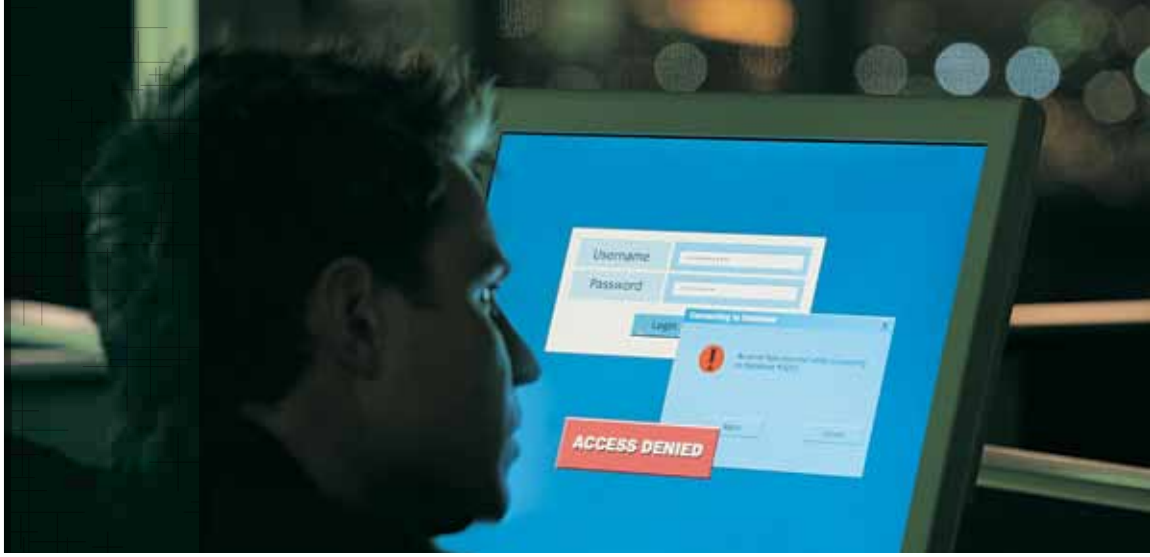
McAfee
An Intel Company

VERWALTUNG VON SICHERHEIT UND RISIKEN

Lösungsleitfaden



Security Connected

Das Security Connected-Framework von McAfee ermöglicht die Integration verschiedener Produkte, Services und Partnerschaften zur zentralen, effizienten und effektiven Risikominimierung. Der Security Connected-Ansatz greift auf mehr als zwei Jahrzehnte bewährter Sicherheitspraktiken zurück und unterstützt Unternehmen aller Größen und Bereiche weltweit bei der Verbesserung ihrer Sicherheitslage, Optimierung der Kosteneffizienz von Sicherheitsmaßnahmen sowie der strategischen Anpassung der Sicherheit an Unternehmens-initiativen. Die Referenzarchitektur für Security Connected bietet einen sicheren Pfad von der ursprünglichen Idee bis zur tatsächlichen Implementierung. Durch ihren Einsatz können Sie die Security Connected-Konzepte an Ihre speziellen Risiken sowie an die Infrastruktur und die Geschäftsziele anpassen. McAfee ist stets auf der Suche nach neuen Möglichkeiten, um seine Kunden umfassend zu schützen.

Laden Sie die neuesten Ressourcen herunter: www.mcafee.com/de/enterprise/reference-architecture/index.aspx.

Gehen Sie das Risiko-Management proaktiv an

Herausforderungen

Compliance und finanzielle Risiken sind die klassischen Hauptsorgen beim Sicherheits- und Risiko-Management. Mit Audits und Compliance-Gewährleistungsprozessen versuchen IT-Verantwortliche, Risiken zu minimieren und den Schutz zu automatisieren. Risiken waren einst relativ statisch. Heute erfolgen Angriffe jedoch entweder langsam und unauffällig (bei gezielten Angriffen) oder blitzschnell (bei Cyber-Aktivismus und Malware-Ausbrüchen), sodass Führungskräfte und IT-Administratoren Ereignissen mehr Aufmerksamkeit widmen und zur Problembehebung schnelle Risiko-orientierte Entscheidungen treffen müssen.

Compliance und finanzielle Risiken sind natürlich ebenfalls dynamisch geworden. Dabei passen Regulierungsbehörden unabhängig voneinander weltweit mehr als 200 Vorschriften an die sich immer weiter verändernden Geschäftsgepflogenheiten an. Das einst statisch wirkende Risikobild ist nun ähnlich wie ein Kaleidoskop in ständiger Bewegung.

Analyse umfangreicher Sicherheitsdaten

Zur Risikoverwaltung müssen heute viele Daten analysiert werden: Schwachstellen-Scans, Anwendungs- und Datenbank-Protokolle, Datenflüsse, Zugriffs- und Sitzungsdaten, Warnmeldungen und Trend-Analysen. Die Datenströme stammen dabei aus verschiedenen Systemen und schützen mehr Benutzer mit mehr Geräten an mehr Orten.

Sowohl interne als auch externe Audits sind ein typisches Beispiel für den hohen Aufwand, der zur Verwaltung dieser Datenfülle betrieben wird. IT-Administratoren müssen Datenstromereignisse erfassen und in einem bestimmten Format zusammenführen, damit sie von Prüfern ausgewertet werden können. Das Augenmerk der Prüfer ist per Definition rückwärts gerichtet, da nur eine statische Analyse vergangener Risiken möglich ist. Sie durchforsten Organisations-Ressourcen und vernachlässigen dabei das präventive Risiko-Management, d. h. die Möglichkeiten, vorauszuschauen sowie die sich verändernden Risiken zu erkennen und zu beseitigen, bevor sie Schaden anrichten.

Risikobewertung

In der heutigen Welt haben wir es mit Big Data zu tun – mit umfangreichen Sicherheitsdaten. Bis zur Erkennung subtiler Sicherheitsbedrohungen können mehrere Tage oder sogar Monate vergehen. Die Datenprobleme der meisten Sicherheits-analysten sind vergleichbar mit den Schwierig-keiten, die IT-Administratoren bei der Umsetzung von Audits haben: Aufgrund der Fülle unabhängiger Datenströme ist es schwierig, sich ein einheitliches und verständliches Bild der Ereignisse zu verschaffen. Je mehr Daten erfasst und analysiert werden, desto chaotischer erscheinen sie und desto länger dauert es, Ereignisketten zu rekonstruieren. Erst das vollständige Bild erlaubt es, (lange nach dem tatsächlichen Ereignis) Richtlinien und Schutzmaßnahmen anzupassen, um eine Wiederholung zu verhindern.

Doch was geschieht, wenn die Attacke schnell und heftig erfolgt – wie bei einem Denial-of-Service-Angriff oder einem sich schnell ausbreitendem Wurm? Wenn die Diagnose Tage oder gar Monate in Anspruch nimmt, können die Auswirkungen des Problems auf die Compliance und die Finanzen erheblich, möglicherweise sogar für das Unternehmen „tödlich“ sein. Welche Ressourcen sind tatsächlich gefährdet und welche durch kompensierende Kontrollen oder Gegenmaßnahmen geschützt? Um diese Frage beantworten zu können, benötigen Administratoren einen Überblick über die Sicherheitslage aller Systeme, einschließlich der wachsenden Anzahl mobiler und privater Mitarbeitergeräte, die auf die Unternehmensnetzwerke zugreifen.

Reaktion auf Ereignisse

Nach der Erkenntnis folgen Auswahl und Problem-behebung. Welche Ressourcen sind am wertvollsten? Welche können warten? Administratoren nutzen häufig verschiedene Verwaltungskonsolen zur Scan-Durchführung, Skript-Ausführung, Update-Installation oder Systemisolierung. Jedes auf dem Sicherheitsmarkt erhältliche Produkt erhöht durch eigene Benutzeroberflächen, Datenformate, Richtlinienstandards oder Berichte die Kosten sowie die Komplexität. So kommt es unweigerlich zu Schutzlücken und Fehlern, die das Unternehmen und seine Ressourcen unnötig – und meist unerkannt – verwundbar machen.

Sie können Risiken nicht mehr über den Blick aus dem Rückspiegel verwalten. Sie müssen – mit einem Weitwinkelobjektiv – nach vorn schauen, um die sich verändernden Risiken erkennen und verwalten zu können. Situationsbezogene Risikodaten legen den dynamischen Kontext innerhalb der globalen Bedrohungsumgebung sowie die Sicherheitslage Ihrer Unternehmens-Ressourcen offen. Automatisierte Risiko-Management-Technologien nutzen diesen Kontext und unterstützen Sie dabei, Ihre Richtlinien und Schutzmaßnahmen zu optimieren.

Lösungen

Umfangreiche Sicherheitsdaten und die damit verbundenen Handhabungsprobleme verkomplizieren das Sicherheits- und Risiko-Management. Eine umfassende Strategie in Verbindung mit moderner Technologie kann jedoch Ordnung in das Chaos bringen. Im Rahmen von Compliance- und Finanzrisiko-Management-Prozessen müssen Sie in Echtzeit die potenziellen Risiken abwägen, die durch externe und interne Ereignisse auftreten. Durch die Zentralisierung dieser Tätigkeiten lassen sich die Prozesse optimieren und automatisierte Reaktionen einrichten, durch die Kosten und Reaktionszeit verringert werden können. Führungskräfte erhalten Einblick in die potenziellen Auswirkungen von Sicherheitsereignissen auf die Risikolage, während Administratoren neben dem Überblick auch die Möglichkeit erhalten, Risiken proaktiv zu beseitigen.

Moderne Systeme zum Sicherheitsinformations- und Ereignis-Management (SIEM) arbeiten eng mit Systemen zum Sicherheits- und Compliance-Management für Geräte, Server, Netzwerke, Anwendungen und Datenbanken zusammen. Diese Sicherheits-Management-Plattform stellt eine Befehls- und Kontrollzentrale dar, die Transparenz und operative Flexibilität ermöglicht. Je enger diese Systeme miteinander sowie mit Risikodaten und Sicherheitssystemen integriert sind, desto einfacher können Sie Risiken erkennen und verwalten. Durch den Plattformansatz werden einzelne und fragmentierte Prozesse, Richtlinien, Arbeitsabläufe sowie Berichte aneinander angepasst und vereinheitlicht. Dank der Einbeziehung aktueller Bedrohungsdaten können die Daten in den Kontext der sich verändernden Risiken gesetzt werden, wodurch Genauigkeit und Relevanz verbessert sowie die zur Minimierung des Risikos erforderliche Reaktionszeit verringert wird.

Schwachstellenanalyse

Die meisten regulierten Organisationen suchen nach Schwachstellen, um Compliance-Anforderungen einzuhalten. Bei den geplanten Scans werden jedoch häufig außerhalb der Organisation verwendete oder nicht aktive Systeme ausgelassen oder geschäftskritische Ressourcen wie Anwendungen und Datenbanken umgangen. Nicht autorisierte Systeme, die möglicherweise ausnutzbare Schwachstellen enthalten, können so übersehen werden. Durch einen gewissenhaften Ansatz bei der Schwachstellenverwaltung aller Ressourcen, die über das Netzwerk verbunden sind, können Sie die vielfältigen Systeme einbeziehen und Compliance-Lücken schließen. Sie können dynamische Risikodaten, Ressourcen-Werte und relevante Gegenmaßnahmen nutzen, um gezielte Scans durchzuführen oder kompensierende Kontrollen zu implementieren.

Verbesserter Überblick über die aktuelle Sicherheitslage

In Anbetracht von Internetangriffen und durchlässigen Netzwerkgrenzen wollen die meisten Unternehmen die sich verändernden Risiken besser verstehen und effektiver darauf reagieren. Der entscheidende Punkt dabei: Sie müssen die entscheidenden Daten dann finden, wenn sie entscheidend sind. Dank der Geschwindigkeit und der Kapazität, mit der SIEM-Tools umfangreiche Sicherheitsdaten verarbeiten können, lassen sich Anwendungen und Datenbanken überwachen, Protokolle verwalten und Ereignisse in korrelierte Dashboards normalisieren. Einige ermöglichen zudem einen Echtzeitüberblick über die Bedrohungslage sowie über Benutzer, Systeme, Daten, Risiken und Gegenmaßnahmen. Mithilfe dieses hilfreichen Kontextabbilds können Sie sicherheitsrelevante sowie vergangene Aktivitäten schnell erfassen. Zuverlässige Analyse-Tools unterstützen Sie bei der Vorhersage und Lokalisierung von Angriffen sowie bei der Behebung von Bedrohungen innerhalb von Minuten anstatt Tagen.

Blick in den Netzwerkverkehr

Netzwerke stellen eine kritische Infrastruktur, gleichzeitig jedoch auch Kanäle dar, über die sensible und regulierte Daten das Unternehmen verlassen können. Durch die Überwachung und Verwaltung des Netzwerkverkehrs (einschließlich des verschlüsselten Verkehrs) können Administratoren unerwünschte oder riskante Internet- und Anwendungsnutzung minimieren sowie sicherstellen, dass Inhaltsrichtlinien umgesetzt werden. Dank der Integration von Netzwerksicherheitsmaßnahmen der nächsten Generation in SIEM und Systemsicherheit können Risiko-Manager Richtlinien erzwingen, vor Zero-Day-Bedrohungen schützen sowie Compliance überwachen, analysieren und dokumentieren.

Optimierung der Protokollverwaltung

Protokolle enthalten vielfältige Daten, die für E-Discovery, Audits und andere Compliance-Anforderungen verwendet werden können – sofern Sie diese Datenströme so erfassen und auslesen können, dass die Fakten für Sie erkennbar sind. Mit einer integrierten, sicheren und leistungsstarken Protokollverwaltungslösung können Sie die Daten aus allen relevanten Quellen in Echtzeit erfassen und die Protokolle anschließend speichern, um eine sichere Kontrollkette zu gewährleisten. Mit Anwendungskontrollen können Sie sicherstellen, dass Anwender keine Protokollierungssysteme kapern können, um ihre Aktionen zu verbergen. Durch die Verbindung von Protokollverwaltungsfunktionen mit anderen Sicherheits- und Risiko-Analysefunktionen erhalten diejenigen Spezialisten Protolldaten, die damit am besten Risiken verwalten können.

Empfehlenswerte Vorgehensweisen

- Vereinheitlichen Sie fragmentierte Prozesse und Kontrollen, und stimmen Sie sie aufeinander ab.
- Automatisieren Sie die Erfassung, Korrelation, Analyse, Reaktion und Überwachung.
- Nutzen Sie dynamische Risikodaten, „Was-wäre-wenn"-Analysen (What-if Analysis) und richtlinienbasierte Reaktionen, um Bedrohungen proaktiv zu erkennen und zu blockieren.
- Stellen Sie sicher, dass Sicherheits- und Risikoanalyseprogramme alle Geräte und Daten sowie die IT-Infrastruktur abdecken.
- Zentralisieren Sie alle Sicherheits- und Risikoinformationen des Unternehmens in einer Plattform, um die Verwaltung effizienter und effektiver zu gestalten.
- Überwachen Sie die Situationen kontinuierlich, und suchen sowie reagieren Sie proaktiv auf sich verändernde Risiken, um die Compliance aufrecht zu erhalten und zukünftige Sicherheitsereignisse zu vermeiden.

Manuelle Sicherheits- und Risikoprozesse bergen mit größerer Wahrscheinlichkeit Fehler und sind die Hauptursache für zu hohe Sicherheits- und Compliance-Kosten.

Wertsteigernde Faktoren

Eine von einer risikobewussten, automatisierten Verwaltungsplattform gestützte umfassende Sicherheits- und Risiko-Management-Strategie bietet folgende Vorteile:

- Sie erhalten dank zahlreicher Kontext- und Analysedateien einen hilfreichen Überblick über die Situation.
- Die Diagnose und Reaktion auf Zwischenfälle erfolgt in Sekunden statt Stunden, wodurch Schäden minimiert, Datenkompromittierungen verhindert und Problembehebungskosten gesenkt werden.
- Die Anzahl der Sicherheits- und Compliance-Zwischenfälle geht zurück, und die Kosten pro Zwischenfall sinken.
- Compliance-Richtlinienprozesse sowie die Berichterstellung werden vereinfacht und damit die Effizienz verbessert.
- Die Menge der Anbieter-Plattformen sowie der Hard- und Software-Versionen, die für die Sicherheitsverwaltung benötigt werden, wird reduziert.
- Die Schulungszeiten und Betriebskosten sinken.

Dazugehöriges Material aus der McAfee Security Connected-Referenzarchitektur

Stufe II

- Kontrolle und Überwachung von Änderungen
- Schutz des Rechenzentrums
- Vorteile von PCI

Stufe III

- Schwachstellenanalyse
- Verbesserter Überblick über die aktuelle Sicherheitslage
- Blick in den Netzwerkverkehr
- Optimierung der Protokollverwaltung
- Untersuchung von Datenkompromittierungen
- Leben mit sozialen Medien
- Schutz geistigen Eigentums

Weitere Informationen zur Security Connected-Referenzarchitektur finden Sie unter: www.mcafee.com/de/enterprise/reference-architecture/index.aspx.

Informationen zum Autor

Barbara G. Kay ist zertifizierte IT-Sicherheitsspezialistin (Certified Information Systems Security Professional, CISSP) und leitende Branchenanalystin der Secure By Design Group. Ihr Spezialgebiet liegt im Informationsschutz für verteilte und mobile Unternehmen sowie in der Benutzerschulung zur sicheren Internetnutzung. Vor der Gründung von Secure By Design im Jahr 2006 war Kay Marketingleiterin der Security and Privacy Initiative von Sun. Sie hat einen Abschluss am Dartmouth College.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de