



## **Kennen Sie sich aus? -**

### **Supportende zum 13.6.2023: Diese Version von Windows 10 kann zum Problem werden**

**Computer, sprich Hard- und Software, sind nicht für die Ewigkeit gemacht. Gerade Betriebssysteme kommen heutzutage immer schneller in die Jahre, unter anderem weil es neue Versionen gibt, die etwa Cyberkriminellen das Leben schwer machen sollen. So kommt es, dass demnächst auch der Support für eine Betriebssystemversion von Windows 10 endet.**

#### **Windows 10 mehr und mehr Geschichte**

Klar ist: Support ist teuer. Um Softwareprodukte sicher zu gestalten, ist eine fortlaufende Aktualisierung durch den Hersteller notwendig. Nur so können Sicherheitslücken geschlossen und Risiken für den Nutzer auf ein Minimum reduziert werden. Dieser Support ist für den Hersteller mit hohen Kosten verbunden. Denn er muss ständig Updates und Sicherheitspatches entwickeln und zur Verfügung stellen. Nach Ablauf des Produktlebenszyklus und mit der Einführung von Nachfolgeprodukten, etwa Windows 11, ist dieser Support für den Hersteller meist nicht mehr wirtschaftlich. Deshalb endet er irgendwann.

#### **Für diese Version besteht jetzt Handlungsbedarf**

Keine Angst: Windows 10 wird nicht in den nächsten Wochen und Monaten von der Bildfläche verschwinden. Konkret wird der Support für eine bestimmte Windows-10-Version eingestellt. Es handelt sich um die Version 21H2. Für diese Version endet der Support zum 13.6.2023. Das bedeutet: Werden nach diesem Zeitpunkt Sicherheitslücken entdeckt, etwa durch Cyberkriminelle, wird Microsoft nichts mehr unternehmen, um diese zu schließen. Das heißt in der Folge auch für Ihr Unternehmen: Je länger diese veraltete Version in Ihrem Unternehmen im Einsatz ist, desto größer wird das Risiko, dass Cyberkriminelle eine Sicherheitslücke ausnutzen können.

#### **Denken Sie an Datenschutzverstöße und Bußgelder**

**Vorsichtig sollten Sie mit Aussagen umgehen wie z. B. „Da wird schon nichts passieren“ oder „Unser Unternehmen ist für Cyberkriminelle nicht interessant“.**

**Auch wenn sich nur „Anfänger“ unter Cyberkriminellen an Ihrem Unternehmen versuchen, können diese erheblichen Schaden anrichten.**

**Ohne Daten zu verschlüsseln oder Lösegeld zu erpressen, können diese trotzdem große Schwierigkeiten mit der Folge erheblichen Aufwands für die Bereinigung und Absicherung der Systeme verursachen.**

#### **Außerdem:**

**Versäumt es Ihr Unternehmen, die nötigen Anpassungen vorzunehmen und beispielsweise auf ein neueres bzw. mit Sicherheitsupdates versorgtes Betriebssystem umzustellen, liegt in der Regel ein Verstoß gegen Art. 32 Datenschutz-Grundverordnung (DSGVO) vor.**

**Ihr Unternehmen hat keine risikoangemessenen – und zumutbaren – Schutzmaßnahmen ergriffen. Und das kann wiederum teuer werden. Gemäß Art. 83 Abs. 4 Buchst. a DSGVO droht ein schmerzhaftes Bußgeld.**

#### **Haben Sie auch ein Auge auf wenig genutzte Geräte**

Überlegen Sie, wo es Geräte geben kann, die unter Umständen durchs Raster fallen können und bei denen ein veraltetes Betriebssystem installiert sein kann. Denken Sie hier etwa an Ersatz- und Ausleihgeräte, die nur ab und an im Einsatz sind. Ähnlich ist es mit Präsentationsrechnern, etwa für Tagungen, Schulungen oder Messestände.

## Checken Sie Ihre Windows-Version

Um die Situation besser abschätzen zu können, können Sie zunächst einmal bei verschiedenen Computern schauen, welche Windows-Version installiert ist.

Das ist kein Hexenwerk. Gehen Sie folgendermaßen vor:

Drücken Sie die Windows-Taste + R und geben Sie „winver“ ein.

Dann werden Ihnen das Betriebssystem und dessen Version angezeigt.



Wird das Betriebssystem tatsächlich noch verwendet, gilt es, einen kühlen Kopf zu bewahren.

Im Vordergrund muss stehen, schnellstens eine Lösung zu erarbeiten.

Dabei ist die Lösung gar nicht so kompliziert:

Es muss auf eine Version aktualisiert werden, für die es noch Support gibt.

### Schauen Sie auch in Richtung Windows 11

Windows 10 wird generell nur bis 14.10.2025 mit Updates versorgt.

Danach ist ein Wechsel zu Windows 11 unerlässlich. Das kann ein größeres Projekt werden.

Doch auch bei Windows 11 gibt es bald veraltete Versionen. Der Support für Windows 11 Version 21H2 endet am 10.10.2023. Entsprechende Informationen finden Sie hier: <https://t1p.de/c9m7>

## Bedenken Sie immer die möglichen Gefahren

Cyberkriminelle wie Hacker, die sich Zugriff auf den „Datenschatz“ Ihres Unternehmens verschaffen; Einschleusen von Schadsoftware wie z. B. von Verschlüsselungstrojanern, um Lösegeld zu erpressen; Zugriff auf und Diebstahl von schützenswerten personenbezogenen Daten und Unternehmensinformationen; Auslösen der Meldepflicht gegenüber der Datenschutzaufsichtsbehörde (Art. 33 DSGVO) und ggf. die Pflicht zur Information aller Betroffenen, was auch zur Negativpresse führen dürfte (Art. 34 DSGVO).

## Nutzen Sie die fachliche Kompetenz Ihres IT-Service und vor allem fragen Sie nach.

Gibt es tatsächlich ein „Versionsproblem“, sollten Sie die Kollegen der IT-Abteilung um einen Vorschlag bitten, wie das Problem schnellstmöglich behoben wird.

Empfehlen Sie, einen Plan für das Installieren erforderlicher Updates zu erstellen, und schauen Sie, ob das aus Ihrer Sicht passt.

Achten Sie insbesondere darauf, dass idealerweise bis zum Supportende eine neuere Version auf den Computern installiert ist.

Ein Plan hat für Sie auch folgenden Vorteil:

Sie haben eine Grundlage, um einen Soll-Ist-Abgleich zu machen.

Prüfen Sie beispielsweise nach Ablauf der festgelegten Termine, ob die Umsetzung der betreffenden Maßnahmen tatsächlich erfolgt ist.

Ist das nicht der Fall, sollten Sie nachhaken.

Benötigen Sie weitere Unterstützung oder haben Sie Fragen, melden Sie sich bitte.

Ihr Datenschutzbeauftragter

Detlef Riese

