Unterbrechungsfreie Netzwerksicherheit im Rechenzentrum in Echtzeit

Mit Schwachstellen in kritischen Rechenzentrumsinfrastrukturen verbundene Kosten

Rechenzentren, die KI-Back-End- und -Inferenzsysteme unterstützen, sind für moderne Geschäftsprozesse unverzichtbar. Dass sie so wichtig sind, erhöht jedoch auch das Risiko. Eine nicht gepatchte CVE-Schwachstelle oder ein Zero-Day-Angriff kann zu finanziellen Verlusten, Reputationsschäden und Serviceunterbrechungen führen.

In der heutigen Bedrohungslandschaft ist diese „Patch-Lücke“ ein kritisches Problem. Während die Angreifer nur wenige Stunden benötigen, um eine CVE-Schwachstelle auszunutzen, dauert es oft Wochen oder gar Monate, bis die Verteidiger Patches in allen Produktionsumgebungen getestet und implementiert haben.

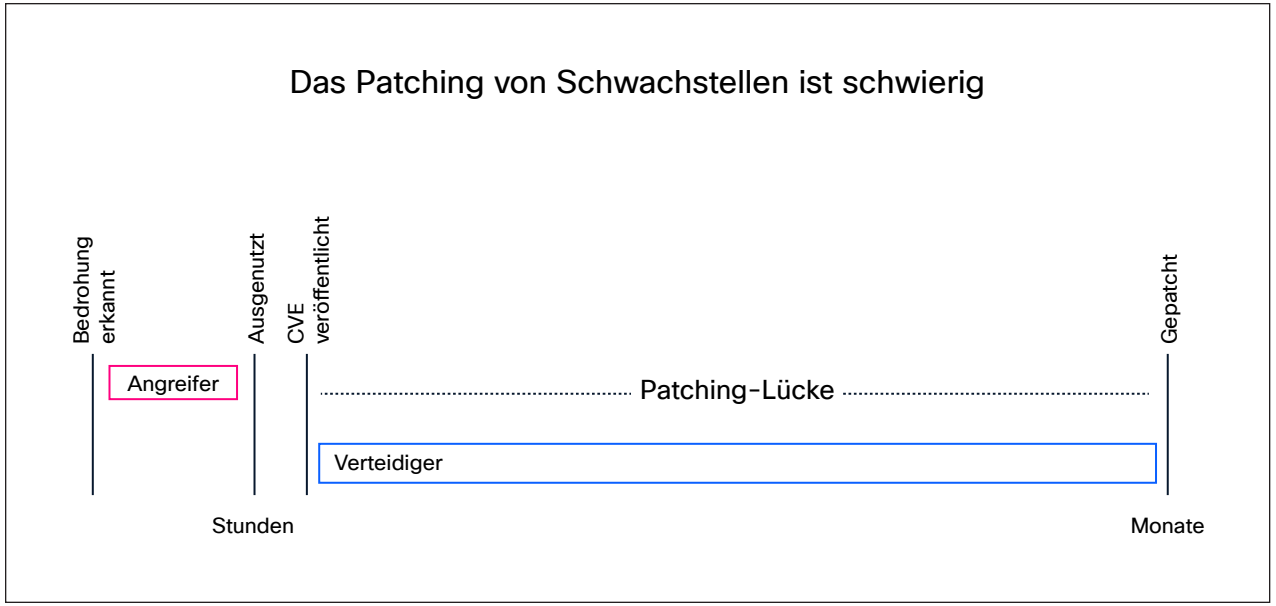

Abbildung 1: Das Patching von Schwachstellen ist eine Herausforderung

Cisco® Live Protect setzt neue Maßstäbe, indem es Cisco Nexus® Switches sofort abschirmt. So können Sie Angriffe aufhalten, ohne Ihr Netzwerk lahmzulegen. Die Wartung der Rechenzentrumsinfrastruktur erfordert konsistente Sicherheit und zuverlässige Verfügbarkeit. Herkömmliches CVE-Patching führt häufig zu Störungen und Ausfallzeiten. Cisco Live Protect für Switches der N9000-Serie bietet Echtzeit-Schutzschilde, um Schwachstellen sofort beheben und so kontinuierlichen Schutz und Stabilität gewährleisten zu können – ohne Wartungsarbeiten oder dringende Upgrades im Ernstfall.

Vorteile von Cisco Live Protect

Herkömmliches Patching erfordert Wartungsfenster, Neustarts und potenzielle Ausfallzeit. Cisco Live Protect bietet einen revolutionären Ansatz für die Sicherheit:

- **Keine Ausfallzeit:** Anwendung von Sicherheitsrichtlinien auf Live-Systeme ohne Switch-Neustart
- **Sofortiger Schutz:** Abschirmung von Schwachstellen, sobald eine Bedrohung erkannt wurde – lange bevor ein standardmäßiges PSIRT-Upgrade geplant ist
- **Kontinuierliche erneute Validierung:** Zuverlässige Sicherheit durch eBPF-gestützte Observability
- **Betriebliche Effizienz:** Entfernung der Sicherheits-SMUs (Schilde), sobald ein vollständiges PSIRT-Paket-Upgrade angewendet wurde

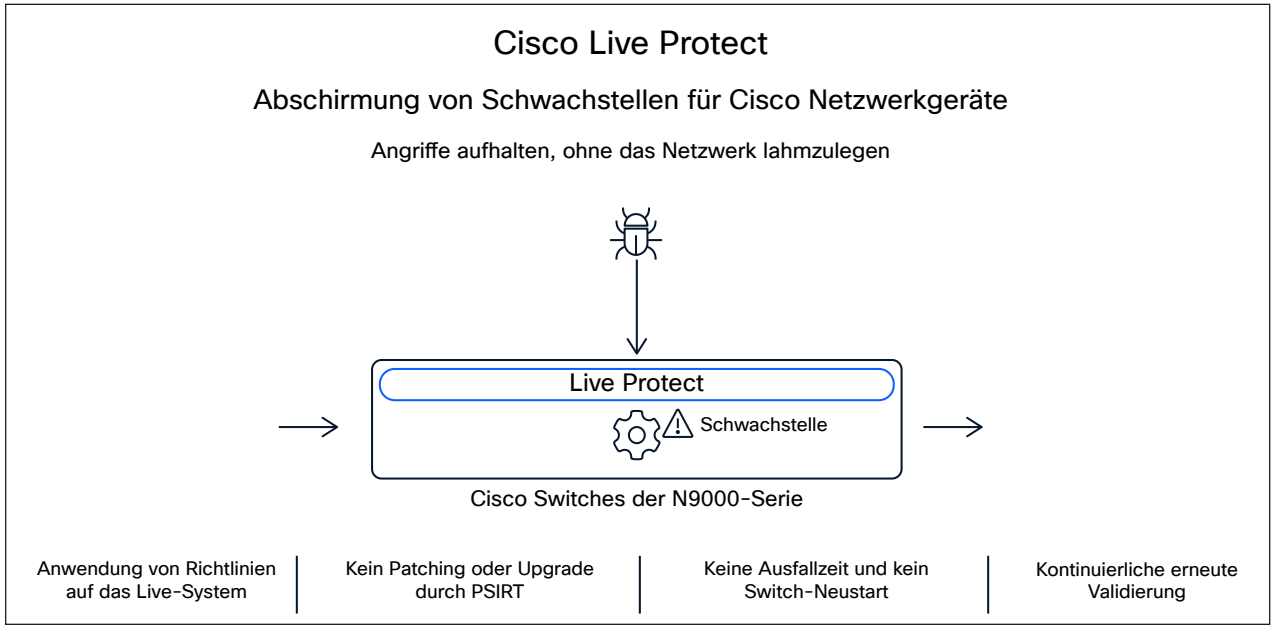

Abbildung 2: Live Protect

Innovation auf der Basis von eBPF

Cisco bringt als erster Anbieter einen Tetragon-Agent der Enterprise-Klasse auf den Markt. Dieser ist direkt in Cisco NX-OS ab Version 10.6(1) F integriert. Mithilfe von eBPF (Extended Berkeley Packet Filter) bietet Live Protect umfassende Sichtbarkeit und Durchsetzung auf Kernel-Ebene für folgende Zwecke:

- Verhinderung einer Rechteausweitung
- Schutz auf Kontrollebene
- API- und CLI-Sicherheit
- Datei-E/A-Überwachung

Unterstützte Plattformen

Live Protect ist für Nexus-Kunden mit einer **Essentials-Lizenz oder einer höheren Lizenz** verfügbar.

Plattformunterstützung (Cisco NX-OS 10.6(2)F):

- Cisco N9300- und N9200-Plattformen mit fester Konfiguration (ab 24 GB RAM)
- Cisco Smart Switches der N9300-Serie
- Cisco Switches der N9400-Serie

Funktionsweise

Cisco Live Protect bietet auf der Grundlage fortschrittlicher eBPF-Technologie Echtzeitsicherheit für Netzwerkgeräte in Rechenzentren.
Die Konfiguration ist flexibel und ermöglicht das Management auf einzelnen Geräten per Cisco NX-OS-CLI oder -API und damit eine vollständige Automatisierung in der gesamten Rechenzentrums-Fabric über CI/CD-Pipelines. Das Nexus Dashboard sorgt für zentrale Orchestrierung und bietet sofortige Einblicke in von CVE-Schwachstellen betroffene Geräte. Außerdem automatisiert es die Bereitstellung von Sicherheitsschilden und ermöglicht die kontinuierliche Überwachung der Effektivität dieser Schilde.

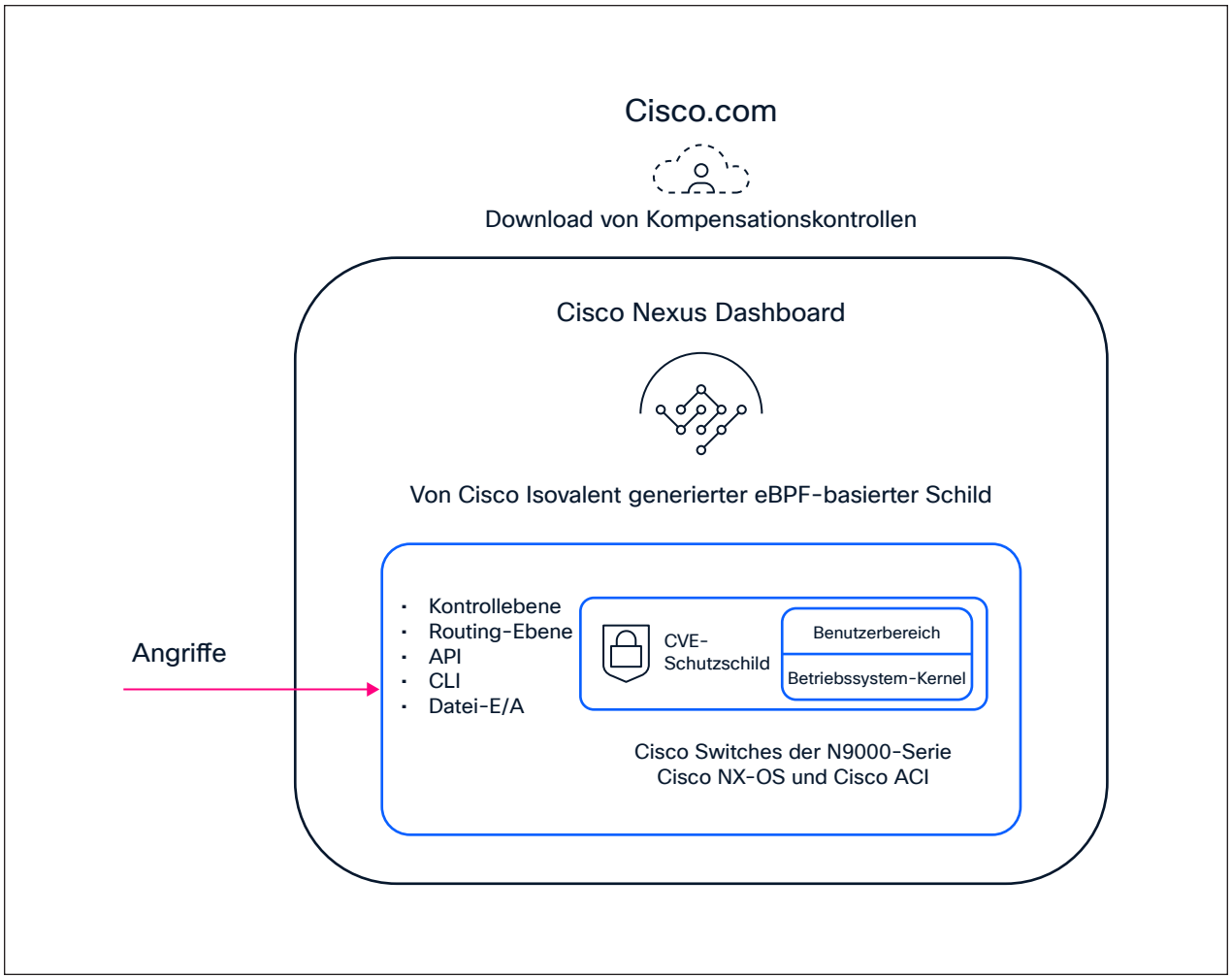

Abbildung 3: Live Protect und CVE-Schwachstellenbehebung für Cisco Switches der N9000-Serie

Bestandteile

- **Cisco Live Protect:** Schutz für Netzwerkgeräte auf Kernel-Ebene mithilfe von eBPF-Technologie
- **Tetragon-Agent** Zusammenstellung von CVE-Kompensationskontrollen zu bereitstellbaren eBPF-Richtlinien
- **Nexus Dashboard:** zentrale Konsole für Orchestrierung, Transparenz und Monitoring über alle Cisco Nexus Switches hinweg
- **Integrationstools:** APIs, CLI und CI/CD-Pipeline-Unterstützung für nahtlose Automatisierung und Verwaltung

Live Protect ermöglicht optimierte Upgrades und eine kontinuierliche Schwachstellenbehebung in Cisco NX-OS- und Cisco ACI®-Umgebungen, sodass die Sicherheit und Performance des Infrastruktur-Cores zuverlässig im gesamten System erhalten bleiben.

Mehr erfahren

Schützen Sie Ihr Rechenzentrum mit Cisco Live Protect für automatisierte Sicherheit in Echtzeit ohne Ausfallzeiten.

Mehr dazu erfahren Sie in unserem Cisco Live Protect-Blog. Sie können sich auch an Ihre Kontaktperson bei Cisco wenden.

Ressourcen

Cisco Live Protect-Webseite

Cisco Live Protect in Aktion – mit Video

Versionshinweise zu Cisco NX-OS

Anwendungsfälle

Branche	Die gängigsten Anwendungsfälle für Cisco Nexus und Live Protect
Finanzdienstleistungen	· CVE-Schwachstellenbehebung in Echtzeit · Schutz vor Zero-Day-Angriffen · Minimierung der Ausfallzeit bei kritischen Anwendungen · Verbesserte Compliance und Audit-Bereitschaft
Gesundheitswesen	· Schutz sensibler Patientendaten · CVE-Schwachstellenbehebung in Echtzeit · Kontinuierliche Verfügbarkeit von Systemen im Gesundheitswesen · Compliance (z. B. HIPAA)
Einzelhandel und E-Commerce	· Sicherheit von Zahlungs- und Kundendaten · Minimierung von Ausfallzeiten in Hochphasen · Schutz vor CVE-Schwachstellen und Zero-Day-Bedrohungen in Echtzeit · Compliance mit PCI DSS
Behörden und öffentlicher Sektor	· Zentralisierung der Sicherheitsorchestrierung · Reaktion auf Zero-Day-Bedrohungen · Einhaltung gesetzlicher Bestimmungen · Schutz vertraulicher Informationen und zuverlässige Verfügbarkeit öffentlicher Services
Telekommunikations- und Service-Provider	· Abwehr komplexer Bedrohungen (z. B. DDoS) · Netzwerkperformance ohne Unterbrechungen · Automatisierung von Sicherheitsverfahren · Zentralisierung des Richtlinienmanagements
Energie- und Versorgungsunternehmen	· Schutz kritischer Kontrollsysteme · Schutz vor CVE-Schwachstellen und Zero-Day-Bedrohungen · Einhaltung gesetzlicher Bestimmungen · Widerstandsfähigkeit und Verfügbarkeit
Bildung und Forschung	· Schutz geistigen Eigentums und vertraulicher Daten · Kontinuierlicher Zugriff auf digitale Ressourcen · Reaktion auf Bedrohungen in Echtzeit · Automatisierung von Sicherheitsverfahren
Fertigung	· Sichere OT- und IT-Umgebungen · Behebung von Schwachstellen in Echtzeit · Schutz geistigen Eigentums · Absicherung des unterbrechungsfreien Betriebs

C22-5771857-00 02/26