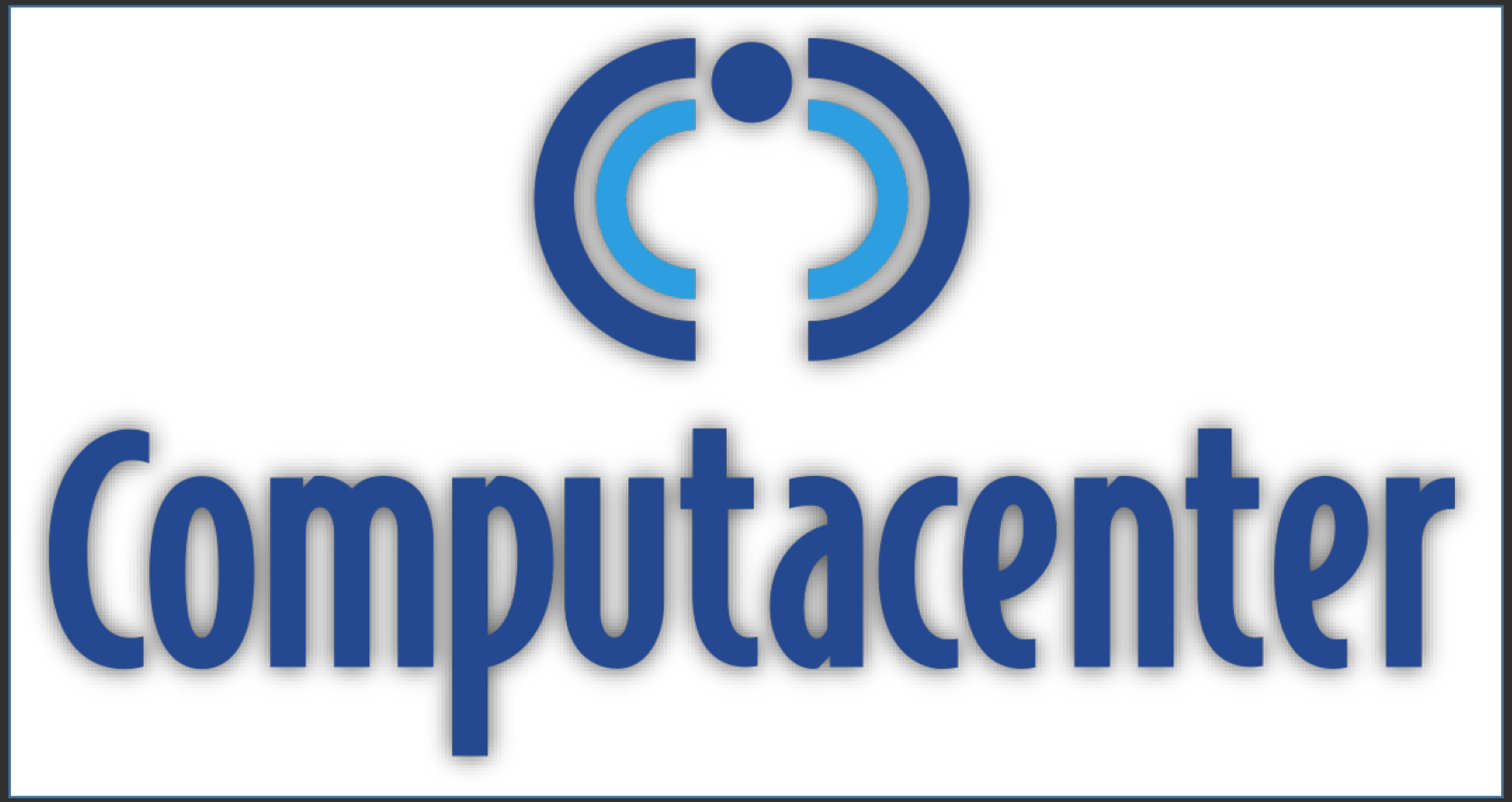
Exchange User Group Meetup Q2 2023

{Hybrid Edition}

11. Mai 2023

Sponsor



https://www.computacenter.com

Sponsor

https://www.enowsoftware.com

Meetup Q2 2022

Microsoft 365 Gruppen – Was ist das und warum braucht man sie?
- *Thomas Stensitzki*

Exchange Online Blockierung veralteter Exchange Server
- *Thomas Stensitzki*

Exchange Q & A

Die Talks werden aufgezeichnet. The sessions will be recorded.
https://go.granikos.eu/EXUSG-Recs

Microsoft 365 Gruppen – Was ist das und warum braucht man sie?

(Update)

Thomas Stensitzki

Exchange Online Blockierung veralteter Exchange Server

Thomas Stensitzki

Worum geht es?

- Throttling and Blocking Email from Persistently Vulnerable Exchange Servers to Exchange Online

  →Blogartikel vom 23. März 2023 / 8. Mai 2023

- Drosselung und Blockierung von eingehenden SMTP-Verbindungen zu Exchange Online

Unsichere Exchange Server

- Sicherheitsrisiko durch kompromittierte lokale Exchange Server
- Versand von E-Mail-Nachrichten an unternehmensinterne und externe Empfänger
  - Phishing, Spam, Malware
- Reputationsrisiko für Microsoft 365

Geplante Maßnahmen

- **Drosselung** (Throttling)
  - Abweisung der SMTP-Verbindung mit SMTP **Statuscode 450**
  - **Erneuter Verbindungsversuch** durch lokalen Exchange Server
  - Verhalten analog zu einer Greylisting-Funktion

- **Blockierung** (Blocking)
  - Abweisung der SMTP-Verbindung mit SMTP **Statuscode 550**
  - **Kein erneuter Verbindungsversuch** durch lokalen Exchange Server
  - Nichtzustellbarkeitsbericht (NDR) an Absender

Abgestufte Umsetzung

Durchsetzungsaktionen				Durchsetzungsdauer
Stufe	**Bericht**	**Drosselung (min/h)**	**Blockierung (min/h)**	**Nicht-Compliant (Tage)**
1	Ja	0	0	30
2	Ja	5	0	10
3	Ja	10	0	10
4	Ja	20	0	10
5	Ja	30	5	10
6	Ja	30	10	10
7	Ja	30	20	10
8	Ja	**0**	**60**	**10**
		Gesamtanzahl der Tage zwischen **Ersterkennung** und **vollständiger Blockierung** der Verbindungen		**90**

Erste Blockierung nach 60 Tagen

Freikaufen

- Die Drosselung oder Blockierung kann für insgesamt 90 Tage je Kalenderjahr ausgesetzt werden

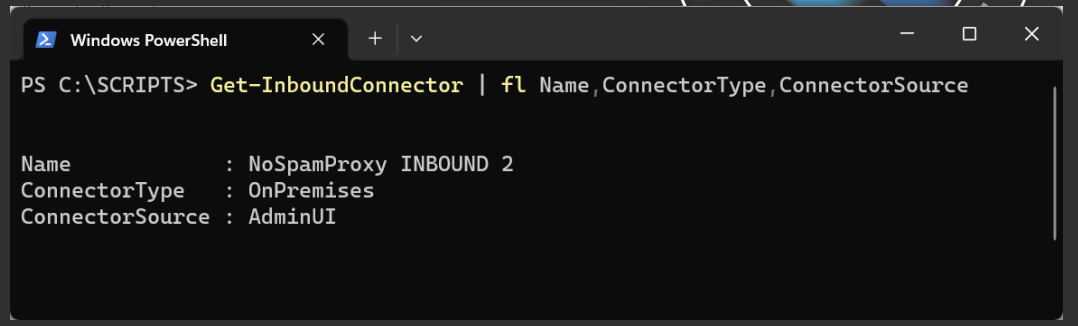
→ Enforcement Pause

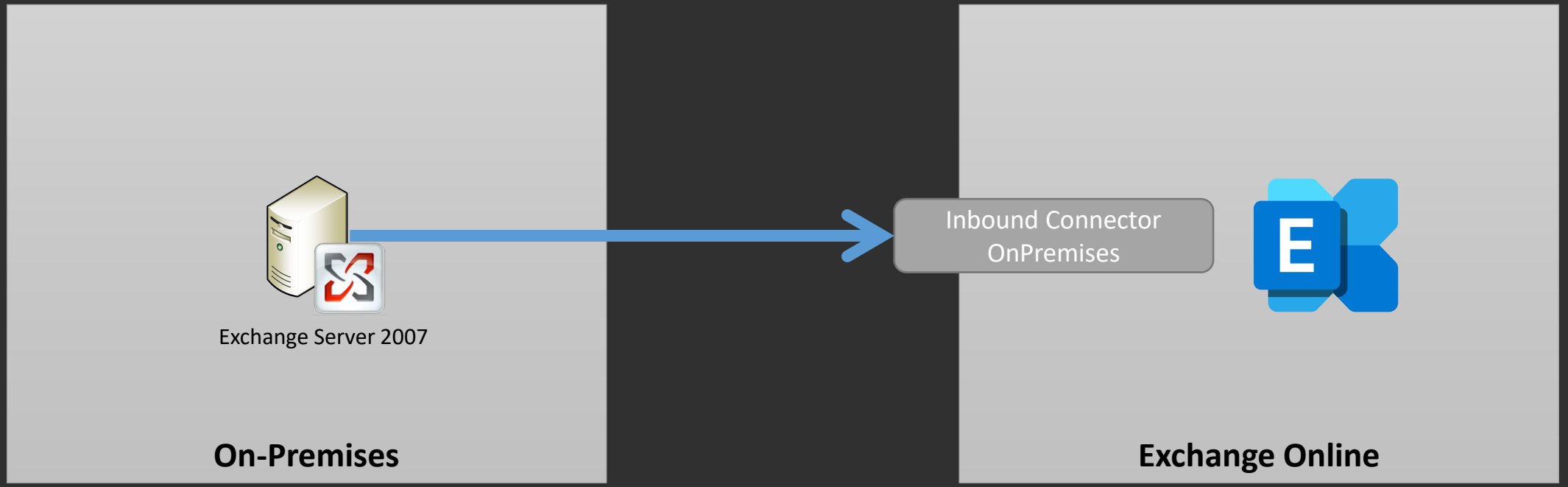
Beispiel

- 15 Tage in Q1
- 20 Tage in Q3

Rest 55 Tage
→ verbleibendes Kontingent **verfällt** am Ende eines Kalenderjahres

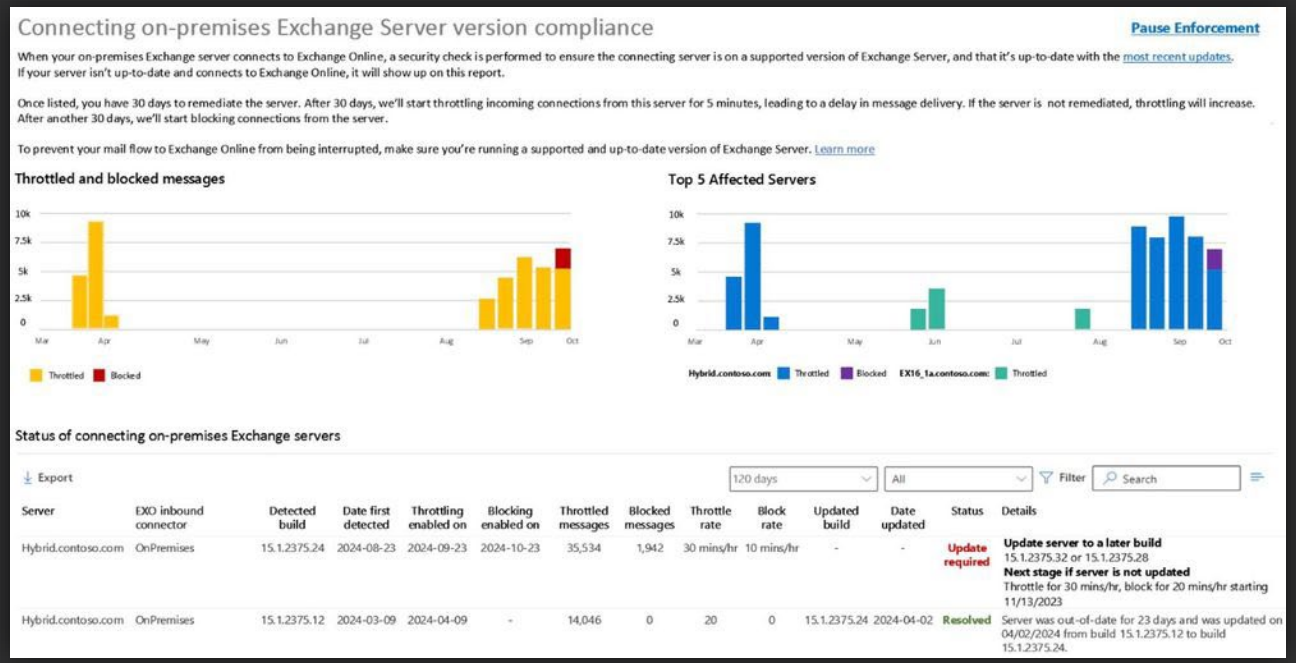
Betroffene Verbindungsart





Benachrichtigung

- Neuer Report im Exchange Online Admin Center



Mockup-Beispiel – Quelle: Microsoft

Benachrichtigung

- Drosselung
  - SMTP-Protokoll des lokalen Exchange Servers

```
450 4.7.230 Connecting Exchange server version is out-of-date; connection
to Exchange Online throttled for 5 mins/hr. For more information see
https://aka.ms/BlockUnsafeExchange.
```

- Blockierung
  - SMTP-Protokoll des lokalen Exchange Servers

```
550 5.7.230 Connecting Exchange server version is out-of-date; connection
to Exchange Online blocked for 10 mins/hr. For more information see
https://aka.ms/BlockUnsafeExchange.
```

Wie werden Versionen erkannt?

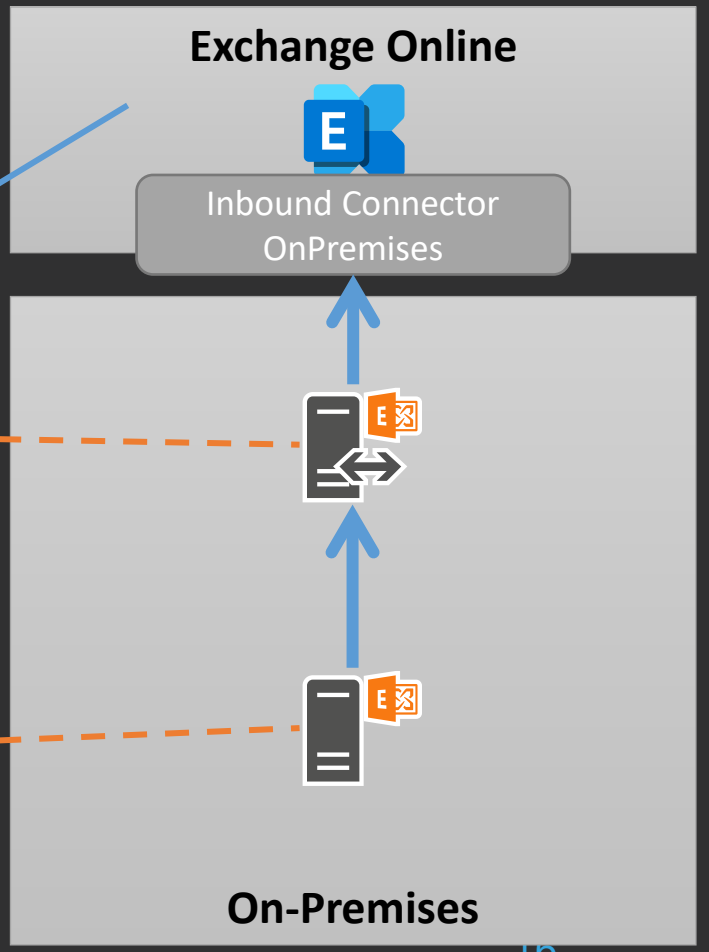
Exchange Server 2016 – Auschnitt Mail-Header

- Alle Informationen sind Bestandteil des E-Mail-Headers

```
Received: from smtpo.verunagroup.de (81.173.212.44) by
 VE1EUR01FT066.mail.protection.outlook.com (10.152.3.94) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id
 15.20.6319.25 via Frontend Transport; Fri, 21 Apr 2023 08:55:17 +0000
```

```
Received: from DEHVNEX01.verunagroup.de (192.16.22.86) by smtpo.verunagroup.de
 (192.17.0.99) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.2507.23; Fri, 21
 Apr 2023 10:55:05 +0200
```

```
Received: from DEHVNEX01.verunagroup.de (192.16.22.86) by DEHVNEX01.verunagroup.de
 (192.16.22.86) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.2507.23; Fri, 21
 Apr 2023 10:55:05 +0200
```



Was bringt die Zukunft

"The enforcement system will eventually apply to all versions of Exchange Server and all email coming into Exchange Online, but we are starting with a very small subset of outdated servers: Exchange 2007 servers that connect to Exchange Online over an inbound connector type of OnPremises."

Blogartikel Throttling and Blocking Email from Persistently Vulnerable Exchange Servers to Exchange Online

Was bringt die Zukunft

"The enforcement system **will eventually** apply to **all versions** of Exchange Server and **all email** coming into Exchange Online, but we are starting with a very small subset of outdated servers: **Exchange 2007** servers that connect to Exchange Online over an **inbound connector type of OnPremises**."

Blogartikel Throttling and Blocking Email from Persistently Vulnerable Exchange Servers to Exchange Online

- Was kommt nach Exchange Server 2007?
  - Exchange Server 2010
  - Exchange Server 2013
  - …
- Haltet eure Exchange Server Umgebung aktuell

Ressourcen

- Throttling and Blocking Email from Persistently Vulnerable Exchange Servers to Exchange Online

Exchange Q & A

Exchange Q & A

- Exchange Server 2019 CU 2023 H1 (CU13)
  - Moderne Authentifizierung (OAuth) für rein lokale Umgebungen mit ADFS
    - Enabling Modern Auth in Exchange on-premises
  - Sicherung und Wiedereinspielung von angepassten Konfigurationen bei CU-Installation
    - Exchange Server custom configuration preservation
  - Verpflichtendes CU für hybride Exchange Organisationen

Exchange User Group

Exchange User Group

Organisatorisches

- **Exchange User Group Team**
  - Registrierung → Link auf Homepage
- **Themenvorschläge**
  - https://go.granikos.eu/EXUSG-Themen
- **Community Sticker**
  - https://go.granikos.eu/CommunitySticker
- **EXUSG Mugs**
  - https://go.granikos.eu/EXUSGMug

Exchange User Group

Organisatorisches

Exchange User Group

Nächster Termin **24. August 2023**

Homepage **https://exusg.de**

Twitter **@exusg**

Recordings **https://go.granikos.eu/EXUSG-Recs**