Red Hat
Enterprise Linux

Eine Zero-Trust-Basis in Linux-Umgebungen entwickeln

Mit einer Zero-Trust-Architektur können Sie Ihre IT-Umgebung und Ihr Unternehmen besser schützen.

Red Hat verwendet mehrere wichtige Prinzipien als Guide für die Implementierung der Zero-Trust-Architektur:

- Kein implizites Vertrauen in Akteure, verifizieren Sie sie stets
- Strategie der geringsten Berechtigung beim Zugriff
- Standardmäßige Annahme, dass Netzwerke und Netzwerkverkehr kompromittiert sind

Moderne IT-Umgebungen erfordern neue Sicherheitsansätze

Herkömmliche perimeterbasierte Sicherheitsansätze können neue, weit verteilte, cloudbasierte Umgebungen nicht effektiv schützen. Zudem nehmen Sicherheitsbedrohungen und die Auswirkungen von Verstößen weiter zu. Angreifer nutzen Schwachstellen aus, die häufig aufgrund veralteter Sicherheitsparadigmen wie Ein-Faktor-Authentifizierung, implizites Vertrauen, perimeterbasierte Architekturen und unzureichende Verfolgung des Verhaltens von Nutzenden und Events bestehen.

Durch das Implementieren einer Zero-Trust-Architektur können Sie Ihre IT-Umgebung und Ihr Unternehmen schützen. Dieser Überblick befasst sich mit den Aspekten beim Errichten von Zero-Trust-Architekturen in Linux®-Umgebungen.

Was ist Zero Trust und wie funktioniert es?

Zero Trust ist ein Architektur-Pattern, bei dem die Sicherheit auf die einzelnen Ressourcen angewendet wird, anstatt die Sicherheit ausschließlich am Netzwerkrand oder über eine zentralisierte Sicherheitsmanagement-Lösung zu verwalten. Die Basis des Zero-Trust-Modells besteht darin, dass keinem Akteur, System, Netzwerk oder Service, der innerhalb oder außerhalb des Sicherheitsperimeters operiert, implizit vertraut wird. Damit eine Ressource eine Verbindung zu einer anderen Ressource herstellen kann, muss die Verbindung sowohl authentifiziert als auch autorisiert sein, um explizites Vertrauen zu schaffen.

Das Identitäts- und Zugangsmanagement ist der zentrale Bestandteil von Zero-Trust-Architekturen. Zero-Trust-Architekturen sollten den Zugang zu Ressourcen standardmäßig verweigern. Jedes Subjekt, das mit einer Ressource interagieren möchte, muss für diese spezifische Interaktion ausdrücklich Zugang beantragen, und das Risiko dieser Interaktion sollte bewertet werden, bevor der Zugang gewährt wird. Ein Verständnis der Identität und der Eigenschaften des Subjekts ist für diese Bewertung von entscheidender Bedeutung. Sie müssen festlegen, wer den Zugriff beantragt, auf welche Ressourcen diese Person zugreifen muss, welchen Zweck die Transaktion hat und wie der Zugriff zeitlich, methodisch und funktional eingeschränkt werden soll.

Sobald die Zugriffsentscheidungen getroffen sind, müssen Sie Identitäten und Identitätsattribute geschützt und konsistent speichern, verwalten, kuratieren und aktualisieren. Die meisten Unternehmen verwenden ein oder mehrere Identitätsmanagement-, Directory Server- und Credential Management-Systeme zum Verwalten dieser Informationen. Außerdem sollten Sie diese Zugangsentscheidungen immer wieder überprüfen, um sicherzustellen, dass sie auch langfristig gültig sind.

Überlegungen zur Implementierung einer Zero-Trust-Architektur

Das Einführen eines Zero-Trust-Sicherheitskonzepts erfordert in der Regel eine Änderung der Sicherheits- und IT-Mentalität und -Prozesse, aber auch eine Reihe von technologischen Fähigkeiten. In den folgenden Abschnitte werden die wichtigsten Funktionen und Merkmale von Betriebssystemen und Identitätsmanagementlösungen erläutert, die beim Einführen einer Zero-Trust-Architektur zu beachten sind.

Möglichkeiten und Funktionen des Betriebssystems

Ihr Betriebssystem bildet die Basis für Ihre IT-Umgebung und Ihre Zero-Trust-Architektur.

Red Hat Enterprise Linux

Was ist eine Vertrauensgrenze?

Als Vertrauensgrenze wird eine logische Trennung zwischen Komponenten bezeichnet, bei denen die teilnehmenden Subjekte einer Interaktion ihren Vertrauenszustand ändern, üblicherweise zwischen den beiden Zuständen *vertrauenswürdig* und *nicht vertrauenswürdig*. Der Übergang von nicht vertrauenswürdig zu vertrauenswürdig erfordert im Allgemeinen 2 Faktoren:

- **Authentifizierung**, Verifizierung und Validierung der Identität der Subjekte
- **Autorisierung**, Verifizierung und Validierung des Rechts auf und der Notwendigkeit des Zugriffs auf eine Ressource.

Bewährte Betriebssystem-Lieferkette

Zero-Trust-Modelle setzen voraus, dass Ihr Betriebssystem so sicher wie möglich ist und standardmäßig sämtlichen Zugriff verweigern kann. Wählen Sie ein sicherheitsorientiertes Betriebssystem, das über eine vertrauenswürdige Softwarelieferkette geliefert wird, um Ihr Risiko zu verringern. Ziehen Sie Anbieter von Betriebssystemen in Betracht, die Folgendes bieten:

- Statische Code-Analyse des gesamten Betriebssystems zur Ermittlung von Fehlern in der Programmierung, der Speicherreferenzierung und der Validierung des Input-Streams sowie zur Sicherstellung der Compliance mit bewährten Codierungsverfahren
- Compiler Flags zum Ausführen von Anwendungen und zum Zuweisen von Speichersegmenten auf nicht prädiktive Weise, um Stack Smashing zu verhindern, Speicherkorruption abzuschwächen und Hardware Support für Kontrollflussintegrität zu bieten
- Umfassende QE-Tests (Quality Engineering) für weniger Sicherheitsmängel vor der Auslieferung
- Patching-Verfahren für Schwachstellen, die regelmäßig Problembehebungen für bekannte Schwachstellen liefern

Mandatory Access Control

Ihr Betriebssystem muss außerdem den Zugriff auf Ressourcen isolieren und individuell steuern können. MAC-Technologien (Mandatory Access Control) wie Security-Enhanced Linux (SELinux) übernehmen genau diese Aufgabe gemäß zentral verwalteten Sicherheitsrichtlinien. Achten Sie auf diese Funktionen des Betriebssystems:

- Integrierte MAC mit granularer, anpassbarer Kontrolle über Dateien, Prozesse, Nutzende und Anwendungen, um das Risiko einer unzulässigen Berechtigungserweiterung zu minimieren
- Möglichkeit, den Zugang standardmäßig zu verweigern, um den Zero-Trust-Prinzipien gerecht zu werden

Moderne, skalierbare und richtlinienbasierte Verschlüsselung

Die Verschlüsselung des Daten- und Netzwerkverkehrs erhöht den Schutz für Ihre IT-Umgebung und Ihr Unternehmen. Mehrere Industriestandards, darunter der Federal Information Processing Standard (FIPS) 140, schreiben systemweite Verschlüsselungseinstellungen vor. Mit der richtlinienbasierten Verschlüsselung können Sie einheitliche Konfigurationen für Ihre verschiedenen Systeme anwenden, um die Compliance-Anforderungen zu erfüllen. Wählen Sie ein Betriebssystem, das Folgendes umfasst:

- Richtlinienbasierte Verschlüsselungskontrollen, mit denen Sie die Einstellungen konsistent auf Ihre Systeme anwenden können
- Standardprofile für gängige Sicherheitsstandards wie FIPS 140
- Automatisierte Anwendung und Durchsetzung von Richtlinien zum Optimieren der Verwaltung, Reduzieren von Fehlern und Entschlüsseln von Dateien und Software-Volumes nur dann, wenn es die Richtlinie ausdrücklich erlaubt
- Anpassbare Richtlinien und Einstellungen, die den Anforderungen Ihres Unternehmens entsprechen

Zulassungslisten für Anwendungen

Bei den Zulassungslisten für Anwendungen handelt es sich um einen Index zugelassener Anwendungen oder ausführbarer Dateien, die von bestimmten Nutzenden auf einem System ausgeführt werden dürfen. Diese Praxis ergänzt die obligatorischen Zugangskontrollen, die das Verhalten von Anwendungen kontrollieren können, aber nicht wissen, welche Anwendungen vertrauenswürdig sind.

Wählen Sie ein Betriebssystem, das integrierte Funktionen für die Anwendungszulassung bietet, wie beispielsweise File Access Policy Daemon (fapolicyd), um nicht zugelassene Anwendungen auf Systemen oder in Netzwerken zu erkennen und deren Ausführung zu verhindern, sowie vordefinierte und anpassbare Richtlinien für die Zulassungsliste.

Red Hat
Enterprise Linux

Hardware-basierte Root-of-Trust

Mit Hardware-basierten Root-of-Trust-Funktionen können Sie die Systemintegrität überprüfen und sicherstellen, dass Ihre Systeme nicht verändert oder manipuliert wurden. Entscheiden Sie sich für ein Betriebssystem, mit dem Sie Ihre kryptografischen Secrets aus der Software auf manipulationssichere Hardwaregeräte wie Smartcards, Hardware-Sicherheitsmodule (HSMs) und Trusted Platform Modules (TPMs) verlagern können.

Compliance Scanning

Die Non-Compliance mit Unternehmens- und Branchenstandards und -vorschriften kann für Ihr Unternehmen kostspielig und riskant sein. System-Scanning-Tools wie Open Security Content Automation Protocol (OpenSCAP) können Audits erleichtern und Sie bei der Problembehebung von nicht konformen Systemen unterstützen. Wählen Sie ein Betriebssystem, das folgende Funktionen bietet:

- Integrierte Scan-Tools mit vordefinierten und anpassbaren Compliance-Profilen
- Funktionen zum Erstellen von Berichten und Baselines zur Erleichterung von Audits und zum Erkennen von Drift
- Automatisierte Problembehebung bei nicht konformen Systemen
- Automatisierung und Integration mit anderen Tools für die Verwaltung in großem Umfang

Monitoring und Protokollierung von Transaktionen

Durch Überwachung und Protokollierung können Sie die Aktionen der Nutzenden überprüfen, um festzustellen, ob eine unerwünschte Aktion stattgefunden hat. Tools zur Aufzeichnung von Sessions und zur Log Aggregation können Ihnen helfen, einen Einblick in die Aktionen in Ihrer gesamten Umgebung zu erhalten. Wählen Sie ein Betriebssystem, das Folgendes umfasst:

- Protokollierung von Input, Output, Systemzustand und Umgebungsvariablen, um einen kontextbezogenen Einblick zu ermöglichen
- Systemunabhängiger Storage zum Schutz vor Manipulationen
- Anpassbare Erfassungseinstellungen für einfacheres Auditing

Wichtige Sicherheitsstandards

- FIPS 140
- Common Criteria (CC)
- Secure Technical Implementation Guidelines (STIG)

Unabhängige Beglaubigung und Sicherheitszertifizierung

Durch die Überprüfung der Compliance Ihres Betriebssystems durch einen Drittanbieter können Sie mit mehr Zuversicht arbeiten. Entscheiden Sie sich für ein Betriebssystem, das Compliance mit gängigen Standards bietet.

Fähigkeiten und Funktionen der Identitätsmanagementlösung

Ihre Identitätsmanagementlösung umfasst Identitäten, deren Attribute, Berechtigungsnachweise, Zertifikate und andere Elemente, die für die Autorisierung und Authentifizierung des Zugriffs auf Ressourcen erforderlich sind.

Identitätsspeicher

Mit einem Domain Controller können Sie Identitäten, Zugriff und Richtlinien für Nutzende, Services und Hosts verwalten. Durch die Nutzung eines zentralen Identitätsspeichers und Domain Controllers können Sie den Verwaltungsaufwand reduzieren, die Sicherheitsverwaltung vereinfachen und die Konsistenz in Ihrer gesamten Umgebung sicherstellen. Ziehen Sie eine Lösung in Betracht, die zentralisierte Identitätsmanagement-Funktionen für optimierte Abläufe und mehr Konsistenz bietet. Ihre Lösung sollte auch die Infrastrukturen und Plattformen unterstützen, die Sie derzeit nutzen und in Zukunft nutzen wollen.

Red Hat Enterprise Linux

Wichtige Authentifizierungsarten

- Normale, einmalige und gehärtete Passwörter
- Remote Authentication Dial-In User Service (RADIUS)
- Public Key Cryptography for Initial Authentication (PKINIT)

Integration mit anderen Systemen für das Identitätsmanagement

Die meisten Unternehmen verwenden bereits ein oder mehrere Identitätsmanagementsysteme für ihre Linux- und Windows-Umgebungen. Mit der Integration dieser Systeme in eine einheitliche Gesamtlösung können Sie die Abläufe zentralisieren und die Konsistenz in Ihrem Unternehmen sicherstellen. Entscheiden Sie sich für eine Identitätsmanagementlösung, die mit gängigen Tools wie Microsoft Active Directory kompatibel ist, um Identitäten in unterschiedlichen Umgebungen zu verwalten.

Richtlinienverwaltung

Mit einem richtlinienbasierten Ansatz für das Identitätsmanagement können Sie Konsistenz, Effizienz und Sicherheit verbessern. Identitätsmanagementlösungen, mit denen Sie über eine zentrale Schnittstelle richtlinienbasierte Kontrollen festlegen und anwenden können, sorgen für die richtige Konfiguration von Identitäten, Zugriff und Ressourcen. Achten Sie auf diese Funktionen und Möglichkeiten:

- Role-based Access Control (RBAC) und richtlinienbasierte Zugangskontrollfunktionen
- Anpassbare Identitäts- und Zugriffsrichtlinien
- Authentifizierungs- und Autorisierungsmanagement-Funktionen
- Aufzeichnung von Sessions, Auditing und Protokollierungsfunktionen

Multi-Faktor-Authentifizierung

Mit der Multi-Faktor-Authentifizierung (MFA) wird eine zusätzliche Sicherheitsebene hinzugefügt, die eine mehrfache Überprüfung der Identität erfordert, bevor der Zugang gewährt wird. Mit hardwarebasierten Root-of-Trust-Funktionen können Sie die Systemintegrität überprüfen und sicherstellen, dass Ihre Systeme nicht verändert oder manipuliert wurden.

Gängige Zertifikatsprotokolle und -standards

- X.509
- Automated Certificate Management Environment (ACME)
- Simple Certificate Enrollment Protocol (SCEP)
- Secure sockets layer (SSL)
- Transport layer security (TLS)

Certificate Management

Digitale Zertifikate enthalten Informationen, die zur Authentifizierung der Identität von Nutzenden, Anwendungen, Websites und anderen Subjekten benötigt werden. Sie sollten nach den Grundsätzen der geringsten Berechtigung erstellt, überwacht, erneuert und außer Kraft gesetzt werden. Entscheiden Sie sich für eine Identitätsmanagementlösung, die Folgendes bietet:

- Vollständiges Lifecycle-Management für Nutzende, Host und Service-Zertifikate
- Unterstützung für gängige Protokolle und Standards
- Automatisiertes Tracking des Ablaufdatums von Zertifikaten, um eine rechtzeitige Erneuerung zu gewährleisten
- Unterstützung für die Authentifizierung über die Public Key Infrastructure (PKI)

Single Sign-On

Die einzelnen Services, Geräte und Server erfordern eine separate Zugriffsauthentifizierung. Single-Sign-On-Systeme (SSO) vereinfachen den Zugang, indem sie einen zentralen Identitätsservice nutzen, mit dem Server nach verifizierten Nutzenden suchen können. Die Nutzenden müssen sich nur einmal authentifizieren und können auf mehrere Services zugreifen. Verwenden Sie eine Identitätsmanagementlösung, die sowohl die Webauthentifizierung als auch die Services unterstützt, die Sie derzeit nutzen und in Zukunft nutzen wollen.

Aufbau einer Zero-Trust-Basis mit Red Hat Enterprise Linux

Red Hat bietet eine Basistechnologie, mit der Sie Zero-Trust-Architekturen entwerfen, aufbauen und verwalten können. Red Hat® Enterprise Linux bietet die Sicherheitstechnologien, Kontrollen, Zertifizierungen und den Support, die für die Einführung von Zero-Trust-Modellen erforderlich sind. Es erfüllt die in dieser

Beschleunigtes Deployment mit fachkundigen Services

Red Hat bietet Services an, die Sie bei der Einführung einer Zero-Trust-Architektur auf der Basis von Plattformen und Produkten von Red Hat unterstützen.

- Red Hat Open Innovation Labs ist eine immersive Residency, die Engineers mit Open Source-Expertinnen und -Experten zusammenbringt, die Sie dabei zu unterstützen, konkrete Geschäftsergebnisse zu erzielen.
- Red Hat Services: Zero Trust Adoption Journey ist eine Consulting-Initiative, die Sie bei der Bewertung Ihrer aktuellen Situation und dem Erstellen eines Plans für den Aufbau einer Zero-Trust-Architektur unterstützt.

Übersicht besprochenen Anforderungen an das Betriebssystem mit der Bereitstellung über eine zuverlässige Lieferkette, SELinux-Zugangskontrollen, systemweiten Verschlüsselungsrichtlinien, Zulassungslisten für Anwendungen, hardwarebasiertem Root-of-Trust, Aufzeichnung von Sessions und Systemrollen. Außerdem enthält es einen integrierten OpenSCAP-Scanner und den Red Hat Insights Service für prädiktive Analysen und Problembehebung. Und nicht zuletzt ist Red Hat Enterprise Linux nach vielen staatlichen Sicherheitsstandards wie CC, FIPS 140, STIG und Section 508 zertifiziert.

Red Hat Identity Management ist in Red Hat Enterprise Linux enthalten und kann Sie dabei unterstützen, das Identitätsmanagement zu zentralisieren, Sicherheitskontrollen durchzusetzen und die Compliance von Sicherheitsstandards in Ihrer gesamten Umgebung einzuhalten. Damit erhalten Sie die Funktionen, die Sie für die Implementierung von Best Practices zu Zero Trust brauchen, und vereinfachen gleichzeitig Ihre Infrastruktur für das Identitätsmanagement. Es kann über Standard-Schnittstellen auch in Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP) und andere Lösungen von Drittanbietern eingebunden werden. Außerdem unterstützt Red Hat Identity Management zertifikatbasierte Authentifizierungs- und Autorisierungsmethoden.

Red Hat Enterprise Linux und Red Hat Identity Management lassen sich in das weitere Red Hat Portfolio integrieren und bilden eine einheitliche Basis für Zero-Trust-Architekturen.

- Red Hat Single Sign-On bietet Web-Single-Sign-On-Funktionen, die auf gängigen Standards basieren.
- Red Hat Satellite ist ein Produkt für das Infrastrukturmanagement, mit dem Sie Ihre Red Hat Enterprise Linux-Umgebungen effizient, sicher und konform ausführen können.
- Red Hat Ansible® Automation Platform bietet ein unternehmensgerechtes Framework für die Entwicklung und Ausführung automatisierter IT-Prozesse in großem Umfang.
- Red Hat Certificate System ist eine Zertifizierungsstelle, die komplexe Managementaktivitäten wie die Provisionierung von Smart Cards, benutzerdefinierte Zertifikatstypen und den geschützten Storage von Secrets unterstützt.
- Red Hat Directory Server ist eine vom Betriebssystem unabhängige, netzwerkbasierte und skalierbare Registry, mit der Sie Identitäts- und Anwendungsdaten für verteilte Directory Topologies zentral speichern können.

Nächste Schritte

- Erfahren Sie mehr über Red Hat Enterprise Linux Security.
- Mehr über das Sicherheitskonzept von Red Hat für die Hybrid Cloud erfahren

Über Red Hat

Red Hat, weltweit führender Anbieter von Open Source Software-Lösungen für Unternehmen, folgt einem community-basierten Ansatz, um zuverlässige und leistungsstarke Linux-, Hybrid Cloud-, Container- und Kubernetes-Technologien bereitzustellen. Red Hat unterstützt Kunden bei der Entwicklung cloudnativer Applikationen, 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 jeder Branche die Vorteile der Innovation mit Open Source erschließen können. 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
F31712_0522_KVM