Red Hat

Eine Basis für Sicherheit mit Zero Trust und Automatisierung schaffen

Wie Sie Zero Trust effektiv nutzen können

Inhaltsverzeichnis

Einleitung

Ihre Organisation existiert rund um die Uhr. Leider gilt das auch für Cyberkriminelle und andere Angreifer, die Ihre Daten stehlen oder Ihrem Unternehmen, Ihren Partnern und Ihren Kunden schaden wollen.

Heutzutage sind Organisationen einer Vielzahl an Cyberbedrohungen ausgesetzt, die IT-, Sicherheits- und Operations-Teams konstant auf Trab halten. Diese Bedrohungen beeinträchtigen Organisationen aller Größen und können Milliarden kosten. Laut einem Bericht von IBM kostete im Jahr 2021 eine durch eine Cyberattacke verursachte Datenpanne durchschnittlich 4,24 Millionen USD. Dies ist eine Steigerung im Vergleich zu Jahr 2020, als diese Kosten noch 3,86 Millionen USD betrugen.[1]

Diese Bedrohungen beschränken sich auch nicht nur auf externe Angreifer. Der 2021 Data Breach Investigations Report von Verizon gibt an, dass 30 % der Datenpannen durch den Zugriff von Beschäftigten auf Systeme ausgelöst wurden, die sich außerhalb Ihrer definierten Rollen und Berechtigungen befanden.[2]

Die Zunahme in Anzahl und Schwere der Attacken wird von mehreren Faktoren ausgelöst. Dazu zählen schnelle Veränderungen in der Netzwerkinfrastruktur, Migrationen von On-Premise zu cloudbasierten Lösungen und der Anstieg von Homeoffice-Arbeit seit dem Jahr 2020.

Die Umstellung auf Homeoffice hat zu einer Vergrößerung der Angriffsflächen geführt, da sowohl dienstliche als auch private Geräte über persönliche und öffentliche Internetverbindungen auf sensible Systeme zugreifen. Weiterhin gibt es einen Anstieg in Anzahl und Qualität der Phishing- und Spear-Phishing-Attacken, da Beschäftigte mit Kolleginnen und Kollegen zusammen arbeiten, die sie nie persönlich getroffen haben.

Die Migration zu cloudbasierten Lösungen bringt einer Organisation viele Vorteile, zu denen unter anderem Kosteneinsparungen und eine signifikante Reduktion des physischen Dokumentations-Storage zählen. Aber für diese Vorteile müssen auch Nutzer-, Anwendungs- und Infrastruktursicherheit für Hunderte bis Tausende Nutzende auf Legacy-On-Premise- und cloudbasierten Systemen verwaltet werden.

Durch die Kombination von Homeoffice und Migration zur Cloud ist der traditionelle VPN-Sicherheitsansatz einer geschlossenen Plattform obsolet geworden. Zusätzlich zu den Beschäftigten, die sich von mehr Geräten mit mehr Systemen verbinden, hat die Einführung von IoT und Edge Computing neue potenzielle Angriffsvektoren für Cyberangreifer geschaffen.

Neben dem Zugriff der Beschäftigten auf Systeme haben Organisationen Teams skaliert, um unterschiedliche Netzwerk- und Sicherheitssysteme zu verwalten. InfoSec-, SysOps-, NetOps- und andere Teams arbeiten oft sowohl gleichzeitig als auch unabhängig voneinander, um Sicherheitsrichtlinien durchzusetzen und auf Vorfälle zu reagieren. Dennoch arbeiten diese Teams oft einzeln und verwenden verschiedene Systeme sowie Prozesse, was sich auf ihre Fähigkeit auswirkt, eine Reaktion zu koordinieren. Wenn es um die Reaktion auf Sicherheitsbedrohungen geht, zählt jedoch jede Sekunde.

1 „Cost of a Data Breach Report 2021", IBM, abgerufen am 16. Juni 2022.
2 „2022 Data Breach Investigations Report", Verizon, abgerufen am 16. Juni 2022.

Sie möchten mehr über Zero Trust erfahren? Dann lesen Sie jetzt weiter.

Sie kennen Zero Trust schon, aber möchten mehr über die Automatisierung erfahren? Weiter mit: **Zero Trust mit Automatisierung skalieren**

Eine weitere Herausforderung, die Cyberattacken begünstigt, ist die mangelnde Integration zwischen Lösungen, die die organisatorische Infrastruktur antreiben und schützen. Wenn die Teams, die diese Lösungen verwalten, nicht effizient kommunizieren können, verhindert dies eine effiziente Reaktion auf Sicherheitsvorfälle.

Diese Cyberrisiken sind nicht nur führenden Sicherheitsfachleuten bekannt. Organisationen und Anbieter haben sich an Richtlinien wie die DSGVO (Datenschutz-Grundverordnung der Europäischen Union) und den CCPA (California Consumer Privacy Act) angepasst. Im Jahr 2021 erkannte die US-Regierung diese zunehmende Bedrohungslage und veröffentlichte eine Verfügung zur Verbesserung der nationalen Cybersicherheit.

Organisationen müssen in ihren Richtlinien, Netzwerken und Anwendungen einen sicherheitsorientierten Ansatz verfolgen, um auf diese Bedrohungen zu reagieren. Viele Organisationen sehen die Zero Trust-Architektur als einen vielversprechenden Ansatz, darunter die US-Regierung, die eine Implementierung von Zero Trust-Architektur in ihren Netzwerken mit einem Mandat voranbringen will.

Doch die Implementierung von Zero Trust ist nur der Anfang, insbesondere in großen Organisationen mit mehreren Standorten und einer Mischung aus On-Premise-, Cloud- und Edge-Systemen. Für die Skalierung der Zero Trust-Architektur benötigen Sie eine unternehmensgerechte Automatisierung. In diesem E-Book erfahren Sie, warum Red Hat® Ansible® Automation Platform die richtige Lösung für Ihre Organisation ist.

Zero Trust als Problemlösung?

Herkömmliche Sicherheitsmodelle wurden für Systeme entwickelt, auf die Beschäftigte von einem physischen Standort aus zugreifen. Als sich Remote-Access-Optionen von Einwahlverbindungen hin zu ständig verfügbaren High-Speed-Verbindungen entwickelten, wurde der externe Zugriff mithilfe von VPNs (Virtual Private Networks) reguliert. Obwohl VPNs eine sichere Authentifizierung in Netzwerken ermöglichen, geben Sie Nutzenden auch Zugriff auf mehr Ressourcen und Systeme als notwendig ist, wodurch potenzielle Sicherheitsrisiken entstehen.

Heutzutage können VPNs und standardmäßige, nutzerbasierte Berechtigungen nicht mehr das Maß an Sicherheit bieten, das für die komplizierte On-Premise, hybride und cloudbasierte Lösungsarchitektur notwendig ist, auf die sich Organisationen für ihre Geschäftstätigkeiten verlassen. Es wurde ein neues Modell benötigt, das grundlegende Veränderungen des Sicherheitsansatzes beinhaltete. Dieser veränderte Sicherheitsansatz heißt Zero Trust-Architektur.

Zero Trust wurde 2010 als Sicherheitsmodell anerkannt und agiert unter der Annahme, dass es innerhalb und außerhalb des Netzwerks Angreifer gibt. Basierend auf dieser Annahme sorgen die Standardeinstellungen bei Zero Trust dafür, dass Interaktionen grundsätzlich in einem nicht vertrauenswürdigen Zustand begonnen werden.

Statt sich ausschließlich auf standort-, rollen- oder nutzerbasierte Berechtigungen zu verlassen, erfordert das Zero Trust-Framework eine Verifizierung von Nutzer, Gerät und Anwendung, um einen vertrauenswürdigen Zustand für die Interaktion herzustellen. Die Implementierung von Zero Trust unterstützt ein völlig neues Sicherheitsverständnis, indem es Systemarchitekten anweist, Nutzende oder Geräte lückenlos bei Transaktionen zu authentifizieren und nur auf Basis des Least Privilege-Konzepts Zugang zu Daten und Systemen zu gewähren.

Lückenlose Transaktionsauthentifizierung

Die Basis einer Zero Trust-Architektur ist es, Interaktionen grundsätzlich als mögliche Bedrohung zu behandeln, unabhängig davon, ob diese innerhalb oder außerhalb des Netzwerks stattfindet. Bevor die Interaktion fortschreiten kann, müssen ihre Komponenten authentifiziert werden. Die Implementierung einer Zero Trust-Architektur benötigt ihre eigenen, besonderen Komponenten. Der Kern besteht aus:

- **Nutzer.** Authentifizieren, dass der Nutzer die erforderlichen Berechtigungen hat, um auf ein Netzwerk, eine Anwendung oder ein cloudbasiertes System zuzugreifen.
- **Anwendung.** Verifizieren, dass der Nutzer die erforderlichen Berechtigungen hat, um auf Daten oder eine Anwendungen zuzugreifen.
- **Gerät.** Bestätigen, dass das Gerät des Nutzers die erforderliche Autorisierung hat, um sich mit dem Netzwerk und der Anwendung zu verbinden.
- **Status.** Überprüfen, ob das verwendete Gerät die erforderlichen Updates, Patches und Verschlüsselung hat, um sicher auf das Netzwerk und die Anwendung zuzugreifen.

Der Umstieg auf Zero Trust findet auch im öffentlichen Sektor statt, besonders in der US-Bundesregierung. Die 2021 veröffentlichte Verfügung zur Verbesserung der nationalen Cybersicherheit (Executive Order on Improving the Nation's Cybersecurity) enthält mehrere Mandate, die die Migration zu sicheren cloudbasierten Lösungen und die Umstellung auf Zero Trust-Architektur für sämtliche Regierungsinfrastrukturen fördern sollen.

Organisationen, die an Regierungsbehörden verkaufen oder diese unterstützen, müssen beim Upgrade ihrer Sicherheit und Infrastruktur die Einhaltung von Zero Trust-Standards sicherstellen.

Herausforderungen bei der Implementierung von Zero Trust

Angesichts der Zunahme an Bedrohungen und Angriffsvektoren ist es absolut notwendig, Zero Trust in Ihrer Organisation zu implementieren. Trotz der vielen Vorteile im Vergleich mit herkömmlicher Sicherheit, gibt es bei der Implementierung von Zero Trust in bestehender Infrastruktur Herausforderungen.

Erstens kann die bestehende Infrastruktur aus mehreren Lösungen von verschiedenen Anbietern bestehen. Auch wenn die meisten Anbieter Fortschritte bei der Einführung von Zero Trust-Prinzipien gemacht haben, bietet nicht jedes System eine Interoperabilität mit den Systemen anderer Anbieter. Interne Teams von SysOps bis NetOps könnten auf Probleme stoßen, bei denen Lösungen nicht korrekt zusammenarbeiten. Nicht verbundene Teams und Systeme könnten bei Problemen in der Interoperabilität sogar zu Lücken in der Bedrohungserkennung führen.

Zweitens erfordert Zero Trust ein konsequentes Umdenken von Führungskräften beim Thema Sicherheit. Der Übergang von der herkömmlichen Vorgehensweise zu einer standardmäßigen Ablehnung erfordert, dass Führungskräfte sich in ihrer Organisation dafür engagieren müssen, Zero Trust-Prinzipien und -Praktiken durchzusetzen, selbst wenn diese mühsam erscheinen. Ohne dieses Engagement können Teams oft auf Legacy-Praktiken zurückfallen oder sogar separate „Schatten-IT"-Angebote erschaffen, die Zero Trust-Architektur, -Richtlinien und -Prozesse umgehen.

Wie man mit Zero Trust-Architektur eine starke Sicherheitsbasis schafft

Herkömmliche Sicherheitsansätze wie VPNs mit physischen oder digitalen Token wurden dazu entwickelt, einen sicheren Remote-Pfad zu einem On-Premise-Netzwerk zu bieten. Der herkömmliche Netzwerksicherheitsansatz wird oft als „Castle-and-Moat"-Modell („Burg und Wassergraben") bezeichnet und legt den Fokus ausschließlich auf einen Eingangspunkt, der als Zugang zu allen Ressourcen auf der anderen Seite fungierte.

Man kann ihn mit dem Konzept eines Schlüsselkarten-Zugangs zu Gebäuden oder zu sicheren Bereichen innerhalb von Gebäuden vergleichen. Eine Organisation geht möglicherweise davon aus, dass ihre physische Sicherheit durch die rollenbasierte Sicherheit für Beschäftige entsteht, mit der diese das Gebäude betreten oder sich in verschiedenen Bereichen bewegen können. Aber diese physische Sicherheit wird gefährdet, wenn ein Angreifer einen Social Engineering-Hack nutzt und sich beispielsweise als Essenslieferant ausgibt, um vom Sicherheitspersonal des Gebäudes Zugang zu erhalten.

Zero Trust ist der Kern und keine Ergänzung

Zero Trust-Prinzipien machen Sicherheit zu einer grundlegenden Komponente aller Projekte, unabhängig davon, ob es um das Entwickeln neuer Produkte oder das Implementieren neuer Infrastruktur geht. Anstatt Sicherheit auf dem Netzwerkzugriff aufzubauen, wird Zero Trust-Architektur standardmäßig auf sämtliche Interaktionen innerhalb der Organisation angewendet.

Der Einstieg mit Zero Trust

Die Implementierung von Zero Trust beginnt nicht bei der Auswahl von Anbietern oder der Migration auf eine andere Sicherheitsplattform. Stattdessen müssen Organisationen sich eine einfache Frage stellen, die signifikante Auswirkungen auf ihre Zero Trust-Strategien hat: Welche Daten, Anwendungen oder Systeme wollen sie beschützen?

- **Inventory erstellen.** Wenn Organisationen verstehen, was geschützt wird, erhalten sie eine Basis, auf der sie die Netzwerk-, Nutzer-, Anwendungs- und Workload-Regeln und -Richtlinien ihrer Zero Trust-Implementierung erstellen können. Diese Basis zeigt außerdem SysOps-, NetOps- und InfoSec-Teams, welche Analysen und Analysetools sie benötigen, um Sicherheitsvorfälle zu entdecken, zu identifizieren und auf diese zu reagieren.
- **Prozesse und Richtlinien entwickeln.** Sobald eine Organisation eine klare Vorstellung davon hat, was genau sie schützt, können interne Teams gemeinsam Zero Trust-Prozesse und -Richtlinien erstellen, mit denen Beschäftigte sicher auf ihre Arbeit zugreifen können.
- **Testen. Ändern. Bereitstellen.** Pläne und ihre tatsächliche Implementierung unterscheiden sich oft. Wenn Operations-, Networking- und Sicherheits-Teams die Prozesse und Richtlinien unter alltäglichen Bedingungen sehen, erhalten sie das benötigte Feedback, mit dem sie Zero Trust in der gesamten Organisation erfolgreich einsetzen können.

Zu verstehen, was geschützt wird, ist die Basis für die Skalierung von Zero Trust durch Automatisierung.

Zero Trust mit Automatisierung skalieren

Erfahren Sie mehr über die Sicherheitsautomatisierung mit Ansible und entdecken Sie in diesem Webcast, wo Sie sich auf Ihrem Automatisierungsprozess befinden.

Eine Zero Trust-Architektur verlangt, dass Ressourcen wie etwa Geräte, Daten und Anwendungen immer auf die gleiche Art und Weise geschützt werden, unabhängig davon, wo sie sich befinden. Wenn eine Workload beispielsweise von einem On-Premise-Rechenzentrum zu einer Private- oder Public Cloud verschoben wird, verlangt die Zero Trust-Architektur, dass dieselben Regeln für das Sicherheitsmanagement angewendet werden. Mit einer Zero Trust-Architektur werden die Entscheidungen von der Workload selbst abstrahiert, wodurch sich der eigentliche Code nicht verändert.

Automatisierung hilft großen Organisationen und schnell wachsenden Unternehmen dabei, ihre Richtlinien, Regeln und Prozesse zu skalieren, wenn neue Tools oder Infrastruktur eingeführt werden. Bevor wir uns anschauen, wie Red Hat® Ansible® Automation Platform eine Automatisierung der Zero Trust-Architektur ermöglicht, sind hier die 5 Vorteile einer Automatisierung von Zero Trust:

Vorteile der Automatisierung

- **Wissen, was Sie schützen.** Zu verstehen, was Sie schützen, ist der Schlüssel für eine Skalierung von Zero Trust in den Geräten, Netzwerken und Anwendungen einer Organisation. Automatisierung hilft Organisationen dabei, diese Ressourcen an mehreren Standorten und in der Cloud zu verfolgen und zu protokollieren.
- **Ständige Compliance.** Die Verwendung von Bots und anderen Automatisierungstools durch Cyberkriminelle erfordert ein Sicherheitssystem, das konstant nach Bedrohungen Ausschau hält. Die Automatisierung von Zero Trust stellt sicher, dass Richtlinien rund um die Uhr durchgesetzt werden.
- **Risikominderung.** InfoSec-Teams können als Reaktion auf Sicherheitsvorfälle Richtlinien und Regeln einführen. Diese Prozesse können dann als Workflows kodifiziert und mithilfe von Automatisierung ausgeführt werden. Dadurch wird das Risiko gemindert, dass dem Administrator bei der Implementierung einer Änderung ein Fehler unterläuft.
- **Verbesserte Reaktionsfähigkeit.** Je länger die Reaktion auf einen Sicherheitsvorfall dauert, desto größer ist das Potenzial für eine Datenschutzverletzung oder Cyberattacke. Die Automatisierung von Zero Trust ermöglicht es Organisationen, schnell und unabhängig von der Anzahl der Nutzenden zu reagieren. Dies geschieht durch automatisierte Aktionen, die nach Bedarf oder durch eventgesteuerte Automatisierung ausgeführt werden können.
- **Schnelles Prototyping.** Automatisierung ermöglicht es Organisationen, Änderungen am Sicherheits-Framework zu prototypisieren, zu testen und zu implementieren und zwar unabhängig davon, wie komplex das Framework ist.

Zero Trust-Automatisierung: Mehr als nur Sicherheit

Wenn Zero Trust auf mehr als nur das Netzwerk und die Sicherheit ausgeweitet wird, können Organisationen Sicherheit zur standardmäßigen Basis ihrer Projekte und Systeme machen. Durch die Automatisierung dieser Prozesse wird der Wert von Zero Trust sogar noch gesteigert, da sichergestellt wird, dass Richtlinien und Prozesse angewendet und geprüft werden, was das Risiko von Cyberangriffen und anderen Attacken reduziert.

Konsistente Sicherheit und Compliance

Automatisierung hilft dabei, Sicherheits- und Compliance-Regeln durchzusetzen, indem sie die Konfigurationen, Anwendungsbereitstellungen und Compliance-Prüfungen verwaltet, die in Entwicklungsprozesse einfließen. Organisationen können die Provisionierung, Konfiguration, Anwendungsbereitstellung und andere Bereiche automatisieren.

Automatisierung sichert aber nicht nur Anwendungen und Komponenten. Sie kann auch zur Verwaltung dieser Komponenten verwendet werden und bietet regelmäßige Compliance-Prüfungen und -Verifizierungen. Sie bietet eine kontinuierliche End-to-End-Durchsetzung des Sicherheitsstatus für den CI/CD-Lifecycle (Continuous Integration and Continuous Development) einer Organisation.

Ganzheitliche Softwaresicherheit

Zero Trust-Prinzipien können außerdem auf Software und Systeme in einer Organisation angewendet werden. Teams und Abteilungen benötigen oft unterschiedliche Anwendungen, Hardware und Lösungen, die keine einsatzbereite Interoperabilität haben. Mithilfe von Automatisierung können Sie mehrere Systeme von verschiedenen Anbietern integrieren, da sie die Erstellung von Automatisierungs-Workflows ermöglicht, mit der Sie eine effiziente und sichere Interoperabilität orchestrieren können.

Intern und extern entwickelte Lösungen können zudem Open Source-Komponenten beinhalten, die eine Überwachung auf Schwachstellen benötigen, damit sie Cyberkriminellen keine neuen Angriffsvektoren bieten können. Dieselbe Automatisierung, die Sie für die Verwaltung der Interoperabilität erstellt haben, können Sie auch dazu nutzen, den korrekten und sicheren Zustand von Anwendungen sicherzustellen.

Automatisierung der Compliance

Automatisierung kann das Auftreten menschlicher Fehler in Compliance-Aufgaben reduzieren. Ein Beispiel ist ein Unternehmen, das Kreditkarten-Transaktionen durchführt. In diesem Fall müssen mehrere Prozesse sowie Hardware- und Software-Überprüfungen stattfinden, um die Compliance mit dem PCI DSS (Payment Card Industry Data Security Standard) sicherzustellen. Für diese Überprüfungen werden auch zeitnahe und akkurate Daten von diesen Systemen benötigt. Statt ein Team oder Beschäftigte zur Überwachung abzustellen, können diese Schritte automatisiert werden. Menschliche Fehler werden reduziert, und mehr Zeit steht für strategische Projekte zur Verfügung.

Automatisieren Sie Zero Trust und mehr mit Red Hat Ansible Automation Platform

Lesen Sie „Red Hat Ansible Automation Platform: Ein Guide für den Einstieg“, um zu erfahren, wie Automatisierung Ihnen weiterhelfen kann.

Zero Trust funktioniert, wenn Organisationen einen klaren Einblick in die Stellen haben, an denen eine Transaktion durchgeführt wird. Red Hat Ansible Automation Platform bringt Zero Trust und andere Automatisierungsfunktionen in Ihre Organisation. Die Plattform bietet einen schnellen ROI (Return on Investment), indem sie die Einstiegsbarrieren für Automatisierung in den Bereichen Sicherheit, Networking, Anwendung, Cloud und Edge Computing senkt.

Zero Trust	**Automatisieren Sie Zero Trust mit Red Hat Ansible Automation Platform**
Zero Trust verfolgt den Ansatz einer standardmäßigen Ablehnung.	Mit Red Hat Ansible Automation Platform können Administrierende Zugangskontrollen durchzusetzen und Berechtigungen, Privilegien und Rollen an Nutzende vergeben. Es automatisiert außerdem die Verschlüsselung, inklusive mTLS (Mutual Transport Layer Security, Prüfpfade und Inventarkontrollen.
Zero Trust nutzt Autorisierungsrichtlinien, um den Zugang zu Anwendungen oder Ressourcen einzuschränken.	Red Hat Insights for Ansible Automation Platform hilft Organisationen bei der Identifizierung und Überwachung von Ausfällen oder potenziellen Risiken, bei denen der Eingriff von SysOps- oder NetOps-Teams erforderlich sein könnte.
Zero Trust stellt sicher, dass Ressourcen gepatcht wurden, bevor auf diese zugegriffen wird.	Red Hat Ansible Automation Platform sorgt dafür, dass Sicherheitspatches und -updates auf die Anwendungsressourcen in der Infrastruktur einer Organisation angewendet werden.

Red Hat Ansible Automation Platform ist das Bindeglied zwischen unterschiedlichen Technologien, die normalerweise nicht gut miteinander interagieren. Es gibt über 100 Red Hat Certified Content Collections, die von Red Hat und unseren Partnern unterstützt werden. Sie bieten eine konsistente Automatisierung für Infrastruktur-Komponenten, unabhängig davon, ob diese hybrid, Cloud oder On-Premise sind.

Sind Sie bereit für Ihre Zero Trust-Automatisierung?

Red Hat Consulting kann Sie bei Ihrem Automatisierungsvorhaben und der Einführung von Zero Trust unterstützen. Absolvieren Sie unseren kurzen Einstufungstest oder nehmen Sie noch heute Kontakt zu Red Hat Consulting auf.

Lernen Sie mehr über IT-Automatisierung und beginnen Sie eine Testversion.

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
F32053