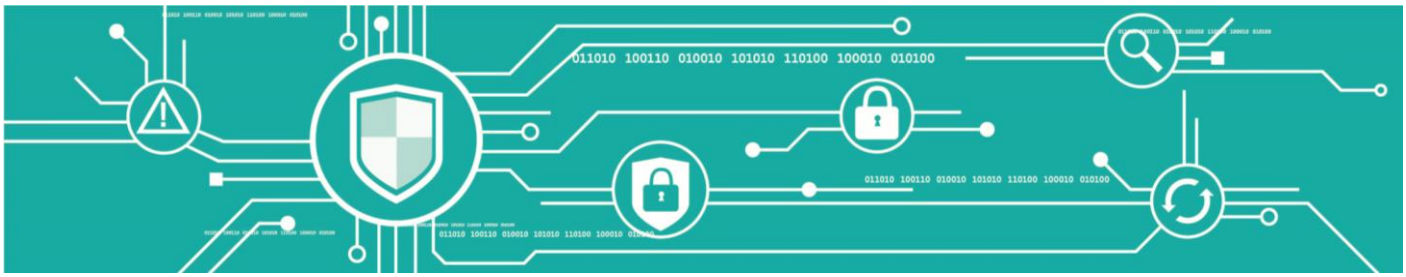

Windows End of Support (EoS)

Im Januar 2020 endet der Support für Windows 7 und Windows Server 2008/2008 R2. Danach gibt es keine Software-Aktualisierungen und keine Sicherheitsupdates von Microsoft mehr.

Um was geht es?

Windows 7 und Windows Server 2008/2008 R2 wurde am 22. Oktober 2009 bereit-gestellt. Microsoft hat sich verpflichtet, dafür zehn Jahre Produktsupport zu bieten.
Am **14. Januar 2020** läuft der Support von Windows 7, Windows Server 2008 und Windows Server 2008 R2 aus. **Ab diesem Tag sind weder technische Unterstützung noch Softwareupdates über Windows Update verfügbar**. Das gilt insbesondere für die wichtigen Sicherheitsupdates.

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

Sobald der erweiterte Support von Windows ausläuft, erhalten die Computer keine Up-dates 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 Sicherheits-Richtlinien nicht mehr eingehalten werden können und bei Problemfällen keine Unterstützung mehr gewährt wird. Alle nach diesem Zeitpunkt entdeckten Sicherheitslücken werden nicht mehr gelöst und können zu Schwachstellen führen. 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 oder Laptop mit den genannten Betriebssystemen laufen störungsfrei weiter. Solange keine Malware, infizierte Computer, infizierte USB-Sticks oder Hacker über das Netzwerk auf die bestehende Infrastruktur zugreifen können, passiert nichts. Sollte es jedoch trotzdem gelingen, wird die Sicherheitslücke im Betriebssystem gnadenlos ausgenützt. Es besteht die Gefahr, dass sämtliche 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 und VSE) empfohlen, dem IKT-Minimalstandard (<5000 Haushalte) sowie IKT-Standard einzuhalten. Dabei geht es um den folgenden Punkt: „Aktualisieren Sie Ihre Software regelmässig“

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

Wie kann ich mich dagegen schützen?

Aus diesem Grund sollten Unternehmen bereits jetzt mit der Planung beginnen, wie die auslaufenden Computer ersetzt werden sollten. 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.

Backup Service
Das Daten-Backup von Rittmeyer ist eine vollständige, Cloudintegrierte Lösung. Gespeichert werden dabei nicht nur die Leitsystemdaten, wie beim manuellen Backup üblich, sondern auch die jeweilige Anlagekonfiguration mit allen Einstellungen. Diese Sicherung ist immer aktuell, da sie täglich durchgeführt wird.

ICT-Security
Sollte trotzdem etwas passieren, unterstützen wir Sie gerne mit unseren zertifizierten ISO-27001-Security-Experten.

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