IBM Security QRadar Risk Manager
Version 7.2.2

Erste Schritte

GI13-3917-00

IBM Security QRadar Risk Manager
Version 7.2.2

Erste Schritte

GI13-3917-00

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 33 gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security QRadar Risk Manager, Version 7.2.2, Getting Started,
IBM Form GI13-4112-00,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
März 2014

Inhaltsverzeichnis

Einführung zu IBM Security QRadar Risk Manager

Diese Informationen beziehen sich auf die Verwendung von IBM® Security QRadar Risk Manager. QRadar Risk Manager ist eine Appliance zum Überwachen von Einheitenkonfigurationen, Simulieren von Änderungen an der Netzumgebung und Priorisieren von Risiken und Schwachstellen im Netz.

Zielgruppe

Dieses Handbuch richtet sich an Netzadministratoren, die für die Installation und Konfiguration von QRadar Risk Manager-Systemen in einem Netz verantwortlich sind.

Technische Dokumentation

Informationen für den Zugriff auf weitere technische Dokumentation, technische Hinweise und Releaseinformationen finden Sie unter Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Kontaktaufnahme mit der Kundenunterstützung

Informationen für die Kontaktaufnahme mit der Kundenunterstützung finden Sie unter Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unzulässigen Zugriff innerhalb des Unternehmens und von außen. Unzulässiger Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unzulässige Verwendung oder einen unzulässigen Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

Kapitel 1. Einführung zu IBM Security QRadar Risk Manager

IBM Security QRadar Risk Manager ist eine separat installierte Appliance. Sie können QRadar Risk Manager zum Überwachen von Einheitenkonfigurationen, Simulieren von Änderungen an der Netzumgebung und Priorisieren von Risiken und Schwachstellen im Netz verwenden.

Der Zugriff auf QRadar Risk Manager erfolgt über die Registerkarte **Risks** (Risiken) in der IBM Security QRadar SIEM-Konsole.

QRadar Risk Manager erweitert die Funktionen von QRadar SIEM, indem es den Administratoren Tools für folgende Aufgaben bereitstellt:

- Zentrales Risikomanagement
- Topologiebasierte Ansicht des Netzes
- Konfiguration und Überwachung der Netzeinheiten
- Ansicht der Verbindungen zwischen Netzeinheiten
- Suche nach Firewallregeln
- Ansicht vorhandener Regeln und Ereigniszählung für ausgelöste Regeln
- Suche nach Einheiten und den Pfaden von Netzeinheiten
- Überwachung und Audit des Netzes auf Konformität
- Definition, Planung und Ausführung von Exploitsimulationen im Netz
- Suche nach Schwachstellen

Für zentrales Risikomanagement und Konformitätsüberwachung zur verstärkten Informationsbeschaffung kann die Zusammenarbeit vieler interner Teams erforderlich sein. Bei der SIEM-Version der nächsten Generation mit zusätzlicher Risikomanagement-Appliance verringert sich die Anzahl der Schritte, die bei SIEM-Produkten der ersten Generation noch erforderlich waren. Die Software ermöglicht die Netzwerktopologie- und Risikobewertung für Assets, die in QRadar SIEM verwaltet werden.

Während des Bewertungsprozesses werden System, Sicherheit, Risikoanalyse und Netzinformationen durch Aggregation und Korrelation konsolidiert, sodass Sie einen uneingeschränkten Einblick in Ihre Netzumgebung erhalten. Darüber hinaus wird ein Portal zu Ihrer Umgebung definiert, das einen umfassenden Einblick in das System ermöglicht, und dies mit einer Effizienz, die durch manuelle Prozesse oder Einzelproduktechnologien nicht zu erreichen ist.

Kapitel 2. IBM Security QRadar Risk Manager implementieren

Die QRadar Risk Manager-Appliance wird mit der neusten Softwareversion von QRadar Risk Manager installiert.

Zunächst muss die Bewertungs-Appliance IBM Security QRadar Risk Manager installiert werden. Sie müssen die Software aktivieren und der QRadar Risk Manager-Appliance eine IP-Adresse zuweisen.

Wenn Sie beim Aktivieren der Software oder Zuweisen einer IP-Adresse Hilfe benötigen, wenden Sie sich an die Kundenunterstützung.

Danach kann die Appliance Informationen von den Netzeinheiten erfassen.

Informationen zum Verwenden von IBM Security QRadar Risk Manager finden Sie im Handbuch *IBM Security QRadar Risk Manager User Guide*.

Damit QRadar Risk Manager in Ihrer Umgebung implementiert werden kann, müssen folgende Voraussetzungen erfüllt sein:

1. Stellen Sie sicher, dass die neuste Version von IBM Security QRadar SIEM installiert ist.
2. Stellen Sie sicher, dass alle Installationsvoraussetzungen erfüllt sind.
3. Richten Sie die QRadar Risk Manager-Appliance ein und schalten Sie sie ein.
4. Installieren Sie das Plug-in für QRadar Risk Manager auf der QRadar SIEM-Konsole.
5. Richten Sie die Kommunikation zwischen QRadar SIEM und der QRadar Risk Manager-Appliance ein.
6. Definieren Sie Benutzerrollen für die QRadar Risk Manager-Benutzer.

Installationsvorbereitung

Vor der Installation von IBM Security QRadar Risk Manager muss die Installation einer IBM Security QRadar SIEM-Konsole abgeschlossen sein. Es hat sich bewährt, QRadar SIEM und QRadar Risk Manager auf demselben Netzswitch zu installieren.

Beachten Sie die Informationen in folgenden Abschnitten:

- Firewall-Port-Zugriff konfigurieren
- Netzeinstellungen ermitteln
- Nicht unterstützte Funktionen in QRadar Risk Manager
- Unterstützte Web-Browser

Vergewissern Sie sich vor der Installation der Bewertungs-Appliance IBM Security QRadar Risk Manager, dass folgende Voraussetzungen erfüllt sind:

- Platz für eine aus zwei Einheiten bestehende Appliance
- Bereits montierte Rackschienen und Baugruppenrahmen

Optional können Sie eine USB-Tastatur und einen standardmäßigen VGA-Monitor für den Zugriff auf die QRadar SIEM-Konsole verwenden.

Portzugriff auf Firewalls konfigurieren

Firewalls, die zwischen der IBM Security QRadar SIEM-Konsole und IBM Security QRadar Risk Manager bestehen, müssen den Datenverkehr über bestimmte Ports zulassen.

Stellen Sie sicher, dass jegliche Firewalls, die zwischen der QRadar SIEM-Konsole und QRadar Risk Manager bestehen, den Datenverkehr über die folgenden Ports zulassen:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time Protocol)

Netzeinstellungen ermitteln

Bevor Sie mit dem Installationsprozess beginnen, müssen Sie Informationen zu den Netzeinstellungen ermitteln.

Stellen Sie folgende Informationen zu den Netzeinstellungen zusammen:

- Hostname
- IP-Adresse
- Netzmaskenadresse
- Teilnetzmaske
- Standardgateway-Adresse
- DNS-Serveradresse (Primary Domain Name System)
- Adresse des sekundären DNS-Servers (optional)
- Öffentliche IP-Adresse für Netze, die NAT-E-Mail-Servernamen (Netzadressumsetzung, NAT) verwenden
- E-Mail-Servername
- Name des NTP-Servers (Network Time Protocol) (nur Konsole) oder des Zeitservers

Nicht unterstützte Funktionen in QRadar Risk Manager

Es ist wichtig, dass Ihnen die Funktionen bekannt sind, die von IBM Security QRadar Risk Manager nicht unterstützt werden.

Folgende Funktionen werden in QRadar Risk Manager nicht unterstützt:

- Hochverfügbarkeit
- Dynamisches Routing für das Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) oder Routing Information Protocol (RIP)
- IPv6
- Nicht zusammenhängende Netzmasken
- Routen mit Lastausgleich
- Referenzzuordnungen
- Store-and-forward-Verfahren

Unterstützte Web-Browser

Damit die Funktionen in IBM Security QRadar ordnungsgemäß ausgeführt werden können, müssen Sie einen unterstützten Web-Browser verwenden.

Beim Zugriff auf das QRadar-System werden Sie zur Eingabe eines Benutzernamens und eines Kennworts aufgefordert. Der Benutzername und das Kennwort müssen vorher vom Administrator konfiguriert werden.

In der folgenden Tabelle werden die unterstützten Versionen der Web-Browser aufgeführt.

Tabelle 1. Unterstützte Web-Browser für QRadar-Produkte

Web-Browser	Unterstützte Version
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32-Bit-Microsoft Internet Explorer, mit aktiviertem Dokumentmodus und Browsermodus	9.0
Google Chrome	Die aktuelle Version ab dem Freigabedatum für IBM Security QRadar V7.2.2-Produkte

Dokumentmodus und Browsermodus im Internet Explorer aktivieren

Wenn Sie Microsoft Internet Explorer zum Zugriff auf IBM Security QRadar-Produkte verwenden, ist die Aktivierung der Optionen 'Dokumentmodus' und 'Browsermodus' erforderlich.

Vorgehensweise

1. Drücken Sie in Ihrem Internet Explorer-Web-Browser F12, um das Fenster **Developer Tools** (Entwickler-Tools) zu öffnen.
2. Klicken Sie auf **Browsermodus** und wählen Sie Ihre Web-Browser-Version aus.
3. Klicken Sie auf **Dokumentmodus**.
   - Wählen Sie für Internet Explorer V9.0 **Internet Explorer 9** aus.
   - Wählen Sie für Internet Explorer V8.0 **Internet Explorer 7.0 Standards** aus.

Zugriff auf die Benutzerschnittstelle von IBM Security QRadar Risk Manager

In IBM Security QRadar Risk Manager werden standardmäßige Anmeldeinformationen für die URL, den Benutzernamen und das Kennwort verwendet.

Der Zugriff auf IBM Security QRadar Risk Manager erfolgt über die QRadar SIEM-Konsole. Verwenden Sie bei der Anmeldung an der IBM Security QRadar SIEM-Konsole die Informationen in der folgenden Tabelle.

Tabelle 2. Standardmäßige Anmeldeinformationen für QRadar Risk Manager

Anmeldeinformationen	Standardwert
URL	https://<IP-Adresse>; dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
Benutzername	admin
Kennwort	Das Kennwort, das QRadar Risk Manager während des Installationsprozesses zugewiesen wurde.
Lizenzschlüssel	Ein standardmäßiger Lizenzschlüssel ermöglicht 5 Wochen lang Zugriff auf das System.

QRadar Risk Manager-Appliance einrichten

Sie müssen die Managementschnittstelle anschließen und sicherstellen, dass die Netzkabel in die QRadar Risk Manager-Appliance eingesteckt sind.

Vorbereitende Schritte

Voraussetzungen lesen und umsetzen.

Informationen zu diesem Vorgang

Die Bewertungs-Appliance IBM Security QRadar Risk Manager ist ein aus zwei Einheiten bestehender Einschubserver. Rackschienen und Baugruppenrahmen gehören nicht zum Lieferumfang der Bewertungs-Appliance.

Die QRadar Risk Manager-Appliance umfasst vier Netzschnittstellen. Verwenden Sie für diese Bewertungs-Appliance die Netzschnittstelle mit der Kennzeichnung 'ETH0' als Managementschnittstelle. Die anderen Schnittstellen sind Überwachungsschnittstellen. Alle Schnittstellen befinden sich an der Abdeckung auf der Rückseite der QRadar Risk Manager-Appliance.

Der Netzschalter befindet sich an der Abdeckung auf der Vorderseite der Appliance.

Vorgehensweise

1. Schließen Sie die Netzmanagementschnittstelle an den Port mit der Kennzeichnung 'ETH0' an.
2. Vergewissern Sie sich, dass die Netzkabel in die zugehörigen Anschlüsse auf der Rückseite der Appliance eingesteckt sind.
3. Optional: Für den Zugriff auf die QRadar SIEM-Konsole müssen eine USB-Tastatur und ein standardmäßiger VGA-Monitor angeschlossen werden.
4. Wenn an der Vorderseite der Appliance eine Abdeckung vorhanden ist, entfernen Sie diese Abdeckung, indem Sie die Laschen auf einer Seite eindrücken und die Abdeckung von der Appliance weg ziehen.
5. Drücken Sie den Netzschalter auf der Vorderseite, um die Appliance einzuschalten.

Ergebnisse

Die Appliance startet den Bootprozess.

QRadar Risk Manager zu QRadar SIEM hinzufügen

Sie müssen IBM Security QRadar Risk Manager als verwalteten Host zu IBM Security QRadar SIEM hinzufügen.

Vorbereitende Schritte

Wenn Sie die Komprimierung aktivieren möchten, muss jeder verwaltete Host mindestens den Versionsstand QRadar SIEM 7.1 oder QRadar Risk Manager 7.1 haben.

Wenn Sie Ihrer Implementierung, in der die QRadar SIEM-Konsole netzadressumsetzungsfähig (Network Address Translation, NAT) ist, einen nicht netzadressumsetzungsfähigen verwalteten Host hinzufügen möchten, müssen Sie die Konsole zu einem netzadressumsetzungsfähigen Host wechseln. Die Änderung der Konsole muss vorgenommen werden, bevor der verwaltete Host Ihrer Implementierung hinzugefügt wird. Weitere Informationen finden Sie im Handbuch *IBM Security QRadar SIEM-Verwaltungshandbuch*.

Vorgehensweise

1. Öffnen Sie einen Web-Browser.
2. Geben Sie die URL `https://<IP-Adresse>` ein, wobei <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole steht.
3. Geben Sie Ihren Benutzernamen und das Kennwort ein.
4. Klicken Sie auf der Registerkarte **Verwaltung** auf **Implementierungseditor**.
5. Wählen Sie in dem Menü **Aktionen** und dann **Add a Managed Host** (Verwalteten Host hinzufügen).
6. Klicken Sie auf **Weiter**.
7. Geben Sie Werte für die folgenden Parameter ein:

Option	Bezeichnung
Enter the IP of the server or appliance to add (IP-Adresse des Servers oder der Appliance eingeben, der oder die hinzugefügt werden soll)	Die IP-Adresse von QRadar Risk Manager.
Enter the root password of the host (Rootkennwort des Hosts eingeben)	Das Rootkennwort für den Host.
Confirm the root password of the host (Rootkennwort des Hosts bestätigen)	Bestätigung Ihres Kennworts.
Host is NATed (Host ist netzadressumsetzungsfähig)	Damit die Netzadressumsetzung (Network Address Translation, NAT) für einen verwalteten Host aktiviert werden kann, muss in dem entsprechenden Netz eine statische Netzadressumwandlung verwendet werden. Weitere Informationen finden Sie im Handbuch *IBM Security QRadar SIEM Administration Guide*.
Enable Encryption (Verschlüsselung aktivieren)	Erstellt einen SSH-Verschlüsselungstunnel für den Host. Damit die Verschlüsselung zwischen zwei verwalteten Hosts aktiviert werden kann, muss auf jedem Host mindestens QRadar SIEM 7.1 oder QRadar Risk Manager 7.1 ausgeführt werden.
Enable Compression (Komprimierung aktivieren)	Ermöglicht die Datenkomprimierung zwischen zwei verwalteten Hosts.

8. Wählen Sie eine der folgenden Optionen aus:
   - Wenn Sie das Kontrollkästchen **Host is NATed** (Host ist netzadressumsetzungsfähig) aktiviert haben, müssen Sie für die Parameter zur Netzadressumsetzung entsprechende Werte eingeben.

Option	Bezeichnung
Enter public IP of the server or appliance to add (Öffentliche IP-Adresse des Servers oder der Appliance eingeben, der oder die hinzugefügt werden soll)	Die öffentliche IP-Adresse des verwalteten Hosts. Der verwaltete Host nutzt diese IP-Adresse bei der Kommunikation mit anderen verwalteten Hosts in anderen Netzen, in denen die Netzadressumsetzung verwendet wird.
Select NATed network (Netzadressumsetzungsfähiges Netz auswählen)	Das Netz, das dieser verwaltete Host verwenden soll. Wenn sich der verwaltete Host in demselben Teilnetz befindet wie die QRadar SIEM-Konsole, wählen Sie die Konsole des netzadressumsetzungsfähigen Netzes aus. Wenn sich der verwaltete Host nicht in demselben Teilnetz befindet wie die QRadar SIEM-Konsole, wählen Sie den verwalteten Host des netzadressumsetzungsfähigen Netzes aus.

- Wenn Sie das Kontrollkästchen **Host is NATed** (Host ist netzadressumsetzungsfähig) nicht aktiviert haben, klicken Sie auf **Weiter**.

9. Klicken Sie auf **Beenden**. Es kann einige Minuten dauern, bis der Prozess abgeschlossen ist. Wenn Ihre Implementierung Änderungen umfasst, müssen alle Änderungen implementiert werden.
10. Klicken Sie auf **Deploy** (Implementieren).

Nächste Schritte

Löschen Sie den Web-Browser-Cache und melden Sie sich dann bei QRadar SIEM an. Die Registerkarte **Risks** (Risiken) ist nun verfügbar.

Kommunikation einrichten

Bevor Sie QRadar Risk Manager konfigurieren können, müssen Sie die Kommunikation zwischen der QRadar Risk Manager-Appliance und der QRadar SIEM-Konsole einrichten.

Informationen zu diesem Vorgang

Es kann einige Minuten dauern, bis der Prozess zum Einrichten der Kommunikation abgeschlossen ist. Wenn Sie die IP-Adresse der QRadar Risk Manager-Appliance ändern oder QRadar Risk Manager mit einer anderen QRadar SIEM-Konsole verbinden müssen, können Sie dies in QRadar SIEM auf der Registerkarte **Verwaltung** über die Risk Manager-Einstellungen tun.

Vorgehensweise

1. Öffnen Sie einen Web-Browser und löschen Sie den Web-Browser-Cache.
2. Melden Sie sich bei QRadar SIEM an. Informationen zur IP-Adresse, zum Benutzernamen und zum Rootkennwort finden Sie im Abschnitt Zugriff auf die Benutzerschnittstelle von IBM Security QRadar Risk Manager.
3. Klicken Sie auf die Registerkarte **Risks** (Risiken).
4. Geben Sie Werte für die folgenden Parameter ein:

Option	Bezeichnung
IP/Hostname	Die IP-Adresse oder der Hostname der QRadar Risk Manager-Appliance.
Root Password (Rootkennwort)	Das Rootkennwort der QRadar Risk Manager-Appliance.

5. Klicken Sie auf **Speichern**.

Nächste Schritte

Definieren Sie Benutzerrollen.

Benutzerrolle 'Risk Manager' (Risikomanager) hinzufügen

Damit Benutzer Zugriff auf QRadar Risk Manager erhalten, müssen Sie ihnen die Benutzerrolle 'Risk Manager' (Risikomanager) zuweisen.

Informationen zu diesem Vorgang

Standardmäßig steht in QRadar SIEM eine Standardadministratorrolle zur Verfügung, die den Zugriff auf alle Bereiche von QRadar Risk Manager ermöglicht. Benutzer, denen Administratorberechtigungen einschließlich der Standardadministratorrolle zugewiesen wurden, können ihren eigenen Account jedoch nicht bearbeiten. Alle erforderlichen Änderungen müssen jeweils von einem anderen Administrator vorgenommen werden.

Informationen zum Erstellen und Verwalten von Benutzerrollen finden Sie im Handbuch *IBM Security QRadar SIEM-Verwaltungshandbuch*.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Systemkonfiguration**.
3. Klicken Sie im Teilfenster **Benutzerverwaltung** auf **Benutzerrollen**.
4. Wählen Sie im linken Teilfenster die Benutzerrolle aus, die Sie bearbeiten möchten.
5. Aktivieren Sie das Kontrollkästchen **Risk Manager** (Risikomanager).
6. Klicken Sie auf **Speichern**.
7. Klicken Sie auf **Schließen**.
8. Klicken Sie auf der Registerkarte **Verwaltung** auf **Änderungen implementieren**.

Kapitel 3. Netzdatenerfassung

QRadar Risk Manager muss so konfiguriert werden, dass es Konfigurationsdaten von den Einheiten im Netz erfassen kann.

Anhand der erfassten Konfigurationsdaten von den Netzeinheiten wird die Topologie des Netzes generiert und in QRadar Risk Manager ein Abbild der Netzkonfiguration erstellt.

Mithilfe der in QRadar Risk Manager erfassten Daten wird die Topologie mit Schlüsselinformationen zur Netzumgebung gefüllt.

Die Datenerfassung erfolgt in drei Schritten:

- Stellen Sie QRadar Risk Manager die Berechtigungsnachweise zur Verfügung, die zum Erfassen der Netzeinheitenkonfigurationen erforderlich sind.
- Starteen Sie das Erkennen von Einheiten, um in Configuration Source Management (CSM) eine Einheitenliste zu erstellen.
- Sichern Sie die Einheitenliste, um die Einheitenkonfigurationen abzurufen und die Topologie mit Informationen zum Netz zu füllen.

Berechtigungsnachweise

Damit der Zugriff auf die Einheitenkonfigurationen und deren Download ermöglicht wird, müssen die Berechtigungsnachweise in QRadar Risk Manager konfiguriert werden. Mithilfe der Berechtigungsnachweise kann QRadar Risk Manager Verbindungen zu Firewalls, Routern, Switches oder IPS-Einheiten (Intrusion Prevention System) herstellen.

Administratoren können die Berechtigungsnachweise für eine bestimmte Einheit über **Configuration Source Management** (CSM) eingeben, damit QRadar Risk Manager Zugriff auf diese Einheit erhält. QRadar Risk Manager kann die Berechtigungsnachweise für eine bestimmte Netzeinheit einzeln speichern. Wenn für mehrere Einheiten dieselben Berechtigungsnachweise verwendet werden, können Sie die Berechtigungsnachweise einer Gruppe von Einheiten zuordnen. Wenn beispielsweise alle Firewalls im Unternehmen dieselbe Kombination aus Benutzername und Kennwort haben, können Sie die Berechtigungsnachweise dieser Gruppe zuweisen. Die Berechtigungsnachweise sind dann den Adressgruppen für alle Firewalls zugeordnet und werden zur Sicherung der Einheitenkonfigurationen für alle Firewalls im Unternehmen verwendet.

Anmerkung: Wenn für eine bestimmte Einheit kein Netzberechtigungsnachweis erforderlich ist, kann der entsprechende Parameter in **Configuration Source Management** (CSM) leer bleiben.

Berechtigungsnachweise konfigurieren

Indem Sie Netzeinheiten konfigurieren, können Sie QRadar Risk Manager Zugriff auf diese Einheiten erteilen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.

3. Klicken Sie im Bereich **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung von Konfigurationsquellen).
4. Klicken Sie im Navigationsmenü auf **Credentials** (Berechtigungsnachweise).
5. Klicken Sie im Teilfenster **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
6. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
7. Geben Sie im Feld **Add address** (Adresse hinzufügen) die IP-Adresse der Einheit ein und klicken Sie auf **Hinzufügen**. Wiederholen Sie diesen Schritt für jede IP-Adresse, die hinzugefügt werden muss.

   Anmerkung: Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, im Bereich für Netzadressen neben dem Feld **Add address** (Adresse hinzufügen) tatsächlich angezeigt werden. Sie dürfen keine Einheitenadressen replizieren, die bereits in anderen Netzgruppen in **Configuration Source Management** (Verwaltung von Konfigurationsquellen) vorhanden sind.
   Sie können eine IP-Adresse, einen IP-Adressenbereich, ein CIDR-Teilnetz oder ein Platzhalterzeichen eingeben. Beispiel für die Verwendung des Platzhalterzeichens '*' (Stern): 10.1.*.*; Beispiel für die Angabe eines CIDR-Teilnetzes: 10.2.1.0/24.
8. Klicken Sie im Teilfenster **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).
9. Geben Sie einen Namen für die neue Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.
10. Wählen Sie den Namen der neu erstellten Berechtigungsnachweisgruppe aus und konfigurieren Sie die Werte für folgende Parameter:

Option	Bezeichnung
Benutzername	Ein gültiger Benutzername für die Anmeldung beim Adapter. Bei Adaptern müssen Benutzername und Kennwort Zugriff auf verschiedene Dateien haben, z. B. 'rule.C', 'objects.C', 'implied_rules.C' und 'Standard.PF'.
Kennwort	Das Kennwort für die Einheit.
Enable Password (Kennwort aktivieren)	Geben Sie das Kennwort für die Authentifizierung der zweiten Ebene ein. Dieses Kennwort ist erforderlich, wenn der Benutzer aufgefordert wird, die Berechtigungsnachweise für den Expertenmodus einzugeben.
SNMP Get Community (SNMP Community abrufen	Optionaler Parameter.
SNMPv3 Authentication Username (Benutzername für die SNMPv3-Authentifizierung)	Optionaler Parameter.
SNMPv3 Authentication Password (Kennwort für die SNMPv3-Authentifizierung)	Optionaler Parameter.
SNMPv3 Privacy Password (SNMPv3-Datenschutzkennwort)	Optionaler Parameter. Das Protokoll, mit dem Sie SNMPv3-Traps entschlüsseln möchten.

11. Klicken Sie auf **OK**.

Einheiten erkennen

Mit dem Erkennungsprozess werden der Topologieschnittstelle neue Netzeinheiten hinzugefügt. Dabei werden die Berechtigungsnachweise verwendet, die Sie zuvor hinzugefügt haben.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung von Konfigurationsquellen).
4. Klicken Sie im Navigationsmenü auf **Discover Devices** (Einheiten erkennen).
5. Geben Sie eine IP-Adresse oder einen CIDR-Bereich ein, um die Position anzugeben, an der Einheiten erkannt werden sollen.
6. Klicken Sie auf das Symbol **Hinzufügen** (Pluszeichen).
7. Wenn Sie im Netz ab der angegebenen IP-Adresse oder dem angegebenen CIDR-Bereich nach Einheiten suchen möchten, aktivieren Sie das Kontrollkästchen **Crawl the network from the addresses defined above** (Netz ab den zuvor angegebenen Adressen durchsuchen).
8. Klicken Sie auf **Run** (Ausführen).

Einheitenkonfiguration abrufen

Zum Sichern einer Einheit können Sie die Einheitenkonfiguration herunterladen, sodass QRadar Risk Manager die Einheitendaten in die Topologie aufnehmen kann.

Vorbereitende Schritte

Bevor Sie Einheitenkonfigurationen herunterladen können, müssen Sie Gruppen von Berechtigungsnachweisen konfigurieren.

Informationen zu diesem Vorgang

Sie können eine einzelne Einheit oder alle Einheiten sichern.

Informationen zur Planung automatisierter Sicherungen von Einheitenkonfigurationen auf der Registerkarte **Jobs** finden Sie im Handbuch *IBM Security QRadar Risk Manager User Guide*.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** (Risikomanager) auf **Configuration Source Management** (Verwaltung von Konfigurationsquellen).
4. Klicken Sie auf die Registerkarte **Devices** (Einheiten).
5. Um die Konfiguration aller Einheiten abzurufen, klicken Sie im Navigationsbereich auf **Backup All** (Alle sichern). Klicken Sie auf **Ja**, um fortzufahren.
6. Um die Konfiguration bestimmter Einheiten abzurufen, wählen Sie die jeweilige Einheit aus. Wenn Sie mehrere Einheiten gleichzeitig für die Sicherung auswählen möchten, halten Sie dabei die STRG-Taste gedrückt. Klicken Sie auf **Sicherung**.

Einheiten importieren

Mit der Funktion 'Geräteimport' können Sie dem Configuration Source Management (CSM) mithilfe einer CSV-Datei eine Liste mit Adaptern und deren IP-Adressen im Netz hinzufügen.

Die Liste für den Geräteimport kann bis zu 5000 Einheiten enthalten. Dabei muss jedoch jeder Adapter mit der ihm zugeordneten IP-Adresse in einer eigenen Zeile der Liste aufgeführt sein.

Beispiel:

```
<Adapter::Name 1>,<IP-Adresse>
<Adapter::Name 2>,<IP-Adresse>
<Adapter::Name 3>,<IP-Adresse>
```

Dabei gilt:

`<Adapter::Name>` enthält den Hersteller- und den Einheitennamen, z. B. 'Cisco::IOS'.

`<IP-Adresse>` enthält die IP-Adresse der Einheit, z. B. '191.168.1.1'.

Tabelle 3. Beispiele für die Geräteimport-Funktion

Hersteller	Name	Beispiel für <Adapter::Name>,<IP-Adresse>
Check Point	SecurePlatform	CheckPoint::SecurePlatform,10.1.1.4
Cisco	IOS	Cisco::IOS,10.1.1.1
Cisco	Cisco Security Appliance	Cisco::SecurityAppliance,10.1.1.2
Cisco	CatOS	Cisco::CatOS, 10.1.1.3
Cisco	Nexus	Cisco::Nexus
Generic	SNMP	Generic::SNMP,10.1.1.8
Juniper Networks	Junos	Juniper::JUNOS,10.1.1.5

CSV-Datei importieren

Sie können eine Master-Einheitenliste als CSV-Datei in Configuration Source Management (CSM) importieren.

Vorbereitende Schritte

Wenn Sie eine Liste mit Einheiten importieren und anschließend in der CSV-Datei eine IP-Adresse ändern, können Sie dabei versehentlich eine Einheit in der Liste in Configuration Source Management duplizieren. Deshalb sollten Sie eine Einheit aus Configuration Source Management löschen, bevor Sie die Master-Einheitenliste erneut importieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü auf **Plug-ins**.
3. Klicken Sie im Teilfenster **Plug-Ins** auf **Geräteimport**.
4. Klicken Sie auf **Durchsuchen**.
5. Suchen und markieren Sie die CSV-Datei und klicken Sie auf **Öffnen**.

6. Klicken Sie auf **Import Devices** (Einheiten importieren).

Ergebnisse

Wenn ein Fehler angezeigt wird, müssen Sie die CSV-Datei überprüfen, eventuelle Fehler korrigieren und die Datei erneut importieren. Der Import der CSV-Datei kann fehlschlagen, wenn die Einheitenliste nicht korrekt strukturiert ist oder falsche Informationen enthält. Beispiele für eine fehlerhafte CSV-Datei sind ein fehlender Doppelpunkt oder Befehl, die Angabe mehrerer Einheiten in einer Zeile oder ein falsch geschriebener Adaptername.

Wenn der Einheitenimport abgebrochen wird, werden keine Einheiten aus der CSV-Datei dem Configuration Source Management (CSM) hinzugefügt.

Fehlerbehebung für Einheitenimport ausführen

Wenn Sie nach dem Import einer Einheit eine Fehlernachricht erhalten, ist möglicherweise der Import der CSV-Datei fehlgeschlagen.

Der Import einer Einheit kann fehlschlagen, wenn die Einheitenliste nicht korrekt strukturiert ist. Dies ist beispielsweise der Fall, wenn in der entsprechenden CSV-Datei Doppelpunkte oder ein Befehl fehlen oder mehrere Einheiten in derselben Zeile angegeben sind.

Eine weitere mögliche Ursache für einen fehlgeschlagenen Einheitenimport sind falsche Informationen in der Einheitenliste. Dies kann beispielsweise ein Schreibfehler in einem Adapternamen sein.

Wenn der Einheitenimport abgebrochen wird, werden keine Einheiten aus der CSV-Datei dem Configuration Source Management (CSM) hinzugefügt. Eine Liste gültiger Adapternamen für die installierten Adapter ist in der Nachricht angegeben. Wenn eine Fehlernachricht angezeigt wird, müssen Sie die CSV-Datei überprüfen und ggf. korrigieren. Sie können die Datei erneut importieren, nachdem alle Fehler korrigiert wurden.

Kapitel 4. Audits verwalten

IBM Security QRadar Risk Manager unterstützt Sie bei der Beantwortung bestimmter Fragen, um die Bewertung von Netzsicherheitsrichtlinien und Konformitätsanforderungen zu erleichtern.

Die Überprüfung der Konformität durch Audits ist für Sicherheitsadministratoren eine notwendige und komplexe Aufgabe. QRadar Risk Manager unterstützt Sie bei der Beantwortung folgender Fragen:

- Wie sind die Netzeinheiten konfiguriert?
- Wie kommunizieren die Netzressourcen miteinander?
- Welche Schwachstellen hat das Netz?

Anwendungsfall: Konfigurationsaudit

Sie können die Konfigurationsdaten, die von QRadar Risk Manager für Netzeinheiten erfasst werden, für die Auditkonformität und zum Planen von Konfigurationssicherungen verwenden.

Konfigurationssicherungen stellen eine zentralisierte und automatische Methode dar, mit der Änderungen an Einheiten für die Auditkonformität aufgezeichnet werden können. Konfigurationssicherungen protokollieren Konfigurationsänderungen und erfüllen deshalb die Funktion eines Langzeitarchivs. Sie können eine Protokollaufzeichnung erfassen oder eine Konfiguration mit einer anderen Netzeinheit vergleichen.

Bei einem Konfigurationsaudit mit QRadar Risk Manager haben Sie folgende Optionen:

- Protokollaufzeichnung der Konfigurationen der Netzeinheiten
- Normalisierte Ansicht mit Anzeige der Änderungen an Einheiten beim Vergleich von Konfigurationen
- Tool für die Suche nach Regeln auf den Einheiten

Die Konfigurationsdaten für die Einheiten werden in den Einheitensicherungen im Configuration Source Management (CSM) erfasst. Bei jeder Sicherung der Einheitenliste durch QRadar Risk Manager wird eine Kopie der Einheitenkonfiguration erstellt, um ein Langzeitarchiv einzurichten. Je häufiger Sie Sicherungen mit Configuration Source Management planen, desto mehr Konfigurationsdatensätze stehen Ihnen zum Vergleich und als Langzeitarchiv zur Verfügung.

Einheitenkonfigurationsprotokoll anzeigen

Sie können das Konfigurationsprotokoll einer Netzeinheit anzeigen.

Informationen zu diesem Vorgang

Sie können die Protokolldaten für Netzeinheiten anzeigen, die gesichert wurden. Diese Daten sind auf der Seite **Configuration Monitor** (Konfigurationsüberwachung) im Teilfenster **Protokoll** zugänglich. Im Protokollteilfenster werden Informationen zu einer Netzeinheitenkonfiguration und das Datum angezeigt, an dem die Einheitenkonfiguration zuletzt mit Configuration Source Management (CSM) gesichert wurde.

In der Konfiguration sind die Dateitypen angegeben, die für die Netzeinheit in QRadar Risk Manager gespeichert sind. Folgende Konfigurationsdateitypen sind üblich:

- **Standard-Element-Document** (SED, Standardelementdokument): dies sind XML-Dateien, die Informationen zu der Netzeinheit enthalten. Einzelne SED-Dateien können im unformatierten XML-Format angezeigt werden. Bei einem Vergleich von zwei SED-Dateien wird die Ansicht normalisiert, damit die Regelunterschiede dargestellt werden können.
- **Config**: Dies sind Konfigurationsdateien, die von bestimmten Netzeinheiten bereitgestellt werden. Der Inhalt dieser Dateien hängt vom Einheitenhersteller ab. Der Inhalt einer Konfigurationsdatei kann durch Doppelklick auf die Datei angezeigt werden.

Anmerkung: Je nach Einheit werden darüber hinaus möglicherweise noch verschiedene andere Konfigurationsdateien angezeigt. Bei einem Doppelklick auf diese Dateien wird deren Inhalt als unformatierter Text angezeigt. Die Ansicht als unformatierter Text in einem Web-Browser-Fenster unterstützt die Funktionen 'Suchen' (STRG+F), 'Einfügen' (STRG+V) und 'Kopieren' (STRG+C).

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Doppelklicken Sie auf eine Konfiguration, um die detaillierten Einheitendaten anzuzeigen.
4. Klicken Sie auf **Protokoll**.
5. Wählen Sie im Teilfenster **Protokoll** eine Konfiguration aus.
6. Klicken Sie auf **View Selected** (Ausgewählte Konfiguration anzeigen).

Einheitenkonfigurationen von einer einzelnen Einheit vergleichen

Sie können verschiedene Konfigurationen von einer einzelnen Einheit miteinander vergleichen.

Informationen zu diesem Vorgang

Wenn die Dateien, die Sie miteinander vergleichen, Standardelementdokumente (SEDs) sind, können Sie die Unterschiede zwischen den beiden Konfigurationsdateien in Bezug auf die Regeln anzeigen.

Wenn Sie normalisierte Konfigurationen vergleichen, kennzeichnen die Farben im Text folgende Arten von Regeln:

- Eine grüne, gepunktete Umrandung kennzeichnet eine Regel oder Konfiguration, die der Einheit hinzugefügt wurde.
- Eine rote, gestrichelte Umrandung kennzeichnet eine Regel oder Konfiguration, die aus der Einheit gelöscht wurde.
- Eine gelbe, durchgezogene Umrandung kennzeichnet eine Regel oder Konfiguration, die in der Einheit geändert wurde.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).

2. Klicken Sie im Navigationsmenü auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Doppelklicken Sie auf eine Einheit, um die detaillierten Konfigurationsdaten anzuzeigen.
4. Klicken Sie auf **Protokoll**, um das Protokoll für diese Einheit anzuzeigen.
5. Wählen Sie die erste Konfiguration für den Vergleich aus.
6. Drücken Sie die STRG-Taste und wählen Sie eine zweite Konfiguration für den Vergleich aus.
7. Klicken Sie im Teilfenster **Protokoll** auf **Compare Selected** (Ausgewählte Konfigurationen vergleichen).
8. Optional: Um die unformatierten Konfigurationsunterschiede anzuzeigen, klicken Sie auf **View Raw Comparison** (Unformatierten Vergleich anzeigen). Wenn der Vergleich mit einer Konfigurationsdatei oder einem anderen Sicherungstyp ausgeführt wird, wird immer der unformatierte Vergleich angezeigt.

Einheitenkonfigurationen von verschiedenen Einheiten vergleichen

Sie können die Konfigurationen von zwei verschiedenen Einheiten miteinander vergleichen.

Informationen zu diesem Vorgang

Wenn die Dateien, die Sie miteinander vergleichen, Standardelementdokumente (SEDs) sind, können Sie die Unterschiede zwischen den beiden Konfigurationsdateien in Bezug auf die Regeln anzeigen.

Wenn Sie normalisierte Konfigurationen vergleichen, kennzeichnen die Farben im Text folgende Arten von Regeln:

- Eine grüne, gepunktete Umrandung kennzeichnet eine Regel oder Konfiguration, die der Einheit hinzugefügt wurde.
- Eine rote, gestrichelte Umrandung kennzeichnet eine Regel oder Konfiguration, die aus der Einheit gelöscht wurde.
- Eine gelbe, durchgezogene Umrandung kennzeichnet eine Regel oder Konfiguration, die in der Einheit geändert wurde.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Configuration Monitor** (Konfigurationsüberwachung).
3. Doppelklicken Sie auf eine Einheit, um die detaillierten Konfigurationsdaten anzuzeigen.
4. Klicken Sie auf **Protokoll**, um das Protokoll für diese Einheit anzuzeigen.
5. Wählen Sie die erste Konfiguration für den Vergleich aus.
6. Klicken Sie auf **Mark for Comparison** (Für Vergleich markieren).
7. Wählen Sie im Navigationsmenü **All Devices** (Alle Einheiten) aus, um zur Einheitenliste zurückzukehren.
8. Doppelklicken Sie auf die Einheit, die verglichen werden soll, und klicken Sie dann auf **Protokoll**.
9. Wählen Sie eine andere Konfigurationssicherung aus, die mit der bereits markierten Konfiguration verglichen werden soll.

10. Klicken Sie auf **Compare with Marked** (Mit markierter Konfiguration vergleichen).
11. Optional: Um die unformatierten Konfigurationsunterschiede anzuzeigen, klicken Sie auf **View Raw Comparison** (Unformatierten Vergleich anzeigen). Wenn der Vergleich mit einer Konfigurationsdatei oder einem anderen Sicherungstyp ausgeführt wird, wird immer der unformatierte Vergleich angezeigt.

Anwendungsfall: Netzpfade in der Topologie anzeigen

In der Topologieansicht zeigt QRadar Risk Manager eine grafische Darstellung der Netzeinheiten an.

Mit einer Pfadsuche in der Topologie können Sie feststellen, wie die Netzeinheiten kommunizieren und welchen Netzpfad sie dabei verwenden. Bei einer Pfadsuche kann QRadar Risk Manager den Pfad zwischen Quelle und Ziel einschließlich der Ports, Protokolle und Regeln visuell darstellen.

Diese Darstellung macht deutlich, wie die Einheiten kommunizieren. Dies ist besonders wichtig bei Assets mit gesichertem oder eingeschränktem Zugriff.

Folgende Schlüsselfunktionen werden bereitgestellt:

- Anzeige der Kommunikation zwischen Einheiten im Netz
- Suche nach bestimmten Netzeinheiten in der Topologie mithilfe von Filtern
- Schnellzugriff auf die Anzeige von Einheitenregeln und -konfigurationen
- Anzeige von Ereignissen, die bei einer Pfadsuche generiert wurden

Topologie durchsuchen

Sie können die Topologie durchsuchen, um Einheitenkommunikation anzuzeigen.

Informationen zu diesem Vorgang

Sie können das Topologiemodell filtern, indem Sie eine Pfadsuche durchführen. Eine Pfadsuche schließt alle Teilnetze ein, die die Quellen-IP-Adressen oder CIDR-Bereiche enthalten, sowie alle Teilnetze, die die Ziel-IP-Adressen oder CIDR-Bereiche enthalten, denen außerdem die Kommunikation über das konfigurierte Protokoll und den konfigurierten Port erlaubt ist. Die Suche umfasst die Untersuchung des Topologiemodells sowie der Einheiten, die zum Kommunikationspfad zwischen Quelle und Ziel gehören, und schließt detaillierte Verbindungsinformationen ein.

Sie können die Suche nach Schwachstellen filtern, sofern die Topologie ein Intrusion-Prevention-System (IPS) umfasst. Weitere Informationen finden Sie im Handbuch *IBM Security QRadar Risk Manager User Guide*.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Topology** (Topologie).
3. Wählen Sie in der Liste **Suchen** den Eintrag **Neue Suche** aus.
4. Wählen Sie im Teilfenster **Search Criteria** (Suchkriterien) die Option **Path** (Pfad) aus.
5. Geben Sie im Feld **Quellen-IP/CIDR** die IP-Adresse oder den CIDR-Bereich ein, nach dem Sie das Topologiemodell filtern möchten. Mehrere Einträge müssen durch Kommas getrennt werden.

6. Geben Sie im Feld **Ziel-IP/CIDR** die Ziel-IP-Adresse oder den CIDR-Bereich ein, nach dem Sie das Topologiemodell filtern möchten. Mehrere Einträge müssen durch Kommas getrennt werden.
7. Optional: Wählen Sie in der Liste **Protokoll** das Protokoll aus, nach dem Sie das Topologiemodell filtern möchten.
8. Optional: Geben Sie im Feld **Zielport** den Zielport ein, nach dem Sie das Topologiemodell filtern möchten. Mehrere Ports müssen durch Kommas getrennt werden.
9. Klicken Sie auf **OK**.
10. Wenn Sie die Maus über eine Verbindungslinie bewegen, werden Details zur Verbindung angezeigt. Wenn die Suche eine Verbindung zu einer Einheit herstellt, die Regeln enthält, wird im Dialogfeld ein Link zu den Einheitenregeln angezeigt.

Anwendungsfall: Attackenpfad eines Angriffs visualisieren

Angriffe in QRadar Risk Manager sind Ereignisse, die vom System generiert werden, um Sie über einen bestimmten Netzzustand oder ein Ereignis zu benachrichtigen.

Die Visualisierung von Attackenpfaden stellt eine Zuordnung zwischen Angriffen und Topologiesuchvorgängen her. Die Visualisierung ermöglicht Sicherheitsspezialisten die Anzeige der Angriffsdetails und des Pfades, auf dem der Angriff im Netz verlief. Der Attackenpfad ist eine visuelle Darstellung dieser Zusammenhänge. Die visuelle Darstellung zeigt Ihnen die Assets im Netz an, deren Kommunikation die Weiterleitung eines Angriffs im Netz ermöglicht hat. Diese Daten sind während eines Audits von kritischer Bedeutung für den Nachweis, dass Sie Ihr Netz auf Angriffe überwachen und dass dem Angriff kein alternativer Pfad im Netz zu einem kritischen Asset zur Verfügung steht.

Die Visualisierung ermöglicht folgende Schlüsselfunktionen:

- Nutzung des in QRadar SIEM vorhandenen Regel- und Angriffssystems
- Visuelle Darstellung eines Pfads für alle Einheiten zwischen der Quelle und dem Ziel eines Angriffs
- Schnellzugriff auf die Einheitenkonfigurationen und -regeln, die den Angriff ermöglicht haben

Attackenpfad eines Angriffs anzeigen

Sie können den Attackenpfad eines Angriffs anzeigen. Der Attackenpfad stellt die Quelle, das Ziel und die zugeordneten Einheiten dar.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Angriffe**.
2. Klicken Sie im Navigationsmenü auf **Alle Angriffe**. Auf der Seite **Alle Angriffe** wird eine Liste der in Ihrem Netz vorliegenden Angriffe angezeigt. Die Angriffe mit dem größten Ausmaß werden zuerst aufgeführt.
3. Doppelklicken Sie auf einen Angriff, um die Zusammenfassung der Angriffe anzuzeigen.
4. Klicken Sie in der Symbolleiste der Seite **Angriffe** auf **View Attack Path** (Attackenpfad anzeigen).

Kapitel 5. Anwendungsfall: Richtlinien überwachen

Richtlinienaudits und Änderungsmanagement sind grundlegende Prozesse, mit denen Administratoren und Sicherheitsspezialisten den Zugriff auf und die Kommunikation zwischen kritischen Geschäftsassets steuern können.

Zu den Kriterien der Richtlinienüberwachung kann die Überwachung von Assets und Kommunikationsprotokollen in folgenden Szenarien gehören:

- Enthält mein Netz Assets mit Konfigurationen, die bei Audits gemäß PCI-Abschnitt 1 als gefährlich eingestuft sind?
- Ermöglichen meine Assets Kommunikationsprotokolle, die bei Audits gemäß PCI-Abschnitt 10 als gefährlich eingestuft sind?
- Wie erfahre ich, dass eine Richtlinienänderung einen Verstoß in meinem Netz auslöst?
- Wie kann ich Schwachstellen für permanent gespeicherte Assets oder Assets mit hohem Risiko anzeigen?
- Wie kann ich Assets mit Schwachstellen und Internetzugriff im Netz anzeigen?

Mit der Richtlinienüberwachung können Sie Tests definieren, die auf den Risikoindikatoren basieren, und anschließend die Testergebnisse mithilfe von Filtern auf bestimmte Ergebnisse, Verstöße, Protokolle oder Schwachstellen eingrenzen.

IBM Security QRadar Risk Manager umfasst verschiedene Fragen der Richtlinienüberwachung, die nach PCI-Kategorie gruppiert sind, z. B. Fragen zu den PCI-Abschnitten 1, 6 und 10. Es können Fragen zu Assets oder zu Einheiten und Regeln erstellt werden, um Netzsicherheitsrisiken offenzulegen. Nachdem eine Frage zu einem Asset, einer Einheit oder einer Regel an die Richtlinienüberwachung übergeben wurde, geben die Ergebnisse die Risikostufe an. Sie können die von den Assets zurückgegebenen Ergebnisse genehmigen oder festlegen, wie das System auf nicht genehmigte Ergebnisse reagieren soll.

Die Richtlinienüberwachung ermöglicht folgende Schlüsselfunktionen:

- Vordefinierte Fragen zur Richtlinienüberwachung, um den Workflow zu unterstützen
- Ermittlung von Fällen, in denen Benutzer verbotene Kommunikationsprotokolle verwendet haben
- Bewertung, ob Benutzer in bestimmten Netzen mit verbotenen Netzen oder Assets kommunizieren können
- Bewertung, ob die Firewallregeln die unternehmensinternen Richtlinien erfüllen
- Fortwährende Überwachung von Richtlinien, die Angriffe oder Alerts für Administratoren generieren
- Priorisieren von Schwachstellen durch Ermittlung von Systemen, die wegen ihrer Einheitenkonfiguration beeinträchtigt werden können
- Ermittlung von Konformitätsproblemen

Anwendungsfall: Assets mit verdächtigen Konfigurationen bewerten

Mithilfe von Unternehmenssicherheitsrichtlinien definieren Unternehmen Risiken und die zulässige Kommunikation zwischen Assets und Netzen. Damit Verstöße gegen die Konformitäts- und Unternehmensrichtlinien vermieden werden, verwenden Unternehmen die Richtlinienüberwachung, um eventuell unbekannte Risiken zu bewerten und zu überwachen.

Die PCI-Konformitätsanforderungen schreiben Folgendes vor: Einheiten, die Karteninhaberdaten enthalten, ermitteln; dann die Kommunikation aufzeichnen und prüfen sowie die Firewallkonfigurationen überwachen, um Assets mit vertraulichen Daten zu schützen. Die Richtlinienüberwachung bietet Methoden, mit denen diese Anforderungen schnell erfüllt werden können, sodass die Administratoren die Unternehmensrichtlinien einhalten. Zu den allgemein üblichen Methoden zur Minderung der Risiken gehört die Ermittlung und Überwachung von Assets, die mit nicht gesicherten Protokollen kommunizieren. Darunter fallen Protokolle von Routern, Firewalls oder Switches, die FTP- oder Telnet-Verbindungen zulassen. Mithilfe der Richtlinienüberwachung können Sie Assets mit gefährlichen Konfigurationen in Ihrer Topologie ermitteln.

Fragen zur Überprüfung der Konformität gemäß PCI-Abschnitt 1 können unter anderem folgende Kriterien betreffen:

- Assets, die gesperrte Protokolle zulassen
- Assets, die gefährliche Protokolle zulassen
- Assets, die nicht richtlinienkonforme Anwendungen netzweit zulassen
- Assets, die nicht richtlinienkonforme Anwendungen in Netzen zulassen, die geschützte Assets enthalten

Einheiten bewerten, die gefährliche Protokolle zulassen

Einheiten, die gefährliche Protokolle zulassen, mit der Richtlinienüberprüfung bewerten

Informationen zu diesem Vorgang

QRadar Risk Manager bewertet die entsprechende Frage und zeigt als Ergebnis diejenigen Assets in der Topologie an, die die Testfrage erfüllen. Die Kommunikation zu bestimmten Assets, die als nicht gefährlich angesehen wird, kann von Sicherheitsspezialisten, Administratoren oder Auditoren genehmigt werden. Diese Personen können auch Angriffe für dieses Verhalten erstellen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie im Listenfeld 'Gruppe' den Eintrag **PCI 1** aus.
4. Wählen Sie folgende Testfrage aus: **Assess any devices (i.e. firewalls) that allow risky protocols (i.e telnet and FTP traffic - port 21 & 23 respectively) from the internet to the DMZ** (Jegliche Einheiten (z. B. Firewalls) bewerten, die gefährliche Protokolle (z. B. Telnet- und FTP-Datenverkehr über Port 21 bzw. 23) vom Internet zur Demilitarized Zone (DMZ) zulassen).
5. Klicken Sie auf **Submit Question** (Frage übergeben).

Anwendungsfall: Assets mit verdächtiger Kommunikation bewerten

Mithilfe der Richtlinienüberwachung können Sie die Konformität gemäß PCI-Abschnitt 10 erfassen, indem Sie den Zugriff auf Netzassets verfolgen, protokollieren und anzeigen.

QRadar Risk Manager unterstützt Sie beim Überprüfen der Konformität gemäß PCI-Abschnitt 10, indem es Assets in der Topologie erfasst, die zweifelhafte oder gefährliche Kommunikationsprotokolle zulässt. QRadar Risk Manager kann die tatsächliche oder mögliche Kommunikation dieser Assets überprüfen. Bei der Überprüfung der tatsächlichen Kommunikation werden Assets angezeigt, die bereits Kommunikationsprotokolle verwendet haben, die von Ihnen als Fragekriterien festgelegt wurden. Bei der Überprüfung der möglichen Kommunikation werden Assets angezeigt, die Kommunikationsprotokolle verwenden können, die von Ihnen als Fragekriterien festgelegt wurden.

Fragen zur Überprüfung der Konformität gemäß PCI-Abschnitt 10 können unter anderem folgende Kriterien betreffen:

- Assets, die eingehende Anfragen zu internen Netzen zulassen
- Assets, die von nicht vertrauenswürdigen Positionen aus mit vertrauenswürdigen Positionen kommunizieren
- Assets, die von einem VPN (Virtual Private Network) aus mit vertrauenswürdigen Positionen kommunizieren
- Assets, die unverschlüsselte, nicht richtlinienkonforme Protokolle innerhalb einer vertrauenswürdigen Position zulassen

Assets suchen, die Kommunikation zulassen

Sie können nach Assets suchen, die vom Internet eingehende Kommunikation zulassen.

Informationen zu diesem Vorgang

QRadar Risk Manager bewertet die entsprechende Frage und zeigt als Ergebnis diejenigen internen Assets an, die vom Internet eingehende Verbindungen zulassen. Die Kommunikation zu den Assets, die als nicht sicher angesehen werden oder Kundendaten enthalten, kann von Sicherheitsspezialisten, Administratoren oder Auditoren genehmigt werden. Wenn häufiger Ereignisse dieser Art auftreten, können Sie in QRadar SIEM Angriffe erstellen, mit denen diese Form der gefährlichen Kommunikation überwacht wird.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie im Listenfeld 'Gruppe' den Eintrag **PCI 10** aus.
4. Wählen Sie folgende Testfrage aus: **Assess any inbound connections from the internet to anywhere on the internal network** (Vom Internet eingehende Verbindungen zu beliebigen Einheiten im internen Netz bewerten).
5. Klicken Sie auf **Submit Question** (Frage übergeben).

Anwendungsfall: Richtlinien für Verstöße überwachen

Mit der Richtlinienüberwachung von QRadar Risk Manager ist eine fortwährende Überwachung von vordefinierten oder benutzerdefinierten Fragen möglich. Wenn Sie den Überwachungsmodus verwenden, werden in QRadar Risk Manager Ereignisse generiert.

Wenn Sie eine Frage zur Überwachung auswählen, analysiert QRadar Risk Manager die Frage stündlich auf Basis Ihrer Topologie, um festzustellen, ob die Änderung eines Assets oder einer Regel zu einem nicht genehmigten Ergebnis führt. Wenn QRadar Risk Manager ein nicht genehmigtes Ergebnis erkennt, kann ein Angriff generiert werden, um Sie auf eine Abweichung in der definierten Richtlinie aufmerksam zu machen. QRadar Risk Manager kann im Überwachungsmodus die Ergebnisse von 10 Fragen gleichzeitig überwachen.

Die Fragenüberwachung ermöglicht folgende Schlüsselfunktionen:

- Stündliche Überwachung der Regel- oder Assetänderungen auf nicht genehmigte Ergebnisse
- Kategorisierung der nicht genehmigten Ergebnisse anhand der von Ihnen festgelegten Ereigniskategorien nach ihrem Schweregrad (höhere/niedrigere Ebene)
- Generierung von Angriffen, E-Mails, Syslog-Nachrichten oder Dashboardbenachrichtigungen über nicht genehmigte Ergebnisse
- Verwendung von Ereignisansichten, Korrelation, Ereignisberichten, angepassten Regeln und Dashboards in QRadar SIEM

Fragen konfigurieren

Sie können mit der Richtlinienüberwachung eine Frage konfigurieren, die überwacht werden soll.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie die Frage aus, die überwacht werden soll.
4. Klicken Sie auf **Überwachung**.
5. Konfigurieren Sie alle Optionen, die zum Überwachen der Frage erforderlich sind.
6. Klicken Sie auf **Save Monitor** (Überwachung speichern).

Ergebnisse

Damit ist die Überwachung dieser Frage aktiviert und es werden ggf. Ereignisse oder Angriffe basierend auf den Überwachungskriterien erstellt.

Anwendungsfall: Risiken auf Basis von Schwachstellen priorisieren

Ungeschützte Schwachstellen sind ein erhebliches Risiko für Netzassets.

QRadar Risk Manager nutzt die Informationen zu Assets und deren Schwachstellen, die mit der Richtlinienüberwachung erfasst wurden. Anhand dieser Informationen kann ermittelt werden, ob die Assets für Eingabeangriffe anfällig sind. Zu dieser Art von Angriffen gehören unter anderem SQL-Injections, verdeckte Felder und Clickjacking.

Die erkannten Schwachstellen der Assets können nach ihrer Netzadresse oder nach einer Verbindung zu einer anderen anfälligen Einheit priorisiert werden.

Fragen zu Schwachstellen von Assets können unter anderem folgende Kriterien betreffen:

- Assets mit neuen Schwachstellen, die nach einem bestimmten Datum dokumentiert wurde
- Assets mit bestimmten Schwachstellen oder bestimmter CVSS-Bewertung.
- Assets mit einer bestimmten Schwachstellenklassifikation, z. B. Eingabemanipulation, Denial-of-Service-Angriffe oder mit OSVDB-Bestätigung (Open Source Vulnerability Database).

Assets mit Schwachstellen suchen

Sie können nach Assets suchen, die Schwachstellen haben.

Informationen zu diesem Vorgang

QRadar Risk Manager bewertet die entsprechende Frage und zeigt als Ergebnis diejenigen Assets an, die die entsprechenden Schwachstellen haben. Assets, die Schwachstellen für bekannte SQL-Injection-Attacken haben, können so von Sicherheitsspezialisten, Administratoren oder Auditoren ermittelt werden. Assets, die mit einem geschützten Netz verbunden sind, können dann sofort korrigiert werden. Wenn häufiger Ereignisse dieser Art auftreten, können Sie in QRadar SIEM Ereignisse oder Angriffe erstellen, mit denen die Assets mit Schwachstellen für SQL-Injection-Attacken überwacht werden.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie in der Liste **Gruppe** den Eintrag **Schwachstelle** aus.
4. Wählen Sie folgende Testfrage aus: **Assess assets with SQL injection vulnerabilities on specific localnet(s) (i.e. protected server network)** (Assets mit Schwachstellen für SQL-Injection-Attacken in bestimmten lokalen Netzen (d. h. in geschützten Servernetzen) bewerten).
5. Klicken Sie auf **Submit Question** (Frage übergeben).

Anwendungsfall: Schwachstellen von Assets nach Zone oder Netzkommunikation priorisieren

Systeme mit Schwachstellen, die sich in demselben Netz wie geschützte Assets befinden, haben eine höheres Risiko für Datenverlust.

Die Erkennung der Schwachstellen von Assets nach Zone oder Netz ist eine wichtige Maßnahme, um das Auftreten von Exploits im Netz zu vermeiden. In den PCI-Abschnitten 6.1 und 6.2 ist festgelegt, dass Systeme innerhalb eines Monats nach Veröffentlichung eines Patch-Release zur Behebung von Schwachstellen überprüft und korrigiert werden müssen. QRadar Risk Manager unterstützt Sie bei der Automatisierung und Priorisierung des Patchprozesses. Wenn Schwachstellen an den Assets erkannt werden, können Sie sie nach ihrer Netzadresse oder nach einer Verbindung zu einer anderen anfälligen Einheit priorisieren. Die Priorisierung ist wichtig für sichere Netze, die eine Verbindung zu verdächtigen Regionen herstellen können, oder für Assets die eine höhere CVSS-Bewertung haben, als nach den unternehmensinternen Richtlinien zulässig ist.

Fragen zu Assets mit Schwachstellen können unter anderem folgende Kriterien betreffen:

- Assets mit einer clientseitigen Schwachstelle, die mit verdächtigen geografischen Regionen kommuniziert haben und geschützte Assets enthalten
- Assets mit Denial-of-Service-Schwachstellen in einem bestimmten Netz
- Assets mit E-Mail-Schwachstellen in einem bestimmten Netz
- Assets mit Schwachstellen und einer bestimmten CVSS-Bewertung (Common Vulnerability Scoring System)

Assets mit Schwachstellen im Netz suchen

Sie können in einem bestimmten Netz nach Assets suchen, die Schwachstellen haben.

Informationen zu diesem Vorgang

QRadar Risk Manager bewertet die entsprechende Frage und zeigt die Ergebnisse an genau der Position an, die die betriebssystemspezifischen Schwachstellen enthält. Die Kommunikation zu den Assets, die als nicht sicher angesehen werden oder Kundendaten enthalten, kann von Sicherheitsspezialisten, Administratoren oder Auditoren genehmigt werden. Wenn häufiger Ereignisse dieser Art auftreten, können Sie Angriffe erstellen, mit denen diese Form der gefährlichen Kommunikation überwacht wird.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Klicken Sie im Navigationsmenü auf **Richtlinienüberwachung**.
3. Wählen Sie im Listenfeld **Gruppe** den Eintrag **Schwachstelle** aus.
4. Wählen Sie folgende Testfrage aus: **Assess assets with OS specific vulnerabilities on a specific localnet(s)** (Assets mit betriebssystemspezifischen Schwachstellen in bestimmten lokalen Netzen bewerten).
5. Klicken Sie auf **Submit Question** (Frage übergeben).

Kapitel 6. Anwendungsfälle für Simulationen

Anwendungsfall: Angriffe auf Netzassets simulieren

Mit einer Simulation können Sie das Netz auf Schwachstellen für Angriffe aus verschiedenen Quellen testen.

Mit Angriffssimulationen können Sie die Konfigurationen von Einheiten im Netz überprüfen.

Simulationen ermöglichen folgende Schlüsselfunktionen:

- Anzeige der theoretischen Pfadumsetzungen, die bei einem Angriff auf das Netz verwendet werden können
- Anzeige der möglichen Verbreitung von Angriffen auf den Netzeinheiten und des möglichen Übergriffs auf andere Assets.
- Erkennung neuer Sites mit Sicherheitslücken durch die Überwachung

Simulation erstellen

Sie können eine Simulation für eine Netzattacke auf ein SSH-Protokoll erstellen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie in der Liste **Aktionen** den Eintrag **Neu**.
4. Geben Sie einen Namen für die Simulation ein.
5. Wählen Sie **Current Topology** (Aktuelle Topologie) aus.
6. Aktivieren Sie das Kontrollkästchen **Use Connection Data** (Verbindungsdaten verwenden).
7. Wählen Sie in der Liste **Where do you want the simulation to begin** (Wo soll die Simulation beginnen) einen Startpunkt für die Simulation aus.
8. Fügen Sie folgende Simulationsattacke hinzu: **Attack targets one of the following open ports using protocols** (Attacke auf einen der folgenden offenen Ports unter Verwendung von Protokollen).
9. Klicken Sie für diese Simulation auf **Offene Ports** und fügen Sie dann Port 22 hinzu.
10. Klicken Sie auf **Protokolle** und wählen Sie dann **TCP** aus. Das SSH-Protokoll verwendet TCP.
11. Klicken Sie auf **OK**.
12. Klicken Sie auf **Save Simulation** (Simulation speichern).
13. Wählen Sie in der Liste **Aktionen** den Eintrag **Run Simulation** (Simulation ausführen). In der Ergebnisspalte wird ein Listenfeld mit dem Datum angezeigt, an dem die Simulation ausgeführt wurde, sowie mit einem Link zum Anzeigen der Ergebnisse.
14. Klicken Sie auf **View Results** (Ergebnisse anzeigen).

Ergebnisse

In den Ergebnissen wird eine Liste der Assets mit SSH-Schwachstellen angezeigt, sodass Netzadministratoren die SSH-Verbindungen genehmigen können, die in diesem Netz zulässig sind oder erwartet werden. Die nicht genehmigte Kommunikation kann auf Ereignisse und Angriffe überwacht werden.

Die angezeigten Ergebnisse liefern Netzadministratoren oder Sicherheitsspezialisten eine visuelle Darstellung des Attackenpfads und der Verbindungen, über die die Attacke im Netz verlief. In einem ersten Schritt wird beispielsweise eine Liste der direkt verbundenen Assets erstellt, die von der Simulation betroffen sind. In einem zweiten Schritt werden die Assets im Netz aufgelistet, die mit den Assets der ersten Ebene in der Simulation kommunizieren können.

Anhand der Informationen, die die simulierte Attacke liefert, können Sie das Netz testen und gegen Tausende möglicher Attackenszenarien verstärken.

Anwendungsfall: Risiko von Netzkonfigurationsänderungen simulieren

Mithilfe eines Topologiemodells können Sie auf Basis Ihres vorhandenen Netzes ein virtuelles Netzmodell definieren. Das von Ihnen erstellte Netzmodell kann auf einer Reihe von Modifikationen basieren, die kombiniert und konfiguriert werden können.

Mithilfe eines Topologiemodells können Sie durch Simulation die Auswirkungen von Konfigurationsänderungen auf das Netz testen.

Topologiemodelle ermöglichen folgende Schlüsselfunktionen:

- Erstellen virtueller Topologien zum Testen von Änderungen im Netz
- Simulation von Attacken auf virtuelle Netze
- Senkung des Risikos und Verringerung der Sicherheitslücken für geschützte Assets durch Tests
- Eingrenzung und Testen von besonders gefährdeten Teilen des Netzes oder Assets mithilfe von virtuellen Netzsegmenten

So simulieren Sie eine Netzkonfigurationsänderung:

1. Topologiemodell erstellen
2. Attacke auf das Topologiemodell simulieren

Topologiemodell erstellen

Sie können ein Topologiemodell erstellen, um Netzänderungen zu testen und Attacken zu simulieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulationen** > **Topology Models (Topologiemodelle)** aus.
3. Wählen Sie in der Liste **Aktionen** den Eintrag **Neu** aus.
4. Geben Sie einen Namen für das Modell ein.
5. Wählen Sie ggf. Modifikationen aus, die auf die Topologie angewendet werden sollen.

6. Konfigurieren Sie die Tests, die dem Teilfenster **Configure model as follows** (Modell wie folgt konfigurieren) hinzugefügt wurden.
7. Klicken Sie auf **Save Model** (Modell speichern).

Nächste Schritte

Erstellen Sie eine Simulation für das neue Topologiemodell.

Attacke simulieren

Sie können eine Attacke auf Ports und Protokolle simulieren.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Risks** (Risiken).
2. Wählen Sie im Navigationsmenü **Simulation** > **Simulationen** aus.
3. Wählen Sie in der Liste **Aktionen** den Eintrag **Neu**.
4. Geben Sie einen Namen für die Simulation ein.
5. Wählen Sie ein von Ihnen erstelltes Topologiemodell aus.
6. Wählen Sie in der Liste **Where do you want the simulation to begin** (Wo soll die Simulation beginnen) einen Startpunkt für die Simulation aus.
7. Fügen Sie folgende Simulationsattacke hinzu: **Attack targets one of the following open ports using protocols** (Attacke auf einen der folgenden offenen Ports unter Verwendung von Protokollen).
8. Klicken Sie für diese Simulation auf **Offene Ports** und fügen Sie dann Port 22 hinzu.
9. Klicken Sie auf **Protokolle** und wählen Sie dann 'TCP' aus. Das SSH-Protokoll verwendet TCP.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf **Save Simulation** (Simulation speichern).
12. Wählen Sie in der Liste **Aktionen** den Eintrag **Run Simulation** (Simulation ausführen). In der Ergebnisspalte wird ein Listenfeld mit dem Datum angezeigt, an dem die Simulation ausgeführt wurde, sowie mit einem Link zum Anzeigen der Ergebnisse.
13. Klicken Sie auf **View Results** (Ergebnisse anzeigen).

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Website Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken oder Servicemarken anderer Hersteller sein.

Hinweise zur Datenschutzrichtlinie

IBM Software-Produkte, einschließlich "Software as a Service"-Lösungen (Softwareangebote) verwenden möglicherweise Cookies oder andere Technologien, um Nutzungsinformationen zum Produkt zu erfassen, die Erfahrung der Endbenutzer zu verbessern, Interaktionen mit dem Endbenutzer zu optimieren usw. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Je nachdem, welche Konfigurationen bereitgestellt sind, kann dieses Softwareangebot Sitzungscookies verwenden, die für das Sitzungsmanagement und die Authentifizierung die Sitzungs-ID jedes Benutzers erfassen. Diese Cookies können inaktiviert werden, dadurch geht aber auch die von diesen bereitgestellte Funktionalität verloren.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der IBM Datenschutzrichtlinie unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzrichtlinie unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und im "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Index

GI13-3917-00