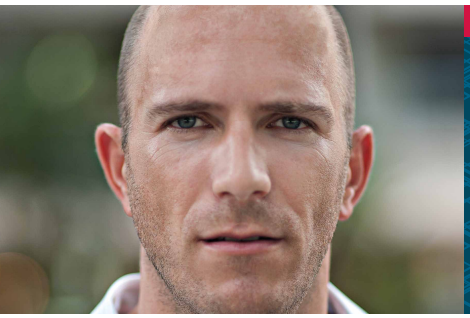

Fünf gute Gründe für eine dedizierte Datenbank-Sicherheitslösung

So richten Sie die kritische letzte Verteidigungslinie ein

Der Schutz der wertvollen und vertraulichen Informationen in Datenbanken ist eine grundlegende Voraussetzung für die Integrität und Wahrung des Rufs von Unternehmen – ganz abgesehen von der Gewährleistung der Compliance mit rechtlichen Vorschriften. Viele Unternehmen verlassen sich jedoch noch immer auf Sicherheitslösungen, die nur eingeschränkt wirksam sind. Angesichts der Komplexität von Datenbankplattformen und der Raffinesse von Internetkriminellen ist der Einsatz einer umfassenden und dedizierten Datenbank-Sicherheitslösung ein Muss. Im Folgenden erläutern wir fünf Gründe dafür.

Vorteile von McAfee Vulnerability Manager

- Volle Transparenz über Datenbank-Sicherheitsmaßnahmen
- Scan mehrerer Datenbanken im gesamten Unternehmen über eine zentrale Konsole
- Erhebliche Kosteneinsparungen dank verkürzter Zeit bis zur Compliance sowie Reduzierung der Audit-Zyklen
- Schnelle Bereitstellung mit minimalen Datenbanksystem-Kenntnissen möglich
- Schnelle Erstellung benutzerdefinierter Berichte in einem leicht verständlichen Format für verschiedene Benutzerrollen

Vorteile von McAfee Database Activity Monitoring

- Maximale Transparenz und Schutz vor allen Angriffsquellen
- Überwachung externer Bedrohungen, mit Berechtigungen ausgestatteter Insider und komplexer Gefahren innerhalb der Datenbank
- Minimierung von Risiken und Haftbarkeit, indem Angriffe aufgehalten werden, bevor sie Schäden verursachen
- Zeit- und Geldersparnis durch schnellere Bereitstellung und effizientere Architektur
- Flexibilität für einfache Bereitstellung auf der gewünschten IT-Infrastruktur

1. Sie können eine Ressource nur dann schützen, wenn Sie von ihrer Existenz wissen

Auch in konservativ geführten Unternehmens-IT-Umgebungen gibt es häufig Hunderte oder gar Tausende von Datenbankinstanzen, die äußerst sensible Daten enthalten. Für die IT-Abteilungen wäre es sehr schwierig, die genaue Anzahl, Speicherorte, Sensibilität und den Sicherheitsstatus dieser Datenbanken zu bestimmen. Das Schlimmste daran: Internetkriminelle wissen das und suchen stets nach nicht überwachten Stellen. Sie haben ausreichend Zeit und die technischen Ressourcen, um Datenbanken anzugreifen, die Sie für sicher halten oder von deren Existenz Sie zunächst nicht einmal wussten. Die fehlende Übersicht der Unternehmen ist die Chance für die Angreifer.

Die volle Transparenz über Ihre Datenbanken können Sie sich nur durch eine vollständige Erkennung aller in Ihrer Umgebung vorhandenen Datenbanken verschaffen. Außerdem muss geprüft werden, welche dieser Datenbanken Zahlungskarteninformationen, Personaldaten, Vertriebszahlen oder andere sensible Daten enthalten. Automatische und lückenlose Tests auf Datenbankschwachstellen sind zur Bestimmung der genauen Risikoart unerlässlich. Diese detaillierten und praxistauglichen Informationen erhalten Sie nur mithilfe einer dedizierten Datenbank-Sicherheitslösung, die Schutzlücken priorisieren und beheben kann. Mit ihr spart Ihr Unternehmen hohe Ausgaben für externe Sicherheitsberater.

McAfee® Vulnerability Manager for Databases erkennt automatisch alle Datenbanken im Netzwerk, ermittelt, ob die neuesten Patches installiert wurden, und führt außerdem Schwachstellen-Scans durch. McAfee Vulnerability Manager bietet über 4.200 Schwachstellenprüfungen für führende Datenbanksysteme und teilt die Bedrohungen in verschiedene Prioritätsstufen ein. Die Lösung stellt darüber hinaus Reparaturskripts und Empfehlungen bereit. Für die Bedienung von McAfee Vulnerability Manager sind nur geringe Kenntnisse über Datenbanksysteme erforderlich. Die Lösung erstellt benutzerdefinierte Berichte in leicht verständlichen Formaten für verschiedene Benutzerrollen und ist über eine zentrale Sicherheitskonsole bedienbar.

2. Sicherheitsmaßnahmen am Perimeter schützen nicht vor internen Angriffen

Es wird viel Zeit, Aufwand und Kapital darin investiert, Firewalls sowie andere Technologien für den Netzwerkschutz auszuwählen und zu implementieren. Jedoch haben nicht alle Datenbank-Sicherheitsverstöße ihren Ursprung außerhalb des Perimeters. Eine jährliche Untersuchung durch das Computer Emergency Response Team (CERT) ergab, dass sogar die Hälfte der Datenbank-Kompromittierungen durch interne Benutzer verursacht wurden. Deshalb müssen Sie Ihre geschäftskritischen Daten vor noch heimtückischeren böswilligen Insidern schützen, die über Berechtigungen verfügen. Viele von ihnen haben die notwendigen Kenntnisse, um die integrierten Sicherheitsfunktionen von Datenbank-Management-Systemen (Database Management Systems, DBMS) zu umgehen, Zugriffsprotokolle zu manipulieren und ihre Spuren zu verwischen.

Die richtige Datenbank-Sicherheitslösung erkennt und verhindert Gefährdungen aus den möglichen Angriffsrichtungen: Bedrohungen, die von außerhalb und insbesondere von innerhalb des Unternehmens kommen. Darüber hinaus liefert sie die Rahmenbedingungen für die einfache Einrichtung und Durchsetzung von Datenbank-Zugriffsrichtlinien, die spezifischen Compliance-Anforderungen entsprechen sowie eine durchgängige Aufgabentrennung sicherstellen.

McAfee Database Activity Monitoring findet automatisch Datenbanken in Ihrem Netzwerk. Es schützt sie mit vorkonfigurierten Schutzmaßnahmen und unterstützt Sie bei der Entwicklung individueller Sicherheitsrichtlinien für Ihre Umgebung. Dadurch können Sie bei Audits leichter Compliance nachweisen und den Schutz kritischer Ressourcen verbessern. McAfee Database Activity Monitoring liefert Informationen über alle Datenbankaktivitäten, zum Beispiel über den Zugriff durch berechtigte Benutzer sowie komplexe Angriffe innerhalb der Datenbank. Es schützt Ihre Daten durch die lokale Überwachung der Aktivitäten auf jedem Datenbank-Server unabhängig vom Speicherort vor allen Bedrohungen. Die Lösung sendet zudem Warnmeldungen oder beendet Sitzungen, die verdächtig sind oder die Sicherheitsrichtlinie verletzen. Sogar in virtuellen oder Cloud-Computing-Umgebungen schützt McAfee Database Activity Monitoring Ihre Datenbanken und setzt Ihre Richtlinien durch.

Vorteile von McAfee Virtual Patching

- Schutz vor Bedrohungen bereits vor der Installation der vom Anbieter freigegebenen Patch-Aktualisierungen
- Keine DBMS-spezifischen Fachkenntnisse bei IT- und Sicherheitsteams erforderlich
- Kein Ausfall der Produktionsdatenbanken dank der auf Unterbrechungsfreiheit ausgelegten Software
- Nahtloser Schutz von Datenbanken mittels automatischer Bereitstellung laufender Aktualisierungen
- Einfache Compliance mit Standards wie PCI DSS, HIPAA usw.

Vorteile von McAfee ePolicy Orchestrator

- Umfassende Transparenz über Datenbanksicherheit und -Compliance über eine zentrale Verwaltungskonsole
- Dank der zentralen Übersicht einfache Einbindung der Datenbanken in ein zentrales Sicherheitsverwaltungsprogramm – vor Ort, standortfern und sogar in der Cloud
- Offene und erweiterbare Architektur, die die Verwaltung von McAfee- und Drittanbieterlösungen mit Ihren LDAP- (Lightweight Directory Access Protocol), IT-Betriebs- und Konfigurationsverwaltungstools verbindet

3. Die Angreifer reagieren schneller als Sie patchen können

Der Patch-Dienstag war immer ein erklärter Feiertag für Hacker. An diesem Tag legen die Datenbankanbieter monatlich die lohnendsten Ziele offen. Für die Angreifer ist der Patch-Dienstag zudem eine Vorwarnung. Sie wissen, wie mühsam es für Datenbank-Verwaltungsteams ist, Datenbanken außer Betrieb zu nehmen, zu patchen und zu testen. Sie verlassen sich darauf, dass eine derartige Betriebsunterbrechung so unbeliebt ist, dass sie solange wie möglich hinausgezögert wird. Dadurch haben sie reichlich Zeit, sich ihren Weg in das System zu bahnen.

Dieser herkömmliche Patch-Prozess und die damit verbundenen Möglichkeiten für die Kriminellen lassen sich nur durch eine dedizierte Datenbank-Sicherheitslösung vermeiden. Diese Lösung muss es Ihnen ermöglichen, die Sicherheitsmaßnahmen für ihre Datenbank in Echtzeit zu aktualisieren, ohne Ihren Mitarbeitern Probleme zu verursachen und den Geschäftsbetrieb zu unterbrechen.

McAfee Virtual Patching for Databases schützt Datenbanken vor Risiken durch ungepatchte Schwachstellen, indem es Angriffs- und Eindringungsversuche in Echtzeit erkennt und verhindert, ohne Datenbankausfallzeiten oder Anwendungstests zu erfordern. Sie können sich darauf verlassen, dass Sie auch in Phasen mit dem höchsten Schwachstellenpotenzial vor Bedrohungen geschützt sind: Im Zeitfenster zwischen der Ausstellung der Anbieter-Patch-Aktualisierungen und der tatsächlichen Installation.

McAfee Database Activity Monitoring ist eine weitere Lösung, die ohne Ausfallzeiten und Beeinträchtigungen zusätzlichen Schutz am Patch-Dienstag und darüber hinaus bietet. Ihre arbeitsspeicherbasierten Sensoren fangen Angriffe auf Datenbanken aus dem Netzwerk, von lokalen auf dem Server angemeldeten Benutzern und auch von innerhalb der Datenbank über gespeicherte Verfahren oder Trigger ab.

4. Keine Compliance-Kompromisse für den unterbrechungsfreien Geschäftsbetrieb

Für alle Branchen – darunter etwa Gesundheitswesen, Finanzsektor und Einzelhandel – gelten rechtliche Compliance-Anforderungen. Sie nehmen immer weiter zu und werden immer strenger. Es ist nicht überraschend, dass sich die Compliance-Vorgaben erheblich auf geschäftskritische Datenbanken auswirken. Sie bestimmen, dass die Datenbanken mit den neuesten DBMS-Patches der Anbieter aktualisiert werden müssen. Da es jedoch sehr mühsam ist, mehrere Datenbanken außer Betrieb zu nehmen, zu patchen und dann zu testen, opfern viele Unternehmen ihre Compliance zugunsten des unterbrechungsfreien Geschäftsbetriebs. Außerdem werden auch alte Datenbanken eingesetzt, für die keine Patch-Aktualisierungen mehr angeboten werden.

Mit McAfee Virtual Patching for Databases stehen unterbrechungsfreier Geschäftsbetrieb und gesetzliche Compliance nicht mehr im Gegensatz zueinander. Mit dieser Lösung können sie Ihre normalen Patch-Maßnahmen nach Ihrem eigenen Zeitplan ausführen, sich aber auf ihre Sicherheit und Compliance verlassen. McAfee Virtual Patching for Databases ermöglicht erhebliche Zeiteinsparungen und eine gültige Kontrolloption für Compliance-Prüfer. Auch alte Datenbanken erhalten damit aktuellen Schutz, wenn sie nicht mehr von Ihren DBMS-Anbietern unterstützt werden.

5. Stark eingeschränkte Transparenz von Daten in der Cloud

Die Cloud bietet enorme Vorteile in Bezug auf IT-Kosten und -Betrieb, hat jedoch auch einen erheblichen Nachteil: Ihre Mitarbeiter können die Kontrolle über sensible Daten verlieren und haben kaum noch einen Überblick darüber, wer darauf zugreifen kann. Wenn Sie jedoch über die richtige Datenbank-Sicherheitslösung verfügen, können Sie Ihre Daten sowohl in physischen als auch virtuellen Umgebungen schützen. Eine geeignete Lösung kann unbefugte Datenbankaktivitäten verhindern und an Ihre eigene Verwaltungskonsole melden, auch wenn die Datenbank virtualisiert ist und sich in der Cloud befindet.

Mit einer einzigartigen arbeitsspeicherbasierten Implementierung kann McAfee Database Activity Monitoring für die automatische Bereitstellung zusammen mit jeder neuen virtuellen Maschine konfiguriert werden. Zudem fordert es Sicherheitsrichtlinien basierend auf den gehosteten Daten an und kann dann Warnmeldungen an den Management-Server senden. Die Sensoren der Lösung funktionieren auch selbständig, wenn keine Verbindung zum Server besteht. Sensible Daten bleiben so unabhängig davon, ob die Datenbank online oder offline ist, sowie unabhängig vom Speicherort jederzeit geschützt. Da der Sensor die Sicherheitsrichtlinie lokal implementiert, sind die Daten auch dann sicher, wenn die Netzwerkverbindung unterbrochen wurde. Warnmeldungen werden in einer Warteschlange vorgehalten, bis der Management-Server wieder erreichbar ist.

Zusätzlich dazu können Sie Cloud-basierte Datenbanken mit der Software McAfee® ePolicy Orchestrator® (McAfee ePO™) überwachen, die eine Sicherheitsverwaltungskonsole beinhaltet, über die Sie dank umfassendem Überblick den Datenbankschutz, die Unternehmenssicherheit sowie die Compliance im gesamten Unternehmen verwalten können.

Dadurch erhalten Sie und Ihre Mitarbeiter einen bestmöglichen Überblick – selbst dann, wenn sich Ihre Daten in der Cloud befinden. McAfee hat die richtige Datenbank-Sicherheitslösung für Ihre IT-Umgebung, ganz gleich wie verteilt Ihre Unternehmensabläufe oder wie sensibel Ihre Daten sind.

Vorteile des McAfee-Schutzes für Datenbanken

- Einfache Bereitstellung und Nutzung
- Volle Transparenz über Datenbank-Sicherheitsmaßnahmen
- Abstimmung der Administrationsabläufe gemäß der Sicherheitsrichtlinie für das gesamte Sicherheits- und Datenbankverwaltungspersonal
- Effiziente Einhaltung der gesetzlichen Compliance
- Minimierung von Risiken und Haftbarkeit, indem Angriffe aufgehalten werden, bevor sie Schäden verursachen
- Verwaltung der Datenbanksicherheit über eine zentrale Konsole

Weitere Informationen zur Sicherheit und Verfügbarkeit von Datenbanken

Wir wissen, dass Sie in Ihren Datenbanken Ihre wichtigsten Geschäfts-Ressourcen speichern. Sie müssen Ihnen rund um die Uhr zur Verfügung stehen und Ihr Unternehmen unterstützen. Ihre Datenbanken können sich keinen Tag freinehmen. Das gilt auch für McAfee. Deshalb ist unsere Devise: Sicherheit muss immer verfügbar sein. Unser Expertenteam für Datenbanksicherheit ist stets um die Sicherheit und Verfügbarkeit Ihrer sensiblen Informationen bemüht und unterstützt Ihr Unternehmen bei der Gewährleistung der Compliance mit internen Richtlinien und gesetzlichen Vorschriften.

Weitere Informationen zum Schutz Ihrer geschäftskritischen Datenbanken mit McAfee-Lösungen erhalten Sie unter www.mcafee.com/de/products/database-security/index.aspx oder von Ihrem örtlichen McAfee-Vertriebsrepräsentanten bzw. -Händler.

Verfolgen Sie uns auf Twitter: @McAfee_DBSecure.

Über McAfee-Lösungen zum Endgeräteschutz

McAfee ist ein hundertprozentiges Tochterunternehmen der Intel Corporation (NASDAQ: INTC) und der weltweit größte auf IT-Sicherheit spezialisierte Anbieter. Unsere Lösungen für Endgeräteschutz der nächsten Generation bieten Sicherheit für alle Ihre Geräte sowie die darauf befindlichen Daten und Anwendungen. Diese umfassenden und maßgeschneiderten Lösungen verringern die Komplexität von mehrschichtigen Endgeräte-Abwehrmaßnahmen, ohne dabei die Produktivität zu beeinträchtigen. Sie sind die perfekte Mischung aus traditionellen intelligenten Malware-Scans, dynamischen Whitelists, verhaltensbasiertem Zero-Day-Schutz vor Eindringlingen, einheitlicher Verwaltung sowie integrierter Bedrohungsanalyse. Weitere Informationen erhalten Sie unter www.mcafee.com/de/products/endpoint-protection/index.aspx.

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

41903brf_top5-db-sec_0212_fnl_ASD