PEINLICHE PANNE

"Jahr 2022 Bug": Microsoft-Fehler bei Exchange sorgt für weltweite Mail-Ausfälle

Wechsel auf das neue Jahr löst verheerenden Fehler aus. Es gibt einen Workaround, Admins sollten schnell handeln

Andreas Proschofsky

1. Jänner 2022, 14:46 / 728 Postings

Foto: Mark Lennihan / AP

Es ist eine äußerst unerfreuliche Überraschung, die Microsoft zum Jahreswechsel für Systemadministratorinnen und Systemadministratoren parat hat. Ein Fehler in Microsoft Exchange sorgt dafür, dass seit dem Jahreswechsel zahlreiche E-Mails nicht mehr zugestellt werden.

Ein trivialer Fehler

Der Grund dafür ist für den Softwarehersteller einigermaßen peinlich, handelt es sich doch um einen recht trivialen Fehler im Umgang mit Datentypen. Aber der Reihe nach: Auslöser des Vorfalls ist ein Update der "MS Filtering Engine", die unter anderem für das Erkennen von gerade kursierender Schadsoftware zum Einsatz kommt, und entsprechend regelmäßig – und automatisch – aktualisiert wird. Das ist auch an sich richtig so, immerhin können nur so Mail-Server rasch auf neue Bedrohungen reagieren.

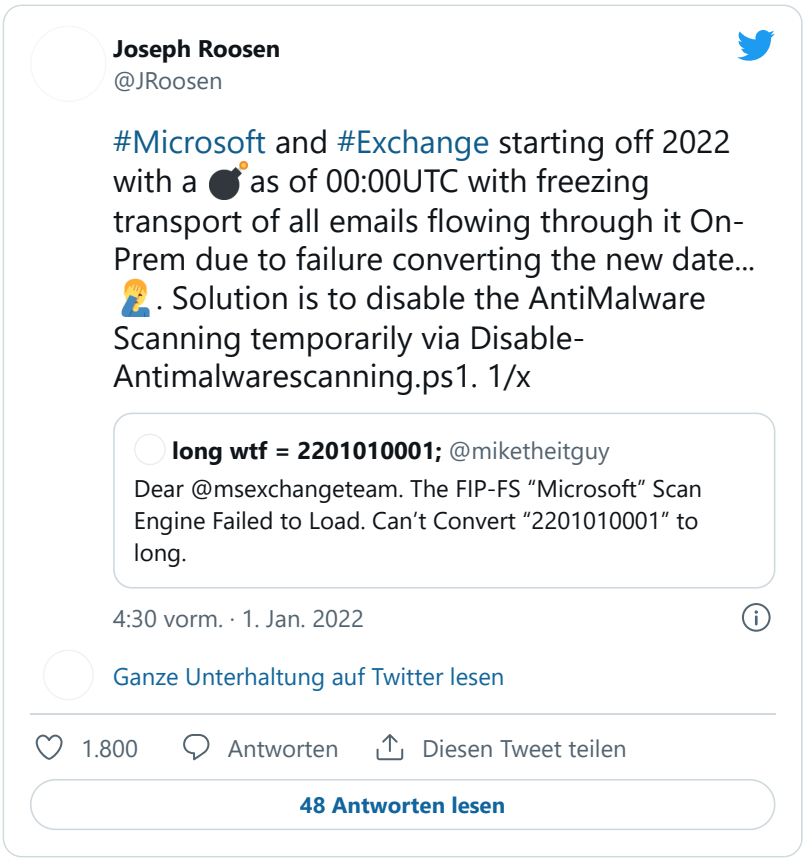
Diese "Filtering Engine" ist mit einer zehn Ziffern langen Versionsnummer versehen, die jeweils mit dem aktuellen Datum beginnt – und zwar zuerst mit der Jahreszahl. Das alleine wäre noch kein Problem, hätte nicht jemand bei Microsoft die – sehr schlechte – Idee gehabt, all das am Exchange-Server in einer Variable des Typs "int32" (mit Vorzeichen) zu speichern. Beträgt die maximale Größe dieses Datentyps doch "2.147.483.647".

Was nun passiert ist, dürfte an der Stelle einigen mit Programmiererfahrung bereits klar sein. Das aktuellste Update der "MS Filtering Engine" wurde kurz nach Mitternacht mit der Versionsnummer "2.201.010.001" ausgeliefert. Der Versuch, diese Version in die betreffende Variable zu schreiben, löste einen Fehler aus, weil

der neue Wert zu hoch ist, also außerhalb des Bereichs der erlaubten Zahlen liegt. Das Ergebnis: Die Filter funktionieren nicht mehr richtig, Mails bleiben hängen und werden nicht mehr korrekt verarbeitet.

Wer ist betroffen?

Von dem Fehler scheinen sämtliche Exchange-Versionen betroffen sein, allerdings mit einer wichtigen Einschränkung: Es betrifft nur selbst gehostete Varianten. Outlook-365-Kunden scheinen also nicht betroffen zu sein. Das klingt in der Theorie allerdings besser, als es in der Praxis oft ist. Denn wie der Systemadministrator Joseph Roosen in einem Twitter-Thread erklärt, haben viele Firmen hybride Lösungen im Einsatz, bei denen zwar Exchange selbst in der Cloud läuft, aber via dem "Centralized Mail Transport" die Mails über diverse Drittfilter geleitet werden – was nun nicht mehr funktioniert.



Der Vorfall kommt zur denkbar schlechtesten Zeit: Sind doch die IT-Abteilungen vieler Firmen derzeit äußerst schwach besetzt, da nach dem Neujahr auch noch ein Sonntag folgt. Dazu kommt, dass der Fehler in vielen Fällen nicht sofort auffallen dürfte. So kann es zum Teil dazu kommen, dass interne Mails sehr wohl zugestellt werden, externe aber nicht. Die Gefahr ist nun, dass über die Feiertage in vielen Firmen niemand was bemerkt und der lokale Speicherplatz langsam mit unabgearbeiteten Mails voll läuft – bis dann irgendwann überhaupt keine neuen Mails mehr akzeptiert werden, und die eingehenden Nachrichten verloren gehen.

Workaround

Zumindest gibt es einen relativ einfachen Workaround, wie Reddit-Nutzer herausgefunden haben [https://www.reddit.com/r/sysadmin/comments/rt91z6/exchange_2019_antimalware_bad_update/] . Die Deaktivierung des Anti-Malware-Filters führt dazu, dass Exchange wieder Mails zustellt und infolge auch den entstandenen Rückstau abarbeitet – vorausgesetzt wie gesagt, dass der Speicherplatz noch nicht voll gelaufen ist. Entsprechend sollten Sysadmins also rasch reagieren, um einen Datenverlust zu vermeiden. Eine Option ist dabei einfach das "Disable-AntiMalwareScanning.ps1"-Skript aus dem Skripte-Verzeichnis im Exchange-

Installationsverzeichnis auszuführen. Danach muss der Mail-Transport-Service noch neu gestartet werden, meist dauert es dann noch einige Minuten, bis die Maßnahme greift.

Ausmaß noch unklar

Eine offizielle Reaktion von Microsoft steht noch aus. Unklar bleibt vorerst auch, wie viele Firmen von dem Vorfall betroffen sind, da aber offenbar wirklich alle lokal gehosteten Exchange-Versionen samt vieler hybrider Lösungen betroffen sind, dürfte die Zahl groß sein. Die Fehlerbereinigung dürfte trivial sein, Microsoft muss nur den fürs Datum gewählten Datentyp ändern – etwa auf eine vorzeichenlose int32-Variable, was die Zahl der verfügbaren Werte verdoppeln würde. Freilich sollte man nicht vergessen, das Thema irgendwann grundlegender zu bereinigen, sonst stellt sich im Jahr 2043 das Problem nämlich erneut. (Andreas Proschofsky, 1.1.2022)

Link

Thread auf Reddit [https://www.reddit.com/r/sysadmin/comments/rt91z6/exchange_2019_antimalware_bad_update/]