Betriebssystem Windows Server 2012 / 2012 R2 End of Life (EoL)

Von der Veröffentlichung eines Produkts bis hin zum Ende des offiziellen Supports sind sämtliche Microsoft-Produkte einem definierten Lebenszyklus unterworfen. Am **10. Oktober 2023** endet der Support für Windows Server 2012/2012 R2. Danach gibt es dafür keine Software-Aktualisierungen und keine Sicherheitsupdates von Microsoft mehr.

Um was geht es?

Windows Server 2012 wurde am 30. Oktober 2012 und Windows Server R2 am 25. November 2013 bereitgestellt. Microsoft hat sich verpflichtet, dafür zehn Jahre Produktsupport zu bieten.
Am **10.Oktober 2023** läuft nun der Support von Windows Server 2012 und Windows Server 2012 R2 aus. **Ab diesem Tag sind weder technische Unterstützung noch Softwareupdates über Windows Update verfügbar**. Das gilt insbesondere für die wichtigen Sicherheitsupdates.

Die Produktlebenszyklen für Windows Betriebssysteme steht im folgenden Link: https://support.microsoft.com/de-ch/hub/4095338/microsoft-lifecycle-policy

Sobald der Support von Windows ausläuft, erhalten die Computer **keine Updates** mehr. Technisch gesehen läuft das Betriebssystem voll funktionsfähig und ohne Probleme weiter. Ein Betrieb von Computer mit Betriebssystemen, welche über das Support-Ende hinaus eingesetzt werden, ist jedoch ein erhöhtes Risiko für Unternehmen, da viele Sicherheitsrichtlinien nicht mehr eingehalten werden können und bei Problemfällen keine Unterstützung mehr gewährt wird. Alle nach diesem Zeitpunkt entdeckten Sicherheitslücken werden nicht mehr geschlossen sind potenzielle Schwachstellen. Diese Schwachstellen werden oft im Internet veröffentlicht und können zu einer Attacke oder ausführen von Malware ausgenutzt werden.

Wie ist die Bedrohungslage auf meiner Anlage?

Ein Server mit den genannten Betriebssystemen läuft störungsfrei weiter. Solange keine Malware, infizierte Computer, infizierte USB-Sticks oder Hacker auf die bestehende Infrastruktur zugreifen können, passiert nichts. Sollte es trotzdem gelingen, wird die Sicherheitslücke im Betriebssystem ausgenützt. Es besteht die Gefahr, dass gefährdete Computer mit Viren verseucht oder verschlüsselt werden. Auch ist es möglich, dass ein Hacker die Kontrolle über die Systeme übernimmt oder manipuliert.

Es unterliegt dem verantwortlichen Betreiber das Risiko abzuschätzen, um die Vertraulichkeit, Verfügbarkeit und Integrität der Informationssicherheit zu bewahren.

Betreiber einer kritischen Infrastruktur wird durch die Verbände (SVGW, VSE und VSA) empfohlen, den IKT-Minimalstandard einzuhalten. Dabei geht es um den folgenden Punkt:
„**Aktualisieren Sie Ihre Software regelmässig**“

Wir helfen Ihnen gerne weitere Fragen zum IKT-Minimalstandard zu beantworten und die richtigen Massnahmen zu bestimmen.

Wie kann ich mich dagegen schützen?

Betroffene Unternehmen sollten bereits jetzt mit der Planung beginnen, wie die auslaufenden Betriebssysteme und Computer ersetzt werden sollen. Es stehen verschiedene Ansätze zur Verfügung.

Setzen Sie sich mit uns in Verbindung, damit wir Ihnen eine optimale Lösung anbieten können.

Für alle **aktuellen** Betriebssysteme bieten wir folgende Module an:

Update Service
Mit dem Update Service übernimmt Rittmeyer das Testen und Installieren der Patches und Hotfix von Microsoft. Besonders für das Betriebssystem wird empfohlen, in regelmässigen Abständen alle verfügbaren Sicherheitsupdates zu installieren, um bekannte Sicherheitslücken zu schliessen.

IKT-Security Assessment
Sollte Sie sich Gedanken über die allgemeine Sicherheit machen, unterstützen wir Sie gerne mit unseren zertifizierten IKT-Minimalstandard und ISO-27001-Security-Experten. Diese können potenzielle **Schwachstellen** und **Bedrohungen** frühzeitig erkennen. Dazu erfassen durch eine IST-Analyse den bestehenden IKT-Schutz und können danach einen individuellen und strukturierten IT-Grundschutz mit entsprechenden **Schutzmassnahmen** erstellen.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity