EFFEKTIVES KONFIGURATIONS-MANAGEMENT

für moderne Unternehmen

Ein Leitfaden für die sichere Navigation durch das SCM

AUTOREN
Steve Marriner
Chris Orr
Tim Erlin

tripwire

INHALTSVERZEICHNIS

EFFEKTIVES KONFIGURATIONS-MANAGEMENT FÜR MODERNE UNTERNEHMEN

EINFÜHRUNG

Das Sicherheitskonfigurationsmanagement (Security Configuration Management, SCM) ist keine neue, aber nach wie vor eine sehr wichtige Sicherheitsmaßnahme. In einer Branche, in der Cyberkriminelle fast täglich neue Methoden entwickeln, sind grundlegende Sicherheitsmaßnahmen wie SCM immer noch die beste Strategie zur Erkennung und Abwehr potenzieller Angriffe sowie zur Sicherstellung der Compliance.

In diesem E-Book stellen wir zuerst die Grundlagen des SCM vor, damit Ihr Sicherheitsprogramm auf einem soliden Fundament steht, und erklären, warum es so wichtig ist. Wir zeigen auch die Unterschiede zwischen SCM und anderen Sicherheitsmaßnahmen auf, die parallel dazu ausgeführt werden können. Dann sehen wir uns einige Herausforderungen moderner Unternehmen genauer an, darunter den Fachkräftemangel, die zunehmende Nutzung von Cloud-Infrastrukturen und die spezifischen Anforderungen industrieller Umgebungen.

Wir analysieren, was ein erfolgreiches SCM in der Praxis ausmacht, und geben einen Überblick über die Standard-Systemeinstellungen, die Konfigurationsüberwachung, die Richtlinienbibliotheken und die Übernahme von Compliance-Frameworks, damit Sie beim nächsten Audit alle Probleme umschiffen. Außerdem erläutern wir, was Sie bei der Wahl einer SCM-Lösung beachten sollten und wie Sie sie in Ihrer Umgebung korrekt implementieren.

SORGFÄLTIGE VORBEREITUNG

Grundlagen des Konfigurations-managements

Das Sicherheitskonfigurationsmanagement ist eine Cybersicherheitsmaßnahme, mit der die korrekte Konfiguration der Systeme, die Erfüllung der Sicherheits- und Compliance-Vorgaben sowie die Minimierung der Cyberrisiken sichergestellt wird. Mit einer sicheren Konfiguration ist ein System gegen Cyberangriffe „gehärtet". Ein weiterer Begriff, den Sie in diesem Zusammenhang vielleicht schon gehört haben, ist „Angriffsfläche". Damit sind die Bereiche eines Systems gemeint, die Angreifer potenziell ausnutzen könnten. Ziel des SCM ist es, die Angriffsfläche zu verkleinern.

SCM dient der Erkennung und Behebung von Fehlkonfigurationen. Dazu werden verschiedene Elemente der Integritätsüberwachung, Konfigurationsvalidierung, Schwachstellenanalyse und Fehlerbehebung im System kombiniert. SCM deckt sowohl On-Premises- als auch Cloud-Konfigurationen ab und erfordert die Zusammenarbeit der Sicherheits- und Ops-Teams. Es ist keine schnelle Maßnahme, die sich innerhalb eines Tages implementieren lässt, aber der Aufwand lohnt sich, denn es wird langfristig entscheidend zur Sicherheit Ihres Systems beitragen.

Ohne SCM bleiben Sicherheitsprobleme wie schwache Passwörter oder Protokolle wie Telnet oder TFTP (Trivial File Transfer Protocol), über die Angreifer auf Daten zugreifen können, möglicherweise lange unerkannt. Unternehmen profitieren daher in zwei wichtigen Bereichen vom SCM: Sicherheit und Compliance.

WAS IST SCM?

Das National Institute of Standards and Technology (NIST) definiert das Security Configuration Management als „die Verwaltung und Überwachung der Konfigurationen eines Informationssystems mit dem Ziel, die Sicherheit zu verbessern und die Risiken zu minimieren".[1]

SCM FÜR MEHR SICHERHEIT

Hacker missbrauchen Fehlkonfigurationen häufig als Einfallstore. Mit korrekt konfigurierten Systemen können Sie die Angriffswahrscheinlichkeit daher entscheidend reduzieren.

Dazu sollten Sie zuerst eine sichere Standardkonfiguration definieren. Dann können Sie regelmäßig Tests durchführen, um nach Abweichungen von dieser Konfiguration zu suchen.

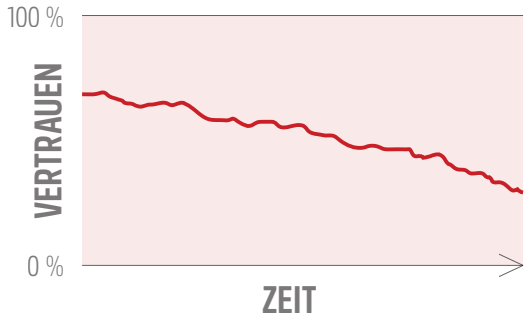
In Unternehmen sollten für alle verwalteten Gerätetypen sichere Konfigurationen definiert sein. Aufgabe des SCM ist es dann, kontinuierlich nach gefährlichen Abweichungen von diesem sicheren und konformen Status zu suchen und diese zu melden.

Wenn Sie eine sichere „Goldstandard-"Konfiguration für Ihre Systeme festlegen und fortlaufend nach Abweichungen davon und nach anderen Gefahrenindikatoren suchen, können Sie Sicherheitsverstöße, die andernfalls vielleicht nicht bemerkt worden wären, schnell aufdecken. Je früher Sicherheitsverletzungen erkannt werden, desto einfacher und effektiver ist die Schadensbegrenzung.

SCM FÜR BESSERE COMPLIANCE

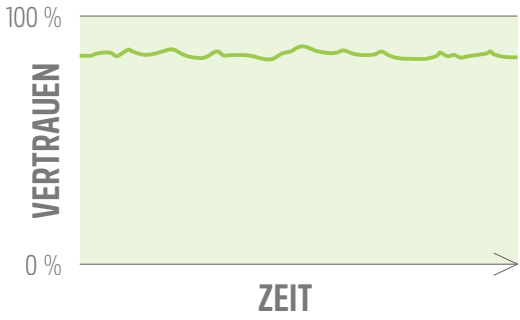
Sichere Konfigurationen haben eine so hohe Priorität, dass nahezu alle Branchenstandards und -verordnungen SCM für die Definition der Konfigurationen vorschreiben. Mit SCM-Tools können Sie sich wesentlich schneller auf einen Audit vorbereiten und diesen auch zügiger durchführen.

Außerdem stellen Sie mit dem SCM sicher, dass das System auch nach dem Audit konform bleibt. Es reicht schließlich nicht aus, nur während der strikten Prüfung alle Vorgaben zu erfüllen. Sie sollten jederzeit den aktuellen Status abrufen können – egal, ob ein Audit ansteht oder nicht.



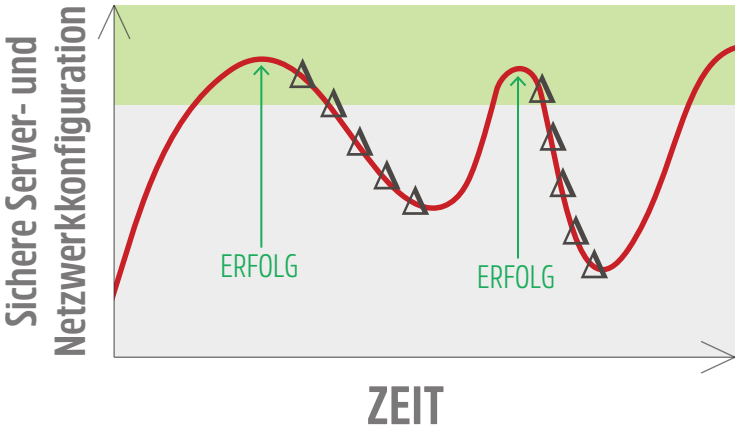
Wenn neue Geräte implementiert und gehärtet werden, vertrauen Unternehmen in der Regel darauf, dass die Konfigurationen sicher sind. Doch Nutzer und Administratoren aktualisieren Software und Betriebssysteme und ändern die Einstellungen, sodass das Vertrauen mit der Zeit schwindet.

Eine SCM-Lösung überwacht die Konfigurationen kontinuierlich und zeichnet alle Änderungen auf. Sie sehen also sofort, welche Änderungen gegen die Compliance-Vorgaben verstoßen, und können diese rückgängig machen. So bleibt das Vertrauen in diese Geräte auf Dauer erhalten.



Ohne SCM-Lösung ist die Vorbereitung auf ein Audit oft aufwendig und kostspielig. Wenn der Audit bestanden ist, werden dann häufig all die Arbeiten durchgeführt, die während der Vorbereitung aufgeschoben wurden. Dabei gehen zu oft die sicheren Standardkonfigurationen verloren, bis der nächste Audit ansteht. Je länger das Unternehmen von den Compliance-Vorgaben abweicht, desto größer wird das Risiko.

Mit SCM können allgemeine oder branchenspezifische Regelwerke mit Empfehlungen zur Härtung, wie CIS, NIST und ISO 27001, sowie branchenübliche Compliance-Vorgaben für Audits, beispielweise PCI DSS (Payment Card Industry Data Security Standard), SOX (Sarbanes-Oxley) oder HIPAA (Health Insurance Portability and Accountability Act), durchgesetzt werden.



FEHLKONFIGURATIONEN VOR DEN HACKERN FINDEN

Ein Hacker kann sich manchmal innerhalb weniger Minuten Zugriff auf ein System verschaffen, aber viele Unternehmen brauchen Tage, Monate oder sogar noch länger, um den Angriff zu bemerken und das Problem zu beheben. Laut dem jährlich erscheinenden *Data Breach Investigations Report*[2] von Verizon hält dieser fatale Trend, der Unternehmen weltweit schon seit Jahren plagt, auch weiterhin an.

Diese gefährliche Situation – dass Angreifer Systeme so schnell infiltrieren und sensible Daten ausschleusen können, während es oft sehr lange dauert, bevor ein Angriff bemerkt und eingedämmt wird – kann mit einem SCM-Tool erheblich entschärft werden. Da Sie sofort über Fehlkonfigurationen informiert werden, die ein System anfälliger machen, können Sie proaktiv die notwendigen Maßnahmen ergreifen.

Das ist nicht nur unsere Schlussfolgerung – auch Cybersicherheitsorganisationen wie das Center for Internet Security (CIS) empfehlen modernen Unternehmen SCM als eine der ersten, grundlegenden Sicherheitsmaßnahmen.

„Die CIS Controls sind ein kostenloses Framework mit Best Practices für die Cybersicherheit, das jedes Unternehmen herunterladen und implementieren kann. Es enthält präzise, nach Priorität sortierte Anleitungen zur Abwehr der am weitesten verbreiteten Cybersicherheitsbedrohungen."[3]

– Center for Internet Security, 2020

DIE WICHTIGSTEN CIS CONTROLS

Diese 20 Sicherheitsmaßnahmen sind nach Priorität aufgelistet. Für ein grundlegendes Cybersicherheitsprogramm sollten Unternehmen unbedingt die ersten sechs Maßnahmen umsetzen. Anschließend können sie der Reihe nach die übrigen implementieren, um Ihr Sicherheitsniveau weiter zu verbessern. SCM hat eine hohe Priorität und steht daher an fünfter Stelle.

1 Inventur und Kontrolle von Hardwareressourcen

Diese Maßnahme hat oberste Priorität. Moderne Unternehmen sind so groß und komplex, dass Sicherheitsteams ein funktionierendes Hardware-Management benötigen, um alle Netzwerkkomponenten im Blick zu behalten.

2 Inventur und Kontrolle von Softwareressourcen

Dies betrifft nicht nur Betriebssysteme, sondern auch andere Software-Ressourcen wie eingebetteten Code, Anwendungen und Services.

3 Kontinuierliches Schwachstellenmanagement

Die Schwachstellenanalyse ist zwar ein wichtiger Teil des Sicherheitsprogramms, ersetzt jedoch nicht das SCM. Sie hilft aber bei der Identifizierung und Priorisierung der durch Sicherheitslücken verursachten Risiken.

4 Kontrolle der Nutzung von Administratorrechten

Entscheidend für ein effektives Cybersicherheitsprogramm ist die Zugriffskontrolle, vor allem für Kreditkarten- und personenbezogene Daten.

5 Sichere Konfiguration von Hardware und Software auf mobilen Geräten, Laptops, Workstations und Servern

Das ist die wichtigste SCM-Maßnahme. Nachdem Sie Ihr System mit SCM wie gewünscht konfiguriert haben, muss es mithilfe anderer Prozesse wie der Überwachung der Dateiintegrität (File Integrity Monitoring, FIM) gepflegt werden, um nicht autorisierte Änderungen an Dateien und anderen Ressourcen zu verhindern.

> ***TIPP VON TRIPWIRE:*** Für ein effektives SCM brauchen Sie einen allgemeinen Überblick über Ihre Umgebung. Diese Informationen erhalten Sie mithilfe der ersten vier CIS Controls: Inventur der Hardware- und Software-Ressourcen, Schwachstellenmanagement und Kontrolle der Zugriffsrechte. Sie können schließlich nur für die korrekte Konfiguration und angemessene Sicherheitsmaßnahmen sorgen, wenn Sie wissen, welche Ressourcen vorhanden sind.

KOORDINIERTE PROZESSE FÜR REIBUNGSLOSE ABLÄUFE

Das SCM ist keine isolierte Maßnahme: Ein effektives SCM ist eng mit anderen grundlegenden Cybersicherheitsprozessen verzahnt. Wenn die verschiedenen Tools ihre Daten untereinander austauschen, erhalten Sie ein umfassendes Bild von der Anfälligkeit und den potenziellen Auswirkungen bestimmter Fehlkonfigurationen oder Systemänderungen.

Unternehmensintegrität

Ein anderer Sicherheitsansatz stellt die Integrität in den Mittelpunkt. Integrität bedeutet dabei, dass es keine Abweichungen vom aktuellen oder erwarteten Status geben darf. Änderungen gehören jedoch zum Alltag und können intern oder extern, autorisiert oder nicht autorisiert, absichtlich oder versehentlich, legitim oder schädlich sein. Allen gemein ist, dass sie eine potenzielle Gefahr für die Integrität des Systems darstellen. Ein effektives Integritätsmanagement gehört daher zu den Grundvoraussetzungen für die Sicherheit.

Nicht ohne Grund ist die Integrität das „I" in „CIA" (Confidentiality, Integrity, Availability), einem weit verbreiteten Framework für zuverlässige Informationssicherheitsrichtlinien. Die anderen beiden Komponenten der Dreiergruppe – Vertraulichkeit und Verfügbarkeit – sind ohne Integrität nicht erreichbar.

Da die Integrität auch für die unternehmensweite Cybersicherheit unverzichtbar ist, kann sie bei der Zielsetzung für Systeme, Netzwerke und Daten als Grundprinzip dienen, wenn verschiedene Arten von Umgebungen in einem koordinierten Programm aufeinander abgestimmt werden sollen.

In diesem größeren Kontext bedeutet das, dass ein Unternehmen ermitteln muss, welche Ressourcen geschützt werden sollen und wie sich unerwünschte Konsequenzen vermeiden lassen. Integrität bildet die Grundlage für Vertrauen und Zuverlässigkeit und ist damit der ultimative Maßstab für die Sicherheit eines Unternehmens. SCM ist eine grundlegende Komponente zur Validierung der Integrität Ihrer Infrastruktur, aber am effektivsten ist es, wenn es mit zuverlässigen Änderungsmanagementprozessen kombiniert wird. Und eine grundlegende Komponente eines erfolgreichen Änderungsmanagements ist das Monitoring der Dateiintegrität (File Integrity Monitoring, FIM).

Monitoring der Dateiintegrität

Um Sicherheitsverstöße möglichst frühzeitig aufzudecken, müssen Sie zuerst die Änderungen erkennen, die den Verstoß ermöglicht haben. Anschließend müssen Sie zweifelsfrei feststellen können, ob die Änderungen aus der Perspektive der Sicherheit und Compliance positiv oder negativ sind. Mithilfe von FIM und SCM können die Folgen aller verdächtigen Änderungen schnell ermittelt und analysiert werden.

WAS IST FIM?

FIM (File Integrity Monitoring, Monitoring der Dateiintegrität) ist ein Sicherheitsprozess, bei dem Änderungen in einer Umgebung erfasst und gemeldet werden, damit Bedrohungen erkannt und behoben werden können. SCM ist auf die FIM-Daten angewiesen – beide Prozesse funktionieren nur in Kombination optimal.

Während SCM vorrangig überprüft, ob die aktuelle Konfiguration mit einer vordefinierten Richtlinie oder Standardkonfiguration übereinstimmt, erkennt FIM Änderungen an Dateien und Systemattributen, die von den vorherigen Einstellungen abweichen. Dazu zählen unter anderem Änderungen an Servern, Netzwerkgeräten, Datenbanken, virtuellen Images und Cloud-Servicekonten.

Zwei weitere Sicherheitsprozesse, die häufig zur Unterstützung implementiert werden, sind das Schwachstellenmanagement und die Logdateiverwaltung.

Schwachstellenmanagement und SCM

Als Schwachstelle wird in der Informationssicherheit ein Softwarefehler bezeichnet, den Hacker ausnutzen können, um sich Zugriff auf ein System oder Netzwerk zu verschaffen. Sie ist nicht dasselbe wie eine Fehlkonfiguration, obwohl beide eine Umgebung anfälliger machen können.

Beim Schwachstellenmanagement werden Netzwerke auf bekannte Sicherheitslücken überprüft – oft anhand einer Liste mit CVEs (Common Vulnerabilities and Exposures). Anschließend werden diese Schwachstellen nach Risikograd priorisiert und behoben. Mit Tools, die sowohl SCM- als auch Schwachstellenmanagementdaten umfassen, erhalten Sie einen besseren Überblick über die Umgebung und können die zu behebenden Fehler aufgrund ihrer potenziellen Auswirkungen priorisieren.

WAS ZEICHNET EIN EFFEKTIVES FIM-TOOL AUS?

Es gibt zahlreiche Lösungen für das Monitoring der Dateiintegrität, die sich in ihrem Funktionsumfang stark voneinander unterscheiden. Einige können nicht zwischen erwarteten und unerwarteten Änderungen unterscheiden und generieren daher zu viele Meldungen und damit einen unnötigen Mehraufwand für das Sicherheitsteam. Im schlimmsten Fall kann das dazu führen, dass wichtige Risiken übersehen werden. Ausgereifte FIM-Lösungen stellen hingegen Kontextinformationen zu jeder Änderung bereit, zum Beispiel welcher Benutzer die Änderung wann vorgenommen hat. Außerdem enthalten sie Tools, die Sie bei der Unterscheidung zwischen autorisierten und potenziell gefährlichen Änderungen unterstützen, und weitere nützliche Funktionen wie die Erkennung von Änderungen in Echtzeit und die automatische Korrektur riskanter Änderungen.

Logdateiverwaltung und SCM

Bei der Logdateiverwaltung werden die Logdateien aller Geräte und Anwendungen einer Infrastruktur erfasst. Da diese Dateien zentral gespeichert werden, können Sicherheitsteams nach Vorfällen auf scheinbar nicht miteinander in Beziehung stehenden Geräten suchen, die dennoch zu einer Ereigniskette gehören. Dank der detaillierten Kontextinformationen der SCM-Daten können Sie sich dann zuerst um Ihre wertvollsten Ressourcen kümmern.

Dies sind nur einige der Cybersicherheitsprozesse, die Sie für ein zuverlässiges Sicherheitsprogramm mit SCM kombinieren sollten.

GEFAHREN AUF HOHER SEE

Bedrohungen für moderne Unternehmen

Eine der größten Herausforderungen für moderne Unternehmen ist der Schutz wachsender, hochgradig vernetzter und nach außen offener Infrastrukturen, die eine riesige Angriffsfläche bieten. Die Anzahl und Vielfalt der Komponenten steigt explosionsartig an und die meisten Endpunkte sind entweder direkt über das Unternehmensnetzwerk oder indirekt über das Internet erreichbar. Jedes dieser Geräte stellt ein potenzielles Einfallstor für Hacker und Cyberkriminelle dar.

In solchen Umgebungen funktionieren ältere Ansätze wie die Sicherheits- und Abwehrmaßnahmen am Perimeter nicht mehr, da der Netzwerkrand zunehmend verschwimmt und durchlässig wird. Nachdem die Angriffe in den letzten zehn Jahren stark zugenommen und erhebliche Schäden in Form von finanziellen Verlusten, Datenschutzverletzungen und dem Diebstahl geistigen Eigentums verursacht haben, können wir mit Sicherheit sagen, dass die Hacker auf Unternehmensnetzwerke zugreifen konnten und die herkömmlichen Sicherheitslösungen damit versagt haben. Datenlecks kosten Unternehmen im Durchschnitt 3,92 Millionen US-Dollar pro Vorfall.[4]

SCM kann den Status der Ressourcen direkt überwachen und Abweichungen von den erwarteten Werten melden – unabhängig davon, ob die Änderungen intern oder extern, versehentlich oder absichtlich vorgenommen wurden. Um wirklich effektiv zu sein, müssen diese Maßnahmen allerdings unternehmensweit eingesetzt werden.

Moderne Unternehmen verwenden nicht mehr nur konventionelle On-Premises-Rechenzentren. Sicherheitsteams müssen die Computing-Ressourcen im gesamten Unternehmen überwachen und verwalten – von den Laptops der Telearbeiter über verteilte Systeme, physische Server und Netzwerkgeräte bis zu Cloud-Ressourcen und SaaS-Anwendungen.

Aber lassen Sie sich von dem Arbeitsaufwand, der für die Implementierung des SCM und der grundlegenden CIS Controls erforderlich ist, nicht abschrecken. Wagen Sie den ersten Schritt und beginnen Sie damit, die Prioritäten festzulegen. Betrachten Sie den Prozess aus der Risikomanagementperspektive: Beginnen Sie mit der Abwehr der gefährlichsten Bedrohungen und optimieren Sie Ihre SCM-Lösung dann kontinuierlich.

REDUZIERUNG DER ANGRIFFSFLÄCHE

Würden Sie Ihr Sicherheitsprogramm anders aufstellen, wenn der Schwerpunkt auf der Reduzierung der Angriffsfläche liegen würde? Das ist ein guter Ansatzpunkt für die Wahl der Sicherheitsstrategie, insbesondere in Bezug auf die grundlegenden Sicherheitsmaßnahmen, die nach wie vor die beste Abwehr gegen Cyberangriffe darstellen.

Was ist eigentlich die „Angriffsfläche"? Dazu müssen wir zuerst den Begriff „Angriffsvektor" klären. Ein Angriffsvektor ist ein Weg, über den ein Angreifer Ihre Systeme und Netzwerke missbrauchen und sich Zugriff auf vertrauliche Daten verschaffen kann.

Die Angriffsfläche ist die Summe aller Angriffsvektoren eines Unternehmens, also alle Pfade, über die Ihre Ressourcen missbraucht werden können – ob On-Premises, in der Cloud, in industriellen Netzwerken oder in hybriden Umgebungen.

In diesem Kapitel sehen wir uns an, wie SCM in den verschiedenen Umgebungen moderner Unternehmen funktioniert und welche Risiken dabei auftreten können.

GRUNDLEGENDES SCM

Die Konfigurationen Ihrer Netzwerkgeräte, Datenbanken, Verzeichnisserver, Bezahlterminals, Workstations, Laptops, Tablets, Betriebssysteme und Anwendungen sind nicht unbedingt von Haus aus sicher. Bei den Standardeinstellungen neuer Geräte steht häufig eher die einfache Installation im Vordergrund als die größte Sicherheit.

Im Verlauf der Zeit werden mitunter unbeabsichtigt Konfigurationsänderungen vorgenommen. Durch diese sogenannte „Konfigurationsdrift" können ebenfalls Schwachstellen entstehen. Die Drift kann verschiedene Formen annehmen, darunter die Ausweitung der Zugriffsrechte und das Öffnen von Kommunikations-Ports oder AWS S3-Buckets (Amazon Web Services).

Diese Ressourcen sind in der Regel im Unternehmen verteilt – in Bürogebäuden, Homeoffices, Campus-Netzwerken, verteilten Rechenzentren und sogar bei verschiedenen Cloud-Anbietern, was die Komplexität zusätzlich erhöht. Auch das Netzwerkfabric, das all diese Ressourcen miteinander verbindet, kann selbst von Konfigurationsdrift betroffen sein. Eine kleine, scheinbar harmlose Änderung an einer Routerkonfiguration kann die Verbindung zu einem gesamten Netzwerk trennen, sodass der Betrieb gestört oder ungehinderter Zugriff über das Internet möglich wird.

Der wichtigste On-Premises-SCM-Prozess für Ihr Sicherheitsteam ist die Überwachung der Konfigurationseinstellungen von Geräten und Anwendungen, damit potenzielle Abweichungen sofort erkannt werden. Die Überwachung muss kontinuierlich stattfinden, nicht nur gelegentlich, denn selbst Unternehmen, die regelmäßig ihre Konfigurationen überprüfen oder Audits bestehen, sind immer nur für kurze Zeit völlig sicher.

Das Risiko steigt nach einem Audit oder einer Prüfung mit jeder Sekunde, denn mit jeder verstreichenden Sekunde wird die sichere Konfiguration mehr eine Annahme und weniger eine Tatsache – und schützt dadurch auch nicht mehr umfassend vor Angriffen.

> ***TIPP VON TRIPWIRE:*** Dynamische Umgebungen bringen spezielle SCM-Herausforderungen mit sich. Zu „dynamischen Umgebung" zählen verschiedene Bereitstellungen, zum Beispiel ein Rechenzentrum mit Hardware-Ressourcen, die regelmäßig außer Betrieb genommen und ersetzt werden. Wenn Ihr SCM-Tool die Deinstallation und Neuinstallation dynamischer Ressourcen nicht überwacht, haben Sie keinen umfassenden Überblick über den Konfigurationsstatus.

Beispiele für Angriffsvektoren, die von grundlegendem SCM blockiert werden

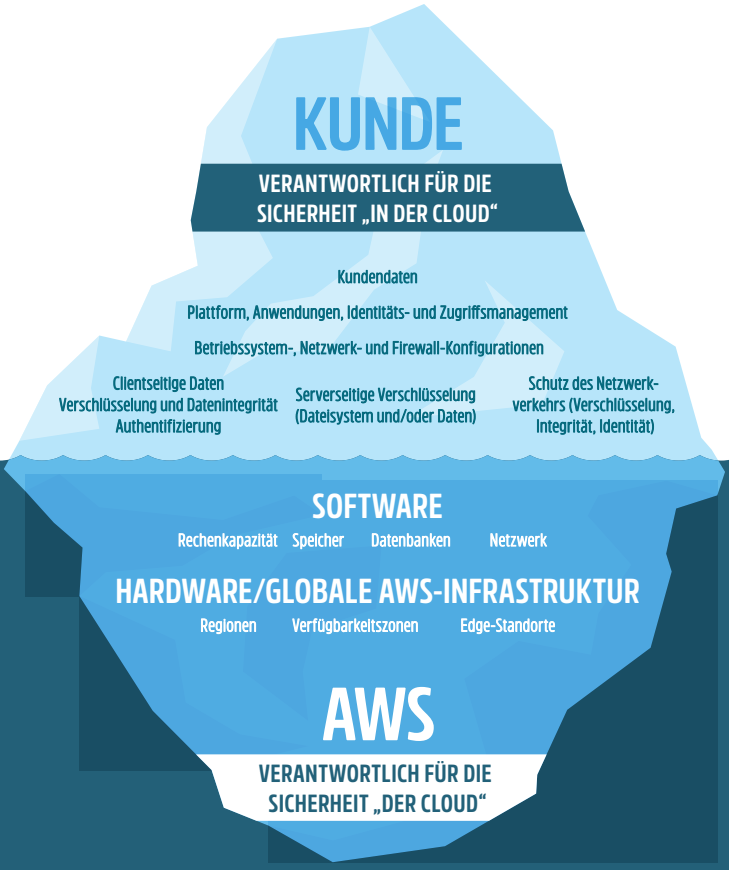
- Ausweitung der Zugriffsrechte
- Zugriff auf Anmeldedaten
- Nicht sichere Services und Protokolle wie Telnet und TFTP

SCM IN DER CLOUD

Die meisten modernen Unternehmen verwenden nicht nur reine On-Premises- oder Cloud-Umgebungen, sondern eine Kombination aus beiden. So profitieren sie von den jeweiligen Vorteilen und können diverse Geschäfts-, IT- und Sicherheitsziele erreichen. Diese Kombination aus Cloud- und On-Premises-Ressourcen wird „hybride" Umgebung genannt.

Hybride Umgebungen bieten dem IT-Team erhebliche Vorteile, vor allem in Bezug auf die Skalierbarkeit, die Kosteneffizienz und die nuancierte Anpassung der Infrastruktur. Sie führen aber gleichzeitig dazu, dass die Angriffsfläche wesentlich komplexer wird. Außerdem werden in diesen Umgebungen meist Lösungen mehrerer Cloud-Anbieter verwendet, um von den zahlreichen unterschiedlichen Angeboten zu profitieren und die Bindung an einen Anbieter zu vermeiden.

Multi-Cloud-Sicherheit lässt sich nur mithilfe von automatisierten SCM-Tools erreichen, die nicht auf die physischen Systeme vor Ort beschränkt sind, sondern eine entsprechende Konfigurationsüberwachung auch in der Cloud leisten können. Die Konfigurationen der AWS S3-Buckets sind beispielsweise ein Cloud-Angriffsvektor, der kontinuierlich überprüft werden muss. Laut dem *DBIR* von Verizon zählen Fehlkonfigurationen des Cloud-Speichers zu den häufigsten Ursachen für Sicherheitsverletzungen.[1]



Es ist verlockend, sich darauf zu verlassen, dass der Cloud-Anbieter automatisch für die Sicherheit der Daten und Systemkonfigurationen sorgt. Tatsächlich aber wird die Verantwortung geteilt. Sie müssen genau wissen, für welche Sicherheitsbereiche Sie zuständig sind und welche Cloud-Anbieter wie AWS, Google Cloud Platform oder Azure übernehmen. Sie sind nicht nur für den Schutz Ihrer Daten und Anwendungen verantwortlich, sondern auch für die Konfigurationen Ihrer Cloud-Konten.

Ein weiterer Bereich, dem Cybersicherheitsteams besondere Aufmerksamkeit widmen sollten, ist DevOps. Bei ihren Bemühungen, die CI/CD-Pipeline so kurz und effizient wie möglich zu gestalten, denken DevOps-Teams nicht immer an die Sicherheit – was schwerwiegende Folgen haben kann. Bevor es Container gab, war der Softwareentwicklungszyklus deutlich länger. Jetzt können neue Versionen sofort an die aktuellen Unternehmensanforderungen angepasst werden. Neue Anwendungen werden häufig in Containern bereitgestellt und Anwendungen und Dienste werden inzwischen nicht mehr als isolierte Einheiten angesehen. Fehlkonfigurationen von Containern und Images müssen als kontinuierlich zu prüfende Quality Gates betrachtet werden, damit auch DevOps in den SCM-Prozess integriert werden kann.

Beispiele für Angriffsvektoren, die von SCM in der Cloud blockiert werden

- Fehlkonfigurationen in öffentlichen Cloud-Speichern
- DevOps-Container
- Ungeschützte GitHub-Repositorys
- Offengelegte Admin-Anmeldedaten

SCM IN INDUSTRIELLEN UMGEBUNGEN

In industriellen Umgebungen wie kritischen Infrastrukturen oder der diskreten Fertigung ist das SCM etwas schwieriger umzusetzen, da neben der Informationstechnologie (IT) auch die Betriebstechnologie (Operational Technology, OT) überwacht werden muss. Außerdem werden dort immer mehr IIoT-Geräte (Industrielles Internet der Dinge) eingesetzt. IIoT-Geräte verbinden die zuvor isolierten physischen Anlagen mit den digitalen Unternehmensinfrastrukturen und dem Internet. Dadurch wächst die Angriffsfläche auf manchmal unvorhersehbare Weise.

In industriellen Steuersystemen (Industrial Control Systems, ICS) werden SCM-Prozesse für die korrekte Konfiguration der Endpunkte wie Workstations, SCADA-Systeme, speicherprogrammierbare Steuerungen (SPS) und Mensch-Maschine-Schnittstellen benötigt. Wie auch in IT-Umgebungen müssen die Konfigurationen kontinuierlich überwacht werden, um die Einhaltung der Compliance-Vorgaben sicherzustellen. Ein zusätzliches Problem ist, dass viele Steuersysteme äußerst sensibel sind. Daher können die Konfigurationsdaten nur über ressourcenschonende oder kontaktlose Methoden abgerufen werden.

Beispiele für Angriffsvektoren, die von SCM in industriellen Umgebungen blockiert werden

- Remote-Zugriff durch die Ausweitung der Zugriffsrechte
- Falsch konfigurierte Workstation-Endpunkte
- Falsch konfigurierte ICS und IIoT-Geräte

TELEARBEIT UND SCM

Auch die Zunahme der Telearbeit und die dabei verwendeten Tools bringen neue Herausforderungen im Konfigurationsmanagement mit sich. Der Wechsel von einer überwiegend aus Büroarbeitern zu einer größtenteils aus Telearbeitern bestehenden Belegschaft verschiebt den Netzwerkperimeter und vergrößert die Angriffsfläche.

Vielen fallen in diesem Zusammenhang zuerst die Laptops der Mitarbeiter im Homeoffice ein, doch mit ihrer Sicherung ist das Problem noch nicht gelöst. Wenn zahlreiche Mitarbeiter an weit verteilten Standorten arbeiten, müssen nicht nur Laptops und Zugriffsrechte organisiert werden, sondern vor allem eine große Infrastruktur für unterstützende Services wie Remote-Zugriff, Authentifizierung und Helpdesk.

Effektives SCM in einer überwiegend aus Telearbeitern bestehenden Umgebung sollte mit einer Inventur der Systeme beginnen. Anhand der Inventarliste können Sie dann das SCM für alle Komponenten implementieren. Auf diese Weise können Sie sicherstellen, dass die Nutzer authentifiziert werden, der Remote-Zugriff korrekt konfiguriert wurde und die Konfigurationen der Remote-Endpunkte sicher und konform sind.

Beispiele für Angriffsvektoren bei der Telearbeit, die von SCM blockiert werden

- Falsch konfigurierte Remote-Endpunkte (z. B. Laptops)
- Falsch konfiguriertes DNS
- Falsch konfigurierte Zugriffskontrollen

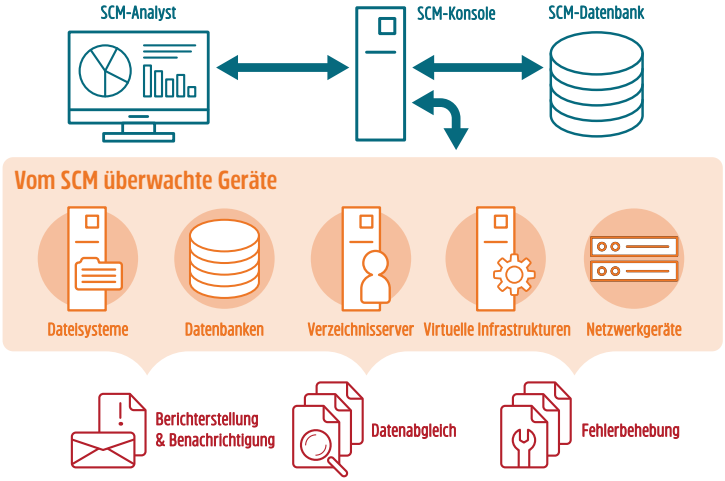
AUF DEM RICHTIGEN KURS

SCM in der Praxis

Schon das Monitoring der Konfigurationen auf einem einzigen Server kann eine Mammutaufgabe sein, da Tausende Ports, Services und Einstellungen überwacht werden müssen. Wenn Sie diese Ports, Services und Einstellungen für die Server, Hypervisoren, Router, Switches und Firewalls des gesamten Unternehmens zusammenrechnen, wird deutlich, warum das SCM automatisiert werden muss.

Die SCM-Konsole erfasst die Daten von allen Endpunkten und kann auch genutzt werden, um gefundene Abweichungen gemäß den festgelegten Compliance-Richtlinien rückgängig zu machen. Die Komponenten der verschiedenen SCM-Lösungen können variieren, doch typischerweise gibt es eine Konsole, in der Sie die SCM-Daten verwalten und konfigurieren sowie Berichte erstellen. In einer Backend-Datenbank werden alle Informationen zu den Standardeinstellungen, Änderungen und Compliance-Vorgaben gespeichert.

Mit einer Kombination aus agentbasierten und agentlosen Technologien können Sie die relevanten SCM-Informationen von diversen Endpunkten erfassen, zum Beispiel Laptops und Workstations, Routern, Switches und Firewalls, Servern, Datenbanken, Verzeichnisservern und anderen Ressourcen – sowohl physischen als auch virtuellen und cloudbasierten.



DIE VIER WICHTIGSTEN PROZESSE EINES ZUVERLÄSSIGEN SCM

Die Geräteerkennung, die Festlegung der Standard-Konfigurationseinstellungen, das Änderungsmanagement und die Fehlerbehebung sind die vier wichtigsten Prozesse des SCM. Ein effektives SCM-Tool automatisiert diese Aufgaben und bietet gleichzeitig einen umfassenden Überblick über das System. Sobald eine Fehlkonfiguration erkannt wird, sollten Sie eine Warnmeldung und detaillierte Empfehlungen zur Korrektur erhalten.

1. **Geräteerkennung:** *Sie können nur verwalten, was Sie kennen. Daher müssen Sie zuerst ermitteln, welche Geräte verwaltet werden müssen. Idealerweise erleichtert eine SCM-Plattform mit integriertem Repository Ihnen das Ressourcenmanagement. Wenn Sie die Ressourcen kategorisieren und mit Tags versehen, vermeiden Sie das Starten nicht erforderlicher Dienste. So müssen die Workstations der Techniker beispielsweise anders konfiguriert werden als Finanzsysteme.*

2. **Festlegung der Standardeinstellungen:** *Zunächst müssen Sie die gewünschten Konfigurationen für jeden verwalteten Gerätetyp festlegen. Viele Unternehmen nutzen Benchmarks von vertrauenswürdigen Organisationen wie CIS oder NIST (National Institute of Standards and Technology) als Ausgangspunkt.*

3. **Änderungsmanagement:** *Anhand dieser Standardeinstellungen kann Ihr SCM-Tool dann Änderungen identifizieren und Sie darüber benachrichtigen. Wenn alle Geräte erfasst und kategorisiert wurden, sollten Sie im nächsten Schritt festlegen, in welchen Abständen Richtlinienprüfungen durchgeführt werden sollen. Echtzeitprüfungen sind nicht in allen Fällen erforderlich (mehr dazu später).*

4. **Fehlerbehebung:** *Wurden Probleme erfasst, müssen sie entweder behoben oder zu einer Ausnahme erklärt werden. Für einen Audit müssen Sie zudem nachprüfen, ob erwartete Änderungen tatsächlich vorgenommen wurden. Wenn Sie eine neue SCM-Lösung implementieren, werden Sie vermutlich nicht sofort alle anstehenden Aufgaben erledigen können. Sie müssen daher priorisieren.*

WICHTIGE TIEFGREIFENDERE SCM-PROZESSE

Die vier Prozesse – Erkennung, Festlegung der Standardeinstellungen, Änderungsmanagement und Fehlerbehebung – bilden die Grundlage des SCM-Programms. Im Folgenden gehen wir im Detail auf Richtlinienbibliotheken, die Funktionsweise von SCM-Prüfungen und die optimale Nutzung der SCM-Funktionen für Dashboards und Berichte ein.

RICHTLINIENBIBLIOTHEKEN

Eine SCM-Richtlinie ist die Gesamtheit der internen und externen Vorgaben, die die überwachten Systeme in Ihrem Unternehmensnetzwerk erfüllen müssen. Achten Sie darauf, dass Ihr Tool über integrierte Richtlinien für Tests zur Einhaltung von Frameworks wie den CIS Controls und dem PCI DSS verfügt. Mit einer ausgereiften Lösung können Sie auch die Einhaltung interner Compliance-Richtlinien überprüfen. Dazu erstellen Sie eigene Tests für die individuellen Richtlinien direkt in Ihrem SCM-Tool.

WAS ZEICHNET GUTE RICHTLINIEN AUS?

Gute Richtlinien sind präzise und aktuell. Damit sie präzise sind, müssen Sie die häufig eher vage gehaltenen Compliance-Anforderungen mit konkreten, effektiven Sicherheitsmaßnahmen umsetzen, die die Auditoren überzeugen. Bei der Aktualität geht es darum, die zahlreichen Änderungen in allen Compliance-Richtlinien zeitnah vorzunehmen.

Individuelle Richtlinien

Eine gute SCM-Lösung sollte sowohl das Importieren einer ganzen Reihe zusätzlicher Richtlinien als auch das Erstellen eigener Richtlinien unterstützen. Jede dieser Richtlinien umfasst die folgenden vier Komponenten:

- **Test** zur Überprüfung einer spezifischen, aktuellen Konfigurationseinstellung
- **Bewertung** des Compliance-Status eines Systems oder Geräts
- **Gewichtung** der relativen Wichtigkeit des Tests
- **Grenzwerte** zur Identifizierung der wichtigsten Abweichungen

Ausnahmeregelungen für Richtlinien

Für Tests oder Richtlinien können Ausnahmeregelungen festgelegt werden, um bestimmten Geschäftsanforderungen oder anderen Faktoren Rechnung zu tragen. Ein Beispiel wäre eine wichtige alte Anwendung, die nur unter Microsoft Windows 2003 ausgeführt werden kann. In den meisten Fällen würde ein Auditor ein so stark veraltetes Betriebssystem beanstanden, aber mit einer dokumentierten Ausnahmeregelung, in der der Grund erklärt und das Risiko vom Unternehmen übernommen wird, kann er diesen Punkt billigen.

> ***TIPP VON TRIPWIRE:*** Wählen Sie ein SCM-Tool, das für die Zuweisung von Ausnahmeregelungen Gruppen und Tags berücksichtigt und nicht nur die starren Beziehungen zwischen bestimmten Ressourcen und Tests. Auf diese Weise können kurzlebige und dynamische Ressourcen von den Richtlinientests ausgenommen werden, da ihre Aktivierung oder Deaktivierung mit der entsprechenden Ressourcengruppe oder einem Tag verknüpft ist. Dann sind Ausnahmeregelungen auch in dynamischen Cloud-Umgebungen möglich.

Festlegung mehrerer Richtlinien

In Unternehmen gibt es häufig mehrere Compliance- oder Sicherheitsanforderungen. Börsennotierte Unternehmen, die Kreditkartendaten verarbeiten, müssen beispielsweise sowohl die Vorschriften des SOX (Sarbanes-Oxley Act) als auch des PCI erfüllen. In einer effektiven SCM-Lösung können Sie ohne großen Aufwand mehrere Richtlinien für die Ressourcen festlegen.

Ressourcen-Tagging

Große Unternehmen sind in der Regel komplex und vielschichtig. Ihre SCM-Lösung muss diese Komplexität widerspiegeln, um relevante Informationen und Empfehlungen zu liefern. Wenn Ihre Unternehmensstruktur beispielsweise Merkmale wie Standort, Systemeigentümer, Abteilungsleiter oder Anwendung für die Unterteilung nutzt, sollte Ihre SCM-Lösung Ressourcen-Tags unterstützen, die dieses logische Unternehmensschema abbilden, denn so lässt sich die SCM-Compliance einfacher und besser nachverfolgen.

RESSOURCENÜBERWACHUNG

Die Festlegung von detaillierten Prozessen und Richtlinien ist ein guter Anfang, aber wenig effektiv, solange sie nicht auch kontrolliert werden. Wenn Sie Ressourcen überwachen und aktiv nach Änderungen suchen, können Sie sicherstellen, dass die Prozesse und Richtlinien korrekt befolgt und bei Abweichungen die zuständigen Mitarbeiter benachrichtigt werden.

Agentbasierte oder agentlose Überwachung

Für die Ressourcenüberwachung gibt es in der Regel zwei Möglichkeiten: entweder mit einem Programm, das speziell auf dem Zielsystem installiert wird (einem sogenannten Agent), oder per Remote-Zugriff. Einige Lösungen unterstützen beide Optionen. Mit der agentbasierten Überwachung erhalten Sie in der Regel detailliertere Informationen, da der Agent die betroffenen Ressourcen direkt inspizieren kann. Die agentlose Überwachung eignet sich vor allem für Fälle, in denen ein Agent einen zu großen Störfaktor darstellen würde (zum Beispiel in industriellen Netzwerken) oder mit bestimmten Aspekten der Umgebung nicht kompatibel wäre (wie bei Systemen mit eingebettetem Windows oder Linux). Für die agentlose Überwachung benötigen Sie die korrekten Anmeldedaten, um per Remote-Zugriff auf die Systeme zugreifen zu können.

In Echtzeit oder in regelmäßigen Abständen

Die meisten SCM-Tools suchen regelmäßig nach Abweichungen von vorab definierten Standardeinstellungen. Für bestimmte kritische Systeme oder äußerst dynamische Umgebungen kann es von Vorteil sein, etwaige Änderungen in Echtzeit zu erfassen. Dadurch werden Sie sofort über potenziell gefährliche Änderungen informiert und können genau sehen, wer wann was geändert hat. Einige überwachte Ressourcen,

wie Router, Netzwerk-Switches und Firewalls, unterstützen allerdings keine Agents. Diese Netzwerkgeräte müssen von der SCM-Lösung in regelmäßigen Abständen überprüft werden.

WORKFLOWS ZUR KORREKTUR

Wenn Sie wissen, welche Ressourcen nicht mehr richtlinienkonform sind, ist der erste Schritt getan. Ihr Ziel ist jedoch erst erreicht, wenn Sie die gefundenen Abweichungen auch zeitnah beheben. Eine effektive SCM-Lösung umfasst Richtlinien, die das Problem nicht nur beschreiben, sondern auch Korrekturempfehlungen für die System- oder Anwendungseigentümer enthalten.

Wird die Lösung mit einem Prozess für das Änderungsmanagement kombiniert oder (idealerweise) in eine automatisierte Änderungsmanagementlösung integriert, kann sie dank der detaillierten Dokumentation die Fehlerbehebung unterstützen und damit einen wichtigen Beitrag zur kontinuierlichen geschäftlichen Verfügbarkeit leisten.

BERICHTE UND DASHBOARDS

Sie müssen entscheiden, in welcher Form Sie die vom SCM-Tool erfassten Informationen erhalten möchten. Denken Sie dabei nicht nur an die Präsentation der technischen Daten, sondern auch an die Berichte mit Übersichtscharakter und an alle Stakeholder – sowohl die Technikexperten als auch fachfremde Verantwortliche –, die die SCM-Berichte nutzen könnten.

Gut strukturierte Berichte und Dashboards sind eine Grundvoraussetzung für eine effektive SCM-Lösung. Unternehmen jeder Größenordnung müssen die entscheidenden Informationen aus den unter Umständen riesigen Datenmengen extrahieren können. Durch das Ressourcen-Tagging können Administratoren problemlos die jeweils relevanten Informationen präsentieren.

Gute SCM-Tools sehen aus wie übersichtliche Dashboards

Dashboards sind eine wichtige Komponente guter SCM-Tools, da sie Stakeholdern im gesamten Unternehmen helfen, sich schnell einen Überblick über die Sicherheits- und Compliance-Maßnahmen zu verschaffen – sowohl zum aktuellen Zeitpunkt als auch im Zeitverlauf. Daher sollten Sie darauf achten, dass es Standardeinstellungen für Experten und Laien gibt und dass die Benutzer die für sie wichtigen Elemente auswählen können. Es sollte auch eine Zugriffskontrolle geben, damit bestimmte Elemente, Richtlinien und/oder Warnmeldungen nur von autorisierten Nutzern oder Gruppen abgerufen werden können. Die entsprechenden Berechtigungen werden in der Regel im Verzeichnis des Unternehmens gespeichert. Bei einer guten Berichterstattung werden die Bereiche hervorgehoben, die von Ihrer vorgegebenen Konfiguration abweichen, und Empfehlungen zur Korrektur gegeben.

KLAR SCHIFF MACHEN

SCM zu Compliance-Zwecken

SCM trägt nicht nur zur Härtung der Angriffsfläche bei, sondern hilft Auditoren auch, die Compliance-Verbesserungen im Zeitverlauf nachzuverfolgen. Wenn ein Audit ansteht, können Sie rückblickend Berichte für jeden beliebigen Zeitraum erstellen, um die Einhaltung der diversen Compliance-Vorgaben nachzuweisen.

Diese Funktionen können sowohl für interne als auch für externe Audits genutzt werden, falls Ihr Unternehmen zum Beispiel neben den externen Audits für die gesetzlich vorgeschriebenen Standards wie PCI DSS oder HIPAA regelmäßig interne Audits durchführt, um die Einhaltung interner Vorgaben zu prüfen.

„Die Auswahl sicherer Konfigurationseinstellungen ist eine komplexe Aufgabe, mit der normale Nutzer gewöhnlich überfordert sind. Mitunter müssen Hunderte oder sogar Tausende Optionen analysiert werden, bevor fundierte Entscheidungen getroffen werden können. Selbst wenn eine starke Konfiguration definiert und installiert wurde, muss sie kontinuierlich verwaltet werden, um eine Verwässerung der Sicherheitsmaßnahmen zu vermeiden, wenn Software aktualisiert oder gepatcht, neue Sicherheitslücken aufgedeckt und Konfigurationen für die Installation neuer Software oder für neue Anforderungen geändert werden. Andernfalls werden Angreifer Wege finden, um sowohl die über das Netzwerk zugänglichen Services als auch die Client-Software auszunutzen.“[5]

– Center for Internet Security

FRAMEWORKS MIT BEST PRACTICES

Es besteht ein entscheidender Unterschied zwischen Frameworks mit Best Practices und gesetzlichen Vorschriften. Frameworks werden von Organisationen wie CIS und NIST herausgegeben und sind Leitfäden, an denen Sie sich bei der Entwicklung eines modernen, effektiven Cybersicherheitsprogramms orientieren können.

Sie enthalten Empfehlungen zu grundlegenden Sicherheitsprozessen wie SCM, deren Umsetzung aber nicht in Audits überprüft wird. Allerdings wird SCM auch in den Verordnungen vorgeschrieben. Durch die Implementierung stellen Sie daher die Einhaltung beider Vorgaben sicher.

Es gibt verschiedene Frameworks für effektive Cybersicherheitsprogramme, Beispiele sind CIS Controls, NIST und MITRE ATT&CK. Dies sind nicht die einzigen Frameworks für ein effektives SCM, aber sie gehören zu den am häufigsten genutzten.

DIE CIS CONTROLS

Wie schon in Kapitel 1 erwähnt, gelten die CIS Controls des Center for Internet Security in der Cybersicherheitsbranche inzwischen als Standard und die meisten Unternehmen berücksichtigen sie für die Sicherheit ihrer Systeme. Die 20 Sicherheitsmaßnahmen sind nach Priorität aufgelistet und werden daher am besten der Reihe nach implementiert. Informationen zu SCM finden Sie in der Maßnahme Nr. 5: „Sichere Konfiguration von Hardware und Software auf mobilen Geräten, Laptops, Workstations und Servern".

Die CIS Controls

Grundlegende CIS Controls

1. *Inventur und Kontrolle von Hardwareressourcen*
2. *Inventur und Kontrolle von Softwareressourcen*
3. *Kontinuierliches Schwachstellenmanagement*
4. *Kontrolle der Nutzung von Administratorrechten*
5. *Sichere Konfiguration von Hardware und Software auf mobilen Geräten, Laptops, Workstations und Servern*
6. *Wartung, Überwachung und Analyse von Auditprotokollen*

Technische CIS Controls

7. *Schutz von E-Mail-Systemen und Webbrowsern*
8. *Schutz vor Malware*
9. *Einschränkung und Kontrolle von Netzwerkports, Protokollen und Services*
10. *Funktionen für die Datenwiederherstellung*
11. *Sichere Konfiguration von Netzwerkgeräten wie Firewalls, Routern und Switches*
12. *Abwehrmaßnahmen an der Netzwerkgrenze*
13. *Datenschutz*
14. *Kontrollierter Zugriff nach dem Need-to-know-PrinzipWLAN-Zugangskontrollen*
15. *Kontrolle und Monitoring von Konten*

Organisatorische CIS Controls

16. *Implementierung eines Programms zur Weiterbildung und zur Steigerung des Sicherheitsbewusstseins*
17. *Sicherheitsfunktionen für Anwendungssoftware*
18. *Incident-Response-Maßnahmen und -Management*
19. *Penetrationstests und Red-Team-Übungen*

NIST

NIST ist ein Framework für die Informationssysteme der US-Bundesbehörden und eng mit dem Federal Information Security Modernization Act (FISMA) verknüpft. Die NIST Special Publication (SP) 800-53 mit dem Titel „Sicherheits- und Datenschutzmaßnahmen für Informationssysteme der US-Bundesbehörden und Organisationen" ist auch für Unternehmen im privaten Sektor hilfreich, da die Empfehlungen für Sicherheitsexperten aus allen Branchen relevant sind.

Darin wird die Nutzung automatisierter Tools für das Konfigurationsmanagement empfohlen: „Automatisierte Tools können auf Unternehmensebene, Projekt-/Prozessebene oder Systemebene auf Workstations, Servern, Notebooks, Netzwerkkomponenten oder mobilen Geräten verwendet werden. ... Zu den automatisierten Sicherheitsmaßnahmen gehören das Deaktivieren bestimmter Systemfunktionen, das Aussetzen der Systemprozesse oder das Senden von Warnmeldungen oder Benachrichtigungen an Mitarbeiter, wenn eine nicht genehmigte Änderung einer Konfiguration erkannt wird."[6]

SCM-Compliance in US-Bundesbehörden

Der Federal Information Security Management Act (FISMA) verpflichtet US-Bundesbehörden per Gesetz zur Implementierung von Sicherheitsmaßnahmen für ihre Systeme. Die in diesem Kapitel aufgeführten Standards und Frameworks sind Beispiele für gängige Vorgaben, die bei einem Audit überprüft werden. Es war jedoch nicht unser Ziel, eine vollständige Liste zu erstellen. Das im vorherigen Abschnitt genannte NIST-Framework dient als Leitfaden für die FISMA-Compliance. Die folgenden NIST Special Publications haben einen Bezug zu SCM:

- **NIST 800-37:** Leitfaden zur Implementierung des Risikomanagement-Frameworks in Informationssystemen der US-Bundesbehörden
- **NIST 800-53:** Empfohlene Sicherheitsmaßnahmen für die Informationssysteme von US-Bundesbehörden
- **NIST 800-128:** Leitfaden für das sicherheitsorientierte Konfigurationsmanagement von Informationssystemen
- **NIST 800-137:** Kontinuierliche Überwachung der Informationssicherheit in Informationssystemen der US-Bundesbehörden
- **NIST 800-171:** Schutz vertraulicher Informationen (Controlled Unclassified Information, CUI) in sonstigen Systemen und Organisationen

„Die NIST-Standards sind vermutlich das umfassendste und am besten recherchierte derzeit verfügbare Framework. Sie können die vorhandenen Prozesse in großen Unternehmen unterstützen, sind aber gleichzeitig auch flexibel genug, um kleineren Unternehmen als Leitfaden zur Verbesserung ihrer Cybersicherheit zu dienen."

– David Meltzer, Chief Technology Officer bei Tripwire

MITRE

MITRE ist eine gemeinnützige Organisation, die staatlich geförderte Forschungs- und Entwicklungszentren betreibt. Ihr ATT&CK-Framework ist ein äußerst hilfreiches Cybersicherheitsmodell, in dem Angreiferverhalten und -taktiken beschrieben und Maßnahmen empfohlen werden, mit denen Sie das Risiko senken und die Sicherheit stärken können.

CIS bietet eine priorisierte Liste mit Maßnahmen zur Systemhärtung. MITRE ATT&CK hingegen geht die Cybersicherheit aus der Angreiferperspektive an.

In einer detaillierten Matrix werden die am häufigsten verwendeten Angriffstaktiken, -techniken und allgemeine Erkenntnisse (Adversarial Tactics, Techniques, and Common Knowledge, ATT&CK) aufgelistet. ATT&CK-Techniken wie die Ausweitung der Zugriffsrechte, Zugriff auf Anmeldedaten und die Ausbreitung im Netzwerk können durch SCM blockiert werden, da diese Aktivitäten die Konfiguration beeinträchtigen würden und daher von SCM-Tools gemeldet werden.

„Das MITRE ATT&CK-Framework (Adversarial Tactics, Techniques, and Common Knowledge) ist eine Wissenssammlung und ein Modell für das Angriffsverhalten von Cyberkriminellen. Es umfasst die verschiedenen Phasen des Angriffszyklus der Hacker und die Plattformen, die sie üblicherweise ins Visier nehmen. Das Framework entstand bei einem Projekt, mit dem die Taktiken, Techniken und Prozesse (TTP) der Hacker nach Angriffen auf Microsoft Windows™-Systeme aufgelistet und kategorisiert wurden, um diese Aktivitäten besser erkennen zu können. Inzwischen umfasst es auch Informationen für Linux™ und MacOS™, Taktiken und Techniken zur Angriffsvorbereitung sowie bestimmte Technologiebereiche wie Mobilgeräte."[7]

– MITRE

COMPLIANCE-VERORDNUNGEN

Nach den gängigen Best Practices und Frameworks für die Implementierung von SCM sehen wir uns jetzt die gesetzlich vorgeschriebenen Compliance-Verordnungen an. In den meisten Branchen gibt es ein vorrangiges Compliance-Gesetz, wie das HIPAA im Gesundheitswesen, aber einige Verordnungen gelten branchenübergreifend, zum Beispiel die DSGVO (Datenschutz-Grundverordnung). Unabhängig von der Vorschrift ist das SCM einer der wichtigsten Prozesse, die bei einem Audit geprüft werden.

PCI DSS

Bei der Digitalisierung der Kreditkartenbranche wurde schnell deutlich, dass Maßnahmen zum Schutz vor Online-Betrug erforderlich waren. Kreditkartenbetrug ist weiterhin ein großes Problem und das Kundenvertrauen in die weltweit größten Unternehmen sinkt mit jeder Schlagzeile zu Datenlecks und Sicherheitsverletzungen.

Der PCI Security Standards Council wurde 2006 gegründet und ist inzwischen eine globale Organisation, die weitreichenden Einfluss darauf hat, wie Geschäfte im digitalen Zeitalter abgewickelt werden. PCI sorgt nicht nur dafür, dass die Daten der Karteninhaber nicht in die falschen Hände gelangen, sondern gibt auch Haftungsbegrenzungen für Kartenaussteller und Banken vor, falls ein Händler Opfer eines Angriffs wird.

Wenn Sie effektives SCM für die Einhaltung der PCI-Vorgaben implementieren möchten, brauchen Sie ein Tool, das diverse Serverbetriebssysteme, Bezahlterminalsysteme, virtuelle Systeme, Ressourcen in der Cloud, Netzwerkgeräte, Verzeichnisserver und Datenbanken unterstützt, um die gängigsten Angriffsvektoren abzudecken. Das SCM-Tool sollte auch Tipps zur Korrektur von Systemkonfigurationen geben, die von den PCI-Vorgaben abweichen. Abschnitt 11.5 nennt insbesondere die Vorteile von FIM-Funktionen zur Warnung vor Änderungen, die zu Konfigurationsabweichungen führen könnten.

HIPAA

Das US-amerikanische Gesetz HIPAA (Health Insurance Portability and Accountability Act) wurde 1996 verabschiedet und unterliegt dem U.S. Department of Health and Human Services. Durch das Gesetz sollen die Risiken der Offenlegung vertraulicher Patientendaten minimiert und die Vertraulichkeit, Integrität und Verfügbarkeit der geschützten Gesundheitsdaten gewährleistet werden.

SCM-Tools überprüfen die Systeme auf nicht autorisierte Änderungen und priorisieren Schwachstellen, damit Patientendaten nicht kompromittiert werden können. In Gesundheitseinrichtungen gibt es zahlreiche Umgebungen und Geräte, die bei einer Fehlkonfiguration Cyberkriminellen den Zugriff auf Patientendaten ermöglichen würden. Im Gesundheitswesen sind die Kosten von Cyberangriffen wesentlich höher als in allen anderen Branchen: Eine gestohlene elektronische Patientenakte (ePA) kostet Gesundheitseinrichtungen im Durchschnitt 429 US-Dollar[8] und kann den Cyberkriminellen im Darknet zwischen 250 und 1.000 US-Dollar einbringen.[9]

Mit einem SCM-Prozess können Sie den aktuellen HIPAA-Compliance-Status jederzeit mit den Bericht- und Dashboard-Funktionen abrufen. Außerdem haben Sie die Möglichkeit, bei Audits Berichte für jeden beliebigen Zeitraum zu generieren, um die Compliance nachzuweisen. In Title II, Part 164, Subpart C, Section 164.312 des HIPAA werden verschiedene technische Anforderungen erläutert, die mit SCM erfüllt werden, zum Beispiel die Zugriffskontrolle.[10]

NERC

Die North American Electric Reliability Corporation (NERC) ist eine internationale Regulierungsorganisation, die in den USA zur Minimierung der Risiken für Stromnetze gegründet wurde. Sie entwickelt Standards fortlaufend weiter und bietet Fortbildungen, Schulungen und Zertifizierungen für Beschäftigte der Branche an.

Cybersicherheitsexperten, die Erzeugungs- und Übertragungssysteme und andere Versorgungszweige für kritische Infrastrukturen betreuen, müssen die NERC CIP-Vorgaben (Critical Infrastructure Protection) einhalten. Da die Nichteinhaltung mit bis zu einer Million US-Dollar pro Tag und pro Verstoß geahndet werden kann, verwundert es kaum, dass Stromversorger sich die NERC-Compliance einiges kosten lassen.[11]

SCM spielt insbesondere im NERC CIP Substandard 010 (*Konfigurationsänderungsmanagement und Schwachstellenanalysen)* eine wichtige Rolle. Laut dieser untergeordneten Norm sollen „nicht autorisierte Änderungen an digitalen Erzeugungs- und Übertragungssystemen erkannt und verhindert werden. Dazu werden die Anforderungen an das Konfigurationsänderungsmanagement und die Schwachstellenanalyse zum Schutz vor Manipulationen definiert, die zu Fehlern oder Ausfällen im System führen könnten".[12]

SOX

Gemäß dem US-amerikanischen Gesetz SOX (Sarbanes-Oxley Act) müssen alle börsennotierten Unternehmen interne Maßnahmen und Prozesse zur Erstellung von Finanzberichten implementieren, um das Betrugsrisiko zu minimieren. SOX schreibt keine spezifischen Maßnahmen vor, verweist aber auf das COBIT-Regelwerk (Control Objective for IT) als Leitfaden für die IT-Governance in Unternehmen.

In Bezug auf das SCM steht im COBIT DS9-Standard (Delivery and Support) Folgendes: „Verwalten Sie die Konfiguration: Um die Integrität der Hard- und Softwarekonfiguration sicherzustellen, muss ein Repository mit korrekten und vollständigen Konfigurationsdaten erstellt und gepflegt werden. Dieser Prozess umfasst eine erste Erfassung der Konfigurationsdaten, die Erstellung einer Basis-/Referenzkonfiguration (engl.: baseline), die Verifikation und Überprüfung der Konfigurationsdaten sowie die Aktualisierung des Repository der Konfigurationsdaten bei Bedarf. Ein effektives Konfigurationsmanagement unterstützt eine höhere Systemverfügbarkeit, minimiert Fehler in der Produktion und trägt zur schnelleren Behebung von Problemen bei."[13] Sie können also für SOX-Compliance sorgen, indem Sie eine COBIT-Richtlinie in Ihr SCM-Tool integrieren.

Die in diesem Kapitel aufgeführten Standards und Frameworks sind Beispiele für gängige Vorgaben, die bei einem Audit überprüft werden. Es war jedoch nicht unser Ziel, eine vollständige Liste zu erstellen.

ALLE MANN AN DECK

Kauf und Implementierung von SCM-Lösungen

Wir beenden unsere Exkursion mit einigen Tipps, die Sie beim Kauf und der Einführung einer neuen SCM-Lösung beachten sollten. Tools für das Konfigurationsmanagement gibt es schon seit einigen Jahren, daher sind hohe Erwartungen durchaus gerechtfertigt. Da Sie jetzt die Aufgaben und Prozesse des SCM kennen, sollten Sie prüfen, ob Ihre SCM-Lösung diese erfüllen kann und ob sie Möglichkeiten zur individuellen Anpassung bietet.

WAS IST EIN CHECKLISTEN-SCM-TOOL?

Ein Checklisten-SCM-Tool verfügt über einige wenige Funktionen, die ausreichen, um einen oberflächlichen Audit zu bestehen. Eventuell bietet es auch eine kleine Bibliothek mit Richtlinien zu allgemeinen Vorgaben, aber nicht für spezifische Verordnungen wie die von NIST oder PCI. Die Produkte einiger anderer Anbieter sind hingegen sehr funktionsreich, lassen sich aber nicht gut skalieren oder bieten nicht die Berichtsfunktionen an, die Ihr Unternehmen benötigt. Wählen Sie eine Lösung oder einen Anbieter aus, die bzw. der alle Ihre Anforderungen erfüllt. Ein Checklisten-Tool mit wenigen Standardoptionen reicht einfach nicht aus.

Wichtige Punkte bei der Umgebungsanalyse

Bevor Sie ein neues SCM-Tool anschaffen, sollten Sie Ihre IT- und/oder OT-Umgebung sowie die spezifischen Anforderungen genau analysieren. Dies sind einige der Punkte, die Sie berücksichtigen sollten:

» ***Hardware-Anforderungen**: Prüfen Sie sorgfältig die Hardware-Anforderungen einer SCM-Lösung, bevor Sie sie anschaffen. Ist ein kostspieliger Server erforderlich? Muss sich ein Mitarbeiter in Vollzeit darum kümmern? Stellt der Anbieter eine gehostete Lösung bereit? Es macht wenig Sinn, einen Anbieter auszuwählen, dessen Tools nur*

unter Linux ausgeführt werden können, wenn Sie überwiegend Windows-Server verwenden. Bedenken Sie auch die Skalierbarkeit: Selbst wenn Sie zu Beginn nur einige Dutzend oder Hundert Server benötigen, sollten Sie überprüfen, ob die Lösung mit Ihrem Unternehmen wachsen kann.

- ***Verteilte Umgebungen:*** *Bei großen Unternehmen befinden sich selten alle Ressourcen an einem Ort. Funktioniert die gewählte SCM-Lösung auch in einer verteilten oder hybriden Umgebung? Das ist wichtig, wenn Sie über On-Premises-, virtuelle und verschiedene cloudbasierte Ressourcen verfügen. Außerdem müssen alle gängigen Cloud-Anbieter unterstützt werden. Wenn ein Tool nur unter AWS funktioniert, Sie aber Workloads in AWS und Azure ausführen, sollten Sie weitersuchen. Nicht zuletzt sollten Sie auch darauf achten, dass Ihr SCM-Anbieter die oft sehr dynamischen Cloud-Umgebungen unterstützt.*

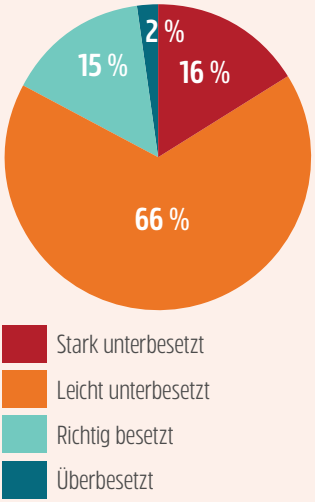
- ***Wichtige Tools von Drittanbietern****: Auf welche bereits vorhandenen Tools und Anwendungen können Sie nicht verzichten? Identifizieren Sie diese Tools und suchen Sie nach einer SCM-Lösung, die diverse Integrationsmöglichkeiten für Produkte von Drittanbietern umfasst, zum Beispiel Bedrohungsdatenquellen, Patch-Management und Ops-Anwendungen, Protokollierungs- und SIEM-Lösungen und Ticketsysteme.*

VORTEILE VERWALTETER SCM-LÖSUNGEN

Die Cybersicherheitsbranche hat seit Jahren ein großes Problem, das nichts mit Cyberkriminellen zu tun hat: den chronischen Fachkräftemangel. Er wird zu einem Risiko, wenn Stellen unbesetzt bleiben oder mit nicht ausreichend qualifizierten Mitarbeitern besetzt werden. Zudem müssen die vorhandenen Sicherheitsprofis sich über die häufig überarbeiteten Framworks und Verordnungen auf dem Laufenden halten. Eine SCM-Lösung umfasst vermutlich zeitnahe Richtlinien-Updates, aber Sie müssen sie in Ihr SCM-Programm einpflegen und anpassen. Solche grundlegenden Sicherheitsaufgaben können per Fernzugriff oder von einem Experten vor Ort erledigt werden, der zum Professional Services-Team eines Cybersicherheitsanbieters gehört. Ein Anbieter für Managed Service kann ganz auf Ihre individuellen SCM-Anforderungen eingehen.[14]

Sicherheitsteams sind weiterhin unterbesetzt

Wie würden Sie die Größe Ihres aktuellen Sicherheitsteams beschreiben?

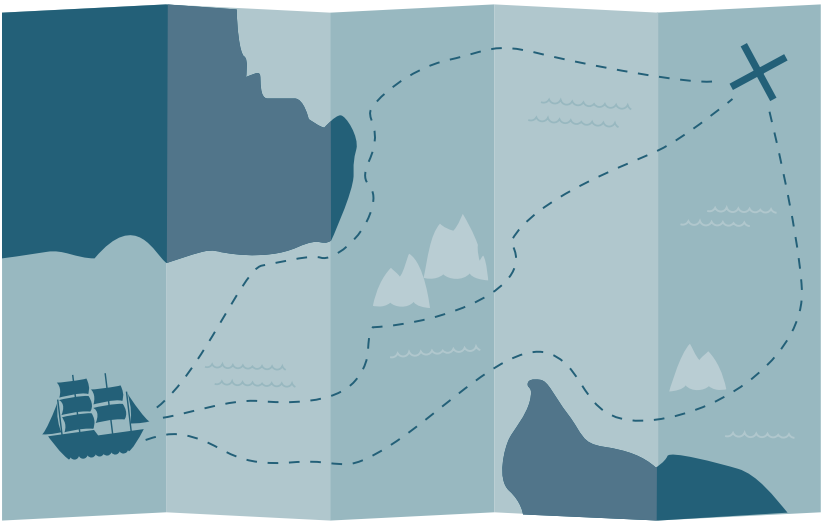


» ***Know-how Ihrer Sicherheits- und IT-Teams:*** *Berücksichtigen Sie unbedingt auch Ihre aktuellen Mitarbeiter. Kleinere Unternehmen haben vielleicht nur einige Administratoren, die verschiedene Aufgaben übernehmen müssen, unter anderem auch die Sicherheitsschulungen. Große Unternehmen haben eventuell so viele Administratoren, dass sich nicht alle am selben Ort befinden und unterschiedliche Sicherheitsgruppen nutzen. Welche Gruppe wird die SCM-Lösung verwalten? An wen sollen Compliance-Probleme gemeldet werden? Sie sollten zudem darauf achten, dass die gewählte SCM-Lösung in den vorhandenen Prozess für das Änderungsmanagement eingebunden werden kann. Andernfalls müssen Sie sich darauf einstellen, diesen anzupassen.*

10 FRAGEN AN IHREN SCM-ANBIETER

1. **Welche spezifischen Maßnahmen bieten Sie für das Endpunktmanagement an?**
   Können die Richtlinien für alle Sicherheitsmaßnahmen in der Konsole verwaltet werden?
2. **Welche Produkte, Geräte und Anwendungen werden unterstützt?**
3. **Welche Standards und/oder Benchmarks werden standardmäßig unterstützt?**
4. **Welche Berichtarten sind standardmäßig verfügbar?**
   Wie können bestimmte Berichte individuell angepasst werden?
5. **Beschäftigen Sie ein internes Forschungsteam?**
   Trägt es zur Verbesserung der Produkte bei?
6. **Wie werden externe und nur gelegentlich verbundene Geräte verwaltet?**
7. **Wo wird Ihre Managementkonsole ausgeführt?**
   Benötigen wir eine spezielle Appliance? Welche hierarchischen Managementstrukturen unterstützt die Umgebung? Wie stark lässt sich die Managementoberfläche anpassen?
8. **Welche Sicherheitsmaßnahmen haben Sie für Ihre Plattform implementiert?**
   Wird eine starke Authentifizierung unterstützt? Haben Sie einen Penetrationstests für Anwendungen auf Ihrer Konsole durchgeführt? Verwendet Ihr Entwicklerteam sichere Prozesse für die Softwareentwicklung?
9. **Welchen Umfang hat die Lösung?**
   Wie viele der jeweiligen Gerätetypen müssen von der ersten erworbenen Lizenz abgedeckt werden? Welche Hardware ist erforderlich und gibt es Skalierungsmöglichkeiten?
10. **Gibt es Professional Services und/oder Schulungen, die dem aktuellen Kenntnisstand unserer Mitarbeiter, unseren Anforderungen und unserem Budget entsprechen?**

WICHTIGE PUNKTE BEI DER BEREITSTELLUNG



Wenn Sie eine SCM-Lösung ausgewählt und die Lizenzen erworben haben, sollten Sie vor der Bereitstellung noch einige Punkte berücksichtigen. Bewerten Sie das Know-how Ihrer Mitarbeiter, um zu ermitteln, ob (und wenn ja, welche) Schulungen vor der Implementierung der SCM-Lösung notwendig sind. Überlegen Sie, ob Sie die Professional Services des Anbieters in Anspruch nehmen möchten – entweder nur für die Implementierung oder auch für die Verwaltung der Lösung per Fernzugriff. Bitten Sie den Anbieter unbedingt um einen detaillierten Projektplan und eine Leistungsbeschreibung, um die Kosten unter Kontrolle zu halten.

Wenn Sie planen, die SCM-Lösung in andere Umgebungsbereiche zu integrieren, ziehen Sie die Experten für die jeweiligen Lösungen hinzu. Der Projektplan und die Leistungsbeschreibung müssen auch die Anforderungen für diese Integrationen beinhalten.

Informieren Sie sich über die Hardwareanforderungen des SCM-Tools. Sorgen Sie dafür, dass die Hardware zur Verfügung steht, wenn das Professional Services-Team eintrifft, um zusätzliche Reisekosten und Spesen zu vermeiden. Vergewissern Sie sich, dass Sie die Port- und Serviceanforderungen der Lösung kennen. Arbeiten Sie eng mit dem Netzwerkteam zusammen, damit diese Anforderungen erfüllt werden.

DER TRIPWIRE-ANSATZ FÜR SCM

Tripwire bietet vollständig integrierte Lösungen für das Richtlinienmanagement, das Monitoring der Dateiintegrität und die Fehlerbehebung. Mit einem umfassendes SCM-Programm von Tripwire können Unternehmen dringende aktuelle Herausforderungen im Bereich Sicherheit und Compliance bewältigen und gleichzeitig eine solide Basis für zukünftige Anforderungen schaffen.

Tripwire hat eine der größten und vielfältigsten Bibliotheken mit unterstützten Richtlinien und Plattformen: mehr als 2.000 Richtlinien für verschiedenste Betriebssystemversionen und Geräte. Sie erhalten einen detaillierten Überblick über die Sicherheitsmaßnahmen und können jederzeit den aktuellen Sicherheitsstatus abrufen. Die Fehlerbehebungsfunktion von Tripwire automatisiert die wichtigsten Schritte und führt Sie durch die schnelle Korrektur von Fehlkonfigurationen.

TRIPWIRE® ENTERPRISE

Tripwire® Enterprise ist eine Suite integrierter Lösungen, die branchenführendes FIM und SCM kombiniert, um Sicherheitsteams Echtzeitdaten zu Änderungen und Bedrohungen bereitzustellen. Gleichzeitig profitieren Compliance-Beauftragte von Funktionen für die automatisierte Durchsetzung von Compliance-Maßnahmen und zur Stärkung der Sicherheitsinfrastruktur. Damit ersparen Sie sich zusätzliche Audit-Runden und die damit verbundenen Kosten. Tausende Unternehmen haben ihr Cybersicherheitsprogramm auf Tripwire Enterprise aufgesetzt.

TRIPWIRE® CONFIGURATION MANAGER

Tripwire Configuration Manager bietet die Möglichkeit, die Konfigurationsüberwachung auf Cloud-Konten und -Ressourcen in Amazon Web Services (AWS), Microsoft Azure und Lösungen anderer Cloud-Anbieter auszudehnen – alles in einer übersichtlichen Konsole. Die Konfigurationsregeln können automatisch durchgesetzt werden und Fehlkonfigurationen lassen sich anhand der Risikoeinschätzung priorisieren, damit sich das Sicherheitsteam zuerst auf die schwerwiegendsten Probleme konzentrieren kann.

TRIPWIRE® EXPERTOPS

Tripwire ExpertOps℠ SCM bietet cloudbasierte Managed Services für das branchenführende SCM. Mit einem einzigen Abonnement erhalten Sie individuelle Beratung durch Experten und praktische Unterstützung bei dem Tool-Management, um Compliance-Vorgaben zu erfüllen und geschäftskritische Ressourcen besser zu schützen.

TRIPWIRE® INDUSTRIAL VISIBILITY

Tripwire Industrial Visibility bietet Betreibern industrieller Steuersysteme einen umfassenden Überblick über die Geräte und Aktivitäten in ihrem Netzwerk. Dank des Änderungsmanagements, der Ereignisprotokollierung und den Bedrohungsmodellen können Sie Ihre sensiblen Ressourcen vor Angriffen schützen.

SIE MÖCHTEN GERN MEHR ERFAHREN?

DANN LADEN SIE DAS
TRIPWIRE ENTERPRISE-DATENBLATT
HERUNTER ODER VEREINBAREN SIE EINE
PRODUKTVORFÜHRUNG.

www.tripwire.com

THE STATE OF SECURITY
tripwire.com/blog

@tripwireinc

AUTOREN

Chris Orr

Chris Orr ist seit September 2000 bei Tripwire beschäftigt. Er war zuerst für die Entwicklung und Präsentation von Schulungsmaterialien zu bewährten Lösungen wie Tripwire for Servers und Tripwire for Routers zuständig, wechselte aber schon bald in die Sales Engineering Group, der er auch heute noch angehört. Ursprünglich bot er technische Beratung in 27 Bundesstaaten und für alle US-amerikanischen Bundesbehörden an. Da unser Kundenstamm gewachsen ist, ist er nun nur noch für die Regionen westlich des Mississippi, aber damit immer noch für die geografisch größte Region des Unternehmens, zuständig. Wenn er nicht gerade zu so hübschen Orten wie Winnipeg oder Boise fliegt, bringt er im malerischen Lake Stevens, Washington, seiner Tochter das Gitarrespielen bei oder unternimmt Ausflüge mit seinem Sohn.

Steve Marriner

Steve Marriner ist Principal der Yosemite Group. Er hat in den letzten 30 Jahren umfassende Erfahrungen im System-, Anwendungs- und Cybersicherheitsbereich gesammelt. Marriner hat führende Unternehmen in der Sicherheitsbranche, darunter Tripwire, Voltage Security und Iovation, in den Bereichen Produktmanagement, Marketing und Strategie beraten. Er hat einen BS-Abschluss in Mathematik und Informatik von der University of Connecticut und einen MBA von der Stanford University.

Tim Erlin

Tim Erlin ist VP of Product Management & Strategy bei Tripwire und Moderator des Tripwire-Podcasts *Talking Cybersecurity*. Zuvor war er für das Schwachstellenmanagement in der Tripwire-Produktfamilie zuständig. Aufgrund seiner Arbeit als Vertriebsingenieur kennt er sich auf den Märkten aus und nutzt sein Know-how in seiner Rolle als Führungskraft und Produktmanager für verschiedene Produkte. Seine Karriere in der Informationstechnologie begann im Projektmanagement, im Kundenservice und in der System- und Netzwerkadministration. Erlin bringt sich mit Blogs, Podcasts, Artikeln sowie öffentlichen Vorträgen und Fernsehauftritten aktiv in die Informationssicherheits-Community ein.

Quellen

1. Johnson, Arnold, et al.: „Guide for Security-Focused Configuration Management of Information Systems", *NIST*, 31. Okt. 2019
2. „2019 Data Breach Investigations Report", *Verizon Enterprise*, 2019
3. „CIS Control 12: Boundary Defense", *CIS*, www.cisecurity.org/controls/boundary-defense/
4. „2019 Cost of a Data Breach Report: *IBM Security*", IBM Security, 2019, databreachcalculator.mybluemix.net/
5. „CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers", *CIS*, www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/
6. „Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)", *NIST CSRC*, 16. Mär. 2020, csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
7. Strom, Blake E., et al.: „MITRE ATT&CK™: Design and Philosophy", *The MITRE Corporation*, 11. Okt. 2019, www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
8. Davis, Jessica: „Data Breaches Cost Healthcare $6.5M, or $429 Per Patient Record", *HealthITSecurity*, HealthITSecurity, 23. Juli 2019, healthitsecurity.com/news/data-breaches-cost-healthcare-6.5m-or-429-per-patient-record
9. Columbus, Louis: „5 Strategies Healthcare Providers Are Using To Secure Networks", *Forbes*, Forbes Magazine, 20. Okt. 2019, www.forbes.com/sites/louiscolumbus/2019/10/20/5-strategies-healthcare-providers-are-using-to-secure-networks/#3299f9954b40
10. „45 CFR § 164.312 – Technical Safeguards", *Cornell Law School*, Legal Information Institute, www.law.cornell.edu/cfr/text/45/164.312
11. „NERC Compliance Regulations & Requirements", *Compliance Guidelines*, 2020, complianceguidelines.com/nerc-compliance.htm
12. „CIP-010-1", NERC, 2020, www.nerc.com/pa/Stand/Pages/CIP0101RI.aspx
13. Tripwire Inc., *„Sustaining SOX Compliance"*, www.tripwire.com/solutions/compliance-solutions/sox-it-compliance/sustaining-sox-compliance-register
14. Tripwire Inc., „2020 *Cybersecurity Skills Gap Survey"*, www.tripwire.com/misc/skills-gap-survey-2019-register/

OPTIMALES KONFIGURATIONSMANAGEMENT

Moderne Unternehmen verwenden nicht mehr nur konventionelle On-Premises-Rechenzentren. Die Sicherheitsteams müssen daher eine Angriffsfläche verteidigen, die durchlässig ist, keine wirkliche Grenze hat und sich zudem ständig vergrößert.

Das Security Configuration Management (SCM) ist eine wichtige Sicherheitsmaßnahme, die den Status der Ressourcen überwacht und (versehentliche oder absichtliche) Abweichungen von den festgelegten Einstellungen meldet.

In diesem Leitfaden sehen wir uns Praxisbeispiele für SCM zu Sicherheits- und Compliance-Zwecken an und Sie erfahren, wie Sie die größten Herausforderungen in Bezug auf Konfigurationen meistern.