BR-Systems

LIFECYCLE & MODERNISIERUNG 2025

Windows 10: End of Support als Modernisierungsprojekt

Wie Unternehmen Geräte, Anwendungen, Identitäten und Daten kontrolliert in den nächsten Lebenszyklus überführen

Dokument-ID	BR-WP-LCM-007
Version	1.0
Fachstand	30. September 2025
Veröffentlicht	14. Oktober 2025
Klassifizierung	Öffentlich – kostenfreier Fachbeitrag
Autor	Benjamin Raulf, BR-Systems
Herausgeber	BR-Systems · IT-Systemhaus · Gronau (Leine)
Standort zum Fachstand	Südstraße 10 · 31028 Gronau (Leine)
Kontakt	info@br-systems.eu · https://br-systems.eu · +49 179 1601700

Executive Summary

Dieses Whitepaper übersetzt aktuelle Anforderungen und technische Entwicklungen in einen umsetzbaren Betriebsansatz. Im Mittelpunkt stehen nicht einzelne Produkte, sondern Verantwortlichkeiten, überprüfbare Kontrollen und ein realistischer Weg vom heutigen Zustand zu einer belastbaren Zielarchitektur.

Die vier wichtigsten Aussagen

- Supportende als Betriebs- und Sicherheitsrisiko bewerten
- Upgrade, Austausch, Ablösung und ESU bewusst unterscheiden
- Anwendungen und Peripherie vor der Umstellung testen
- Datenlöschung, Wiederverwendung und Entsorgung nachweisbar planen

Inhalt

1. Der Stichtag und seine Bedeutung

Microsoft beendete den regulären Support für Windows 10 am 14. Oktober 2025. Der Rechner funktioniert danach grundsätzlich weiter, erhält im normalen Supportmodell aber keine regulären Sicherheitsupdates und keinen technischen Support mehr [1]. Für Unternehmen ist dies kein Anlass zu Panik, aber ein klarer Lifecycle-Termin. Nicht unterstützte Systeme erhöhen mit wachsender Zeit das Risiko und erschweren Versicherungs-, Kunden- oder Compliance-Nachweise.

Eine seriöse Planung beginnt mit einer verifizierten Bestandsaufnahme. Gerätename, Modell, Alter, Windows-Edition, Hardwareeignung, Benutzer, Standort, Verschlüsselung, Anwendungen, Spezialperipherie und Kritikalität werden erfasst. Erst danach lässt sich entscheiden, ob ein In-Place-Upgrade, eine Neuinstallation, ein Geräteaustausch, die Ablösung einer Anwendung oder eine zeitlich begrenzte Übergangslösung sinnvoll ist.

2. Vier Entscheidungswege

Technisch geeignete Geräte können nach Prüfung auf Windows 11 aktualisiert werden. Eine Neuinstallation bietet eine sauberere Ausgangslage, benötigt aber mehr Vorbereitung für Daten, Einstellungen und Anwendungen. Wirtschaftlich oder technisch ungeeignete Hardware sollte ersetzt werden. Wo eine Altanwendung unvermeidbar bleibt, ist eine isolierte Übergangsumgebung mit klarer Befristung häufig sicherer als ein unkontrollierter Weiterbetrieb.

Microsoft bietet Extended Security Updates als befristete Option an; Bedingungen und Umfang müssen aktuell beim Anbieter geprüft werden [2]. ESU ist kein Ersatz für Modernisierung: Es adressiert bestimmte Sicherheitsupdates, löst aber weder alte Hardware, inkompatible Anwendungen noch fehlende Betriebsprozesse. Die Entscheidung wird mit Kosten, Enddatum, Schutzmaßnahmen und Ablöseplan dokumentiert.

Für Spezialmaschinen, Messplätze oder ältere Produktionssoftware kann eine unmittelbare Migration technisch unmöglich sein. Dann wird die Ausnahme als eigenes Risikoszenario behandelt: Netzwerkzugriffe werden auf erforderliche Ziele begrenzt, Internetzugang wird soweit möglich entfernt, Benutzerrechte werden reduziert und Datenaustausch kontrolliert. Ein aktuelles vorgeschaltetes System, Anwendungsvirtualisierung oder Remote-Bereitstellung kann die Exposition verringern, muss aber getestet und lizenziert sein. Die Altumgebung erhält einen benannten Eigentümer, Überwachung, Backup und ein verbindliches Ablösedatum. „Läuft noch“ ist keine Lifecycle-Strategie.

3. Anwendung, Identität und Hardware testen

Geschäftskritische Anwendungen benötigen fachliche Testfälle. Ein Programmstart allein beweist keine Kompatibilität. Druck, Scan, Signatur, Schnittstellen, Office-Integration, Datenbankzugriff, Treiber, Lizenzierung und Benutzerrechte werden geprüft. Eine Pilotgruppe sollte reale Rollen und verschiedene Hardwaremodelle abbilden. Fehler und Rückfallkriterien werden vor der breiten Welle festgelegt.

Die Umstellung ist eine gute Gelegenheit, lokale Administratorrechte, alte Konten, Verschlüsselung, MFA und Gerätekonfiguration zu bereinigen. Hardwareanforderungen von Windows 11 – darunter kompatibler Prozessor, UEFI/Secure Boot und TPM 2.0 – sind anhand der aktuellen Microsoft-Vorgaben zu prüfen [3]. Umgehungen der Anforderungen schaffen keinen verlässlichen Unternehmensstandard.

4. Rollout in kontrollierten Wellen

Jede Welle braucht Zielgeräte, Wartungsfenster, Kommunikationsweg, Backup oder Datensicherung, Erfolgskriterien und Rückfall. Zunächst werden Pilot und technisch einfache Gruppen umgesetzt, danach kritische Rollen. Mobile Beschäftigte und Geräte mit Spezialperipherie erhalten eigene Planung. Statusberichte unterscheiden inventarisiert, geprüft, bereit, migriert, abgenommen und Ausnahme.

Ein Rollout ist erst abgeschlossen, wenn Schutzstatus, Updates, Verschlüsselung, Anwendungen, Datenzugriff, Monitoring und Backup funktionieren. Nicht mehr benötigte Geräte werden gesperrt und aus Verwaltung, Identitätsplattform und Inventar entfernt. Dadurch bleiben keine Schattenendpunkte zurück, die später unbeachtet online gehen.

Kommunikation reduziert vermeidbare Störungen. Beschäftigte erfahren Termin, erwartete Dauer, notwendige Vorbereitung, Änderungen und erreichbaren Support. Lokale Daten und Browserprofile werden nicht stillschweigend als vollständig gesichert angenommen. Für Leitung, Außendienst oder Schichtbetrieb werden passende Zeitfenster geplant. Das Projektteam führt ein Entscheidungsprotokoll für Ausnahmen und wiederkehrende Fehler. Nach jeder Welle werden Bearbeitungszeit, Rückfälle, Supportanfragen und fachliche Abnahme ausgewertet. Diese Daten verbessern die nächste Welle und liefern eine belastbare Restaufwandsprognose.

5. Datenlöschung und Hardware-Lifecycle

Bei Wiederverwendung, Rückgabe oder Entsorgung muss der Umgang mit Datenträgern festgelegt werden. Die Löschmethode richtet sich nach Medium, Schutzbedarf, Vertragslage und geplanter Weiterverwendung. Ein einfaches Zurücksetzen ist nicht in jedem Szenario ein ausreichender Nachweis. Seriennummer, Eigentümer, Methode, Ergebnis, Datum und ausführende Person gehören in ein nachvollziehbares Protokoll.

Wer mit zertifizierter Datenlöschung wirbt, muss Zertifikat, Geltungsbereich, Verfahren und tatsächliche Leistung korrekt belegen können. Eine persönliche Schulung oder ein Tool allein macht nicht automatisch jede Löschung zertifiziert. Bis entsprechende Nachweise vorliegen, ist die sachliche Formulierung „dokumentierte Datenlöschung nach vereinbartem Verfahren“ belastbarer.

6. Dauerhafter Lifecycle statt einmaliger Aktion

Nach dem Projekt sollte ein Lifecycle-Register Supportenden für Betriebssysteme, Server, Netzwerkgeräte, Anwendungen und Firmware enthalten. Zwölf bis achtzehn Monate Vorlauf vermeiden Notkäufe. Beschaffung berücksichtigt Reparierbarkeit, Garantien, Treiberpflege, Verschlüsselung, zentrale Verwaltung und sichere Löschung. Damit wird der nächste Stichtag planbar.

Eine Managementübersicht zeigt Geräte im Support, Ausnahmen, technische Schulden und fällige Entscheidungen. Das Ziel ist nicht, jedes Gerät möglichst früh auszutauschen. Ziel ist eine begründete, sichere und wirtschaftliche Nutzung über den gesamten Lebenszyklus – einschließlich sauberem Exit. Quartalsweise werden Supportfristen, Ersatzbedarf, Ausnahmegenehmigungen und Budget gemeinsam überprüft. Das verhindert, dass bekannte Altlasten unbemerkt zu dringenden und teuren Sicherheitsproblemen werden können.

Auch Kosten werden über den Lebenszyklus betrachtet. Neben Kaufpreis oder Lizenz zählen Vorbereitung, Benutzerunterstützung, Anwendungstests, Ausfallfenster, Zubehör, Entsorgung und interne Arbeitszeit. Ein weiter genutztes Altgerät kann auf dem Papier günstig sein, durch fehlende Ersatzteile, schwache Leistung oder Sicherheitsausnahmen aber dauerhaft Aufwand erzeugen. Umgekehrt ist ein Austausch ohne geprüften Bedarf weder nachhaltig noch wirtschaftlich. Ein gestaffelter Plan bündelt kompatible Gerätegruppen, vermeidet

hektische Beschaffung und hält Reservegeräte für kritische Rollen bereit. Erkenntnisse aus dem Windows-10-Projekt werden anschließend als Standard für Server, Netzwerkkomponenten und Fachanwendungen übernommen. Nach Projektende werden außerdem Rechnungen, Garantieinformationen, Wiederherstellungsschlüssel, Gerätezuteilung und Entsorgungsbelege zentral abgelegt. Die technische Dokumentation nennt verwendete Installationsprofile und Abweichungen. Damit kann ein späterer Defekt reproduzierbar bearbeitet werden, ohne dass jede Einrichtung erneut erfunden wird. Regelmäßige Stichproben prüfen, ob Geräte weiterhin den freigegebenen Zustand besitzen und Ausnahmen rechtzeitig auslaufen.

7. Vom Konzept zum belastbaren Betrieb

Technische Maßnahmen entfalten ihren Wert erst in einem geregelten Betrieb. Dazu gehören ein benannter Service Owner, eine aktuelle Systemdokumentation, ein Änderungsprozess und ein fester Kontrollrhythmus. Der Umfang darf zur Organisation passen. Ein kleiner Betrieb benötigt keine Sitzungsbürokratie wie ein Konzern. Er benötigt jedoch Klarheit darüber, wer entscheidet, wer umsetzt, wer prüft und wie Abweichungen behandelt werden.

Bei jeder Maßnahme sollten vier Fragen beantwortet werden: Welches konkrete Risiko wird reduziert? Woran erkennen wir, dass die Maßnahme aktiv ist? Wer reagiert auf Fehler oder Alarme? Wie verlassen oder ersetzen wir die Lösung später? Diese Fragen schützen vor Scheinsicherheit und unnötiger Herstellerbindung. Sie machen Angebote vergleichbarer und erleichtern die Übergabe zwischen internen und externen Verantwortlichen.

Dokumentation ist kein Selbstzweck. Sie verkürzt Störungen, macht Änderungen sicherer und verhindert, dass kritisches Wissen ausschließlich bei einer Person liegt. Gute Dokumentation ist knapp genug, um gepflegt zu werden, und konkret genug, um in einer Störung zu helfen. Dazu gehören Übersichten, Abhängigkeiten, Verantwortliche, Zugangsverfahren, Wiederanlaufhinweise und der Stand der letzten Prüfung.

Ein Management-Review sollte Risiken nicht in technischen Einzelmeldungen verstecken. Sinnvoll sind wenige verständliche Kennzahlen: ungeklärte kritische Schwachstellen, Abdeckung starker Authentisierung, erfolgreiche Restore-Tests, überfällige Offboardings, nicht unterstützte Systeme und offene Maßnahmen nach Priorität. Die Kennzahlen dienen Entscheidungen, nicht dem Schönrechnen eines Ampelstatus.

Die beste Roadmap ist umsetzbar. Maßnahmen werden in kleine, prüfbare Pakete geschnitten und mit Termin sowie Verantwortlichem versehen. Kritische Sofortmaßnahmen stehen vor Komfortprojekten. Nach jedem Abschnitt wird geprüft, ob das Risiko tatsächlich gesunken ist. So entsteht über Monate ein belastbarer Betrieb, ohne das Tagesgeschäft durch einen unrealistischen Komplettumbau zu blockieren.

Beschaffung und Betrieb sollten getrennt bewertet werden. Ein günstiger Einstieg kann durch aufwendige Administration, unklare Lizenzbedingungen, fehlende Exportmöglichkeiten oder schwachen Support später teuer werden. Umgekehrt ist eine umfangreiche Plattform nicht automatisch die bessere Wahl. Vor einer Entscheidung werden deshalb fünf Jahre Betrieb, interne Zeit, notwendige Kompetenzen, Ausfallfolgen, Datenmigration und Rückbau betrachtet. Diese Gesamtsicht verhindert, dass ein kurzfristiger Preisvergleich die langfristige Handlungsfähigkeit bestimmt.

Auch Kommunikation ist eine Sicherheits- und Qualitätskontrolle. Mitarbeitende müssen wissen, wo sie Störungen, verdächtige Nachrichten oder Fehlbedienungen ohne Angst vor Schuldzuweisung melden können. Führungskräfte benötigen eine verständliche Lage, keine Sammlung unbewerteter Warnungen. Dienstleister brauchen eindeutige Freigaben und erreichbare Ansprechpartner. Ein kurzer, regelmäßig geübter Kommunikationsweg reduziert im Ernstfall Verzögerungen und Fehlentscheidungen deutlich.

Vor dem Produktivstart gehört eine unabhängige Abnahme in den Plan. Dabei wird nicht nur geprüft, ob Funktionen vorhanden sind, sondern ob Berechtigungen, Protokollierung, Sicherung, Alarmierung,

Dokumentation und Rückfallweg tatsächlich funktionieren. Festgestellte Abweichungen werden mit Risiko, Verantwortlichem und Zieltermin protokolliert. Eine bewusste Rest-Risikoentscheidung ist legitim; eine unbemerkte Lücke ist es nicht. Diese Abnahme schafft eine belastbare Ausgangslage für den späteren Regelbetrieb.

Technische Standards müssen außerdem mit dem Arbeitsalltag vereinbar sein. Eine Kontrolle, die regelmäßig umgangen wird, schützt schlechter als eine etwas einfachere Lösung, die zuverlässig genutzt und überwacht wird. Pilotgruppen helfen, Nebenwirkungen früh zu erkennen. Rückmeldungen aus Fachabteilungen werden dokumentiert, ohne die Schutzziele aus dem Blick zu verlieren. So entsteht Akzeptanz nicht durch Marketing, sondern durch nachvollziehbare Entscheidungen und funktionierende Abläufe.

Mindestens einmal jährlich sollte die Organisation ihre Annahmen neu prüfen. Geschäftsprozesse, Mitarbeiterzahl, Standorte, Anwendungen, Bedrohungen und gesetzliche Rahmenbedingungen verändern sich. Ein früher sinnvoller Schwellenwert oder Vertrag kann später unpassend sein. Das Review betrachtet neue Abhängigkeiten, abgeschaltete Systeme, offene Ausnahmen, Wirksamkeitsnachweise und geplante Veränderungen. Daraus entsteht die nächste überschaubare Roadmap statt eines jahrelang unveränderten Dokuments.

Praxis-Checkliste

- Vollständigen Windows-10-Bestand mit Anwendungen und Peripherie erfassen
- Upgrade, Neuinstallation, Austausch, Isolierung oder ESU je Gerät entscheiden
- Pilotgruppe und fachliche Anwendungstests definieren
- Rolloutwellen mit Kommunikation, Abnahme und Rückfall planen
- Verschlüsselung, MFA, Schutzstatus und lokale Rechte mitprüfen
- Ausnahmen mit Risiko, Kompensation und verbindlichem Enddatum führen
- Wiederverwendung, Datenlöschung und Entsorgung nachweisbar dokumentieren

Fazit

Die Qualität einer IT-Entscheidung zeigt sich nicht am Prospekt, sondern im Betrieb: an klaren Rollen, nachvollziehbaren Änderungen, getesteter Wiederherstellung und einer realistischen Exit-Option. BR-Systems unterstützt bei Bestandsaufnahme, Konzeption, Migration, Umsetzung und laufendem Betrieb - herstellerbewusst, aber nicht verkaufsgetrieben.

Quellen und weiterführende Informationen

[1] Microsoft: Windows 10 support ends on October 14, 2025
https://support.microsoft.com/en-us/windows/windows-10-support-ends-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281

[2] Microsoft Learn: Windows 10 Extended Security Updates
https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates

[3] Microsoft: Windows 11 specifications and system requirements
https://www.microsoft.com/en-us/windows/windows-11-specifications

Historischer bzw. fachlicher Bezugsstand: 30. September 2025. Veröffentlicht: 14. Oktober 2025. Online-Quellen zuletzt geprüft: 30. September 2025. Der Fachstand ist kein vorgetäuschtes Veröffentlichungsdatum. Dokument-ID BR-WP-LCM-007, Version 1.0.

Über BR-Systems

- Herstellerunabhängige Beratung mit Blick auf Nutzen, Betrieb und Exit-Fähigkeit
- Umsetzung und Betreuung für Microsoft 365, Security, Proxmox, Backup, Netzwerk und Open Source
- Ein fester Ansprechpartner, nachvollziehbare Dokumentation und transparente Leistungsgrenzen

Nächster Schritt

Sie möchten das Thema auf Ihre Umgebung übertragen? BR-Systems beginnt mit einer Bestandsaufnahme und einem klar begrenzten Maßnahmenplan. Kontakt: info@br-systems.eu oder +49 179 1601700.