Technology Blueprint

McAfee
An Intel Company

SCHUTZ VON DATENBANKEN

Besserer Schutz vor Angriffen und Datenverlusten

SECURITY CONNECTED-REFERENZARCHITEKTUR

STUFE 1 2 **3** 4 5

Security Connected

Das Security Connected-Framework von McAfee ermöglicht die Integration mehrerer Produkte, Dienste und Partnerschaften, um eine zentrale, effiziente sowie effektive Risikominimierung zu erreichen. Mit der Basis von mehr als zwei Jahrzehnten bewährter Sicherheitspraktiken, hilft der Security Connected-Ansatz Unternehmen aller Größen und Bereiche aus der ganzen Welt bei der Verbesserung ihrer Sicherheitslage, der Optimierung der Sicherheit für eine höhere Wirtschaftlichkeit sowie bei der strategischen Sicherheitsausrichtung auf Geschäftsinitiativen. Die Security Connected-Referenzarchitektur bietet einen konkreten Weg von der Idee zur Implementierung. Nutzen Sie sie, um die McAfee Security Connected-Konzepte an Ihre speziellen Risiken, Ihre Infrastruktur und Geschäftsziele anzupassen. McAfee ist stets auf der Suche nach neuen Möglichkeiten, um seine Kunden umfassend zu schützen.

Besserer Schutz vor Angriffen und Datenverlusten

Die Situation

Im Jahr 2010 stieg die Zahl an Datenschutzverstößen auf ein Rekordniveau, wobei es bei 47 Prozent aller Angriffe nur wenige Minuten oder Stunden dauerte, bis ein Schaden entstand. Weitere 44 Prozent waren in Tagen erfolgreich wie der Verizon/U.S. Secret Service 2011 Untersuchungsbericht zu Datenkompromittierungen darlegt. Die Bösewichte erhalten also Zugriff, und zwar schnell. Und die Guten können nur sehr langsam reagieren. Die Zeit vom entstandenen Schaden bis zur Entdeckung dauerte zum Teil Wochen (38 Prozent) oder gar Monate (36 Prozent).[1] Das ist für Straftäter ausreichend Zeit, um das mitzunehmen, was sie suchen und unbemerkt zu entkommen.

Die Bösen benötigen also nur Minuten und Tage, während die Guten Wochen oder Monate benötigen. Wie kann es also sein, dass sie so schnell sind? Die Antwort sind neue Taktiken. Die führend verwendeten Taktiken waren Hacking (50 Prozent) sowie Malware (49 Prozent). Zudem wurde in dem Bericht erläutert, dass die Angreifer es auf „leichte Ziele" abgesehen haben, also kleinere Unternehmen mit weniger gut gesicherten Systemen und nicht auf riesige Server-Systeme mit Millionen an Datensätzen.

Häufig erhalten die Angreifer zudem ungewollt Hilfe von Mitarbeitern. Durch Social Engineering und Benutzerdaten-Diebstahl finden Angreifer spielend einfach Wege, sich als interne Mitarbeiter mit legitimem Zugriff auszugeben. Bei wertvollen Datenbank-Ressourcen und der trüben Wirtschaftslage funktioniert selbst Bestechung. Laut desselben Berichts waren Anstiftung und Bestechung im letzten Jahr die häufigsten Social Engineering-Taktiken. Sie können also nicht nur auf Perimeterschutz vertrauen, um die Sicherheit Ihrer Datenbank zu gewährleisten, und Sie können auch nicht darauf vertrauen, dass alle Ihre Mitarbeiter richtig handeln.

Bestehende Probleme

In Datenbanken werden nicht nur kritische Informationen gespeichert, sondern sind häufig auch an mehrere Systeme angeschlossen, die wichtige Unternehmensleistungen liefern. Jede Unterbrechung, ungewollte Veröffentlichung oder jeglicher Datenverlust in den Datenbanken hat das Potential, die Betriebsabläufe und den Ruf des gesamten Unternehmens zu gefährden. Zudem entspricht eine Datenbank-Kompromittierung meist auch einem Compliance-Verstoß, da eine Datenbank regulierte und sensible Daten beinhaltet. Dies hat dann hohe Beseitigungskosten, den Verlust des Kundenvertrauens und möglicherweise drastische Marktkapitalisierungseinbußen zur Folge.

Um sensible Daten vor externen und internen Bedrohungen zu schützen, ist eine Echtzeitüberwachung der Datenbankaktivitäten erforderlich. Die meisten Unternehmen verwenden heutzutage datenbankeigene Protokoll- und Audit-Tools für diese Art von Schutz. Jedoch sind viele dieser Tools absolut unangemessen, wenn man es mit modernen Hacking- und Social Engineering-Taktiken zu tun hat. Um eine Datenbank richtig gegen bösartigen Code und Datenverlust zu sichern, müssen die folgenden Punkte bedacht werden:

- **Überwachung von Aktivitäten und Veränderungen**. Alle Datenbanken reagieren auf Kommandos. Solange ein Kommando zu dem Nutzer passt, der die Daten anfordert, wird es erfolgreich sein. Da die Angriffe und Tools immer origineller werden, können Angreifer typische Erkennungsmethoden umgehen und ihre Privilegien ausweiten. Schwache Zugriffskontrollen machen es ihnen sogar noch einfacher. Für gewöhnlich übersteigt der Zugriffslevel, den Nutzern gewährt wird, um Längen die Zugriffsrechte, die sie im System oder für ihre Rolle benötigen. Inaktive Benutzerkonten und schwache Kontrollen von neuen Benutzerkonten bieten Angreifern einfache Schlupflöcher. Diese haben es zuerst auf leichte Standardpasswörter abgesehen und erweitern dann ihre Privilegien. Die netzwerkbasierte Aktivitätsüberwachung hat sich als unzureichend für dieses Problem herausgestellt, da lokale Zugriffsmethoden diese netzwerkbasierten Überwachungssysteme umgehen können.

- **Auditing-Tools**. Die eingebauten Protokoll- und Auditing-Fähigkeiten von Datenbanken bieten bei Weitem nicht die erforderliche Transparenz. Bei den meisten werden die gemachten Änderungen, verwendeten Privilegien, involvierten Administratoren oder Änderungen auf Systemebene nicht ausreichend erfasst. Zudem können in der Datenbank integrierte Protokoll- und Auditing-Aktivitäten die Datenbankleistung beeinträchtigen. Da diese Funktionen nur zur Überwachung dienen und nicht zur Sicherheit, können sie von Administratoren einfach abgeschaltet werden, wodurch jeglicher Nutzen eliminiert wird.
- **Vermeidung von Downtime während Patching-Phasen**. Einnahmen, die Aktivität der Systeme sowie die Verfügbarkeit sind meist wichtiger als die Sicherheit. Manche Unternehmen haben einen Patch-Zyklus von gut über 12 Monaten. Es gibt jedoch jedes Jahr Hunderte neuer Bedrohungen, aber aufgrund der Wichtigkeit der Datenbanken stellt Downtime keine Option dar. Unternehmen möchten durchgehend geschützt sein, ohne die Datenbank patchen zu müssen.
- **Cloud-bereit**. Da immer mehr Unternehmen auf Cloud-Systeme zurückgreifen, muss die Datenbank so angepasst werden, dass man über Cloud-Services auf sie zugreifen kann und sie überwachen kann, ohne auf ein lokales Netzwerk zurückgreifen zu müssen.
- **Compliance-Nachweis für Industrie-, Regierungs- und interne Normen**. Abhängig von der Rolle Ihrer Datenbank müssen Sie unter Umständen verschiedene Richtlinien befolgen, sie aufrechterhalten und entsprechende Berichte anfertigen. Beispiele sind PCI DSS, Sarbanes-Oxley, HIPAA, SAS 70, GLBA und FERPA. Wenn Sie zudem Geschäfte mit anderen Ländern tätigen, haben diese meist ähnliche Datenschutz- und Finanzkontrollanforderungen. Darüber hinaus hat Ihr Unternehmen womöglich seine eigenen empfohlenen Vorgehensweisen und Betriebsstandards entwickelt, und die Führungskräfte erwarten Dashboards, die den Status der Governance-Standards anzeigen.

Entscheidungsfaktoren
Diese Faktoren können Ihre Architektur beeinflussen:

- Welche behördlichen Anforderungen muss Ihr Unternehmen einhalten?
- Wie messen Sie die Compliance mit gesetzlichen Vorschriften und wie erstellen Sie dazu Berichte?
- Betreiben Sie Datenbanken, die auf 64-Bit-Systemen laufen? Welche sind diese?
- Kennen Sie das Sicherheits-Level Ihrer Datenbank?
- Wie oft werden Ihre Datenbanken gepatcht?

Lösungsbeschreibung

Jedes Unternehmen ist für seine Tätigkeiten von einer Datenbank abhängig. Wenn wir uns nicht auf die Schutzmechanismen von Betriebssystemherstellern verlassen können, warum geben wir uns dann mit den vom Hersteller zur Verfügung gestellten Tools zufrieden, die unsere wertvollsten Datenbank-Ressourcen schützen sollen? Datenbanken bergen einzigartige Herausforderungen und werden in der Regel in die Hände von Datenbank-Administratoren gegeben, die die Sicherheitsrichtlinien und -standards implementieren. Aufgrund der hohen Anzahl an Datenbank-Kompromittierungen in letzter Zeit, muss unter Umständen ein neuer Ansatz gefunden werden, mit dem sichergestellt werden kann, dass die Integrität von Datenbanken vor bösartigem Code und—traurig aber wahr—unseren eigenen internen Mitarbeitern geschützt werden kann.

Um diese Probleme zu adressieren, muss eine Lösung den folgenden Voraussetzungen entsprechen:

- **Überwachung von Aktivitäten und Veränderungen**. Eine Lösung muss das gesamte Datenbankverhalten und alle Aktivitäten von einem Ort außerhalb der Datenbank überwachen können. Fände diese Überwachung ausschließlich innerhalb der Datenbank statt, könnten die Datenbank-Administratoren diese Funktionalität (vorsätzlich oder ungewollt) deaktivieren. Eine Lösung muss außerdem eine Sitzung beenden können, die gegen die Richtlinien verstößt, und Warnmeldungen an eine zentral verwaltete Konsole senden sowie böswillige oder nicht-konforme Benutzer unter Quarantäne stellen können. Eine Lösung muss Eindringtechniken identifizieren und diese verhindern können.
- **Auditing-Tools**. Auditing-Tools sind ebenso ineffektiv, wenn sie von einem Administrator deaktiviert werden können. Eine Lösung muss geschützte Audit- und Protokollfähigkeiten außerhalb der Datenbank bieten, um gewährleisten zu können, dass die Datensätze erfasst werden und für die Analyse verfügbar sind. Während der forensischen Analyse nach Sicherheitsvorfällen können Sie sich mithilfe dieses Audit-Protokolls ein Bild vom Umfang der kompromittierten Daten machen und einen besseren Einblick in die böswilligen Aktivitäten gewinnen. Eine Lösung muss einen Audit-Trail sowie Berichte bieten, die mit SOX, PCI und anderen Compliance-Audit-Anforderungen konform sind.
- **Vermeidung von Downtime während Patching-Phasen**. Eine Lösung muss Angriffe identifizieren können, mit denen bekannte Schwachstellen sowie übliche Bedrohungsvektoren ausgenutzt werden. Sie sollte so konfiguriert sein, dass entweder eine Warnmeldung ausgelöst oder die Sitzung in Echtzeit beendet wird. Darauf zu warten, dass der Datenbank-Anbieter einen Patch anbietet oder Patches auszulassen, um Produktionsverluste zu umgehen, macht Ihre Datenbank anfällig für viele Bedrohungen. Ein virtuelles Patch-Konzept hilft Ihnen beim Schutz gegen Zero-Day-Bedrohungen und neu entdeckte Schwachstellen und kann ohne Downtime der Datenbank implementiert werden, wodurch sensible Daten so lange geschützt sind, bis ein neuer Patch verfügbar ist.

- **Cloud-bereit**. Es ist in den enorm dynamischen und verteilten Architekturen, die für die Datenzentren-virtualisierung und Cloud-Computing verwendet werden, entweder unmöglich oder ineffizient, sich auf eine Analyse des Netzwerk-Traffics zu verlassen, wenn es um die Identifizierung von Richtlinienverstößen geht. Eine Lösung muss so konfiguriert sein, dass sie automatisch auf jede neue Datenbank abgestimmt wird, die Sicherheitsrichtlinie basierend auf den Daten, die sie hostet, abfragt und dann damit beginnt, mögliche Warnmeldungen an den Verwaltungs-Server zu senden. Selbst wenn die Netzwerkverbindung unterbrochen wird, müssen die Daten noch über lokal erzwungene Richtlinien geschützt sein.
- **Compliance mit Industrie-, Regierungs- und internen Normen**. Wenn sich die Normen und Vorschriften ändern, müssen Sie auch die Berichte ändern, die Sie erstellen. Eine Lösung muss Vorlagen zur Einhaltung gesetzlicher Vorgaben bieten, die mit den neuesten Kontrollen und Bedrohungsleitlinien aktuell gehalten werden. Eine Lösung muss Bedrohungen identifizieren können, wenn sie entstehen, und Berichte zu Prävention und zur Verringerung des Risikos und der Verantwortlichkeiten erstellen. Vorkonfigurierte Vorlagen sollten PCI DSS, Sarbanes-Oxley, HIPAA und SAS 70 beinhalten, die alle von einer zentral verwalteten Plattform aus einsehbar sind.

In der McAfee-Lösung verwendete Technologien

McAfee bietet zwei Produkte, die speziell zur Datenbanksicherheit konzipiert wurden, McAfee® Vulnerability Manager for Databases und McAfee Database Activity Monitoring. Die zentrale Verwaltung über McAfee ePolicy Orchestrator® (McAfee ePO™) verknüpft diese zwei Produkte in einer vereinten Sicherheits- und Compliance-Management-Plattform für Ihre gesamte Infrastruktur.

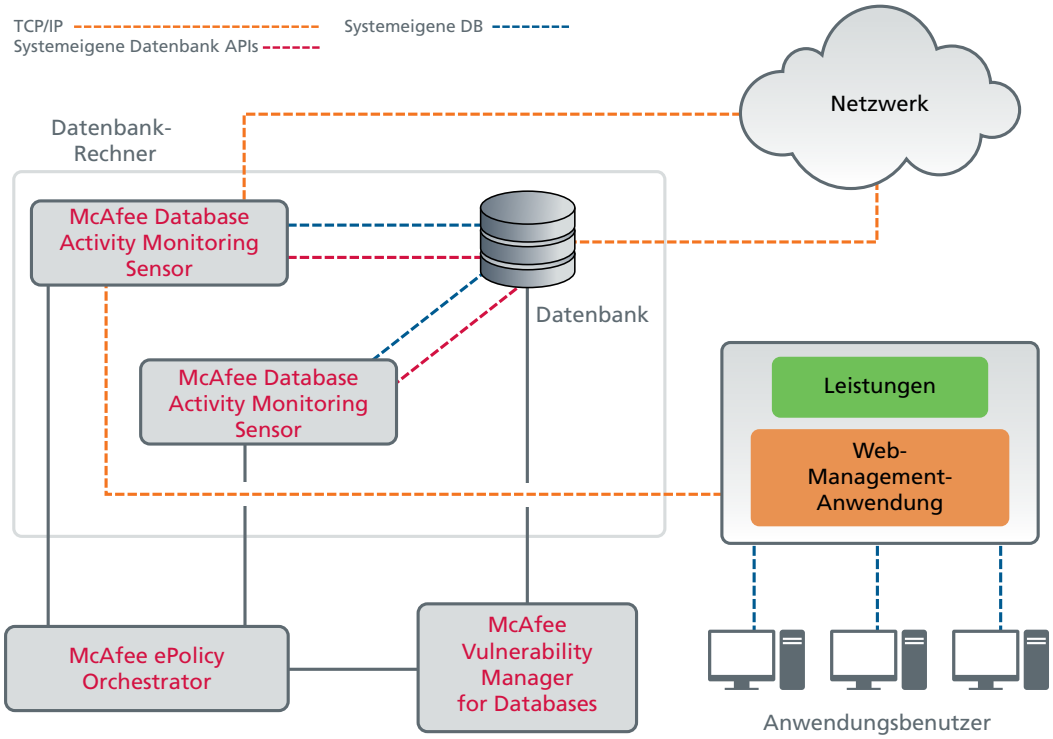
McAfee Vulnerability Manager for Databases führt mehr als 3.000 Schwachstellenprüfungen gegen führende Datenbanksysteme durch, einschließlich SQL Server, DB2 und MySQL. Durch die Übersicht über die Datenbankschwachstellen und die Expertenempfehlungen für Behebungsmaßnahmen reduziert McAfee Vulnerability Manager for Databases die Wahrscheinlichkeit eines schädigenden Sicherheits-verstoßes. Die dank dieser Lösung bessere Vorbereitung ermöglicht zudem Kostenreduzierungen für Audits sowie Einhaltung von behördlichen Vorgaben. McAfee Vulnerability Manager for Databases hilft dabei, die Angriffsfläche zu reduzieren, indem typische Schwachstellen identifiziert werden, auf die es Hacker abgesehen haben, wie unsichere Passwörter, gemeinsam genutzte Passwörter und Standard-konten. Um Ihnen dabei zu helfen, verdächtige Ereignisse zu verfolgen und darauf zu reagieren, liefert die Anwendung Informationen über Version-/Patch-Level, geänderte Objekte, modifizierte Privilegien und forensische Spuren von bekannten Hacker-Tools.

Anders als standardmäßige Audit- oder Protokollanalysen, die Ihnen nur sagen, was passiert ist, bietet McAfee Database Activity Monitoring einen Echtzeitüberblick und Intrusion Prevention-Möglichkeiten, die Ihnen dabei helfen, die Kompromittierung zu stoppen, bevor Schaden angerichtet werden kann. Sie erhalten mehr als 380 vordefinierte Regeln, die allgemeine Angriffsprofile sowie einzelne Probleme abdecken, für die Datenbankhersteller Patches herausgegeben haben. Vorerstellte Richtlinienvorlagen können so konfiguriert werden, dass Regeln für gewollte und konforme Datenbankzugriffe und -prozesse unterstützt werden.

Es werden direkt Warnmeldungen an das Überwachungs-Dashboard gesendet, mit allen Details jeglicher Richtlinienverstöße, damit gegen diese vorgegangen werden kann. Verstöße mit hohem Risiko können so konfiguriert werden, dass verdächtige Sitzungen automatisch beendet werden und böswillige Nutzer unter Quarantäne gestellt werden, damit das Sicherheitsteam so die Zeit hat, dem Eingriff nachzugehen.

Angriffe, die auf wertvolle Daten abzielen, die in Datenbanken gespeichert sind, können von überall aus dem Netzwerk ausgehen, von lokalen Benutzern, die auf den Servern selbst angemeldet sind und sogar von innerhalb der Datenbank über gespeicherte Verfahren oder Auslöser.

McAfee Database Activity Monitoring verwendet speicherbasierte Sensoren, um Aktivitäten zu überwachen und alle drei Bedrohungstypen mit einer einzigen, nicht-intrusiven Lösung zu identifizieren. Virtuelle Patching-Updates werden regelmäßig für neu entdeckte Schwachstellen zur Verfügung gestellt und können ohne Datenbank-Downtime implementiert werden, wodurch sensible Daten geschützt werden, bis ein Patch vom Datenbank-Anbieter veröffentlicht wird und verwendet werden kann. Aktivitäts- und Ereignisinformationen können dann verwendet werden, um für Auditzwecke die Compliance nachzuweisen und die allgemeine Sicherheit zu optimieren.



Spezielle Schutzmaßnahmen ermöglichen McAfee, Datenbankschwachstellen zu analysieren sowie böswillige und riskante Aktionen zu identifizieren.

McAfee Vulnerability Manager for Databases

Konzipiert, um erste Scans zu beschleunigen und sofort verfügbare Berichte für die meisten Compliance-Anforderungen zu verwenden, kann McAfee Vulnerability Manager for Databases mehrere Datenbanken von einer einzigen Konsole aus erkennen und scannen. Die Anwendung wird Tabellen, die sensible Informationen enthalten, finden sowie identifizieren und einen schnellen Port-Scan durchführen, der die Datenbankversion und den Patch-Status liefert. Zusätzlich zur Funktionalität, die Sicherheit von Standardpasswörtern zu bestimmen (einfache, standardmäßige und gemeinsam genutzte Passwörter), kann sie gespeicherte gehashte Passwörter scannen, beispielsweise in SHA-1, MD5 oder DES. Sie wird auch auf Anfälligkeiten für datenbankspezifische Risiken testen, darunter SQL-Injektion, Buffer Overflow und böswilliger oder unsicherer PL/SQL-Code. Die Resultate werden in vorkonfigurierten Berichten zur Verwendung mit den üblichen Compliance-Normen präsentiert.

McAfee Database Activity Monitoring

McAfee Database Activity Monitoring ist ein kleiner Aktivitätssensor, ein Software-Programme, dass auf dem Host-Server der Datenbank selbst installiert ist und alle Aktivitäten überwacht. Der Sensor ist ein Standalone-Prozess, der in C++ geschrieben ist, und der auf dem Hostrechner der Datenbank läuft. Er ist unter Verwendung standardmäßiger Plattform-Tools (RPM, PKG, DEPOT, BFF oder EXE) in einem separaten Betriebssystem-Benutzerkonto auf dem System installiert. Der Sensor identifiziert automatisch alle Datenbanken auf dem Rechner und kann mehrere Instanzen gleichzeitig überwachen, selbst unterschiedliche Datenbanktypen auf demselben Host-Rechner.

Wenn der Sensor läuft, hängt er sich an den Instanzspeicherbereich des SQL-Caches an und verwendet Read-Only-Mechanismen sowie Application Programming Interfaces (APIs) und beginnt die Überwachung mit einem Memory Sampling-Abfrage-Loop. Für jeden Sampling-Zyklus analysiert der Sensor die aktuell laufenden und vorherigen Anweisungen für jede Sitzung in der Datenbank-Instanz und bestimmt anhand einer vom Server erhaltenen, vordefinierten Richtlinie, welche Anweisungen gemeldet oder geblockt werden sollen. Anweisungen, die gegen die Richtlinie verstoßen, werden als Warnmeldungen in Echtzeit an die Management-Konsole gesendet. Der Sensor kann auch so konfiguriert werden, dass er Sitzungen bei bestimmten Verstößen beendet und die Nutzer unter Quarantäne stellt. Diese Methode ist nicht-intrusiv und verbraucht nur wenige CPU-Ressourcen (weniger als fünf Prozent eines einzelnen CPU-Kerns, selbst bei Multi-CPU-Rechnern). Die Präventionsfähigkeiten des Sensors werden anhand von bestehenden Datenbank-APIs implementiert, mit denen er Datenbank-Sitzungen beenden kann, ohne die Datenintegrität zu gefährden.

McAfee ePolicy Orchestrator (McAfee ePO)

McAfee ePO ermöglicht ein zentrales, automatisches Softwareausbringungs- und Richtlinien-Management. McAfee Vulnerability Manager for Databases ist in das McAfee ePO-Dashboard integriert und bietet so zentrale Berichtsfunktionen sowie zusammenfassende Informationen für alle Ihre Datenbanken. McAfee ePO stellt auch eine Verbindung zu McAfee Database Activity Monitoring her und bietet so eine zentrale Ansicht sowie optimierte Berichtsfunktionen.

Nutzen der Lösung

Durch die Einführung von speziellen Schutzfunktionen für Angriffe und Datenverlustvektoren von Datenbanken, können Sie Ihre Fähigkeit, externe Angriffe zu identifizieren und diese abzuwehren, optimieren und auch die Wahrscheinlichkeit einer Kompromittierung oder Störung innerhalb des Netzwerks reduzieren.

McAfee bietet durch Überwachung und Warnmeldungen bei verdächtigen Ereignissen Echtzeit-Ansichten und -Schutz vor allen möglichen Angriffstypen. McAfee hilft dabei, die Risiken und Gefahren zu minimieren, indem Angriffe gestoppt werden, bevor Sie Schäden anrichten können - egal ob die Bedrohung aus dem Netzwerk kommt, von lokalen Benutzern, die auf dem Server selbst angemeldet sind, oder von innerhalb der Datenbank. Virtuelles Patching von neu entdeckten Datenbank-Schwachstellen bietet einen sofortigen Schutz ohne Datenbank-Downtime.

Vordefinierte Vorlagen und Regeln, automatisierte und aktualisierte Prüfungen und Wizard-basierte Schnittstellen beschleunigen die Bereitstellung und helfen Ihnen dabei, eine effiziente Datenbank-sicherheitsarchitektur zu erhalten, die unkompliziert auditiert werden kann.

Weitere Hilfsmittel

www.mcafee.com/de/solutions/database-security/database-security.aspx
www.mcafee.com/de/products/vulnerability-manager-databases.aspx
www.mcafee.com/de/products/database-activity-monitoring.aspx
www.mcafee.com/de/products/epolicy-orchestrator.aspx

Für weitere Informationen über die Security Connected-Referenzarchitektur, besuchen Sie:
www.mcafee.com/de/enterprise/reference-architecture/index.aspx.

Informationen zum Autor

Uy Huynh ist Senior Director für Sales Engineering bei McAfee. Er ist dafür verantwortlich, dass sein Team die richtigen Sicherheitslösungen, -Designs und empfohlenen Vorgehensweisen liefert, um den Kunden dabei zu helfen, ihre Sicherheitslage zu verbessern und ihre wichtigsten digitalen Daten zu schützen. Uy ist ein Sicherheitsexperte, der mit großen Fortune 100-Kunden wie HP, Oracle, ATT, McKesson und anderen gearbeitet und mit ihnen die passenden Sicherheitsprodukte ausgewählt hat, die ihren komplexen Anforderungen entsprechen.

Vor seiner Tätigkeit bei McAfee leitete und gründete er die SE-Organisation bei Foundstone. Dort entwickelte er empfohlene Vorgehensweisen für das Schwachstellen-Management und Risiko-Management für große Netzwerke und Systeme. Vor seiner Tätigkeit bei Foundstone war er Senior Consultant bei ISS, wo er eine Vielzahl an Sicherheitslösungen, -richtlinien und -technologien bei großen Unternehmen einrichtete.

[1] http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

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

38600bp_protecting-databases-L3_1111