IBM Security
Thought-Leadership White Paper

Oktober 2016

Sicherheitsbedrohungen mit Informationen und Kontrollen zur Sicherheit an Endpunkten beseitigen

Mit IBM QRadar und IBM BigFix Sicherheitslücken priorisieren und deren Beseitigung beschleunigen

IBM

Inhalt

Einleitung

Die Zahl hochentwickelter Sicherheitsbedrohungen – von angepasster Malware bis hin zu Zero-Day-Exploits – nimmt weltweit enorm zu und die Angriffe werden raffinierter als je zuvor durchgeführt. Die Cyberkriminellen von heute sind äußerst versiert darin, potenzielle Opfer über E-Mail- oder webbasierte Angriffe sowie durch das Ausnutzen von Sicherheitslücken an den Endpunkten selbst zu ermitteln. Umfassende, koordinierte und operativ ausgereifte Angriffe werden heutzutage in weiten Teilen des Internets unter Umgehung der herkömmlichen Sicherheitsverfahren durchgeführt. Und die Zahl der Schäden durch Malware steigt immer weiter an.

Wie kann sich Ihr Unternehmen vor solch hochentwickelten Sicherheitsbedrohungen schützen? Das Aufrechterhalten eines hohen Niveaus an Grundsicherheit durch die einheitliche Umsetzung von Sicherheitsrichtlinien und Patch-Leveln an Endpunkten und auf Servern ist definitiv nötig und wichtig. Wenn bei der Überprüfung von Netzwerken allerdings mehrere Schwachstellen pro IP-Adresse festgestellt werden, können sich gefährliche Sicherheitslücken ergeben, wenn die Schwachstellen zu langsam beseitigt und Patches nur mit Verzögerung installiert werden. IT-Mitarbeiter müssen im heutigen Geschäftsumfeld schwierige, risikobasierte Entscheidungen darüber treffen, auf welche Bereiche sie ihre Maßnahmen konzentrieren. Häufig haben sie dabei keinen vollständigen Überblick über die Sicherheitsumgebung. Das ist umso kritischer, wenn die Zahl der Sicherheitslücken im Unternehmen zunimmt, während für deren Beseitigung nicht genügend Mitarbeiter und Fachkenntnisse zur Verfügung stehen. Unternehmen müssen nicht nur in der Lage sein, Sicherheitslücken effizient zu erkennen, sondern auch deren Gesamtzusammenhang zu berücksichtigen und ihnen Risiko-Level zuzuordnen, damit sie die Maßnahmen für die Beseitigung der Sicherheitslücken auf die Bereiche mit den größten Risiken konzentrieren können.

In diesem White Paper wird erläutert, wie hochentwickelte Sicherheitsbedrohungen durch die Einführung eines integrierten, intelligenten und automatisierten Konzepts für die Sicherheit an Endpunkten bewältigt werden können. Es wird zudem erläutert, wie Zusammenhänge und Funktionen der IBM® QRadar Security Intelligence-Plattform mit Informationen und Kontrollen von IBM BigFix zur Sicherheit an Endpunkten ausgeweitet werden, um Sicherheitsrisiken zu identifizieren, zu priorisieren und zu beseitigen. In diesem White Paper wird auch auf die strategischen Vorteile durch die gemeinsame Nutzung dieser Lösungen zur Bekämpfung moderner Methoden bei Hackerangriffen eingegangen.

IBM QRadar Security Intelligence-Plattform

Die QRadar Security Intelligence-Plattform ist eine zentrale Lösung, um Unternehmen dabei zu helfen, immer raffiniertere Angriffe wirksam zu bekämpfen. Die Unternehmen können damit ihre Netzwerkumgebungen absichern, ihr geistiges Eigentum schützen und Unterbrechungen der Geschäftsabläufe vermeiden. Die Lösung übernimmt mehr als nur die Überwachung von Protokollen und Netzwerkübertragungsdaten. Sie sammelt vielmehr Daten und Aktivitäten aus einer Vielzahl von Datenquellen und führt Echtzeitkorrelationen basierend auf Regeln und Informationen über Sicherheitsbedrohungen durch, damit Sicherheitsverstöße, die möglicherweise sofortige Maßnahmen erfordern, schnell erkannt werden.

IBM QRadar Risk Manager basiert auf der QRadar Security Intelligence-Plattform und bietet Unternehmen die Möglichkeit, Konfigurationen von Netzwerkgeräten proaktiv zu verwalten und mit der Netzwerktopologie zu verknüpfen. So können Sicherheitsrisiken und mögliche Angriffspfade analysiert und identifiziert werden.

IBM QRadar Vulnerability Manager basiert ebenfalls auf der QRadar Security Intelligence-Plattform und ermöglicht die effiziente Erkennung von Sicherheitslücken auf allen Geräten im Netzwerk. Damit können zudem Überprüfungsergebnisse von verschiedenen Schwachsellenscannern gesammelt und konsolidiert werden. QRadar Vulnerability Manager bietet sich aufgrund der Nutzung von Daten der QRadar Security Intelligence-Plattform und aus QRadar Risk Manager als zentraler Kontrollpunkt für Berichte über Sicherheitslücken und die Priorisierung im gesamten Unternehmen an.

IBM BigFix für die Sicherheit an Endpunkten

Der beste Schutz vor Sicherheitsbedrohungen an Endpunkten ist, Schwachstellen in der Software oder in Konfigurationen zu erkennen und die Endpunkte zu schützen, bevor ein Hacker die Schwachstellen ausnutzt und Schäden im Netzwerk auftreten. BigFix ist eine Lösung für das Management und die Sicherheit von Endpunkten. Der Kunde kann hiermit Konfigurationen, installierte Software, Betriebssystem- oder Anwendungspatches und die Einhaltung von Richtlinien an Endpunkten für alle Geräte dauerhaft überwachen. Die Grundlage hierfür sind entweder direkt verfügbare oder angepasste Richtlinien. Mit BigFix kann zudem die Nichteinhaltung von Bestimmungen mithilfe von IBM Fixlet-Nachrichten sofort behoben werden. Sie dienen dazu, den Konfigurationsstatus an einem Endpunkt zu ändern, die geeigneten Patches zu installieren, Malware-Dateien zu entfernen oder verdächtige Prozesse zu stoppen. Durch diesen kontinuierlichen Zyklus aus Überwachung, Berichterstellung und Fehlerbehebung lassen sich die Zeiträume für mögliche Angriffe deutlich verkürzen.

Nach den Ergebnissen im „Data Breach Investigations Report 2015“ wurde fast die Hälfte der neu berichteten Sicherheitslücken in den ersten vier Wochen nach deren Mitteilung ausgenutzt, weil Hacker wissen, dass viele Unternehmen neu aufgetretene Sicherheitslücken nicht wirksam beseitigen können.[1] Die Installation wirksamer Patches ist weiterhin die beste Vorgehensweise, um das Risiko zu vermeiden, dass neue Sicherheitslücken von Malware ausgenutzt werden. BigFix bietet einen automatisierten, vereinfachten und effizienten Patching-Prozess für alle Endpunkte innerhalb oder außerhalb des Unternehmensnetzwerks sowie für verschiedene Betriebssysteme und Anwendungen. Durch das Patching über BigFix können die Zeiträume für Patchzyklen verkürzt und die Betriebskosten spürbar verringert werden.

Bei Sicherheitslücken, für die noch keine Patches verfügbar sind (Zero-Day-Sicherheitslücken), bietet BigFix Unternehmen eine Remote-Quarantänefunktion zur Abgrenzung der betroffenen Endpunkte vom Netzwerk. Diese können damit vor Hackerangriffen geschützt werden und es wird verhindert, dass andere Endpunkte beschädigt werden, bis ein Patch oder eine andere Maßnahme zur Fehlerbehebung verfügbar ist.

Diskrepanzen beim Management von Sicherheitslücken beseitigen

Zum Schutz vor Sicherheitsbedrohungen benötigen Unternehmen ein umfassendes Konzept für die Identifizierung und die Vermeidung von Risiken mit hoher Priorität in einer sich ständig verändernden IT-Umgebung. Dieses Konzept sollte folgende Aufgaben beinhalten:

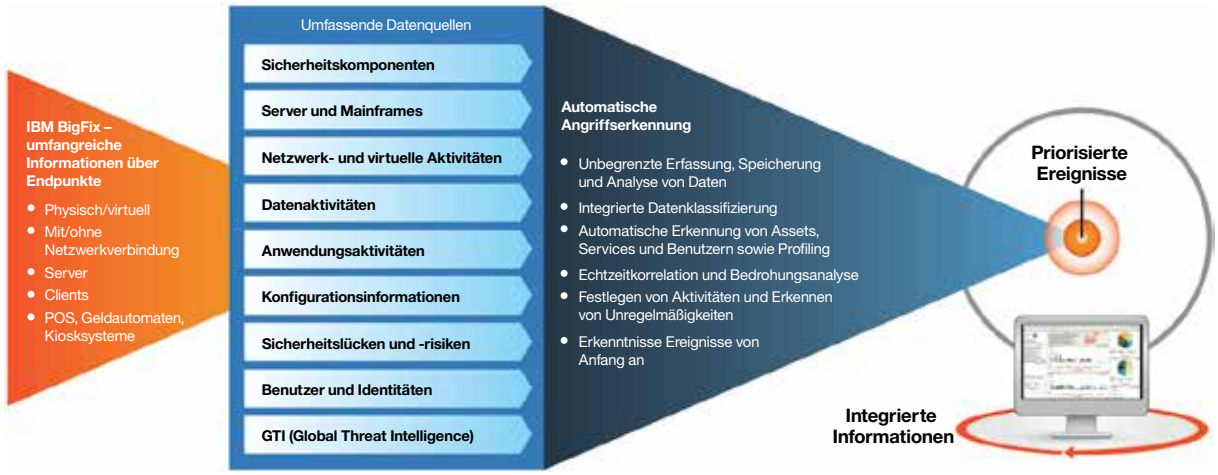
- Erkennen des aktuellen Status verschiedener Endpunkte
- Identifizieren der Sicherheitslücken an jedem Endpunkt
- Priorisieren der Sicherheitslücken
- Schnelle Durchführung von Maßnahmen zur Beseitigung oder Vermeidung von Sicherheitslücken mit hoher Priorität an Endpunkten oder Verschieben der betroffenen Geräte in Quarantäne
- Bestätigung, dass sich der Endpunkt durch die Maßnahmen zur Fehlerbehebung wieder in einem Status mit höherer Sicherheit befindet

Bei vielen Lösungen für das Management von Sicherheitslücken liegt der Schwerpunkt auf der Identifizierung oder Priorisierung von Sicherheitslücken. Sie bieten aber nicht die nötigen Informationen und Funktionen, um die priorisierten Sicherheitslücken wirksam zu beseitigen. IBM kann Unternehmen durch die Kombination von BigFix mit der QRadar Security Intelligence-Plattform dabei helfen, diese Lücke beim Management von Sicherheitslücken zu schließen. Mithilfe dieser integrierten Lösung können Unternehmen Sicherheitslücken in Betriebssystemen oder Anwendungssoftware identifizieren und priorisieren, die Hacker ausnutzen können. Die Unternehmen können die Sicherheitslücken anschließend beseitigen, um einen Angriff zu verhindern oder die Folgen für das Unternehmen auf ein Minimum zu reduzieren.

In sich geschlossenes Risikomanagement mit Informationen über Endpunkte einrichten

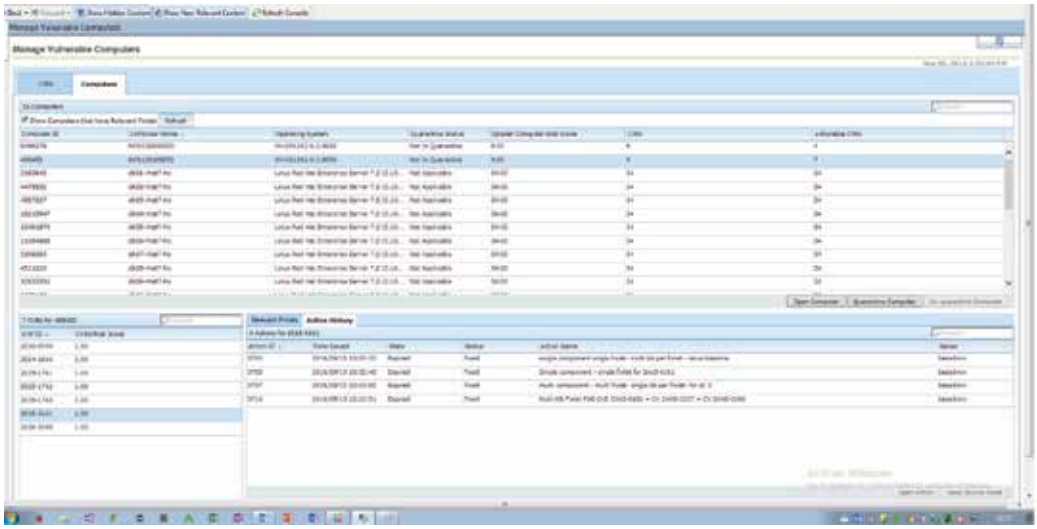
Die hochentwickelten Sicherheitsbedrohungen von heute erfolgen immer mehr im Verborgenen, mit mehr Dynamik und richten weit mehr Schäden als bisher an. Integrierte, intelligente und automatisierte Ressourcen werden daher dringender als je zuvor benötigt. Mit einer integrierten Lösung, bei der die QRadar Security Intelligence-Plattform und BigFix miteinander kombiniert werden, können IT Operations- und Sicherheitsteams zusammenarbeiten, um die Ressourcen vor immer raffinierteren Angriffen zu schützen.

BigFix liefert umfangreiche Informationen zum Status von Endpunkten nahezu in Echtzeit. Dies umfasst Berichte über installierte Patches, aktuelle Änderungen an der Konfiguration und mehr zur QRadar Security Intelligence-Plattform, um die Genauigkeit von Risikoanalysen des Systems zu erhöhen. Genauer gesagt beurteilt der BigFix Agent, der auf einem Endpunkt innerhalb oder außerhalb des Unternehmensnetzwerks ausgeführt wird, konfinuierlich die Konfiguration und die Einhaltung von Patch-Richtlinien. Der neueste Status wird jeweils an QRadar weitergeleitet, damit QRadar den Status des Endpunkts mit anderen Sicherheitsereignissen oder Netzwerkaktivitäten korrelieren kann, um verdächtige Ereignisse aufzuzeigen.



IBM BigFix übertragt den neuesten Status von Endpunkten an IBM QRadar. Dort wird der Status mit anderen Sicherheitsereignissen korreliert, um verdächtige Ereignisse aufzuzeigen und zu priorisieren.

Mit QRadar Vulnerability Manager können Sicherheitslücken untersucht oder aus BigFix und anderen Schwachstellenscannern für Endpunkte gesammelt werden. Außerdem kann für jede Ressource basierend auf einem größeren Kontext (beinhaltet Netzwerktopologie und Kommunikationsaktivitäten), der von QRadar Risk Manager bereitgestellt wird, eine Risikobewertung vorgenommen werden. Die Risikobewertung für die Sicherheitslücken und Ressourcen wird anschließend an BigFix übertragen. Für jede von QRadar erkannte Sicherheitslücke kann BigFix die geeigneten Maßnahmen zur Fehlerbehebung (Patching oder Quarantäne) identifizieren, die die IT-Mitarbeiter durchführen sollten. Die IT-Mitarbeiter können wiederum auf der Grundlage der Risikobewertung für die Ressourcen, der Anzahl an Sicherheitslücken an jedem Endpunkt oder der verfügbaren Maßnahmen zur Fehlerbehebung ihre Maßnahmen priorisieren, damit die kritischsten Sicherheitslücken zuerst beseitigt werden.



Mit IBM BigFix können von QRadar Vulnerability Manager identifizierte Sicherheitslücken effektiv beseitigt werden. Es liefert verschiedene Kennzahlen, auf deren Grundlage der Kunde Maßnahmen zur Fehlerbehebung priorisieren kann.

Nach der Durchführung der Maßnahmen zur Fehlerbehebung wird der aktuelle Status des Endpunkts an QRadar übertragen. Dort wird der Status erneut mit anderen Sicherheitsereignissen oder Netzwerkaktivitäten korreliert und die Angaben über die zuvor berichteten verdächtigen Ereignisse werden möglicherweise aktualisiert. Durch die Verknüpfung der Informationen und Kontrolle über Endpunkte in BigFix mit den unternehmensweiten Sicherheitsinformationen von QRadar können Unternehmen ein dauerhaftes Programm für ein in sich geschlossenes Risikomanagement auf den Weg bringen und Sicherheitsbedrohungen effektiv beseitigen.

- Erhöht Genauigkeit der Assetdatenbank
- Verbessert Risikobewertungen
- Verbessert Complianceberichte

- Beschleunigt Risikopriorisierung von Sicherheitsbedrohungen und -lücken
- Weitet Bewertungen von Sicherheitslücken auf Endpunkte außerhalb des Netzwerks aus

IBM BigFix und IBM QRadar bilden gemeinsam ein integriertes System für ein in sich geschlossenes Risikomanagement, mit Echtzeitinformationen über Endpunkte und unternehmensweiten Sicherheitsanalysen.

Fazit

Um das Management von Sicherheitslücken effektiver zu gestalten, benötigen Unternehmen ein integriertes Konzept, das sowohl Informationen über Endpunkte als auch Zusammenhänge im Netzwerk beinhaltet. Die IT-Mitarbeiter müssen wissen, für welche Sicherheitslücken von einem Endpunktmanagement-System Patches installiert werden sollen und für welche nicht. Damit kann sichergestellt werden, dass Maßnahmen zur Fehlerbehebung effizient priorisiert werden. Außerdem müssen die IT-Mitarbeiter in der Lage sein, schnell Maßnahmen im Zusammenhang mit Sicherheitsinformationen durchzuführen und die notwendigen Updates an allen Endpunkten im Unternehmen vorzunehmen.

QRadar- und BigFix-Lösungen können zusammenarbeiten, um Unternehmen bei der Beseitigung hochentwickelter Sicherheitsbedrohungen zu helfen. Dieser intelligente, automatisierte und integrierte Ansatz bietet einen strategischen Nutzen, da die Grundlagen für ein konsolidiertes Management und die effiziente Nutzung von Sicherheitsressourcen geschaffen werden. Die Reaktionszeiten bei Sicherheitsereignissen, einschließlich der Verzögerungen zwischen dem Auftreten und dem Erkennen von Sicherheitslücken, können verkürzt werden, wenn Sie die nahezu in Echtzeit bereitgestellten Details zum Endpunktstatus aus BigFix mit den Sicherheitsinformationen von QRadar-Lösungen kombinieren. Dadurch lassen sich Millionen von Sicherheitsereignissen auf eine überschaubare, priorisierte Anzahl von Schwachstellen verringern. Unternehmen können auf diese Weise eine proaktive Vorgehensweise zum Schutz ihrer IT-Ressourcen vor den beständigsten Sicherheitsbedrohungen umsetzen und Risiken spürbar reduzieren.

Nationale Sicherheit erfordert die Einhaltung von Bestimmungen an Endpunkten in Echtzeit

Bundesbehörden müssen eine Vielzahl von Sicherheitsbedrohungen bewältigen. Dies hat zu regulatorischen Bestimmungen für die Einführung von Lösungen geführt, mit denen Sicherheitslücken kontinuierlich überwacht, verwaltet und beseitigt werden können. Die Einbindung von QRadar- und BigFix-Lösungen bietet Bundesbehörden einen enormen geschäftlichen Nutzen.

Mit einer für Großunternehmen konzipierten Lösung zur Cybersicherheit können staatliche Behörden Sicherheitsbedrohungen bekämpfen und Schwachstellen beseitigen. Z. B. haben über 50 amerikanische Bundesbehörden BigFix als Standardlösung eingeführt. Sie verwalten und schützen damit über drei Millionen Workstations, physisch vorhandene und virtuelle Server und andere Endpunkte mit einem breiten Spektrum von Betriebssystemen. Solche Lösungen liefern dauerhaft Echtzeitinformationen über die Sicherheit und Compliance an Endpunkten, indem sie auf eine Bibliothek mit vielen Tausenden von Checks zurückgreifen.

Weitere Informationen

Wenn Sie mehr über die IBM QRadar Security Intelligence-Plattform, IBM BigFix oder andere Lösungen von IBM Security erfahren möchten, wenden Sie sich bitte an den zuständigen IBM Vertriebsbeauftragten oder IBM Business Partner, oder besuchen Sie uns unter: **ibm.com**/security

Informationen zu IBM Security-Lösungen

IBM Security bietet eines der innovativsten und am besten aufeinander abgestimmten Portfolios mit Sicherheitsprodukten und -services für Unternehmen. Das Portfolio, das durch die weithin bekannte Forschungs- und Entwicklungsgruppe IBM X-Force unterstützt wird, bietet die notwendige Security-Intelligence, um Unternehmen beim umfassenden Schutz von Personen, Infrastrukturen, Daten und Anwendungen zu unterstützen. Erreicht wird dies durch die Bereitstellung von Lösungen für Identitäts- und Zugriffsmanagement, Datenbanksicherheit, Anwendungsentwicklung, Risikomanagement, Endpunktmanagement, Netzwerksicherheit und vieles mehr. Diese Lösungen unterstützen Unternehmen beim erfolgreichen Risikomanagement und bei der Implementierung integrierter Sicherheit für mobile, Cloud-, Social Media- und andere Geschäftsarchitekturen. IBM betreibt eine der weltweit größten Einrichtungen für die Erforschung, Entwicklung und Bereitstellung von Sicherheitstechnologien, überwacht täglich ca. 13 Milliarden Sicherheitsereignisse in mehr als 130 Ländern und besitzt mehr als 3.000 Patente im Bereich Sicherheitstechnologie.

IBM Global Financing bietet darüber hinaus zahlreiche Zahlungsoptionen, damit Sie die erforderliche Technologie zur Ausweitung Ihrer Geschäftstätigkeit erwerben können. Wir übernehmen das Management von IT-Produkten und -Services über den gesamten Lebenszyklus, von der Anschaffung bis zur Entsorgung. Weitere Informationen finden Sie unter: **ibm.com**/financing

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

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

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

[1] „2015 Data Breach Investigations Report“, *Verizon*, April 2015. https://msisac.cisecurity.org/whitepaper/documents/1.pdf

Bitte der Wiederverwertung zuführen

WGW03051-DEDE-02