TECHCARE

TECHCARE RESEARCH · WHITEPAPER NR. 02

EOSL-Strategie

für Server, Storage & Netzwerk.

End-of-Service-Life ist ein vertraglicher und kaufmännischer Meilenstein — kein technisches Verfallsdatum. Wann sich Verlängern lohnt, wann Sicherheit den Austausch erzwingt und wie eine belastbare, dokumentierte Entscheidung aussieht.

Juni 2026 · TechCare Research

TechCare Solutions GmbH · Hahnstätten · techcaresolutions.de

Inhalt

KAPITEL 01

Management Summary

Die Kernthese dieses Whitepapers lautet: **End-of-Service-Life (EOSL) ist ein kaufmännischer und vertraglicher Meilenstein, kein Verschleiß-Datum.** Der Tag, an dem ein Hersteller den Support für ein Produkt endgültig einstellt, sagt nichts darüber aus, ob die Hardware am Folgetag ausfällt. Trotzdem wird EOSL in vielen Organisationen reflexhaft mit „muss ersetzt werden" gleichgesetzt — und damit Budget gebunden, das anderswo mehr Wirkung entfaltet.

Dieser Reflex ist verständlich, aber teuer. Er entsteht aus der Vermischung zweier verschiedener Dinge: dem Auslaufen eines Wartungsvertrags (ein Datum, das der Hersteller aus Geschäftsgründen festlegt) und dem physikalischen Lebensende eines Geräts (das der Physik von Bauteilen, Temperatur und Last folgt). Beide fallen meist gar nicht zusammen — wer sie gleichsetzt, übergibt eine kaufmännische Entscheidung stillschweigend an den Marketing-Kalender des Herstellers.

Eine fundierte EOSL-Entscheidung ist deshalb keine Ja/Nein-Frage entlang eines Kalenderdatums, sondern ein **bewerteter, dokumentierter Keep/Extend/Replace-Beschluss**, der Zuverlässigkeit, Sicherheits- und Compliance-Lage, Ersatzteil-Verfügbarkeit, Kosten und Nachhaltigkeit gegeneinander abwägt. Drei Beweisstränge stützen diesen Ansatz und bilden das Rückgrat der folgenden Kapitel.

Erstens — die Hardware-Realität. Ausfalldaten aus großen Festplatten-Flotten (Backblaze, Google) zeigen eine klassische „Badewannenkurve": hohe Frühausfälle, dann eine lange, flache und stabile Nutzungsphase, erst danach der Verschleiß-Anstieg. Diese flache Phase reicht typischerweise über das fünfjährige Standard-Supportfenster der Hersteller hinaus. Für den Betreiber heißt das: Das Gerät ist im Jahr sechs statistisch nicht riskanter als im Jahr drei — der Vertrag endet, die Zuverlässigkeit bleibt.

Zweitens — der Hyperscaler-Beweis. Microsoft, Google/Alphabet, Amazon und Meta haben in geprüften Geschäftsberichten die bilanzielle Nutzungsdauer ihrer Server von vier bzw. fünf auf **sechs Jahre** angehoben — mit Milliarden-Effekten auf die Abschreibungen. Das ist kein Marketing, sondern eine von Wirtschaftsprüfern testierte Aussage. Wenn die am höchsten ausgelasteten Server-Betreiber der Welt ihre Hardware ein Jahr länger laufen lassen, ist das ein belastbares Signal — gerade für den Mittelstand mit seinem milderen Lastprofil.

Drittens — das Sicherheits-Tor. Die Verlängerung steht unter einem klaren Vorbehalt: Hardware, die nicht mehr sicher betreibbar ist — fehlende Sicherheits-Patches, offene ausgenutzte Schwachstellen, regulatorische Pflichten aus NIS2 und BSI-Grundschutz — muss ersetzt oder außer Betrieb genommen werden. Sicherheit ist kein Abwägungsfaktor, sondern ein Veto. Damit kehrt sich die übliche Logik um: Nicht das Support-Ende erzwingt den Austausch, sondern die Sicherheitslage.

Was das für den Betreiber bedeutet

Praktisch verschiebt dieser Ansatz die EOSL-Frage von einer einmaligen Beschaffungsentscheidung zu einem laufenden Risiko-Prozess. Statt „Wann kaufen wir neu?" lautet die Frage „Welche Assets dürfen unter welchen Auflagen wie lange weiterlaufen — und wann prüfen wir das erneut?". Der Hersteller bleibt damit eine wichtige, aber nicht mehr die alleinige Stimme: Sein LDoS-Datum geht als *ein* Eingangswert neben Ausfalldaten, Sicherheitslage und Kosten in die Bewertung ein. Das Ergebnis ist nicht nur günstiger und ökologisch sauberer, sondern auch prüffest — genau die dokumentierte Risiko-Abwägung, die NIS2, BSI-Grundschutz und CSRD von der Geschäftsleitung verlangen.

> **Kernaussage**
> EOSL terminiert einen Vertrag, nicht ein Gerät. Die richtige Reaktion ist ein scorebasierter, dokumentierter Beschluss — gestützt durch Ausfalldaten und Hyperscaler-Evidenz, begrenzt durch ein hartes Sicherheits- und Compliance-Tor.

KAPITEL 02

EOL, EOS, EOSL — die Begriffe sauber getrennt

Vier Begriffe werden im Alltag häufig vermischt, beschreiben aber klar verschiedene Stationen im Produktleben. Eine saubere Trennung ist die Grundlage jeder belastbaren Lifecycle-Planung. Wer in Vertrag, Angebot oder Audit „EOL" sagt und „EOSL" meint, trifft Entscheidungen auf der falschen Frist — und verschenkt im Zweifel Jahre nutzbarer Betriebszeit oder übersieht ein Sicherheitsrisiko, das schon Monate früher eingetreten ist.

End-of-Life (EOL) — die Ankündigung

EOL ist die offizielle **Ankündigung** des Herstellers, dass ein Produkt das Ende seines Lebenszyklus erreicht. EOL ist der Startschuss einer Reihe gestaffelter Fristen — nicht das Ende des Betriebs. Ab hier beginnt der geordnete Rückzug von Verkauf und Support. Für den Betreiber ist EOL vor allem ein Planungssignal: Ab jetzt läuft die Uhr, und die nachgelagerten Stichtage lassen sich aus der Ankündigung ableiten und in den Lifecycle-Plan eintragen.

End-of-Sale (EoS) — Verkaufsstopp

Ab dem End-of-Sale wird das Produkt nicht mehr neu verkauft. Es bleibt aber unter bestehenden Verträgen weiter supportet. EoS ist in der Regel der Anker, von dem aus die nachgelagerten Support-Fristen gezählt werden. Wichtig für die Planung: Nach EoS ändert sich am laufenden Betrieb zunächst gar nichts — der eigentliche Countdown der Support-Leistungen startet erst ab diesem Datum und läuft dann gestaffelt ab.

End-of-Software-Support — keine Updates mehr

Ab diesem Zeitpunkt liefert der Hersteller keine Software- bzw. Firmware-Updates mehr — insbesondere keine Sicherheits-Patches. Dieser Meilenstein ist sicherheitskritisch: Ab hier altert die Angriffsfläche ungebremst. Genau dieser Stichtag — und nicht das spätere EOSL — ist für die Sicherheitsbewertung der relevante. Ein Gerät kann formal noch Hardware-Support genießen und trotzdem sicherheitstechnisch bereits „blind" sein.

End-of-Service-Life (EOSL) / Last-Date-of-Support (LDoS)

EOSL — beim Hersteller oft als **Last-Date-of-Support (LDoS)** bezeichnet — ist das endgültige Ende jeder Hersteller-Unterstützung: kein Support, keine Ersatzteile, keine RMA, kein Bugfix. Ab diesem Datum ist die Organisation für Betrieb und Risiko allein verantwortlich (ggf. abgesichert über Drittanbieter-Wartung). EOSL ist damit der Punkt, an dem die kaufmännische Frage „verlängern oder ersetzen" akut wird — aber, und das ist der Kern dieses Whitepapers, eben eine kaufmännische und keine physikalische Frage.

> **Der häufigste Irrtum**
> „EOSL = Hardware fällt aus." Falsch. EOSL beendet die *Vertragsbeziehung* zum Hersteller. Der physikalische Zustand der Hardware ist davon unberührt — er folgt der Ausfallkurve (Kapitel 04), nicht dem Kalender.

Die praktische Konsequenz: Im Lifecycle-Plan gehören zu jedem Asset mindestens drei Daten — das Ende des Software-Supports (sicherheitsrelevant), das LDoS/EOSL (vertraglich-kaufmännisch) und das geschätzte Verschleiß-Fenster (physikalisch). Erst diese drei zusammen erlauben eine Entscheidung, die weder zu früh Budget verbrennt noch zu spät ein Sicherheitsrisiko stehen lässt.

Für den Betreiber ist der wichtigste Merksatz: Der sicherheitsrelevante Stichtag ist das Ende des Software-Supports, nicht das spätere EOSL. Wer seine Risiko-Uhr am LDoS ausrichtet, betreibt womöglich monatelang Geräte ohne Patch-Versorgung im falschen Glauben, noch „im Support" zu sein; umgekehrt verleitet das frühe EoS-Datum zu voreiliger Beschaffung — beide Fehler entstehen aus derselben Wurzel.

KAPITEL 03

Der Hersteller-Lebenszyklus (Cisco · HPE · Dell)

Die großen Infrastruktur-Hersteller folgen einem ähnlichen Phasenmodell, unterscheiden sich aber in Fristen und Begriffen. Die folgenden Angaben spiegeln die jeweils veröffentlichten Policies wider; im Einzelfall gilt stets die produktspezifische Ankündigung.

Cisco

Laut Cisco-„End-of-Life-Policy" wird das End-of-Sale typischerweise rund sechs Monate im Voraus angekündigt. Nach EoS erhalten Vertragskunden gestaffelten Support: typischerweise etwa ein Jahr Hardware-Fehleranalyse, rund zwei Jahre Bugfixes und bis zu fünf Jahre kritische Sicherheits-Fixes. Von EoS bis zum Last-Date-of-Support liegen damit etwa fünf Jahre.

HPE

HPE gewährt Support laut der veröffentlichten EOS/EOSL-Dokumentation in der Regel etwa fünf Jahre ab End-of-Sale. HPE behält sich vor, diese Fenster je nach Produkt zu verkürzen oder zu verlängern.

Dell

Dell bietet im Standard bis zu fünf Jahre Support ab Auslieferung; mit der **Lifecycle Extension** unter ProSupport bis zu sechs Jahre, im Post-Standard-Support insgesamt rund sieben Jahre — vorbehaltlich der Ersatzteil-Verfügbarkeit.

> **Das Muster**
>
> Quer über die Hersteller ergibt sich ein **Standard-Supportfenster von rund fünf Jahren ab End-of-Sale**, mit Hersteller-Verlängerungen auf sechs bis sieben Jahre. Genau hier beginnt die strategische Frage: Das Support-Ende fällt nicht mit dem Nutzungs-Ende der Hardware zusammen.

Typische Phasen und Fenster (policy-basiert, produktabhängig)

Hersteller	Standard-Support	Verlängerung	Anker
Cisco	~5 Jahre bis LDoS	krit. Sicherheits-Fixes bis ~5 J.	ab End-of-Sale
HPE	~5 Jahre	produktabhängig kürzer/länger	ab End-of-Sale
Dell	bis 5 Jahre	bis 6 J. (Lifecycle Ext.), ~7 J. gesamt	ab Auslieferung

Die Lebenszyklus-Phasen aus Betreibersicht

Hinter den Hersteller-Begriffen steckt ein wiederkehrendes Phasenmodell. Die folgende Tabelle übersetzt es in das, was an jeder Station für den laufenden Betrieb tatsächlich passiert — auf Basis der oben genannten Cisco-, HPE- und Dell-Policies. Die Zeitfenster sind typische Größenordnungen; maßgeblich bleibt die produktspezifische Ankündigung.

OEM-Lebenszyklus-Phasen · Meilenstein → Wirkung für den Betreiber → typisches Fenster

Phase	Hersteller-Meilenstein	Was sich für den Betreiber ändert	Typisches Fenster
Aktiv	Produkt im Verkauf, voller Support	Normalbetrieb, volle RMA & Updates	bis EoS
End-of-Sale	Verkaufsstopp angekündigt (Cisco: ~6 Mon. Vorlauf)	Kein Neukauf; Support-Countdown startet ab hier (Anker bei Cisco/HPE)	EoS = Tag 0
Voller Vertrags-Support	Bugfixes + HW-Fehleranalyse (Cisco: ~1–2 J.)	Updates und RMA wie gewohnt; Risiko niedrig	~0–2 J. nach EoS
Nur Sicherheits-Fixes	Cisco: krit. Security-Fixes bis ~5 J.	Funktions-Updates enden; nur noch Sicherheits-Patches — Patch-Status beobachten	~2–5 J. nach EoS
Verlängerter Support	Dell Lifecycle Extension (~6 J.) / Post-Standard (~7 J.)	Support nur noch nach Vereinbarung, Ersatzteile knapper	~5–7 J. (ab Auslieferung bei Dell)
LDoS / EOSL	Endgültiges Support-Ende	Kein OEM-Support, kein RMA — Drittwartung oder Außerbetriebnahme	ab LDoS

Die Tabelle macht zwei Dinge sichtbar. Erstens: Der Übergang von „voller Support" zu „nur noch Sicherheits-Fixes" ist für den Betreiber oft wichtiger als das ferne LDoS — ab hier kommen keine Funktions- und Stabilitäts-Updates mehr, nur noch Patches. Zweitens: Die Verlängerungs-Optionen (Cisco- Security-Fixes, Dell Lifecycle Extension) zeigen, dass die Hersteller selbst das fünfjährige Fenster nicht als hartes Ende betrachten — sie verlängern es kommerziell. Genau diese Logik greift dieses Whitepaper auf und führt sie über das LDoS hinaus weiter.

KAPITEL 04

Wie lange hält Hardware wirklich?

Wenn das Support-Ende kein Verschleiß-Datum ist — wie lange hält Hardware dann tatsächlich? Die beste öffentlich verfügbare Evidenz stammt aus großen Festplatten-Flotten, weil rotierende Magnetspeicher zu den am stärksten beanspruchten Komponenten gehören und ihr Ausfallverhalten gut dokumentiert ist.

Die Badewannenkurve

Das Ausfallverhalten folgt einer **Badewannenkurve**: eine hohe „Kindersterblichkeit" in den ersten Wochen, dann eine lange, flache und stabile Nutzungsphase mit niedriger Ausfallrate, und erst danach der Verschleiß-Anstieg. Entscheidend: Die flache Phase reicht typischerweise über das fünfjährige OEM-Supportfenster hinaus.

Die drei Phasen lohnen eine genauere Betrachtung, weil jede eine eigene betriebliche Lehre trägt. **Frühausfall (Kindersterblichkeit):** In den ersten Wochen und Monaten fallen überdurchschnittlich viele Geräte aus — Material- und Fertigungsfehler, die sich unter Last früh zeigen. Praktisch heißt das: Ein Gerät, das das erste halbe Jahr übersteht, hat seine riskanteste Phase bereits hinter sich, nicht vor sich. **Nutzungs-Plateau:** Es folgt die lange, flache Mitte mit niedriger, weitgehend konstanter Ausfallrate. Hier ist die Hardware am verlässlichsten — und genau hier liegt, statistisch, das fünfte und oft auch das sechste Betriebsjahr. **Verschleiß-Anstieg:** Erst danach steigt die Rate spürbar an, wenn mechanische und thermische Alterung kumulieren. Die Kunst der EOSL-Entscheidung besteht darin, das Ende des Plateaus zu erkennen — nicht das Support-Ende mit dem Verschleiß-Beginn zu verwechseln.

Evidenz

Die **Backblaze Drive Stats 2024** (Flotte von rund 301.000 Laufwerken) weisen eine annualisierte Ausfallrate (AFR) von etwa 1,57 % über alle Laufwerke aus (Lebenszeit-AFR rund 1,31 %). Laufwerke im Alter von zwei bis vier Jahren bewegen sich „niedrig und stabil"; die Ausfallraten steigen „spürbar an, sobald Laufwerke fünf Jahre überschreiten" — einzelne Modelle jenseits der fünf Jahre erreichten rund 3 % AFR.

Die ältere, aber methodisch grundlegende **Google-Studie (Pinheiro u.a., USENIX FAST '07)** über mehr als 100.000 Laufwerke fand altersabhängige AFR zwischen rund 1,7 % und 8,6 %. Wichtige Nebenerkenntnis: SMART-Werte allein sind ein schwacher Prädiktor für den Einzelausfall — Alter und Population sagen mehr aus als ein einzelner Sensorwert. (Die Daten stammen aus 2007 und dienen hier der Kurvenform, nicht absoluten Zahlen.)

Beide Datensätze zeigen dasselbe Bild aus zwei Jahrzehnten: Die Backblaze-Zahlen aus 2024 — eine AFR von rund 1,57 % über eine moderne Flotte von gut 300.000 Laufwerken — und die Google-Daten aus 2007 zeichnen übereinstimmend ein flaches Plateau, dessen Anstieg erst *jenseits* der fünf Jahre einsetzt. Genau dort, wo das standardmäßige OEM-Supportfenster endet, ist die Hardware empirisch noch nicht in der Verschleiß-Phase. Diese zeitliche Lücke zwischen Vertrags-Ende und physischem Risiko-Anstieg ist der quantitative Kern dieses Whitepapers: Sie ist der Raum, in dem eine Verlängerung kein Hasardspiel, sondern eine statistisch begründete Entscheidung ist. Wichtig bleibt die Einordnung — es handelt sich um Flotten-Statistik, nicht um eine Garantie für das Einzelgerät; deshalb tritt in Kapitel 07 die individuelle Ausfallhistorie als eigene Bewertungsdimension hinzu.

> **Die Schlussfolgerung**
>
> Hardware fällt nicht zum Support-Ende aus. Die niedrige, stabile Nutzungsphase erstreckt sich regelmäßig über das fünfjährige OEM-Fenster hinaus. Der Anstieg setzt empirisch erst *jenseits* der fünf Jahre ein — das schafft den Raum, in dem eine Verlängerung kaufmännisch sinnvoll wird.

KAPITEL 05

Der Hyperscaler-Beweis: sechs Jahre Nutzungsdauer

Den überzeugendsten Beleg liefern nicht Labortests, sondern testierte Geschäftsberichte. Die größten Server-Betreiber der Welt haben ihre bilanzielle Nutzungsdauer angehoben — eine von Wirtschaftsprüfern geprüfte Aussage darüber, wie lange Server wirtschaftlich genutzt werden.

Verlängerte bilanzielle Nutzungsdauer (geprüfte Offenlegungen)

Betreiber	Änderung	Wirksam	Bilanz-Effekt (Größenordnung)
Microsoft	Server & Netzwerk 4 → 6 Jahre	FY2023 (ang. Jul 2022)	rund 3–4 Mrd. USD Vorteil FY2023
Alphabet/Google	Server 4 → 6 J.; Teile Netzwerk 5 → 6 J.	2023	Abschreibung ~3,9 Mrd. USD geringer; Nettogewinn ~+3,0 Mrd. USD ($0,24/Aktie)
AWS / Amazon	Server 5 → 6 Jahre	ab 1. Jan 2024	~+900 Mio. USD Nettogewinn Q1 2024
Meta	Server Richtung 5 Jahre (Non-AI)	2022	~1,5 Mrd. USD Vorteil 2022

Der gemeinsame Nenner ist eindeutig: Für **universell einsetzbare Server-Hardware** hat sich ein Sechs-Jahres-Konsens etabliert. Wer Hardware bei höchster Auslastung und unter maximalem Kostendruck betreibt, dehnt die Nutzungsdauer nicht über das technisch Vertretbare hinaus — die Anhebung ist daher ein konservatives, marktbreites Signal.

Die ehrliche Nuance: General-Purpose vs. AI/GPU

2025 hat AWS die Server-Nutzungsdauer teilweise wieder von sechs auf fünf Jahre zurückgenommen, und auch Microsoft hat einzelne Refresh-Zyklen gestrafft. **Treiber war jedoch nicht Verschleiß, sondern der AI/GPU-Erneuerungsdruck**: KI-Beschleuniger veralten funktional schnell, weil neue Generationen drastisch mehr Leistung pro Watt liefern. Für klassische, universell einsetzbare Server-Hardware — die für den Mittelstand relevante Klasse — bleibt der Sechs-Jahres-Konsens bestehen.

Warum ist dieser Beleg so viel stärker als ein Hersteller- oder Beratungs-Versprechen? Weil eine bilanzielle Nutzungsdauer kein Marketing ist, sondern eine testierte Annahme mit unmittelbarer Wirkung auf Gewinn und Aktienkurs. Dass gleich vier der größten Betreiber diesen Schritt gegangen sind, ist daher ein bewusst konservatives Signal — und für den Mittelstand verstärkt es sich sogar: Hyperscaler fahren ihre Server unter nahezu Dauerlast, ein typischer mittelständischer Server steht in einem deutlich milderen Lastprofil. Wenn schon die am härtesten beanspruchte Hardware der Welt geprüft sechs Jahre trägt, ist die Reserve bei moderater Last eher größer als kleiner.

> **Übertragung auf den Mittelstand**
>
> Die für mittelständische Rechenzentren relevante General-Purpose-Hardware wird von den größten Betreibern der Welt geprüft auf sechs Jahre abgeschrieben. Das fünfjährige OEM-Supportfenster ist damit kein technisches Limit, sondern eine kaufmännische Marke.

KAPITEL 06

Sicherheit & Compliance: NIS2, BSI OPS.1.1.3, CVE/EOL-Risiko

Die Verlängerung steht unter einem nicht verhandelbaren Vorbehalt: Hardware muss **sicher betreibbar** bleiben. Drei regulatorische Stränge definieren, was das konkret bedeutet.

NIS2 — Richtlinie (EU) 2022/2555

Die NIS2-Richtlinie war bis zum 17. Oktober 2024 in nationales Recht umzusetzen (Anwendung ab dem 18. Oktober 2024). Sie weitet Anwendungsbereich und Pflichten der Cybersicherheit deutlich aus und macht EOSL-Hardware zu einem ausdrücklich regulierten Risiko. Drei Stränge der Richtlinie sind für die Lifecycle-Entscheidung unmittelbar relevant.

Artikel 21 — Risikomanagement-Maßnahmen. Art. 21 verlangt einen verhältnismäßigen Katalog technischer und organisatorischer Maßnahmen — ausdrücklich einschließlich **Lieferketten-Sicherheit** und der **Behandlung von Schwachstellen** (Vulnerability Handling). Genau hier wird EOSL-Hardware fassbar: Ein Gerät ohne Patch-Versorgung lässt sich im Sinne von Art. 21 nicht mehr ordnungsgemäß gegen Schwachstellen behandeln — es sei denn, kompensierende Maßnahmen (Segmentierung, virtuelles Patchen, erhöhtes Monitoring) treten nachweislich an seine Stelle.

Die Meldekaskade. NIS2 koppelt an Sicherheitsvorfälle eine dreistufige Meldepflicht mit harten Fristen: eine **Frühwarnung binnen 24 Stunden** nach Kenntnis, eine **Vorfallsmeldung binnen 72 Stunden** mit erster Bewertung und ein **Abschlussbericht binnen eines Monats**. Diese Taktung ist im Tagesbetrieb nur einzuhalten, wenn das Inventar, die Abhängigkeiten und der Patch-Status der Assets bereits dokumentiert vorliegen — ein weiterer Grund für den strukturierten EOSL-Prozess.

Bußgelder. Bei wesentlichen Einrichtungen reichen die Bußgelder bis zu **10 Mio. EUR oder 2 % des weltweiten Jahresumsatzes** (der höhere Wert gilt). Die Größenordnung allein verschiebt die EOSL-Frage aus der reinen IT-Kostenrechnung in die unternehmerische Risikobetrachtung.

Deutschland — NIS2UmsuCG (BSIG-Novelle)

Deutschland hat die Oktober-2024-Frist verfehlt; das NIS2-Umsetzungsgesetz wurde Ende 2025 (verkündet im Dezember 2025) in Kraft gesetzt. Der Anwendungsbereich umfasst rund 30.000 deutsche Unternehmen über 18 Sektoren (etwa 8.250 „besonders wichtige" und rund 21.600 „wichtige" Einrichtungen). Zentrale BSIG-Paragraphen lassen sich dabei klar zuordnen:

BSIG-Paragraphen (NIS2UmsuCG) — Zuordnung zur EOSL-Entscheidung

§	Regelungsgegenstand	EOSL-Bezug
§28	Anwendungsbereich (wer ist betroffen)	Klärt, ob das Asset überhaupt im NIS2-Scope liegt (Dim. 6)
§30	Risikomanagement-Maßnahmen	Pendant zu Art. 21 — EOSL-Geräte brauchen kompensierende Maßnahmen
§32	Meldepflichten	24h/72h/1-Monat-Kaskade setzt dokumentiertes Inventar voraus
§38	**Haftung der Geschäftsleitung**	**Leitung ist persönlich verantwortlich** — hebt die Entscheidung auf Vorstandsebene
§65	Bußgeldvorschriften	Sanktionsrahmen für Verstöße gegen §30/§32

Der für dieses Whitepaper entscheidende Paragraph ist **§38**: Die Geschäftsleitung muss die Risikomanagement-Maßnahmen billigen und ihre Umsetzung überwachen — und haftet dafür persönlich. Damit ist eine ungeprüfte EOSL-Hardware nicht länger ein reines IT-Thema, sondern ein Haftungsrisiko des Managements. Eine dokumentierte, scorebasierte Keep/Extend/Replace-Entscheidung ist genau der Nachweis, den §38 von der Leitungsebene verlangt.

BSI IT-Grundschutz — Baustein OPS.1.1.3

Der BSI-Baustein OPS.1.1.3 „Patch- und Änderungsmanagement" (Edition 2023) ist hier das entscheidende Scharnier: Werden Produkte eingesetzt, die vom Hersteller nicht mehr unterstützt werden, MUSS geprüft werden, ob sie noch sicher betrieben werden können; **ist das nicht der Fall, DÜRFEN solche Produkte nicht verwendet werden.** Das ist eine verbindliche MUSS-Anforderung — und genau das Sicherheits-Tor, das jede Verlängerungsentscheidung passieren muss.

Regulatoren behandeln EOL-Geräte als akute Gefahr

Dass dies keine theoretische Sorge ist, zeigt die CISA Binding Operational Directive 26-02 (Februar 2026): eine US-Bundesanweisung, End-of-Support-Edge-Geräte gestaffelt zu inventarisieren und zu entfernen (Inventar binnen 3 Monaten, gelistete Geräte binnen 12 Monaten, übrige binnen 18 Monaten). Begründung: Angreifer nutzen zunehmend nicht mehr unterstützte Edge-Geräte aus. CISA pflegt dazu den Known-Exploited- Vulnerabilities-(KEV)-Katalog. Die Botschaft ist klar: EOL-Hardware ist für Aufsichtsbehörden ein aktives, kein latentes Risiko.

> **Das Sicherheits-Tor**
> „Sicher betreibbar — oder außer Betrieb." Hardware jenseits des Software-Supports, mit offenen, ausgenutzten Schwachstellen und ohne kompensierende Maßnahmen, fällt durch dieses Tor. Dann gilt: ersetzen, unabhängig vom Score.

KAPITEL 07

Der EOSL-Risiko-Score (6 Dimensionen)

Um aus den vorigen Kapiteln eine reproduzierbare Entscheidung zu machen, bewertet der EOSL-Risiko-Score jedes Asset entlang von **sechs Dimensionen** mit je 1 bis 5 Punkten (in Anlehnung an ISO 31000 und gängige Asset-Valuation-/Kritikalitäts-Modelle). Eine Dimension hat dabei Veto-Charakter.

Die sechs Bewertungsdimensionen (je 1–5 Punkte)

#	Dimension	Leitfragen
1	Geschäftskritikalität	Welcher Schaden entsteht bei Ausfall? Single Point of Failure?
2 ⚑	Sicherheits- & Patch-Status (VETO)	Jenseits LDoS? Offene ausgenutzte CVEs? Sicher betreibbar nach BSI OPS.1.1.3?
3	Ersatzteil- & Support-Verfügbarkeit	OEM- oder Drittanbieter-Wartung verfügbar? Ersatzteile am Markt?
4	Zuverlässigkeit / Alter vs. Kurve	Wo auf der Badewannenkurve? Beobachtete Ausfallhistorie?
5	Leistung / Kapazitäts-Reserve	Genügend Headroom? Engpass absehbar?
6	Compliance / Audit-Exposition	NIS2-Scope? CSRD-Scope-3? Dokumentierte Risiko-Akzeptanz?

Das Veto in Dimension 2

Dimension 2 ist **kein gewichteter Summand, sondern ein hartes Veto**. Ein Asset, das nicht sicher betreibbar ist — jenseits des Software-Supports, mit offenen ausgenutzten Schwachstellen und ohne wirksame kompensierende Maßnahmen — ist unabhängig von allen anderen Dimensionen ein Ersetzen-Fall. Kein noch so guter Wert in Kritikalität, Kosten oder Headroom kann ein gerissenes Sicherheits-Tor aufwiegen.

Entscheidungsbänder

Band	Profil
VERLÄNGERN	moderate Kritikalität, sicher betreibbar, Ersatzteile verfügbar, flache Ausfallkurve, ausreichend Headroom
BEOBACHTEN	Mittelfeld — instrumentieren, kompensierende Maßnahmen, vierteljährlich neu bewerten
ERSETZEN	nicht mitigierbares Sicherheitsrisiko, BSI-Tor gerissen, keine Ersatzteile oder harter Performance-Blocker — besonders bei Geschäftskritikalität

Ein durchgerechnetes Beispiel

Das folgende Beispiel zeigt den Score in Aktion an drei typischen Asset-Typen. **Die Punktwerte sind illustrativ gewählt**, um die Mechanik zu demonstrieren — sie sind kein reales Bewertungsergebnis und keine Aussage über konkrete Geräte. Höhere Punkte bedeuten höheres Risiko bzw. dringlicheren Handlungsbedarf; Dimension 2 (Sicherheit) wirkt als Veto.

Illustratives Beispiel / Illustrative example — keine realen Daten

Asset (Beispiel)	D1 Krit.	D2 Sich. ⚑	D3 Teile	D4 Alter	D5 Reserve	D6 Compl.	Empfehlung
Core-Switch, 6 J. alt	4	2	2	2	2	3	VERLÄNGERN
Geschäftskritisch (D1=4), aber Security-Tor bestanden (D2=2, patchbar), Ersatzteile verfügbar, flaches Plateau, genug Headroom → kontrolliert verlängern mit Spare-Pool und Quartals-Review.							
Backup-Storage, 7 J. alt	3	3	4	4	3	2	BEOBACHTEN
Sekundär-System (D1=3), Security grenzwertig aber mitigierbar (D2=3), Ersatzteile werden knapp (D3=4), jenseits des Plateaus (D4=4) → instrumentieren, Spares sichern, Austausch budgetieren, vierteljährlich neu bewerten.							
Edge-Firewall, nach LDoS	5	5	4	3	3	5	ERSETZEN
Exponiertes Edge-Gerät jenseits LDoS ohne Patches (D2=5 → Veto), geschäftskritisch (D1=5), NIS2-/KEV-exponiert (D6=5) → das gerissene Sicherheits-Tor erzwingt den Austausch unabhängig von allen anderen Werten.							

Die dritte Zeile zeigt das Veto in Reinform: Obwohl Alter (D4) und Reserve (D5) mittel ausfallen, überstimmt der Sicherheitswert von 5 jede kaufmännische Erwägung. Die erste Zeile zeigt den Gegenfall — hohe Kritikalität allein erzwingt keinen Austausch, solange das Sicherheits-Tor passiert ist. Genau diese Asymmetrie — Sicherheit als Veto, alles andere als Abwägung — ist der Kern des Modells.

KAPITEL 08

Kosten & Budget: Verlängern vs. Ersetzen

Die kaufmännische Frage lautet nicht „neu oder alt", sondern: Wiegt der Aufwand **einer weiteren Betriebsperiode** die Kosten und Risiken des Austauschs auf? Beide Optionen unterscheiden sich fundamental in ihrer Kostenstruktur.

Capex vs. Opex

Ersetzen ist Capex — eine sprunghafte Investition, abgeschrieben über fünf bis sechs Jahre, zuzüglich Migrationsaufwand. **Verlängern ist Opex** — planbare jährliche Kosten für (Dritt-)Wartung, Ersatzteile und Energie. Die Entscheidung wägt damit Capex plus Migrationsarbeit plus abgeschriebene graue Energie des Neugeräts gegen die Kosten und Risiken einer weiteren Betriebsperiode ab.

Quantifizierter Anker statt erfundener Prozente

Neutrale „€-pro-Server"-Einsparungs-Benchmarks aus herstellerunabhängigen Quellen sind rar — das soll hier ehrlich gesagt sein. Belastbar sind dagegen die testierten Hyperscaler-Abschreibungsdeltas aus Kapitel 05: Die Verlängerung von fünf auf sechs Jahre senkte die jährliche Abschreibung je Asset-Klasse grob um die **Größenordnung von rund 20 %** (abgeleitete Schätzung). Dieser Wert ist der seriöseste verfügbare Proxy für den kaufmännischen Hebel einer Verlängerung.

> **TCO-Faustregel**
> Eine verbreitete TCO-Faustregel besagt: Der reine Hardware-Einkauf macht **weniger als 20 % der Lebenszyklus-TCO** aus; rund 80 % entfallen auf die Zeit danach — Support, Energie, Personal. Wer nur auf den Anschaffungspreis schaut, optimiert den kleinsten Hebel.

Die kaufmännische Wirkung einer Verlängerung speist sich aus zwei Effekten: dem **Zeitwert-Effekt** (jede sicher überbrückte Betriebsperiode schiebt eine große Capex-Position um ein Jahr nach hinten) und dem **Glättungs-Effekt** (planbare kleinere Opex-Posten statt eines sprunghaften Investitionsblocks). Beides ist real, aber standortspezifisch — deshalb beziffert dieses Whitepaper bewusst keine Pauschal-Ersparnis.

> **Illustratives Modell — keine Kundenzusage**
> **Illustratives Modell / Illustrative model.** Angenommen, ein abgeschriebener Server kostet im verlängerten Betrieb pro Jahr nur Dritt-Wartung und Energie, während ein Austausch sofortige Capex plus mehrere Personentage Migration auslöst: Dann verschiebt jede sicher überbrückte Betriebsperiode die Investition und glättet das Budget. Konkrete Beträge sind streng standortspezifisch und hier bewusst nicht beziffert — dies ist kein Versprechen einer Ersparnis, sondern ein Strukturmodell.

KAPITEL 09

Nachhaltigkeit: graue Energie, CSRD/ESRS E1, E-Schrott

Nachhaltigkeit ist beim EOSL kein Beiwerk, sondern zunehmend eine Berichtspflicht — und sie kippt das Bauchgefühl „neu ist grüner" oft um.

Graue Energie (embodied carbon) vs. operativer Anteil

Der CO_2-Fußabdruck eines Servers zerfällt in zwei Teile. Die **graue Energie** (embodied carbon) entsteht *einmalig* bei Herstellung, Rohstoffgewinnung und Transport — sie ist beim Kauf bereits „bezahlt", egal wie lange das Gerät danach läuft. Der **operative Anteil** entsteht *laufend* durch den Stromverbrauch im Betrieb. Über Studien hinweg liegt die graue Energie bei rund **20–30 %** des Lebenszyklus-Fußabdrucks (Spanne etwa 15–43 %), der operative Anteil entsprechend bei rund 70–80 %.

Diese Aufteilung ist der Schlüssel zum Nachhaltigkeits-Argument. Ein durchgerechnetes Beispiel des **Tech Carbon Standard** weist für einen Server rund **5.657 kg CO_2e** über den Lebenszyklus aus, davon etwa **1.726 kg (30,5 %)** graue Energie. Diese 1.726 kg fallen unabhängig von der Nutzungsdauer an — sie werden umso besser amortisiert, je länger das Gerät läuft. Ein vorzeitiger Austausch wirft den noch nicht „abgewohnten" Teil dieser grauen Energie weg und löst sofort die volle graue Energie des Neugeräts aus. Genau hier kippt das Bauchgefühl „neu ist grüner": Solange das Altgerät effizient läuft, ist Weiterbetrieb häufig die CO_2-ärmere Option.

E-Schrott

Die zweite ökologische Dimension ist der Abfallstrom. Der UN Global E-waste Monitor 2024 beziffert das weltweite E-Schrott-Aufkommen 2022 auf **62 Mio. Tonnen**, mit Kurs auf **82 Mio. Tonnen bis 2030**. Nur **22,3 %** wurden 2022 dokumentiert gesammelt und recycelt — Europa führt mit 42,8 %, in vielen Regionen liegt die Quote weit darunter. Jede vermiedene vorzeitige Ausmusterung reduziert diesen Strom unmittelbar und vermeidet zugleich die graue Energie eines Ersatzgeräts. Lebensdauer-Verlängerung wirkt damit doppelt: weniger neue Emission, weniger neuer Abfall.

CSRD / ESRS E1

Unter der CSRD ist Scope-3-Berichterstattung verpflichtend, wo wesentlich, geregelt über ESRS E1. Eingekaufte IT-Hardware zählt zu Scope 3 (Kategorie 2 Capital Goods / Kategorie 1). Eine Verlängerung der Nutzungsdauer amortisiert die bereits angefallene Herstellungs-Emission und verschiebt die Ersatz-Emission — ein **berichtsfähiger Scope-3-Reduktionshebel**.

> **Ehrlicher Vorbehalt (Uptime Institute)**
>
> Austausch senkt CO_2 *nicht automatisch*. Solange neue Hardware nicht hoch ausgelastet ist, holen Effizienzgewinne die graue Energie des Ersatzes womöglich nicht herein. Das Uptime Institute bevorzugt Konsolidierung gegenüber pauschalem Refresh. Eine Verlängerung gewinnt CO_2-seitig nur, wenn das Gerät effizient und ausgelastet bleibt.

KAPITEL 10

Entscheidung: Verlängern, Ersetzen, Beobachten

Score und Bänder aus Kapitel 07 münden in eine von drei Empfehlungen. Entscheidend ist die Reihenfolge der Prüfung: Das Sicherheits-Veto kommt zuerst, erst danach die gewichtete Abwägung.

Verlängern

Empfohlen bei moderater Geschäftskritikalität, bestandenem Sicherheits-Tor, verfügbaren Ersatzteilen (OEM oder Dritt), flacher Position auf der Ausfallkurve und ausreichendem Leistungs-Headroom. Die Verlängerung wird über einen definierten Zeitraum vereinbart und mit vierteljährlicher Neubewertung versehen.

Ersetzen

Zwingend bei nicht mitigierbarem Sicherheitsrisiko, gerissenem BSI-Tor, fehlenden Ersatzteilen oder hartem Performance-Blocker — insbesondere wenn das Asset geschäftskritisch ist. Hier schlägt das Veto jede kaufmännische Erwägung.

Beobachten / Evaluieren

Das Mittelfeld: Assets, die heute noch tragen, deren Risiko aber steigt. Sie werden instrumentiert (Monitoring, Spare-Pool, kompensierende Sicherheitsmaßnahmen) und **vierteljährlich neu bewertet**. So wird aus einer Einmal-Entscheidung ein laufender Prozess — die einzige Form, die der Realität von Ausfallkurven und Bedrohungslage gerecht wird.

> **Prüf-Reihenfolge**
>
> 1) Sicherheits-Veto (Dim. 2) — gerissen? → Ersetzen. 2) Andernfalls gewichteten Score bilden. 3) Band ableiten. 4) Entscheidung dokumentieren und Wiedervorlage setzen.

Wichtig ist, dass keine der drei Empfehlungen ein Endzustand ist. „Verlängern" trägt eine Wiedervorlage in sich, „Beobachten" ist per Definition ein Zwischenstand, und selbst ein „Ersetzen" mündet in ein neues Asset, das ab Tag eins wieder im Lifecycle-Plan steht — drei Zustände in einem Kreislauf, kein Endpunkt.

KAPITEL 11

Ein 6-Schritte-Vorgehen

Der folgende Ablauf macht aus dem Score einen wiederholbaren, prüffesten Prozess.

1. **Inventarisieren.** Vollständige Asset-Liste mit Modell, Alter, LDoS-Datum, Funktion und Abhängigkeiten erstellen. Ohne belastbares Inventar ist jede EOSL-Entscheidung Stückwerk.
2. **Bewerten (Score).** Jedes Asset entlang der sechs Dimensionen mit 1–5 Punkten bewerten — Dimension 2 explizit als Veto-Flag.
3. **Sicherheits-Tor.** Vor jeder kaufmännischen Abwägung prüfen: sicher betreibbar nach BSI OPS.1.1.3? Offene ausgenutzte CVEs (KEV)? Nein → direkt in den Ersetzen-Pfad.
4. **Kosten- & CO_2-Modell.** Capex/Opex, Migrationsaufwand, graue Energie und Scope-3-Effekt je Option gegenüberstellen — mit den Hyperscaler-Deltas als Anker und ehrlich gekennzeichneten Annahmen.
5. **Entscheiden.** Band ableiten (Verlängern / Ersetzen / Beobachten) und Empfehlung mit Begründung festhalten.
6. **Dokumentieren & quartalsweise neu bewerten.** Entscheidung, Annahmen und Risiko-Akzeptanz revisionssicher ablegen (NIS2/CSRD-relevant) und vierteljährlich aktualisieren.

> **Warum quartalsweise?**
> Bedrohungslage und Ausfallkurve sind dynamisch: Eine neue ausgenutzte Schwachstelle oder ein gehäufter Ausfall kann ein „Verlängern" über Nacht in ein „Ersetzen" kippen. Die Re-Bewertung hält die Entscheidung lebendig — und liefert nebenbei die Dokumentation, die §38 BSIG und ESRS E1 verlangen.

KAPITEL 12

Entscheidungs-Checkliste

Diese Liste fasst die Entscheidung in prüfbare Punkte. Sie ist als Arbeitsvorlage je Asset gedacht.

- ☐ Vollständiges Inventar mit Modell, Alter und LDoS-Datum vorhanden
- ☐ Geschäftskritikalität und Abhängigkeiten je Asset bewertet (Dim. 1)
- ☐ Sicherheits- & Patch-Status geprüft: jenseits LDoS? offene ausgenutzte CVEs? (Dim. 2 / Veto)
- ☐ Sichere Betreibbarkeit nach BSI OPS.1.1.3 dokumentiert bestätigt
- ☐ Ersatzteil- und Support-Verfügbarkeit (OEM oder Dritt) geklärt (Dim. 3)
- ☐ Position auf der Ausfallkurve und Ausfallhistorie bewertet (Dim. 4)
- ☐ Leistungs- und Kapazitäts-Headroom geprüft (Dim. 5)
- ☐ Compliance-Exposition geklärt: NIS2-Scope, CSRD-Scope-3 (Dim. 6)
- ☐ Kosten- und CO_2-Modell je Option (Verlängern/Ersetzen) gerechnet
- ☐ Entscheidungsband abgeleitet und Empfehlung begründet
- ☐ Risiko-Akzeptanz und Begründung revisionssicher dokumentiert
- ☐ Wiedervorlage zur quartalsweisen Neubewertung gesetzt

KAPITEL 13

Fazit

EOSL ist ein Datum im Vertrag, kein Zustand der Hardware. Wer beide gleichsetzt, bindet Budget ohne Notwendigkeit — oder, schlimmer, betreibt unsicheres Gerät im falschen Vertrauen auf das Kalenderblatt.

Die Evidenz ist konsistent: Ausfallkurven zeigen eine lange stabile Nutzungsphase über das fünfjährige OEM-Fenster hinaus, und die größten Server-Betreiber der Welt schreiben General-Purpose-Hardware geprüft auf sechs Jahre ab. Damit ist eine maßvolle Verlängerung kaufmännisch und ökologisch oft die bessere Wahl — **vorausgesetzt, das Sicherheits- und Compliance-Tor wird passiert.**

Die richtige Antwort auf EOSL ist deshalb kein Reflex, sondern ein Verfahren: ein scorebasierter, dokumentierter Keep/Extend/Replace-Beschluss mit hartem Sicherheits-Veto und vierteljährlicher Wiedervorlage. Das schützt Budget, erfüllt NIS2/CSRD und macht die Entscheidung — bis hinauf zur nach §38 BSIG persönlich haftenden Geschäftsleitung — prüffest.

In einem Satz

Bewerten statt reflexartig ersetzen — und jede Verlängerung am Sicherheits-Tor messen.

KAPITEL 14

Über TechCare & Quellen

TECHCARE

Über TechCare Solutions

TechCare Solutions GmbH mit Sitz in Hahnstätten begleitet mittelständische Organisationen bei Betrieb, Wartung und Lebenszyklus-Strategie ihrer Server-, Storage- und Netzwerk-Infrastruktur. Wir verbinden herstellerunabhängige Wartung mit einem strukturierten EOSL-Bewertungsprozess — damit Lifecycle-Entscheidungen kaufmännisch belastbar, sicherheitskonform und dokumentiert sind.

Kontakt: techcaresolutions.de · 24/7 Service-Desk (DE/EN) · Hahnstätten

Methodik & Transparenz

Alle konkreten Zahlen dieses Whitepapers stammen aus den unten genannten, öffentlich zugänglichen Primär- und Sekundärquellen (Hersteller-Policies, testierte Geschäftsberichte, behördliche Vorgaben, Forschungs- und Branchenstudien). Wo Quellen Spannen oder ungesicherte Angaben enthalten, ist dies sprachlich gekennzeichnet („rund", „etwa", „Größenordnung", „laut Geschäftsbericht"). Kosten-Aussagen sind als illustratives Modell ausgewiesen und stellen keine Kundenzusage dar. Hersteller-Fristen folgen den jeweils veröffentlichten Policies; maßgeblich ist im Einzelfall die produktspezifische Ankündigung.

Quellen

[1] **Cisco — End-of-Life Policy.** cisco.com/c/en/us/products/eos-eol-policy.html

[2] **HPE — EOS/EOSL Support.** support.hpe.com/hpesc/public/docDisplay?docId=a00125046en_us

[3] **Dell — Lifecycle Extension / Networking Warranty.** dell.com/en-us/lp/networking-warranty

[4] **Backblaze — Drive Stats 2024.** backblaze.com/blog/backblaze-drive-stats-for-2024/

[5] **Pinheiro/Barroso (Google) — USENIX FAST '07.** research.google/pubs/failure-trends-in-a-large-disk-drive-population/

[6] **The Register — Amazon 6-Jahre-Nutzungsdauer.** theregister.com/2024/02/02/amazon_q4_2023/

[7] **The Register — Microsoft Server-Lebensdauer.** theregister.com/2022/08/02/microsoft_server_life_extension/

[8] **Datacenter Dynamics — Google Server-Nutzungsdauer.** datacenterdynamics.com/en/news/google-increases-server-life-to-six-years-will-save-billions-of-dollars/

[9] **Computer Weekly — Google Einsparungen.** computerweekly.com/news/366557152/Google-saves-almost-3bn-by-running-servers-for-six-years

[10] **Data Center Frontier — Meta.** datacenterfrontier.com

[11] **Europäische Kommission — NIS2-Richtlinie.** digital-strategy.ec.europa.eu/en/policies/nis2-directive

[12] **OpenKRITIS — NIS2UmsuCG / BSIG.** openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

[13] **BSI — IT-Grundschutz, Baustein OPS.1.1.3.** bsi.bund.de

[14] **CISA — Known Exploited Vulnerabilities (KEV) Catalog.** cisa.gov/known-exploited-vulnerabilities-catalog

[15] **UN — Global E-waste Monitor 2024.** ewastemonitor.info/the-global-e-waste-monitor-2024/

[16] **Uptime Institute — Embedded Carbon of IT.** journal.uptimeinstitute.com/what-does-embedded-carbon-of-it-really-represent/

[17] **Tech Carbon Standard.** techcarbonstandard.org

[18] **ISACA Journal — IT Asset Valuation & Risk Model.** isaca.org

[19] **ESRS E1 (CSRD) — EU-Delegierte Verordnung.** eur-lex.europa.eu