IP-Adresse gesperrt – Ursache finden und erneute Sperrung vermeiden

18.08.2026 - Mailadministration

Wenn beim Zugriff auf Fairgate Webmail oder über ein E-Mail-Programm die Meldung erscheint, dass Ihre IP-Adresse blockiert wurde, hat eine automatische Schutzfunktion des Mailservers den Zugriff von Ihrer aktuellen öffentlichen IP-Adresse vorübergehend gesperrt.

Eine solche Sperre wird ausgelöst, wenn von derselben öffentlichen IP-Adresse wiederholt fehlgeschlagene oder auffällige Anmeldeversuche erkannt werden. Das kann beispielsweise passieren, wenn ein Mailprogramm auf einem Computer, Smartphone oder Tablet weiterhin mit einem alten oder falschen Passwort versucht, sich anzumelden.

Die Sperre schützt den Mailserver unter anderem vor automatisierten Anmeldeversuchen und Angriffen. Sie kann jedoch auch durch ein eigenes Gerät oder eine Anwendung ausgelöst werden, auf der nicht mehr gültige Zugangsdaten gespeichert sind.

> **Wichtig:** Das Entsperren der IP-Adresse beseitigt nur die aktuelle Sperre, nicht deren Ursache. Wenn danach weiterhin fehlerhafte Anmeldeversuche erfolgen, kann die IP-Adresse erneut automatisch gesperrt werden.

Dieser Artikel richtet sich bewusst an Anwenderinnen und Anwender ohne technisches Vorwissen und hilft Ihnen, die häufigsten Ursachen systematisch zu prüfen.

Was genau wurde gesperrt?

Bei dieser Art von Sperre ist nicht Ihre einzelne E-Mail-Adresse blockiert, sondern die **öffentliche IP-Adresse Ihres Internetanschlusses**.

In der Sperrmeldung kann beispielsweise folgender Text erscheinen:

```
Blocked
```

```
Your IP address is blocked.
```

Zusätzlich wird in der Regel die betroffene öffentliche IP-Adresse angezeigt.

Mehrere Geräte innerhalb desselben Netzwerks verwenden nach aussen häufig dieselbe öffentliche IP-Adresse. Dazu können beispielsweise gehören:

- Computer und Notebooks
- Smartphones
- Tablets
- Drucker, Scanner oder Kopierer
- Server und NAS-Systeme
- andere Geräte im gleichen WLAN oder Netzwerk

Das bedeutet: Die Sperrmeldung kann auf Ihrem Computer erscheinen, obwohl die fehlerhaften Anmeldeversuche beispielsweise von einem Tablet, einem anderen Computer oder einem technischen Gerät im gleichen Netzwerk verursacht werden.

Warum wird eine IP-Adresse gesperrt?

Die Schutzfunktion reagiert auf wiederholte fehlgeschlagene Anmeldeversuche.

Ein einzelner Benutzer muss diese Anmeldeversuche nicht bewusst ausführen. Viele Mailprogramme und Geräte prüfen E-Mails automatisch im Hintergrund und versuchen bei einer fehlerhaften Konfiguration immer wieder, sich anzumelden.

Typische Ursachen sind:

Mögliche Ursache	Beispiel
Altes Passwort gespeichert	Das Mailpasswort wurde geändert, auf einem Gerät ist aber noch das vorherige Passwort hinterlegt.
Falsches Passwort gespeichert	Beim Einrichten des Kontos wurde ein falsches Passwort gespeichert.
Mehrere Geräte	Das gleiche Postfach ist auf Computer, Smartphone und Tablet eingerichtet.
Gemeinsam verwendetes Postfach	Mehrere Personen verwenden beispielsweise eine Adresse wie `info@`, `vorstand@` oder `marketing@`.
Altes oder vergessenes Gerät	Ein früher verwendetes Smartphone oder Tablet versucht weiterhin E-Mails abzurufen.
Mehrfach eingerichtetes Konto	Das gleiche Konto ist auf einem Gerät oder in einem Mailprogramm mehrfach eingerichtet.
Veraltetes Mailprogramm	Ein älteres Programm verwendet noch alte Zugangsdaten oder eine nicht mehr passende Konfiguration.
Separater Postausgang	Beim Empfang sind die Daten korrekt, beim Mailversand ist aber noch ein falsches Passwort hinterlegt.
Technisches Gerät	Scanner, Kopierer, NAS oder andere Geräte verwenden das Mailkonto für Benachrichtigungen oder den Mailversand.
Server oder Anwendung	Eine Website, Vereinssoftware oder andere Anwendung versendet E-Mails mit den Zugangsdaten des Postfachs.
Zentrales Netzwerkgerät	Eine Firewall, ein Router oder ein anderes System verwendet das Mailkonto beispielsweise für Benachrichtigungen.
Schadsoftware	Ein kompromittiertes Gerät führt ungewollt Anmeldeversuche durch.

Besonders häufig: Das Passwort wurde geändert

Nach einer Passwortänderung wird das neue Passwort nicht automatisch auf allen Geräten übernommen.

Ist das gleiche Mailkonto beispielsweise auf folgenden Geräten eingerichtet:

- Computer
- Notebook
- Smartphone
- Tablet

muss das neue Passwort auf **jedem dieser Geräte** aktualisiert werden.

Bereits ein einziges Gerät, auf dem weiterhin das vorherige Passwort hinterlegt ist, kann im Hintergrund wiederholt fehlgeschlagene Anmeldeversuche erzeugen.

Dasselbe gilt, wenn das Postfach von mehreren Personen verwendet wird. Hat beispielsweise nur eine Person das neue Passwort eingetragen, während auf den Geräten anderer Benutzer weiterhin das alte Passwort

gespeichert ist, können die fehlerhaften Anmeldeversuche weiterlaufen.

> **Wichtig:** Ein erneuter Passwortwechsel allein löst dieses Problem nicht. Nach jeder Passwortänderung müssen die Zugangsdaten auf allen berechtigten Geräten und Anwendungen aktualisiert werden.

Schritt 1: Prüfen Sie alle Geräte, auf denen das Mailkonto eingerichtet sein könnte

Erstellen Sie zuerst eine Übersicht aller Geräte, auf denen die betroffene E-Mail-Adresse aktuell oder früher eingerichtet wurde.

Denken Sie insbesondere an:

- Desktop-Computer
- Notebook
- privates Smartphone
- geschäftliches Smartphone
- Tablet
- iPad
- ältere Smartphones
- ältere Tablets
- ältere Computer oder Notebooks
- Geräte anderer Personen, die das gleiche Postfach verwenden

Berücksichtigen Sie auch Geräte, die nur selten verwendet werden.

Ein älteres Tablet kann beispielsweise wochenlang unbemerkt im Hintergrund versuchen, E-Mails mit einem nicht mehr gültigen Passwort abzurufen.

Schritt 2: Prüfen Sie alle Mailprogramme und Mail-Apps

Auf jedem dieser Geräte können unterschiedliche Programme auf das Mailkonto zugreifen.

Prüfen Sie beispielsweise:

- Microsoft Outlook
- Apple Mail
- Mozilla Thunderbird

- Mail-App auf iPhone oder iPad
- Mail-App auf Android-Geräten
- andere installierte E-Mail-Programme

Prüfen Sie ebenfalls, ob die gleiche E-Mail-Adresse möglicherweise mehrfach eingerichtet wurde.

Es kann beispielsweise vorkommen, dass ein Postfach einmal korrekt und zusätzlich noch mit einer älteren Konfiguration eingerichtet ist. Der Benutzer sieht dann nur das funktionierende Konto, während die zweite Konfiguration im Hintergrund weiterhin fehlerhafte Anmeldeversuche verursacht.

Schritt 3: Mailprogramme und Geräte vorübergehend stoppen

Wenn nicht sofort ersichtlich ist, welches Gerät die Anmeldeversuche verursacht, sollten Sie die möglichen Quellen zunächst stoppen.

Schliessen Sie auf allen Computern und mobilen Geräten die Mailprogramme vollständig.

Bei Smartphones und Tablets reicht es nicht in jedem Fall aus, die Mail-App nur zu verlassen. E-Mail-Konten können auch im Hintergrund automatisch synchronisiert werden.

Falls Sie die Ursache nicht anders eingrenzen können:

1. Schalten Sie die möglichen Geräte vorübergehend aus oder trennen Sie sie vom Netzwerk.
2. Aktivieren Sie anschliessend nur ein Gerät.
3. Prüfen Sie dieses Gerät vollständig.
4. Aktivieren Sie danach das nächste Gerät.

So lässt sich die Ursache wesentlich besser eingrenzen, als wenn alle Geräte gleichzeitig mit dem Mailserver verbunden bleiben.

Schritt 4: Prüfen Sie das gespeicherte Passwort

Kontrollieren Sie bei jedem eingerichteten Mailkonto, ob tatsächlich das aktuelle Passwort verwendet wird.

Achten Sie insbesondere darauf, ob:

- das Passwort kürzlich geändert wurde,
- das Passwort durch einen Administrator zurückgesetzt wurde,
- ein altes Passwort weiterhin gespeichert ist,
- das Konto mehrfach eingerichtet ist,
- das Betriebssystem alte Zugangsdaten gespeichert hat.

Auf einigen Betriebssystemen können Zugangsdaten zusätzlich in einem Schlüsselbund oder einer zentralen Anmeldeverwaltung gespeichert sein.

Wenn Sie nicht sicher sind, ob die Konfiguration korrekt ist, kann es sinnvoller sein, das Mailkonto aus dem betroffenen Mailprogramm zu entfernen und anschliessend neu einzurichten.

> **Wichtig:** Entfernen Sie ein Mailkonto nur aus dem Mailprogramm, wenn Sie über die benötigten aktuellen Zugangsdaten verfügen und das Konto anschliessend wieder einrichten können.

> **Wichtig:** Entfernen oder löschen Sie das Mailkonto nicht, solange nicht sichergestellt ist, dass alle benötigten E-Mails serverseitig vorhanden oder anderweitig gesichert sind.

Schritt 5: Auch den Postausgang prüfen

Ein Mailkonto verwendet Einstellungen für den Empfang und den Versand von E-Mails.

Es kann deshalb vorkommen, dass das Abrufen von E-Mails funktioniert, während beim Versenden weiterhin falsche Zugangsdaten verwendet werden.

Prüfen Sie deshalb nicht nur den Posteingang, sondern auch die Einstellungen für den **Postausgang bzw. SMTP-Versand**.

Insbesondere nach einer Passwortänderung kann in einzelnen Programmen für den Postausgang weiterhin ein altes Passwort gespeichert sein.

Schritt 6: Anmeldung über Fairgate Webmail testen

Ein wichtiger Test ist die direkte Anmeldung über Fairgate Webmail.

Verwenden Sie dafür:

- Ihre vollständige E-Mail-Adresse
- das aktuelle Passwort des Postfachs

Webmail funktioniert, ein Mailprogramm aber nicht

Wenn die Anmeldung über Webmail funktioniert, das Mailkonto in Outlook, Apple Mail oder einem anderen Programm jedoch nicht, spricht dies dafür, dass die Zugangsdaten oder Einstellungen des betreffenden Programms geprüft werden müssen.

Entfernen Sie das Konto bei Bedarf aus dem Programm und richten Sie es neu ein.

> **Wichtig:** Entfernen Sie ein Mailkonto nur aus dem Mailprogramm, wenn Sie über die benötigten aktuellen Zugangsdaten verfügen und das Konto anschliessend wieder einrichten können.

> **Wichtig:** Entfernen oder löschen Sie das Mailkonto nicht, solange nicht sichergestellt ist, dass alle benötigten E-Mails serverseitig vorhanden oder anderweitig gesichert sind.

Webmail zeigt ebenfalls die IP-Sperre

Wenn Webmail weiterhin meldet, dass Ihre IP-Adresse blockiert ist, betrifft die Sperre weiterhin die öffentliche IP-Adresse Ihres aktuellen Internetanschlusses.

Für eine Entsperrung benötigt der Fairgate Support die aktuell betroffene öffentliche IP-Adresse.

Warum funktioniert es über Mobilfunk, aber nicht über WLAN?

Ein Smartphone oder Tablet kann über verschiedene Internetverbindungen auf den Mailserver zugreifen.

Beispielsweise:

- WLAN zu Hause
- WLAN im Büro
- öffentliches WLAN
- Mobilfunk

Diese Verbindungen verwenden normalerweise unterschiedliche öffentliche IP-Adressen.

Deshalb kann folgende Situation entstehen:

- Zugriff über WLAN: blockiert
- Zugriff über Mobilfunk: funktioniert

Das bedeutet nicht automatisch, dass die Ursache behoben wurde. Es bedeutet zunächst nur, dass die verwendete Mobilfunkverbindung nicht von derselben IP-Sperre betroffen ist.

Umgekehrt kann auch eine Mobilfunk-IP betroffen sein.

> **Hinweis:** Ein Wechsel in ein anderes Netzwerk oder ein Neustart des Routers kann die sichtbare Sperre unter Umständen verändern, beseitigt aber nicht die Ursache der fehlgeschlagenen Anmeldeversuche.

Gemeinsam verwendete Mailadressen vollständig prüfen

Funktionsadressen werden in Vereinen und Organisationen häufig von mehreren Personen verwendet, beispielsweise:

- `info@`
- `sekretariat@`
- `vorstand@`
- `marketing@`
- `finanzen@`

In diesem Fall müssen **alle Personen**, die das Postfach verwenden, ihre Geräte und Programme kontrollieren.

Es reicht nicht aus, nur das Gerät der Person zu prüfen, bei der die Sperrmeldung angezeigt wird.

Prüfen Sie gemeinsam:

- Wer verwendet das Postfach?
- Auf welchen Geräten ist es eingerichtet?
- Welche Programme werden verwendet?
- Wurde das Passwort bei allen Personen aktualisiert?
- Gibt es frühere Benutzer, deren Geräte möglicherweise noch eingerichtet sind?

Seltene, aber wichtige Verursacher: Scanner, Fax, Kopierer und andere Geräte

E-Mail-Zugangsdaten werden nicht nur in klassischen Mailprogrammen gespeichert.

Viele technische Geräte können E-Mails versenden, beispielsweise um eingescannte Dokumente, Statusmeldungen oder Warnungen zu verschicken.

Prüfen Sie deshalb auch:

- Scanner
- Faxgeräte
- Kopierer
- Multifunktionsdrucker
- Drucker mit Scan-to-Mail-Funktion
- NAS-Systeme
- Backup-Systeme
- Server
- Telefonanlagen
- Überwachungs- oder Kamerasysteme
- Alarm- oder Zutrittssysteme
- Netzwerküberwachung
- andere Geräte mit E-Mail-Benachrichtigungen

Ein solches Gerät kann über Jahre mit denselben Zugangsdaten konfiguriert sein. Wird das Passwort des Mailkontos geändert, versucht das Gerät möglicherweise weiterhin, das bisherige Passwort zu verwenden.

Besonders Scanner und Multifunktionsgeräte werden dabei leicht übersehen, weil sie nicht als klassisches E-Mail-Gerät wahrgenommen werden.

Websites und andere Anwendungen prüfen

Auch externe Anwendungen können ein Mailkonto für den Versand verwenden, z. B. eine separate Webseite, externe Software oder andere Programme mit SMTP-Mailversand.

Prüfen Sie dort nach einer Passwortänderung ebenfalls die hinterlegten Zugangsdaten.

> **Hinweis:** Fairgate selbst bzw. das Fairgate CMS verursacht solche Anmeldeversuche nicht. Gemeint sind ausschliesslich externe Anwendungen oder Drittanbieter-Systeme, in denen Ihr Fairgate-Mailkonto hinterlegt wurde.

Router, Firewall und zentrale Netzwerkgeräte

Ein normaler Router oder eine Firewall verursacht nicht allein deshalb Mail-Anmeldeversuche, weil der Internetverkehr darüber läuft.

Solche Geräte können jedoch selbst ein Mailkonto verwenden, wenn beispielsweise E-Mail-Benachrichtigungen eingerichtet wurden.

Prüfen Sie deshalb insbesondere bei professionellen oder zentral verwalteten Netzwerken:

- Router mit E-Mail-Benachrichtigungen
- Firewall
- Security-Appliance
- Mail-Gateway
- Monitoring-System
- Netzwerkcontroller
- Server
- NAS
- andere zentrale Netzwerkgeräte

Falls Sie nicht selbst für diese Systeme zuständig sind, wenden Sie sich an Ihre interne IT oder Ihren IT-Dienstleister und lassen Sie prüfen, ob die betroffene E-Mail-Adresse dort für Benachrichtigungen oder den SMTP-Versand hinterlegt ist.

Vereins-, Firmen- und Organisationsnetzwerke

In Vereins- und Organisationsnetzwerken können mehrere Benutzer und Geräte über dieselbe öffentliche IP-Adresse auf das Internet zugreifen.

Das ist beispielsweise möglich in:

- Vereinen

- Verbänden
- gemeinsam genutzten Vereins- oder Geschäftsräumen
- Firmen
- Schulen und Verwaltungen
- zentral verwalteten Netzwerken

Dadurch kann eine Sperre mehrere Personen oder Geräte betreffen. Das Gerät, auf dem die Meldung angezeigt wird, muss nicht zwingend das Gerät sein, das die fehlgeschlagenen Anmeldeversuche verursacht.

In solchen Netzwerken sollte die zuständige IT oder der betreuende IT-Dienstleister prüfen, welche Geräte oder externen Anwendungen das betreffende Mailkonto verwenden.

VPN, Proxy und andere gemeinsame Internetzugänge

Auch VPN-Verbindungen, zentrale Internet-Gateways oder ähnliche Dienste können dazu führen, dass mehrere Geräte nach aussen über dieselbe öffentliche IP-Adresse erscheinen.

Wenn Sie ein VPN verwenden:

1. Prüfen Sie, ob die Sperre nur bei aktivem VPN erscheint.
2. Prüfen Sie trotzdem die eingerichteten Mailkonten und Zugangsdaten.
3. Informieren Sie bei einem zentral verwalteten VPN gegebenenfalls Ihre IT.

Das Ausschalten eines VPN kann den Zugriff über eine andere öffentliche IP-Adresse ermöglichen, behebt aber eine fehlerhafte Mailkonfiguration nicht.

Kann ein altes Mailprogramm die Ursache sein?

Ja. Ein älteres oder nicht mehr gepflegtes Mailprogramm kann weiterhin alte Zugangsdaten gespeichert haben oder wiederholt versuchen, eine nicht mehr funktionierende Konfiguration zu verwenden.

Prüfen Sie deshalb bei älteren Geräten und Programmen insbesondere:

- ob das Programm noch benötigt wird,
- ob das Mailkonto dort noch eingerichtet ist,
- ob das aktuelle Passwort gespeichert ist,
- ob eine aktuelle Programmversion verfügbar ist.

Wenn ein sehr altes Gerät oder Programm nicht mehr benötigt wird, sollte das Mailkonto daraus entfernt werden.

Kann Schadsoftware die Ursache sein?

Schadsoftware ist möglich, aber nicht automatisch die Ursache einer IP-Sperre.

Wenn sich trotz vollständiger Prüfung der bekannten Geräte, Mailprogramme und Anwendungen keine Ursache finden lässt, empfehlen wir zusätzlich einen vollständigen Viren- bzw. Malware-Scan.

Verwenden Sie dafür eine aktuelle Sicherheitssoftware und prüfen Sie insbesondere Computer und Geräte, auf denen das betroffene Mailkonto eingerichtet ist.

Zusätzliche Anzeichen, bei denen eine Sicherheitsprüfung besonders sinnvoll ist, können sein:

- unbekannte oder unerklärliche Aktivitäten
- unerwarteter Mailversand
- Programme oder Prozesse, die Sie nicht kennen
- wiederkehrende Anmeldeprobleme ohne erkennbare lokale Ursache
- Verdacht darauf, dass Zugangsdaten Dritten bekannt geworden sind

Wenn der Verdacht besteht, dass das Passwort kompromittiert wurde, sollte das Passwort geändert werden.

> **Wichtig:** Aktualisieren Sie nach einem Passwortwechsel das neue Passwort auf allen berechtigten Geräten und Anwendungen. Andernfalls können die bisherigen Geräte wiederum fehlgeschlagene Anmeldeversuche verursachen.

Verwenden Sie ein sicheres Passwort, das Sie nicht für andere Dienste wiederverwenden.

Nach der Entsperrung: Geräte nicht sofort alle wieder verbinden

Wenn Ihre IP-Adresse entsperrt wurde und Sie die Ursache noch suchen, aktivieren Sie nicht sofort wieder alle Geräte und Mailprogramme gleichzeitig.

Gehen Sie stattdessen schrittweise vor:

1. Lassen Sie alle nicht benötigten Mailprogramme und Geräte zunächst deaktiviert.
2. Verwenden Sie ein bereits geprüftes Gerät.
3. Testen Sie dort den Zugriff.
4. Aktivieren Sie danach das nächste Gerät.
5. Beobachten Sie, ob das Problem erneut auftritt.
6. Fahren Sie fort, bis alle benötigten Geräte geprüft sind.

Wenn die Sperre unmittelbar nach Aktivierung eines bestimmten Geräts oder Programms erneut auftritt, sollte dessen Mailkonfiguration besonders genau geprüft werden.

Was Fairgate bei einer Sperre sehen kann

Fairgate kann serverseitig unter anderem feststellen, dass von einer bestimmten öffentlichen IP-Adresse fehlgeschlagene Anmeldeversuche auf den Mailserver erfolgen.

Innerhalb eines Heim-, Firmen- oder Vereinsnetzwerks verwenden jedoch häufig mehrere Geräte dieselbe öffentliche IP-Adresse.

Der Mailserver kann deshalb nicht in jedem Fall erkennen, welches konkrete Smartphone, welcher Computer, welcher Scanner oder welches andere Gerät innerhalb Ihres lokalen Netzwerks die Anmeldeversuche verursacht.

Die Prüfung der lokalen Geräte und Anwendungen muss deshalb durch den Benutzer, den Administrator des Vereins bzw. der Organisation oder den zuständigen IT-Dienstleister erfolgen.

Ihre öffentliche IP-Adresse ermitteln

Wenn eine Sperrmeldung angezeigt wird, benötigen wir für die Prüfung die **aktuell betroffene öffentliche IP-Adresse**.

Ihre öffentliche IP-Adresse können Sie beispielsweise auf der Schweizer Seite https://ipy.ch einsehen.

Beachten Sie, dass sich eine öffentliche IP-Adresse ändern kann. Teilen Sie uns deshalb die IP-Adresse mit, die aktuell angezeigt wird, während das Problem besteht.

Welche Informationen benötigt der Fairgate Support?

Wenn die IP-Adresse nach der Prüfung weiterhin blockiert ist, senden Sie uns bitte folgende Angaben:

- betroffene E-Mail-Adresse
- aktuell angezeigte öffentliche IP-Adresse
- Screenshot der Sperrmeldung
- ungefährer Zeitpunkt, zu dem die Sperre aufgetreten ist
- Information, ob die Anmeldung über Webmail möglich ist
- Information, ob die Sperre im WLAN, Mobilfunk oder einem anderen Netzwerk auftritt
- Information, ob ein VPN verwendet wird
- Information, welche Geräte und Mailprogramme bereits geprüft wurden
- Information, ob das Postfach von mehreren Personen verwendet wird
- Information, ob Scanner, Kopierer, NAS, Server oder andere Anwendungen das Postfach verwenden
- Information, ob die Sperre nach einer früheren Entsperrung erneut aufgetreten ist

> **Wichtig:** Senden Sie uns niemals Ihr Mailpasswort. Fairgate benötigt Ihr Passwort nicht, um eine IP-Sperre zu prüfen oder aufzuheben.

Warum hilft eine erneute Entsperrung manchmal nur kurz?

Eine Entsperrung setzt lediglich die bestehende IP-Sperre zurück.

Wenn beispielsweise ein Tablet unmittelbar danach weiterhin automatisch versucht, sich mit einem falschen Passwort anzumelden, entstehen erneut fehlgeschlagene Anmeldeversuche.

Dasselbe kann durch einen Scanner, einen alten Computer, eine Website oder ein anderes System passieren.

Die IP-Adresse kann deshalb nach einer Entsperrung erneut blockiert werden.

> **Wichtig:** Bei wiederholten Sperren muss zuerst das Gerät oder die Anwendung gefunden werden, das bzw. die weiterhin fehlerhafte Anmeldeversuche verursacht. Wiederholtes Entsperren allein löst die zugrunde liegende Ursache nicht.

Zusammenfassung

Eine IP-Sperre ist eine automatische Schutzmassnahme des Fairgate-Mailservers gegen wiederholte fehlgeschlagene Anmeldeversuche.

In vielen Fällen befindet sich die Ursache auf einem Gerät oder in einer Anwendung, auf der weiterhin ein altes oder falsches Passwort gespeichert ist. Dabei muss es sich nicht um den Computer handeln, auf dem die Sperrmeldung angezeigt wird.

Berücksichtigen Sie deshalb nicht nur klassische Mailprogramme, sondern auch Smartphones, Tablets, alte Geräte, gemeinsam verwendete Postfächer, Scanner, Faxgeräte, Kopierer, NAS-Systeme, Server, Websites, Anwendungen sowie gegebenenfalls Router, Firewalls und andere zentrale Systeme mit eingerichteter E-Mail-Funktion.

Das reine Entsperren der öffentlichen IP-Adresse beseitigt die Ursache nicht. Erst wenn die fehlerhaften Anmeldeversuche beendet wurden, lässt sich vermeiden, dass die IP-Adresse erneut automatisch gesperrt wird.