Sehr geehrter Kunde,

Microsoft arbeitet weiter an der Verbesserung der Sicherheit von Active Directory und es werden Patches für alle supporteten Betriebssysteme zur Verfügung gestellt.
Die neuen Patches werden sich ab Juli 2023 auf ältere, nicht mehr supportete Betriebssysteme auswirken, was bedeutet, dass diese Computer und Server mit älteren Betriebssystemen nicht mehr in der Lage sein werden, Netlogon (NTLM) und Kerberos-Authentifizierung zu verwenden.

In diesem Fall werden für diese veralteten Systeme zentrale ActiveDirectory-Ressourcen nicht mehr erreichbar sein.

Microsoft wird Maßnahmen in zwei Bereichen ergreifen:

- Ab 11. Juli 2023: Durchsetzung der Versiegelung von NetLogon-RPC-Paketen (signiert und verschlüsselt). Voraussichtlicher Echtbetrieb am 18. Juli 2023.
- Ab dem 11. Oktober 2023: Durchsetzung der Kerberos-PAC-Header-Signatur und -Verifizierung. Voraussichtlicher Echtbetrieb ab dem 18. Oktober 2023.

Microsoft-bezogene Artikel:

So verwalten Sie die Netlogon-Protokolländerungen im Zusammenhang mit CVE-2022-38023:
https://support.microsoft.com/de-de/topic/kb5021130-so-verwalten-sie-die-netlogon-protokoll%C3%A4nderungen-im-zusammenhang-mit-cve-2022-38023-46ea3067-3989-4d40-963c-680fd9e8ee25

So verwalten Sie Kerberos-Protokolländerungen im Zusammenhang mit CVE-2022-37967
https://support.microsoft.com/de-de/topic/kb5020805-so-werwalten-sie-kerberos-protokoll%C3%A4nderungen-im-zusammenhang-mit-cve-2022-37967-997e9acc-67c5-48e1-8d0d-190269bf4efb

Dies bedeutet:

Microsoft hat eine neue Reihe von Sicherheitsverbesserungen veröffentlicht, die im kumulativen Rollup-Paket vom 22. November 2022 und später enthalten sind und die diese wichtigen Änderungen durchsetzen werden:

- Ermöglicht ein Auditing-Framework für das RPC-Sealing-Feature, das in den Betriebssystemen ab Windows XP vorhanden ist, und führt einen neuen Registrierungsschlüssel ein, mit dem das Feature deaktiviert, dieses Auditing aktiviert oder das Feature zusammen mit den vorherigen zugehörigen Registrierungsschlüsseln durchgesetzt werden kann.

- Ermöglicht eine völlig neue Funktion im Kerberos-Sicherheitsmechanismus zur Einführung einer Signatur des PAC-Headers. Diese neue Header-Anforderung kann über einen neu eingeführten Registrierungsschlüssel mit drei Modi gesteuert werden: Disabled, Audit, Enable the enforcement.

In mehreren Patches im Laufe des Jahres 2023 wird dieser Registrierungsschlüssel seine Funktionalitäten verlieren.

1. Es verschwindet die Fähigkeit, deaktiviert zu werden und der Audit-Modus wird durchgesetzt.
2. Es wird der Erzwingungsmodus aktiviert, aber er kann immer noch in den Audit-Modus zurückkehren.
3. Es wird der erzwungene Modus aktiviert und es sind **keine anderen Optionen verfügbar**!

Was ist betroffen?

Die von Microsoft unterstützten Betriebssysteme für diese Änderungen sind:

- Serversysteme: Windows Server 2012-Familie und aufwärts, wenn sie eine CU vom November 2022 oder später installiert haben. Für W2K8 bedeutet dies, dass ESU (Extended Security Updates Keys) erworben und installiert sein müssen und eine Verbindung zu Windows Update bestehen muss. Dieses Microsoft-Support Modell muss separat erworben und installiert sein. Ob dies in Ihrem Fall eine Möglichkeit darstellt, ist im Einzelnen zu prüfen.
- Clientsysteme Windows 10 und höher
- Alles, was älter ist, ist UNSUPPORTED und kann im Juli betroffen sein, wird aber ab Oktober definitiv nicht mehr in der Lage sein, Kerberos zu nutzen.

Veraltete Authentifizierungsmodule von Drittanbietern sind **UNSUPPORTED** (nicht unterstützt):

- Es werden keine veralteten Linux-Distributionen unterstützt
- Linux PAM Kerberos5 oder NTLM Module und Bibliotheken müssen auf dem neuesten Stand sein
- Speichergeräte (NAS/SAN) müssen auf dem neuesten Stand sein
- Jedes Netzwerkgerät, das AD-Authentifizierung nutzt, muss überprüft und/oder aktualisiert werden:
  - Netzwerkgeräte
  - Drucker
  - Handheld-Scanner
  - Sonstige Geräte

Was ist zu tun?

Um die Sicherheit und den Betrieb der IT-Anwendungen zu gewährleisten, müssen Sie so schnell wie möglich handeln und ein Upgrade durchführen.

Option 1: Upgrade des Betriebssystems (empfohlen)

Windows: Führen Sie ein Upgrade des Betriebssystems in Ihrem Bereich auf ein unterstütztes Betriebssystem durch.
Um einen langen Support-Zyklus zu gewährleisten, sollten Sie diese Betriebssysteme wählen:

- Windows Server 2019 o Windows Server 2022, in der Serverfamilie.*
- Windows 10 und Windows 11 in der Client-Familie.

* *Windows Server 2016 ist ebenfalls akzeptabel, aber bedenken Sie, dass der allgemeine Support bereits abgelaufen ist und der erweiterte Support bis zum 12. Januar 2027 läuft.*

Zu Nicht-Windows-Geräten, Linux oder jegliche Drittanbieter-Appliance:
Arbeiten Sie mit Ihrem Hardware- und Software-Anbieter zusammen, um sicherzustellen, dass er auf dem neuesten Stand ist und die Konfiguration den aktuellen AD-Anforderungen entspricht.

Option 2: Austausch oder Neuinstallation unter Verwendung derselben Maschine (sofern möglich)

Option 3: Außerbetriebnahme des Systems (falls Sie es nicht benötigen oder es nicht unerlässlich ist).

Option 4: Wenn keine der drei oben genannten Optionen durchführbar ist und mehr Zeit als die bis Oktober 2023 verbleibende Zeit für den Austausch von einzelnen Systemen benötigt wird, ist zu prüfen, wie das alte Betriebssystem noch einige Zeit weiterarbeiten kann (Trennen vom Active Dicrectory, arbeiten mit lokalen Anmeldeinformationen, Profiländerungen, manuellen Implementierungen usw.), bis Sie eine der oben genannten Optionen wählen können.

Wir wissen es zu schätzen, dass Sie dieses Problem ernst nehmen, denn es gilt zeitnah zu handeln.

Zusammenfassung:

Microsoft veröffentlicht zur Verbesserung der Sicherheit von Active Directory einige Patches für alle **supporteten** Betriebssysteme.

Ab 18. Oktober 2023 werden voraussichtlich für **veraltete** Betriebssysteme **zentrale ActiveDirectory-Ressourcen nicht mehr erreichbar sein**, was signifikante **Einschränkungen** für Ihren IT-Betrieb bedeuten kann.

Um die Sicherheit und den Betrieb Ihrer IT-Anwendungen zu gewährleisten, müssen Sie so schnell wie möglich handeln und ein Upgrade der veralteten Betriebssysteme durchführen.