BR-Systems

TECHNOLOGIESTRATEGIE & OPEN SOURCE 2026

Kommerzielle Software oder echte Open-Source-Alternativen?

Ein herstellerunabhängiger und praxisnaher Entscheidungsleitfaden für Office, Zusammenarbeit, Infrastruktur und IT-Betrieb

Dokument-ID	BR-WP-OSS-009
Version	1.0
Fachstand	27. Juni 2026
Veröffentlicht	11. Juli 2026
Klassifizierung	Öffentlich – kostenfreier Fachbeitrag
Autor	Benjamin Raulf, BR-Systems
Herausgeber	BR-Systems · IT-Systemhaus · Unterlüß
Standort zum Fachstand	Unterlüß
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

- Nicht nach Lizenzmodell, sondern nach Anforderungen entscheiden
- LibreOffice, Nextcloud, Proxmox und weitere Optionen realistisch einordnen
- Betrieb, Integration, Support und Exit in die Gesamtkosten aufnehmen
- Mit Pilot, Abnahmekriterien und Rückfall statt mit Glaubenssätzen arbeiten

Inhalt

1. Die falsche Frage: kostenlos oder kommerziell?

Open Source und kommerzielle Software sind keine Gegensätze mit automatisch guten oder schlechten Eigenschaften. Open Source beschreibt zunächst den Zugang zum Quellcode und die Rechte der jeweiligen Lizenz. Kommerzielle Anbieter können Open-Source-Produkte mit Support verkaufen; proprietäre Produkte können offene Standards und gute Exportmöglichkeiten bieten. Die sinnvolle Frage lautet deshalb: Welche Lösung erfüllt den fachlichen Bedarf, lässt sich sicher betreiben und hält das Unternehmen langfristig handlungsfähig? Auch Datenschutz, Barrierefreiheit, Branchenanforderungen und die vorhandenen Fähigkeiten der Mitarbeitenden gehören von Beginn an in diese Bewertung.

Ein reiner Lizenzpreisvergleich führt in die Irre. Zur Gesamtbetrachtung gehören Einführung, Migration, Schnittstellen, Hardware, Schulung, Administration, Monitoring, Backup, Hochverfügbarkeit, Support, Ausfälle und ein späterer Wechsel. Open Source kann Abhängigkeiten reduzieren und Eigenbetrieb ermöglichen. Es verlagert jedoch Verantwortung zum Betreiber. Proprietäre Cloud-Dienste können Integration und Komfort bieten, schaffen aber Abhängigkeit von Produktstrategie, Preisen, Datenmodellen und Kündigungsbedingungen. Beide Modelle benötigen klare Eigentümer, überprüfbare Sicherheitskontrollen und eine dokumentierte Notfallvorsorge.

2. Office und Dokumente: Microsoft 365, LibreOffice und Online-Office

LibreOffice umfasst Writer, Calc, Impress, Draw, Base und Math und unterstützt neben ODF zahlreiche Microsoft-Dateiformate [1]. Für Briefe, normale Kalkulationen, Präsentationen und standardisierte Vorlagen kann es eine sehr leistungsfähige Alternative sein. Grenzen müssen mit echten Dateien geprüft werden: komplexe Makros, Access-Anwendungen, spezielle Add-ins, Pivotmodelle, Schriftarten oder pixelgenaue Kundenvorlagen können Anpassungen benötigen.

Für gemeinsame Bearbeitung im Browser kommen beispielsweise Nextcloud Office mit Collabora oder andere Online-Office-Lösungen infrage. Sie ersetzen jedoch nicht automatisch Exchange, Teams, SharePoint, Identitätsmanagement, Gerätesteuerung oder Sicherheitsfunktionen. Ein Unternehmen kann LibreOffice lokal einsetzen, Dokumente in Nextcloud verwalten und E-Mail separat betreiben. Ebenso kann eine hybride Lösung sinnvoll sein, bei der nur Rollen mit zwingender Microsoft-Abhängigkeit entsprechende Lizenzen erhalten.

3. Dateien, Kommunikation und Zusammenarbeit

Nextcloud kombiniert selbst gehostete Dateiablage und Synchronisation mit Freigaben, Kalendern, Kontakten, Talk, Groupware und optionalem Online-Office [2]. Das kann Datenkontrolle und Anpassbarkeit verbessern. Dafür benötigt die Plattform Härtung, Updates, Backup, Monitoring, ausreichende Ressourcen und einen verantworteten Betrieb. Videokonferenzen, große Datenbestände und externe Freigaben müssen unter realer Last getestet werden.

E-Mail ist ein eigener Dienst mit hohen Anforderungen an Zustellbarkeit, Spamabwehr, Archivierung, Hochverfügbarkeit und Missbrauchsschutz. Ein selbst betriebener Mailserver ist möglich, aber nicht automatisch wirtschaftlich. Häufig ist eine Kombination aus gemanagtem E-Mail-Dienst und selbst kontrollierter Datei- oder Kollaborationsplattform sinnvoller. Entscheidend sind klare Datenflüsse, Identitäten, Aufbewahrung, mobile

Geräte, Gastzugänge und ein getesteter Export.

Als Alternative zu Microsoft Teams kann Nextcloud Talk Chat, Audio-/Videoanrufe, Bildschirmfreigabe, Webinare und die Zusammenarbeit mit Dateien innerhalb einer selbst betriebenen Plattform verbinden [6]. Weitere mögliche Bausteine sind Matrix/Element, Mattermost, Rocket.Chat oder Jitsi, jeweils mit anderem Schwerpunkt. Ein Funktionsvergleich muss Gäste, Föderation, mobile Apps, Besprechungsräume, Telefonie, Aufzeichnung, Moderation, Barrierefreiheit und Last berücksichtigen. Für größere Videokonferenzen können zusätzliche Komponenten und ausreichend Bandbreite erforderlich sein. Ein Pilot mit internen und externen Teilnehmern ist unverzichtbar.

4. Infrastruktur, Backup, Monitoring und Service Management

In der Virtualisierung bietet Proxmox VE eine offene Plattform; Proxmox Backup Server ergänzt deduplizierte, verschlüsselte und überprüfbare Sicherungen sowie Remote-Synchronisation und Tape-Unterstützung [3]. Das kann Alternativen zu VMware, Hyper-V oder proprietären Backup-Suiten schaffen. Architektur, Storage, Netzwerk, Quorum, Hardwareunterstützung und Wiederherstellung müssen dennoch geplant und getestet werden. Open Source ersetzt keine Betriebsdisziplin.

Für Monitoring und Inventarisierung existieren unter anderem Zabbix, Icinga, Checkmk, GLPI und weitere Werkzeuge. Für Tickets und Wissensmanagement kommen beispielsweise Zammad oder GLPI infrage. Die Auswahl darf nicht zu einem unverbundenen Werkzeugzoo führen. Schnittstellen, Rollen, Alarmwege, Updatefähigkeit, Dokumentation und verantwortliche Personen sind wichtiger als die Anzahl installierter Funktionen. Eine kleinere, gepflegte Plattform schützt besser als fünf unbeachtete Dashboards.

5. Passwörter, Security und kreative Werkzeuge

KeePassXC speichert Zugangsdaten verschlüsselt in einer lokalen Datenbank und arbeitet plattformübergreifend ohne erzwungenen Cloud-Dienst [4]. Für Einzelpersonen oder kleine klar geregelte Teams kann dieses Modell gut passen. Gemeinsame Tresore benötigen jedoch Berechtigungs-, Synchronisations-, Backup- und Offboardingregeln. Passbolt oder andere serverbasierte Lösungen können Zusammenarbeit erleichtern, erhöhen dafür Betriebs- und Integrationsaufwand.

Für ein zentrales Passwortmanagement im Unternehmen ist Passbolt eine offene Plattform für das gemeinsame, fein abgestufte Verwalten und Teilen von Zugangsdaten; sie kann selbst betrieben oder als Dienst bezogen werden [5]. Zentral bedeutet mehr als eine gemeinsame Passwortdatei: Benutzerlebenszyklus, Gruppen, Freigaben, MFA, Wiederherstellung, Auditprotokolle, Browsererweiterungen, mobile Nutzung, Backup und Notfallzugang müssen geregelt sein. Besonders privilegierte Konten können darüber hinaus Funktionen eines Privileged-Access-Managements benötigen, die ein normaler Team-Tresor nicht vollständig ersetzt.

Bei Firewalls stehen Open-Source-Plattformen wie OPNsense oder pfSense neben kommerziellen UTM-Angeboten von Securepoint und anderen Herstellern. Entscheidend sind nicht allein Anschaffungskosten oder Featurelisten, sondern Updates, Reaktionszeiten, VPN, Reporting, zentrale Verwaltung, Hardwaretausch, Support und vorhandenes Know-how. In regulierten oder zeitkritischen Umgebungen kann ein klarer Hersteller-Supportweg erheblichen Wert besitzen. In anderen Szenarien bietet eine offene Plattform mehr Flexibilität.

Für Bildbearbeitung und Gestaltung existiert nicht „die eine“ Photoshop-Alternative. GIMP ist ein plattformübergreifender Open-Source-Bildeditor für Retusche, Komposition und Bildbearbeitung [7]. Krita richtet sich besonders an digitales Malen und Illustration [8]. darktable ist ein nichtdestruktiver RAW-Workflow für Fotografie [9], während Inkscape Vektorgrafiken bearbeitet [10]. Welche Kombination passt, hängt von RAW-Entwicklung, Farbmanagement, Druck, CMYK-Workflow, Ebenen, Automatisierung, Plugins, Dateiaustausch und Zusammenarbeit ab. Bestehende PSD-Dateien und Agenturprozesse müssen mit repräsentativen Projekten geprüft werden.

6. Eine belastbare Auswahlmatrix und Pilotierung

Eine Entscheidungsmatrix gewichtet fachliche Abdeckung, Interoperabilität, Datenkontrolle, Sicherheit, Betriebskompetenz, Support, Portabilität, Kosten und Benutzerakzeptanz. Ausschlusskriterien werden vor dem Vergleich festgelegt. Herstellerangaben und Community-Versprechen werden durch Dokumentation, Referenzen und einen Pilot überprüft. Datenexport, Wiederherstellung und Rückfall gehören zwingend zum Test, nicht erst zum Vertragsende.

Der Pilot nutzt repräsentative Benutzer, Dokumente, Geräte, Datenmengen und reale betriebliche Störungen. Er misst nicht nur, ob Funktionen vorhanden sind, sondern Bearbeitungszeit, Supportaufwand, Kompatibilität, Performance und Wiederherstellbarkeit. Ergebnisse werden mit belastbaren und nachvollziehbaren Nachweisen dokumentiert. Die Entscheidung kann kommerziell, Open Source oder hybrid ausfallen. Herstellerunabhängigkeit bedeutet, dass der Kundennutzen die Auswahl bestimmt – nicht, dass jedes proprietäre oder jedes offene Produkt grundsätzlich abgelehnt wird.

Nach der Einführung wird die Entscheidung regelmäßig überprüft. Preise, Supportmodelle, Lizenzen, Produktroadmaps, Schwachstellen und interne Fähigkeiten verändern sich. Ein jährlicher Exit-Test kann exemplarisch Daten und Konfigurationen exportieren, Zugangsvoraussetzungen prüfen und die Dokumentation aktualisieren. Dadurch bleibt ein Wechsel eine realistische Option. Gute Anbieterbindung entsteht durch verlässlichen Nutzen und Support, nicht durch fehlende Auswege.

Auch Beschaffung und Vertrag müssen zum Modell passen. Bei Community-Software ist zu klären, wer Fehler analysiert und innerhalb welcher Zeit Unterstützung verfügbar ist. Bei Enterprise-Subscriptions werden Leistungsumfang, Reaktionszeit, unterstützte Versionen und Eskalationsweg geprüft. Bei SaaS kommen Datenstandort, Auftragsverarbeitung, Unterauftragnehmer, Preisänderungen, Kündigung, Exportformat und Löschbestätigung hinzu. Für kritische Systeme wird ein benannter Dienstleister oder internes Kompetenzteam vorgesehen. Die Organisation dokumentiert, welche Komponenten ohne Herstellervertrag betrieben werden und welches Risiko sie dabei bewusst übernimmt. So wird aus „kostenlos heruntergeladen“ ein verantwortetes Betriebsmodell.

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

- Fachliche Anforderungen und Ausschlusskriterien vor Produkten definieren
- Gesamtkosten über mindestens drei bis fünf Jahre vergleichen
- Repräsentative Dateien, Integrationen, Benutzerrollen und Geräte pilotieren
- Betrieb, Updates, Monitoring, Backup und Support verbindlich zuordnen
- Datenexport, Wiederherstellung, Dokumentation und Exit praktisch testen
- Kommerzielle, offene und hybride Modelle gleichberechtigt bewerten
- Entscheidung jährlich anhand realer Betriebsdaten überprüfen

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] LibreOffice: Funktionsumfang, Formate und Einsatz im Unternehmen
https://www.libreoffice.org/discover/libreoffice/

[2] Nextcloud: Open-Source-Plattform für Zusammenarbeit
https://nextcloud.com/platform/

[3] Proxmox Backup Server: Open-Source-Backup-Plattform
https://www.proxmox.com/en/proxmox-backup-server

[4] KeePassXC: lokaler, plattformübergreifender Open-Source-Passwortmanager
https://keepassxc.org/

[5] Passbolt: zentrales Open-Source-Passwort- und Secret-Management
https://www.passbolt.com/

[6] Nextcloud Talk: selbst betriebener Chat und Videokonferenzen
https://nextcloud.com/talk/

[7] GIMP: plattformübergreifender Open-Source-Bildeditor
https://www.gimp.org/

[8] Krita: Open-Source-Programm für digitales Malen und Illustration
https://krita.org/en/

[9] darktable: Open-Source-Fotoworkflow und RAW-Entwicklung
https://www.darktable.org/

[10] Inkscape: Open-Source-Vektorgrafikeditor
https://inkscape.org/

[11] BSI IT-Grundschutz: SYS.2.3 Clients unter Linux und Unix
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/07_SYS_IT_Systeme/SYS_2_3_Clients_unter_Linux_und_Unix_Edition_2023.pdf?__blob=publicationFile&v;=3

Historischer bzw. fachlicher Bezugsstand: 27. Juni 2026. Veröffentlicht: 11. Juli 2026. Online-Quellen zuletzt geprüft: 27. Juni 2026. Der Fachstand ist kein vorgetäuschtes Veröffentlichungsdatum. Dokument-ID BR-WP-OSS-009, 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.