Schutz vor von KI erkannten Bedrohungen

> Jede Woche müssen wir Sicherheitsscans durchführen … und Schwachstellen in den Paketen auflisten, die auf den Betriebssystemen installiert sind. Werden welche entdeckt, können wir direkt auf der Website von Red Hat umfassende Erklärungen zu den Schwachstellen aufrufen und so feststellen, ob wir betroffen sind. Bei anderen Linux-Distributionen macht das niemand. Ohne diesen Service würde der Betrieb einer Produktivumgebung für Behörden schnell zum Albtraum werden, da wir diese Recherchen Monat für Monat selbst durchführen müssten.[2]

Ryan Kimbrell,
Senior Cloud Operations Engineer bei Zoom

Schutz vor KI-Schwachstellen

Die Bedrohungslandschaft hat sich grundlegend verändert. KI-gestützte Discovery Tools finden potenzielle Schwachstellen in einer Geschwindigkeit, die exponentiell höher ist als die historischen Normen. Die Sicherheitsteams von Unternehmen gerieten bereits 2025 mit durchschnittlich 132 entdeckten CVEs pro Tag an ihre Grenzen.[2] Im 1. Quartal 2026 ist diese Zahl bereits um 26 % gestiegen. Durch die kontinuierlichen Fortschritte bei Discovery Tools für KI-Schwachstellen wie Mythos könnten herkömmliche Ansätze zum Management von CVEs bald nicht mehr tragfähig sein.[1]

Im Jahr 2020 hatten Teams in der Regel 44 Tage Zeit, eine Schwachstelle zu beheben, bevor diese ausgenutzt werden konnte.[3] 2025 hatte sich dieser Vorsprung in ein 7-Tage-Defizit verwandelt.[4] Böswillige Akteure können nun bereits eine Woche, bevor neue CVEs überhaupt veröffentlicht werden, neue Schwachstellen für sich nutzen.

Unterdessen arbeiten die Sicherheitsverantwortlichen in Unternehmen weiterhin im menschlichen Tempo: manuelle Triage, Änderungsmanagement-Meetings und SLAs für Patches, die sich in Wochen oder Monaten bemessen.

Traditionelle IT-Sicherheitsansätze können mit der Triage, die für die Verwaltung der steigenden Anzahl von CVEs erforderlich ist, nicht Schritt halten. In großen Unternehmen werden durchschnittlich 37 % der in einem Jahr entdeckten Schwachstellen nicht gepatcht. Die durchschnittliche MTTR (Mean Time to Remediation) in der Softwarebranche liegt bei 55 Tagen.[5] Dies stellt eine untragbare Sicherheitslücke dar, die Unternehmen große Probleme bereiten kann.

4 entscheidende Herausforderungen für Unternehmenssicherheitsteams heutzutage

Unternehmen haben derzeit gegen 4 zusammenwirkende Faktoren zu kämpfen:

1. **Schnellere Maschinen:** KI-Modelle entdecken neue Schwachstellen in einer Geschwindigkeit, der menschliche Sicherheitsteams und manuelle Prozesse nicht gewachsen sind.
2. **Übermäßiges Volumen:** Eine massive Zunahme der Patch-Releases von Anbietern kann Sicherheitsteams überfordern, zu deutlicher Alarmermüdung führen und traditionelle Workflows für das Schwachstellenmanagement überlasten.
3. **Stabilität über Sicherheit:** Teams verzögern Patching-Maßnahmen, um eine Unterbrechung von Produktionsanwendungen zu vermeiden.
4. **Konfigurationsdrift:** Traditionelle Umgebungen und Konten mit zu vielen Berechtigungen lassen sich weitaus schneller in für KI ausnutzbare Pfade umsetzen als dies bei einer traditionellen manuellen Bewertung möglich ist.

Die Lösung liegt nicht in noch mehr Sicherheitssoftware. Bei bestehenden Kunden von Red Hat befinden sich die erforderlichen integrierten Fehlerbehebungsfunktionen wahrscheinlich bereits in ihrem Portfolio. Sie müssen nur noch aktiviert werden.

Aufbau einer sicherheitsorientierten Basis mit Red Hat Enterprise Linux

Mit Red Hat® Enterprise Linux® lassen sich die Auswirkungen von CVEs minimieren und Unternehmen können gleichzeitig Patches prüfen, testen und bereitstellen. Der Image-Modus für Red Hat Enterprise Linux stellt die Plattform als signiertes, versioniertes Container-Image mit einer Software Bill of Materials (SBOM) bereit. SELinux (Security-Enhanced Linux) und fapolicyd (File Access Policy Daemon) ergänzen dies um Runtime-Ebenen, mit denen sich unbefugte Ausführungen verhindern und kompromittierte Prozesse einschränken lassen.

Erkennung realer Sicherheitsrisiken mit Red Hat Lightspeed

Bevor Fehlerbehebungen in großem Umfang erfolgen können, müssen die Teams wissen, wo genau die Sicherheitslücken sind, und zwar nicht in einer allgemeinen Schwachstellendatenbank, sondern in ihrer spezifischen Umgebung, unter Berücksichtigung ihrer tatsächlichen Konfigurationen und aktiven Workloads.

Mit Red Hat Lightspeed können Unternehmen CVEs auf Systemen mit Red Hat Enterprise Linux priorisieren. Dazu werden Paket- und Sicherheitshinweisdaten mit von Red Hat kuratierten Sicherheitsregeln, Workload-Gruppierungen und konfigurationsbezogenen Bewertungen kombiniert, einschließlich Kontrollmechanismen wie SELinux und servicebezogenen Sicherheitsrisiken. Im Gegensatz zum versionsbasierten Scan unterscheidet Red Hat Lightspeed zwischen Systemen mit ausnutzbaren Schwachstellen und solchen, die zwar anfällig, aber nicht betroffen sind. Dadurch können sich die Teams zunächst auf jene Risiken konzentrieren, die sie selbst beseitigen können. In Tests auf 90 Hosts reduzierte die automatisierte Erkennung und Behebung mit Red Hat Lightspeed den Zeitaufwand praktischer Administrationsteams im Vergleich zur manuellen Skripterstellung um bis zu 79 % für CVEs und 86 % für bekannte operative Probleme[6].

Diese kontextbezogene Präzision ist heute wichtiger denn je. Die große Menge an neu entdeckten Schwachstellen hat zu einer neuen Form der operativen Lähmung geführt: Alarmermüdung. Wenn Hunderte von CVEs in einem komprimierten Fenster offengelegt werden, kann kein Team sie manuell auswerten. Mit Red Hat Lightspeed lässt sich individuell Unzutreffendes ausblenden, sodass Teams ihre Maßnahmen zur Fehlerbehebung gezielt auf die Ergebnisse konzentrieren können, die erhebliche Auswirkungen auf ihre jeweilige Umgebung haben.

Überprüfung und Kontrolle von Patches mit Red Hat Satellite

Wenn bekannt ist, was zu patchen ist, ist die halbe Arbeit schon erledigt. Um den richtigen Patch zu testen, zu überprüfen, zu genehmigen und in die Produktion zu überführen, ohne dabei neue Instabilitäten zu verursachen, ist ein kontrollierter, wiederholbarer Prozess erforderlich.

Red Hat Satellite bietet Errata-Management On-Premise und Staging von Inhalten in großem Umfang für lokale, hybride und vollständige Air Gap-Infrastrukturen. Satellite erzeugt Inhaltsansichten – verifizierte Software-Snapshots zu einem bestimmten Zeitpunkt – und erstellt sie in verschiedenen, abgetrennten Lifecycle-Umgebungen (von der Entwicklung über die Testphase bis zur Produktion). Patches müssen festgelegte Genehmigungsstufen durchlaufen, bevor sie in die Produktion gelangen, damit sie vor dem Deployment umfassend geprüft werden können.

Satellite trägt auch zum Schutz der Softwarelieferkette bei: In die Umgebung eingehende Pakete sind kryptografisch signiert und stammen aus den verifizierten Repositories von Red Hat. Für Unternehmen, die in stark regulierten oder isolierten Umgebungen tätig sind, bietet Satellite dieselben Funktionen auch in Umgebungen ohne direkten Internetzugang – und ermöglicht so die Kontrolle darüber, welche Software in die Infrastruktur gelangen darf. Die Compliance-Berichterstellung erfolgt automatisiert mithilfe des OpenSCAP-Scan-Frameworks (Open Security Content Automation Protocol). Dabei werden auditfähige Berichte erstellt, die den Anforderungen von CI (Continuous Integration), DISA STIG (Defense Information Systems Agency's Security Technical Implementation Guides) sowie den Baseline-Anforderungen für Entwicklungs-Sandboxes von PCI (Payment Card Industry) entsprechen.

Fehlerbehebung in großem Umfang mit Red Hat Ansible Automation Platform

Sobald Patches geprüft und für die Bereitstellung vorbereitet sind, gilt es schließlich, sie einheitlich in einer komplexen Hybrid-Infrastruktur anzuwenden, die sich über Tausende von Servern, mehrere Cloud-Umgebungen, On-Premise-Rechenzentren und Air Gap-Umgebungen erstreckt. Dabei darf kein manueller Backlog entstehen, der erneut zu einer Verlangsamung führt.

Red Hat Ansible® Automation Platform wendet Fehlerbehebungen in großem Umfang auf den gesamten hybriden Bestand an und sorgt mithilfe von Policy as Code (PaC) für Konsistenz, Auditierbarkeit und Wiederholbarkeit. Event-Driven Ansible (EDA) schließt den Kreislauf durch Automatisierung des Workflows für die Fehlerbehebung: Wenn Satellite eine Repository-Synchronisierung mit einem neuen Sicherheitspatch beendet, sendet ein Webhook automatisch ein Signal an Ansible Automation Platform, um anfällige Systeme zu identifizieren und das Remediation Playbook auszulösen. Hochrisikosysteme können automatisch isoliert werden, noch bevor ein Patch bereitgestellt wird. Dadurch lässt sich das Sicherheitsrisiko während des kritischen Reaktionsfensters begrenzen. Die einzelnen Aktionen werden mithilfe von Red Hat Ansible Certified Content Collections ausgeführt, wodurch ein klarer PaC-Auditpfad gewährleistet ist, der zur Erfüllung der Compliance-Anforderungen ohne zusätzliche Tools beiträgt.

Die Closed-Loop-Lösung von Red Hat zur Fehlerbehebung ist kein Patchwork aus separaten Produkten. Es handelt sich dabei um ein einzelnes integriertes Portfolio, das im Rahmen 1 Subskription bereitgestellt und von 1 Team betreut wird. Für Unternehmen, die bereits Lösungen von Red Hat einsetzen, sind die erforderlichen Tools zur Abwehr von KI-gesteuerten Bedrohungen wahrscheinlich bereits vorhanden. Durch deren Vernetzung verkürzt sich die durchschnittliche MTTR von Wochen manueller Arbeit auf wenige Stunden automatisierter Bearbeitung. Dabei werden umfassende, belegbare Auditnachweise für die verschiedenen Systeme in der Infrastruktur erstellt.

Weitere Informationen zu Red Hat Lightspeed

Sind Sie bereit, die Fehlerbehebung für CVE zu beschleunigen? Erfahren Sie mehr über Red Hat Lightspeed.

Weitere Informationen zu Red Hat Satellite

Weitere Informationen darüber, wie Sie mit Red Hat Satellite das Infrastrukturmanagement in großem Umfang optimieren können, finden Sie auf der Produktseite.

Informationen zu vollständig optimierter Automatisierung

Besuchen Sie die Produktseite, um zu erfahren, wie Sie mit Red Hat Ansible Automation Platform menschliche Fehler in sich wiederholenden Prozessen reduzieren können.

1. CVE-Programm: „Metrics“ CVE: Common Vulnerabilities and Exposures, abgerufen im Juni 2026
2. Red Hat Case Study: „Zoom for Government verbessert die Sicherheit mit einer Plattform von Red Hat“, 10. März 2023
3. Google Cloud Blog: „How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends“, 15. Okt. 2024
4. Google Cloud Blog: „M-Trends 2026: Data, Insights, and Strategies From the Frontlines“, 23. März 2026
5. Edgescan: „2026 Vulnerability Statistics Report“ Edgescan, 2026
6. Principled Technologies, gesponsert von Red Hat. „Sparen Sie Zeit bei der Administration mit den automatisierten Funktionen zur Problembehebung von Red Hat Lightspeed“, Nov. 2025 (überarbeitet)

Über Red Hat

Red Hat, weltweit führender Anbieter von Open Source-Softwarelösungen für Unternehmen, folgt einem communitybasierten Ansatz, um zuverlässige und leistungsstarke Cloud-, Entwicklungs-, KI-, Linux-, Automatisierungs- und Anwendungsplattform-Technologien bereitzustellen. Red Hat unterstützt Kunden bei der Entwicklung cloudnativer Anwendungen, der Integration neuer und bestehender IT-Anwendungen sowie der Automatisierung 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 dabei zu wachsen, sich zu transformieren und sich für die digitale Zukunft zu rüsten.

Nordamerika	1-888-REDHAT1	www.redhat.com	@red-hat
Asien-Pazifik	+65 6490 4200	apac@redhat.com	@redhat
Lateinamerika	+54 11 4329 7300	info-latam@redhat.com	@redhat
Europa, Naher Osten und Afrika	00800 7334 2835	europe@redhat.com	@red_hat