
# Exchange User Group {Online Edition}

4. November 2021

# Meetup Q4 2021

- Exchange Server Emergency Mitigation Service

  *Thomas Stensitzki*

- Exchange Q & A

Die Talks werden aufgezeichnet. The sessions will be recorded.


# Exchange Server Emergency Mitigation Service

Thomas Stensitzki

# Thomas Stensitzki

Enterprise Consultant
Granikos GmbH & Co. KG

MVP | MCT Regional Lead

@stensitzki
thomas.stensitzki@granikos.eu


# Exchange Server CU September 2021

***Exchange Server 2016 / 2019***

- Neue Installationsvoraussetzung
  - IIS URL-Rewrite Modul
  - Update for Universal C Runtime in Windows für Windows Server 2012 und 2012R2
- Neuer Kommandozeilen-Schalter für Installation
  - /IAcceptExchangeServerLicenseTerms_**DiagnosticDataON**
  - /IAcceptExchangeServerLicenseTerms_**DiagnosticDataOFF**

# Exchange Emergency Mitigation Service

***Exchange Server CU September 2021***


- Neuer Exchange Service für Postfachrolle
  → Nicht für die Edge Transport Rolle
- Aktivierung / Deaktivierung
  - Organisationsweit MitigationsEnabled: True|False
  - Je Exchange Server mit Postfachrolle
- Abkürzungen
  - EEMS – Exchange Emergency Mitigation Service
  - EOMT – Exchange On-Premises Mitigation Tool
  - OCS – Office Config Service

# Exchange Emergency Mitigation Service

***Exchange Server CU September 2021***


- Stündliche Prüfung der EEMS Informationen beim OCS
  - https://officeclient.microsoft.com/getexchangemitigations
  - Signierte XML-Datei mit Konfigurationen
- Implementierung eines Notfall-Workarounds
  - Sicherung bis zur Verfügbarkeit eines Security Patches
- Security Patch muss manuell installiert werden
- Einzelne Mitigations können deaktiviert werden

# Exchange Server Mitigation


```
# Abfrage der verfügbaren Mitigations
cd $exscripts
.\Get-Mitigations.ps1

# Export der verfügbaren Mitigations
.\Get-Mitigations.ps1 -ExportCSV C:\Scripts\Mitigations.csv

# Test der Verbindung zum Mitigationendpunkt
.\Test-MitigationServiceConnectivity.ps1
```

# Exchange Server Mitigation


```
# Aktivierung auf Organisationsebene
Set-OrganizationConfig – MitigationsEnabled:$true
# Deaktivierung auf Organisationsebene
Set-OrganizationConfig – MitigationsEnabled:$false

# Abfrage der Mitigationstatus auf Serverebene
Get-ExchangeServer | Sort-Object Name | FT Name,Miti* -AutoSize

# Deaktivierung der Mitigations M1 und M2 auf einem Server
Set-ExchangeServer SERVER –MitigationsBlocked M1,M2 –MitigationsEnabled:$null
# Aktivierung der Mitigation M1 auf einem Server
Set-ExchangeServer SERVER –MitigationsBlocked M2 –MitigationsEnabled M1
```

# Exchange Server Diagnostic Data


- Exchange Server Build
  - CU/SU Build-Information, z.B. 15.1.2375.7
- Emergency Mitigation Service-Status
  - Information zum Konfigurationsstatus, werden Daten übertragen ja/nein
- Immutable Device ID
  - Eindeutige GUID für den HTTP-Request, nicht identisch mit der GUID des Exchange Server Objektes
- Immutable Org ID
  - Eindeutige GUID der Exchange Organisation

# Exchange Server Diagnostic Data


- Applied Mitigations
  - Liste der auf dem Server angewandten Mitigations
- Blocked mitigations
  - Liste der auf dem Server blockierten Mitigations

```
# Deaktivierung
Set-ExchangeServer -Identity <ServerName> -DataCollectionEnabled:$false
# Aktivierung
Set-ExchangeServer -Identity <ServerName> -DataCollectionEnabled:$true
```

Protokolldateien → **V15\Logging\MitigationService**

# Exchange Server Sicherheit


- Prüfung der aktuellen Konfiguration mit HealthChecker
  - https://aka.ms/ExchangeHealthChecker
- Exchange Update Wizard
  - https://aka.ms/ExchangeUpdateWizard
- Exchange On-Premises Mitigation Tool
  - https://aka.ms/eomt

# Exchange Server AMSI & MDAV

***Exchange Server CU Juni 2021***

- AMSI – Antimalware Scan Interface
  - Prüft eingehende HTTP-Anfragen
  - Windows Server 2016 / 2019
  - Interagiert mit MDAV und ist automatisch aktiv
- MDAV – Microsoft Defender Antivirus
  - Automatische Prüfung auf neue Signatur-Dateien
    → Internetverbindung erforderlich
  - Bei Nutzung einer Drittanbieter AV-Lösung automatisch deaktiviert


# Demo

# Ressourcen

- IIS URL-Rewrite Modul
  - Automatische Installation via Web Platform Installer
  - Manuelle Installation
- Update for Universal C Runtime in Windows
- New security feature in September 2021 Cumulative Update for Exchange Server
- Addressing Your Feedback on the Exchange Emergency Mitigation Service
- One-Click Microsoft Exchange On-Premises Mitigation Tool – March 2021
- News About the June 2021 Cumulative Update for Exchange Server


# Exchange Q & A


# Exchange User Group

# Exchange User Group

***Organisatorisches***


Exchange
User Group

Nächster Termin: 3. März 2022

Homepage https://exusg.de

Twitter @exusg

# Exchange User Group

***Organisatorisches***

- Exchange User Group Team
  - Im Microsoft Community Tenant
- Community Sticker
  - https://go.granikos.eu/CommunitySticker
- EXUSG Mugs
  - https://go.granikos.eu/EXUSGMug