Whitepaper: Windows 10 Support-Ende 2025 – Was KMU-Geschäftsführer wissen müssen

Hintergrund: Supportende von Windows 10 am 14. Oktober 2025

Microsoft wird den **Support für Windows 10** am 14. Oktober 2025 offiziell beenden. Ab diesem Datum erhalten Windows-10-Systeme **keine Sicherheitsupdates, Fehlerbehebungen oder technischen Support** mehr. Windows 10, das im Juli 2015 erschien, blickt damit auf einen typischen 10-Jahres-Lebenszyklus zurück[1]. Schon im Oktober 2020 endete der sog. „Mainstream-Support" (mit Funktionsupdates), und am 14. Oktober 2025 läuft nun auch der erweiterte Support endgültig aus.

Die **Bedeutung dieses End-of-Life (EOL)** ist erheblich: Weltweit und auch in Deutschland ist Windows 10 noch weit verbreitet. Allein in Deutschland liefen Ende 2024 rund **32 Millionen PCs** mit Windows 10 – etwa **78 % Marktanteil** unter Desktop-Betriebssystemen[2]. IT-Experten warnen, dass das Weiternutzen von Windows 10 ohne Updates ein potenzielles „Security-Fiasko" nach sich ziehen könnte[3]. Obwohl Windows 10-Geräte technisch weiterfunktionieren, nimmt die Verwundbarkeit solcher Systeme ab Oktober 2025 rapide zu. Es ist daher für Unternehmen wichtig zu verstehen, welche Konsequenzen das Supportende hat und welche Handlungsoptionen bestehen.

Inhalt

[1] security-insider.de
[2] security-insider.de
[3] heise.de

Risiken für kleine und mittlere Unternehmen (KMU)

Ohne offiziellen Support wird Windows 10 in kurzer Zeit zu einem **Sicherheitsrisiko**. Insbesondere KMU, die oft begrenzte IT-Ressourcen haben, sind von folgenden Risiken betroffen:

- **Ungeschlossene Sicherheitslücken:** Nach dem Supportende werden neu entdeckte Schwachstellen in Windows 10 *nicht mehr durch Updates behoben*. Damit bleiben bekannte Lücken im System offen und können von Cyberkriminellen ausgenutzt werden. Das BSI warnt, dass *Angreifer Tür und Tor geöffnet* sind, wenn Windows 10 weiterhin ohne Updates betrieben wird[4]. Infolgedessen steigt das Risiko erfolgreicher Malware-Infektionen (z. B. Ransomware) mit jedem Tag, an dem keine Sicherheitsupdates mehr eingespielt werden.

- **Verstöße gegen Compliance und Datenschutz:** Unternehmen, die veraltete und unsichere Systeme einsetzen, könnten **gegen gesetzliche Datenschutz- und Compliance-Vorgaben verstoßen**. In der EU schreibt etwa die DSGVO vor, geeignete technische Schutzmaßnahmen zu treffen – der Betrieb eines nicht mehr gepatchten Betriebssystems kann als Verletzung der IT-Sicherheitspflicht gewertet werden. Dies *kann hohe Bußgelder* nach sich ziehen. Microsoft weist ebenfalls darauf hin, dass Organisationen mit Windows 10 nach dem EOL *Schwierigkeiten haben könnten, regulatorische Compliance-Anforderungen zu erfüllen*[5].

- **Versicherungsdeckung in Gefahr:** Viele KMU haben Cyber-Versicherungen abgeschlossen, die im Schadensfall finanzielle Hilfe leisten. Doch die **Weiternutzung von Windows 10 nach Supportende kann den Versicherungsschutz gefährden**. Versicherer verlangen oft, dass Sicherheitsupdates zeitnah installiert und Altsysteme abgelöst werden – dies ist als Obliegenheit in den Versicherungsbedingungen verankert. Ein Verstoß (z. B. durch den Betrieb eines nicht mehr unterstützten Windows 10) *gilt als Obliegenheitsverletzung* und kann dazu führen, dass Ansprüche gekürzt oder ganz abgelehnt werden. Im Klartext: Wurde ein Cyberangriff durch eine ungepatchte Windows-10-Lücke begünstigt, könnte der Versicherer die Zahlung verweigern. Zwar prüfen Versicherer im Einzelfall eine Kausalität, aber das Risiko für KMU ist real. Branchenexperten raten betroffenen Firmen deshalb dringend zu rechtzeitigen Schutzmaßnahmen oder zu einer Absprache mit dem Versicherer (z. B. Nutzung von Extended Support oder isolierte Offline-Nutzung)[6].

- **Inkompatibilitäten bei Software und Hardware:** Nach 2025 wird neue Anwendungssoftware möglicherweise **Windows 10 nicht mehr unterstützen**. Hersteller fokussieren sich auf aktuelle Betriebssysteme; wichtige Fachanwendungen könnten unter Windows 10 künftig nicht mehr korrekt laufen oder installierbar sein. Ähnliches gilt

[4] BSI
[5] blogs.windows.com
[6] procontra-online.de

für **Hardware-Treiber**: Neue Peripheriegeräte (Drucker, Scanner, etc.) erhalten eventuell keine Treiber mehr für Windows 10. Ein KMU riskiert somit Funktionsstörungen, wenn es neue Software oder Geräte in einer veralteten Windows-Umgebung einsetzen will.

- **Kein Hersteller-Support & mögliche Ausfallzeiten:** Ohne Support steht Microsoft für Windows 10-Probleme *nicht mehr zur Verfügung*. Bei Störungen oder Systemfehlern muss das Unternehmen selbst Lösungen finden oder auf Drittanbieter-Support zurückgreifen. Dies erhöht die Gefahr längerer **Betriebsausfälle**. Kombiniert mit den Sicherheitsrisiken kann es im Worst Case zu Systemabstürzen oder erfolgreichen Angriffen (z. B. durch Ransomware) kommen, die **Datenverlust** oder Stillstand wichtiger Geschäftsprozesse verursachen[7].

Fazit der Risiken: Ein unbeaufsichtigtes Weiterlaufen von Windows 10 nach dem 14. Oktober 2025 stellt ein erhebliches Geschäftsrisiko dar – von **IT-Sicherheitsvorfällen** über **Rechts- und Compliance-Probleme** bis hin zu **finanziellen Schäden** durch Ausfälle oder verlorene Versicherungsleistungen. Behörden wie das BSI und Branchenverbände warnen eindringlich davor, Windows 10 nach seinem Supportende produktiv weiter einzusetzen[8].

Microsoft-Optionen nach dem Supportende von Windows 10

Microsoft bietet betroffenen Kunden mehrere offizielle Handlungsoptionen, um die Zeit *nach* dem Windows-10-Supportende zu bewältigen. Im Wesentlichen stehen drei Ansätze im Microsoft-Ökosystem zur Verfügung:

1. Upgrade auf Windows 11

Der primäre empfohlene Weg ist das **Upgrade auf Windows 11**, den offiziellen Nachfolger von Windows 10. Windows 11 wird von Microsoft voraussichtlich *bis in die 2030er-Jahre* unterstützt und erhält regelmäßige Updates, Sicherheitsaktualisierungen und neue Funktionen. Ein Umstieg bietet somit langfristige Sicherheit und moderne Features. Microsoft selbst rät allen Windows-10-Nutzern, möglichst bald kostenlos auf Windows 11 zu wechseln.

Hardware-Anforderungen: Wichtig zu beachten ist, dass Windows 11 **höhere Systemvoraussetzungen** hat, die nicht jeder ältere PC erfüllt. Insbesondere verlangt Windows 11 unter anderem:

- **64-Bit-fähiger Prozessor** (mind. 2 Kerne, 1 GHz) aus relativ aktueller Generation, z. B. Intel Core der **8. Generation** (ca. ab 2017) oder AMD Ryzen **ab 2. Generation (Zen +)**. Ältere CPUs werden offiziell nicht unterstützt.
- **Trusted Platform Module (TPM) 2.0** als Sicherheitschip und UEFI-Firmware mit Secure Boot. (Nahezu alle Business-PCs ab ~2016/2017 haben TPM 2.0, aber in manchen Fällen muss es im BIOS aktiviert werden.)
- Mindestens **4 GB RAM** und **64 GB Speicher**, sowie ein Display mit mind. 9 Zoll und 720p-Auflösung (für Laptops).

[7] verbraucherzentrale.de
[8] heise.de

Viele Windows-10-Rechner, die nur wenige Jahre alt sind, *scheitern dennoch an diesen hohen Anforderungen*. Microsoft hat klargestellt, dass einige ältere Geräte – selbst wenn sie noch einwandfrei laufen – **nicht auf Windows 11 aufrüstbar** sind und ggf. ersetzt werden müssen[9]. Diese strikten Hardware-Vorgaben führten bei manchen Nutzern zu Frust, insbesondere wenn regelmäßige Hardwareanschaffungen finanziell schwierig sind.

Vorteile eines Upgrades: Windows 11 gilt als das **sicherste Windows** aller Zeiten, da es moderne Sicherheitsfeatures (TPM 2.0, Virtualisierung-basierte Sicherheit, Smart App Control etc.) *standardmäßig aktiviert* mitbringt[10]. Neue Windows 11-PCs verzeichnen bis zu **62 % weniger Sicherheitsvorfälle** im Vergleich zu Windows 10-Systemen. Außerdem bietet Windows 11 Leistungsverbesserungen (schnellere Updates, bessere Performance) und Produktivitätsfunktionen wie ein modernes UI, Snap-Layouts fürs Multitasking und künftig integrierte KI-Features (z. B. Windows Copilot). Für die meisten Unternehmen stellt Windows 11 somit die **zukunftssicherste Plattform** dar. Ein rechtzeitiges Upgrade vor Oktober 2025 erspart zudem die Kosten für etwaige Übergangslösungen (siehe ESU) und verhindert hektische Umstellungen unter Zeitdruck.

Nachteile/Beschränkungen: Hauptnachteil sind die erwähnten **Hardwarekosten**, falls bestehende PCs nicht kompatibel sind. KMU müssen unter Umständen in neue Geräte investieren oder Upgrades der Komponenten prüfen. Hinzu kommt ein **Planungsaufwand**: Applikationen und Geräte im Unternehmen sollten vorab auf Kompatibilität mit Windows 11 getestet werden. Gegebenenfalls sind Updates für Fachsoftware nötig. Außerdem erfordert das Upgrade *Schulung* der Mitarbeiter bezüglich kleiner Änderungen in Bedienung und Oberfläche, um Produktivitätsverluste zu vermeiden. Trotz dieser Hürden gilt der direkte Umstieg auf Windows 11 als von Microsoft bevorzugte und langfristig günstigste Lösung.

2. Extended Security Updates (ESU) für Windows 10

Für Organisationen, die nicht sofort auf Windows 11 wechseln können, bietet Microsoft ein **Extended Security Updates (ESU)**-Programm an. Über ESU können zahlende Kunden auch *nach* Oktober 2025 noch **wichtige Sicherheitsupdates für Windows 10** erhalten[11]. Dieses Programm war bereits beim Supportende von Windows 7 im Einsatz und wird nun für Windows 10 fortgeführt.

Funktionsweise: ESU stellt **keine neuen Features oder Qualitätsupdates** bereit, sondern lediglich Patches für kritische Sicherheitslücken. Die Updates werden über die normalen Update-Kanäle ausgeliefert, jedoch *nur an Geräte mit gültiger ESU-Lizenz*. Voraussetzung ist, dass auf dem PC Windows 10 Version 22H2 installiert ist (ältere Versionen werden nicht unterstützt).

Kosten und Laufzeit: ESU-Lizenzen sind kostenpflichtig und **pro Gerät** zu erwerben. Der Preis steigt mit jedem Jahr deutlich an, um den Anreiz zum Umstieg nicht zu schmälern. Konkret nennt Microsoft folgende Preismodelle für Geschäfts- und Volumenlizenzkunden: **61 USD pro Gerät im 1. Jahr**, der Preis *verdoppelt sich* im 2. Jahr auf 122 USD und erneut im 3. Jahr auf 244 USD. Maximal werden 3 Jahre ESU angeboten (bis Oktober 2028). **Hinweis:** Kauft ein Unternehmen erst im 2. Jahr ein, müssen *rückwirkend* die Gebühren für Jahr 1 mitbezahlt werden– die Kosten sind also **kumulativ**, unabhängig vom Einstiegszeitpunkt. Für

[9] pcwelt.de
[10] blogs.windows.com
[11] learn.microsoft.com

Privatanwender (Windows 10 Home) gibt es ein separates Angebot (30 USD/Jahr), das für KMU jedoch weniger relevant ist.

Diese Kosten gelten für die meisten Unternehmen über Volumenlizenz- oder Cloud Solution Provider (CSP) Programme. Ein **Mindestabnahmevolumen** gibt es jedoch nicht – bereits **eine einzelne Lizenz** kann bezogen werden.

Cloud-Vorteil: Ein wichtiger Aspekt für Unternehmen mit Cloud-Strategie: **Für Windows-10-Instanzen, die in bestimmten Microsoft-Cloud-Diensten laufen, ist ESU kostenfrei**. Microsoft berechnet *keine zusätzlichen Gebühren* für Sicherheitsupdates, wenn Windows 10 als virtuelle Maschine in folgenden Umgebungen betrieben wird:

- **Windows 365 Cloud-PC** (Cloud-PCs mit Windows 10)
- **Azure Virtual Desktop** (AVD)
- Azure-VMs und verwandte Azure-Dienste (Azure Virtual Machines, Dedicated Host, Azure VMware Solution etc.)

Ebenso sind **Windows-10-Geräte, die auf einen Windows 365 Cloud-PC zugreifen**, automatisch für ESU berechtigt, solange ein aktives Windows 365-Abonnement vorliegt. Für KMU bedeutet dies: Wer z. B. virtuelle Desktops in Azure nutzt oder auf Cloud-PCs setzt, kann **bis 2028 ohne Zusatzkosten Windows 10 sicher weiterbetreiben**. Dieser Vorteil unterstreicht Microsofts Strategie, Kunden Richtung Cloud-Services zu bewegen.

Bewertung ESU: Das ESU-Programm bietet Unternehmen **Zeitgewinn**. KMU, die es nicht schaffen, bis Oktober 2025 alle Systeme auf Windows 11 umzustellen (etwa wegen Budgetrestriktionen oder inkompatibler Spezialsoftware), können über ESU zumindest die **Sicherheit für bis zu 36 Monate verlängern**. Dies kann Teil einer Übergangsstrategie sein, um Migrationen *schrittweise* umzusetzen, ohne das Risiko ungepatchter Systeme einzugehen. Microsoft betont jedoch, dass ESU eine **temporäre Lösung** ist – spätestens 2028 ist endgültig Schluss mit Windows 10. Unternehmen sollten ESU daher als „Gnadenfrist" nutzen, *um die Windows-11-Migration geordnet nachzuholen*, nicht um Windows 10 auf ewig beizubehalten.

Nachteile und Kostenabwägung: Die **laufenden Kosten** für ESU können erheblich sein, besonders im 3. Jahr. Beispiel: Für 50 PCs summiert sich ESU über drei Jahre auf über 50.000 USD. Dieses Budget könnte stattdessen in neue Hardware mit Windows 11 fließen. Zudem beseitigt ESU zwar Sicherheitsrisiken, *aber keine funktionalen Einschränkungen*: Windows 10 bleibt ein altes System ohne neue Features oder Support. Probleme, die nicht sicherheitskritisch sind, werden im Rahmen von ESU nicht behoben. Auch **technischer Produktsupport** durch Microsoft ist in ESU *nicht* enthalten– es werden wirklich nur Updates geliefert. ESU eignet sich daher primär als **Notlösung**, um unverzichtbare Windows-10-Geräte noch begrenzte Zeit betreiben zu können (z. B. für Legacy-Anwendungen), während parallel die Umstellung vorbereitet wird. Unternehmen sollten genau abwägen, für welche Geräte sich ESU lohnt und möglichst einen konkreten **Exit-Plan bis 2028** haben.

3. Cloud-basierte Windows-Lösungen: Windows 365 & Azure Virtual Desktop

Eine weitere offizielle Option im Microsoft-Umfeld sind **Cloud-PC- und Virtual-Desktop-Lösungen**, speziell **Windows 365** und **Azure Virtual Desktop (AVD)**. Diese Ansätze ermöglichen es, Windows auf moderner Hardware in der Cloud laufen zu lassen und auf bestehenden (auch

älteren) Endgeräten nur noch als Stream bereitzustellen. Damit können KMU *sofort* auf eine aktuelle Windows-Umgebung umsteigen, **ohne alle Arbeitsplatzrechner gleichzeitig austauschen zu müssen**.

Windows 365 (Cloud-PC): Windows 365 ist ein von Microsoft angebotener **Cloud-PC-Dienst**. Hier erhält jeder Nutzer einen *persönlichen Windows-Cloudrechner*, der in einem Microsoft-Rechenzentrum läuft. Auf diesen virtuellen PC kann von nahezu jedem Endgerät (egal ob alter Windows-10-PC, Thin Client oder Tablet) per Internet zugegriffen werden. Technisch wird meist Windows 11 als Betriebssystem im Cloud-PC eingesetzt, sodass der Nutzer ein vollwertiges Windows-11-Desktop-Erlebnis hat – selbst wenn sein lokaler Rechner dafür ungeeignet wäre[12]. **Sicherheit und Updates** werden zentral in der Cloud gepflegt; der Cloud-PC erhält automatisch alle Aktualisierungen. **Extended Security Updates** für ein evtl. auf Windows 10 basierendes Cloud-System sind, wie oben erwähnt, bereits im Service inbegriffen. Für Unternehmen im **Healthcare-, Finanz- oder Rechtsbereich** kann Windows 365 besonders attraktiv sein, da Cloud-PCs zentral gemanagt, gegen Datenabfluss geschützt (kein lokaler Datenspeicher) und mit allen aktuellen Security-Features ausgestattet sind. Microsoft bewirbt Windows 365 als **kosteneffiziente und nachhaltige Alternative** zum Device-Tausch, um Windows 11 bereitzustellen. Die Abrechnung erfolgt pro Benutzer/Monat, abhängig von der gewählten Cloud-PC-Leistung (CPU, RAM, Speicher).

Azure Virtual Desktop (AVD): Azure Virtual Desktop ist eine **Cloud-Infrastruktur für virtuelle Desktops und Anwendungen** in Microsoft Azure. Im Unterschied zu Windows 365, das ein vollständig verwalteter SaaS-Dienst pro Nutzer ist, bietet AVD mehr Flexibilität: Unternehmen können in Azure eigene VM-Hosts aufsetzen und dort entweder **persönliche Desktops** für Nutzer oder **pools von Desktops/Apps** bereitstellen. AVD erlaubt z. B. mehrere Nutzer pro VM (via Windows 10/11 Multi-Session) und Integration ins Firmen-Netzwerk. Für KMU ohne eigene IT-Abteilung ist AVD jedoch komplexer zu administrieren als Windows 365. In vielen Fällen arbeiten KMU daher über einen IT-Dienstleister mit AVD. Aus Anwendersicht erreicht man sein *Cloud-Windows* bei AVD ebenfalls über Internet mittels Remote-Desktop-Client. **Lizensiert** wird AVD über bestimmte Microsoft 365 Lizenzen oder Azure-Nutzungsgebühren. *Auch hier gilt:* Wenn weiterhin Windows 10 als OS in der Azure-VM genutzt würde, fallen dank ESU-Cloud-Privilege keine Updatekosten an. Oft wird man aber gleich Windows 11 als virtuelles Desktop-OS wählen.

Vor- und Nachteile der Cloud-Option: Beide Cloud-Lösungen ermöglichen einen **schnellen Umstieg auf ein modernes Windows**, ohne upfront in viele neue PCs investieren zu müssen. Ein altes Windows-7/8/10-Gerät kann weiter als *Thin Client* dienen, da die Rechenarbeit in der Cloud passiert. Das ist besonders nützlich, um kurzfristig Sicherheitsrisiken zu eliminieren: Statt ESU zu bezahlen, könnte ein KMU z. B. temporär Windows 365-PCs mieten, bis die Hardwareerneuerung umgesetzt ist. Die **IT-Sicherheit** im Cloud-Szenario ist hoch, da Microsoft die Umgebung aktuell hält und Cloud-PCs in der Regel besser gegen Angriff exponiert sind als lokale Alt-PCs. Zudem erleichtern Cloud-Desktops das **Mobile Arbeiten** und Homeoffice, da der Desktop von überall gleich erreichbar ist.

Es gibt jedoch wichtige **Aspekte zu bedenken**: Erstens benötigen Cloud-PCs und virtuelle Desktops eine **stabile, schnelle Internetanbindung**. Wenn die Verbindung ausfällt oder zu langsam ist, können Mitarbeiter nicht effizient arbeiten. Zweitens entstehen **laufende Kosten pro Nutzer**, die sich über Jahre durchaus mit Hardwareinvestitionen vergleichen müssen. Je

[12] blogs.windows.com

nach Tarif und Anforderungen (Leistung, Speicher) kann Windows 365 bspw. ca. 20–40 € pro Monat und Nutzer kosten. Über 3 Jahre summiert sich das pro Nutzer ähnlich wie ein neuer PC – allerdings verteilt und mit inkludiertem Management. Drittens müssen Unternehmen sich mit Fragen der **Datenhaltung und Compliance** auseinandersetzen: Die Daten liegen in der Cloud (in europäischen Rechenzentren verfügbar), was jedoch mit dem richtigen Anbieter (Microsoft) und Verträgen wie dem Data Processing Agreement in der Regel konform zu DSGVO etc. gestaltet werden kann. Viertens ist ein *Wechsel zur Cloud* auch ein organisatorischer Wandel – man benötigt ggf. neue Konzepte für IT-Support, Mitarbeiterschulungen in Bezug auf Cloud-Desktops und eventuell Anpassungen bei Peripheriegeräten (z. B. lokale Drucker oder USB-Geräte in der Cloud nutzen).

Zusammengefasst: Cloud-Lösungen wie Windows 365 und AVD sind ein **modernes Ausweichmodell** für Unternehmen, die schnell weg von Windows 10 müssen oder eine flexible Infrastruktur bevorzugen. Sie **überbrücken Hardware-Engpässe** und können teils sogar langfristig klassische PCs ersetzen. Dennoch sind sie kein Allheilmittel: Die individuellen Anforderungen (Kosten, Internet, Datenschutz) eines KMU entscheiden, ob diese Option sinnvoll ist. Microsoft offeriert zumindest zeitlich begrenzte Rabatte, um den Einstieg zu erleichtern (z. B. 20 % Nachlass im ersten Jahr für neue Windows 365-Kunden).

Vorteile und Nachteile der Handlungsoptionen im Überblick

Im Folgenden werden die **Vor- und Nachteile** der drei genannten Optionen für den Umgang mit dem Windows-10-Supportende gegenübergestellt, um KMU eine Entscheidungsgrundlage zu bieten.

Option 1 – Upgrade auf Windows 11:

- *Vorteile:* **Langfristige Lösung** (voller Support bis mindestens 2030er), **höchste Sicherheit** durch modernes OS (Schutz gegen aktuelle Bedrohungen, neueste Funktionen), **einmaliger Umstellungsaufwand** statt fortlaufender Gebühren, keine Abhängigkeit von Internet (lokales OS bleibt erhalten), verbessert Compliance und Versicherungsposition sofort (System ist „up to date“).
- *Nachteile:* **Hardware-Investitionen** können nötig sein, wenn PCs nicht kompatibel sind. **Projektaufwand** für Migration: Kompatibilitätstests, evtl. Updates von Software, Schulung der Mitarbeiter für neue UI. Kurzfristig höherer **Kapitalbedarf** für neue Geräte und Rollout. Möglicher **Widerstand der Nutzer** bei Veränderungen im Workflow (Change Management erforderlich).

Option 2 – Extended Security Updates (ESU):

- *Vorteile:* **Gewinnt Zeit** für eine geordnete Migration– bis zu 3 Jahre Aufschub mit weiterem Schutz. Keine sofortige Hardware-Beschaffung nötig; bestehende Systeme können weiterlaufen. **Einfache Implementierung:** ESU aktiviert weiterhin die gewohnten Windows-10-Sicherheitsupdates (minimale Umstellungen für Nutzer). Bei wenigen Geräten relativ **überschaubare Kosten im 1. Jahr** (ca. $61 pro PC). Lässt sich flexibel **jährlich verlängern oder beenden**, je nach Fortschritt der Umstellung (kein „Lock-in“ über 3 Jahre – man kann theoretisch nach Jahr 1 aufhören zu zahlen, wenn bis dahin migriert wurde).

- *Nachteile:* **Hohe Gesamtkosten** bei voller Ausnutzung der 3 Jahre (Preissteigerung jährlich, im dritten Jahr $244 pro Gerät). Investition verpufft ohne bleibenden Wert, da man letztlich dennoch neue Systeme anschaffen muss – ESU *verzögert nur* die Ausgaben. **Kein Funktionsgewinn:** Windows 10 bleibt alt; neue Features oder Performance-Verbesserungen von Windows 11 fehlen. Mögliche neue Software oder Hardware bleibt u.U. inkompatibel trotz ESU. Zudem bleibt ein **Restrisiko**: ESU deckt nur *bekannte* Sicherheitslücken mit Updates ab – sollte eine kritische Lücke auftreten, die nicht rechtzeitig gepatcht wird, ist man weiterhin verwundbar. Unternehmen könnten außerdem in der **Versicherungsprüfung** nachweisen müssen, dass sie ESU nutzen, um Versicherungsschutz aufrechtzuerhalten (administrativer Aufwand).

Option 3 – Cloud-PC (Windows 365) / Azure Virtual Desktop:

- *Vorteile:* **Sofortige Modernisierung** ohne Geräteaustausch – alte PCs können als Zugangsterminals weiterverwendet werden. **Hohe Sicherheit und Aktualität** durch zentral gemanagtes System in der Cloud (inkl. automatischer Updates und Backups). **Skalierbarkeit & Flexibilität:** Neue Mitarbeiter erhalten schnell einen Cloud-Arbeitsplatz, Auslastungsspitzen können durch Hoch-/Herunterskalieren von Cloud-Ressourcen gemanagt werden. **OpEx statt CapEx:** Kosten planbar pro Monat/Nutzer statt großer Einmalinvestitionen; kann finanziell attraktiv sein, insbesondere wenn Hardwareleasing oder -abschreibungen berücksichtigt werden. Ermöglicht **ortsunabhängiges Arbeiten** und leichtes Einrichten von Remote-Arbeitsplätzen. Und nicht zuletzt: Durch die Einbindung von Windows 365/AVD kann man *ESU-Kosten sparen*, da Windows 10 in diesen Umgebungen kostenlos verlängert unterstützt wird.

- *Nachteile:* **Laufende Betriebskosten:** Über Jahre können Abo-Gebühren die Kosten von eigenen Geräten erreichen oder übersteigen, insbesondere bei leistungshungrigen Konfigurationen. **Abhängigkeit von Internet:** Ein Ausfall der Verbindung legt die Arbeitsumgebung lahm; Latenz und Bandbreite beeinflussen die Nutzererfahrung. **Komplexität/Know-how:** Einführung von Cloud-Desktops erfordert IT-Kenntnisse oder externe Dienstleister, v. a. bei Azure Virtual Desktop. Kleinere Unternehmen ohne IT-Personal könnten mit Verwaltung und Support überfordert sein. **Drittabhängigkeit:** Verlagerung der Daten und Anwendungen in die Cloud erfordert Vertrauen in den Anbieter (Microsoft) und bringt potenzielle Compliance-Fragen (Datenhoheit) mit sich – zwar liegen Daten bei Windows 365 in zertifizierten Rechenzentren, dennoch muss man vertragliche Regelungen prüfen. **Gerätekosten nicht komplett eliminiert:** Auch für den Zugang benötigt man weiterhin Endgeräte (wenn auch weniger leistungsfähig); sehr alte oder defekte PCs müssen ggf. dennoch ersetzt werden oder es fallen Kosten für Thin Clients an.

Handlungsempfehlungen für KMU: Jetzt Vorbereiten

Angesichts des nahenden Stichtags sollten **Geschäftsführer von KMU frühzeitig Maßnahmen einleiten**, um einen reibungslosen Übergang sicherzustellen. Nachfolgend einige Empfehlungen, wie Sie Ihr Unternehmen auf das Windows-10-Supportende **proaktiv vorbereiten** können:

1. **IT-Bestandsaufnahme durchführen:** Verschaffen Sie sich einen Überblick, **welche und wie viele Geräte** in Ihrem Unternehmen noch Windows 10 nutzen. Erfassen Sie Alter, Leistungsdaten (CPU, RAM, TPM-Fähigkeit) und installierte Software dieser Systeme.

Diese Inventur bildet die Basis für alle weiteren Schritte. Prüfen Sie mit Microsofts **PC Health Check**-App oder ähnlichen Tools, welche Geräte **Windows 11-kompatibel** sind. Kategorisieren Sie die PCs z. B. in *kompatibel*, *upgradefähig mit kleiner Hardware-Nachrüstung (z. B. RAM)* und *nicht kompatibel*. Identifizieren Sie auch geschäftskritische Anwendungen und prüfen Sie deren Kompatibilität mit Windows 11 oder potentiell notwendigen Updates.

2. **Migrationsplan und Strategie festlegen:** Entscheiden Sie auf Basis der Bestandsaufnahme, welche der oben erläuterten Optionen – oder welche Kombination – für Ihre Situation am sinnvollsten ist. Etwa:
    - **Direktumstieg auf Windows 11** für alle kompatiblen PCs (ggf. nach Aufrüstung von Komponenten).
    - **Hardware-Refresh** für nicht kompatible Geräte: Planen Sie Neuanschaffungen oder Leasing von Windows 11-fähigen Rechnern. Beachten Sie Bestellzeiten und Budgetzyklen.
    - **Übergangsweise ESU nutzen** für spezifische Altsysteme, die aus bestimmten Gründen nicht sofort ersetzt werden können (z. B. Maschinensteuerung, spezialisierte Software). Definieren Sie aber klare Fristen, bis wann auch diese Systeme migriert werden.
    - **Pilotierung von Cloud-Lösungen**: Testen Sie ggf. mit einigen Nutzern Windows 365 oder Azure Virtual Desktop, vor allem wenn Hardwarebeschaffung schwierig ist oder dauerhaft ein hybrides Arbeitsmodell unterstützt werden soll. Ein Proof-of-Concept kann zeigen, ob Leistung und Handhabbarkeit Ihren Anforderungen entsprechen.

Legen Sie eine **Timeline** fest: Idealerweise sollten kritische Systeme *vor* Oktober 2025 umgestellt sein, um keine Lücke im Schutz zu haben. Berücksichtigen Sie Puffer für Unvorhergesehenes. Das BSI empfiehlt, das Upgrade frühzeitig einzuleiten, **um nicht in Zeitdruck zu geraten**. Beispielsweise könnte der Migrationsplan so aussehen: Q4 2024 Planung & Tests, Q1–Q2 2025 Beschaffung Hardware/Software, Q3 2025 Umsetzung Rollout, Abschluss *spätestens* bis September 2025.

3. **Budgetierung und Ressourcen einplanen:** Auf Basis der Strategie sollten Sie **Budget freigeben** und Ressourcen zuteilen. Kalkulieren Sie Anschaffungskosten für neue Hardware (unter Einbezug von Mengenrabatten oder Leasingangeboten). Berücksichtigen Sie Lizenzkosten – Windows 11 ist als Upgrade kostenlos, aber ggf. fallen neue **Microsoft 365-Lizenzen** an, wenn Sie Cloud-PCs oder AVD nutzen wollen. Planen Sie auch die **ESU-Kosten** ein, falls relevant, und setzen Sie diese ins Verhältnis zu den Kosten alternativer Maßnahmen. Möglicherweise sind 61 USD pro PC eine vertretbare Summe für 1 Jahr Schonfrist, aber für 3 Jahre summiert es sich erheblich. Stellen Sie sicher, dass auch **interne Personalkapazitäten oder externe Dienstleister** für das Migrationsprojekt budgetiert werden (z. B. für Installation, Rollout, Mitarbeiter-Support). Eine realistische Kostenplanung und frühzeitige Finanzierungsentscheidung verhindern Engpässe kurz vor dem Supportende.

4. **Sicherheitsvorkehrungen bis zur Umstellung treffen:** Solange in Ihrem Betrieb noch Windows 10-Rechner laufen, sollten Sie das **Sicherheitsrisiko minimieren**. Installieren Sie unbedingt **alle ausstehenden Updates bis 14. Oktober 2025**. Prüfen Sie Ihre

Antivirus-Lösungen und stellen Sie sicher, dass diese aktuell sind – sie bieten zwar keinen vollständigen Schutz ohne Systemupdates, aber erkennen zumindest bekannte Malware. Schränken Sie die Nutzung älterer Windows-10-Systeme soweit wie möglich ein: Für sensible Tätigkeiten (z. B. Online-Banking, Zugang zu Kundendaten) verwenden Sie bevorzugt bereits migrierte Geräte. In besonders kritischen Bereichen ziehen Sie in Betracht, **Windows-10-Rechner vom Internet zu trennen** oder streng zu segmentieren. Eine konsequente Netzwerktrennung (Isolation) alter Systeme kann laut Versicherungsbranche ein Weg sein, das Risiko und die Haftung zu reduzieren. Schulen Sie Ihre Mitarbeiter in dieser Übergangsphase, **phishing**-Mails und andere Angriffsversuche besonders wachsam zu behandeln – die menschliche Firewall ist umso wichtiger, wenn technische Lücken bestehen. Und nicht zuletzt: Führen Sie **regelmäßige Backups** wichtiger Daten durch, um im Falle eines Zwischenfalls (Malwarebefall, Systemausfall) schnell handlungsfähig zu sein.

5. **Kommunikation und Einbindung der Stakeholder:** Beziehen Sie alle relevanten Parteien frühzeitig ein. Informieren Sie Ihre **Mitarbeiter** über die anstehenden Änderungen – z. B. dass ein neuer PC oder ein Upgrade kommt – und bieten Sie ggf. kurze Einweisungen an, um Akzeptanz zu schaffen. Stimmen Sie sich mit Ihrer **IT-Abteilung oder externen IT-Betreuung** eng ab; falls Sie keinen internen IT-Administrator haben, ist jetzt der Zeitpunkt, mit einem IT-Dienstleister einen Migrationsfahrplan abzusprechen. Überprüfen Sie auch Verträge mit **Softwarelieferanten**: Benötigen Sie Updates oder neue Versionen, damit Ihre Anwendungen unter Windows 11 laufen? Planen Sie diese Updates ein. **Kontaktieren Sie gegebenenfalls Ihren Cyber-Versicherer**, um sicherzustellen, dass dieser über Ihre Übergangsmaßnahmen informiert ist – vor allem, wenn Sie von dem Standard (immer unterstützte Software einzusetzen) temporär abweichen. Manche Versicherer tolerieren den Weiterbetrieb mit Windows 10 *nur* bei Nachweis von ESU oder ähnlichen Schutzvorkehrungen. Eine offene Kommunikation kann hier Klarheit schaffen und Ihren Versicherungsschutz bestätigen.

6. **Testläufe und Pilotprojekte:** Bevor Sie eine unternehmensweite Migration durchführen, setzen Sie auf **Pilotprojekte**. Rüsten Sie z. B. in einer Abteilung einige Rechner auf Windows 11 um oder richten Sie zwei, drei Windows 365 Cloud-PCs für freiwillige Tester ein. Deren Feedback hilft, etwaige Probleme (Softwareinkompatibilitäten, Performanceengpässe, Usability-Fragen) frühzeitig zu erkennen und gegenzusteuern. Nutzen Sie auch die Pilotphase, um ein **Rollback-Szenario** durchzuspielen: Stellen Sie sicher, dass Sie im Falle von kritischen Problemen mit Windows 11 (die unwahrscheinlich, aber möglich sind) einen Plan haben, wie Mitarbeiter weiterarbeiten können (zur Not temporär via Cloud oder einem ESU-geschützten Gerät, bis der Fehler behoben ist).

7. **Dokumentation und Policy-Updates:** Passen Sie interne **IT-Richtlinien** an das neue Umfeld an. Wenn Sie z. B. auf Cloud-PCs umsteigen, brauchen die Nutzerrichtlinien eventuell Ergänzungen bezüglich Datenhandling in der Cloud. Dokumentieren Sie außerdem den Ablauf der Migration, die aktualisierten **Asset-Listen** (mit neuen Geräten oder OS-Versionen) und entfernen Sie veraltete Windows-10-Systeme aus Ihrem Inventar, sobald diese außer Betrieb gehen. Diese Dokumentation ist nicht nur für die eigene Übersicht wertvoll, sondern kann im Fall eines Audits (etwa durch Kunden, Partner oder Versicherer) als Nachweis dienen, dass Sie der Sicherheitsverantwortung nachgekommen sind.

8. **Nach dem Umstieg – Nachbereitung:** Sobald Ihr Unternehmen vollständig auf Windows 11 oder alternative Lösungen umgestellt hat, überprüfen Sie nochmals Ihre **Sicherheitsstrategie**. Windows 11 bringt neue Sicherheitsfunktionen – stellen Sie sicher, dass diese (z. B. BitLocker, Secure Boot, Virtualisierungsbasierte Sicherheit) aktiviert und konfiguriert sind. Entsorgen oder recyclen Sie alte Hardware datenschutzgerecht (Löschung aller Daten). Nutzen Sie die Gelegenheit, um **Lessons Learned** zu sammeln: Was lief gut in diesem Migrationsprojekt, wo gab es Engpässe? Diese Erkenntnisse helfen bei künftigen IT-Projekten.

Fazit

Das Supportende von Windows 10 am 14. Oktober 2025 ist ein kritischer Meilenstein für alle KMU, die noch mit diesem Betriebssystem arbeiten. Ohne Vorbereitung drohen **erhebliche Sicherheits- und Geschäftsrisiken**. Die gute Nachricht ist, dass es im Microsoft-Umfeld **klare Handlungsoptionen** gibt: Vom Wechsel auf Windows 11 über temporäre Extended Security Updates bis hin zu modernen Cloud-PC-Lösungen. Jede Option hat **Vor- und Nachteile**, doch keine Handlung ist keine Lösung – ein Aussitzen würde die IT-Sicherheit und Compliance Ihres Unternehmens massiv gefährden.

Für Geschäftsführer von KMU lautet die Kernempfehlung: **Planen Sie jetzt voraus.** Entscheiden Sie strategisch, welcher Weg für Ihr Unternehmen passt, und stellen Sie die Weichen frühzeitig. Ob Sie nun in neue Hardware investieren, Übergangs-Support einkaufen oder auf die Cloud setzen – wichtig ist, dass Sie das Ende von Windows 10 nicht unvorbereitet trifft. Mit einer rechtzeitigen Umstellung schützen Sie nicht nur Ihre Daten und Systeme, sondern erhalten auch die **Handlungsfähigkeit und Wettbewerbsfähigkeit** Ihres Unternehmens in einer Zeit, in der sichere und moderne IT-Infrastruktur ein Muss ist.