IBM Security QRadar Vulnerability Manager

Mehr Sicherheit und Compliance durch Priorisierung von Sicherheitslücken bei der Problemlösung

Highlights

- Weniger Sicherheitsverstöße durch frühzeitige Erkennung von Schwachstellen mit hohem Risiko über ein zentrales, integriertes Dashboard
- Priorisierung von Korrektur- und Risikominderungsmaßnahmen durch ein fundiertes Verständnis des gesamten Netzwerkkontexts
- Nahtlose Integration in IBM Security QRadar SIEM als Basis für dynamische, aktuelle Assetinformationen für ein proaktives Schwachstellenmanagement
- Schnelle Netzwerk-Scanoperationen in regelmäßigen oder dynamischen Abständen zum Aufspüren von Sicherheitslücken und zur Minimierung von Risiken
- Automatisierte Complianceprozesse durch effiziente Erfassung, Korrelation und Berichterstellung

Für viele Unternehmen ist das Management von Netzwerkschwachstellen oft ein Problem. Schwachstellenscans werden in der Regel erst als Reaktion auf Compliancevorgaben durchgeführt und können je nach Netzwerkgröße durchaus Tausende von Sicherheitsrisiken offenlegen. Die Ergebnisse solcher Scans erweisen sich oft als komplexes Puzzle aus fehlerhaft konfigurierten Geräten, nicht gepatchter Software und veralteten Systemen. Sicherheitsadministratoren stehen daher vor dem Problem, die Sicherheitsrisiken mit dem größten Gefährdungspotenzial innerhalb kürzester Zeit erkennen und korrigieren zu müssen.

Gleichzeitig steigt die Anzahl der Sicherheitsverstöße in den Unternehmen weiterhin stark an. Dies reicht von großen Unternehmen aus Branchen wie E-Commerce und Social Networking bis zu Unternehmen aus den Bereichen Gesundheitswesen, Universitäten, Banken und Behörden – die Bandbreite der Zielgruppen ist enorm. Neben der steigenden Anzahl der festgestellten Sicherheitslücken hat sich auch die Anzahl der Vorfälle, durch die es zum Verlust, Diebstahl oder zur Offenlegung personenbezogener Daten kam, um nahezu 40 Prozent erhöht. [1]

Mit IBM Security QRadar Vulnerability Manager können Unternehmen Probleme bei der Netzwerksicherheit minimieren. Erreicht wird dies durch einen proaktiven Ansatz bei der Suche nach Schwachstellen und die Verringerung potenzieller Risiken. Dabei kommen bewährte Schwachstellenscanner zum Einsatz, die immer aktuelle Ergebnisse liefern. Im Gegensatz zu anderen Lösungen nutzt die Vulnerability Manager-Lösung von IBM das Leistungsspektrum der IBM QRadar Security Intelligence Platform, um die Daten im Gesamtkontext von Netzwerknutzung, Sicherheit und möglichen Sicherheitsrisiken darzustellen. Durch die Konsolidierung der Ergebnisse der Schwachstellenscanner, von Risikomanagementlösungen und externen sicherheitsspezifischen

Informationsressourcen funktioniert QRadar Vulnerability Manager ähnlich wie ein zentrales Control-Center. So lassen sich kritische Schwachstellen schnell erkennen und beheben, um weitere Attacken zu vermeiden.

QRadar Vulnerability Manager unterstützt Sicherheitsteams in vielen Bereichen: Erkennung von Ressourcenkonfigurationsproblemen, Verstehen der Auswirkungen von Zeitplänen für die Implementierung von Software-Patches, Koordination mit Intrusion Prevention-Systemen zum Blocken offener Verbindungen und Einrichtung einer kontinuierlichen Systemüberwachung. All dies erfolgt über ein zentrales, integriertes Dashboard. Mit QRadar Vulnerability Manager lassen sich zahlreiche Informationen mit den Schwachstellendaten korrelieren: QRadar SIEM-Ereignis- und Risikoanalysen, Analyse von Gerätekonfigurationen und Netzwerkverkehr über IBM Security QRadar Risk Manager und externe Datenbanken (wie z. B. IBM X-Force Threat Intelligence). So hilft diese Lösung Unternehmen dabei, durchdachte Pläne zu erarbeiten, um die IT-Mitarbeiter gezielt einzusetzen. Hinzu kommt, dass durch die Vorabintegration in die QRadar Security Intelligence Platform die Sicherheitsteams ein System weniger installieren, konfigurieren und verwalten müssen.

Eine priorisierte Übersicht möglicher Schwachstellen

Mit QRadar Vulnerability Manager lässt sich genau festlegen, wie IT-Sicherheitsteams Daten für die Schwachstellenanalyse erfassen und nutzen – dadurch entfallen aufwendige monatliche oder vierteljährliche Scanoperationen und Berichterstellungen zugunsten eines detaillierten und kontinuierlichen Überwachungsprozesses. Die intuitive Benutzeroberfläche der Lösung bietet umfassende Transparenz in alle dynamischen, mehrschichtigen Netzwerke. So organisieren Sie Ihren Scan:

- Wählen Sie eine Dashboardsicht und Klicken Sie durch die jeweiligen Tabs, um Sicherheitsverletzungen, Protokollereignisse, Netzwerkflüsse, Assetstatusinformationen und -konfigurationen, Berichte, Risiken und Schwachstellen zu prüfen.
- Erstellen, bearbeiten und speichern Sie Assetsuch- und -scanoperationen für die intelligente Assetüberwachung.
- Treffen Sie schnellere und fundiertere Entscheidungen durch eine konsolidierte Sicht mit Prioritätenvergabe zu den Scandaten.
- Koordinieren Sie auf effiziente Weise alle Aktivitäten beim Patching und virtuellen Patching und steuern Sie gezielt Intrusion Prevention-Systeme (IPSs), um mögliche Attackenpfade effektiv zu blocken.

IBM Security QRadar Vulnerability Manager bietet ein zentrales, integriertes Dashboard für die Anzeige mehrerer Feeds zu Schwachstellenanalysen und Informationsressourcen zu Sicherheitsbedrohungen. Auf diese Weise können Sicherheitsteams sehr schnell die Sicherheitsrisiken erkennen, die die größte Gefährdung darstellen.

Mit der integrierten Scan-Engine von QRadar Vulnerability Manager können sowohl dynamische als auch periodische Scanoperationen durchgeführt werden. So ergibt sich eine echtzeitnahe Transparenz zu Schwachstellen, die andernfalls nicht offengelegt werden könnten. Mit den Passive Asset Discovery-Funktionen der IBM Security QRadar QFlow- und Log Collector-Appliances kann jedes neue Asset im Netzwerk sofort gescannt werden. Dadurch können Unternehmen Sicherheitsrisiken auf intelligente Sicherheitsbedrohungen zwischen den regelmäßigen Scanzyklen reduzieren und die Einhaltung aller aktuellen Sicherheitsbestimmungen gewährleisten.

Da QRadar Vulnerability Manager denselben regelbasierten Ansatz wie QRadar SIEM QRadar nutzt, lassen sich Fehlalarme minimieren und Sicherheitslücken herausfiltern, die bereits als „harmlos“ klassifiziert wurden. So können beispielsweise Anwendungen auf einem Server installiert sein, die noch nicht aktiviert wurden und daher kein Sicherheitsrisiko darstellen. Geräte, die als mögliche Schwachstelle identifiziert werden, können durch eine Firewall geschützt werden. Ein weiteres Beispiel wären Endpunkte mit Schwachstellen, für die jedoch bereits Patches zu einem geplanten Zeitpunkt implementiert werden.

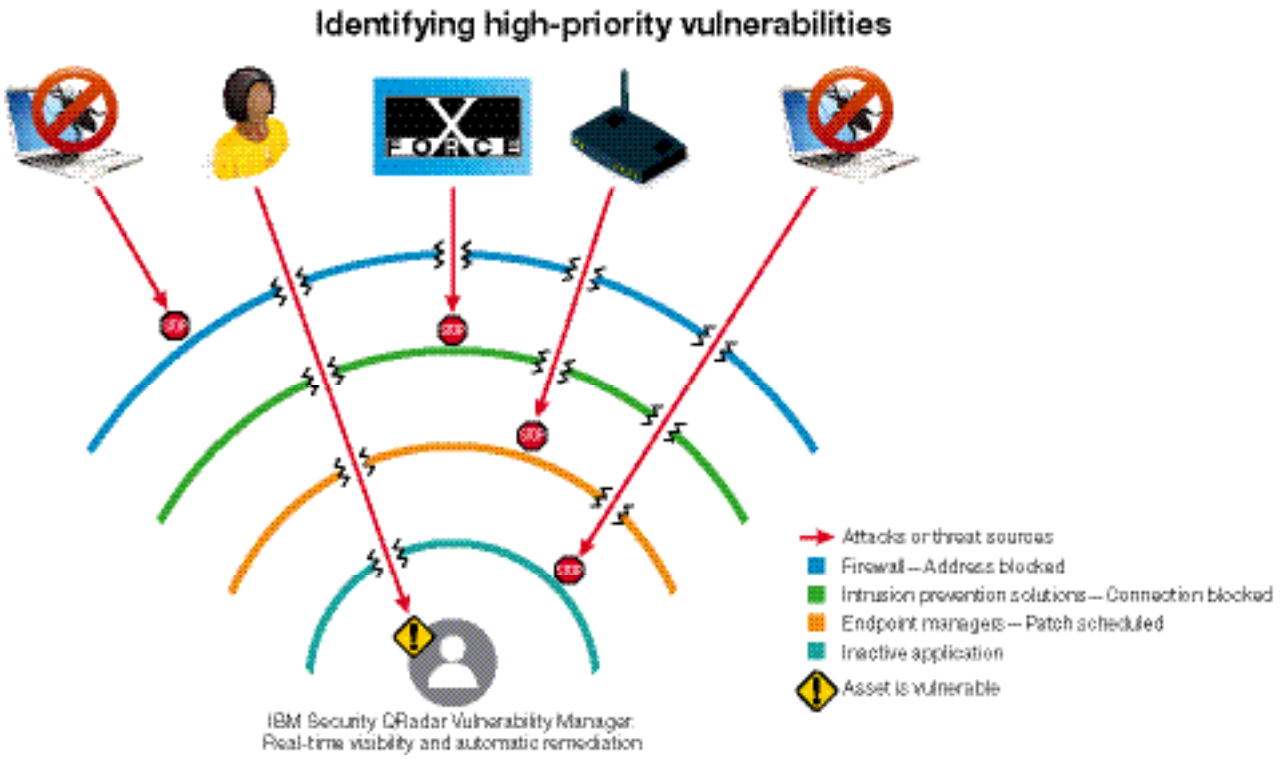
QRadar Vulnerability Manager stellt eine aktuelle netzwerkspezifische Sicht zu allen erkannten Sicherheitslücken bereit – einschließlich Detailinformationen wie Zeitpunkt der Feststellung von Sicherheitslücken, letztmaliges Auftreten, verwendete Scan-Jobs und Zuweisung der Sicherheitslücken zu den zuständigen Mitarbeitern, um geeignete Korrektur- oder Risikominderungsmaßnahmen einzuleiten. Darüber hinaus bietet die Software Langzeitsichten zu täglichen, wöchentlichen und monatlichen Trends. Zudem können langfristige Trendberichte erstellt werden, wie beispielsweise in der Payment Card Industry (PCI) übliche monatliche Trendberichte, in denen aufgetretene Schwachstellen im abgelaufenen Jahr dokumentiert werden.

Bei eigenständigen, unabhängigen Lösungen für die Schwachstellensuche kann das Scannen großer Adressräume für Assets, Server und Services sehr zeitaufwendig sein, sodass die Scanergebnisse oft nicht mehr aktuell sind. Solche Einzellösungen erfordern zudem weitere Infrastrukturen und beinhalten unterschiedliche Technologien für das Scannen von Netzwerken, Anwendungen und Datenbanken – und erhöhen dadurch den Verwaltungsaufwand. Selbst nach dem Erkennen einer unüberschaubar großen Zahl häufig unvollständiger Schwachstellen bieten die Einzellösungen keine Kontextinformationen, die den Sicherheitsteams bei der Priorisierung ihrer Fehlerkorrekturaufgaben weiterhelfen könnten.

Intelligente Sicherheitsrisiken vermeiden

Im Gegensatz zu in der Vergangenheit üblichen zufälligen Brute-Force-Attacken müssen sich Unternehmen heute gegen Advanced Persistent Threats (APT) wehren. Hierbei handelt es sich um Attacken, die häufig über einen langen Zeitraum auftreten. Mithilfe verschiedener Taktiken wie Zero-Day-Exploits, spezielle Malware oder die Suche nach ungepatchten Systemen sondieren die Angreifer konsistent ihre Ziele mithilfe eines „Low-and-Slow“-Ansatzes, bis sie eine Sicherheitslücke finden. Unternehmen können dem intelligente Tools wie QRadar Vulnerability Manager entgegensetzen, um ihre Verteidigungsstrategien zu optimieren, indem sie regelmäßig so viele gravierende Schwachstellen wie möglich scannen und beheben.

Die meisten Schwachstellenscanner identifizieren jedoch einfach nur eine große Anzahl an Sicherheitslücken und überlassen den Sicherheitsteams die Einschätzung des Schweregrads der Risiken. Diese Tools sind zudem in vielen Fällen nicht in die vorhandene Sicherheitsinfrastruktur integriert. Die Anpassung an die aktuelle Netzwerktopologie, Nutzungsinformationen und Sicherheitsprozesse ist daher sehr aufwendig. Viele dieser Tools werden in der Regel nur für Compliancezwecke eingesetzt und weniger als integraler Bestandteil eines Sicherheitsrisiko- und -management-programms gesehen.



QRadar Vulnerability Manager nutzt Sicherheitsdaten, um Schwachstellen herauszufiltern. Dadurch erkennen Unternehmen schneller, wie sie ihre Korrekturmaßnahmen oder Risikominderungsaktivitäten priorisieren müssen.

QRadar Vulnerability Manager bietet auch hier Unternehmen viele Möglichkeiten:

- Nutzen der bestehenden Appliance-Infrastruktur und Sicherheitsdaten, um problemlos automatisierte Scanoperationen für Schwachstellen im Netzwerk durchführen zu können.
- Erkennen, wann neue Assets dem Netzwerk hinzugefügt wurden, ein abnormales Verhalten aufweisen oder möglicherweise beeinträchtigt werden. Hierfür werden Protokollereignisse und Netzwerkflussdaten verwendet, sodass unmittelbar Scanoperationen durchgeführt werden können, um die Assets entsprechend zu schützen und die Netzwerktransparenz zu verbessern.
- Verbessern der Produktivität, da sich die Sicherheitsteams auf eine kleine Anzahl einfach zu verwaltender Ereignisse mit hoher Priorität konzentrieren können. So lassen sich Fehlalarme vermeiden und Ergebnisse schneller mit Aktivitäten zur Netzwerkblockung korrelieren.

Complianceanforderungen einhalten

Gesetzliche Bestimmungen zwingen Unternehmen aller Größenordnungen, Programme für das Schwachstellenmanagement zu entwickeln, um die ordnungsgemäße Kontrolle vertraulicher IT-Ressourcen sicherzustellen. QRadar Vulnerability Manager hilft diesen Unternehmen, solche Bestimmungen ohne großen Aufwand einzuhalten, indem das Netzwerk regelmäßig gescannt wird und detaillierte Prüfprotokolle geführt werden. Dabei wird jede Sicherheitslücke mithilfe einer Sicherheitseinstufung und einer Gefährdungsstufe kategorisiert. Neben den internen und externen Scanoperationen können die Sicherheitsteams mithilfe von QRadar Vulnerability Manager Tickets erstellen. So behalten Sie den Überblick über die Korrekturmaßnahmen und können zudem Ausnahmebedingungen in einem umfassenden Prüfprotokoll aufzeichnen.

Die Vorteile von QRadar Vulnerability Manager in diesem Bereich:

- Koordination einer großen Anzahl parallel ablaufender Prüfungen ohne Störung des normalen Netzwerkbetriebs – mehrere Personen können das Netzwerk nach Bedarf (auch mehrmals) scannen, um die Wirksamkeit ihrer Korrekturmaßnahmen zu prüfen.
- Auswertung der Schwachstellenanalysen nach Tag, Woche und Monat, um Berichte effektiv nutzen und Trends transparenter darstellen zu können.
- Durchführen von Scanoperationen innerhalb und außerhalb des Netzwerks.
- Aufzeichnen eines Prüfprotokolls zu allen Aktivitäten in Bezug auf das Schwachstellenmanagement wie Erkennung, Zuweisung, Hinweise, Ausnahmebedingungen und Korrekturen.

Sicherheitsdaten erweitern

QRadar Vulnerability Manager kombiniert die sicherheitsspezifische Echtzeittransparenz der QRadar Security Intelligence Platform mit den Ergebnissen der bewährten Technologie für die Schwachstellensuche. Als Teil der QRadar SIEM-Architektur lässt sich QRadar Vulnerability Manager innerhalb kürzester Zeit über einen Lizenzschlüssel aktivieren – ohne zusätzliche Hardware oder Software. Dies kann beträchtliche Kosteneinsparungen mit sich bringen, da die Sicherheitsteams in der Regel keine neuen Technologien implementieren oder neue Benutzeroberflächen erlernen müssen. Vielmehr können sie problemlos Berichte über die vertraute Benutzeroberfläche der QRadar-Produktfamilie generieren.

Die wichtigsten Integrationsprodukte für QRadar Vulnerability Manager sind nachfolgend aufgeführt:

- **QRadar SIEM:** Bietet die Appliance-Infrastruktur für Netzwerk-Scanoperationen, die Assetdatenbank für die Protokollierung/Verfolgung der Aktivitäten für das Schwachstellenmanagement und die Passive Network Detection-Funktionen für das Erkennen neu hinzugefügter Assets. Außerdem werden über diese Infrastruktur alle kontextbezogenen Sicherheitsdaten bereitgestellt, die für die Erstellung und Durchführung der Schwachstellenmanagementpläne gebraucht werden.
- **QRadar Risk Manager:** Stellt aktuelle Daten und Langzeitdaten zur Netzwerkverbindung bereit. So kann der Bezug zwischen den Schwachstellen und der gesamten Netzwerktopologie aufgezeigt werden. Hierzu gehört auch die Darstellung, wie sich Firewall- und IPS-Regeln auf die Verwertbarkeit bestimmter Assets aus riskanten internen und externen Quellen auswirken.
- **IBM Security SiteProtector™ System:** Bietet Funktionen für das virtuelle Patching mithilfe netzwerkspezifischer IPS-Signaturen, um sich gegen identifizierte Sicherheitsrisiken zu schützen, indem zugehörige Verbindungen geblockt werden.
- **X-Force Threat Intelligence Feed:** Stellt aktuelle Informationen zu empfohlenen Fixes und sicherheitsspezifische Empfehlungen zu aktiven Schwachstellen, Viren, Computerwürmern und Sicherheitsrisiken bereit.
- **IBM Endpoint Manager:** Optimiert Korrekturmaßnahmen durch automatisiertes Patch-Management für hunderte oder gar tausende von Endpunkten wie z. B. aktuelle mobile Geräte. Darüber hinaus steht eine integrierte Berichterstellungsfunktion für die Echtzeitüberwachung des gesamten Patchprozesses zur Verfügung.
- **IBM Security AppScan:** Unterstützt bei der Schwachstellenprüfung für Webanwendungen, sodass QRadar Vulnerability Manager im integrierten Dashboard transparent und nach Prioritäten geordnet Sicherheitslücken in Webanwendungen darstellen kann.
- **IBM InfoSphere Guardium Vulnerability Assessment:** Unterstützt das Scannen von Datenbankinfrastrukturen, sodass QRadar Vulnerability Manager im integrierten Dashboard transparent und nach Prioritäten geordnet Sicherheitslücken bei Datenbanken darstellen kann.

Proaktive Sicherheit

In einer Welt, in der kein Netzwerk wirklich sicher ist, hilft QRadar Vulnerability Manager Unternehmen durch umfassende proaktive Schutzmaßnahmen, ihre Umgebungen effektiv zu schützen:

- Schnelle interne Scanoperationen, um eine hohe Netzwerkleistung und -verfügbarkeit zu gewährleisten
- Unterstützung bei der Durchführung von Scanoperationen, nicht authentifizierten und authentifizierten sowie OVAL-Scanoperationen (Open Vulnerability Assessment Language)
- Externe Scanfunktionen, um das Netzwerk aus der Sicht eines Angreifers sehen und Compliancevorgaben leichter erfüllen zu können
- Benutzerfreundliche Untersuchungsoptionen über Dashboardanzeigen und umfassende, regelbasierte, schnelle Suchfunktionen, um mehr zu bestimmten Ereignissen zu erfahren oder langfristige Trends zu erkennen
- Unterdrückung zulässiger Schwachstellen, Fehlalarme oder anderer bisher nicht beseitigter Schwachstellen aus der laufenden Berichterstellung
- Lebenszyklusmanagement für Schwachstellenzuordnungen und -korrekturen
- Vollständiges Prüfprotokoll für die Einbindung in Complianceberichte

Warum IBM?

IBM Security bietet beim Thema Unternehmenssicherheit eines der innovativsten Produkt- und Serviceportfolios mit dem höchsten Integrationsfaktor. Das Lösungsportfolio, das von der weltweit anerkannten X-Force-Forschungs- und Entwicklungsgruppe unterstützt wird, stellt Sicherheitsdaten bereit, mit denen Unternehmen mit einem ganzheitlichen Ansatz Mitarbeiter, Infrastrukturen, Daten und Anwendungen schützen können. Hierfür steht eine große Anzahl von Lösungen für die unterschiedlichsten Bereiche zur Verfügung: Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Mit diesen Lösungen können Unternehmen ihr Risikomanagement wesentlich effektiver gestalten und integrierte Sicherheitsmechanismen für Mobile-, Cloud-, Social Media- und andere Geschäftsarchitekturen implementieren. IBM betreibt eine der weltweit größten Organisationen im Bereich der Erforschung, Entwicklung und Bereitstellung von Sicherheitslösungen, verwaltet die Überwachung von 13 Mrd. Sicherheitsereignissen pro Tag in mehr als 130 Ländern und besitzt über 3.000 Sicherheitspatente.

Weitere Informationen

Wenn Sie mehr über IBM Security QRadar Vulnerability Manager erfahren möchten, wenden Sie sich an Ihren IBM Ansprechpartner oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/software/products/us/en/category/SWI60

Finanzierungslösungen von IBM Global Financing können Ihnen bei der kosteneffizienten und strategisch richtigen Anschaffung von Softwarefunktionalität für Ihr Unternehmen helfen. Wir arbeiten bei der Ausarbeitung einer auf Ihre Geschäfts- und Entwicklungsziele abgestimmten Finanzierungslösung mit bonitätsgeprüften Kunden zusammen, um für Sie eine effektive Finanzdisposition und eine Reduzierung der Gesamtbetriebskosten zu erreichen. Finanzieren Sie Ihre kritischen IT-Investitionen und bringen Sie Ihr Unternehmen nach vorne mit IBM Global Financing. Weitere Informationen finden Sie unter: **ibm.com**/financing

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

[1] „IBM X-Force 2012 Trend and Risk Report“, *IBM Security Systems, März 2013.* http://www-03.ibm.com/security/xforce/downloads.html

WGD03027-DEDE-00