

Erfolgreiche Verwaltung Ihrer Linux-Umgebung

Ein Guide zu modernen Best Practices, Tools und Techniken für effektives Systemmanagement



Inhaltsverzeichnis

Seite 1

Über dieses E-Book

Seite 2

Linux – die Basis für die Zukunft

Seite 3

System-Lifecycle-Management

Seite 4

Content- und
Provisionierungsmanagement

Seite 5

Subskriptionsmanagement
und Abweichungsanalyse

Seite 6

Konfigurationsmanagement

Seite 7

Sicherheitsschwachstellen und
Compliance-Management

Seite 8

Schwachstellen-, Compliance-
und Patch-Management

Seite 9

Best Practices

Seite 10

Empfohlene Tools

Seite 11

Einheitliches und integriertes Linux
-Management mit Profi-Tools

Seite 12

Red Hat Managementtools für Linux

Seite 13

Customer Success Highlight:
Brinker International

Seite 14

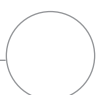
Customer Success Highlights:
Gesundheitswesen und
Finanzdienstleistungen

Seite 15

Customer Success Highlights:
Telekommunikation und Herstellung

Seite 16

Bereit für den Einstieg?



Über dieses E-Book

Dieses E-Book bietet fachkundige Anleitung für Teams, die sich um Linux® Architekturen und deren Administration kümmern und die Verwaltung von Umgebungen mit modernen Best Practices und automatisierten Tools optimieren wollen. Unternehmen, die diesen Empfehlungen gefolgt sind, verzeichneten positive Auswirkungen im Hinblick auf IT-Effizienz, Sicherheit, Zuverlässigkeit und Kosten und sorgten gleichzeitig für geschäftsfördernde Innovationen und Erkenntnisse.

Mit den Empfehlungen in diesem E-Book kann Ihr Unternehmen folgende Vorteile erzielen:



**Bis zu
4,5 x**
höhere IT-Effizienz
und Geschwindigkeit¹



**Bis zu
20 %**
geringere Betriebs-
Kosten für Linux-
Umgebungen²



**Bis zu
25 %**
geringere Support-
Kosten für
Linux-Umgebungen¹



**Bis zu
98 %**
schnellere
Provisionierung von
Storage³

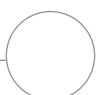


Auf den nächsten Seiten finden Sie weitere Details zu diesen Punkten und erfahren, wie Sie Ihre Linux-Systeme mit flexibler Automatisierung, prädiktiven Analysen und integrierten Tools effektiver managen können.

¹ Red Hat Case Study: „Sunrise Communications standardisiert auf kostengünstiger Software von Red Hat“, April 2018. redhat.com/de/resources/sunrise-communications-customer-case-study.

² Red Hat Case Study: „CTOS verbessert Agilität mit Red Hat zur schnelleren Geschäftsexpansion“, November 2017. redhat.com/de/resources/ctos-case-study.

³ Red Hat Case Study: „NXP Semiconductors optimiert Produktdesignprozesse mit Red Hat“, Mai 2018. redhat.com/de/resources/nxp-semiconductors-customer-case-study.



Linux – die Basis für die Zukunft

Linux® ist eines der am weitesten verbreiteten Betriebssysteme der Welt. Es kommt in zahlreichen Branchen und mit vielen Erfolg versprechenden Technologien zum Einsatz.⁴ Es wird für hochverfügbare, zuverlässige und betriebswichtige Workloads in Rechenzentren und Cloud Computing-Umgebungen verwendet und unterstützt zahlreiche Use Cases, Zielsysteme und Geräte. Die wichtigen Public Cloud-Anbieter, darunter Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) und Alibaba Cloud, bieten in ihren Märkten mehrere Linux-Distributionen an. Zur Unterstützung moderner, digitaler Geschäftsinitiativen bietet Linux Folgendes:

- Open Source-Innovation
- Konsistenz für viele verschiedene Infrastrukturen
- Container- und Anwendungs-Portierbarkeit
- Massive Skalierbarkeit für Workloads und Plattformen
- Durchgehende Sicherheitsfunktionen
- Eine flexible Plattform für die Anwendungsentwicklung

Moderne Managementtools und -ansätze sind für große Linux-Umgebungen von entscheidender Bedeutung. Diese Umgebungen können Hunderte von Systemen umfassen, die von großen Teams betrieben werden. Dabei fallen potenziell Tausende von Sicherheits-Patches, Bug Fixes und Konfigurationsänderungen an, die sich manuell einfach nicht nachverfolgen und implementieren lassen.

Hinzu kommt, dass viele Unternehmen ihre Workloads in hybriden Umgebungen bereitstellen, die sich aus Bare Metal-, virtualisierten sowie Private und Public Cloud-Ressourcen zusammensetzen. Durch diese Komplexität geht oft der Überblick über die gesamte Umgebung verloren und die Herausforderungen beim Management nehmen zu.

Mit einer umfassenden Managementstrategie können Sie Ihre Linux-Umgebung optimal nutzen und gleichzeitig Ihre Assets und Ihr Unternehmen schützen. Eine **Standardbetriebsumgebung (Standard Operating Environment, SOE)** mit konsistenten Betriebssystemen und Tools ist ein zentraler Bestandteil effektiver Managementstrategien. SOEs können Ihre IT-Infrastruktur vereinfachen und so die Effizienz steigern, Kosten reduzieren, Ausfallzeiten minimieren, die Bereitstellung beschleunigen sowie Sicherheit und IT-Produktivität verbessern.

Dieses E-Book behandelt die Herausforderungen, die das Verwalten großer Linux-Umgebungen mit sich bringt, und beleuchtet nützliche Tools und Best Practices.

Linux in Zahlen

Mehr als

75 %

der cloudfähigen Unternehmen nutzen nach eigenen Angaben Linux als primäre Cloud-Plattform.⁴

54 %

der Anwendungen in Public Cloud-Infrastrukturen werden auf virtuellen Maschinen in Linux ausgeführt.⁵

80 %

der Personalverantwortlichen stellen Linux-Fachkräfte ein.⁶

⁴ The Linux Foundation: „Linux is the most successful open source project in history“. linuxfoundation.org/projects/linux. Abgerufen: 1. November 2019.

⁵ Management Insight Technologies, gesponsert von Red Hat: „Linux in Public Clouds für Unternehmen“, Februar 2018. redhat.com/de/resources/state-of-linux-in-public-cloud-for-enterprises.

⁶ The Linux Foundation and Dice: „The 2018 Open Source Jobs Report“, 2018.



System-Lifecycle-Management

Sämtliche Systeme, Ressourcen und Workloads unterliegen einem bestimmten Lifecycle. System-Lifecycle-Management – ein zentraler Bestandteil effektiver Managementstrategien – bezeichnet die Administration eines Systems von der Provisionierung über den Betrieb bis hin zur Stilllegung. Ein optimaler Lifecycle-Management-Ansatz unterstützt Sie bei Folgendem:



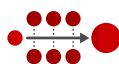
Aufbau

Systeme zuverlässig automatisch und skalierbar erstellen



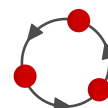
Überwachung

Systeme, Assets und Subskriptionen überwachen und nachverfolgen



Wartung

Die Einheitlichkeit von Systemen über den gesamten Lifecycle sicherstellen



Einstellung

Systeme und Ressourcen bei Bedarf stilllegen

Häufige Herausforderungen beim Lifecycle-Management

Ein effektives System-Management kann durch zahlreiche Umstände erschwert werden.

- **Umgebungswachstum:** Große Umgebungen enthalten eine Vielzahl von Systemen, was die Überwachung des Systemstatus und der Ereignisse in Ihrer Organisation kompliziert macht.
- **Technische Schulden:** Altsysteme erfordern nicht selten spezielle Managementtools und -prozesse, was eine einheitliche und effiziente Verwaltung sämtlicher Systeme praktisch unmöglich macht.
- **Begrenzte Personalkapazitäten:** Die Größe von IT-Teams nimmt in der Regel nicht so schnell zu wie die Größe der Infrastruktur, die sie verwalten. Dies bedeutet einen ständig steigenden Arbeitsaufwand für die gleiche Anzahl an Mitarbeitenden und sorgt dafür, dass Unternehmen hinter technologischen Änderungen, Innovation und geschäftlichen Anforderungen zurückbleiben.
- **Business Continuity-Anforderungen:** Da Unternehmen zunehmend auf IT angewiesen sind, muss ihre IT-Infrastruktur noch zuverlässiger und verfügbarer werden. Das Systemmanagement muss daher so durchgeführt werden, dass es zentrale geschäftliche Abläufe nicht beeinträchtigt.

Best Practices beim Lifecycle-Management



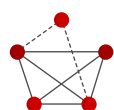
Stilllegung von Ressourcen am Ende ihrer Lebensdauer

Verwaiste und ungenutzte Ressourcen bedeuten unnötigen Arbeitsaufwand und vermeidbare Kosten. Implementieren Sie einen Prozess zur Stilllegung nicht verwendeter Systeme und sparen Sie so Verwaltungsaufwand und -kosten.



Automatisierung

Mit der Größe Ihrer Infrastruktur wächst auch der Verwaltungsaufwand. Mit Automatisierung können Sie häufige Aufgaben vereinheitlichen, manuelle Fehler reduzieren und Ihre Teams entlasten, damit diese sich auf Innovationen konzentrieren können.



Vernetzung von Tools

Integrieren Sie Ihre Tools über verfügbare APIs (Application Programming Interfaces). Nutzen Sie Ihre bevorzugten Schnittstellen, um Aufgaben in anderen Tools auszuführen, Abläufe zu vereinheitlichen und produktiver zu werden.

Die folgenden Abschnitte behandeln einige wichtige Bereiche des System-Lifecycle-Managements.



Content- und Provisionierungsmanagement



Content-Management

Content-Management umfasst die Lieferkette und Administration von Software, Paketen und Patches, die Sie in Ihrer Umgebung einsetzen.

Warum ist das wichtig?

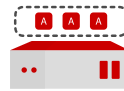
Der Einsatz von unsignierter, nicht geprüfter oder veralteter Software kann Risiken für Ihr Unternehmen mit sich bringen. So kann es dadurch zu Sicherheitsschwachstellen, Instabilitäten und Performance-Problemen kommen. Tatsächlich hat die Zahl der Angriffe auf die Lieferkette, bei denen Endziele über Schwachstellen bei Drittanbieter-Services und -Software attackiert werden, 2018 um 78 % zugenommen.⁷

Ein manuell durchgeführtes Content-Management kann jedoch zeitaufwendig und fehleranfällig sein.

Best Practices und Empfehlungen

Mit einem effektiven Content-Management sorgen Sie dafür, dass die Lieferkette für Software, die Sie in der Produktion nutzen, geschützt wird. Sie sollten deshalb:

- Die Quelle von Inhalten kennen
- Die Inhalte auf eine mögliche Manipulation bei der Übertragung prüfen und betroffene Inhalte ablehnen
- Patches vor der Bereitstellung in der Produktivumgebung testen
- Inhalte in geografisch verteilten Umgebungen so nah wie möglich an den Zielsystemen platzieren und
- Tools nutzen, mit denen Inhalte einfach und automatisch zentralisiert, erfasst, kuratiert und verbreitet werden können.



Provisionierungsmanagement

Provisionierungsmanagement umfasst die Definition und Kontrolle der Provisionierung und Bereitstellung von Systemen.

Warum ist das wichtig?

Unternehmen sind auf ihre IT-Systeme angewiesen. Wenn die richtigen Systeme nicht schnell genug verfügbar sind, kann dies das Geschäft beeinträchtigen oder dazu führen, dass Nutzende zur Erfüllung ihrer Anforderungen auf unautorisierte Ressourcen zurückgreifen, die sich außerhalb der Kontrolle der IT-Abteilung befinden.

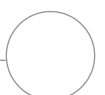
Viele IT-Teams haben Schwierigkeiten, ihre Provisionierungsprozesse zu standardisieren, da es bei der Systemprovisionierung unzählige Möglichkeiten gibt und viele Plattformen Managementtools enthalten, die spezifisch für die jeweilige Plattform sind.

Best Practices und Empfehlungen

Für ein effektives Provisionierungsmanagement müssen Systeme auf verschiedenen Plattformen und geografisch verteilten Umgebungen provisioniert und skaliert werden können.

- Trennen Sie die Systemdefinition von der Systemprovisionierung, indem Sie plattformunabhängige Tools nutzen.
- Führen Sie ein umfassendes, plattformübergreifendes Tool ein, mit dem Sie Systeme nur einmal und ohne zusätzliche plattformspezifische Implementierungsdetails definieren müssen und dann konsistent für verschiedenste Plattformen bereitstellen können, wie etwa Bare Metal- und virtualisierte Umgebungen sowie Private und Public Clouds.

⁷ Symantec: „Internet Security Threat Report, Volume 24“, Februar 2019.



Subskriptionsmanagement und Abweichungsanalyse



Subskriptionsmanagement

Mithilfe von Subskriptionsmanagement ermitteln Sie die Anzahl und Eigenschaften der von Ihnen eingesetzten Assets. Dies kann häufig auch ein Erfassungssystem für Ihre Assets beinhalten.

Warum ist das wichtig?

Wenn Sie Software auf Subskriptionsbasis einsetzen, verfügen Sie über einen Vertrag, der angibt, wie viele Subskriptionen eines Produkts Sie nutzen können. Eine Bereitstellung auf zu vielen Systemen stellt eine Vertragsverletzung dar, die zu Geldstrafen, der Beendigung des Vertrags oder zu fehlendem Support führen kann. Wenn Sie hingegen mehr Subskriptionen kaufen, als Sie wirklich brauchen, entstehen Ihrem Unternehmen unnötige Kosten.

Best Practices und Empfehlungen

Mit einem effektiven Subskriptionsmanagement können Sie Ihre Kosten optimieren und dabei die Compliance mit Anbieterverträgen wahren. Was Sie tun sollten:

- Wählen Sie ein Tool, mit dem Sie einen Überblick darüber haben, wie viele Subskriptionen Ihr Unternehmen verwendet und wie diese genutzt werden. Dadurch können Sie für eine effiziente Subskriptionsnutzung sorgen und stellen außerdem fest, wann Sie zusätzliche Subskriptionen benötigen.
- Entscheiden Sie sich für Plattformen, die sich mit Ihren vorhandenen und geplanten Inventory-Management-Produkten verbinden lassen.
- Implementieren Sie Prozesse und Sicherheitsmaßnahmen, die dafür sorgen, dass nur autorisierte Nutzende Subskriptionen auf neuen Systemen bereitstellen können und dass diese Subskriptionen richtig zugeteilt werden.
- Führen Sie Abläufe zur Identifikation und Stilllegung alter oder nicht genutzter Systeme ein, um nicht für Subskriptionen zu zahlen, die Sie nicht benötigen.



Konfigurationsbewertung und Abweichungsanalyse

Konfigurationsbewertung bezeichnet das Scannen von Systemen zur Identifizierung aktueller Konfigurationen und solcher, die Maßnahmen erfordern. Bei der Abweichungsanalyse werden Systeme anhand der Konfigurationsbewertung mit Basiskonfigurationen, früheren Konfigurationen sowie anderen Systemen verglichen, um Ähnlichkeiten und Unterschiede zu finden.

Warum ist das wichtig?

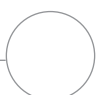
Während sich Basis-Images genau konfigurieren lassen, können sich Systeme mit der Zeit ändern, etwa aufgrund von Anpassungen und Installationen für Endbenutzende, Ad-hoc-Fixes und neuer Image-Deployments. Eine regelmäßige Überwachung der Systemkonfigurationen ist daher entscheidend. Das manuelle Nachverfolgen von Konfigurationen ist jedoch bestenfalls zeitaufwendig, in großen Umgebungen sogar fast unmöglich. Selbst mit einem Scanning-Tool kann es sich als schwierig erweisen, massive Dateien zu durchsuchen, um festzustellen, welche Systeme aktualisiert und gepatcht werden müssen.

Best Practices und Empfehlungen

Eine effektive Konfigurationsbewertung und Abweichungsanalyse kann Ihnen einen Überblick über Ihre Systemkonfigurationen geben, damit Sie operative und Performance-Probleme identifizieren, nicht konforme Systeme erkennen und Abweichungen steuern können.

Wählen Sie ein Managementtool, mit dem Sie Konfigurationsänderungen regelmäßig und kontinuierliche nachverfolgen können. Wir empfehlen Ihnen eine tägliche Überwachung. Mit dem optimalen Tool ist Folgendes möglich:

- Erfassen und Dokumentieren von Systemkonfigurationen
- Erkennen von Konfigurationsänderungen und von Systemen, die von der Baseline abweichen
- Validieren von angewandten Updates
- Rückkehr zu vorherigen Konfigurationen
- Vergleich von Systemkonfigurationen zur Ermittlung von Unterschieden
- Automatisiertes Überwachen für optimierte Abläufe, regelmäßige Scans und Konsistenz



Konfigurationsmanagement



Konfigurationsmanagement

Konfigurationsmanagement umfasst das Definieren eines gewünschten Systemzustands und die dementsprechende Entwicklung und Erhaltung von Systemen. Dieser Prozess ist eng mit der Konfigurationsbewertung und Abweichungsanalyse verbunden und nutzt beide, um Systeme zu ermitteln, die Updates, eine Neukonfiguration oder Patching erfordern.

Warum ist das wichtig?

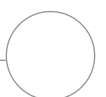
Fehlkonfigurationen und veraltete Einstellungen können zu unzureichender Performance, Inkonsistenzen und Nicht-Compliance mit Standards führen und damit Geschäftsbetrieb und Sicherheit beeinträchtigen. Der Prozess der Identifizierung von zu prüfenden Systemen, Festlegung von Abhilfemaßnahmen, Priorisierung von Aktionen, Nachverfolgung einer erfolgreichen Durchführung und Validierung ist jedoch zu komplex und lässt sich daher für große Systeme manuell nicht durchführen.

Best Practices und Empfehlungen

Bei einem effektiven Konfigurationsmanagement können Sie Systemkonfigurationen konsistent definieren und Ihre Systeme nach diesen Baselines entwickeln und warten. Ein optimales Konfigurationsmanagementtool bietet Ihnen folgende Möglichkeiten:

- Klassifizieren und Verwalten von Systemen nach Gruppen und Untergruppen
- Zentrales Modifizieren von Basiskonfigurationen und Rollout neuer Einstellungen auf infrage kommende Systeme
- Automatisches Identifizieren, Patchen und Aktualisieren von Systemen mit veralteten, leistungsschwachen und nicht konformen Konfigurationen
- Einfaches Priorisieren von Maßnahmen für bestimmte Ergebnisse
- Anwenden vorgegebener Abhilfemaßnahmen

Begrenzen Sie die Zahl der von Ihnen gemanagten Basis-Konfigurationen auf das Nötigste. Je mehr unterschiedliche Konfigurationen Sie haben, umso mehr Zeit und Arbeitsaufwand erfordert das Management. Systeme, die sich gleichen, können mit weniger Zeit, Arbeitsaufwand und Personal gemanagt werden.



Sicherheitsschwachstellen und Compliance-Management

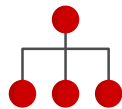
IT-Sicherheit ist ein aktuelles Thema in jedem Unternehmen. 30 % der CEOs betrachten Cyberattacken als größte Bedrohung für den wirtschaftlichen Erfolg ihres Unternehmens.⁸ Und die Sicherheitsbedrohungen nehmen zu. Das durchschnittliche Ausmaß von Datenpannen ist seit 2018 um 3,9 % gestiegen, und auch die Wahrscheinlichkeit, innerhalb der nächsten 2 Jahre Opfer einer Datenpanne zu werden, hat um 29,6 % zugenommen.⁹ Zudem ändern sich derzeit diesbezügliche Branchen- und gesetzliche Richtlinien.

Das Risiko-Management von Sicherheit und Compliance erfordert die Überwachung und Analyse von Systemen, um sicherzustellen, dass Sicherheitsrichtlinien und gesetzliche Vorgaben eingehalten werden. Ein optimaler Ansatz für Sicherheitsschwachstellen und Compliance-Management bietet Ihnen folgende Möglichkeiten:



Analyse

Identifizieren von Systemen, die nicht konform, fehleranfällig oder nicht gepatcht sind.



Organisation

Priorisieren von Korrekturmaßnahmen nach Aufwand, Auswirkungen und Schweregrad des Problems.



Behebung

Schnelles und einfaches Patchen und Neukonfigurieren von Systemen, die Maßnahmen erfordern.



Bericht

Sicherstellen, dass Änderungen angewendet wurden und die entsprechenden Ergebnisse melden.

Bekannte Herausforderungen in Sachen Sicherheit und Compliance

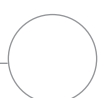
Mehrere Faktoren machen Sicherheitslücken und Compliance-Management schwierig.

- **Sich verändernde Sicherheits- und Compliance-Landschaften:** Sicherheitsbedrohungen und Compliance-Änderungen entwickeln sich schnell und erfordern eine unmittelbare Reaktion auf neue Bedrohungen und sich ändernde Vorschriften.
- **Verteilte Umgebungen mit mehreren Plattformen:** Infrastrukturen sind zunehmend über Onsite-Systeme, Cloud-Plattformen und geografische Standorte verteilt. Das verhindert einen vollständigen Überblick über Ihre Umgebung. Gehostete Anbieter stellen oft ihre eigenen plattformspezifischen Managementtools zur Verfügung. Die Ansichten und Berichte dieser Tools müssen einzeln zusammengesetzt werden, damit sie einen Überblick über den Compliance- und Sicherheitsstatus Ihrer Umgebung bieten.
- **Große Umgebungen und Teams:** Große, komplexe Infrastrukturen und Teams können die Koordination in Ihrer Umgebung und Organisation erschweren. Tatsächlich kann die Systemkomplexität die Kosten von Datenpannen um 10,96 US-Dollar pro gelöschtem oder gestohlenen Datensatz erhöhen.⁹

Die folgenden Abschnitte behandeln einige wichtige Bereiche des Sicherheits- und Compliance-Managements.

⁸ PWC: „22nd Annual Global CEO Survey: CEO's curbed confidence spells caution“, 2019.

⁹ IBM Security: „2019 Cost of a Data Breach Report“, 2019. [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach).



Schwachstellen-, Compliance- und Patch-Management



Identifizierung und Behebung von Sicherheitslücken

Die Erkennung von Sicherheitslücken und ihre Behebung sind Bestandteile der Infrastrukturanalyse. Dabei werden Systeme erkannt und repariert, die für Angriffe anfällig sind. Diese Sicherheitslücken können durch neue Bedrohungen, veraltete Patches oder eine fehlerhafte Systemkonfiguration entstehen. Zu den Maßnahmen für die Fehlerbehebung zählen häufig Patches, Updates und die Neukonfiguration von Systemen, um die Sicherheitslücke zu schließen.

Warum ist das wichtig?

Schwachstellen können zu kostspieligen Sicherheitsverletzungen und sogar zu entgangenen Geschäftschancen führen. Die Kosten einer Datenpanne belaufen sich auf durchschnittlich 3,92 Millionen US-Dollar.¹⁰ Dabei entfallen 36,2 % der durchschnittlichen Kosten von Datenpannen auf entgangene Geschäftschancen.¹⁰

Mitre veröffentlicht jährlich Tausende von CVEs (Common Vulnerabilities and Exposures).¹¹ Die meisten IT-Teams können bei diesem Tempo nicht mithalten und prüfen daher nicht alle CVEs, um festzustellen, ob und inwieweit sich diese auf ihre Infrastruktur auswirken. Dadurch verpassen Sie möglicherweise relevante CVEs und bleiben entsprechenden Angriffen gegenüber ungeschützt.



Compliance-Management

Durch Compliance-Management wird sichergestellt, dass Systeme nicht gegen Unternehmensrichtlinien, Branchenstandards und geltende Vorschriften verstoßen. Dazu gehört eine Infrastrukturbewertung zur Identifizierung von Systemen, die aufgrund von geänderten Vorschriften, Richtlinien oder Standards, Fehlkonfigurationen oder aus anderen Gründen nicht konform sind.

Warum ist das wichtig?

Compliance-Verstöße können – abgesehen von Sicherheitsverletzungen – Bußgelder nach sich ziehen, dem Ruf des Unternehmens schaden und zum Verlust von Zertifizierungen führen.



Patch-Management

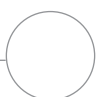
Patch-Management beinhaltet das Identifizieren von Systemen, die gepatcht oder aktualisiert werden müssen, das Durchführen der erforderlichen Patches und Updates sowie Tests, um zu validieren, dass diese erfolgreich installiert wurden und funktionsfähig sind.

Warum ist das wichtig?

Nicht gepatchte und veraltete Systeme können eine Ursache für Compliance-Probleme und Sicherheitslücken darstellen.

¹⁰ IBM Security: „2019 Cost of a Data Breach Report“, 2019. [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach).

¹¹ Weitere Information zu Mitre und CVEs finden Sie unter [mitre.org](https://www.mitre.org).



Best Practices

Regelmäßige System-Scans

Durch die tägliche Überwachung können Sie Compliance-Probleme und Sicherheitslücken identifizieren, bevor sie sich auf den Geschäftsbetrieb auswirken oder zu einer Datenpanne führen. Die Erkennung und Eindämmung einer Datenpanne dauerte 2019 im Durchschnitt 279 Tage. Wird eine Sicherheitsverletzung innerhalb von 200 Tagen oder weniger entdeckt und bekämpft, können dies die Kosten um durchschnittlich 1,22 Millionen US-Dollar senken.¹²

Automatisierung

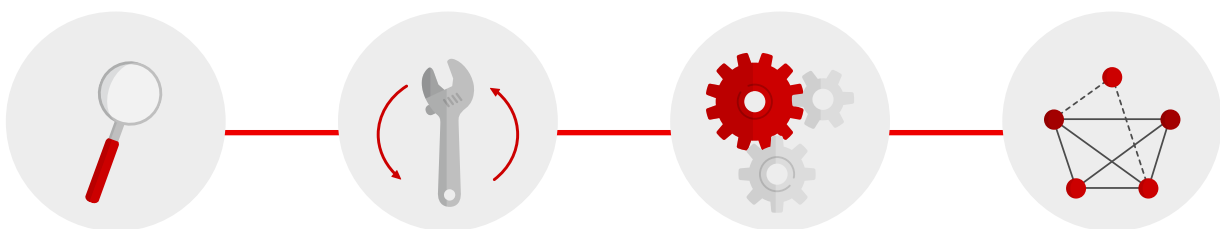
Je größer Ihre Infrastruktur, desto schwieriger wird das manuelle Management. Nutzen Sie Automatisierung, um häufige Aufgaben zu optimieren, die Konsistenz zu erhöhen und eine regelmäßige Überwachung und Berichterstellung sicherzustellen. Durch eine Vollautomatisierung der Sicherheit können die durchschnittlichen Kosten für eine Sicherheitsverletzung um 95 % reduziert werden. Doch nur 16 % der Unternehmen nutzen diese Möglichkeit.¹²

Häufige Patches, zahlreiche Tests

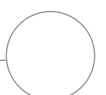
Wenn die Systeme auf dem neuesten Stand sind, wirkt sich das positiv auf die Sicherheit, Zuverlässigkeit, Performance und Compliance aus. Um mit wichtigen Problemen Schritt halten zu können, sollten Sie Patches einmal im Monat einspielen. Patches für kritische Fehler und Defekte sollten so schnell wie möglich installiert werden. Führen Sie für gepatchte Systeme einen Abnahmetest durch, bevor Sie diese wieder in den Produktivmodus versetzen.

Vernetzung von Tools

Verteilte Umgebungen beinhalten häufig unterschiedliche Managementtools für die einzelnen Plattformen. Integrieren Sie diese Tools über APIs. Nutzen Sie Ihre bevorzugten Benutzeroberflächen, um Aufgaben mit anderen Tools auszuführen. Mit einer geringeren Anzahl von Benutzeroberflächen können Sie die Betriebsabläufe optimieren und die Übersicht über den Sicherheits- und Compliance-Status aller Systeme in Ihrer Umgebung verbessern.



¹² IBM Security: „2019 Cost of a Data Breach Report“, 2019. [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach).



Empfohlene Tools

Ideale Sicherheits- und Compliance-Tools haben mehrere wichtige Funktionen.



Proaktive Scans

Der erste Schritt zur Optimierung von Sicherheit und Compliance besteht darin, sich einen guten Überblick zu verschaffen. Durch Tools für automatische Scans kann sichergestellt werden, dass Systeme in regelmäßigen Abständen überwacht werden. So werden Sie ohne großen Zeit- und Kostenaufwand auf Probleme aufmerksam gemacht.

Verwertbare Erkenntnisse

Mit Tools, die auf Ihre Umgebung zugeschnittene Informationen liefern, können Sie schneller erkennen, welche Compliance-Probleme und Sicherheitslücken vorliegen, welche Systeme betroffen sind und welche potenziellen Auswirkungen Sie erwarten können.

Anpassbare Ergebnisse

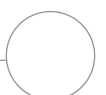
Einige Compliance-Prüfungen sind aufgrund ihrer besonderen Konfiguration, ihrer Nutzung oder Workload unter Umständen nicht mit bestimmten Systemen kompatibel. Tools, mit denen Sie den Geschäftskontext definieren können, sind ideal geeignet, um falsche positive Ergebnisse zu reduzieren, Geschäftsrisiken zu managen und Ihnen so eine realistischere Sicht auf Ihren Sicherheits- und Compliance-Status zu liefern.

Präskriptive priorisierte Fehlerbehebung

Durch Tools, die definierte Fehlerbehebungen bereitstellen, entfällt die Notwendigkeit, selbst nach Maßnahmen zu suchen, was Zeit spart und das Fehlerrisiko verringert. Durch die Priorisierung von Maßnahmen basierend auf potenziellen Auswirkungen und betroffenen Systemen können Sie begrenzte Patch-Fenster optimal nutzen.

Verständliche Berichte

Tools, die klar verständliche Berichte dazu erstellen, welche Systeme gepatcht sind, welche gepatcht werden müssen und welche nicht den Sicherheits- und Gesetzesrichtlinien entsprechen, erhöhen die Auditierbarkeit und ermöglichen einen besseren Überblick über den Status Ihrer Umgebung.



Einheitliches und integriertes Linux-Management mit Profi-Tools

Red Hat verwendet einen ganzheitlichen Ansatz für das IT-Management, mit dem Sie die Schnelligkeit, Skalierbarkeit und Stabilität Ihrer gesamten IT-Umgebung steigern können – von Bare Metal- und virtualisierten Servern bis hin zu Private, Public und Hybrid Cloud-Infrastrukturen. Die Managementtools von Red Hat® basieren auf jahrelanger Linux-Entwicklung und Support-Erfahrung. Die einzelnen Tools arbeiten reibungslos zusammen, um die IT-Administration zu optimieren. Hiervon profitiert Ihr Team, das Zeit und Mühen spart, aber auch Ihre Umgebung, die sicherer und zuverlässiger wird.



Konfigurierbare Tools und Baselines reduzieren die Anzahl von falsch-positiven Ergebnissen und verschaffen Ihnen einen genauen Überblick über den Status Ihrer Infrastruktur.



Durch Automatisierungsfunktionen wird die Konfigurations- und Patching-Genauigkeit erhöht und die Anzahl von menschlichen Fehlern reduziert.



Anpassbare Ansichten liefern im Handumdrehen die richtigen Informationen zum richtigen Zeitpunkt.



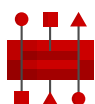
Mit automatisierten und proaktiven Korrekturmaßnahmen können Sie Probleme schneller beheben, ohne den Support zu kontaktieren.



Detaillierte, gezielte Informationen erhalten Sie rund um die Uhr in einer umfangreichen Ressourcen-Library.

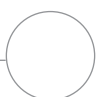


Dank Onsite- und SaaS-Optionen können Sie stets die Tools einsetzen, die Sie benötigen.



APIs verbinden Ihre bevorzugten Tools und Oberflächen.

Weiter Informationen zum IT-Management mit Red Hat finden Sie unter redhat.com/de/topics/management.



Red Hat Managementtools für Linux



Systemmanagement für Infrastrukturen von Red Hat

Red Hat Satellite vereinfacht die Bereitstellung, Verwaltung und Skalierung der Infrastrukturen von Red Hat. So können Sie die Effizienz steigern, die Betriebskosten senken und Ihre IT auf strategische geschäftliche Anforderungen konzentrieren.

- Für physische, virtuelle und Cloud-Umgebungen
- Content-, Patch-, Konfigurations-, Provisionierungs- und Subskriptionsmanagement
- Unterstützung für Onsite-, Cloud- und nicht verbundene Umgebungen
- Vollständige Kontrolle von System-Lifecycles
- Automatisierung der meisten Systemwartungsarbeiten

Cloud-Managementservices für Red Hat Enterprise Linux

SaaS-Infrastrukturmanagement (Software-as-a-Service)

Cloud-Managementservices für Red Hat Enterprise Linux optimieren die Analyse von Sicherheitsschwachstellen, Compliance und Konfigurationsdrift und verbessern so Ihre Red Hat Umgebung.

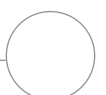
- Schwachstellen- und Compliance-Bewertung und Überwachung
- Automatisierte Problembeseitigung
- Reduzierte Tool-Wartungsanforderungen durch SaaS-basierten Service
- Zentrale Übersicht über sämtliche Hosts in Ihrer Umgebung
- Das gleiche zentrale Repository für Daten und Inventory wie Red Hat Insights



Prädiktive Analysen von IT-Risiken

Red Hat Insights unterstützt IT-Teams dabei, Bedrohungen in Bezug auf Sicherheit, Performance, Verfügbarkeit und Stabilität proaktiv zu erkennen und zu beseitigen, um Probleme, Ausfälle sowie ungeplante Ausfallzeiten zu vermeiden und sicherzustellen, dass ihre Red Hat Umgebung optimal ausgeführt wird.

- Schneller und unkomplizierter Einstieg
- In aktiven Red Hat Enterprise Linux Subskriptionen enthalten
- Jahrelange Support-Expertise
- Umsetzbare Kenntnisse und Automatisierung
- Minimaler Zugriff auf Systemmetadaten
- Dynamische Erstellung von **Red Hat Ansible® Automation Platform** Playbooks zur Automatisierung von Behebungsmaßnahmen



Brinker International

Digitale Gastronomieerlebnisse mit Lösungen von Red Hat

Herausforderung

Das Unternehmen Brinker International, Inc., die Muttergesellschaft von Chili's Grill & Bar und Maggiano's Little Italy, konzentriert sein Geschäft auf besondere kulinarische Erlebnisse mit einem innovativen digitalen Touch. Brinkers Angebote für digitale Restaurantgäste entwickelte sich in den letzten Jahren weiter, aber seine veraltete Technologie blieb hinter dieser Entwicklung zurück. Die Aktualisierung des Website-Codes dauerte stundenlang und erforderte Ausfallzeiten. Eine konsistente Konfiguration konnte dabei trotzdem nicht sichergestellt werden. Brinker musste seine digitalen Plattformen in einer neuen E-Commerce-Umgebung vereinen, um seinen Gästen ein konsistenteres Erlebnis zu bieten und die Annahme seiner digitalen Angebote zu verbessern.

Lösung

Um die notwendige Innovation und Flexibilität zu erzielen, entschied sich Brinker für den Einsatz von Open Source-Technologie. Die Wahl fiel auf die Plattform von Red Hat als Basis der neuen E-Commerce-Umgebung, die auch Chilis neuen digitalen Lieferservice hostet. Brinker integrierte für die Bereiche Storage, Management und Datenanalysen Lösungen von Red Hat. Die neue einheitliche E-Commerce-Umgebung unterstützt eine schnellere Entwicklung und Bereitstellung, kann bei Nachfragespitzen entsprechend skaliert werden und schützt Kundendaten.



„Red Hat Insights bietet Risikominderung und Transparenz über den Zustand unserer Systeme. Das hilft uns dabei, sicherzustellen, dass unsere IT-Umgebungen und Daten durch automatisierte Bedrohungsabwehr geschützt werden.“

Pankaj Patra
Senior Director of IT Enterprise Solutions,
Brinker International



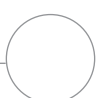
Verbesserter Schutz sensibler Kundendaten



Entwicklung einer innovativen, skalierbaren E-Commerce-Umgebung



Beschleunigte Entwicklung und Launch von Features und Services



Gesundheitswesen und Finanzdienstleistungen



HCA Healthcare benutzt seine Datenressourcen, um innovative Lösungen für langandauernde Herausforderungen in der Branche zu finden, etwa das Erkennen einer potenziell lebensbedrohlichen Sepsis. Das Unternehmen aus dem Gesundheitswesen hat die SPOT-Plattform (Sepsis Prediction and Optimization of Therapy) entwickelt, ein Produkt für prädiktive Echtzeitanalysen, das auf optimierter Container- und Automatisierungstechnologie basiert. Mithilfe von SPOT kann das Unternehmen eine Sepsis jetzt schnell erkennen und dadurch Leben retten.



CTOS Data Systems Sdn. Bhd., Malaysias größte private Kreditauskunftei (Private Credit Reporting Agency, CRA) wollte seine nationale Marktreichweite und sein Produktportfolio erweitern. CTOS migrierte von einer Community-Version der Linux-Plattform zu einer virtuellen Umgebung, die auf Technologien von Red Hat basiert. Die neue Umgebung senkte die Betriebskosten, optimierte Management und Sicherheit und bot die erforderliche Skalierbarkeit, um mit den Geschäftsanforderungen und Ansprüchen der Kunden Schritt zu halten.



Schnellere Diagnose einer Sepsis um bis zu 20 Stunden



Neue Erkenntnisse durch Algorithmen für maschinelles Lernen



Geringere Innovationsrisiken und -kosten



Weniger Ausfallzeiten, vereinfachtes Management und kompetenter Support



Sicherheit auf Unternehmensniveau zum Schutz von Daten

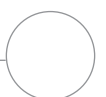


Senkung der Betriebskosten der Linux-Umgebung um etwa 20 %



„Die Lösung von Red Hat hat unser Vertrauen bezüglich unserer Arbeit bestärkt und uns ein Gefühl von mehr Sicherheit gegeben. Wir können nachts alle beruhigt schlafen und müssen uns keine Sorgen über unsere Infrastruktur machen.“

Benjamin Lau
IT-Manager, CTOS Data Systems Sdn. Bhd.



Telekommunikation und Herstellung

Sunrise

Sunrise Communications, der größte private Telekommunikationsanbieter der Schweiz, brauchte stabile, sichere und flexible IT-Services und kostengünstige Abläufe. Das Unternehmen konsolidierte seine gesamte IT-Infrastruktur auf SAP® HANA® und unternehmensgerechter Software von Red Hat und reduzierte dadurch seine Kosten, erhöhte die Geschwindigkeit und verbesserte die Performance. Gleichzeitig kann es jetzt die Entwicklung der Open Source Community nutzen, um innovative, kostengünstige Services bereitzustellen.



NXP Semiconductors N.V., einer der weltweit größten Hersteller von Elektrokomponenten, brauchte mehr Rechenleistung, um die Simulationen und Tests seiner 10.000 Design Engineers zu ermöglichen. Mit einer effizienten, auf Technologie von Red Hat basierenden IT-Umgebung verkürzte das Unternehmen die Provisionierungszeit, verbesserte die Qualität durch Standardisierung und vereinfachte die Verwaltung. Jetzt kann es qualitativ hochwertige Komponenten schneller auf den Markt bringen.



Verbesserte IT-Effizienz um einen Faktor von 4,5



Mehr Effizienz durch vereinfachte und automatisierte Verwaltung



Um 25 % geringere Supportkosten für die SAP-Umgebung



Weltweit optimierte Tätigkeit durch standardisierte IT-Konfigurationen



Zugriff auf Open Source-Fachwissen und -Support

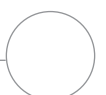


Verkürzung der Storage-Provisionierungszeit von 8 Stunden auf 5 Minuten



Red Hat Enterprise Linux ist effizienter, da es zentral mit Red Hat Ansible und Red Hat Satellite gemanagt wird.

Sebastiaan Laurijsse
Senior Director, IT Infrastructure Services, NXP Semiconductors



Bereit für den Einstieg?

Linux ist in modernen Rechenzentren eine wichtige Plattform. Mit einer umfassenden Managementstrategie können Sie Ihre Linux-Umgebung optimal nutzen und gleichzeitig Ihre Assets und Ihr Unternehmen schützen.

Red Hat bietet interoperable Managementtools, mit denen Sie die Performance, Zuverlässigkeit und Sicherheit großer Linux-Umgebungen verbessern können.



Erfahren Sie mehr über die Managementtools von Red Hat:
redhat.com/management