Security Spotlight:
Die Kosten menschlicher Fehler und die Vorteile der Automatisierung

Warum Regierungsbehörden manuelle Ansätze beim Sicherheitsmanagement überdenken, und wie mit intelligenter Automatisierung potenzielle Bedrohungen durch kostspielige Sicherheitslücken verhindert werden können

Weiter

Inhaltsverzeichnis:

01 Einleitung: Die wachsende Bedrohung durch Cyberkriminalität

Cyberkriminalität nimmt zu. Die Zahl der Cyberangriffe hat im Jahr 2021 um 15,5 % zugenommen, und die Zahl der Vertragsverletzungen ist um 24,5 % angestiegen.[1] Dennoch äußern 34 % der Organisationen im öffentlichen Sektor, dass sie nicht gut auf die schnelle Veränderung der Bedrohungslage vorbereitet sind.[1]

Während Regierungsbehörden neue Technologien einführen und sich an hybride Arbeitsmodelle anpassen, arbeiten auch Cyberkriminelle an ihren Fähigkeiten. Personal und Computing-Ressourcen befinden sich zunehmend an verschiedenen Standorten, und die sich rasant ändernde Landschaft der IT-Infrastruktur bietet Angreifern neue Möglichkeiten, Sicherheitslücken und -schwachstellen auszunutzen. All dies sorgt dafür, dass die organisatorischen Kosten durch Datenpannen anwachsen. Selbst eine Organisation, die einen starken Sicherheitsstatus aufweist, ist in dieser Umgebung mehr Risiken ausgesetzt.

Proaktive Sicherheit gegen Cyberkriminelle

Während Cyberkriminelle neue Methoden erfinden, um in geschützte Systeme und Daten einzudringen, lastet auf Organisationen der interne und externe Druck, einen strategischeren und proaktiveren Schutz vor Cyberangriffen zu entwickeln. Hinzu kommt, dass ihre Datensicherheit und -schutzmaßnahmen mit umfassenderen Regeln und Richtlinien konform sein müssen.

Und dieser Trend hin zu vermehrten Sicherheitsrichtlinien findet standort- und branchenübergreifend statt. Beispielsweise beinhaltet die DSGVO (Datenschutz-Grundverordnung) der Europäischen Union strenge Regeln, die festlegen, wie persönliche Daten gesammelt, verwendet und geschützt werden sollen. Die Cybersicherheitsverordnung von Singapur bildet ein Framework, in dem Besitzer wichtiger Informationsinfrastrukturen spezifische Best Practices für Governance, Zugangskontrolle, Vorfallserkennung und -reaktion sowie für andere Bereiche erfüllen müssen. Das Dirección Nacional de Ciberseguridad von Argentinien veröffentlicht ebenfalls nationale Richtlinien für den Schutz wichtiger Informationsinfrastrukturen und die Verbesserung von Prävention, Erkennung, Reaktion und Behebung von Sicherheitsvorfällen. Und Behörden in den Vereinigten Staaten müssen bis Ende 2024 auf Zero Trust-Architekturen umstellen, um die Cybersicherheitsziele der Regierung zu erreichen.

Stärken Sie Ihre Sicherheitsmaßnahmen

Organisationen, die ihre Cybersicherheit verbessern wollen, sollten zuerst bestehende Schwachstellen identifizieren. Oftmals können menschliches Versagen und ein mangelndes Bewusstsein die Sicherheit beeinträchtigen, auch wenn bereits umfassende Strategien entwickelt wurden. Wenn solche kleinen Fehler nicht behoben werden, können sie Ihre Systeme gefährden und ein bereits komplexes Problem noch verschlimmern. Aus diesem Grund verwenden Organisationen Automatisierung in ihrer Sicherheitsstrategie, um die Zuverlässigkeit zu erhöhen und Risiken zu mindern.

In diesem E-Book zeigen wir Ihnen, wie sich Risiken, die durch menschliche Fehler verursacht wurden, auf den Kampf gegen die Cyberkriminalität auswirken. Weiterhin besprechen wir, wie die Automatisierung von wichtigen Cybersicherheitsstrategien zur Risikominderung Ihre Sicherheit verbessern und gleichzeitig das Volumen zeitraubender Aufgaben für Ihr IT-Team verringern kann.

Die globalen Kosten von Cyberkriminalität

24,5 %

Zunahme der Vertragsverletzungen im Jahr 2021[1]

4,35 Milliarden USD

Globale Durchschnittskosten einer Datenpanne[2]

60 %

Anteil der Organisationen, die aufgrund einer Datenpanne die Preise für ihre Services oder Produkte anheben mussten[2]

1. ThoughtLab. „Cybersecurity Solutions for a Riskier World.“ 2022
2. IBM. „Cost of a Data Breach Report 2022.“ Juli 2022.

02 Effektive Sicherheitsstrategien sollten alle etwas angehen

Menschen machen Fehler

Selbst innerhalb von IT-Teams unterschätzen oder missverstehen Beschäftigte oft die Schwachstellen ihrer Systeme und die daraus resultierenden Sicherheitsrisiken. Unsere Unfähigkeit, Risiken korrekt einzuschätzen, kann Organisationen sehr viel Geld kosten.

Stellen Sie sich folgendes Beispiel vor: In einer Firewall findet ein Produktionsausfall statt, weshalb ein Firewall-Engineer eine Richtlinie manuell und unter extremem Druck aktualisieren muss. Durch die Aktualisierung wird der Ausfall behoben, jedoch wird dadurch auch ein neuer Angriffsvektor hinzugefügt, der von Cyberkriminellen ausgenutzt werden kann.

In diesem Szenario könnte eine manuelle, überstürzte Konfigurationsänderung in der Firewall mehrere negative Konsequenzen haben. Dazu zählen Datenpannen, die Verletzung von Branchen- und Regierungsrichtlinien zum Datenschutz, Serviceunterbrechungen sowie Systemausfälle, die alle auf die Organisation zurückfallen.

Angefangen beim Patchen von Anwendungen und dem Aktualisieren von Firewalls bis hin zum Festlegen und Durchsetzen administrativer Berechtigungen können viele Elemente der Sicherheitsstrategie fehlschlagen, wenn sie manuell durchgeführt werden. Und da Cyberkriminelle immer besser darin werden, Schwachstellen zu erkennen und auszunutzen, kann es negative oder sogar nicht korrigierbare Konsequenzen nach sich ziehen, wenn Sie sich bei diesen Aufgaben allein auf manuelle Abläufe verlassen.

Fachkräftemangel kann Sicherheitslücken vergrößern

Cybersicherheits-Fähigkeiten sind Mangelware, was die Wahrscheinlichkeit für menschliche Fehler bei manuellen Aufgaben erhöht. Es gibt schlicht und einfach nicht genügend Leute, die die Ausbildung und Fähigkeiten haben, um Sicherheitsrisiken zu erkennen und zu beheben. Laut der (ISC)[2] Cybersecurity Workforce Studie werden 2,72 Millionen weitere IT-Sicherheitskräfte benötigt, um die weltweite Cybersicherheits-Lücke zu schließen.[3]

Dieser chronische Mangel an Cybersicherheits-Fachkräften erschwert Organisationen ein angemessenes Risikomanagement. IT-Teams sind bereits überarbeitet und haben weder Zeit, Sicherheitsprozesse zu entwickeln, noch diese im gesamten Unternehmen durchzusetzen.

Automatisierung für Sicherheitsteams

Zu erkennen, dass sowohl manuelle Sicherheitsprozesse als auch der Fachkräftemangel die Risiken für Organisationen erhöhen, ist für den Kampf gegen Cyberkriminalität unerlässlich, und Automatisierungslösungen bieten eine vielversprechende Lösung. Nachfolgend zeigen wir, wie die Automatisierung von Sicherheitsprozessen in der gesamten Organisation für dringend benötigte Konsistenz, Genauigkeit und Skalierbarkeit sorgt.

Das Risiko manueller Sicherheitsmaßnahmen

„Organisationen mit vollständig bereitgestellter Sicherheits-KI und -Automatisierung konnten eine Sicherheitsverletzung sehr viel schneller entdecken und beseitigen als Organisationen, die keine Sicherheits-KI und -Automatisierung bereitgestellt hatten.“ [4]

3. (ISC)[2] Cybersecurity Workforce Studie. „A Resilient Cybersecurity Profession Charts the Path Forward.“ 2021.
4. IBM. „Cost of a Data Breach Report 2022.“ Juli 2022.

03 Häufige Herausforderungen beim Risikomanagement

Behörden brauchen ein besseres Risikomanagement

Um die Vertraulichkeit, Integrität und Verfügbarkeit von offiziellen Informationen sicherzustellen, müssen Behörden in der Lage sein, Risiken korrekt und effizient zu identifizieren und zu mindern. Sicherheitsbedrohungen verändern sich fortgehend, weshalb Risikoprofil und Sicherheitsstatus einer Organisation flexibel bleiben sollten. Um auf diese Veränderungen schnell reagieren zu können, ist es äußerst wichtig, Abläufe zu automatisieren.

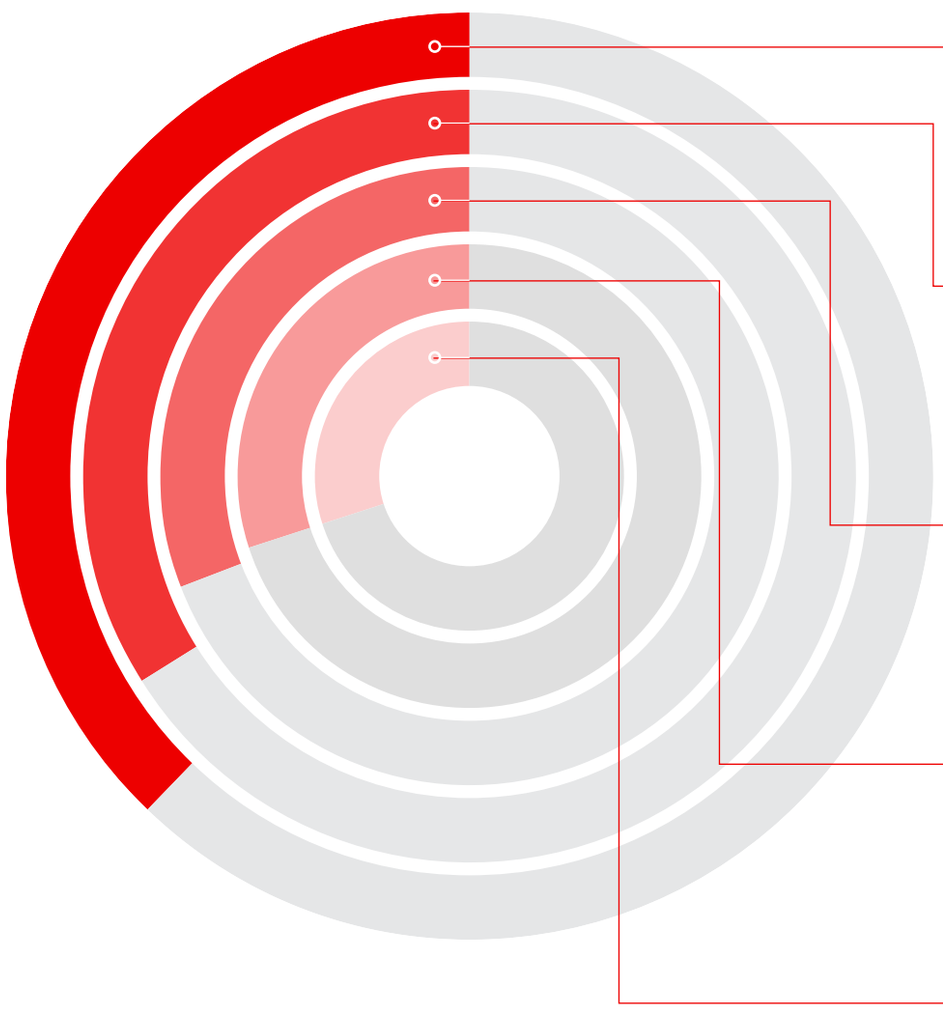
Hindernisse bei der Veränderung von Sicherheitspraktiken

In ihrem Vorhaben, die Sicherheit zu verbessern, stehen Behörden vor mehreren Herausforderungen, die vor allem mit dem Umgang mit Veränderung zu tun haben. Häufige Fragen sind unter anderem:

- Wie skalieren wir unser Team, um eine neue Cybersicherheitsinitiative zu implementieren?
- Wie unterstützen wir verschiedene Teile der Organisation, um sicherzustellen, dass neue Sicherheitsprotokolle befolgt werden?
- Was können wir tun, um unsere bestehenden Systeme, die wichtige Services bereitstellen, besser zu schützen, und wie können wir gleichzeitig die modernen Sicherheitsstrategien einführen, die die Organisation braucht?
- Können wir Strategien wie Zero Trust in bestehende Architekturen einführen?

Anstatt diese Überlegungen als eine Bürde zu sehen, können Organisationen die sich wandelnde Sicherheitslandschaft als eine gute Möglichkeit betrachten, um ihre Sicherheitspraktiken neu zu bewerten und strengere Protokolle zu implementieren.

Häufige Herausforderungen in der Cybersicherheit



38%

Schritt halten mit sich schnell wandelnden Bedrohungen[5]

34%

Aufklärung über Risiko und Verhalten[5]

31%

Verstärkung des internen Cybersicherheitsstatus[5]

30%

Bedarf an Cybersicherheitstraining[5]

30%

Rechtliche/finanzielle Konsequenzen von Datenpannen[5]

5. „State of the Channel 2021.“ CompTIA, Aug. 2021.

04 Mit Automatisierung Ihre Sicherheitslage verbessern

Häufige Themen bei Sicherheitsrichtlinien

Datensicherheit, Zugangskontrolle und das Erkennen von, Reagieren auf sowie der Schutz vor Vorfällen sind branchen- und standortübergreifend häufige Themen in Cybersicherheits-Richtlinien und -Initiativen. Manche dieser Richtlinien enthalten Details zur Implementierung, andere wiederum machen Vorgaben und verlangen bestimmte Ergebnisse. Das führt dazu, dass Organisationen herausfinden müssen, wie sie diese Richtlinien mit ihrer aktuellen Lage, Personalsituation und Infrastruktur am besten einhalten können.

Sicherheitsautomatisierung kann Regierungsbehörden und Organisationen bei der Einhaltung von Richtlinien und dem Kampf gegen Cyberkriminalität unterstützen. Indem sie wiederholbare Alltagsarbeit automatisieren, können sich ihre Cybersicherheits-Team auf wichtigere, strategische Aufgaben konzentrieren. Zusätzlich verhindert Automatisierung eine Überlastung der IT-Teams durch zu viele Aufgaben, die zu einer höheren Wahrscheinlichkeit für menschliche Fehler und einem erhöhten Sicherheitsrisiko führen kann.

Sicherheitsautomatisierung verbindet Teams

Sicherheitsautomatisierung besteht aus einer Vielzahl an Praktiken, die Teams und Domains in Ihrer Organisation verbindet und es ihnen ermöglicht, Risiken wirksamer zu managen, sich gegen Cyberbedrohungen zu wehren und Vorfälle zu mindern. Beispielsweise können Sicherheitsanalysten die Automatisierung für ihren Vorfalls- und Fehlerbehebungsprozess nutzen. IT-Operations-Teams können automatisch Systeme patchen und Compliance durchsetzen. Netzwerkadministrierende können Netzwerkzugangskontrollen einrichten und verwalten.

Sicherheitsautomatisierung hilft Ihren IT- und Sicherheitsteams auch dabei, effektiver mit anderen Bereichen Ihrer Organisation zusammenzuarbeiten, die von Sicherheitsrichtlinien betroffen sind. Dazu zählen unter anderem die Rechts- und Personalabteilung sowie der Kundendienst. Die meisten Organisationen müssen beispielsweise ihre Sicherheitskontrollen verifizieren und Cybervorfälle melden, um rechtliche Vorgaben zu erfüllen. Behördliche Auditoren benötigen Nachweise für die Einhaltung der Compliance, interagieren aber möglicherweise nicht direkt mit den Sicherheitssystemen einer Organisation. Externe Logging-Systeme können in die Sicherheitsautomatisierung integriert werden, und Aktionen können aufgezeichnet werden, um die Berichte und Nachweise zu erstellen, die bei Audits verlangt werden.

Risikoverwaltung mit Automatisierung

Die Automatisierung wichtiger Prozesse innerhalb Ihrer Organisation kann Ihren aktiven und passiven Sicherheitsstatus stärken. In den folgenden Abschnitten stellen wir Ihnen mehrere Bereiche vor, in denen Sicherheitsautomatisierung Sie unabhängig von Ihrem Standort bei der Einhaltung von Regulationen unterstützen und Ihrer Organisation einen realen Mehrwert bieten kann.

Reaktion auf Sicherheitsvorfälle und Problembehebung

Im Jahr 2022 dauerte es im Durchschnitt 277 Tage, bis eine Datenpanne identifiziert und behoben wurde.[6] Werden Datenpannen innerhalb von 200 oder weniger Tagen entdeckt und behoben, kann dies die durchschnittlichen daraus entstandenen Kosten um 26,5 % senken[6] Dennoch kann es kompliziert, zeitaufwendig und fehleranfällig sein, einen Sicherheitsvorfall manuell auf mehreren Plattformen, Tools und Umgebungen zu entdecken und zu beheben.

Bei der Reaktion auf Sicherheitsvorfälle geht es um schnelles Handeln, um die Ausweitung einer Verletzung zu verhindern. Wenn eine Verletzung entdeckt wird, muss das Sicherheitsteam schnell und in großem Umfang reagieren, um den Schaden einzudämmen. Die Reaktion auf Sicherheitsvorfälle umfasst jedoch häufig eine Vielzahl manueller Aufgaben, die in unverbundenen Systemen durchgeführt werden. Dadurch wird die Problembehebung verlangsamt, und Ihr Unternehmen bleibt den Sicherheitsrisiken längere Zeit ausgesetzt.

Indem Sie die Fehlerbehebung in wiederholbare, vorgefertigte Playbooks kodifizieren, kann die Sicherheitsautomatisierung Sie dabei unterstützen, schneller auf Vorfälle zu reagieren. Sie können Aufgaben wie das Blockieren von Angreifer-IP-Adressen oder -Domains beschleunigen und gleichzeitig sicheren Datenverkehr zulassen, gefährdete Zugangsdaten einfrieren und verdächtige Workloads zur weiteren Untersuchung isolieren, um den Schaden des Vorfalls zu minimieren.

Patching und System-Updates

Um Angriffen vorzubeugen, empfehlen viele Cybersicherheits-Standards ein regelmäßiges Patchen und Aktualisieren von Systemen und Anwendungen. Allerdings besteht beim manuellen Patchen und Aktualisieren immer die Gefahr menschlicher Fehler, und insbesondere in großen Organisationen kann dieser Prozess zudem sehr zeitaufwendig sein.

Patching ist ein guter Use Case für automatisierte Workflows. Anstatt sich auf manuelle Tests, Kontrollen und Patch-Deployment zu verlassen, können Organisationen die Verifizierung und Bewertung automatisieren. Dadurch stellen sie sicher, dass diese Schritte nahtlos, effizient und mit den korrekten Sicherheitsvorkehrungen ablaufen.

Management von Zugangsdaten und Berechtigungen

Gestohlene oder gefährdete Zugangsdaten sind der häufigste Auslöser von Datenpannen.[6] Wenn Sie Privileged Access zentralisieren und kontrollieren, können Sie Ihr Risiko mindern und Sicherheits- und Datenschutzvorschriften einhalten.

Verwenden Sie das Least Privilege-Prinzip, um Nutzenden nur die Zugriffsberechtigungen zu geben, die sie auch tatsächlich benötigen. Obwohl Sie die aktuellen Zugangsrechte für Nutzende überprüfen und neu bewerten müssen, hilft Ihnen diese Vorgehensweise dabei, die Auswirkungen gestohlener oder beschädigter Zugangsdaten zu minimieren.

Eine zentrale Aufbewahrung von Zugangsdaten macht die direkte und anfällige Eingabe in Anwendungen überflüssig. Durch die Automatisierung der PAM-Workflows (Privileged Access Management) wird der Prozess einfacher, zuverlässiger und konsistenter. Sie ist außerdem die Basis für Zero Trust-Architekturen und -Ansätze.

Compliance und Durchsetzen von Richtlinien

Fehlkonfigurationen waren der Hauptauslöser für 44 % der größten Sicherheitsverletzungen in Organisationen.[7] Falsch konfigurierte Systeme können für Angriffe anfälliger sein. Und falls Organisationen keine strengen Änderungskontrollen durchführen, können Systeme, die zum Zeitpunkt der Provisionierung korrekt konfiguriert wurden, im Laufe der Zeit auch anfällig werden.

Indem Sie Richtlinien über den gesamten Lifecycle Ihrer Systeme und Anwendungen durchsetzen, können Sie sicherstellen, dass diese zu Beginn korrekt konfiguriert sind und im Laufe der Zeit diese Konfiguration auch beibehalten. Mit Automatisierung können Sie dies schnell und in großem Umfang erreichen und gleichzeitig die Konsistenz in verteilen Systemen und Umgebungen erhöhen. Weiterhin können Sie Automatisierung dazu nutzen, um Kontrollprozesse so zu ändern, dass Änderungsanfragen genehmigt werden, und um Änderungsaktivitäten zu protokollieren und Berichte für Audits zu generieren.

Die Bedeutung einer schnellen Reaktion

277 Tage

waren im Jahr 2022 der durchschnittliche Zeitraum, bis Datenpannen erkannt und behoben wurden[6]

26,5 %

Kosteneinsparungen bei Datenpannen, die in maximal 200 Tagen entdeckt und identifiziert wurden[6]

6. IBM. „Cost of a Data Breach Report 2022.“ Juli 2022.
7. ThoughtLab. „Cybersecurity Solutions for a Riskier World.“ 2022

Zero Trust-Architekturen

Wenn Sie die zuvor genannten Bereiche automatisieren, sammelt Ihre Organisation wertvolle Erfahrungen und legt den Grundstein für eine Zero Trust-Architektur. Zero Trust ist ein Architektur-Pattern, bei dem die Sicherheit auf die einzelnen Ressourcen angewendet wird, anstatt die Sicherheit ausschließlich am Netzwerkrand zu verwalten. Keinem Akteur, System, Netzwerk oder Service, der innerhalb oder außerhalb des Sicherheitsperimeters operiert, wird implizit vertraut. Damit ein Nutzer oder Subjekt eine Verbindung zu einer Ressource herstellen kann, muss die Verbindung sowohl authentifiziert als auch autorisiert sein, um explizites Vertrauen zu begründen.

Das Identitäts- und Zugangsmanagement ist der zentrale Bestandteil von Zero-Trust-Architekturen. Jedes Subjekt, das mit einer Ressource interagieren möchte, muss für diese spezifische Interaktion 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 kontextuelle Informationen ermitteln, wie etwa, wer den Zugriff beantragt, auf welche Ressourcen diese Person zugreifen muss, welchen Zweck die Transaktion hat und wie der Zugriff 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 Identitäts- und Zugangs-Managementsysteme zum Verwalten dieser Informationen. Außerdem sollten Sie diese Zugangsentscheidungen immer wieder überprüfen, um sicherzustellen, dass sie weiterhin gültig sind.

Da für jede Interaktion eine Risikobewertung erforderlich ist, benötigen Zero Trust-Ansätze große Daten- und Informationsmengen, die in Ihrer Infrastruktur und Organisation gesammelt werden. Genau deshalb ist Automatisierung so wichtig. Erstens ist die Anzahl der Interaktionen schlichtweg zu groß, als dass ein IT-Team diese manuell verarbeiten könnte. Es wäre unmöglich, zeitnah Zugriff auf Ressourcen zu gewähren, wenn jede dieser Interaktionen manuell überprüft werden müsste.

Zweitens kann Automatisierung Ihnen dabei helfen, Daten aus verschiedenen Systemen innerhalb Ihrer Organisation zu sammeln. Wenn beispielsweise jemand auf eine interne Anwendung zugreifen möchte, müssen Sie mindestens Anstellungsinformationen aus einem Personaldatensystem, Identitätsinformationen aus einem IT-System sowie Update-Status und Standortdaten vom Computer der beschäftigten Person sammeln und verifizieren. Da eine Automatisierungsplattform Systeme und Domains miteinander verbinden kann, die normalerweise nicht miteinander agieren (oder agieren können), ermöglicht sie es Ihnen, schnell und einfach Informationen zu sammeln, zusammenzutragen und zu analysieren. Sie können diese Informationen auch beliebig an das SIEM (Security Information Event Management) und andere zentralisierte Sicherheitssysteme senden.

Und schließlich können Sie mithilfe von Automatisierung dynamisch auf Nutzer-Events und Statusveränderungen reagieren. Wenn Nutzende eine neue Rolle in Ihrer Organisation bekommen oder diese verlassen, können Sie mithilfe von eventgesteuerter Automatisierung den Systemzugriff sofort ändern, anstatt auf manuelle Aktionen warten zu müssen.

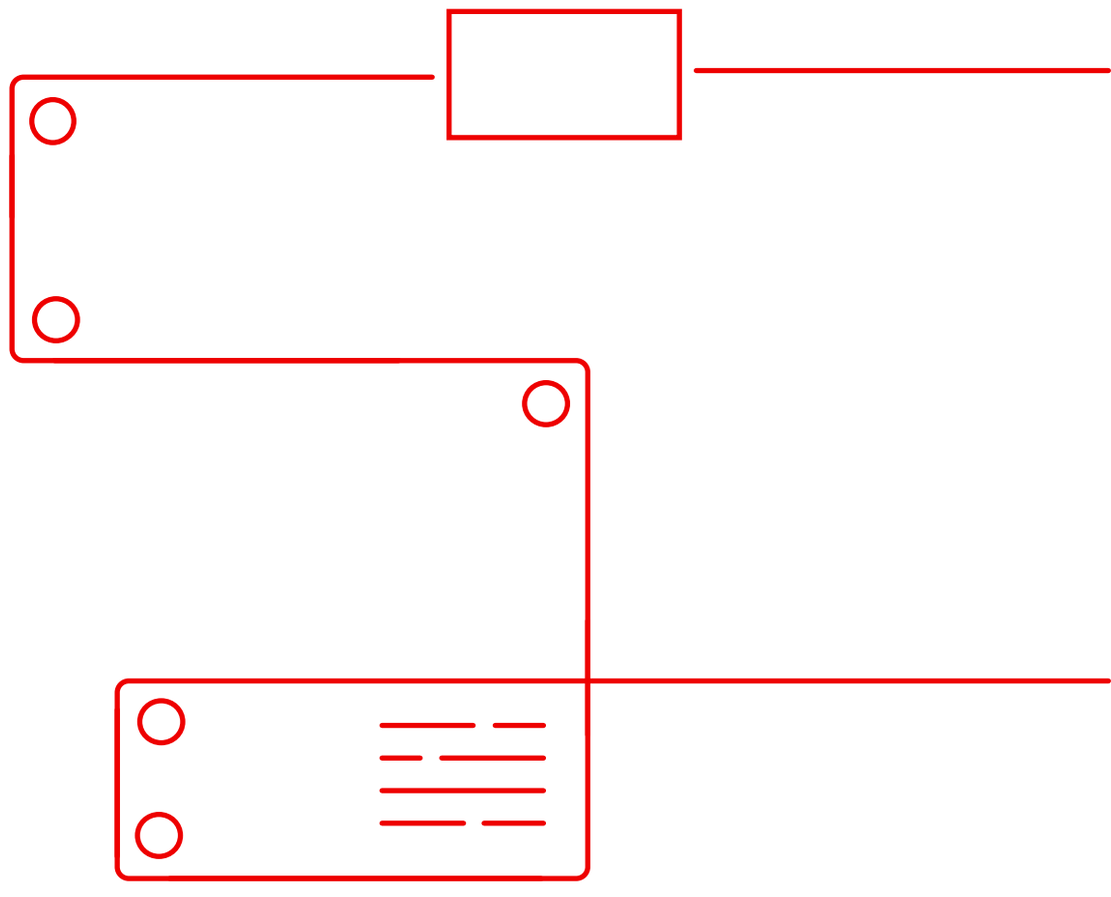
Die Vorteile von Zero Trust-Ansätzen

20,5 %

Kosteneinsparung bei Datenpannen für Organisationen, die Zero Trust einsetzen[8]

1,65 Mio. USD

durchschnittliche Kosteneinsparungen bei Datenpannen im Zusammenhang mit einem ausgereiften Zero Trust-Deployment im Vergleich zu einem Deployment ohne Zero Trust[8]



8. IBM. „Cost of a Data Breach Report 2022.“ Juli 2022.

05 Wie Red Hat Sie beim Thema Cybersicherheit unterstützen kann

Die Cybersicherheit der Zukunft

Mit Automatisierung als Grundlage für ein Weiterentwicklungsmodell Ihrer Cybersicherheit können Sie praktische Schritte durchführen, um schnell und iterativ manuelle Prozesse zu ersetzen, Risiken zu verwalten und Ihren Sicherheitsstatus zu verbessern. Die Lösungen von Red Hat® unterstützen Sie bei der Automatisierung Ihrer bestehenden manuellen Prozesse und ermöglichen es Ihnen, das Risiko von Versäumnissen zu mindern, die durch überforderte und unterbesetzte IT-Teams in Ihrer Organisation entstehen können. Unsere Open Source-Produkte bieten Ihnen Flexibilität und Skalierbarkeit in Cloud-Umgebungen und -Architekturen. Dadurch können Sie heute Ihre Sicherheit stärken und sich gleichzeitig auf die Unsicherheiten der Zukunft vorbereiten.

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform wurde mit einer von Menschen lesbaren Automatisierungssprache entwickelt, die komplexe, manuelle Prozesse in automatisierte Workflows verwandelt. Ansible Automation Platform ermöglicht es Ihren IT-Teams, unternehmensweit Sicherheitsprotokolle zu automatisieren und zu integrieren. Mit dieser Plattform kann Ihre Organisation kuratierte und zertifizierte Automatisierungsinhalte nutzen, um Bedrohungen auf eine koordinierte und einheitliche Art und Weise zu untersuchen und auf diese reagieren. Sie können außerdem folgende Bereiche automatisieren:

- Updates und Patching für CVEs (Common Vulnerabilities and Exposures)
- Rollout von Anwendungskontrollen
- Backup-, Wiederherstellungs- und Verifizierungsprozesse

Red Hat Ansible Automation Platform bietet ein sicherheitsorientiertes, stabiles und unternehmensgerechtes Framework für die Entwicklung und Ausführung automatisierter IT-Prozesse in großem Umfang – von der Hybrid Cloud- bis hin zu Edge-Umgebungen. Mit dieser Automatisierungslösung können Nutzende unternehmensweit Automatisierungsinhalte und Playbooks erstellen, verwalten und untereinander teilen, von Entwicklungs- und Operations- bis hin zu Sicherheits- und Netzwerkteams. IT-Führungskräfte können Richtlinien erstellen, die festlegen, wie Automatisierung in einzelnen Teams genutzt wird, und Entwicklungsteams im Bereich Automatisierung können Aufgaben auf der Basis von bereits vorhandenem Wissen erstellen.

Zusätzlich kann Ansible Automation Platform als Integrationspunkt für Sicherheitslösungen fungieren. Dazu zählen Inhalte von zertifizierten Partnern wie CyberArk, IBM und Splunk, mit denen Sie die Verwaltung und Integration von Sicherheitstechnologien automatisieren können.

Mehr über Red Hat Ansible Automation Platform erfahren ›

Red Hat Enterprise Linux

Red Hat Enterprise Linux bietet eine konsistente und sichere Basis für das Skalieren Ihrer vorhandenen Anwendungen und das Bereitstellen neuer Technologien auf Bare Metal-, virtuellen, Cloud- und Edge-Footprints.

Red Hat Enterprise Linux nutzt einen praktischen 3-Punkte-Ansatz zur Bewältigung von Sicherheitsherausforderungen:

- Risikominderung: Reduzieren Sie das Risiko von Sicherheitsverletzungen mithilfe von Sicherheitsmanagement, bevor Ihre Daten und Systeme oder Ihr Ansehen gefährdet werden.
- Sicherheit: Automatisieren Sie Sicherheitskontrollen und verwalten Sie diese langfristig, in großem Umfang und mit minimalen Ausfallzeiten.
- Compliance: Optimieren Sie die Compliance-Standards für Unternehmen mit stark regulierten Umgebungen.

Red Hat Enterprise Linux enthält zusätzlich integrierte Sicherheitsrichtlinien, die auf viele Regulationen und Standards abgestimmt sind. Dazu gehören CC (Common Criteria), FIPS (Federal Information Processing Standard) 140 und STIG (Secure Technical Implementation Guidelines). Sie können Sicherheitskontrollen automatisch und konsistent auf neue digitale Services anwenden, wodurch Ihr Sicherheitsmanagement verbessert wird.

Mehr über Red Hat Enterprise Linux erfahren ›

Red Hat

Zurück

Mehr Sicherheit mit Red Hat

Red Hat unterstützt Sie dabei, die Sicherheit Ihrer digitalen Services zu verbessern

Red Hat hilft Ihnen, regulatorische Standards und Anweisungen zu automatisieren und Risiken mithilfe automatisierter Sicherheitsintegrationen besser zu managen.

Kontaktieren Sie uns für weitere Informationen >