

TLSv1.2 (oder neuer) erforderlich

Situation

Zum 1. März 2020 haben wir die für **HTTPS, POP3 und IMAP** verwendeten veralteten SSL/TLS-Verschlüsselungsprotokolle **TLSv1.0 und TLSv1.1 deaktiviert**. Zum 15. Februar 2021 haben wir die gleiche Abschaltung für **SMTP** (für den Versand von E-Mails über die TCP-Ports 465 bzw. 587) vorgenommen. Somit kann auf unsere authentifizierten E-Mail-Dienste seit dem 15. Februar 2021 ausschließlich über das SSL/TLS-Verschlüsselungsprotokoll TLSv1.2 (oder neuer) zugegriffen werden.

Technisch begründet wird die Mindestanforderung von TLSv1.2 z.B. durch [RFC 7525](#) bzw. [PCI DSS](#). Darüber hinaus haben wir die bei TLSv1.2 möglichen Cipher-Suites auf die nachfolgenden beschränkt; diese bieten alle [Perfect Forward Secrecy](#) und [Authenticated Encryption](#) und erfüllen damit die von TLSv1.3 verpflichtend geforderten Eigenschaften.

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256

Probleme

Allerdings haben Microsoft **Windows 7 SP1 und 8** als auch Microsoft **Windows Server 2008 R2 und 2012** standardmäßig **TLSv1.2 nicht aktiviert** ist und somit schlägt unter Umständen der **Zugriff** auf die Groupware-Cloud **mittels Microsoft Outlook fehl**. Bei Microsoft Windows 8.1 und 10 bzw. Microsoft Windows Server 2016 und 2019 ist TLSv1.2 bereits standardmäßig aktiviert, so dass hierbei kein Handlungsbedarf erforderlich ist.

Ähnlich verhält es sich bei macOS (auch: Mac OS X bzw. OS X): TLSv1.2 wird **erst seit macOS Sierra (10.12.6) bzw. High Sierra (10.13)** unterstützt, insbesondere wenn Sie die vom Betriebssystem mitgelieferte E-Mail-Software „Mail“ verwenden.

Umgehung

Sollten Sie auf unsere **Groupware-Cloud mittels Microsoft Outlook in Verbindung mit einer älteren Windows-Version zugreifen**, bitten wir Sie den **Microsoft Easy Fix 51044 (MSI-Datei)** sowie die **Registry-Anpassung (REG-Datei)** einzuspielen. Starten Sie bitte nach dem Einspielen beider Anpassungen Ihr Microsoft Outlook neu; anschließend sollte der Zugriff wieder funktionieren.

Lösung

Da Microsoft Windows 7 SP1 und Microsoft Windows 2008 R2 seitens Microsoft bereits zum 14. Januar 2020 eingestellt wurden, sollte ein Wechsel auf eine neuere Windows-Version unbedingt erfolgen sollte, da Sie bereits seit zuvor genanntem Datum keine Sicherheitsupdates mehr erhalten.

Bei macOS (auch: Mac OS X bzw. OS X) wurde macOS Sierra (10.12) bereits im Oktober 2019 eingestellt und macOS High Sierra (10.13) ist im Dezember 2020 eingestellt worden. Noch ältere Betriebssystem-Versionen wie OS X El Capitan (10.11), Yosemite (10.10), Mavericks (10.9), Mountain Lion (10.8) oder Lion (10.7) unterstützen gar keine moderne Verschlüsselung. Auch hier sollte ein Wechsel auf eine aktuelle Version unbedingt erfolgen, da Sie bei diesen Betriebssystem-Versionen, teilweise bereits seit vielen Jahren, keine Sicherheitsupdates mehr erhalten.

Siehe auch

- [Zu altes System/Mail-Client \(für SMTP\)](#)
- [Microsoft-Update bei Groupware-Cloud-Benutzern erforderlich](#)

Revision #2

Created 27 August 2021 07:10:51 by Admin

Updated 15 December 2022 12:12:34 by Robert Scheck