O'REILLY®
Report

Die Betriebssystem auswahl wird neu definiert

Transformation Ihrer Linux-Strategie in einen Wettbewerbsvorteil

Ned Bellavance und Chris Hayner

Red Hat
Enterprise Linux

Die Auswahl Ihres Betriebssystems als Wettbewerbsvorteil

Unterstützen Sie schnelle Innovationen mit einer modernen Plattform. Erfahren Sie, wie Sie sich mit Red Hat Enterprise Linux flexibel und kontrolliert an sich ändernde Anforderungen anpassen können.

Mehr erfahren

Die Betriebssystemauswahl wird neu definiert

Transformation Ihrer Linux-Strategie in einen Wettbewerbsvorteil

Ned Bellavance und Chris Hayner

O'REILLY®

Die Betriebssystemauswahl wird neu definiert
von Ned Bellavance und Chris Hayner

Veröffentlicht von O'Reilly Media, Inc., 141 Stony Circle, Suite 195, Santa Rosa, CA 95401.

Bücher von O'Reilly können für Bildungs-, Geschäfts- und Werbezwecke erworben werden. Für die meisten Titel sind auch Online-Editionen verfügbar (*http://oreilly.com*). Weitere Informationen erhalten Sie von unserer Vertriebsabteilung für Unternehmen/Institutionen: 800-998-9938 oder *corporate@oreilly.com*.

Acquisitions Editing: Megan Laddusaw
Development Editing: Gary O'Brien
Production Editing: Jonathon Owen
Copy Editing: Stephanie English
Cover-Design: Ellie Volckhausen
Interior Design: David Futato
Inside Illustration: Kate Dullea

Februar 2026: Erste Ausgabe

Versionsverlauf der ersten Edition
13.02.2026: Erste Version

Diese Arbeit ist Teil einer Zusammenarbeit zwischen O'Reilly und Red Hat. Lesen Sie unsere Erklärung der redaktionellen Unabhängigkeit.

979-8-341-66786-0

[LSI]

Inhaltsverzeichnis

Einleitung

In der Vergangenheit haben Unternehmen ihre Strategie zum Deployment von Betriebssystemen nur zögerlich geändert. Die Unternehmen agierten nach einfachen technischen Anforderungen sowie Präferenzen und führten nur dann mehrere Betriebssysteme ein, wenn es absolut notwendig war. Änderungen wurden entweder durch die technischen Anforderungen einer wichtigen Anwendung oder durch erzwungene Upgrades von einem Betriebssystem, das das Ende des Supports erreicht, erforderlich. Dies führte dazu, dass Unternehmen die Auswahl des Betriebssystems als eine bereits geklärte Angelegenheit betrachteten – vor allem als technische Notwendigkeit. Die Geschwindigkeit, mit der sich die moderne globale Technologielandschaft weiterentwickelt, macht die Auswahl des Betriebssystems zu einem strategischen Imperativ.

Heutzutage sehen sich Unternehmen mit Veränderungen konfrontiert, die ihre bisherigen Erfahrungen bei weitem übersteigen. In nur wenigen Jahren haben Technologien wie die Containerisierung Workflows flexibler gemacht und die Tools und Strategien für die Anwendungsbereitstellung haben sich radikal verändert. Zudem haben Technologien wie KI und Quantencomputing die bisherigen Vorstellungen völlig auf den Kopf gestellt. Wenn Unternehmen ihre technologischen Anforderungen überdenken, müssen sie auch ihre Strategie bei der Auswahl von Betriebssystemen anpassen, um sich auf diese turbulenten Zeiten einzustellen.

In diesem Bericht werden die treibenden Faktoren dieses neuen strategischen Imperativs untersucht. Wir stützen uns auf empirische Untersuchungen, darunter Umfragen und Analystenberichte, um die

spezifischen Herausforderungen zu ermitteln, denen moderne IT-Organisationen gegenüberstehen. Wie Sie sehen, wird der Wandel von einigen strategischen und modernen Triggern vorangetrieben. Neue Anwendungen, Hardware und Plattformen sind darauf ausgerichtet, mit der beschleunigten Innovationen Schritt zu halten. Abgesehen von der Innovation haben Organisationen mit einem unsicheren wirtschaftlichen Umfeld, anspruchsvollen modernen Cybersicherheitsbedrohungen und geopolitischen Bedenken wie Datenhoheit sowie Validierung der Lieferkette zu kämpfen.

Wir zeigen, wie Unternehmen das Konzept der Betriebssystemauswahl von der operativen Notwendigkeit zum strategischen Wettbewerbsvorteil umdefinieren.

KAPITEL 1

Der strategische Wandel bei der Auswahl von Betriebssystemen

Die Anforderungen einer modernen IT-Umgebung führen zu einem grundlegenden Wandel in der Infrastruktur unternehmensweiter Betriebssysteme und der Strategie zur Anwendungsbereitstellung. Die traditionellen Vorteile eines gleichbleibenden und unerprobten Betriebssystems – vereinfachtes Management und Deployment, reduzierter Trainingsbedarf usw. – werden angesichts des modernen Tempos des Fortschritts neu überdacht. Unternehmen erkennen zunehmend, dass starre Präferenzen hinsichtlich Betriebssystemen eher eine Belastung als eine Stärke darstellen. Flexibilität und die schnelle Erweiterung der Kapazitäten sind wichtiger als die Aufrechterhaltung des Status quo. Unternehmen, die dies nicht berücksichtigen, riskieren, von flexibleren und besser vorbereiteten Mitbewerbern überholt zu werden. Die Geschwindigkeit, mit der sich das technologische Umfeld verändert, wird außerdem durch geopolitische Faktoren erschwert, die sich direkt auf Beschaffungsentscheidungen auswirken.

Wichtige Faktoren und Änderungen

Mehrere Faktoren beeinflussen derzeit die Entscheidungsfindung bei der Auswahl von Betriebssystemen in Unternehmen. Dabei handelt es sich nicht um vereinzelte Trends, sondern um ineinandergreifende Entwicklungen, die den Ansatz von Unternehmen bei ihrer Infrastrukturstrategie grundlegend verändern. Wir gehen später in diesem Bericht ausführlicher auf diese ein.

Die Beschleunigung von Innovationen ist der vorherrschende Faktor bei der Entscheidung für die Auswahl von Betriebssystemen. Einfach ausgedrückt: KI, Automatisierung, Edge und Cloud Computing, IoT und neue benutzerdefinierte Hardware entwickeln sich so schnell, dass ein Teil nicht mithalten kann. Unternehmen machen sich Sorgen über technische Schulden, da sich die Technologie immer schneller weiterentwickelt. Früher benötigten neue Technologien Jahre, um die Produktionsbereitschaft zu erreichen. Jetzt können sie die Bereitschaft innerhalb weniger Monate von der Idee bis zum Deployment erreichen. Das ist der Hauptgrund für die Untersuchung von Betriebssystemen, die Unternehmen im Wettbewerb unterstützen.

Die globale Unsicherheit in Bezug auf Lieferketten nimmt seit einigen Jahren zu. Dies veranlasst Unternehmen dazu, über ihr lokales Umfeld hinaus auf die gesamte Lieferkette zu blicken, die die von ihnen benötigten Tools, Software und Services bereitstellt. Viele Unternehmen betrachten die Abhängigkeit von einem Einzelanbieter, insbesondere im Handel mit dem Ausland, angesichts der Wahrscheinlichkeit von Unterbrechungen in der Lieferkette als potenzielles Risiko. Diese Bedenken haben die Anbieterdiversifizierung sowohl zur Risikominderung als auch zur strategischen Notwendigkeit gemacht.

Der wirtschaftliche Druck hat zugenommen und Unternehmen konzentrieren sich auf Optimierung und ROI (Return on Investment). Der ROI hat nicht nur finanzielle Auswirkungen. Der Fachkräftemangel ist ebenso ein Problem wie Budgetbeschränkungen, die die Auswahl des Betriebssystems erschweren. Früher war es selten, dass ein einzelner Admin sich mit vielen Betriebssystemen auskannte. Es war für ein Unternehmen einfach nicht realistisch, mehrere hochrangige Fachleute zu beschäftigen – einer der Gründe dafür, warum eine Umgebung mit einem einzigen Betriebssystem der Standard war. Daher hat die nachweisliche Benutzerfreundlichkeit des Betriebssystems hohe Priorität.

Aus Sicherheitsgründen haben sich die Infrastrukturanforderungen neu definiert. Immer mehr Systeme werden schneller bereitgestellt, wodurch sich die Angriffsfläche für Unternehmen drastisch vergrößert. Darüber hinaus erfordert die neue Welt der KI-Implementierungen, moderner Cyberbedrohungen und der Compliance moderne Ansätze.

Zu guter Letzt hat die *KI* unser gesamtes bisheriges Verständnis von der Arbeit mit Computern auf den Kopf gestellt. Die Geschwindigkeit, mit der Administrations- oder Entwicklungsteams mithilfe von Large Language Models (LLMs) neue Anwendungen erstellen können, ist ebenfalls beispiellos. Unabhängig davon, ob Sie sich einfach nur mit einem LLM verbinden, um Fragen zu stellen, Ihren eigenen Chatbot entwickeln oder ausgereifte agentische KI-Tools entwickeln – Sie benötigen das beste Betriebssystem für die Aufgabe.

Die Bedeutung der Betriebssystemauswahl

Wie wir gesehen haben, sind bei der Auswahl eines Betriebssystems viel mehr Eingaben erforderlich als je zuvor. Eine schlechte Wahl beim Betriebssystem kann den Zugriff auf wichtige KI-Funktionen einschränken, die Performance beeinträchtigen und Unternehmen Sicherheitsrisiken oder Schwachstellen in der Lieferkette aussetzen. Im Gegensatz dazu kann die Auswahl des richtigen Betriebssystems ein Sprungbrett in diese schnelllebige, moderne und produktive Welt sein. Mit einer sorgfältigen und strategischen Auswahl eines Betriebssystems lassen sich Wettbewerbsvorteile und digitale Flexibilität realisieren – beides ist unerlässlich für Unternehmen, die von neuen Technologiechancen profitieren wollen.

Sehen wir uns nun die einzelnen Auswahlfaktoren etwas genauer an.

Beschleunigte Innovationen

Der unaufhaltsame Fortschritt hat das Standardmodell für Infrastrukturentscheidungen grundlegend verändert. Dieser Abschnitt untersucht diese beschleunigenden Faktoren und wie Unternehmen aufgrund dieser Faktoren ihre Ansätze für Deployment-Strategien ändern.

Schnellere Technologiezyklen

Im Bericht „McKinsey Technology Trends Outlook“ für 2025 heißt es: „Die globale Technologielandschaft erfährt derzeit erhebliche Veränderungen, die von rasanten technologischen Innovationen

vorangetrieben werden."[1] Einfach ausgedrückt: Bei technologischen Entwicklungen wird ein Tempo gemessen, das es noch nie gegeben hat – und die Geschwindigkeit nimmt zu. Betrachten Sie beispielsweise die Geschwindigkeit der Cloud-Einführung. In vielen Fällen begannen Unternehmen langsam und stellten zuerst Entwicklungs-/Testumgebungen in der Cloud bereit und steigerten dann im Laufe der Jahre die vollständigen Produktiv-Workloads. Betrachten Sie außerdem die generative (gen KI) oder agentische KI, die sich innerhalb weniger Monate vom Gedankenexperiment zum Unternehmensprodukt entwickelt hat.

Bei einer traditionellen Infrastrukturstrategie nutzen Unternehmen ihre vorhandenen Betriebssysteme und finden einen Weg, die neue Technologie in diese einzubinden. Das Tempo auf dem modernen globalen Markt ist einfach zu hoch, sodass das nicht praktikabel ist. Entwicklungsteams probieren zunehmend neue Plattformen aus – auf der Suche nach denen, die am besten mit den neuesten Technologien harmonieren –, anstatt zu versuchen, ihre alte Infrastruktur nachzurüsten, damit sie funktioniert. Das ist ein starker Faktor für das Experimentieren mit Betriebssystemen: Wenn das aktuelle Betriebssystem nicht das bieten kann, was Entwicklungs- und Engineering-Teams erwarten, werden sie nach einem Betriebssystem suchen, das dies leisten kann.

Gezielte Investitionen

Überarbeitungen und Änderungen am Betriebssystem werden vor allem durch neue Technologien angestoßen. Dies spiegelt den bereits erwähnten Trend wider, dass sich Entwicklungs- und Administrationsteams vermehrt auf eine hochwertige Infrastruktur verlassen, statt sich mit ihren internen bevorzugten Lösungen zu befassen. Das heißt aber nicht, dass Unternehmen bereit sind, unbegrenzte Ressourcen auszugeben. Es besteht der starke Wunsch, begrenzte Mittel gleich beim ersten Mal richtig auszugeben. Die Auswahl des Betriebssystems ist nicht nur eine Entscheidung bezüglich eines einzelnen Servers, sondern Teil einer viel größeren Plattform. Daher ist die Investitionsentscheidung umso wichtiger.

---

[1] McKinsey & Company, „McKinsey Technology Trends Outlook 2025", 22. Juli 2025, *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top- trends-in-tech*.

Diese Investitionen werden getätigt, um geschäftliche Anforderungen zu erfüllen. Die Technologie entwickelt sich weiter, und Unternehmen müssen mit dieser Entwicklung Schritt halten. So erkennen Unternehmen beispielsweise, dass KI-Funktionen spezielle Infrastruktur- und Entwicklungstools erfordern und dass ihr Standardbetriebssystem dieser Aufgabe möglicherweise nicht gewachsen ist. Unternehmen waren gezwungen, riesige Anlagen mit GPU-basierten Servern aufzubauen, nur um mit den Anforderungen der KI-Tools Schritt zu halten. Vorausschauende Unternehmen erkennen das Tempo von Innovationen und passen ihre Infrastrukturstrategien an, um deren Potenzial zu maximieren. Unternehmen möchten sich schnell genug weiterentwickeln, um den maximalen Wert einer Technologie zuversichtlich zu nutzen, anstatt sie nur bereitzustellen und auf das Beste zu hoffen.

Globale Unsicherheit

Die globale Unsicherheit hat sich zu einem Faktor in der Technologiestrategie entwickelt. Geopolitische Spannungen, die zu wirtschaftlichen Bedenken führen, haben größere Auswirkungen auf die Entscheidungsfindung als in den vergangenen Jahren. Daher können Organisationen ihre Anbieter nicht isoliert betrachten, sondern müssen ihre Optionen unter geopolitischen Aspekten abwägen. Die Sorge der Unternehmen angesichts dieser Unsicherheiten ist größer als je zuvor.[2] Unternehmen müssen sich sowohl mit Tarifen und Vorschriften als auch mit Exportkontrollen befassen. Die anhaltenden und unsicheren geopolitischen Spannungen stellen eine Bedrohung für globale Lieferketten dar, was dazu führen könnte, dass Unternehmen ihre Tech-Ökosysteme innerhalb ihrer eigenen Grenzen belassen.

Tarife und Exportkontrollen

Tarifliche Bedenken und daraus möglicherweise resultierende Währungsverschiebungen verändern die Sichtweise von Unternehmen auf überregionale Einkäufe. Ein langfristiger Vertrag kann ein Jahr nach seiner Unterzeichnung ganz anders aussehen,

[2] McKinsey & Company, „Navigating the New Geopolitical Uncertainty," 16. Januar 2025, *https://www.mckinsey.com/capabilities/geopolitics/our-insights/navigating-the-new-geopolitical-uncertainty*.

wenn es zu starken Schwankungen kommt, die die Währungsdynamik zwischen den Ländern verändern. Dies ist ein entscheidendes Problem, das derzeit die gesamte IT-Strategie betrifft. Das Hinzufügen dieser wirtschaftlichen Dimension bei der Anbieterauswahl ist eine deutliche Abweichung von den bisherigen Überlegungen zu IT-Kaufentscheidungen.

Digitale Souveränität

Der geopolitische Druck geht aber über wirtschaftliche Aspekte hinaus – es gibt regulatorische Anforderungen, die sich von Land zu Land unterscheiden und die Dynamik zwischen Kunden und Anbietern verändern. Dies zeigt sich am deutlichsten beim Cloud Computing, wo regulatorische Bedenken wie die DSGVO (Datenschutz-Grundverordnung) dazu führen, dass Unternehmen „reine EU"-Clouds fordern, um zu gewährleisten, dass ihre Daten innerhalb der EU bleiben. Der Grundstein dafür war der jahrelange Streit, der eine große Anzahl von Unternehmen dazu veranlasste, aktiv nach Cloud-Anbietern zu suchen, die ihren spezifischen regulatorischen Anforderungen besser gerecht wurden.

Wirtschaftliche Unsicherheit

Wirtschaftlicher Druck hat sich schon immer auf die IT ausgewirkt. Der schnelle Wandel in Kombination mit dem globalen Druck macht die Sache noch komplizierter. Die verfügbaren Mittel sind begrenzt, und es herrscht Fachkräftemangel, was bedeutet, dass selbst wenn Mittel für eine neue Administrationsrolle zur Verfügung stehen, möglicherweise keine geeignete Person gefunden werden kann, um diese Stelle zu besetzen.

Aufgrund von Budgetbeschränkungen ist die Kostenoptimierung zu einem wichtigen Faktor bei der Auswahl von Betriebssystemen geworden. Unternehmen konzentrieren sich zunehmend auf ROI und Ausgabeneffizienz. Die Betonung der Kostenoptimierung hat Auswirkungen auf die Auswahl des Betriebssystems, sowohl in Bezug auf finanzielle Ausgaben als auch auf den ROI.

Sicherheit und Datenpannen

Die Sicherheit von IT-Ressourcen ist seit vielen Jahren ein zentrales Anliegen, und Umfragen wie die „2025 Developer Survey" von Stack

Overflow zeigen deutlich, dass Sicherheit, Schwachstellenanalyse und Tests für Entwicklungsteams oberste Priorität haben. „Sicherheits- und Datenschutzbedenken“ wurden als einer der häufigsten Gründe für die Abkehr von Entwicklungsteams von einer bestimmten Technologie genannt.

Angriffe auf die Lieferkette

Zu wissen, woher Software stammt, ist nur ein Teil der Herausforderung. Immer mehr Unternehmen müssen auch wissen, woher die Abhängigkeiten ihrer Software stammen. Dies kann an sich ein Sicherheitsproblem sein: Wird ein Nebenpaket kompromittiert, das für ein großes Softwareangebot entscheidend ist, besteht Gefahr für das Unternehmen. Das wohl bekannteste Beispiel hierfür ist der SolarWinds-Hack aus dem Jahr 2021, bei dem unzählige SolarWinds-Kunden aufgrund einer unsicheren Lieferkette von SolarWinds Datenpannen ausgesetzt waren. Das Problem der Abhängigkeiten ist jedoch immer noch vorherrschend. Vor kurzem wurde das JavaScript Repository npm Opfer eines Lieferketten-Angriffs, durch den vermeintlich sichere Pakete auf den Geräten der Nutzenden installiert wurden, um Kryptowährung zu schürfen.

KI ist nachweislich sowohl ein Sicherheitsrisiko als auch ein Vorteil für Produktivität und Geschäftsfunktionen. KI-gestützte Angriffe sind in den letzten Jahren explodiert und es gibt keine Anzeichen einer Verlangsamung. In einem aktuellen Bericht der Kreditauskunftei Experian wird KI als eine so bedeutende Bedrohung identifiziert, dass sie ab 2026 menschliche Fehler als Hauptursache von Datenpannen überholen wird.[3]

Bedenken hinsichtlich der Quantenverschlüsselung

Die neue Bedrohung durch Quantencomputing wurde in den letzten Jahren erkannt und erforscht. Die Sorge ist, dass aufgrund der völlig anderen Herangehensweise von Quantencomputern an das Problem der klassischen Verschlüsselung letztendlich (wahrscheinlich noch in diesem Jahrzehnt, doch dieser Zeitrahmen ist umstritten) alle bestehenden Verschlüsselungsalgorithmen innerhalb von Sekunden geknackt werden können. Dadurch werden alle „klassisch“

[3] Experian, 2026 Data Breach Industry Forecast, 5. Dezember 2025, *https://www.experian.com/ Thought-leadership/business/2026-data-breach-industry-forecast- report*.

verschlüsselten Dateien und Datenspeicher komplett angreifbar. Hacker wissen das und haben so viel wie möglich heruntergeladen, obwohl sie die Verschlüsselung noch nicht überwinden können. Dieses Sicherheitsrisiko wird auch als „Harvest now, decrypt later (Jetzt sammeln, später entschlüsseln)“ bezeichnet.

Post-Quanten-Kryptografie (PQC) bezieht sich auf die nächste Generation von Verschlüsselung, die speziell für die Leistungsfähigkeit von Quantencomputern entwickelt wurde. Diese Art der Kryptographie ist ein neues Thema in der Informatikforschung, und noch nicht alle Betriebssysteme nutzen sie. Das Verschlüsseln von Technologie mit PQC-Algorithmen bedeutet, dass Hacker beim Sammeln von Informationen und späteren Entschlüsselungen keinen Erfolg haben.

KI

KI hat sich zu einer dominierenden Kraft entwickelt, die viele Kaufentscheidungen im Technologiebereich beeinflusst. Dieser Trend ist seit einiger Zeit klar, und die Dynamik scheint sich nicht abzuschwächen. Interessanterweise bestimmt die KI, ebenso wie die sie umgebende Technologie, zunehmend die Auswahl des Betriebssystems.

Vibe Coding

Dank KI hat sich der moderne Use Case eines Betriebssystems verändert. Programmierung, Datenanalyse und Geschäftsanalyse sind jetzt auch für Personen ohne spezielle oder technische Kenntnisse zugänglich. Um ein einzelnes Beispiel zu nennen: Vibe Coding ist eine KI-gestützte Methode zur Anwendungsentwicklung, ohne dass Nutzende unbedingt Profis im Programmieren oder in der Anwendungsentwicklung sein muss. Auf dem Markt werden zunehmend Betriebssysteme bevorzugt, die mit KI-gestützten Entwicklungstools arbeiten, die solche Methoden ermöglichen.

Hardwarebeschleunigung

Darüber hinaus gibt es bei KI nach wie vor traditionelle Use Cases, die umfangreiche Betriebssystemfunktionen erfordern. Wenn Sie Aufgaben wie Inferenz, Modelltraining oder das Hosting eines LLM-basierten Chatbots ausführen, müssen die Betriebssysteme effektiv

mit GPUs und anderer benutzerdefinierter Hardware interagieren. Spezialisierte Chips ermöglichen schnellere, umfangreichere und vielseitigere KI-Funktionen, wodurch die Hardwarekompatibilität zu einem entscheidenden Faktor bei der Auswahl wird. KI-gesteuerte Automatisierungs- und Verwaltungsfunktionen werden weiterhin die verfügbaren Hardwareressourcen eines Betriebssystems belasten. Folglich wirkt sich die Fähigkeit eines Betriebssystems, mit moderner Hardware zu interagieren, auf die Auswahl des Betriebssystems aus.

Fazit

Die Marktveränderungen, die Unternehmen dazu veranlassen, die Auswahl ihres Betriebssystems zu überdenken, bieten eine strategische Chance, neue Möglichkeiten auszuloten. Unternehmen erkennen die beispiellosen Chancen, die das aktuelle globale Chaos und die Innovationsexplosion mit sich bringen. Sie arbeiten zunehmend proaktiv daran, neue Möglichkeiten zu erkunden, anstatt zu versuchen, bestehende Plattformen beizubehalten, die möglicherweise nicht mit den Änderungen Schritt halten können. Dieser Wandel der Auswahl des Betriebssystems von einem Problem hin zur Chance stellt eine der wichtigsten Möglichkeiten zur Verbesserung der geschäftlichen Abläufe dar. Es geht darum, inmitten eines stürmischen Wandels das beste Tool für die jeweilige Aufgabe zu finden, anstatt einfach so weiterzumachen wie bisher.

KAPITEL 2

Vom Problem zur Lösung

In Kapitel 1 haben wir mehrere kritische Faktoren für die Auswahl von Betriebssystemen identifiziert: Innovationsbeschleunigung, globale Unsicherheit, wirtschaftlicher Druck, Sicherheitsbedenken und die Anforderungen von KI. Diese Probleme zu erkennen ist jedoch nur der Anfang. Die Herausforderung für IT-Führungskräfte besteht darin, effektiv auf diesen Druck zu reagieren, ohne dabei neue operative Verwirrung oder Schwachstellen zu schaffen. Erfolgreiche Unternehmen sind sich dieser Probleme bewusst und reagieren darauf auf produktive und wettbewerbsfähige Weise. In diesem Kapitel befassen wir uns mit diesen Herausforderungen und erläutern, wie wir vom Problem zur Lösung kommen können.

Strategien zur beschleunigten Innovation

Die Beschleunigung von Innovationen hat sich zu einer treibenden Kraft für IT-Führungskräfte entwickelt. Das liegt nicht nur an der Notwendigkeit, mit der Konkurrenz mitzuhalten. Dank Konzepten wie dem Pioniervorteil sichern sich die Organisationen, die am schnellsten handeln können, die größten Gewinne. Dies hat erhebliche Auswirkungen auf die Strategien zur Auswahl von Betriebssystemen, da das Betriebssystem die Basis für die beschleunigten Innovationen bildet, die ein Unternehmen nutzen möchte. Solche Innovationen führen Unternehmen in unbekanntes Terrain. Deshalb ist ein umsichtiges Vorgehen wichtig, und Entscheidungen sollten auf der Basis klar erkennbarer Anforderungen und Vorteile getroffen werden. Innovationsbeschleunigung bedeutet nicht, dass Änderungen nach Lust und Laune vorgenommen werden.

Ein modernes Betriebssystem muss Experimente ermöglichen und gleichzeitig Sicherheit, Performance und Zuverlässigkeit bieten.

Durchdachtes Experimentieren bei hohem Tempo

Die Beschleunigung der technologischen Innovation hat zu Marktbedingungen geführt, bei denen herkömmliche Entwicklungs- und Bewertungsmethoden einfach nicht schnell genug sind. In der Anwendungsentwicklung ist dies seit einiger Zeit ein Trend: vom jährlich wiederkehrenden Release-Zyklus nach dem Wasserfallmodell über die agile Softwareentwicklung und die durch DevOps ermöglichte kontinuierliche Bereitstellung bis hin zu den heutigen hyperschnellen Deployment-Modellen mit mehreren Updates pro Tag. Derselbe Trend lässt sich in der gesamten Technologielandschaft beobachten, und IT-Führungskräfte erkennen, dass sie nachziehen müssen, um der Entwicklung einen Schritt voraus zu sein.

Eine solche Innovationsgeschwindigkeit erfordert schnelle Entwicklungs- und Testzyklen bei gleichzeitiger Einhaltung einer Sicherheits-Baseline, die die Unternehmen nicht gefährdet. Für effektive Experimente sind moderne Sandbox-Umgebungen erforderlich, die ähnliche Bedingungen wie in der Produktion bieten, ohne die Unternehmensdaten (oder das Betriebssystem, das die Anwendung hostet) zu gefährden. Dies ist die effizienteste Methode, um realistische Testumgebungen bereitzustellen, mit denen sich die Performance unter tatsächlichen Produktionsbedingungen schnell bewerten lässt.

In ähnlicher Weise benötigen Anwendungen einen schnellen, zuverlässigen Prozess vom Test bis hin zur Produktion. Dieser Prozess sollte nahtlos ablaufen und sicherstellen, dass Anwendungen, die sich im Testbetrieb bewährt haben, auch im Produktionsbetrieb zuverlässig funktionieren. Dabei geht es nicht nur um Benutzerfreundlichkeit: Dank der Zuverlässigkeit und Wiederholbarkeit sind Upgrades genauso effizient (und sicher) wie das anfängliche Test-Deployment.

Angesichts dessen bietet es sich an, bei der Auswahl eines Betriebssystems eine vorsichtig offene Haltung einzunehmen. Agilität ist in Zeiten beschleunigter Innovation ein klarer strategischer Vorteil. Das Betriebssystem hostet letztendlich die betreffenden Anwendungen. Da sich die Anwendungsanforderungen so schnell ändern, müssen Unternehmen darauf vertrauen können, dass das Betriebssystem mit diesen Anforderungen mithalten kann. Dieser differenzierte Ansatz wurde durch Studien und Analysen von

Unternehmen wie IDC und McKinsey bestätigt. Im Juni 2024 stellte McKinsey fest: „Die Wahrheit ist, dass es keinen einheitlichen Ansatz gibt. Stattdessen können Unternehmen ihr Streben nach Innovation mit der Notwendigkeit einer robusten und zuverlässigen technologischen Infrastruktur in Einklang bringen.“[1]

Dennoch müssen Tools und Technologien sorgfältig ausgewählt werden. Veränderungen zum Selbstzweck sind ein Risiko – es entsteht zusätzliche Komplexität ohne erkennbaren Nutzen, wenn eine so grundlegende Komponente wie ein Betriebssystem ohne angemessene Kontrolle verändert wird. Der stärkste Indikator für eine solche Veränderung ist derjenige, der klare Vorteile im Hinblick auf die organisatorische Leistungsfähigkeit aufzeigt. Diese Vorteile müssen nachweisbar sein, damit ein neues Betriebssystem nicht nur deshalb ausgeführt werden kann, weil es neu ist. Daher sollten Organisationen nicht nur auf ihre aktuellen Funktionen achten, sondern auch auf das zukünftige Potenzial und die Stabilität ihres Betriebssystems.

Sicherheitsorientierte Architektur

Das Tempo technologischer Innovationen kommt nicht nur legitimen Unternehmen zugute. Cyber-Sicherheitsbedrohungen entwickeln sich ständig weiter, sodass Unternehmen anfällig für Angriffe bleiben, wenn sie nicht für ausreichende Sicherheit sorgen. Marktstudien wie der „*2025 Global Threat Report*“ von CrowdStrike zeigen deutlich, dass sich Cyber-Bedrohungen weiterhin schneller entwickeln als die Cyber-Abwehr. Die moderne Bedrohungslandschaft stellt in nie dagewesenem Ausmaß sich ständig weiterentwickelnde Herausforderungen, für deren Bewältigung viele traditionelle Sicherheits-Frameworks und IT-Tools einfach nicht ausgelegt sind. Auf diese modernen Bedrohungen vorbereitet zu sein, ist zu einer strategischen Notwendigkeit geworden.

Bei der Implementierung eines neuen Betriebssystems muss daher die Sicherheitsarchitektur berücksichtigt werden. Unternehmen, die Sicherheitsfragen und -überprüfungen nicht in die Auswahlprozesse für Betriebssysteme integrieren, sehen sich einem doppelten Risiko gegenüber: den auf dem System gehosteten Anwendungen und der

[1] McKinsey, „Rethinking Conventional Wisdom: Future of Digital Tech Infrastructure“, 26. Juni 2024, *https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/ tech-forward/rethinking-conventional-wisdom-future-of-digital-tech-infrastructure*.

Sicherheit sowie Zuverlässigkeit des Systems selbst. Dies gilt insbesondere zum Zeitpunkt der Erstellung dieses Dokuments, da Betriebssystemanbieter zunehmend KI-Features in ihre Betriebssysteme integrieren und ihnen enorme Zugriffsrechte gewähren, um Systemadministrationsaufgaben automatisiert durchzuführen.

Datensicherheit ist unerlässlich

Dies führt zum wichtigsten Punkt: Betriebssysteme müssen Umgebungen bieten, in denen Anwendungen sicher ausgeführt und Daten sicher gespeichert werden können. Ein Unternehmen muss sich darauf verlassen können, dass alles, was ausgeführt wird, sicher bleibt – unabhängig davon, ob es sich um eine integrierte Komponente eines Betriebssystems oder eine Anwendung handelt, die ein Betriebssystem hostet. Dabei sind die folgenden 3 Kategorien von Datensicherheit zu berücksichtigen:

*Data at Rest (*Daten im Ruhezustand)
: Diese Daten werden für die spätere Verwendung gespeichert.

Data in Motion (Daten in Bewegung)
: Diese Daten werden auf unterschiedliche Weise übertragen, sei es zwischen verschiedenen Systemen oder innerhalb eines Systems, von Anwendung zu Anwendung.

Data in Use (Daten in Verwendung)
: Diese Daten werden aktiv von der Computing-Plattform verarbeitet.

Die Sicherung von Daten im Ruhezustand und Daten in Bewegung wird häufig durch Verschlüsselung gelöst. Die Sicherung von Daten in Verwendung ist eine größere Herausforderung. Moderne Betriebssystemarchitekturen lösen dieses Problem durch die Integration einer Trusted Execution Environment (TEE). Dies ist ein Teil des Systems, der auf hochvertrauenswürdige Software beschränkt ist und nur über streng kontrollierte Mechanismen zugänglich ist. Sämtliche Prozesse, die innerhalb einer TEE ausgeführt werden, sind von außerhalb der TEE in der Regel nicht zugänglich. Dabei kann es sich sowohl um eine hardware- als auch eine softwarebasierte Lösung handeln, die oft über einen Server hinausgeht und erfordert, dass Treiber und Kompatibilität aktuell gehalten werden, um keine Funktionen zu verlieren. Wie dies in der Praxis aussieht, ist je nach

Anbieter unterschiedlich und wird in diesem Bericht nicht behandelt. Es ist jedoch unerlässlich, dass Anwendungen in solchen sicheren Umgebungen ausgeführt werden können.

KI-Workloads brauchen mehr als nur Schutz

Während verschiedene Arten von Rechen-Workloads die zuvor erörterten Anforderungen an Datenschutz und Datensouveränität erfordern, sind KI-Workloads aus 2 zusätzlichen Gründen besonders anfällig: Sie sind neu, datenintensiv und rechenintensiv.

Dass KI-Workloads neu sind bedeutet, dass Produktions-Workloads nicht so gründlich getestet werden konnten wie Standard-Workloads. Sicherheit ist eine gemeinsam zu bewältigende Aufgabe, und der Markt kann viel mehr Tests und Qualitätssicherung leisten, als es ein einzelner Anbieter allein könnte. Dies gilt sowohl für das Produkt selbst als auch für die Art und Weise, wie es konfiguriert/genutzt wird. In seinem *„Tenable Cloud Security Risk Report 2025“* berichtete Tenable, dass Cloud-Workloads, die KI unterstützen, anfälliger sind als andere Workloads. Unabhängig davon, wo die Workload gehostet wird, erfordert die datenintensive Natur von KI in Kombination mit persistenten Fehlkonfigurationen und Schwachstellen ein neues Maß an Sorgfalt beim Thema Cybersicherheit.

Unternehmen müssen bei der Bewertung eines Betriebssystems KI-spezifische Risiken berücksichtigen. Andernfalls kommt es zu einem unbekannten Risiko, das aktuelle und zukünftige Workloads gefährden könnte.

Fazit

Eine bewusste Entscheidungsfindung für Betriebssysteme erfordert grundlegende Änderungen der Art und Weise, wie Unternehmen Technologien bewerten. Die in diesem Kapitel vorgestellten Herausforderungen bieten die notwendige Struktur, um durch die richtigen Entscheidungen einen Wettbewerbsvorteil zu maximieren. Am Ende dieses Berichts befassen wir uns mit einem Entscheidungsprozess, der sämtliche dieser Entscheidungen umfasst. Derzeit ist klar, dass in Bezug auf das Deployment von Betriebssystemen neue Denkweisen erforderlich sind: Moderne Herausforderungen erfordern moderne Lösungen. Unternehmen, die sich diesen Herausforderungen stellen und strategisch denken, sind

besser in der Lage, neue Technologien zu nutzen und ihren Wettbewerbsvorteil zu maximieren.

KAPITEL 3

Die moderne Linux-Plattform

Moderne Unternehmen haben Serverabläufe weitgehend auf Linux standardisiert. Dies wurde mindestens in den letzten 10 Jahren in zahlreichen Studien bestätigt. Um nur eine zu zitieren: Das SQ Magazine berichtete im August 2025, dass 61,4 % der großen Unternehmen mindestens eine unternehmenskritische Workload auf Linux ausführen und dass 78,3 % der mit dem Internet verbundenen Webserver mit Linux ausgeführt werden.[1] Diese vorherrschende Position ist das Ergebnis vieler Jahre des Wachstums – ein Trend, der keine Anzeichen einer Verlangsamung zeigt.

In vielen Fällen gehen Aussagen jedoch nie auf einzelne Distributionen ein, was viele Entscheidungstragende zu der Annahme verleitet, dass „sämtliche Linux-Versionen gleich sind". Das stimmt nicht. Zwar verwenden sämtliche Linux-Distributionen den grundlegenden Linux-Kernel, aber die Art und Weise, wie der Kernel bereitgestellt wird, und die Tools und Anwendungen, die er umfasst, können sich sehr unterscheiden.

Ein Unternehmen muss daher die wichtigsten Unterscheidungsmerkmale der Betriebssysteme identifizieren, die es in die engere Wahl zieht. Viele moderne Betriebssysteme verfügen mittlerweile über hochmoderne Features, doch manche setzen diese anders um als andere, und manche Features sind schlichtweg nicht überall verfügbar. Zu den nützlichsten Features gehören moderne, sichere Deployment-Modelle, KI-integrierte Systemtools, Flottenmanagementtools, unternehmensgerechte Sicherheit sowie

[1] Robert A. Lee, „Linux Statistics 2025: Desktop, Server, Cloud & Community Trends," *SQ Magazine*, aktualisiert am 18. November 2025, *https://sqmagazine.co.uk/linux-statistics*.

erweiterter Support und Partnerzertifizierungen. Darüber hinaus müssen die Funktionen eines Betriebssystems im Hinblick auf die Anforderungen der darauf ausgeführten Workloads betrachtet werden – erstklassige Funktionen, die den modernen Anforderungen gerecht werden.

Revolutionäres Betriebssystem-Deployment

Am Deployment von Betriebssystemen hat sich im Laufe der Jahre nicht viel geändert. Bei dem herkömmlichen Deployment installierte ein Installationsprogramm den Kernel und andere Tools auf der Festplatte, woraufhin die Nutzenden die Anwendungen installierten. Die Einführung der Paketverwaltung war ein großer Fortschritt für die Anwendungsverwaltung und die Systemadministration, da die Nutzenden dadurch nicht mehr bei den einzelnen Installationen oder Aktualisierungen von Anwendungen den Code immer wieder neu kompilieren mussten.

Eine moderne Linux-Distribution sollte einen Deployment-Modus bieten, bei dem Systeme im Wesentlichen unveränderliche Container sind, die nach Bedarf ein- und ausgelagert werden können. Sie können ein neues -Image herunterladen und ein einfacher Neustart genügt, um ein Upgrade (oder Downgrade) der jeweiligen Komponente des Systems durchzuführen. Dies sorgt für Sicherheit, Zuverlässigkeit und die Gewissheit, dass auf sämtlichen Systemen der Flotte die erwarteten Versionen der Binärdateien und Libraries ausgeführt werden.

Sie können die erstellten Images auf dieselbe Weise wie Anwendungscontainer (oder Images) verwalten, jedoch in noch kleinerem Umfang – Binärdateien und sogar den Betriebssystem-Kernel selbst. Dies ist eine wesentliche Verbesserung gegenüber dem vorherigen paketbasierten Update-Modell. Obwohl Pakete ein besseres Deployment-Modell der Kompilierung aus dem Quellcode darstellen, haben sie dennoch eigene Probleme mit der Kompatibilität, Paketanforderungen und potenziellen Versionskonflikten. Ein containerbasiertes Modell beseitigt diese Probleme, da sämtliche Inhalte in einem Image enthalten sind. Die Versionen sämtlicher im Container enthaltenen Komponenten bleiben konsistent, wodurch die Bedenken vieler Systemadministratoren hinsichtlich eines Konfigurationsdrifts erheblich gemindert werden. Außerdem ist die Image-Installation

viel schneller und einfacher – Sie müssen das Image einfach nur herunterladen, anwenden und neu starten.

Images bieten auch Sicherheitsvorteile, da sie unveränderlich sind. Das bedeutet, dass ein Angreifer oder eine Malware das Image weder vor Ort modifizieren noch ersetzen können. Da diese Images ähnlich wie Anwendungscontainer verwaltet werden, können Sie das Image mit Standard-Containertools wie Podman oder vielen anderen gängigen Containerplattformen anzeigen. Dank dieser Vertrautheit mit den Tools können Administrationsteams, die bereits mit Anwendungscontainern vertraut sind, Betriebssystem-Images schnell und sicher bereitstellen.

Schließlich können die von Ihnen erstellten Images beliebig verwendet werden. Es spielt dabei keine Rolle, ob Sie das Deployment in physischen, virtualisierten, Cloud- oder Edge-Umgebungen durchführen. Das Image wird überall auf dieselbe Weise bereitgestellt und ausgeführt. Außerdem lassen sich Images von Anfang bis Ende einfacher verwalten. Abbildung 3-1 zeigt einen beispielhaften Prozess im Image-Modus in 3 einfachen Schritten: Erstellen von Images, Bereitstellen von Images und Verwalten der Images nach dem Deployment.

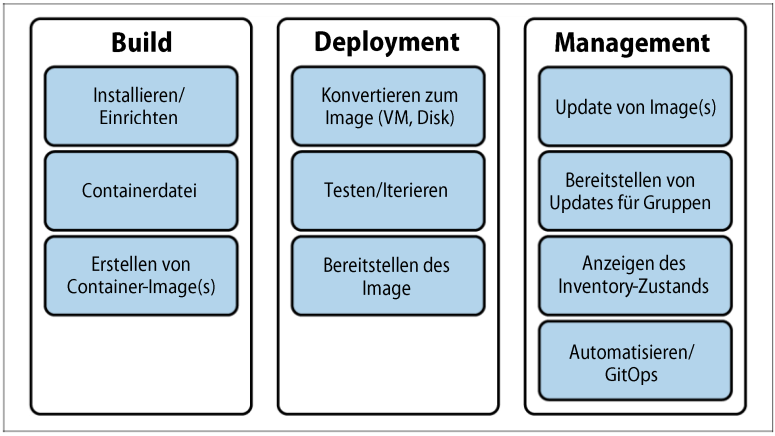

Abbildung 3-1. Ein Beispiel für ein containerisiertes (Image-Modus) Betriebssystem-Deployment-Modell

KI-gestützte Systemadministration

Viele Anwendungsentwicklungsteams beginnen damit, KI direkt in Tools zur Systemadministration wie Terminal-Emulators zu integrieren, die Zugriff auf die Befehlszeile bieten. Sie sind äußerst nützlich, da Administratoren damit die LLMs ihrer Wahl abfragen können, ohne ein Browserfenster oder eine separate Anwendung öffnen zu müssen. Der nächste logische Schritt für Betriebssystemhersteller ist, dasselbe zu tun und KI direkt in das Betriebssystem selbst zu integrieren. Anschließend kann der KI-Assistent über die Befehlszeile aufgerufen werden, unabhängig davon, welches Terminal der Endbenutzende wählt. Diese Funktion bietet einen großen Vorteil für Admins mit unterschiedlichen Kompetenzniveaus, doch insbesondere unerfahrene Admins können davon profitieren, dass sie einem KI-Assistenten direkt über die Befehlszeile Fragen stellen können, um ihre Vorgehensweise spontan zu überprüfen und sicherzustellen, dass sie das Richtige auf die richtige Art und Weise tun.

Wie bei der Verwendung sämtlicher KI-Tools ist auch bei der Nutzung von Befehlszeilenassistenten Vorsicht geboten. Es kann sein, dass Sie Ihre Frage an einen Befehlszeilenassistenten präzisieren müssen, um eine genaue Antwort zu erhalten, insbesondere wenn Sie den Assistenten bitten, Code zu generieren, wie etwa ein Shell-Skript.

Im Zweifelsfall sollten unerfahrene Admins ihre erfahrenen Kolleginnen und Kollegen fragen, ob die Antworten des KI-Assistenten tatsächlich das leisten, was sie erwarten.

Das Tool könnte leistungsfähiger sein als bloß Grundlagen zu verstehen, wie einfaches Bash-Skripten – Befehlszeilenassistenten können praktische Tipps zur Konfiguration von Anwendungen und Services geben und Betriebssystemffeatures zur Fehlerbehebung nutzen. Entscheidend ist, dass diese Assistenten speziell für Linux im Allgemeinen und die Feinheiten der Distribution sowie für ihre spezifischen Bedürfnisse und Anforderungen trainiert werden. Diese Art des Fine Tunings ist eine bekannte Technik in der KI: Ein speziell angepasstes Modell im Gegensatz zu einem generischen LLM, das ausschließlich auf die richtigen Arten von Dokumentation trainiert und darauf ausgelegt ist, Halluzinationen zu minimieren, macht ein solches Tool zu einem bedeutenden Unterscheidungsmerkmal bei integrierten Tools.

Ein Befehlszeilenassistent ist besonders nützlich für Tools wie Security-Enhanced Linux (SELinux) und die integrierte Firewall. Beide sind für den Systembetrieb sehr wichtig, aber auch komplex, und ihre Konfigurationen werden in den meisten Fällen nur selten geändert. Ein Systemadministrator wird schnell merken, dass sich diese Tools viel schneller und einfacher konfigurieren lassen, wenn dabei ein Befehlszeilenassistent genutzt wird. Darüber hinaus verfügt das KI-Tool über eine Vielzahl geprüfter Beispiele, sodass es ein gutes Verständnis von Best Practices hat und Fehlkonfigurationen erkennen kann, die selbst für erfahrenen Admins nicht offensichtlich sind.

Schließlich können Befehlszeilenassistenten eingesetzt werden, um die Struktur der verwendeten Tools zu verstehen. Wenn Sie beispielsweise wissen möchten, wie moderne hostbasierte Firewalls implementiert sind, können Sie einfach den Assistenten fragen. Dieser fragt relevante Dokumentationsressourcen nach Best Practices und Beispielen ab, die auf Ihren Eingaben basieren. Sie erhalten eine leicht verständliche Antwort, die die Änderungen an der Konfiguration oder am Quellcode ergänzt, damit Sie besser verstehen, was empfohlen wird und warum.

Flottenmanagement-Tools

Die beiden besprochenen Tools sind leistungsstark und vereinfachen das Systemmanagement auf individueller Systemebene erheblich. Das nächste Tool geht noch einen Schritt weiter und hilft Nutzenden dabei, ihre gesamte bereitgestellte Linux-Umgebung proaktiv zu managen. Ein solches Tool sollte über umfassende Anbindungen an sämtliche Funktionen eines Betriebssystemherstellers verfügen, sodass die gesamte Plattform von einem einzigen Ort aus gemanagt werden kann, was die Verwaltung und die Auditanforderungen vereinfacht. Im Idealfall sollte es auch ein Planungsfeature beinhalten, mit der Unternehmen die Lifecycles ihrer bereitgestellten Anwendungen besser verstehen und wissen können, wie diese sich auf die in ihrer Umgebung ausgeführten Systeme auswirken. Diese Integrationen könnten Sicherheits- und Konfigurationsvalidierungen im gesamten Unternehmen in Echtzeit ermöglichen.

Roadmap-Features liefern detaillierte Informationen über bevorstehende App- und Betriebssystem-Releases, sodass Unternehmen Upgrades auf der Basis erwarteter neuer Features

planen könnten, anstatt zu reagieren, sobald diese veröffentlicht werden.

Flottenmanagementtools könnten ebenfalls dazu verwendet werden, die Systeme auf dem neuesten Stand zu halten. Koordiniertes Patching (entweder automatisiert oder geplant und als erfolgreich bestätigt), Feature-/Software-Updates oder Rollouts und ein zentralisiertes Konfigurationsmanagement machen das Management von 1.000 Servern so einfach wie das Management eines einzelnen Servers.

Unternehmensgerechte Sicherheit

Ein Betriebssystem, das im Hinblick auf die Sicherheit entwickelt wurde, sollte mehr bieten als die zuvor erwähnten Sicherheitsvorteile wie unveränderliche Images und Konfigurationsmanagement.

Einer der am meisten diskutierten zukünftigen Angriffe dreht sich um die Post-Quanten-Kryptografie. Wie bereits in einem vorherigen Kapitel erläutert, bietet PQC Organisationen quantenresistente Algorithmen für Schlüssel, Verschlüsselung und digitale Signaturen. Dies trägt zur Zukunftssicherheit von Daten und Anwendungen bei und ist ein wichtiges Merkmal, das Sie beim Vergleich von Betriebssystem-Distributionen beachten sollten.

Ein unternehmensgerechtes Betriebssystem bietet außerdem robuste Sicherheitsfeatures für die Lieferkette. Dies beschränkt sich nicht nur auf das Betriebssystem – es handelt sich um eine Plattformstrategie, die Entwicklungsteams und Unternehmen, die nach dem DevSecOps-Ansatz arbeiten möchten, neue Möglichkeiten eröffnet. Das einfachste Beispiel hierfür ist ein vertrauenswürdiger Speicherort zum Hosten bekanntermaßen fehlerfreier Anwendungsabhängigkeiten, aber dies kann noch viel tiefer gehen. Die ideale DevSecOps-Plattform sollte Entwicklungsteams eine End-to-End-Sicherheits-Pipeline für ihre Anwendungen und Abhängigkeiten bieten.

Die Kombination aus PQC-Schutz, automatisierten Sicherheitstools für Administrations- und Entwicklungsteams und proaktivem Software-Management bildet eine mehrschichtige Abwehrmaßnahme für aktuelle Bedrohungen und Herausforderungen. Entscheidend ist, dass diese Sicherheit durch die vom Unternehmen verwendeten Tools und das Betriebssystem gewährleistet wird, sodass es sich um eine voll funktionsfähige Plattform handelt. Unternehmen sind somit nicht

gezwungen, umfangreiche Investitionen in externe Sicherheitslösungen von Drittanbietern zu tätigen.

Erweiterter Hardware- und Software-Support sowie Zertifizierung

So leistungsstark ein Betriebssystem auch ist, Unternehmen benötigen für ihren Betrieb dennoch externe Kompatibilität. Dies gilt sowohl für die Hardware, auf der das Betriebssystem ausgeführt wird, als auch für die Drittanbietersoftware, die im laufenden System selbst genutzt wird.

In der heutigen Zeit unterliegt die Hardwarekompatibilität einem rasanten Wandel. Insbesondere KI-Hardware verändert sich extrem schnell und erfordert Kompatibilität und Betriebssystemtreiber. Es ist wichtig, dass die von Ihnen gewählte Distribution hier herausragende Leistungen erbringt und aktuelle KI-Libraries, -Treiber und -Anwendungen sowie Hardware-Optimierungen für Hersteller wie NVIDIA, Intel und AMD bietet. Neben diesen 3 Hauptanbietern müssen Betriebssystemhersteller jedoch über ein robustes Drittanbieter-Ökosystem verfügen, das seinen Endbenutzenden die aktuellsten Funktionen schnell, sicher und zuverlässig bereitstellt.

Fazit

Die Sicherheit, das IT-Ökosystem und der Umfang der Features eines Betriebssystems wirken zusammen, um die zu Beginn dieses Berichts identifizierte Herausforderung zu bewältigen, die darin besteht, dass die Prüfung anderer Betriebssysteme eine strategische Notwendigkeit darstellt. Die in diesem Kapitel beschriebenen Hauptmerkmale heben ein Betriebssystem sowohl hinsichtlich seiner Leistungsfähigkeit als auch seiner Verwaltbarkeit von seinen Mitbewerbern ab. Die technologischen Fortschritte in Verbindung mit den starken Partnerprogrammen stellen strategisch wichtige Differenzierungsmerkmale dar, die bei der Auswahl einer neuen Betriebssystemplattform unbedingt berücksichtigt werden müssen.

KAPITEL 4

Nächste Schritte

Die Auswahl des Betriebssystems ist eine grundlegende Entscheidung für Unternehmen, die Auswirkungen auf ihre Wettbewerbsposition und das interne Infrastrukturmanagement hat. Angesichts des Drucks durch die beschleunigte Innovation, globale Unsicherheiten, wirtschaftliche Zwänge, moderne Sicherheitsanforderungen und KI ist eine Plattform erforderlich, die speziell darauf ausgelegt ist, diese Herausforderungen auf integrierte Weise zu bewältigen.

Diese Auswahl ist keine leichtfertige Entscheidung. Wenn Unternehmen Entscheidungen über zukünftige Betriebssysteme und Plattformen treffen, sollten sie 4 wichtige Evaluierungsschritte berücksichtigen:

- Identifizieren Sie die Stressfaktoren, die für Ihr Unternehmen am wichtigsten sind.
- Ordnen Sie Ihre Workloads den Funktionsanforderungen zu.
- Bewerten Sie den allgemeinen Wert für das Unternehmen.
- Validieren Sie die Sicherheit und Langlebigkeit der Lieferkette.

Identifizierung der wichtigsten Stressfaktoren

Unternehmen stellen fest, dass verschiedene Teams unterschiedlichen Anforderungen ausgesetzt sind: KI-Produktteams legen den Schwerpunkt auf Innovation und Hardware-Anforderungen, während regulierte Branchen einen stärkeren Fokus auf Sicherheits- und Compliance-Fähigkeiten legen. Unternehmen sollten die einzelnen Stressfaktoren (beschleunigte Innovation, globale Unsicherheit, wirtschaftliche Zwänge, Sicherheitsanforderungen und

KI) anhand ihrer aktuellen und erwarteten zukünftigen Bedeutung bewerten und diese Liste nutzen, um bei künftigen Bewertungen eine Unterscheidung zwischen „unverzichtbaren“ und „wünschenswerten“ Aspekten zu treffen.

Zuordnung Ihrer Workloads zu den Funktionsanforderungen

Ein Faktor, der die Anforderungen bestimmt, sind die Workloads, die für ein Unternehmen am wichtigsten sind. Eine Workload-Analyse zeigt, ob Ihr Unternehmen von einer workloadspezifischen Optimierung profitiert oder ob ein umfassenderer Standardisierungsansatz sinnvoller wäre. Davon profitieren Unternehmen beliebiger Größe, da Anzahl und Bedeutung von Workloads nicht unbedingt von der Unternehmensgröße abhängig sind.

Bewertung des geschäftlichen Mehrwerts

Sobald die Workloads analysiert wurden, hat ein Unternehmen einen soliden Überblick über die Anzahl der Server, die Anzahl der Beschäftigten (und die Kompetenzstufen) sowie die Gesamtzahl der gemanagten Workloads. So lassen sich direkte Kosten wie Lizenzen für das Betriebssystem, Support und Infrastrukturbedarf abschätzen. Eine Bewertung kann auch helfen, indirekte Kosten abzuschätzen, wie etwa das Ausmaß der internen Expertise, Verzögerungen beim Workload Deployment aufgrund unvorhergesehener Einschränkungen und entgangene Geschäftschancen aufgrund einer mangelnden Infrastrukturflexibilität. Sobald diese Daten erfasst sind, können Unternehmen fundierte strategische Entscheidungen treffen, die die operative Effizienz verbessern und den Wettbewerbsvorteil erhöhen.

Validierung der Sicherheit und Langlebigkeit der Lieferkette

Ein Unternehmen, das sich für ein Betriebssystem oder eine Plattform entscheidet, muss sicher sein können, dass das betreffende Betriebssystem oder die betreffende Plattform langfristig verfügbar sein wird. Es ist wichtig, die Unternehmensgeschichte zu kennen, aber ebenso wichtig ist

das Wissen um folgende Aspekte: wie das Unternehmen seine Anwendungen prüft, wie umfangreich und vielfältig sein Partnerportfolio ist sowie welche Erfahrungen und Kompetenzen es in Bezug auf entscheidende Aspekte wie die Compliance mit gesetzlichen Vorschriften und hochmoderne Features wie KI besitzt. Unternehmen setzen beim Deployment von Workloads auf mehrjährige Lifecycles. Daher ist es unerlässlich, sicherzustellen, dass die Plattform diese Workloads sowohl aktuell als auch in Zukunft bewältigen kann.

Fazit

Der Schlüssel zum Erfolg in diesem Prozess ist das Bewusstsein dafür, dass Infrastrukturentscheidungen zu Abhängigkeiten führen. Heute getroffene Entscheidungen ermöglichen entweder den geschäftlichen Erfolg oder schränken die Fähigkeiten ein und verzögern Projekte auf Jahre hinaus. Unternehmen, die die Auswahl eines Betriebssystems strategisch angehen und dabei klare Anforderungen sowie ein Evaluierungs-Framework berücksichtigen, können Innovationen aggressiv umsetzen, Unsicherheiten erfolgreich bewältigen und sowohl ihre Produktivität als auch ihre Sicherheit jetzt und in Zukunft optimieren.

Über die Autoren

Ned Bellavance ist IT-Experte und technischer Ausbilder mit mehr als 20 Jahren Erfahrung in diesem Bereich. Er war als Helpdesk-Operator, Systemadministrator, Cloud-Architekt und Produktmanager tätig. Derzeit leitet Ned das Unternehmen „Ned in the Cloud LLC", wo er Kurse entwickelt, mehrere Podcasts betreibt, Bücher schreibt und eigene Inhalte für Technologieanbieter erstellt. Ned ist seit 2017 MVP von Microsoft und seit 2020 HashiCorp Ambassador. Für ihn stehen 3 zentrale Säulen im Vordergrund: Sich auf Unbequemlichkeit einlassen, Scheitern planen und freundlich sein.

Chris Hayner ist ein erfahrener IT-Experte mit jahrzehntelangen Erfahrungen in den Bereichen Betriebssysteme, Infrastruktur, Cloud Computing und Cybersicherheit. Seine Karriere begann im Rechenzentrum, wo er eine Vielzahl von Systemen verwaltete, von Mainframes über AlphaServer bis hin zu White-Box-x86-Servern. Von da an erweiterte sich sein Aufgabenbereich um Virtualisierung, Cloud-Technologien und übergreifende Cybersicherheits- und IT-Strategien. Seit 15 Jahren ist Chris im Consulting-Bereich tätig und hat dort als Fachexperte (SME), Architekt und Analyst gearbeitet. In diesen Rollen hat er Hunderte von Organisationen dabei unterstützt, die Lücke zwischen Geschäftszielen und IT-Lösungen zu schließen und so Innovation und operativen Erfolg zu steigern. Neben seiner CISSP-Zertifizierung und zahlreichen Hersteller- und Branchenzertifizierungen hat Chris einen MBA der Temple University erworben, wodurch er über eine einzigartige Kombination aus technischem Fachwissen und unternehmerischem Gespür verfügt.