut beidem**: Die eingegebene Absenderadresse muss entweder als Parameter von **MAIL FROM:** oder im Feld **From** im Header der E-Mail angegeben sein. Die eingegebene Empfängeradresse muss entweder als Parameter von **RCPT TO:** oder im Feld **To** im Header der E-Mail angegeben sein.

9. Geben Sie je nach der Art der Eingabe einen Suchbegriff, einen Wert oder den Namen eines Verzeichnisses in die Eingabefelder der Bedingungen ein.

> **Hinweis:**
>
> Ein Suchbegriff wird als literaler oder regulärer Ausdruck auch gefunden, falls er von Text umgeben ist.

> **Hinweis:**
>
> Um genauere und vielseitigere Regeln zu definieren, können Sie reguläre Ausdrücke verwenden. Eine Beschreibung des Aufbaus und der Funktionalität von regulären Ausdrücken finden Sie unter Reguläre Ausdrücke auf Seite 61 und Erklärung der regulären Ausdrücke auf Seite 62. Unter Ausnahmen bei regulären Ausdrücken auf Seite 70 finden Sie eine Übersicht nicht unterstützter Zeichen.
>
> Reguläre Ausdrücke können nur in Regeln des Typs **Erweitert** verwendet werden.

> **Hinweis:**
>
> Geben Sie in das Feld **Größer als** die maximale E-Mail-Größe in Megabyte ein.

10. Optional: Geben Sie unter **Beschreibung (optional)** eine Beschreibung der Filterregel ein.

Abbildung 10: Filterregel beschreiben

11. Klicken Sie auf **Hinzufügen**.

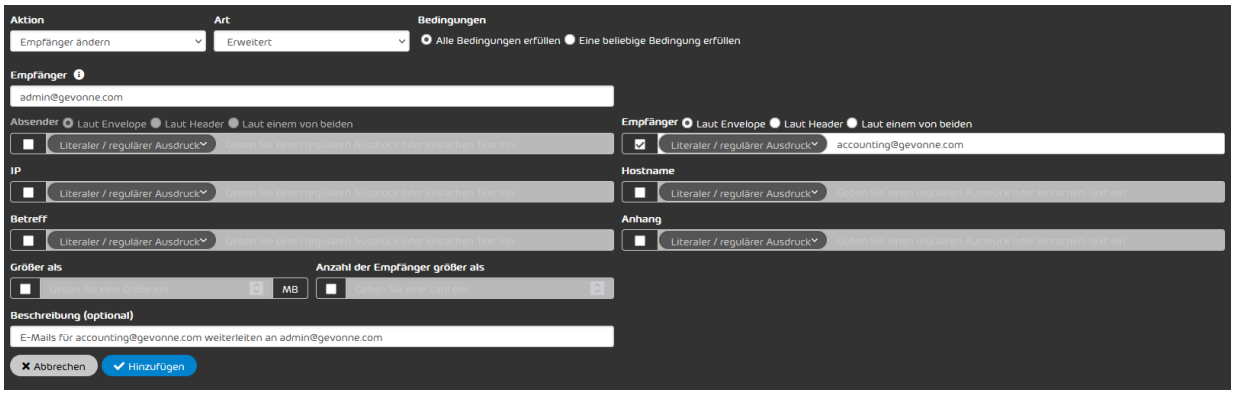

Abbildung 11: Filterregel hinzufügen

Die Filterregel wird zu der Tabelle unter **Regeln für ausgehende E-Mails** hinzugefügt (siehe Anzeige von Filterregeln auf Seite 26). Die Filterregel erhält die niedrigste Priorität aller bestehenden Filterregeln und wird an das Ende der Tabelle gesetzt. Die Filterregel wird aktiviert.

Eine Filterregel für ausgehende E-Mails ist erstellt worden.

Anschließend können Sie die Filterregel bearbeiten (siehe Filterregel bearbeiten auf Seite 39), die Priorität der Filterregel ändern (siehe Priorität einer Filterregel ändern auf Seite 41), die Filterregel vorübergehend deaktivieren (siehe Filterregel des Compliance Filters deaktivieren auf Seite 50) oder löschen (siehe Filterregel des Compliance Filters löschen auf Seite 51).

Anzeige von Filterregeln

Die Filterregeln für eingehende und ausgehende E-Mails werden nach deren Erstellung in der entsprechenden Tabelle unter den Abschnitten **Regeln für eingehende E-Mails** und **Regeln für ausgehende E-Mails** angezeigt.

Beide Tabellen enthalten folgende Spalten:

- **Priorität**: Anwendungspriorität der Filterregel. Eine Filterregel mit einer kleineren Zahl in diesem Feld greift schneller als eine Filterregel mit einer größeren Zahl ein. Filterregeln werden in der Tabelle nach absteigender Priorität sortiert.
- **Aktiv**: Ein Häkchen in der Checkbox gibt an, dass die Filterregel aktiviert ist.
- **Aktion**: Hier wird die Aktion angegeben, die durch die Filterregel ausgeführt wird.
  - Aktionen für eingehende E-Mails: **Empfänger ändern**, **Umleiten**, **BCC hinzufügen**, **Als „Gültig “ markieren**, **Als „Spam “ markieren**, **Als „Threat “ markieren**.
  - Aktionen für ausgehende E-Mails: **Ablehnen**, **Empfänger ändern**, **Umleiten**, **BCC hinzufügen**, **Absender benachrichtigen**.

  Hinweis:

  Die verfügbaren Aktionen werden im Kapitel Aktionen in Filterregeln auf Seite 28 beschrieben.
- **Art**: Hier wird die Art der Filterregel angegeben.
- **Bedingungen**: Hier werden die Filterbedingungen in der eingestellten Systemsprache angegeben. Wird in einer erweiterten Regel ein Verzeichnis referenziert, wird dieses mit dem Kürzel **D** angegeben. Bei dem folgenden Beispiel werden die Absender aus dem Verzeichnis **forbiddensenders** für die Regel berücksichtigt: **Absender: ?A=?D=forbiddensenders**. Zudem können die Einträge aus einem Verzeichnis negiert werden. Bei dem folgenden Beispiel werden

die Absender aus dem Verzeichnis **forbiddensenders** nicht berücksichtigt: **Absender: ?A=?D!=forbiddensenders**.

> **HINWEIS:**
>
> Bei den Filterbedingungen **Absender** und **Empfänger** wird darüber hinaus das Feld oder Felder angegeben, auf das oder die sich der eingegebene Wert bezieht (**Laut Envelope**, **Laut Header** und **Laut beidem** wie im Kapitel Arten von Filterregeln auf Seite 31 beschrieben). Das wird jeweils mit den Kürzeln **E** (für **Envelope**), **H** (für **Header**) und **A** (für **Any**) sprachunabhängig angegeben.
>
> Zum Beispiel würde die Angabe **Absender:?E=mueller@gevonne.com** bedeuten, dass eine Filterregel auf E-Mails mit dem Envelope Sender **mueller@gevonne.com** angewendet werden soll.

- **Beschreibung**: Vom Ersteller der Filterregel vergebene Beschreibung.
- **ID**: Automatisch vom System vergebene Zahl zur Kennzeichnung der Filterregel.

Aktionen in Filterregeln

Jeder Filterregel des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) ist eine Aktion zugeordnet. Sobald die Filterregel auf eine E-Mail angewendet wird, wird diese Aktion durchgeführt.

Für eingehende und ausgehende E-Mails sind unterschiedliche Aktionen verfügbar.

Die folgenden Aktionen sind nur für eingehende E-Mails verfügbar:

- **Als „Gültig “ markieren**
- **Als „Spam “ markieren**
- **Als „Threat “ markieren**

Die Aktion **Absender benachrichtigen** ist nur für ausgehende E-Mails verfügbar.

In der folgenden Tabelle sind alle Aktionen für Filterregeln im Modul **Compliance Filter** beschrieben. Falls im Modul **Compliance Filter** eine Aktion ausgewählt wird, für die zusätzliche Angaben erforderlich sind, wird für die Aktion ein zusätzliches Feld angezeigt. Diese Felder sind ebenfalls in der Tabelle beschrieben.

Tabelle 1: Aktionen für Filterregeln

AKTION	BESCHREIBUNG
Ablehnen	**ACHTUNG:** Die E-Mail wird abgelehnt. Der versendende E-Mail-Server wird über den Verbindungsabbruch per Fehlercode und Text informiert (**554 5.6.9 customer rule based reject by Compliance-Filter**). Für weitere Informationen siehe "Kategorisierungsgründe" im Control-Panel-Handbuch. Die Information des Absenders liegt in der Verantwortung des versendenden E-Mail-Servers.

AKTION	BESCHREIBUNG
Empfänger ändern	Die E-Mail wird statt an den ursprünglichen Empfänger an eine oder mehrere andere E-Mail-Adressen zugestellt. Falls diese Aktion ausgewählt wird, wird das Feld **E-Mail senden an:** angezeigt. In dieses Feld müssen Administratoren auf Kundenebene alle E-Mail-Adressen eingeben, an die die E-Mail weitergeleitet werden soll. Die Administratoren können beliebig viele E-Mail-Adressen in das Feld eingeben. Falls mehrere E-Mail-Adressen eingegeben werden, müssen diese mit einem Semikolon voneinander getrennt werden.
Umleiten	Die E-Mail wird über eine andere IPv4-Adresse oder einen anderen Hostname umgeleitet. Falls diese Aktion ausgewählt wird, wird das Feld **IP oder Hostname** angezeigt. In dieses Feld müssen Administratoren auf Kundenebene die IPv4-Adresse oder den Hostname eingeben, über den die E-Mail umgeleitet werden soll. Administratoren können nur eine IPv4-Adresse oder einen Hostname eingeben.

AKTION	BESCHREIBUNG
BCC hinzufügen	Zu der E-Mail werden automatisch ein oder mehrere BCC-Empfänger hinzugefügt. Falls diese Aktion ausgewählt wird, wird das Feld **E-Mail senden an:** angezeigt. In dieses Feld müssen Administratoren auf Kundenebene die E-Mail-Adressen eingeben, an die Blindkopien der E-Mail geschickt werden sollen. Die Administratoren können beliebig viele E-Mail-Adressen in das Feld eingeben. Falls mehrere E-Mail-Adressen eingegeben werden, müssen diese mit einem Semikolon voneinander getrennt werden.
Absender benachrichtigen	Der Absender wird per E-Mail benachrichtigt, sobald die ausgehende E-Mail vom Ziel-Server angenommen wurde.
Als „Gültig “ markieren	Die eingehende E-Mail wird als **Gültig** eingestuft.
Als „Spam “ markieren	Die eingehende E-Mail wird als **Spam** eingestuft.
Als „Threat “ markieren	Die eingehende E-Mail wird als **Threat** eingestuft.

Arten von Filterregeln

Bei der Erstellung von Filterregeln im Modul **Compliance Filter** (siehe Über den Compliance Filter auf Seite 6) müssen Administratoren auf Kundenebene die Art der Filterregel auswählen. Mit der Art der Filterregel legen die Administratoren die Merkmale der E-Mails fest, auf die die Filterregel

angewendet werden soll. Für jede Art von Filterregel werden im Modul **Compliance Filter** Felder für unterschiedliche Merkmale eingeblendet.

Die folgenden Tabellen zeigen eine Übersicht der Felder, die für jede Art von Filterregel zur Verfügung stehen. Die Tabellen enthalten Beschreibungen der Merkmale und Beispiele für mögliche Eingaben.

Hinweis:

Um genauere und vielseitigere Regeln zu definieren, können reguläre Ausdrücke verwendet werden. Für eine Beschreibung des Aufbaus und der Funktionalität von regulären Ausdrücken siehe Reguläre Ausdrücke auf Seite 61 und Erklärung der regulären Ausdrücke auf Seite 62. Für eine Übersicht nicht unterstützter Zeichen siehe Ausnahmen bei regulären Ausdrücken auf Seite 70.

Hinweis:

Um die Verwaltung von Bedingungen zu vereinfachen, können Administratoren auf Kundenebene mehrere Ausdrücke in Verzeichnissen zusammenfassen. Verzeichnisse können in den Eingabefeldern der Bedingungen von Filterregeln referenziert werden. Für weitere Informationen zur Funktionsweise, Erstellung und Verwaltung von Verzeichnissen siehe Verzeichnisse auf Seite 53.

Tabelle 2: Art Header

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Filter: Header	Der Header der E-Mail wird nach dem eingegebenen Suchbegriff durchsucht.	Rechnung

Tabelle 3: Art Body

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Filter: Body	Der decodierte Body der E-Mail wird nach dem eingegebenen Suchbegriff durchsucht. **Hinweis:** Anhänge sind von der Suche im Body der E-Mail ausgeschlossen.	Zahlungsanweisung

Tabelle 4: Art Erweitert

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Absender	Die Absenderadresse der E-Mail wird nach dem eingegebenen Suchbegriff oder nach den Einträgen aus dem referenzierten Verzeichnis (siehe Verzeichnisse auf Seite 53) durchsucht. **Hinweis:** Administratoren auf Kundenebene können aus den folgenden Optionen auswählen, welche Art von Absenderadresse durchsucht wird (siehe Filterregel für eingehende E-Mails erstellen): • **Laut Envelope**: Absenderadresse aus dem Envelope (**MAIL FROM:**) • **Laut Header**: Absenderadresse aus dem Header (**To:**) • **Laut beidem**: eine beliebige der beiden Absenderadressen	**user@gevonne.com**

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Empfänger	Die Empfängeradressen werden nach dem eingegebenen Suchbegriff oder nach den Einträgen aus dem referenzierten Verzeichnis durchsucht. **Hinweis:** Administratoren auf Kundenebene können aus den folgenden Optionen auswählen, welche Art von Empfängeradresse durchsucht wird (siehe Filterregel für eingehende E-Mails erstellen): • **Laut Envelope**: Empfängeradresse aus dem Envelope (**RCPT TO:**) • **Laut Header**: Empfängeradresse aus dem Header (**From:**) • **Laut beidem**: eine beliebige der beiden Empfängeradressen **Hinweis:** Falls eine E-Mail an	**user.extern@yahoo.com**

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
IP	Die öffentliche IPv4-Adresse des versendenden E-Mail-Servers wird nach dem eingegebenen Suchbegriff oder nach den Einträgen aus dem referenzierten Verzeichnis durchsucht. **Hinweis:** Geben Sie als Suchbegriff die IPv4-Adresse ohne Subnetzmaske ein.	Richtig: **0.0.0.0** Falsch: **0.0.0.0/24**
Hostname	Der Hostname (PTR-Eintrag), der durch Rückwärtsauflösung der IPv4-Adresse des E-Mail-Servers erhalten wird, wird nach dem eingegebenen Suchbegriff oder nach den Einträgen aus dem referenzierten Verzeichnis durchsucht. Je nachdem, ob die Regel für eingehende oder ausgehende E-Mails gilt, handelt es sich hierbei um den Hostnamen des Ausgangs- oder Zielservers.	**mailserver.domain.com**

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Betreff	Der Betreff der E-Mail wird nach dem eingegebenen Suchbegriff oder nach den Einträgen aus dem referenzierten Verzeichnis durchsucht.	**Spam**

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Anhang	Die Dateinamen und die Dateiendungen der E-Mail-Anhänge werden nach dem eingegebenen Suchbegriff oder nach den Einträgen aus dem referenzierten Verzeichnis durchsucht. **Hinweis:** Es kann nach einer Dateiendung oder nach einem Bestandteil des Dateinamens gesucht werden. Um nach einer Dateiendung zu suchen, muss als Suchbegriff die Dateiendung eingegeben werden. Um nach einem Bestandteil des Dateinamens zu suchen, muss als Suchbegriff der gesuchte Bestandteil eingegeben werden. **Hinweis:** Für den Compliance Filter können die Sammelbegriffe für Dateianhänge nicht	**.jpg** **express**

FELD	BESCHREIBUNG	BEISPIEL FÜR EINGABE
Größer als	Es wird geprüft, ob die E-Mail die eingegebene Größe überschreitet. **Hinweis:** Die maximale E-Mail-Größe wird in Megabyte angegeben.	**500**
Anzahl der Empfänger größer als	Es wird geprüft, ob die Anzahl der Empfänger die eingegebene Größe überschreitet.	**10**

Filterregel bearbeiten

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11) und Filterregeln für den Compliance Filter erstellt (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 oder Filterregel für ausgehende E-Mails erstellen auf Seite 19).

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie bestehende Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) bearbeiten.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.

5. Klicken Sie in der Liste der Filterregeln für eingehende oder ausgehende E-Mails auf den Menüpfeil neben der Filterregel, die Sie bearbeiten möchten.

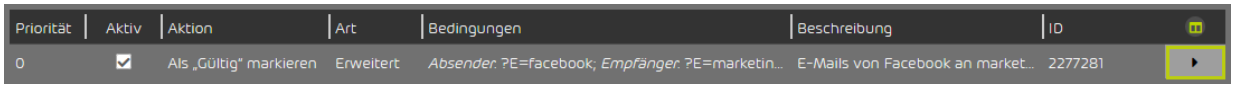

Abbildung 12: Menü öffnen

6. Klicken Sie auf **Regel bearbeiten**.

Abbildung 13: Filterregel bearbeiten

Ein Menü mit den aktuellen Einstellungen der Filterregel öffnet sich.

7. Ändern Sie die Einstellungen nach Ihren Wünschen.

> **Hinweis:**
>
> Weitere Informationen finden Sie unter Filterregel für eingehende E-Mails erstellen auf Seite 13 oder Filterregel für ausgehende E-Mails erstellen auf Seite 19.

8. Klicken Sie auf **Änderungen übernehmen**.

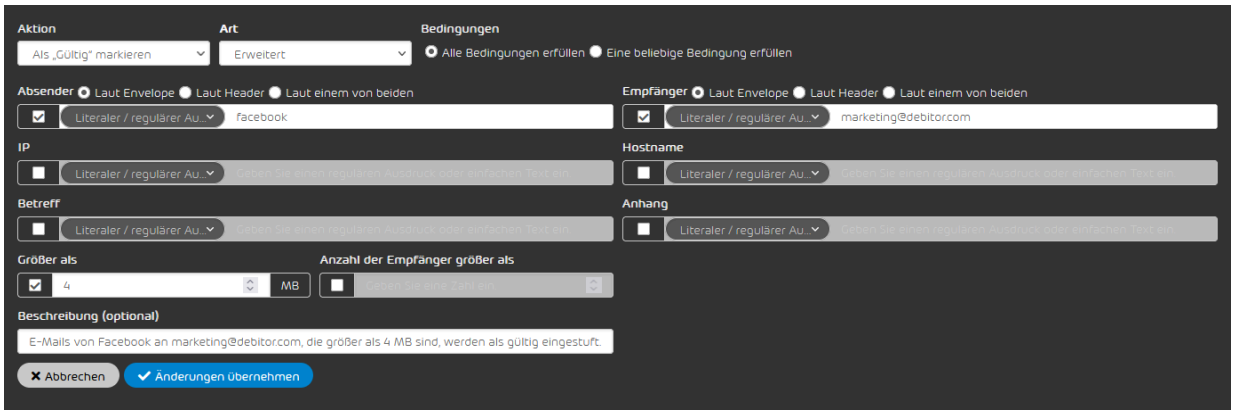

Abbildung 14: Änderungen übernehmen

Die Änderungen werden übernommen.

Eine Filterregel ist bearbeitet worden.

Priorität einer Filterregel ändern

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11) und Filterregeln für den Compliance Filter erstellt (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 oder Filterregel für ausgehende E-Mails erstellen auf Seite 19).

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie die Reihenfolge ändern, in der die Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) abgearbeitet werden. Um die Reihenfolge der Filterregeln zu ändern, ändern Sie die Priorität der Filterregeln.

WICHTIG:

In welcher Reihenfolge die Filterregeln des Compliance Filters abgearbeitet werden, hängt neben der Priorität auch von der Art der Filterregeln ab (siehe Reihenfolge der Filterregeln auf Seite 43).

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.
5. Klicken Sie in der Liste der Filterregeln für eingehende oder ausgehende E-Mails auf den Menüpfeil neben der Filterregel, deren Priorität Sie ändern möchten.

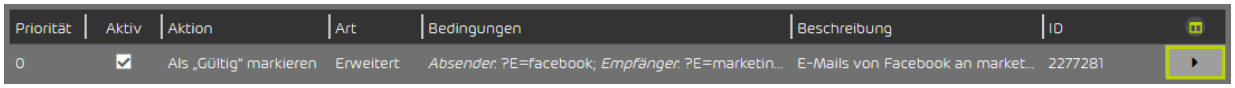

Abbildung 15: Menü öffnen

Ein Menü öffnet sich.

6. Klicken Sie auf **Priorität ändern**.

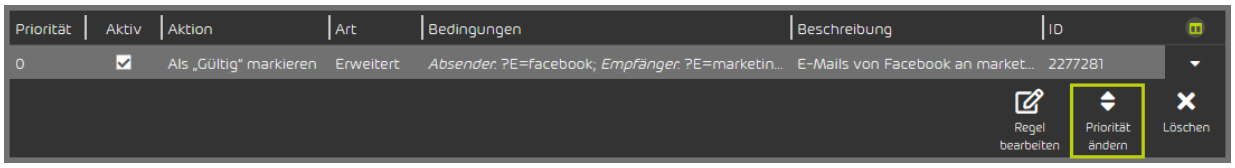

Abbildung 16: Priorität ändern

Ein Menü öffnet sich.

7. Geben Sie unter **Priorität** die neue Priorität der Filterregel ein.

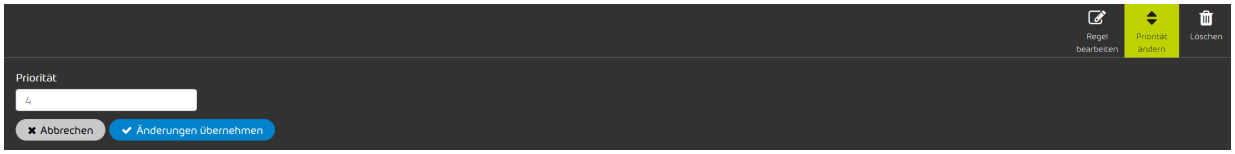

Abbildung 17: Priorität eingeben

8. Klicken Sie auf **Änderungen übernehmen**.

Die neue Priorität wird der Filterregel zugewiesen. Die Filterregel wird in der Liste an die Stelle verschoben, die der neuen Priorität entspricht.

Die Priorität einer Filterregel ist geändert worden. Dadurch hat sich die Reihenfolge geändert, in der die Filterregeln abgearbeitet werden.

Reihenfolge der Filterregeln

WICHTIG:

Beachten Sie, wie sich der Compliance Filter in die Reihenfolge unserer Services einordnet (siehe Regelreihenfolge innerhalb aller Services auf Seite 8). Sobald eine Regel eines Services auf eine E-Mail zutrifft, wird die Abarbeitung weiterer Regeln gestoppt. Auf die E-Mail werden keine weiteren Regeln angewendet.

Aufgrund dieser Reihenfolge können Sie Ausnahmen für Content Control mit Filterregeln des Compliance Filters erstellen, die E-Mails als **Gültig** kategorisieren.

Die Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) werden nach ihrer Art (siehe Arten von Filterregeln auf Seite 31) in der folgenden Reihenfolge abgearbeitet:

1. **Body**
2. **Header**
3. **Erweitert**

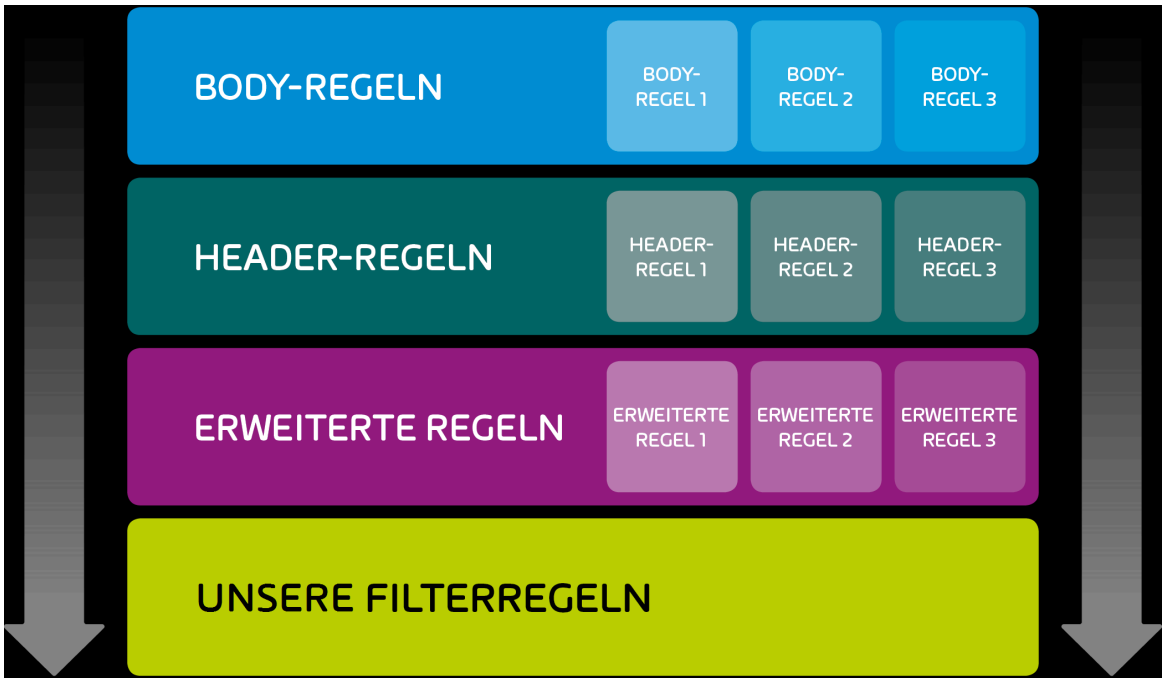

Abbildung 18: Reihenfolge der Filterregeln nach Art

Filterregeln der gleichen Art werden nach ihrer Priorität geordnet und in dieser Reihenfolge abgearbeitet.

Hinweis:

Je höher die Zahl ist, desto niedriger ist die Priorität der Filterregel.

Administratoren auf Kundenebene können die Priorität einer Filterregel ändern (siehe Priorität einer Filterregel ändern auf Seite 41).

Die folgenden Beispiele verdeutlichen die Reihenfolge der Regelabarbeitung.

Einfache Abarbeitung der Filterregeln

Ausgangssituation:

Ein Administrator auf Kundenebene hat Filterregeln für den Compliance Filter definiert. Auf das Fallbeispiel treffen keine Regeln anderer Services zu.

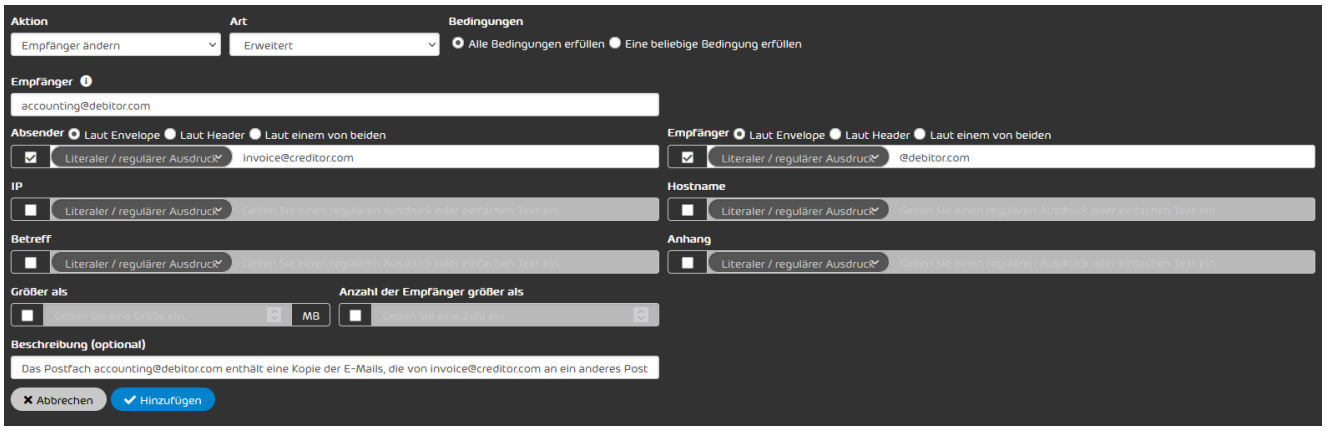

Abbildung 19: Filterregel: Weiterleiten

Ablauf:

1. Eine E-Mail von **invoice@creditor.com** wird an einen beliebigen Benutzer der Domain debitor.com gesendet.
2. Der Compliance Filter durchsucht zunächst die Filterregeln der Art **Body**, dann die Filterregeln der Art **Header** und erzielt einen Treffer in den Filterregeln der Art **Erweitert**.
3. Die Filterregel wird angewendet. Der Compliance Filter sucht nicht nach weiteren Übereinstimmungen mit anderen Filterregeln.

Konflikt zwischen mehreren Filterregeln derselben Art

Ausgangssituation:

Ein Administrator auf Kundenebene hat für den Compliance Filter zwei unterschiedliche Filterregeln der Art **Erweitert** für den Fall definiert, dass eine ausgehende E-Mail an **sales@creditor.com** gesendet wird. Beide Filterregeln legen fest, dass zu der E-Mail ein BCC-Empfänger hinzugefügt wird. Für die eine Filterregel ist **purchasing@creditor.com** als BCC-Empfänger definiert, für die andere **ceo@creditor.com**. Die Filterregel mit dem BCC-Empfänger **purchasing@creditor.com** hat eine höhere Priorität als die Filterregel mit dem BCC-Empfänger **ceo@creditor.com** und befindet sich in der Übersicht der Filterregeln über der anderen Filterregel. Auf das Fallbeispiel treffen keine weiteren Filterregeln zu.

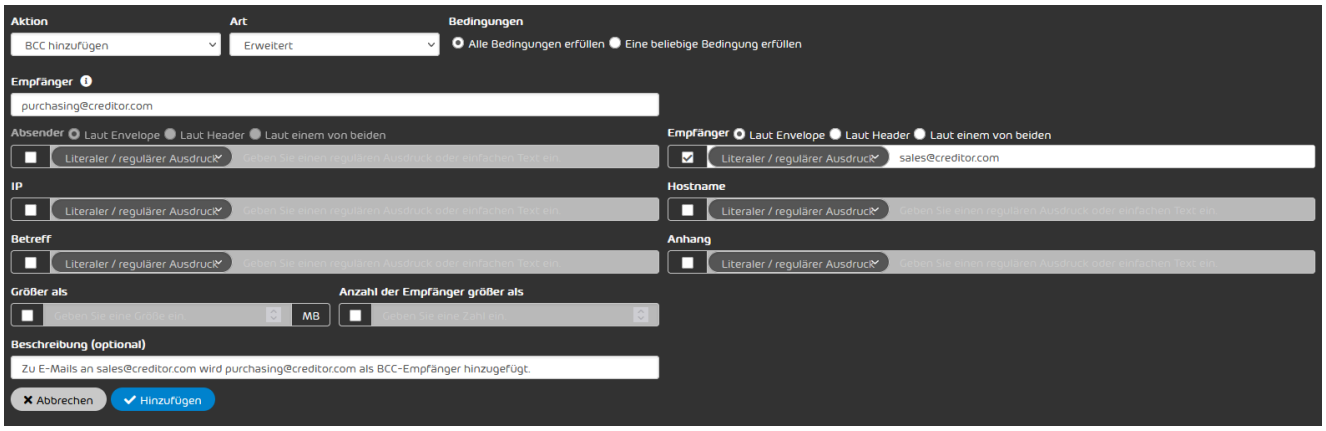

Abbildung 20: Filterregel: purchasing@creditor.com als BCC-Empfänger hinzufügen

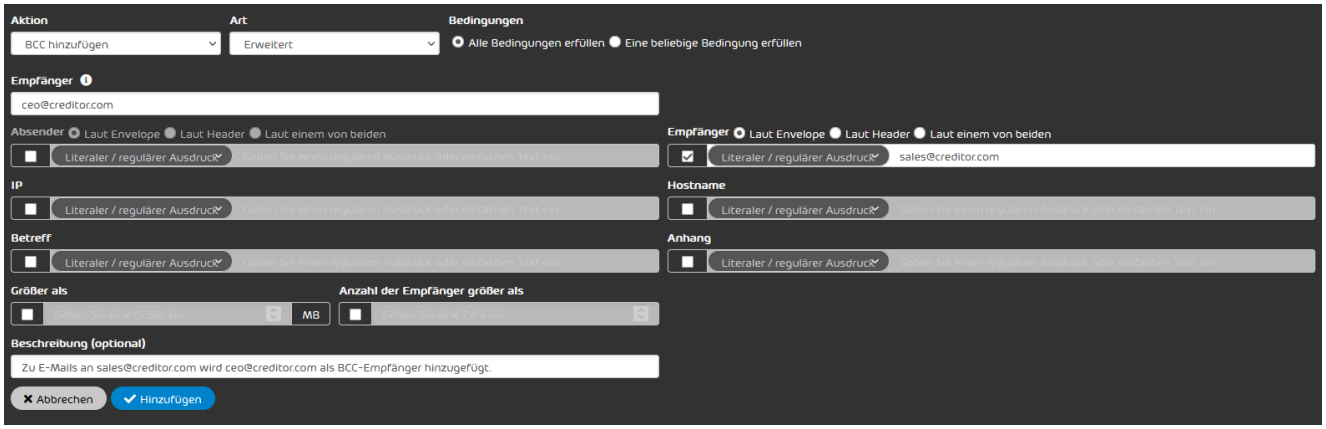

Abbildung 21: Filterregel: ceo@creditor.com als BCC-Empfänger hinzufügen

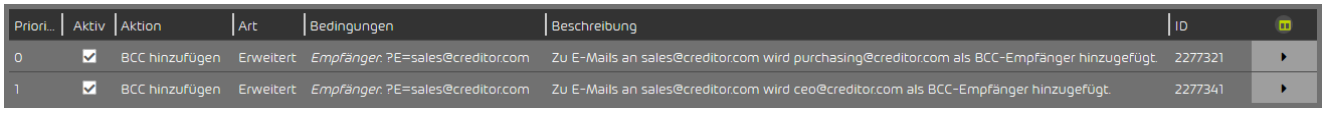

Abbildung 22: Reihenfolge der Filterregeln

Ablauf:

1. Eine E-Mail von einem beliebigen Absender wird an **sales@creditor.com** gesendet.
2. Der Compliance Filter durchsucht zunächst die Filterregeln der Art **Body**, dann die Filterregeln der Art **Header** und erzielt einen Treffer in den Filterregeln der Art **Erweitert**.

3. Die Filterregel mit der höheren Priorität (BCC an **purchasing@creditor.com**) wird angewendet. Der Compliance Filter sucht nicht nach weiteren Übereinstimmungen mit anderen Filterregeln. Die Filterregel mit der niedrigeren Priorität (BCC an **ceo@creditor.com**) wird nicht angewendet.

Konflikt zwischen Regeln unterschiedlicher Arten

Ausgangssituation:

Ein Administrator auf Kundenebene hat eine Filterregel definiert, dass eingehende E-Mails mit einem Link zu Facebook als **Spam** eingestuft werden. In einer anderen Filterregel hat der Administrator eine Ausnahme für den Empfänger **marketing@debitor.com** definiert. Als Ausnahme hat der Administrator festgelegt, dass E-Mails, die direkt von Facebook an **marketing@debitor.com** geschickt werden, als **Gültig** eingestuft werden. Die Filterregel mit der Ausnahme für **marketing@debitor.com** hat eine höhere Priorität als die Filterregel für E-Mails mit Links zu Facebook und befindet sich in der Übersicht der Filterregeln über der anderen Filterregel. Auf das Fallbeispiel treffen keine weiteren Filterregeln zu.

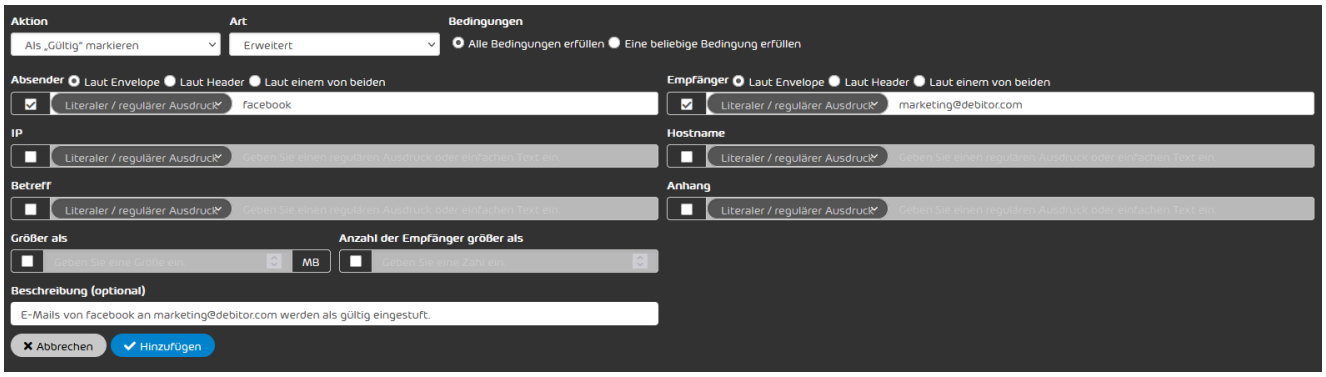

Abbildung 23: Filterregel: Als Gültig markieren

Abbildung 24: Filterregel: Als Spam markieren

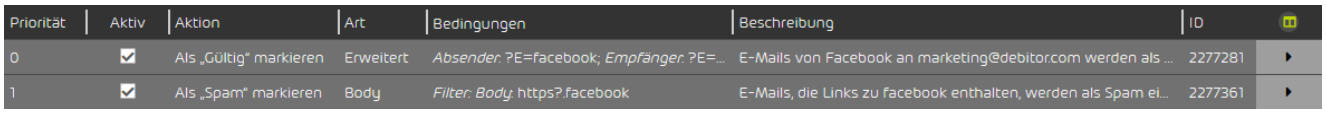

Abbildung 25: Reihenfolge der Filterregeln

Ablauf:

1. Facebook schickt an **marketing@debitor.com** eine E-Mail, die einen Link enthält.
2. Der Compliance Filter durchsucht zunächst die Filterregeln der Art **Body** und erzielt einen Treffer bei der Filterregel für E-Mails, die Links von Facebook enthalten.
3. Die Filterregel wird auf die E-Mail angewendet und die E-Mail wird als **Spam** eingestuft. Der Compliance Filter sucht nicht nach weiteren Übereinstimmungen mit anderen Filterregeln. Die Filterregel mit der Ausnahme für **marketing@debitor.com** wird trotz ihrer höheren Priorität nicht angewendet, weil die Filterregeln der Art **Body** Vorrang vor den Filterregeln der anderen Arten haben.

Konflikt zwischen dem Compliance Filter und unseren Filterregeln

Ausgangssituation:

Da von einer IPv4-Adresse vermehrt Spam verschickt wird, hat ein Administrator auf Kundenebene eine Filterregel definiert, dass E-Mails von dieser IP-Adresse als Spam markiert werden. Auf das Fallbeispiel treffen keine weiteren Filterregeln des Compliance Filters zu. Neben der Filterregel des Compliance Filters trifft eine von uns definierte Filterregel auf das Fallbeispiel zu.

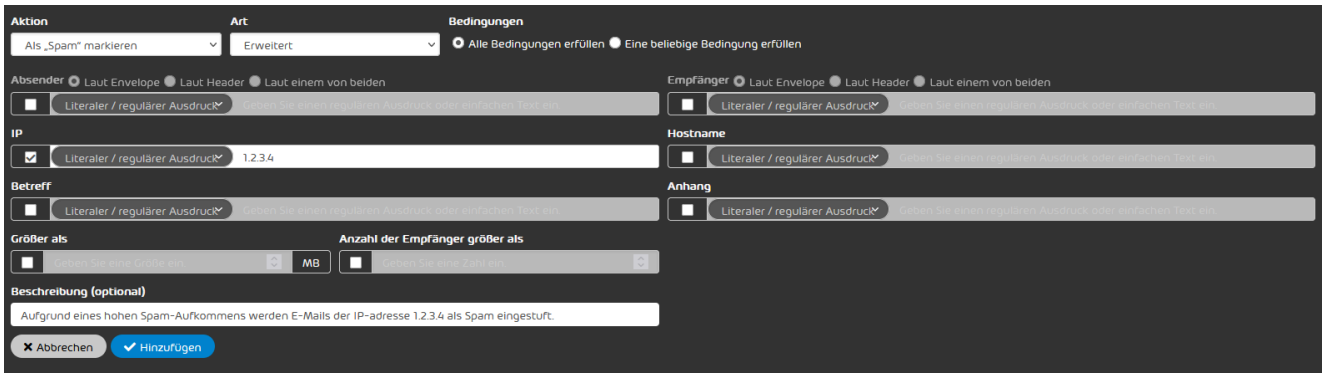

Abbildung 26: Filterregel: E-Mails einer IPv4-Adresse als Spam markieren

Ablauf:

1. Ein Absender von der Domain hinter der IPv4-Adresse sendet eine E-Mail an einen beliebigen Empfänger.
2. Der Compliance Filter durchsucht zunächst die Filterregeln der Art **Body**, dann die Filterregeln der Art **Header** und erzielt einen Treffer in den Filterregeln der Art **Erweitert**.
3. Die Filterregel wird auf die E-Mail angewendet und die E-Mail wird als **Spam** eingestuft. Der Compliance Filter sucht nicht nach weiteren Übereinstimmungen mit anderen Filterregeln.
4. Wir haben für dieses Fallbeispiel bereits eine genauere Filterregel definiert. Das erhöhte Spam-Aufkommen ließ sich auf den Absender **info@** eingrenzen. Andere E-Mail-Adressen der Domain versenden keine Spam-Mails. Da unsere Filterregeln nicht weiter durchsucht werden, gilt die vom Administrator auf Kundenebene definierte Filterregel, die einen zu großen Gültigkeitsbereich hat. Eine gültige E-Mail könnte also als Spam markiert werden.

Filterregel aktivieren

Sie haben eine Filterregel des Compliance Filters deaktiviert (siehe Filterregel des Compliance Filters deaktivieren auf Seite 50).

Sobald Sie eine deaktivierte Filterregel des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) wieder anwenden möchten, können Sie die Filterregel im Modul **Sicherheitseinstellungen** > **Compliance Filter** aktivieren.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.
5. Wählen Sie aus der Liste der Filterregeln für eingehende oder ausgehende E-Mails die gewünschte Filterregel aus und aktivieren Sie die Checkbox in der Spalte **Aktiv**.

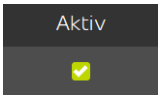

Abbildung 27: Filterregel aktivieren

Die Filterregel wird aktiviert. Die Filterregel wird wieder auf den E-Mail-Verkehr der Domain angewendet.

Eine Filterregel des Compliance Filters ist aktiviert worden.

Filterregel des Compliance Filters deaktivieren

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11) und Filterregeln für den Compliance Filter erstellt (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 oder Filterregel für ausgehende E-Mails erstellen auf Seite 19).

Falls Sie eine Filterregel des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) vorübergehend nicht anwenden möchten, können Sie sie im Modul **Sicherheitseinstellungen** > **Compliance Filter** deaktivieren.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus.

3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.
5. Wählen Sie aus der Liste der Filterregeln für eingehende oder ausgehende E-Mails die gewünschte Regel aus und deaktivieren Sie die Checkbox in der Spalte **Aktiv**.

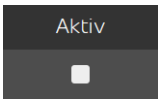

Abbildung 28: Filterregel deaktivieren

Die Filterregel wird deaktiviert. Die Filterregel wird nicht mehr auf den E-Mail-Verkehr der Domain angewendet.

Eine Filterregel des Compliance Filters ist deaktiviert worden.

Anschließend können Sie die Filterregel wieder aktivieren, sobald Sie wieder angewendet werden soll (siehe Filterregel aktivieren auf Seite 49).

Filterregel des Compliance Filters löschen

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11) und Filterregeln für den Compliance Filter erstellt (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 oder Filterregel für ausgehende E-Mails erstellen auf Seite 19).

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie Filterregeln des Compliance Filters löschen, die Sie nicht mehr benötigen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie eine Filterregel löschen möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Regeln** aus.

5. Klicken Sie in der Liste der Regeln für eingehende oder ausgehende E-Mails auf den Menüpfeil neben der Filterregel, die Sie löschen möchten.

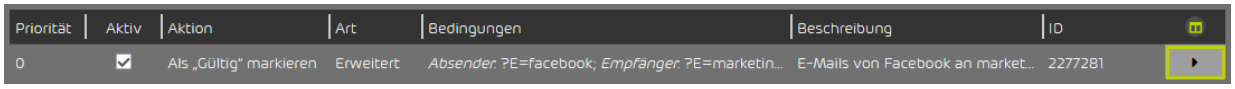

Abbildung 29: Menü öffnen

- Ein Menü öffnet sich.

6. Klicken Sie auf **Löschen**.

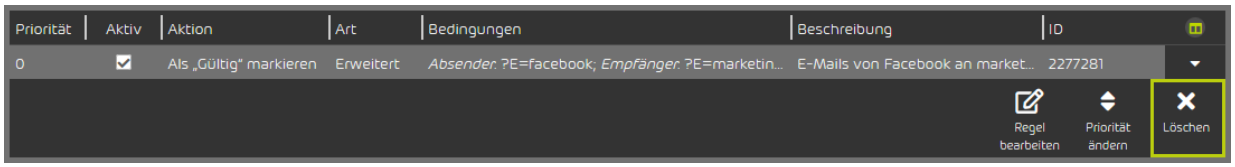

Abbildung 30: Filterregel löschen

- Eine Warnmeldung wird angezeigt.

7. Klicken Sie auf **Bestätigen**.

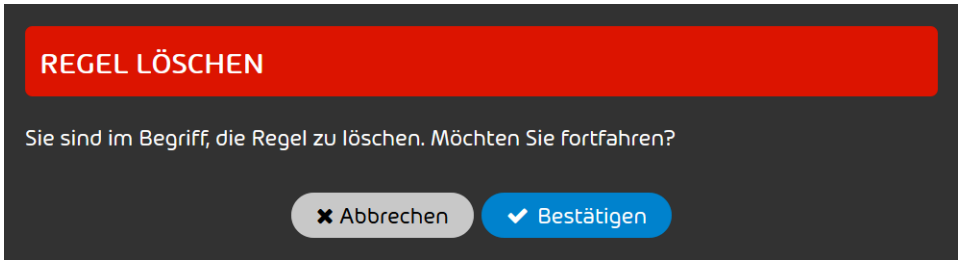

Abbildung 31: Löschung bestätigen

- Die Filterregel wird gelöscht.

Eine Filterregel des Compliance Filters ist gelöscht worden.

Verzeichnisse

Verzeichnisse sind Sammlungen von Ausdrücken, die für die Erstellung von Filterregeln im Modul **Sicherheitseinstellungen** > **Compliance Filter** (siehe Über den Compliance Filter auf Seite 6) verwendet werden können. Die Ausdrücke eines Verzeichnisses können entweder alle als literale Ausdrücke oder als reguläre Ausdrücke gedeutet werden. Dabei bieten reguläre Ausdrücke eine höhere Treffgenauigkeit und reduzieren die Anzahl der Einträge, die erstellt und gepflegt werden müssen.

Hinweis:

Für eine Hauptdomain können bis zu 250 Verzeichnisse erstellt werden.

Verzeichnisse mit regulären Ausdrücken können bis zu 1000 Einträge enthalten, wohingegen Verzeichnisse mit literalen Ausdrücken bis zu 15000 Einträge enthalten können.

Bei der Erstellung von Filterregeln der Art **Erweitert** (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 oder Filterregel für ausgehende E-Mails erstellen auf Seite 19) können Administratoren auf Kundenebene bei einigen Bedingungen ein Verzeichnis referenzieren, statt einen einzelnen Ausdruck einzugeben. Um ein bestehendes Verzeichnis zu referenzieren, müssen Administratoren den Namen des Verzeichnisses in das Eingabefeld der Bedingung eingeben und in einem Drop-down-Menü auswählen, wie die Ausdrücke aus dem Verzeichnis von der Filterregel gedeutet werden sollen. Mit der Option **Im Verzeichnis enthalten** trifft die Filterregel zu, falls mindestens ein Ausdruck aus dem Verzeichnis mit einer E-Mail übereinstimmt. Die Ausdrücke des Verzeichnisses werden also innerhalb der Bedingung logisch mit einem ODER miteinander verknüpft. Mit der Option **Nicht im Verzeichnis enthalten** trifft die Filterregel zu, falls für keinen Ausdruck eine Übereinstimmung gefunden wird.

Verzeichnisse vereinfachen die Erstellung von Filterregeln des Compliance Filters, da eine einzige Filterregel auf E-Mails zutreffen kann, die unterschiedliche Werte für eine Bedingung aufweisen. So können beispielsweise durch eine einzige Filterregel E-Mails von den Absendern **@facebook**, **@instagram** oder **@tiktok** an E-Mail-Adressen aus der Marketing-Abteilung als gültig markiert werden, indem ein Verzeichnis mit den drei Begriffen erstellt und in der Bedingung **Absender** referenziert wird (siehe Arten von Filterregeln auf Seite 31). Um das gleiche Verhalten des Compliance Filters ohne eine Referenz auf ein Verzeichnis zu erzielen, wären entweder drei

verschiedene Filterregeln mit jeweils einem literalen Ausdruck für einen Absender oder eine einzelne Filterregel mit einem regulären Ausdruck mit ODER-Verknüpfungen zwischen den verschiedenen Absendern erforderlich. Letzteres könnte bei einer großen Anzahl hinterlegter Absender unübersichtlich werden.

Ein anderer Anwendungsfall ist es, alle eingehenden E-Mails abzuweisen, die Schimpfwörter enthalten. Dazu könnte ein Administrator auf Kundenebene ein Verzeichnis mit Schimpfwörtern erstellen und dieses in einer Filterregel für eingehende E-Mails referenzieren. Stattdessen einzelne Filterregeln für jedes Schimpfwort zu erstellen und zu pflegen, wäre dagegen deutlich aufwendiger.

Administratoren auf Kundenebene können Verzeichnisse erstellen (siehe Verzeichnis erstellen auf Seite 54), bestehende Verzeichnisse bearbeiten (siehe Verzeichnis bearbeiten auf Seite 57) und löschen (siehe Verzeichnis löschen auf Seite 59).

Verzeichnis erstellen

Sie haben den Compliance Filter für die ausgewählte Domain aktiviert (siehe Compliance Filter aktivieren auf Seite 11).

Im Modul **Compliance Filter** > **Verzeichnisse** können Sie Verzeichnisse (siehe Verzeichnisse auf Seite 53) für den Compliance Filter erstellen. Mit Verzeichnissen können Sie mit wenig Aufwand komplexe Filterregeln erstellen (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 und Filterregel für ausgehende E-Mails erstellen auf Seite 19).

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie ein Verzeichnis erstellen möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Verzeichnisse** aus.

5. Klicken Sie auf **Hinzufügen**.

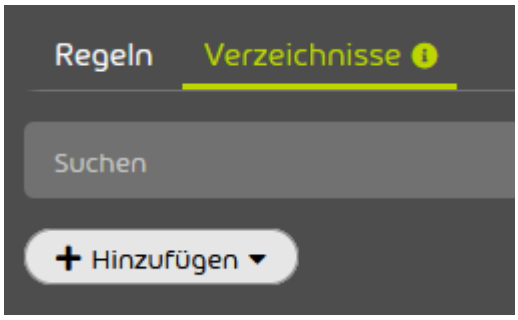

Abbildung 32: Verzeichnis hinzufügen

Ein Formular zur Erstellung eines Verzeichnisses wird angezeigt.

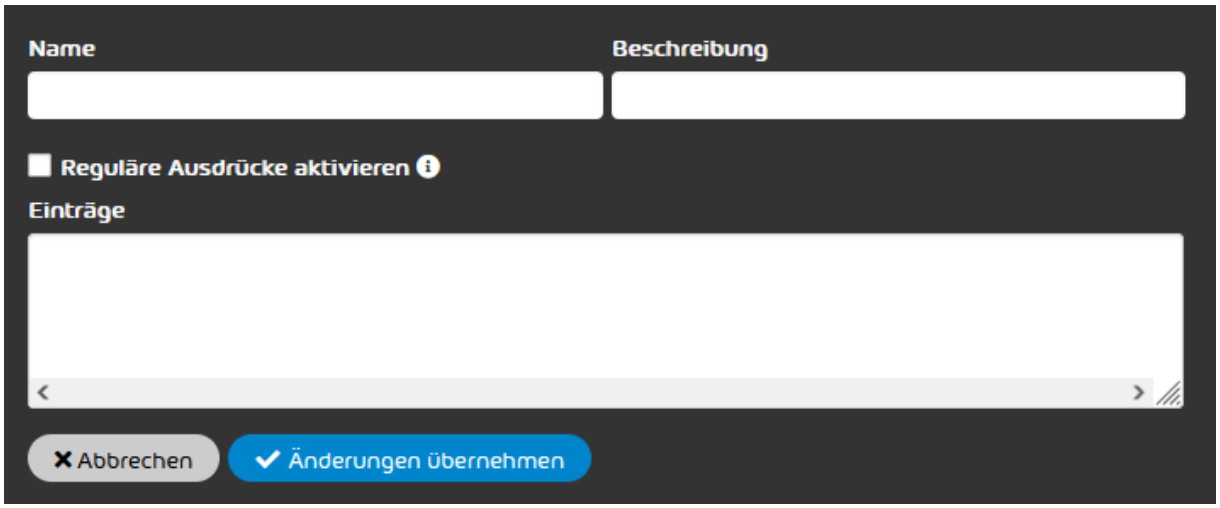

Abbildung 33: Formular für ein Verzeichnis

6. Geben Sie in das Feld **Name** einen Namen für das Verzeichnis ein.

> **Hinweis:**
>
> Der Name darf die folgenden Zeichen enthalten:
>
> - lateinische Kleinbuchstaben von a-z
> - Ziffern von 0-9
> - Sonderzeichen **- _ . , =**
>
> Leerzeichen und Doppelpunkte sind nicht erlaubt.

7. Optional: Geben Sie in das Feld **Beschreibung** eine Beschreibung des Verzeichnisses ein.
8. Optional: Falls die Einträge des Verzeichnisses als reguläre Ausdrücke interpretiert werden sollen, setzen Sie ein Häkchen in der Checkbox **Reguläre Ausdrücke aktivieren**.

> **Hinweis:**
>
> Falls diese Option ausgewählt wird, müssen bei allen Einträgen des Verzeichnisses die Regeln der regulären Ausdrücke (siehe Erklärung der regulären Ausdrücke auf Seite 62) sowie deren Ausnahmen (siehe Ausnahmen bei regulären Ausdrücken auf Seite 70) beachtet werden.

9. Geben Sie in das Feld **Einträge** die gewünschten Ausdrücke ein.

> **Hinweis:**
>
> Jede Zeile entspricht einem Eintrag. Die maximale Zeilenlänge beträgt 1000 Zeichen. Die Anzahl der Einträge ist für literale Ausdrücke auf 15000 und für reguläre Ausdrücke auf 1000 begrenzt. Leerzeilen und doppelte Einträge werden ignoriert und beim Speichern des Verzeichnisses entfernt.

10. Klicken Sie auf **Änderungen übernehmen**.

Falls ein Häkchen in der Checkbox **Reguläre Ausdrücke aktivieren** gesetzt worden ist, werden die regulären Ausdrücke auf Korrektheit geprüft.

Das Formular wird geschlossen, das Verzeichnis wird gespeichert und zu der Tabelle der Verzeichnisse hinzugefügt.

Ein Verzeichnis ist erstellt worden.

Anschließend können Sie das Verzeichnis bearbeiten (siehe Verzeichnis bearbeiten auf Seite 57) oder löschen (siehe Verzeichnis löschen auf Seite 59). Sie können das Verzeichnis in Filterregeln des Compliance Filters referenzieren (siehe Filterregel für eingehende E-Mails erstellen auf Seite 13 und Filterregel für ausgehende E-Mails erstellen auf Seite 19).

Verzeichnis bearbeiten

Sie haben ein Verzeichnis erstellt (siehe Verzeichnis erstellen auf Seite 54).

Im Modul **Sicherheitseinstellungen** > **Compliance Filter** können Sie bestehende Verzeichnisse (siehe Verzeichnisse auf Seite 53) des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) bearbeiten.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie ein Verzeichnis bearbeiten möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Verzeichnisse** aus.
5. Klicken Sie in der Liste der Verzeichnisse auf den Menüpfeil neben dem Verzeichnis, das Sie bearbeiten möchten.

Abbildung 34: Menü öffnen

6. Klicken Sie auf **Bearbeiten**.

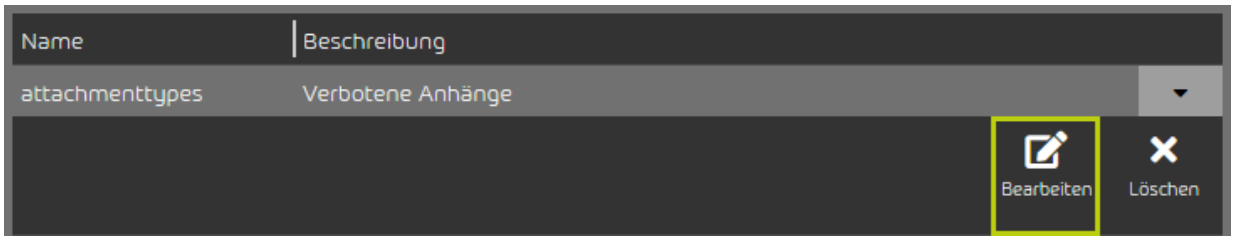

Abbildung 35: Verzeichnis bearbeiten

Ein Formular mit den aktuellen Einstellungen des Verzeichnisses öffnet sich.

7. Ändern Sie die Einstellungen nach Ihren Wünschen.

> **Hinweis:**
>
> Für weitere Informationen siehe Verzeichnis erstellen auf Seite 54.

8. Klicken Sie auf **Änderungen übernehmen**.

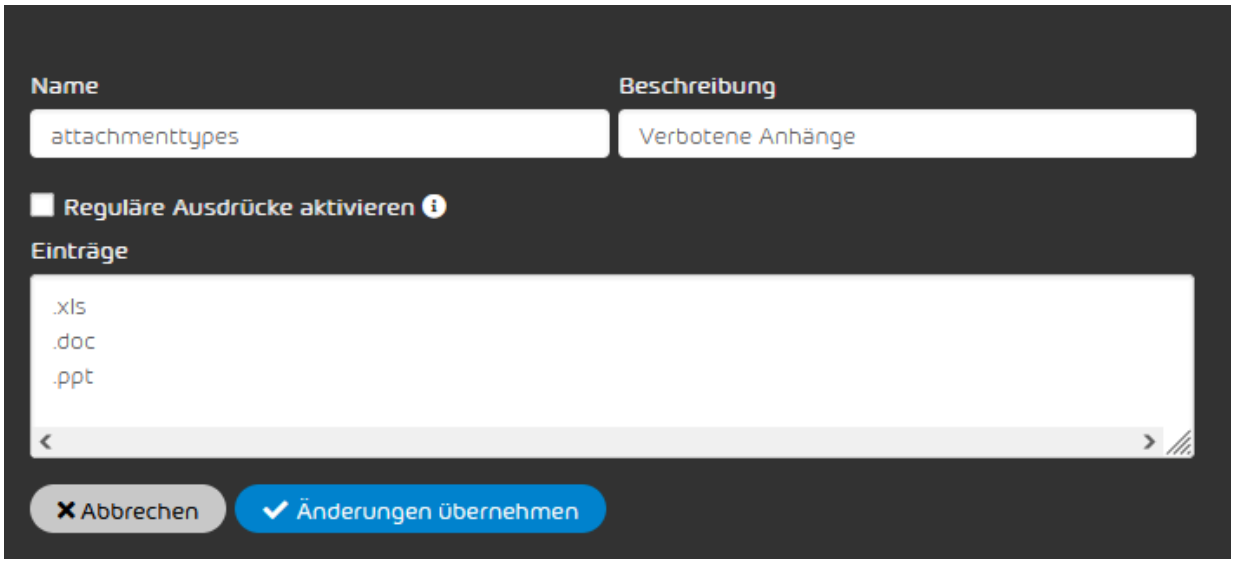

Abbildung 36: Änderungen übernehmen

Die Änderungen werden übernommen.

Hinweis:

Falls der Name des Verzeichnisses geändert worden ist und das Verzeichnis bereits in Filterregeln referenziert wird, wird in diesen Filterregeln auch der Name des Verzeichnisses aktualisiert.

Ein Verzeichnis ist bearbeitet worden.

Verzeichnis löschen

Sie haben ein Verzeichnis erstellt (siehe Verzeichnis erstellen auf Seite 54). Das Verzeichnis wird in keiner Filterregel des Compliance Filters referenziert.

Falls Sie ein bestehendes Verzeichnis (siehe Verzeichnisse auf Seite 53) des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) nicht mehr benötigen, können Sie es im Modul **Sicherheitseinstellungen** > **Compliance Filter** löschen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie ein Verzeichnis löschen möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Wählen Sie den Tab **Verzeichnisse** aus.
5. Klicken Sie in der Liste der Verzeichnisse auf den Menüpfeil neben dem Verzeichnis, das Sie löschen möchten.

Abbildung 37: Menü öffnen

Ein Menü öffnet sich.

6. Klicken Sie auf **Löschen**.

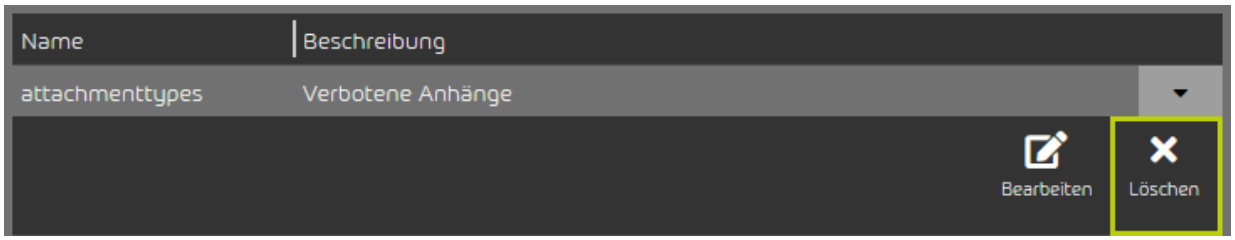

Abbildung 38: Verzeichnis löschen

Eine Warnmeldung wird angezeigt.

7. Klicken Sie auf **Bestätigen**.

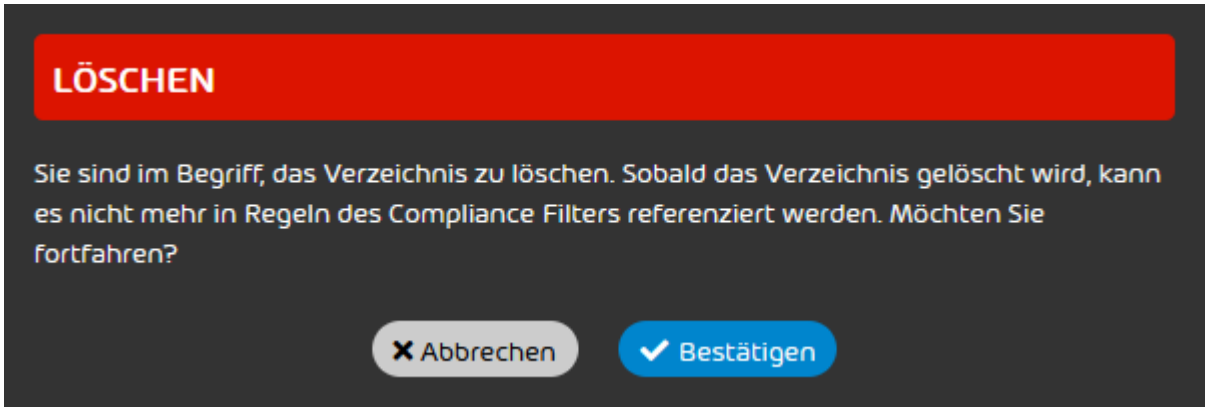

Abbildung 39: Löschung bestätigen

Es wird geprüft, ob das Verzeichnis in Filterregeln des Compliance Filters referenziert wird. Falls es nicht referenziert wird, wird das Verzeichnis gelöscht.

Ein Verzeichnis ist gelöscht worden.

Reguläre Ausdrücke

In den Filterregeln des Compliance Filters (siehe Filterregeln auf Seite 12) können reguläre Ausdrücke (kurz RegEx) verwendet werden, um Informationen aus einer Zeichenkette zu extrahieren. Auf diese Weise ist es möglich, Muster in Betreffzeilen oder anderen E-Mail-Komponenten zu erkennen und E-Mails zu filtern.

Hinweis:

Das System setzt automatisch die Sequenz **.*** an den Beginn und an das Ende der regulären Ausdrücke im Modul **Compliance Filter**, außer der reguläre Ausdruck fängt mit **^** an oder endet auf **$**.

Hinweis:

Die Quantifizierer **+** und ***** (siehe die Tabelle Syntaxelemente und Sonderzeichen im Kapitel Erklärung der regulären Ausdrücke auf Seite 62) werden durch ein nachgestelltes Fragezeichen automatisch träge gemacht, bevor die regulären Ausdrücke evaluiert werden.

"Träge" ist das Gegenteil von "gierig" und bedeutet, dass die Suche mit der kürzestmöglichen Übereinstimmung endet. Zum Beispiel würde der gierige reguläre Ausdruck **a.*b** in der Zeichenkette **aabcaabcdf** die Übereinstimmung **aabcaab** finden. Dagegen würde der träge Ausdruck **a.*?b** in derselben Zeichenkette zweimal die Übereinstimmung **aab** finden.

WICHTIG:

Im Modul **Compliance Filter** können reguläre Ausdrücke nur in Filterregeln des Typs **Erweitert** (siehe Arten von Filterregeln auf Seite 31) und in Verzeichnissen (siehe Verzeichnisse auf Seite 53) verwendet werden.

Für eine Erklärung der regulären Ausdrücke sowie für Beispiele von regulären Ausdrücken siehe Erklärung der regulären Ausdrücke auf Seite 62 und Beispiele für komplexe reguläre Ausdrücke auf Seite 73.

Im Compliance Filter können reguläre Ausdrücke nach Perl Compatible Regular Expressions gebildet werden. Andere Bibliotheken werden nicht unterstützt. Weitere Informationen finden Sie unter: http://www.pcre.org/. Zudem gibt es besondere Einschränkungen, die unter Ausnahmen bei regulären Ausdrücken auf Seite 70 erklärt werden.

Beispiel: Verwendung von regulären Ausdrücken im Compliance Filter

Benutzer bekamen häufig E-Mails, bei denen der Betreff das Wort „porn" enthielt. Eine Filterregel wurde definiert, um diese als Spam zu markieren. In letzter Zeit wurde aber ein vermehrtes Aufkommen von E-Mails beobachtet, in denen Leetspeak benutzt wird, um diesen Filter zu umgehen. Es gehen zum Beispiel E-Mails mit dem Betreff „p0rn" ein, die der Compliance Filter nicht markiert. In diesem Fall ist die Nutzung eines regulären Ausdrucks zielführender:

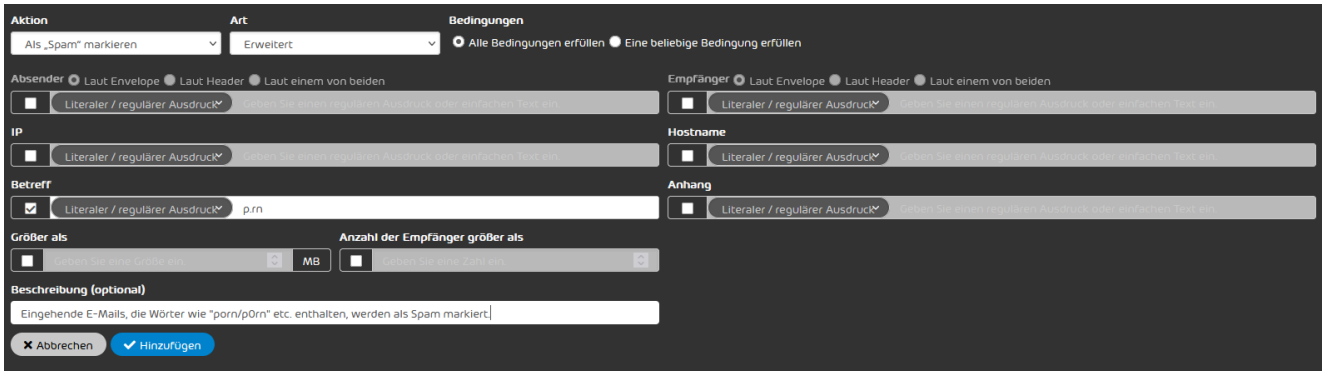

Abbildung 40: Verwendung eines regulären Ausdrucks im Compliance Filter

Anstelle des Punktes wird jedes Zeichen als gültig interpretiert. Der Filter ist an dieser Stelle nicht mehr nur auf das „o" festgelegt, sondern reagiert auch auf alle Buchstaben, Zahlen und Sonderzeichen.

Erklärung der regulären Ausdrücke

In den nachfolgenden Beispielen für reguläre Ausdrücke werden in der rechten Spalte reguläre Ausdrücke gebildet, die auf Texte in der linken Spalte angewendet werden. Die Markierung gibt den Teil des Textes an, der von dem regulären Ausdruck erfasst wurde.

Einzelne Zeichen

Tabelle 5: Buchstaben erfassen

TEXT	REGEX
abcdef	**abc**
abcde	
Abcd	

Mit Buchstaben kann überall innerhalb des Textes nach entsprechenden Treffern gesucht werden.

Tabelle 6: Zeichen aus Zeichenauswahl erfassen

TEXT	REGEX
ac**bde**f	**[abc]de**
adefg	

Mit einer Zeichenauswahl wird nach jeweils einem der Zeichen gesucht, die durch eckige Klammern zu einer Auswahl zusammengefasst sind.

Tabelle 7: Zeichen aus Zeichenbereichen erfassen

TEXT	REGEX
1 Wort	**[1-5] [A-Z]**
7 Wörter	
2 verschiedene Wörter	

Mit eckigen Klammern können auch Zeichenbereiche angegeben werden. Das erste und letzte Zeichen des Bereichs werden durch einen Bindestrich voneinander getrennt. Die Reihenfolge der Zeichen entspricht der Reihenfolge in der ASCII-Tabelle. Großbuchstaben kommen also vor Kleinbuchstaben. Der reguläre Ausdruck **[A-z]** findet daher alle ASCII-Zeichen vom Großbuchstaben A bis hin zum Kleinbuchstaben z. Der reguläre Ausdruck **[a-Z]** ist hingegen ungültig und findet keine Treffer.

WICHTIG:

Der Zeichenbereich **[A-z]** enthält nur lateinische Buchstaben. Die folgenden Zeichen sind nicht im Zeichenbereich enthalten:

- Umlaute (äöü)
- Buchstaben mit Akzenten (zum Beispiel áéíóú)
- sprachspezifische Buchstaben (zum Beispiel ñ oder ß)

Tabelle 8: Zahlen erfassen

TEXT	REGEX
number - **123**	**123** oder **\d\d\d**
var number - **123**	
ab**123**fg	

Zahlen erzielen die gleiche Wirkung wie Buchstaben. Anstatt einer expliziten Zahl kann die Zeichenklasse **\d** verwendet werden, um bei jeder beliebigen Zahl einen Treffer zu erzielen.

Tabelle 9: Buchstaben erfassen

TEXT	REGEX
a12**b**34**c**	\w

Der Ausdruck **\w** sucht nach beliebigen lateinischen Buchstaben von A bis z (siehe oben) ohne Sonderzeichen oder sprachspezifische Buchstaben.

Tabelle 10: Jegliche Zeichen erfassen

TEXT	REGEX
bob.	···\.
tom.	
?!a.	
abc1	

Der einfache „.“ drückt aus, dass jedes Zeichen einen Treffer erzeugt. Um das Vorkommen eines Punktes zu prüfen, muss der Punkt mit „\.“ maskiert werden.

Tabelle 11: Zeichen mehrmals erfassen

TEXT	REGEX
abcc	ab*c
a**abbbbbc**c	
bb**ac**cc	

Wiederholungen

Das nachgestellte Sternzeichen bedeutet, dass das vorangestellte Zeichen beliebig oft vorkommen darf. Das Zeichen kann also gar nicht, einmal oder mehrfach vorkommen.

Tabelle 12: Zeichen mindestens einmal erfassen

TEXT	REGEX
aaaaaaaaa**abc**	**ab+c**
a**abbbc**	
ac	

Das nachgestellte Plus-Zeichen bedeutet, dass das Zeichen mindestens einmal vorkommen muss und mehrfach vorkommen darf. Kommt es nicht vor, wird kein Treffer erzielt.

Tabelle 13: Anzahl der Wiederholungen von Zeichen bestimmen

TEXT	REGEX
12 **123 4544 1564**14	**\d{3,4}**

In geschweiften Klammern kann eine feste Zahl oder ein Intervall für die Anzahl von Wiederholungen des vorangestellten Zeichens angegeben werden. Im obigen Beispiel wird nach Zeichenketten gesucht, die nur aus Ziffern bestehen und 3 bis 4 Zeichen lang sind. Die folgenden Kombinationen sind möglich:

- {m}: Das vorangestellte Zeichen muss genau m Mal vorkommen.
- {m,}: Das vorangestellte Zeichen muss mindestens m Mal vorkommen.
- {m,n}: Das vorangestellte Zeichen muss mindestens m Mal und höchstens n Mal vorkommen.

Tabelle 14: Optionale Zeichen

TEXT	REGEX
3 users online	\d+ users? online
150 users online	
20 users online	
1 user online	
no user online	

Ein nachgestelltes "?" markiert das voranstehende Zeichen als optional.

Gruppen

Tabelle 15: Regulären Ausdruck in Gruppen aufteilen

TEXT	REGEX
dump025.csv	\w+\d+\.(\w+)
dump026.csv	

Runde Klammern um einen Teil des regulären Ausdrucks lösen Gruppen aus. Im obigen Beispiel wird die Dateiendung nach dem Punkt als Gruppe erfasst. Gruppen werden von verschiedenen Operatoren als Einzelzeichen behandelt. Nachgestellte Quantoren wie ?, *, + oder geschweifte Klammern wirken sich daher auf die Gruppe als Ganzes statt nur auf das letzte Zeichen aus.

Zum Beispiel wäre die ganze Gruppe **(abc)?** optional. Darüber hinaus ermöglichen Gruppen fortgeschrittene Operationen wie die Rückwärtsreferenz (siehe unten). Ein weiterer Vorteil ist, dass Gruppen die Übersichtlichkeit erhöhen.

Tabelle 16: Entweder-oder-Auswahl

TEXT	REGEX
data.csv	**.*\.(exe|xlsx)**
bild.jpg	
moving.gif	
document.pdf	
virus.exe	
locky.xlsx	

Mit einem senkrechten Strich | innerhalb von runden Klammern werden Zeichenketten voneinander getrennt, nach denen jeweils alternativ gesucht werden soll.

Tabelle 17: Rückwärtsreferenz

TEXT	REGEX
From: "local@domain.de" <local@domain.de>	**From: "(.*@.*\.de)" <\1>**
From: "local@domain.de" <hacker@hackeddomain.de>	

Die Rückwärtsreferenz \1 nimmt die Gruppendefinition (.*@.*\.de) auf. Es wird nur ein Treffer erzeugt, falls der Treffer der Gruppe an der referenzierten Stelle erneut auftritt.

Syntaxelemente und Sonderzeichen

Folgende Syntaxelemente sind für die Konstruktion von regulären Ausdrücken im Compliance Filter zulässig:

Tabelle 18: Syntaxelemente

WILDCARD/ZEICHENKLASSE	FUNKTION
abc…	Buchstaben
123…	Zahlen
[abc]	Eins der Zeichen a, b oder c
[a-z]	Eins der ASCII-Zeichen im angegebenen Bereich
\d	Jede Zahl
.	Jedes Zeichen
\. \/ \ *	Maskierung der fett markierten Zeichen
\w	Jedes alphanumerische Zeichen
*	0 oder mehr Wiederholungen des vorangestellten Ausdrucks
+	1 oder mehr Wiederholungen des vorangestellten Ausdrucks
?	Der vorangestellte Ausdruck ist optional
{m}	Genau m Wiederholungen des vorangestellten Ausdrucks
{m,}	Mindestens m Wiederholungen des vorangestellten Ausdrucks

WILDCARD/ZEICHENKLASSE	FUNKTION
{m, n}	m bis n Wiederholungen des vorangestellten Ausdrucks
\s	Jedes Leerzeichen
(…)	Extraktionsgruppe
(.*)	Alles
(abc|def)	abc oder def
^	Anfang der Zeichenkette
$	Ende der Zeichenkette

Die Sonderzeichen aus der obigen Tabelle werden standardmäßig als Teil eines regulären Ausdrucks interpretiert. Es ist jedoch auch möglich, buchstäblich nach diesen Sonderzeichen zu suchen. Dazu müssen die Funktionen dieser Sonderzeichen mit einem vorangestellten umgekehrten Schrägstrich **** umgangen werden. Beispielsweise findet der Ausdruck **a*** nicht beliebig viele As, sondern die buchstäbliche Zeichenkette **a***.

Ausnahmen bei regulären Ausdrücken

Die Erstellung von regulären Ausdrücken für Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6 und Filterregeln auf Seite 12) unterscheidet sich von der PCRE-konformer Ausdrücke, da im Compliance Filter nicht alle Syntaxelemente verwendet werden können. Grundsätzlich sind Zeichen aus der erweiterten ASCII-Tabelle gestattet. Bei der Prüfung regulärer Ausdrücke wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Für Ausdrücke, die direkt in die Eingabefelder von Filterregeln im Modul **Compliance Filter** eingegeben werden, und Ausdrücke in Verzeichnissen (siehe Verzeichnisse auf Seite 53) gelten unterschiedliche Einschränkungen.

Die folgenden Zeichen können **nicht** in den Eingabefeldern von Filterregeln im Modul **Compliance Filter** verwendet werden, deren Werte als reguläre Ausdrücke interpretiert werden:

- Semikolon ;
- Gradzeichen ˚
- Sternchen * am Anfang eines Eintrags
- Schrägstrich / (außer wenn er mit \ maskiert wird)

Die folgenden Zeichen können **nicht** in Verzeichnissen des Moduls **Compliance Filter** verwendet werden, deren Einträge als reguläre Ausdrücke interpretiert werden:

- Gradzeichen ˚
- Schrägstrich / (außer wenn er mit \ maskiert wird)

Hinweis:

Der senkrechte Strich | (Pipe) ist sowohl in Eingabefeldern von Filterregeln als auch in Verzeichnissen nur innerhalb einer Gruppe erlaubt, die von runden Klammern umgeben ist. Zudem wird der senkrechte Strich | in seiner Funktion als ODER immer einzeln verwendet. Zwei senkrechte Stiche || werden als Wildcard interpretiert und führen dazu, dass alle Zeichen akzeptiert werden.

Häufige Anwendungsfälle von regulären Ausdrücken

Im Folgenden werden beispielhafte reguläre Ausdrücke (siehe Erklärung der regulären Ausdrücke auf Seite 62) für häufige Anwendungsfälle im Compliance Filter (siehe Über den Compliance Filter auf Seite 6) vorgestellt.

Unterschiedliche Hostnamen mit gleicher Endung

Bei der Erstellung von Filterregeln für E-Mails, die von den oder an die E-Mail-Server verschiedener Subdomains einer bestimmten Domain versendet werden, kann mit der Bedingung **Hostname** im Modul **Sicherheitseinstellungen** > **Compliance Filter** nach Zeichenketten gesucht werden, die auf eine bestimmte Weise enden.

Für diese Suche kann der folgende reguläre Ausdruck verwendet werden:

Zeichenkette$

Das Dollarzeichen bedeutet, dass die gesuchte Zeichenkette am Ende des untersuchten Hostnamens gefunden werden muss. Zum Beispiel würde der Ausdruck **.*domain\.tld$** E-Mails von oder an den E-Mail-Server der Domain **domain.tld** und all ihrer Subdomains (z. B. **marketing.domain.tld**, **sales.domain.tld**, **accounting.domain.tld**) finden.

Nummerierte Hostnamen von E-Mail-Servern

Häufig unterscheiden sich die verschiedenen E-Mail-Server einer Domain nur in ihrer Nummerierung. Um E-Mails an oder von diesen E-Mail-Servern durch Filterregeln des Compliance Filters zu verarbeiten, kann mit der Bedingung **Hostname** nach Zeichenketten gesucht werden, die sich nur in der Nummerierung unterscheiden.

Für diese Suche kann der folgende reguläre Ausdruck verwendet werden:

(Zeichenkette vor Nummerierung)\d+(Zeichenkette nach Nummerierung)

> **Hinweis:**
>
> Die Klammern in diesem Ausdruck sind optional und wurden für eine bessere Übersichtlichkeit verwendet.

Die Sequenz **\d+** steht für "mindestens eine Ziffer". Zum Beispiel würde der reguläre Ausdruck **mx\d+\.domain\.tld** E-Mails von oder an die folgenden E-Mail-Server finden: **mx3.domain.tld**, **mx30.domain.tld**, **mx100.domain.tld**.

Mehrere konkrete E-Mail-Adressen einer Domain

Damit eine Filterregel auf eine kleine Anzahl von E-Mail-Adressen von einer Domain angewendet wird, kann für die Bedingung **Absender** oder **Empfänger** ein regulärer Ausdruck nach dem folgenden Muster verwendet werden:

(benutzer1|benutzer2|benutzer3)@domain

Das Symbol | trennt verschiedene alternative Zeichenketten voneinander, von denen eine gefunden werden muss. Die alternativen Zeichenketten müssen in Klammern stehen. Zum Beispiel würde der reguläre Ausdruck **(klaus|peter|petra)@domain.com** E-Mails von oder an die folgenden E-Mail-Adressen finden: **klaus@domain.com**, **peter@domain.com**, **petra@domain.com**.

Beispiele für komplexe reguläre Ausdrücke

Abschließend betrachten wir die Anwendung von komplexen regulären Ausdrücken (siehe Erklärung der regulären Ausdrücke auf Seite 62) innerhalb von Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6).

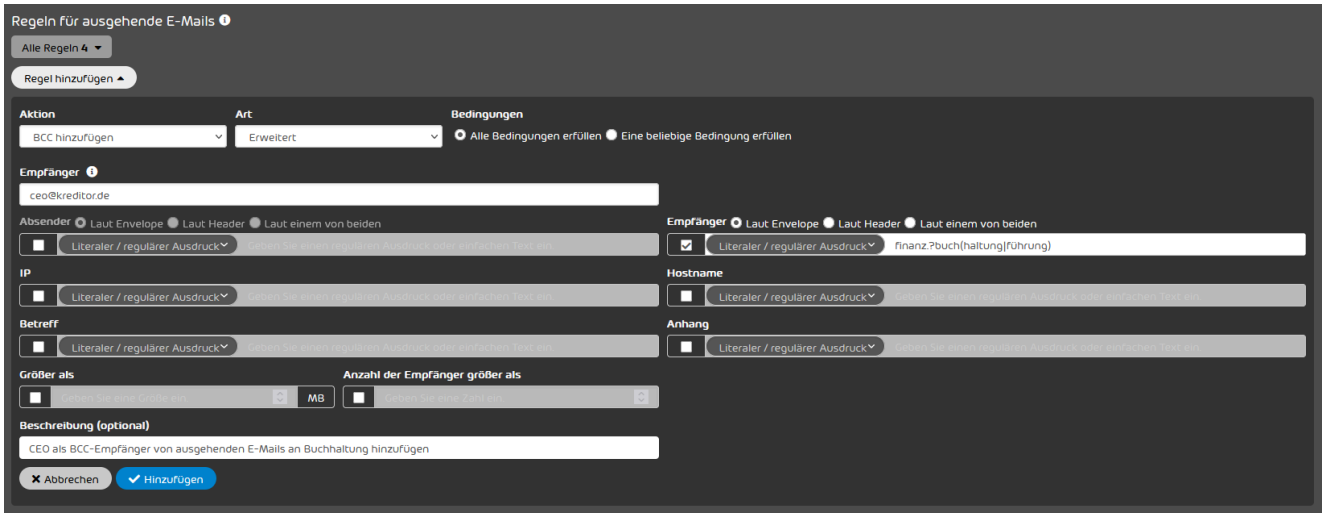

Abbildung 41: Suche nach Empfängern

In diesem ersten Beispiel möchte ein Kunde, dass sein Geschäftsführer eine Blindkopie von ausgehenden E-Mails erhält, die an die Buchhaltung der Kunden des Unternehmens gesendet werden. Diese E-Mail-Adressen sind nach einem bestimmten Muster aufgebaut. Mit dem regulären Ausdruck **finanz.?buch(haltung|führung)** können die folgenden Textsegmente und viele weitere Kombinationen erfasst werden:

- **finanzbuchhaltung@test.de**
- **finanz_buchhaltung@test.de**

- **finanzbuchführung@test.de**
- **finanzbuchführung@einanderertest.de**

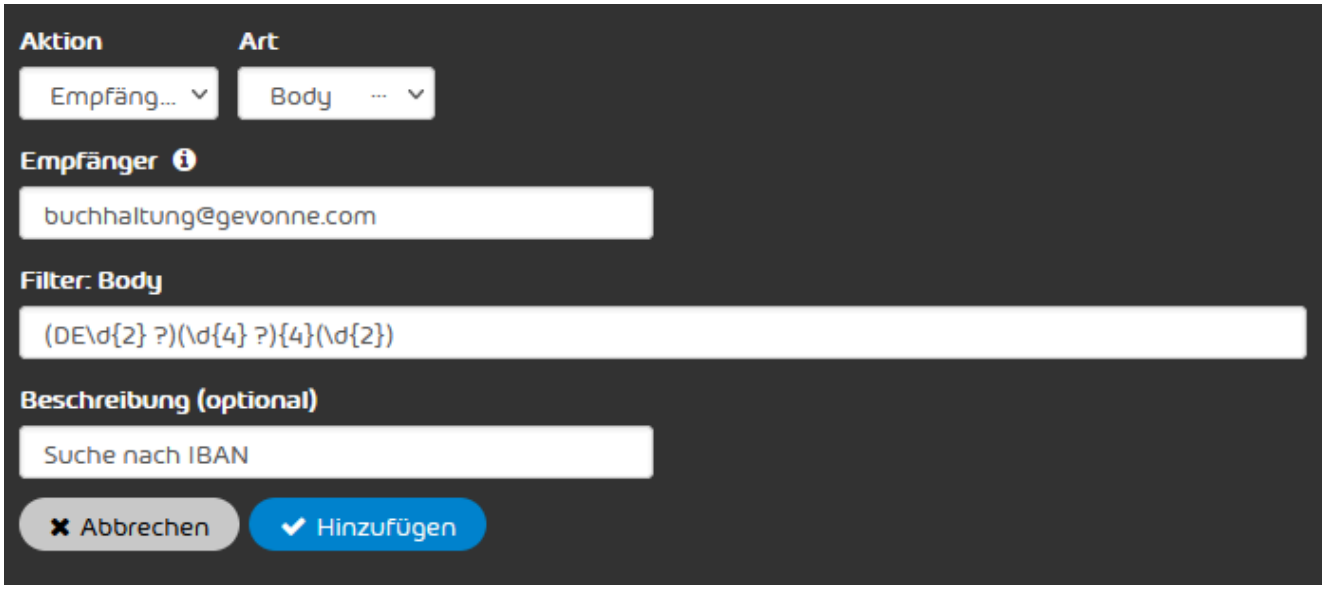

Abbildung 42: Suche nach IBAN im E-Mail-Body

In diesem Beispiel möchte ein Kunde alle eingehenden E-Mails, die deutsche IBAN-Kontonummern im E-Mail-Body enthalten, an seine Buchhaltung weiterleiten. Mit dem regulären Ausdruck **(DE \d{2} ?)(\d{4} ?){4}(\d{2})** kann nach deutschen IBAN-Kontonummern gesucht werden. Dieser reguläre Ausdruck findet sowohl deutsche IBAN-Kontonummern ohne Leerzeichen als auch deutsche IBAN-Kontonummern, die gemäß der üblichen Schreibweise in 4-Zeichen-Blöcke und einen abschließenden 2-Zeichen-Block unterteilt sind:

- **DE12345678901234567890**
- **DE12 3456 7890 1234 5678 90**

Compliance Filter deaktivieren

Falls Sie die Filterregeln des Compliance Filters (siehe Über den Compliance Filter auf Seite 6) nicht mehr verwenden möchten, können Sie den Compliance Filter im Modul **Sicherheitseinstellungen** > **Compliance Filter** deaktivieren. Dabei werden alle erstellten Regeln gelöscht.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie in der Bereichsauswahl die Domain aus, für die Sie den Compliance Filter deaktivieren möchten.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Compliance Filter**.
4. Betätigen Sie den Schalter **Compliance Filter aktivieren**.

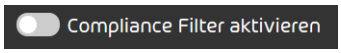

Abbildung 43: Compliance Filter deaktivieren

Ein Bestätigungsfenster öffnet sich.

5. Klicken Sie auf **Bestätigen**.

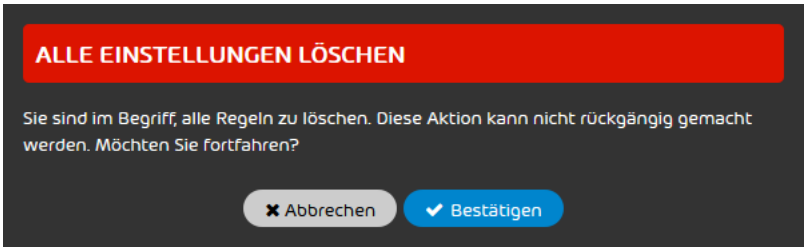

Abbildung 44: Bestätigen

Der Compliance Filter wird deaktiviert. Alle Regeln werden gelöscht. Die Einstellungen im Modul **Compliance Filter** werden gesperrt. Es ist keine weitere Eingabe möglich.

Der Compliance Filter ist deaktiviert worden.

Index

A

Aktionen
    Erklärung 28
aktivieren
    Compliance Filter 11
    Filterregel 49
ändern
    Priorität einer Filterregel 41
Anwendungsfall
    regulärer Ausdruck, *Siehe* regulärer Ausdruck Beispiel
Art
    Felder 31
    Filterregel, *Siehe* Filterregel Art
Ausnahme
    regulärer Ausdruck 70

B

bearbeiten
    Filterregel 39
    Verzeichnis, *Siehe* Verzeichnis bearbeiten
Bedingung
    Filterregel, *Siehe* Filterregel Bedingung
Beispiel
    komplexer regulärer Ausdruck 73
    regulärer Ausdruck, *Siehe* regulärer Ausdruck Beispiel

C

Compliance Filter
    aktivieren 11
    deaktivieren 75
    Erklärung 6

D

deaktivieren
    Compliance Filter 75
    Filterregel 50
Dokumentation
    Hinweise 4
    Symbole 4

E

Erklärung
    Aktionen 28
    regulärer Ausdruck 62
    Sicherheitshinweise 4
    Verzeichnis 53
    Warnhinweise 4
erstellen
    Filterregel für ausgehende E-Mails 19
    Filterregel für eingehende E-Mails 13
    Verzeichnis, *Siehe* Verzeichnis erstellen

F

Felder
    Art, *Siehe* Art Felder
Filterregel
    aktivieren 49
    Art 31
    bearbeiten 39
    Bedingung 31
    deaktivieren 50
    löschen 51
Filterregel für ausgehende E-Mails
    erstellen 19
Filterregel für eingehende E-Mails
    erstellen 13
Filterregeln
    Reihenfolge 43

H

Hinweise
    Dokumentation 4

K

komplexer regulärer Ausdruck
    Beispiel 73

L

löschen
    Filterregel, *Siehe* Filterregel löschen
    Verzeichnis, *Siehe* Verzeichnis löschen

P

Priorität einer Filterregel
    ändern 41

R

Regelreihenfolge innerhalb aller Services 8
regulärer Ausdruck
    Anwendungsfall, *Siehe* regulärer Ausdruck Beispiel
    Ausnahme 70
    Beispiel 71
    Erklärung 62
Reihenfolge
    Filterregeln, *Siehe* Filterregeln Reihenfolge

S

Sicherheitshinweise
    Erklärung 4
Symbole
    Dokumentation 4

V

Verzeichnis
    bearbeiten 57
    Erklärung 53
    erstellen 54
    löschen 59

W

Warnhinweise
    Erklärung 4

U.S. SALES 1.800.734.9905

INTERNATIONAL SALES +1.206.613.0895

www.watchguard.com | pandasecurity.com