

End-of-Life-Software im Geschäftsumfeld – Warum das ein Problem ist

1. Sicherheitsrisiken

Neu entdeckte Sicherheitslücken werden **nicht mehr durch Patches geschlossen**. Angreifer kennen und nutzen bekannte Schwachstellen in EOL-Software gezielt aus – ein beliebtes Einfallstor für Ransomware, Datenlecks und unbefugten Zugriff.

“ **Fazit:** EOL-Software ist ein aktives Sicherheitsrisiko für das gesamte Netzwerk.

2. Compliance und rechtliche Anforderungen

Viele Normen und Gesetze fordern den Einsatz **aktuell unterstützter und gepatchter Software** :

Vorschrift / Norm	Relevanz
DSGVO	Technische und organisatorische Maßnahmen (Art. 32) müssen dem Stand der Technik entsprechen
ISO 27001	Patch-Management und Softwarepflege sind Pflichtbestandteile
BSI IT-Grundschutz	Verlangt ausdrücklich den Einsatz gepflegter Software
Branchenspezifische Vorgaben	z. B. im Gesundheitswesen, Finanzsektor etc.

☐ **Fazit:** Der Betrieb von EOL-Software kann als Verstoß gegen Sorgfaltspflichten gewertet werden – mit Haftungsfolgen für die Geschäftsführung.

3. Ausfall von Versicherungsschutz

Viele **Cyber-Versicherungen** schließen Schäden ausdrücklich aus, wenn EOL-Software im Einsatz war. Im Schadensfall kann die Versicherung die Leistung verweigern, wenn nachweisbar bekannte Sicherheitslücken nicht behoben wurden.

“☐ **Fazit:** Der vermeintliche Kostenvorteil durch ausbleibende Updates kann im Schadensfall zum vollständigen Verlust des Versicherungsschutzes führen.

4. Kompatibilitätsprobleme

EOL-Software wird von anderen Systemen, Diensten und Schnittstellen zunehmend **nicht mehr unterstützt**:

- Neue Betriebssystem-Versionen sind ggf. nicht kompatibel
- Cloud-Dienste und APIs stellen ältere Protokolle ein (z. B. TLS 1.0/1.1)
- Drittanbieter-Software verweigert die Integration mit veralteten Komponenten

“☐ **Fazit:** EOL-Software bremst Modernisierungsvorhaben und führt zu technischen Abhängigkeiten.

5. Fehlender Support und steigende Betriebskosten

- Kein Hersteller-Support mehr bei Problemen

- Fehlerbehebung nur noch durch interne Ressourcen oder teure Drittanbieter
- Spezialwissen wird intern zur Pflege benötigt und ist schwer zu beschaffen

“ **Fazit:** Der laufende Betrieb von EOL-Software verursacht versteckte Kosten, die die Lizenzersparnis oft übersteigen.

Zusammenfassung

Risikobereich	Auswirkung
Sicherheit	Ungepatchte Lücken, Angriffsfläche
Compliance / Recht	Haftung, Bußgelder, Verstöße
Versicherung	Leistungsausschluss im Schadensfall
Kompatibilität	Technischer Stillstand
Betrieb	Steigende versteckte Kosten

Empfehlung

EOL-Software sollte **zeitnah abgelöst oder migriert** werden. Wenn ein sofortiger Wechsel nicht möglich ist, sind zumindest **kompensierende Maßnahmen** zu treffen (z. B. Netzwerksegmentierung, erhöhtes Monitoring, Zugriffsbeschränkung) – und der Zustand ist zu **dokumentieren und zu begründen**.

Version #1

Erstellt: 2026-08-03 14:39:42 UTC von Frank Böttger

Zuletzt aktualisiert: 2026-08-03 14:41:28 UTC von Frank Böttger