Optimierte Linux-Sicherheit mit Red Hat

Der Geschäftswert von Red Hat Enterprise Linux

Laut IDC konnten Unternehmen mit einer Standardisierung auf Red Hat Enterprise Linux erhebliche Sicherheitsvorteile realisieren, darunter:[1]

- 33 % mehr Effizienz bei Sicherheitsteams
- 46 % schnelleres Durchführen von Sicherheitsupdates
- 47 % schnellere Reaktion auf Sicherheitsschwachstellen

Nicht alle Linux-Distributionen verfolgen denselben Sicherheitsansatz

Für die Sicherheit der IT-Infrastruktur treten täglich neue Bedrohungen auf und es kommen ständig neue Compliance-Anforderungen hinzu. Die Standardisierung auf eine sicherheitsorientierte Basis ist für den Schutz von Anwendungen, Prozessen und Workloads unerlässlich. Obwohl sämtliche Linux®-Distributionen auf Open Source basieren, verfolgen die einzelnen Distributionen unterschiedliche Sicherheitsansätze.

Bei der Auswahl einer Linux-Distribution zur Standardisierung müssen Sie berücksichtigen, wie gut Sie darauf vorbereitet sind, neu auftretende Risiken zu minimieren und die aktuellsten Anforderungen zu erfüllen. Wie werden die Sicherheitsfunktionen der Distribution entwickelt? Wie effizient können Sie die Schutzmaßnahmen der Distribution in Ihren Umgebungen anwenden? Wie unterstützt und verbessert die Distribution Ihre Sicherheitslage über den Point of Sale hinaus, um Ihre Infrastruktur jetzt und in Zukunft vor neuen Bedrohungen zu schützen?

Red Hat® Enterprise Linux ist ein gehärtetes Betriebssystem, das auf über 30 Jahren Linux-Erfahrung basiert und von einem branchenführenden Technologieanbieter bereitgestellt wird, dem mehr als 90 % der Fortune-500-Unternehmen[2] vertrauen. Es erweitert eine *umfassende mehrstufige* Sicherheitsstrategie auf die Lösungsentwicklung, Konfiguration, Verwaltung und den Support. In diesem Überblick wird untersucht, wie die einzelnen Elemente zu einer starken Sicherheitslage beitragen und zusammenwirken, um ein zuverlässiges, sicherheitsorientiertes Betriebssystem zu bilden.

Red Hat Enterprise Linux wurde speziell für geschäftskritische Sicherheit und Zuverlässigkeit entwickelt

Red Hat basiert auf Open Source und wird von einer globalen, dezentralen und transparenten Community internationaler Engineers entwickelt, für die Sicherheit an erster Stelle steht. Red Hat Enterprise Linux konzentriert sich von Anfang an auf Sicherheit, ermöglicht ein einfacheres Anwenden von Sicherheitsfunktionen während des Builds und unterstützt Nutzende durch kontinuierliche Überwachung und Behebung neu auftretender Bedrohungen.

Sicherheitsorientierter Softwareentwicklungs-Lifecycle

Bei der Auswahl einer Linux-Distribution müssen unbedingt die Standards berücksichtigt werden, die während der Entwicklungsphase angewandt wurden.

Für Red Hat hat Sicherheit während des gesamten Entwicklungs-Lifecycles oberste Priorität. Wir orientieren uns dabei am Secure Software Development Framework (SSDF) des National Institute of Standards and Technology (NIST), den Richtlinien des Open Worldwide Application Security Project (OWASP) und den Standards der Internationalen Organisation für Normung (ISO).

Red Hat Product Security fördert kontinuierliche Sicherheitsverbesserungen in den Produkt-Pipelines von Red Hat und unterstützt gleichzeitig die Systeme und Teams, die für die Vertraulichkeit, Verfügbarkeit und Integrität der Produkte und Services von Red Hat sorgen. Für die zahlreichen Kunden von Red Hat, die in stark regulierten Branchen tätig sind, ist die Gewährleistung der Sicherheit der Softwarelieferkette eine Voraussetzung für das Deployment.

1 IDC Whitepaper, gesponsert von Red Hat. „Der Geschäftswert der Standardisierung auf Red Hat Enterprise Linux". Dokument Nr. US52594324, Sept. 2024.

2 Red Hat Kundendaten und Liste der Fortune 500, Juni 2024

In die Produktion integrierte Sicherheit

Die beste Linux-Plattform für Ihr Unternehmen ist eine Distribution, mit der Ihr Team Schutzmaßnahmen auf der Basis von Best Security Practices effizient anwenden kann. Red Hat integriert mehrere Schichten mit Sicherheitsmechanismen in seine Linux-Plattform, darunter sichere Konfigurationen (Secure-by-Standard), Zugriffskontrolle nach dem Least Privilege-Prinzip und Automatisierung.

Eine der Funktionen, mit denen Nutzende von Red Hat Enterprise Linux von Beginn an Sicherheit in ihre Images integrieren können, sind die verschiedenen Sicherheitsprofile, die Standardkonfigurationen bieten. Diese Sicherheits-Baselines basieren auf Best Practices und ermöglichen es Administrationsteams, Konfigurationen zum Zeitpunkt der Entwicklung anzuwenden. So können sie sicherstellen, dass ihr Deployment den Anforderungen an Compliance und Sicherheitsrichtlinien des Unternehmens entspricht. Dadurch lässt sich nicht nur das Risiko senken, sondern auch menschliches Versagen bei manuellen Aufgaben nach dem Erstellen des Builds vermeiden.

Eine Roadmap für den Umgang mit zukünftigen Bedrohungen

Eine starke Sicherheitslage bedeutet, auf zukünftige Bedrohungen vorbereitet zu sein und neue Anforderungen erfüllen zu können. Bei einigen Linux-Distributionen müssen die Nutzenden diese Vorbereitung eigenständig treffen, sodass sie nach Community-Lösungen suchen müssen.

Red Hat Enterprise Linux wird von einem Produkt- und Entwicklungsteam unterstützt, das aktiv nach neuen Bedrohungen sucht und Ansätze zu deren Bewältigung entwickelt. Diese Fachkräfte von Red Hat sind aktive Mitglieder der Sicherheits-Community, wobei viele von ihnen am OpenSCAP-Projekt beteiligt sind, einem Open Source Framework für die Sicherheits- und Compliance-Überwachung von Linux-Systemen.

Einhaltung globaler Anforderungen für regionale Compliance

Ein weiterer wichtiger Aspekt bei der Auswahl einer Linux-Distribution ist die Frage, ob sie die verschiedenen Compliance-Anforderungen Ihrer Teams und Kunden erfüllen kann. Unterstützt sie eine Vielzahl gängiger Cybersicherheitsvalidierungen und -zertifizierungen, oder muss Ihr Team dies später selbst regeln?

Red Hat hat jahrelang erhebliche Investitionen getätigt, um sicherzustellen, dass Red Hat Enterprise Linux Unternehmen bestmöglich dabei unterstützt, die strengen globalen Sicherheitsanforderungen ihrer Region zu erfüllen und sie damit zu befähigen, die Vorteile bewährter Sicherheitsverfahren so effizient wie möglich zu nutzen. Mit über 100 Niederlassungen in mehr als 40 Ländern weiß das Team von Red Hat, dass zahlreiche Compliance-Vorschriften existieren, die sich von Land zu Land unterscheiden.

Zur Einhaltung regionaler Compliance-Anforderungen bietet Red Hat eine Vielzahl von Validierungen und Zertifizierungen für seine Produkte und Lösungen, darunter Red Hat Enterprise Linux.

Effiziente Deployment-Methoden

Das Erfüllen von Sicherheitsanforderungen und Einhalten der erforderlichen Best Practices kann für Sicherheitsteams eine große Arbeitsbelastung darstellen. Das Scannen, Validieren und Attestieren kann zeitaufwendig sein und einen hohen Arbeitsaufwand für mehrere Teams erfordern.

Der Image-Modus, eine Deployment-Methode für Red Hat Enterprise Linux, verfolgt einen containernativen Ansatz für das Erstellen, Bereitstellen und Verwalten des Betriebssystems. Das bedeutet, dass Sicherheitsteams Containersicherheitstools – von Scan- und Validierungstools bis hin zu Kryptografie- und Authentifizierungstools – auf die Grundelemente des Betriebssystems anwenden können. Das macht ihre Arbeit wesentlich unkomplizierter. Dieser Ansatz trägt nicht nur zur Risikominderung bei, sondern erhöht auch die Effizienz.

Red Hat Enterprise Linux hilft Kunden, ihre Sicherheitsziele zu erreichen

Als die University of Sussex geschäftskritische Server auf ein vollständig unterstütztes Betriebssystem migrieren musste, arbeitete sie mit dem IT-Beratungsunternehmen WM Promus zusammen, um Red Hat Enterprise Linux einzuführen. Dadurch konnte sie das Risiko von Cyberangriffen reduzieren und eine wichtige staatliche Zertifizierung für den Nachweis einer hohen Betriebssicherheit erhalten.

„Die Universität verfügt über einen riesigen IT-Bestand. Mit Red Hat Enterprise Linux konnten wir Ausfallzeiten minimieren und Risiken schnell minimieren."[3]

Eileen O'Mahony,
General Manager, WM Promus

3 Red Hat Case Study. „WM Promus unterstützt Universitäten dabei, Effizienz und Sicherheit zu verbessern." 23. Okt. 2024.

Proaktives Risikomanagement

Mit Ihrem Betriebssystem sollten Ihre Teams einfach und effizient über potenzielle Bedrohungen und sicherheitsrelevante Probleme auf dem Laufenden bleiben können.

Mithilfe von Red Hat Lightspeed, einer in Red Hat Enterprise Linux integrierten End-to-End-Systemverwaltungslösung, können Nutzende von Red Hat Enterprise Linux Probleme selbst identifizieren und melden, Risiken anhand ihrer potenziellen Auswirkungen auf ihr Unternehmen priorisieren sowie die nächste Maßnahme in einer automatisierten Toolchain auslösen. Red Hat Lightspeed kann nach CVEs (Common Vulnerabilities and Exposures) suchen und so dazu beitragen, Abhilfemaßnahmen anhand der Art, Schwere und Auswirkung des Risikos zu priorisieren.

So können Ihre Teams proaktiv die Compliance mit OpenSCAP-Richtlinien überprüfen, nicht konforme Systeme korrigieren und Compliance-Berichte erstellen. Außerdem können Sie Red Hat Lightspeed dazu nutzen, aktive Malware-Signaturen in Systemen Ihrer gesamten Hybrid Cloud-Umgebung schnell zu erkennen.

Kontinuierlicher Sicherheits-Support

Die Auswahl der Linux-Plattform, auf die Sie standardisieren möchten, hat Auswirkungen auf Ihr Unternehmen für viele Jahre. Daher müssen Sie genau prüfen, welche Art von Unterstützung Sie nach dem Deployment und auch in Zukunft erwarten können.

Nutzende von Red Hat Enterprise Linux können sich darauf verlassen, dass sie 10 Jahre lang Updates und Support für Hauptversionen erhalten und Zugang zum Red Hat Customer Portal haben. Das Portal informiert über aktuelle Sicherheitslücken und wichtige Maßnahmen, mit denen Teams deren Auswirkungen mindern können. Das Product Security Incident Response Team (PSIRT) von Red Hat unterstützt Nutzende dabei, die Risiken und Auswirkungen neu auftretender CVEs zu erkennen, und gibt Hinweise zur Behebung.

Bewährte Partnerschaften und langjährige Zusammenarbeit

Red Hat arbeitet mit vielen branchenspezifischen Programmen zur koordinierten verantwortungsvollen Offenlegung zusammen. Red Hat kann auf eine lange und dokumentierte Geschichte der Mitwirkung in Sicherheitsorganisationen wie dem Forum of Incident Response and Security Teams (FIRST), der Open Source Security Foundation (OpenSSF), Oasis und anderen zurückblicken und ist nach wie vor ein globaler Partner beim Thema Sicherheitszusammenarbeit.

Als eines von weltweit 6 Unternehmen, die eine besondere Rolle als Root-Teilnehmer bei der CVE-Organisation innehaben, arbeitet Red Hat mit CVE.org zusammen, um offengelegte Cybersicherheitslücken zu identifizieren, zu definieren und zu katalogisieren. Zusätzlich zur Root-Rolle ist Red Hat auch eine CVE Numbering Authority (CNA). Dadurch kann Red Hat Schwachstellen CVE-Nummern zuweisen und CVE-Datensätze veröffentlichen. Das heißt, wenn Nutzende von Red Hat Enterprise Linux über ein neues CVE benachrichtigt werden, ist ein Team von Sicherheitsfachkräften, die mit der Plattform bestens vertraut sind, bereits aktiv an der Suche, Bewertung und Untersuchung erforderlicher Behebungsmaßnahmen beteiligt.

Teilen in der Community

Selbst Nutzende anderer Linux-Distributionen profitieren wahrscheinlich von den Sicherheitsmaßnahmen von Red Hat. Im Einklang mit dem Open Source-Ethos setzt Red Hat auf die Zusammenarbeit innerhalb der Community, wenn es um schnelle Reaktionen, Patches und Strategien zur Behebung von Schwachstellen geht, die das Linux-System betreffen. Damit möchte das Unternehmen den Ruf von Linux als äußerst sicheres Betriebssystem aufrechterhalten.

Das Team von Red Hat arbeitet weltweit mit Teams bei der Entwicklung von Open Source-Sicherheitspraktiken zusammen. Einige Beispiele dafür sind die Entwicklung von OpenSCAP, die Mitgliedschaft in OpenSSF und Beiträge zu OSV.dev.

Diese Zusammenarbeit erstreckt sich auch auf Red Hat Code, der den Community-Mitgliedern zur Ansicht, Prüfung, Überprüfung und Mitwirkung zur Verfügung steht.

Optimierte Linux-Sicherheit mit Red Hat

Mit der Standardisierung auf Red Hat Enterprise Linux setzen Sie auf ein Unternehmen, das auf Security-by-Design setzt. Erfahren Sie mehr darüber, wie Red Hat Ihr Unternehmen beim Aufbau einer sicherheitsorientierten Linux-Plattform unterstützen kann.

Über Red Hat

Red Hat, weltweit führender Anbieter von Open Source-Softwarelösungen für Unternehmen, folgt einem communitybasierten Ansatz, um zuverlässige und leistungsstarke Linux-, Hybrid Cloud-, Container- und Kubernetes-Technologien bereitzustellen. Red Hat unterstützt Kunden bei der Entwicklung cloudnativer Anwendungen, der Integration neuer und bestehender IT-Anwendungen sowie der Automatisierung, Sicherung und Verwaltung komplexer Umgebungen. Als bewährter Partner der Fortune 500-Unternehmen stellt Red Hat vielfach ausgezeichnete Support-, Trainings- und Consulting-Services bereit, die unterschiedlichen Branchen die Vorteile der Innovation mit Open Source erschließen. Als Mittelpunkt eines globalen Netzwerks aus Unternehmen, Partnern und Communities unterstützt Red Hat Unternehmen bei der Steigerung ihres Wachstums und auf ihrem Weg in die digitale Zukunft.

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com