Fehlermeldungen bei der E-Mail-Zustellung und deren Bedeutung

28.05.2026 - Mailversand

Wenn eine E-Mail nicht zugestellt werden kann, sendet der empfangende oder zwischengeschaltete Mailserver in vielen Fällen eine Statusmeldung zurück. Diese Rückmeldung wird häufig als **Bounce**, **Unzustellbarkeitsmeldung** oder **Delivery Status Notification (DSN)** bezeichnet.

Solche Meldungen enthalten meist technische Fehlercodes. Diese Codes helfen dabei, die Ursache einzugrenzen: zum Beispiel eine falsch geschriebene Empfängeradresse, ein volles Postfach, ein DNS-Problem oder eine Ablehnung aufgrund von SPF, DKIM oder DMARC.

Wie liest man einen Statuscode?

Eine typische Fehlermeldung kann zum Beispiel so aussehen:

```
550 5.1.1 User unknown
```

Die einzelnen Bestandteile bedeuten:

Bestandteil	Bedeutung
`550`	SMTP-Antwortcode des empfangenden Servers
`5.1.1`	Erweiterter Mail-Statuscode, auch Enhanced Status Code genannt
`User unknown`	Beschreibungstext des empfangenden Servers

Der Beschreibungstext kann je nach Anbieter unterschiedlich formuliert sein. Für die Auswertung sind die numerischen Codes in der Regel zuverlässiger als der freie Text.

Temporäre und permanente Fehler

Die erste Ziffer des erweiterten Statuscodes zeigt, ob es sich um einen temporären oder permanenten Fehler handelt.

Codeklasse	Bedeutung	Interpretation
`2.x.x`	Erfolgreich	Die Nachricht wurde angenommen oder erfolgreich verarbeitet.
`4.x.x`	Temporärer Fehler	Die Zustellung ist momentan nicht möglich. Ein späterer Versuch kann erfolgreich sein.
`5.x.x`	Permanenter Fehler	Die Zustellung wurde dauerhaft abgelehnt. Ohne Änderung wird ein erneuter Versuch voraussichtlich wieder fehlschlagen.

Beispiele:

```
421 4.4.2 Connection timed out
550 5.1.1 User unknown
552 5.2.2 Mailbox full
550 5.7.1 Message rejected due to policy
```

Kategorien der erweiterten Statuscodes

Die zweite Ziffer des erweiterten Statuscodes beschreibt die Fehlerkategorie.

Kategorie	Codebereich	Bedeutung
Allgemein	`x.0.x`	Allgemeiner oder nicht genauer spezifizierter Fehler
Adresse	`x.1.x`	Problem mit Empfängeradresse, Absenderadresse oder Domain
Postfach	`x.2.x`	Problem mit dem Postfach des Empfängers
Mail-System	`x.3.x`	Problem mit dem Mailserver oder dessen Konfiguration
Netzwerk / DNS / Routing	`x.4.x`	Problem mit Verbindung, DNS, Routing oder Erreichbarkeit
SMTP-Protokoll	`x.5.x`	Problem mit SMTP-Kommandos, Syntax oder Protokollablauf
Inhalt / Format / Grösse	`x.6.x`	Problem mit Nachrichtengrösse, Inhalt, Zeichensatz oder Anhängen
Sicherheit / Policy / Mail-Auth	`x.7.x`	Ablehnung aufgrund von Sicherheit, Authentifizierung, Reputation oder Richtlinien

---

Häufige Fehlercodes und ihre Bedeutung

1. Allgemeine Fehler: x.0.x

Allgemeine Fehlercodes werden verwendet, wenn der empfangende Server die Ursache nicht genauer einordnet oder nur eine allgemeine Ablehnung zurückgibt.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
`4.0.0`	Temporary failure	Temporärer, nicht genauer beschriebener Fehler	Später erneut senden.
`5.0.0`	Permanent failure	Permanenter, nicht genauer beschriebener Fehler	Bounce-Text prüfen und Ursache eingrenzen.
`5.0.1`	Message rejected	Nachricht wurde allgemein abgelehnt	Empfängeradresse, Inhalt und Authentifizierung prüfen.

Hinweise

Allgemeine Codes sind weniger aussagekräftig. Für die genaue Analyse sollte immer der vollständige Bounce-Text berücksichtigt werden.

---

2. Adressfehler: x.1.x

Adressfehler gehören zu den häufigsten Ursachen für unzustellbare E-Mails. Sie betreffen die Empfängeradresse, die Domain oder in bestimmten Fällen auch die Absenderadresse.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
`5.1.0`	Address rejected / Other address status	Allgemeines Adressproblem	Adresse, Domain und Schreibweise prüfen.
`5.1.1`	User unknown / Mailbox unavailable	Die Empfängeradresse existiert nicht.	Adresse korrigieren oder aus dem Verteiler entfernen.
`5.1.2`	Bad destination system address	Die Zieldomain ist ungültig oder nicht erreichbar.	Domain und MX-Einträge prüfen.
`5.1.3`	Bad destination mailbox address syntax	Die Empfängeradresse hat ein ungültiges Format.	Adresse auf Tippfehler, Leerzeichen oder Sonderzeichen prüfen.
`5.1.4`	Destination mailbox address ambiguous	Die Adresse ist nicht eindeutig.	Empfänger kontaktieren und korrekte Adresse erfragen.
`5.1.6`	Mailbox has moved	Das Postfach wurde verschoben oder ist unter dieser Adresse nicht mehr erreichbar.	Neue Adresse beim Empfänger erfragen.
`5.1.8`	Bad sender system address	Die Absenderadresse oder Absenderdomain wird abgelehnt.	Absenderdomain, DNS und Return-Path prüfen.

Typische Ursachen

- Tippfehler in der Empfängeradresse

- Empfängeradresse wurde gelöscht
- Postfach wurde umbenannt oder migriert
- Domain existiert nicht mehr
- Domain hat keine gültigen MX-Einträge
- Absenderadresse ist technisch ungültig

Beispiel

```
550 5.1.1 User unknown
```

Bedeutung: Die Adresse vor dem `@` wurde beim empfangenden Mailserver nicht gefunden.

---

3. Postfachfehler: x.2.x

Diese Codes betreffen das konkrete Postfach des Empfängers. Das Zielsystem ist grundsätzlich erreichbar, aber das Postfach kann die Nachricht nicht annehmen.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
`4.2.1` / `5.2.1`	Mailbox disabled	Das Postfach ist deaktiviert oder nimmt keine Nachrichten an.	Empfänger über alternativen Kanal kontaktieren.
`4.2.2` / `5.2.2`	Mailbox full / Quota exceeded	Das Postfach ist voll.	Später erneut senden oder Empfänger informieren.
`5.2.3`	Message length exceeds administrative limit	Die Nachricht ist für dieses Postfach zu gross.	Anhänge verkleinern oder Datei per Link bereitstellen.
`4.2.4` / `5.2.4`	Mailing list expansion problem	Ein Verteiler konnte nicht korrekt aufgelöst werden.	Verteileradresse prüfen lassen.

Temporär oder permanent?

Ein volles Postfach wird häufig als temporärer Fehler gemeldet, kann aber auch als permanenter Fehler erscheinen. Entscheidend ist der konkrete Code:

- `4.2.2` = temporär, später erneut versuchen
- `5.2.2` = dauerhaft abgelehnt, Empfänger muss Speicherplatz schaffen

Beispiel

```
552 5.2.2 Mailbox full
```

Bedeutung: Das Postfach des Empfängers hat sein Speicherlimit erreicht.

---

4. Mail-Systemfehler: x.3.x

Mail-Systemfehler betreffen den empfangenden Mailserver oder dessen Konfiguration.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
`4.3.0` / `5.3.0`	Other mail system status	Allgemeiner Fehler im Zielsystem	Bounce-Text prüfen.
`4.3.1`	Mail system full	Das Zielsystem hat ein Speicher- oder Kapazitätsproblem.	Später erneut senden.

4.3.2 / 5.3.2	System not accepting messages	Der Zielserver nimmt aktuell keine Nachrichten an.	Später erneut versuchen oder Empfänger-Admin kontaktieren.
5.3.4	Message too big for system	Die Nachricht überschreitet das Grössenlimit des Zielsystems.	Nachricht verkleinern oder Anhänge auslagern.
5.3.5	System incorrectly configured	Das Zielsystem ist fehlerhaft konfiguriert.	Empfänger-Admin kontaktieren.

Typische Ursachen

- Mailserver des Empfängers ist überlastet
- Mailserver ist falsch konfiguriert
- Grössenlimit auf Empfängerseite wurde überschritten
- Zielsystem nimmt vorübergehend keine Nachrichten an

Beispiel

```
552 5.3.4 Message size exceeds fixed maximum message size
```

Bedeutung: Die Nachricht ist grösser als vom empfangenden System erlaubt.

---

5. Netzwerk-, DNS- und Routingfehler: x.4.x

Diese Fehler treten auf, wenn der sendende Server den empfangenden Server nicht korrekt erreichen kann oder kein gültiger Zustellweg gefunden wird.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
4.4.1	No answer from host	Der Zielhost antwortet nicht.	Später erneut senden.
4.4.2	Connection timed out / Bad connection	Die Verbindung wurde unterbrochen oder ist abgelaufen.	Später erneut senden.
4.4.3	DNS failure / Directory server failure	DNS- oder Verzeichnisdienstproblem.	MX- und DNS-Auflösung prüfen.
4.4.4 / 5.4.4	Unable to route	Es wurde kein Zustellweg gefunden.	Domain, MX und Routing prüfen.
4.4.5	Mail system congestion	Das Mail-System ist überlastet.	Später erneut senden.
4.4.6	Routing loop detected	Eine Weiterleitungsschleife wurde erkannt.	Weiterleitungen, Aliase und Verteiler prüfen.
4.4.7	Delivery time expired	Die maximale Zustellzeit ist abgelaufen.	Vorherige Fehlermeldungen im Bounce-Verlauf prüfen.

Typische Ursachen

- DNS-Einträge der Empfängerdomain sind fehlerhaft
- MX-Server ist nicht erreichbar
- Netzwerkverbindung bricht ab
- Firewall oder Empfänger-Gateway blockiert die Verbindung
- Falsch konfigurierte Weiterleitung oder Alias-Schleife

Beispiel

```
451 4.4.2 Connection timed out
```

Bedeutung: Die Verbindung zum empfangenden Mailserver konnte nicht stabil aufgebaut oder gehalten werden.

---

6. SMTP-Protokollfehler: x.5.x

SMTP-Protokollfehler entstehen, wenn während der technischen Kommunikation zwischen den Mailservern ein ungültiger Befehl, eine falsche Syntax oder eine nicht unterstützte Funktion verwendet wird.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
`5.5.0`	Other protocol status	Allgemeiner SMTP-Protokollfehler	Bounce-Text prüfen.
`5.5.1`	Invalid command	Ein SMTP-Kommando ist ungültig oder wurde in falscher Reihenfolge gesendet.	Versandsoftware oder SMTP-Client prüfen.
`5.5.2`	Syntax error	Die SMTP-Syntax ist fehlerhaft.	Absenderadresse, Empfängeradresse und Client prüfen.
`5.5.3`	Too many recipients	Es wurden zu viele Empfänger in einer Nachricht angegeben.	Versand in kleinere Gruppen aufteilen.
`5.5.4`	Invalid command arguments	Ein SMTP-Kommando enthält ungültige Parameter.	Versandsoftware prüfen.
`5.5.6`	Authentication Exchange line too long	Die Authentifizierungszeile ist zu lang.	SMTP-Client oder Authentifizierungsmethode prüfen.

Typische Ursachen

- Fehlerhafte SMTP-Client-Konfiguration
- Zu viele Empfänger in einem Versandvorgang
- Ungültige Zeichen in Adressen
- Veraltete oder nicht kompatible Versandsoftware
- Problem bei SMTP AUTH

Beispiel

```
503 5.5.1 Error: need RCPT command
```

Bedeutung: Der SMTP-Dialog wurde in einer falschen Reihenfolge geführt.

---

7. Inhalts-, Format- und Grössenfehler: x.6.x

Diese Codes betreffen den Inhalt der Nachricht, die Kodierung, Anhänge oder Zeichensätze.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
`5.6.0`	Media error	Der Inhalt kann nicht verarbeitet werden.	Nachricht und Anhänge prüfen.
`5.6.1`	Media not supported	Der Inhaltstyp wird nicht unterstützt.	Dateityp ändern oder Anhänge anders bereitstellen.
`5.6.3`	Conversion required but not supported	Eine erforderliche Konvertierung ist nicht möglich.	Nachricht einfacher formatieren.
`5.6.5`	Conversion failed	Die Konvertierung der Nachricht ist fehlgeschlagen.	HTML, Encoding und Anhänge prüfen.

5.6.7	Non-ASCII addresses not permitted	Internationale Zeichen in Adressen werden nicht akzeptiert.	ASCII-kompatible Adresse verwenden.
5.6.9	UTF-8 header message cannot be transferred	UTF-8-Header können nicht übertragen werden.	Sonderzeichen und Zeichensatz prüfen.
5.6.10	Recipient address has null MX	Die Domain signalisiert, dass sie keine E-Mails annimmt.	Empfängeradresse oder Domain prüfen.

Typische Ursachen

- Anhang ist zu gross oder blockiert
- Dateityp wird vom Empfänger nicht akzeptiert
- Nachricht enthält fehlerhafte Kodierung
- Sonderzeichen in Headern oder Adressen verursachen Probleme
- Zielsystem unterstützt benötigte Formatierung nicht

Beispiel

```
554 5.6.1 Message content rejected
```

Bedeutung: Der Inhalt oder ein Anhang wurde vom empfangenden System nicht akzeptiert.

---

8. Sicherheit, Policy und Mail-Authentifizierung: x.7.x

Diese Kategorie ist bei modernen Zustellproblemen besonders wichtig. Sie umfasst Ablehnungen durch Sicherheitsrichtlinien, Spamfilter, SPF, DKIM, DMARC, Blocklisten, Reputation, SMTP-Authentifizierung und Verschlüsselung.

Code	Typische Meldung	Bedeutung	Empfohlene Massnahme
4.7.0 / 5.7.0	Security or policy status	Allgemeiner Sicherheits- oder Policy-Fehler	Bounce-Text genau prüfen.
5.7.1	Delivery not authorized / Message refused	Zustellung durch Richtlinie verweigert.	SPF, DKIM, DMARC, Reputation und Inhalt prüfen.
5.7.2	Mailing list expansion prohibited	Versand an Verteiler ist nicht erlaubt.	Berechtigungen beim Empfänger prüfen.
5.7.5	Cryptographic failure	Kryptografische Prüfung fehlgeschlagen.	DKIM-Schlüssel und Signatur prüfen.
5.7.7	Message integrity failure	Integritätsprüfung fehlgeschlagen.	DKIM, Weiterleitungen und Gateways prüfen.
5.7.8	Authentication credentials invalid	SMTP-Zugangsdaten sind ungültig.	Benutzername, Passwort oder App-Passwort prüfen.
5.7.9	Authentication mechanism too weak	Die Authentifizierungsmethode ist zu schwach.	Sichere Authentifizierung und TLS verwenden.
5.7.10	Encryption needed	Verschlüsselung ist erforderlich.	SMTP mit TLS oder STARTTLS verwenden.
5.7.11	Encryption required for requested authentication mechanism	Die gewünschte Authentifizierung erfordert Verschlüsselung.	STARTTLS aktivieren.
5.7.13	User account disabled	Das Benutzerkonto ist deaktiviert.	Konto prüfen oder Provider kontaktieren.
5.7.23	SPF validation failed	SPF-Prüfung fehlgeschlagen.	SPF-Record und Versandserver prüfen.
5.7.26	Unauthenticated email not accepted	Nachricht besteht SPF/DKIM/DMARC-Anforderungen nicht.	SPF, DKIM und DMARC prüfen.

Typische Ursachen

- SPF-Record fehlt, ist falsch oder enthält den Versandserver nicht
- DKIM-Signatur fehlt oder ist ungültig
- DMARC-Richtlinie lehnt nicht authentifizierte Nachrichten ab
- Absenderdomain hat schlechte Reputation
- IP-Adresse oder Domain steht auf einer Blockliste
- Nachricht wird als Spam oder Phishing eingestuft
- SMTP-Login ist falsch oder unverschlüsselt
- Empfänger hat eine restriktive Sicherheitsrichtlinie

Beispiel

```
550 5.7.1 Message rejected due to policy
```

Bedeutung: Die Nachricht wurde nicht wegen einer ungültigen Adresse, sondern aufgrund einer Sicherheits- oder Empfänger-Richtlinie abgelehnt.

Mail-Authentifizierung: SPF, DKIM und DMARC

SPF

SPF steht für **Sender Policy Framework**. Damit legt eine Domain im DNS fest, welche Mailserver berechtigt sind, E-Mails für diese Domain zu versenden.

Typische Fehlermeldungen:

```
550 5.7.1 SPF check failed
550 5.7.23 SPF validation failed
550 5.7.1 Sender Policy Framework validation failed
```

Häufige Ursachen

- SPF-Record fehlt
- SPF-Record enthält den verwendeten Versandserver nicht
- SPF-Record enthält zu viele DNS-Lookups
- E-Mail wird über ein externes System versendet, das nicht autorisiert ist
- Weiterleitung verändert die technische Absenderprüfung

Empfohlene Prüfung

- Ist ein SPF-Record für die Absenderdomain vorhanden?

- Ist der verwendete Versandserver im SPF-Record enthalten?
- Wird über ein externes Newsletter-, CRM- oder Vereinsverwaltungssystem versendet?
- Gibt es mehrere SPF-Records für dieselbe Domain?

DKIM

DKIM steht für **DomainKeys Identified Mail**. Dabei wird eine Nachricht digital signiert. Der empfangende Server prüft im DNS, ob die Signatur zur Domain passt.

Typische Fehlermeldungen:

```
550 5.7.1 DKIM signature verification failed
550 5.7.5 Cryptographic failure
550 5.7.7 Message integrity failure
```

Häufige Ursachen

- DKIM-Signatur fehlt
- DKIM-DNS-Eintrag fehlt oder ist falsch
- DKIM-Schlüssel passt nicht zur Signatur
- Nachricht wurde nach der Signatur verändert
- Weiterleitung, Disclaimer oder Mail-Gateway verändert den Inhalt

Empfohlene Prüfung

- Ist DKIM für die Versanddomain aktiviert?
- Existiert der passende DKIM-DNS-Eintrag?
- Wurde die Nachricht nach dem Versand verändert?
- Nutzt der Versanddienst den korrekten DKIM-Selector?

DMARC

DMARC steht für **Domain-based Message Authentication, Reporting and Conformance**. DMARC baut auf SPF und DKIM auf und definiert, wie empfangende Server mit Nachrichten umgehen sollen, die nicht korrekt authentifiziert sind.

Typische Fehlermeldungen:

```
550 5.7.1 DMARC policy reject
550 5.7.26 Unauthenticated email from domain is not accepted
550 5.7.1 Message rejected due to DMARC policy
```

Häufige Ursachen

- SPF schlägt fehl
- DKIM schlägt fehl
- SPF oder DKIM bestehen zwar technisch, passen aber nicht zur sichtbaren Absenderdomain
- DMARC-Richtlinie der Absenderdomain steht auf `quarantine` oder `reject`
- Versand erfolgt über ein nicht autorisiertes Drittsystem

Empfohlene Prüfung

- Existiert ein DMARC-Record für die Absenderdomain?
- Besteht SPF?
- Besteht DKIM?
- Stimmen SPF- oder DKIM-Domain mit der sichtbaren Absenderdomain überein?
- Ist die DMARC-Policy auf `none`, `quarantine` oder `reject` gesetzt?

Häufige SMTP-Antwortcodes

SMTP-Antwortcodes sind dreistellig. Sie erscheinen oft zusammen mit einem erweiterten Statuscode.

SMTP-Code	Bedeutung	Typische Einordnung
`421`	Service nicht verfügbar	Temporäres Server- oder Verbindungsproblem
`450`	Mailbox nicht verfügbar	Temporäres Empfänger- oder Postfachproblem
`451`	Lokaler Fehler bei der Verarbeitung	Temporärer Server-, DNS- oder Policy-Fehler
`452`	Nicht genügend Speicherplatz oder Systemressourcen	Temporärer Kapazitätsfehler
`500`	Syntaxfehler	SMTP-Protokollproblem
`501`	Syntaxfehler in Parametern	Adresse oder SMTP-Parameter ungültig
`503`	Falsche Befehlsreihenfolge	SMTP-Protokollproblem
`530`	Authentifizierung erforderlich	SMTP AUTH oder TLS fehlt
`535`	Authentifizierung fehlgeschlagen	Benutzername oder Passwort falsch
`550`	Nachricht oder Empfänger abgelehnt	Häufig Adresse, Policy, Spamfilter oder Authentifizierung
`551`	Benutzer nicht lokal	Empfängeradresse nicht am Zielsystem vorhanden
`552`	Speicherlimit oder Nachrichtengrösse überschritten	Postfach voll oder Nachricht zu gross
`553`	Mailboxname ungültig	Ungültige Empfänger- oder Absenderadresse
`554`	Transaktion fehlgeschlagen	Allgemeine Ablehnung, oft Policy oder Inhalt

---

Praktische Einordnung nach Problemtyp

Von der technischen Meldung zur konkreten Prüfung

Die vorherigen Abschnitte erklären die Fehlercodes nach ihrer technischen Kategorie. Dieser Abschnitt dient nicht dazu, dieselben Codes nochmals inhaltlich zu erklären. Er übersetzt die Codes in konkrete Prüfschritte für die Praxis.

Das ist hilfreich, weil eine Bounce-Meldung im Support-Alltag selten nur als technischer Code betrachtet wird. Entscheidend ist meist die nächste Frage: Muss die Empfängeradresse korrigiert werden, liegt das Problem beim Postfach, muss DNS geprüft werden, ist die Nachricht zu gross oder wurde sie durch eine Sicherheitsrichtlinie abgelehnt?

Die folgende Einordnung hilft deshalb bei der schnellen Triage: Sie zeigt, welche Fehlercodes typischerweise zu welchem Prüfpfad gehören und welche Massnahmen daraus folgen.

Empfängeradresse prüfen

Relevant bei:

```
5.1.0
5.1.1
5.1.2
5.1.3
5.1.4
5.1.6
```

Massnahmen:

- Adresse auf Tippfehler prüfen
- Sonderzeichen und Leerzeichen entfernen
- Domain prüfen
- Empfänger über alternativen Kanal kontaktieren
- Nicht mehr gültige Adresse aus Verteiler entfernen

Postfach oder Empfänger-System prüfen

Relevant bei:

```
4.2.1
5.2.1
4.2.2
5.2.2
5.2.3
4.3.2
5.3.2
```

Massnahmen:

- Später erneut senden
- Empfänger informieren

- Nachricht verkleinern
- Anhänge als Link bereitstellen
- Empfänger-Admin kontaktieren

DNS und Routing prüfen

Relevant bei:

```
4.4.1
4.4.2
4.4.3
4.4.4
5.4.4
4.4.6
4.4.7
```

Massnahmen:

- MX-Einträge der Empfängerdomain prüfen
- DNS-Auflösung prüfen
- Erreichbarkeit des Zielservers prüfen
- Weiterleitungen und Aliase prüfen
- Bei temporären Fehlern später erneut senden

Nachricht und Anhänge prüfen

Relevant bei:

```
5.2.3
5.3.4
5.6.0
5.6.1
5.6.5
5.6.7
5.6.9
```

Massnahmen:

- Nachricht verkleinern
- Anhänge reduzieren oder entfernen
- Dateityp ändern
- ZIP-Dateien vermeiden, falls blockiert
- Sonderzeichen in Betreff, Absendername und Dateinamen prüfen

- HTML-Signaturen und eingebettete Bilder prüfen

SPF, DKIM, DMARC und Reputation prüfen

Relevant bei:

```
5.7.0
5.7.1
5.7.5
5.7.7
5.7.23
5.7.26
```

Massnahmen:

- SPF-Record prüfen
- DKIM-Signatur prüfen
- DMARC-Record prüfen
- Versanddomain und sichtbare Absenderdomain vergleichen
- IP- und Domain-Reputation prüfen
- Blocklisten prüfen
- Inhalt auf Spam- oder Phishing-Merkmale prüfen

SMTP-Login und Verschlüsselung prüfen

Relevant bei:

```
5.7.8
5.7.9
5.7.10
5.7.11
530
535
```

Massnahmen:

- Benutzername prüfen
- Passwort oder App-Passwort prüfen
- SMTP-Server und Port prüfen
- STARTTLS oder TLS aktivieren
- Authentifizierungsmethode prüfen

- Konto auf Sperrung oder Deaktivierung prüfen