Verbesserung der Cyber-Compliance mit Infrastrukturautomatisierung

Überwachen Sie Events in mehreren Behörden. Automatisieren Sie die Reaktion mit behördenspezifischen Playbooks.

Lösungen von Red Hat

Red Hat Integration verbindet Daten von den Netzwerkgeräten, Servern und Edge-Geräten mehrerer Behörden miteinander.

Mit Open Data Hub auf Red Hat OpenShift können Sie Machine Learning-Modelle trainieren, sodass sie bösartige Muster erkennen.

Red Hat Decision Manager ordnet Sicherheitsevents Reaktionen entsprechend den Regeln der jeweiligen Behörde zu.

Red Hat Ansible Automation Platform löst entsprechend dem Behörden-Playbook automatisch die Aktion der Behörde aus, wenn eine Bedrohung erkannt wird.

Malware setzt sich über Abteilungsgrenzen hinweg

Die Vollzugsbehörden der Bundesregierung müssen sensible Daten schützen. Zu diesen Daten zählen unter anderem Strafregister und Ermittlungen, biometrische Daten, Steuererklärungen, Aufzeichnungen von Überwachungskameras und persönliche Unterlagen. Die Offenlegung sensibler Daten kann Abläufe stören, das Personal bedrohen und das Vertrauen in die Regierung schmälern. Häufige Attacken sind unter anderem die Datenexfiltration und DoS (Denial of Service).

Bei der Cyber-Compliance im Gesetzesvollzug treten folgende Hindernisse auf:

- **Begrenzte Personalkapazitäten:** Die Sicherheitsteams der Behörden haben nicht die Ressourcen, um ein zunehmendes Volumen an Traffic zu überwachen, wozu auch Streams von Edge-Geräten wie IP-Kameras zählen, die Malware übertragen können. Wenn Bedrohungen zu langsam erkannt und behoben werden, führt dies dazu, dass Behörden länger verwundbar sind.
- **Fehlende zentrale, behördenübergreifende Überwachung:** Attacken, die auf mehrere Behörden abzielen, sind oft raffinierter und bringen ein höheres Risiko für große Geschäftsausfälle und Datenverlust mit sich. Wenn sich Behörden nicht bewusst sind, dass ein Sicherheitsevent Teil einer behördenübergreifenden Attacke ist, unterschätzen sie womöglich dessen Ausmaß.
- **Die Problembehebung darf die Abläufe nicht unterbrechen:** Vollzugsbehörden können oftmals ein betroffenes Gerät nicht abschalten, ohne dabei die Abläufe zu unterbrechen. Sie benötigen eine verfeinerte Fehlerbehebung, die an den Schweregrad der Bedrohung angepasst ist.

Lösung: Ganzheitliche Betrachtung von und automatisierte Reaktion auf Netzwerkevents

Für den Schutz öffentlicher Daten sind zwei Voraussetzungen erforderlich, die Vollzugsbehörden heutzutage nicht erfüllen. Die erste ist eine ganzheitliche Betrachtung der Netzwerk- und Serveraktivität über mehrere Behörden hinweg. Die andere ist eine automatisierte Fehlerbehebung, die auf der Art der Bedrohung und dem Playbook der Behörde basiert. Beispiele hierfür sind die Durchsetzung der gleichen Liste blockierter Netzwerkadressen in mehreren Behörden, das Versenden von Warnmeldungen, wenn diese Adressen erkannt werden, das Verschieben einer verdächtigen Workload in Quarantäne, bis sie untersucht werden kann, das Abschalten eines virtuellen Servers, der ungewöhnliches Verhalten zeigt und das Starten eines neuen virtuellen Servers von einer vertrauenswürdigen Quelle.

Folgende Vorteile bietet die automatisierte Cyber-Compliance im Gesetzesvollzug:

- Schnellere Erkennung von Vorfällen.
- Beschleunigte Fehlerbehebung, wodurch die Schwachstelle schneller geschlossen werden kann.
- Reduzierte Ressourcenanforderungen für die Bedrohungsminderung.
- Erhöhte Jobzufriedenheit, da Cybersicherheitsprofis sich nicht mehr mit banalen Überwachungsaufgaben befassen müssen, sondern sich auf wichtigere Arbeiten konzentrieren können. Dies ist ein Wettbewerbsvorteil, was die Suche nach und Bindung von Mitarbeitenden angeht.

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

Warum Red Hat?

Verbesserte Sicherheit: Unsere Lösungen erfüllen strenge Sicherheitsanforderungen der Bundesregierung.

Partnernetzwerk: Arbeiten Sie mit unseren Partnern zusammen, um Lösungen für Dateninterrogation und automatisierte Problemlösung zu verknüpfen.

Bewährt bei Bundesregierungen: Das US-Ministerium für Innere Sicherheit, das US-Verteidigungsministerium und andere zivile Behörden verwenden Red Hat OpenShift.

Flexibilität durch offene APIs: Wenn Sie neue Geräte hinzufügen, können Sie diese mithilfe von offenen APIs gemeinsam mit bestehenden Geräten überwachen.

Niedrigere Kosten: Unsere Subskriptionen sind oft günstiger als proprietäre Softwarelizenzen und Supportverträge.

Der Ansatz von Red Hat für automatisierte Cyber-Compliance

Wir bieten eine umfassende Lösung, die Cyber-Compliance mithilfe von Infrastrukturautomatisierung stärkt.

Trainieren Sie ein Machine Learning-Modell, sodass es zwischen normaler und ungewöhnlicher Aktivität unterscheiden kann. Verwenden Sie die KI-Plattform Open Data Hub auf Red Hat® OpenShift®. Testen Sie das Modell, indem Sie Bedrohungen simulieren. Passen Sie das Modell kontinuierlich an, indem Sie Daten über neu entdeckte Bedrohungen und die Effektivität der Reaktion an es weitergeben.

Ordnen Sie verschiedene Bedrohungsarten der Fehlerbehebung zu. Mit Red Hat Decision Manager können Sie Reaktionen festlegen, wie etwas das Blockieren der IP-Adresse eines Angreifers, das Whitelisting von nicht bedrohlichem Traffic, das Verschieben einer verdächtigen Workload in Quarantäne, das Abschalten eines infizierten virtuellen Servers und das Starten eines neuen.

Automatisieren Sie die Überwachung und Reaktion über mehrere Behörden hinweg. Verwenden Sie Red Hat Ansible® Automation Platform, um Protokolle von den Firewalls, IDS, Edge-Geräten und Partnerprodukten mehrerer Behörden, wie Sensu für Log Aggregation oder ServiceNow für das operative Fallmanagement zu sammeln. Ansible Automation Platform führt automatisch die im Playbook festgelegte Aktion durch. Falls die Aktion das Problem nicht behebt, sendet Ansible Automation Platform eine Warnung und erstellt ein Ticket in ServiceNow.

Geben Sie Behörden die Kontrolle über ihre eigenen Playbooks. Die einzelnen Behörden wissen genau, wie viel Risiko sie aushalten können, bevor sie einen bestimmten Service abschalten müssen. Mit Ansible Automation Platform können behördliche Cybersicherheits-Teams eine Webschnittstelle verwenden, um Schwellenwerte, Hostnamen und Playbooks an die erforderlichen Anforderungen anzupassen.

Mehr erfahren. Besuchen Sie redhat.com/government, um mehr darüber zu erfahren, wie Red Hat die Innovation der behördlichen IT vorantreibt.

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 Integration neuer und bestehender IT-Anwendungen, der Entwicklung cloudnativer Applikationen, der Standardisierung auf unserem branchenführenden Betriebssystem sowie der Automatisierung, Sicherung und Verwaltung komplexer Umgebungen. Dank der vielfach ausgezeichneten Support-, Trainings- und Consulting-Services ist Red Hat ein bewährter Partner der Fortune 500-Unternehmen. Als strategischer Partner von Cloud-Providern, Systemintegratoren, Applikationsanbietern, Kunden und Open Source Communities unterstützt Red Hat Unternehmen auf ihrem Weg in die digitale Zukunft.

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

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

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

de.redhat.com
#F26748_0121

Copyright © 2021 Red Hat, Inc. Red Hat, OpenShift, Ansible und das Red Hat Logo sind Marken oder eingetragene Marken von Red Hat, Inc. oder dessen Tochterunternehmen in den USA und anderen Ländern. Linux® ist eine in den USA und anderen Ländern eingetragene Marke von Linus Torvalds.