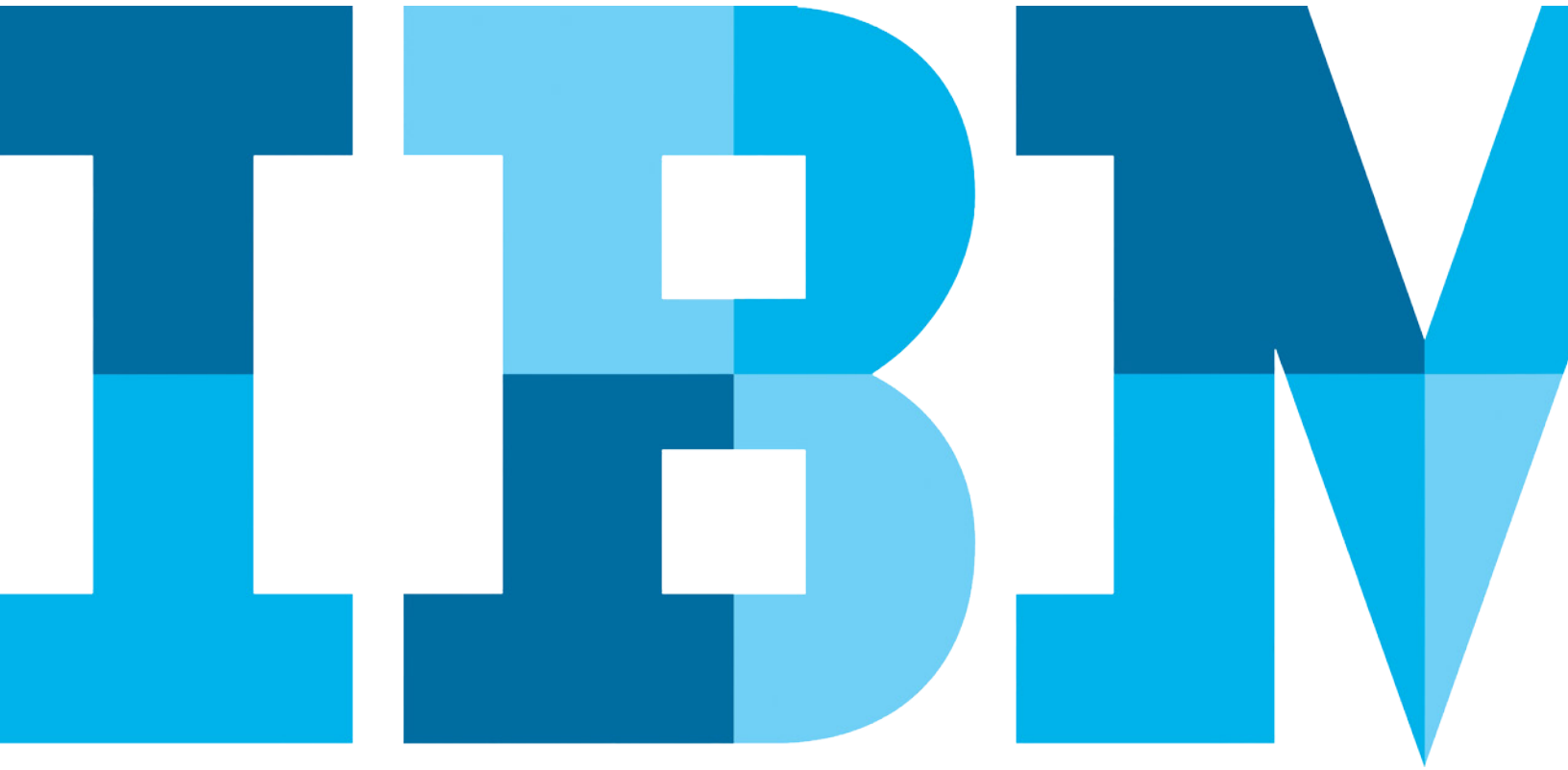
IBM Corporation
Thought-Leadership-Artikel

Dezember 2014

Vier wichtige Schritte zur Behebung von Datenbankschwachstellen, bevor es zu einer verheerenden Datenpanne kommt

Schwachstellen kennen und bewerten – Grundlage eines proaktiven Sicherheitsansatzes



IBM

Datenpannen können verheerende Auswirkungen haben. Durchschnittlich fallen heute bei Datenpannen Kosten in Höhe von 3,5 Millionen US-Dollar an. Das ergibt sich aus der jüngsten Studie des Ponemon Institutes zu den Kosten von Datenpannen (Cost of Data Breach Study), bei der IT-und Sicherheitsfachleute in 314 Unternehmen aus der ganzen Welt befragt wurden. Pro verlorener oder gestohlener Datenquelle mit sensiblen oder vertraulichen Informationen fallen im Durchschnitt 145 US-Dollar an.[1]

Außerdem geht aus der Untersuchung hervor, dass sich vor allem der Imageschaden und verlorene Kunden im Endergebnis niederschlagen – ausufernde Kosten belasten das Geschäft noch lange nach dem Vorfall. Dazu heißt es im Bericht: „Nach einer Datenpanne müssen Unternehmen viel Geld ausgeben, um den Imageschaden ihrer Marke zu reparieren und neue Kunden zu gewinnen."[2]

Nichts Neues für IT-Führungskräfte, CIOs, Sicherheitsfachleute oder Compliance-Manager. Überraschend dürfte aber auch für sie sein, dass in vielen Unternehmen trotz der weltweiten Aufmerksamkeit, die Datenpannen heutzutage erregen, nach wie vor nicht proaktiv mit der Frage Datensicherheit umgegangen wird. Oft ist vielen nicht einmal klar, in welcher Gefahr sie schweben.

In einer aktuellen Forrester-Umfrage mit 200 Entscheidungsträgern des Bereichs Sicherheit aus den USA, Großbritannien und Deutschland kamen mehrere kritische Lücken zutage, durch die Unternehmen zunehmend anfällig für Datenpannen werden.[3] Diese sind:

- **Unternehmen setzen Compliance fälschlicherweise mit Sicherheit gleich.** Der Bericht dazu: „Compliance ist das absolute Minimum, kein Ersatz für eine solide Sicherheitsstrategie. Die Änderung von Compliance-Standards nimmt viel Zeit in Anspruch. Bedrohungen und Technologien entwickeln sich aber ständig weiter. Daher ist es nicht ungewöhnlich, dass es auch in Unternehmen, die alle Standards einhalten, zu Datenpannen kommt."

- **Beim Thema Datensicherheit tun sich viele Unternehmen schwer und sind noch nicht in der Lage, den Erfolg ihrer Datensicherheitsinitiativen ausreichend zu messen.** Für ausgereiftere Datensicherheitspraktiken muss mit dem Übergang von der netzwerk- und gerätezentrierten zur datenzentrierten Sicherheit laut Forrester ein deutlicher Wandel der Unternehmenskultur einhergehen.

- **Eine Datenpanne ist für viele Unternehmen ein – sehr kostspieliger – Weckruf.** 45 % der betroffenen Unternehmen implementierten nach einer Datenpanne neue Sicherheitskontrollen und -strategien. Doch für viele war es da schon zu spät: 35 % gaben an, dass die Panne beträchtliche Auswirkungen gehabt habe, und bei 18 % hatte die Datenpanne sogar Entlassungen zur Folge. Doch meistens werden Unternehmen nur bei konkreten Problemen aktiv und „hoffen eben das Beste".

Angesichts der potenziell katastrophalen Konsequenzen einer Datenpanne sollten IT- und Sicherheitsführungskräfte

wissen, dass es einfache und vor allem kostengünstige Wege gibt, mit denen jedes Unternehmen seine Sicherheit sofort verbessern und das Risiko senken kann.

Wie kann es Ihrem Unternehmen gelingen, das Risiko durch eine proaktive Datensicherheitspolitik zu senken? Befolgen Sie einfach diese vier Hauptschritte:

Schritt 1: Verstehen, wo – und warum – man verwundbar ist.

Zunächst muss Ihnen klar sein, dass es bei Sicherheitsverletzungen meistens um Daten geht und dass diese Daten hauptsächlich auf Datenbankservern lagern. Dort befinden sich Ihre wertvollsten Informationen – und somit die Daten, die auch für Hacker, Internetkriminelle und alle anderen, die Ihrem Unternehmen schaden wollen, am interessantesten sind.

Typischerweise enthalten Datenbankserver Informationen wie Finanzdaten, Kundeninformationen, Kreditkarten- und andere Kontendaten, Krankenakten und personenbezogene Informationen. Laut einer Umfrage befanden sich 96 % aller gestohlenen Daten auf Datenbankservern. Bei größeren Organisationen waren es sogar 98 %.[4]

Gleichzeitig geht aus derselben Umfrage hervor, dass 97 % dieser Pannen durch simple oder mäßig komplexe Kontrollen hätten vermieden werden können. Traurige Realität ist aber, dass viele Unternehmen nicht einmal die grundlegendsten Kontrollen umsetzen, indem sie ermitteln, welche Datenbanken und Datenbankserver am meisten gefährdet sind. Erschwert wird das Ganze noch durch das rapide Datenwachstum und die ausufernde Verbreitung von Datenbanken in Unternehmen. Die Datensicherheit zählt bei vielen Datenbankadministratoren einfach nicht zu den Hauptschwerpunkten: Patches werden nicht durchgehend angewandt und die Unternehmen sind nicht in der Lage, für Systeme zahlreicher verschiedener Anbieter in mehreren Versionen einheitliche Kontrollen und Berichte durchzusetzen.

Wer seine Datenbanken unter Kontrolle bekommen möchte, sollte am besten klein anfangen und sich den Datenbanken mit dem höchsten Risiko zuerst widmen. Wie macht man das am besten? Beginnen Sie mit Schritt 2, nämlich …

Schritt 2: Eine Schwachstellenanalyse durchführen.

Es gibt unkomplizierte, kostengünstige Tools, mit denen Sie die Anfälligkeit aller Datenbanken Ihrer Organisation bewerten können. In den Bereichen, in denen das höchste Risiko besteht, sollten Sie Abhilfe schaffen. Welche Möglichkeiten bieten Ihnen diese Tools? Hier die Hauptfunktionen und Features, auf die Sie achten sollten:

- **Bieten Sie flexible Unterstützung für mehrere Datenbankplattformen:** So kann Ihre Organisation nicht nur Datenbanken wie IBM DB2, Oracle und Microsoft SQL Server prüfen, sondern auch in neueren, bei Big Data Analytics verbreiteten Technologien wie NoSQL nach Schwachstellen suchen.

- **Nutzen Sie automatisierte Tests für sämtliche Datenbanken** zum Schutz vor allen bekannten Arten von Schwachstellen. Das entlastet die ohnehin schon knappen Sicherheits- und IT-Ressourcen und gewährleistet die konsistente Durchführung der Tests.

- **Führen Sie diese automatisierten Tests innerhalb von Minuten aus**, ohne komplexe oder störende Installationen. Mühsame Installations- und Konfigurationsprozesse entfallen, sodass Administratoren eher geneigt sind, entsprechende Tools tatsächlich anzuwenden.

- **Sorgen Sie dafür, dass die Tests stets auf dem neuesten Stand gehalten werden**, mithilfe von in der Branche anerkannten Best Practices – somit ist der Schutz von Daten ein fester Bestandteil Ihrer Geschäftsstrategie und Sie können sich neuen Bedrohungen kontinuierlich anpassen.

Diese Art von Untersuchung können Unternehmen ohne Weiteres und vor allem ohne nennenswerten Einfluss auf das IT-Budget durchführen. Am Ende dieses Artikels finden Sie sogar den Link zu einem kostenlosen Schwachstellenanalysetool, das anhand von Best Practices und automatisierten Prozessen ermittelt, wo Ihr Unternehmen anfällig sein könnte und was Sie dagegen tun können.

Schritt 3: Schwachstellen beheben, Verbesserungen messen und den Erfolg auf die gesamte Organisation übertragen.

Selbstverständlich ist es wichtig, seine Schwachstellen zu kennen. So weiß man, wo man steht. Doch Sie brauchen auch die richtigen Tools, um Ihre Probleme zu erkennen, sie zu beheben und Ihren Fortschritt zu messen. Natürlich wollen Sie den Unterschied zwischen „vorher“ und „nachher“ sehen können. Suchen Sie sich daher im Rahmen der Schwachstellenanalyse eine Lösung, die auch Folgendes bietet:

- **Priorisierter Bericht** Ihres Status-quo, der alle Datenbankinstanzen einschließt.

- **Empfehlungen** zur Behebung der einzelnen Probleme.

- **Grafische Darstellungen** der Verbesserungen im Zeitverlauf, aus denen die genauen Änderungen hervorgehen.

- **Umfassende Liste von Berechtigungen** mit Links zu einem Compliance-Workflow- und Datenbank-Aktivitätsüberwachungssystem, das die Umsetzung von Änderungen verfolgt.

Haben Sie erst einmal die Probleme in den anfälligsten Datenbanken ermittelt und behoben, können Sie den Prozess und seine Vorteile in der gesamten Organisation salonfähig machen. So bringen Sie auch die für Geschäft und Technik zuständigen Personen anderer Abteilungen dazu, ihre eigenen Schwachstellen zu beheben – statt zu warten, bis sie durch eine Datenpanne auf das Problem aufmerksam werden.

Schritt 4: Eine proaktive Strategie zum Schutz Ihrer Daten implementieren.

Datenschutz ist kein einmaliges Unterfangen, sondern eine fortlaufende Geschäftsstrategie. So dient z. B. die Sicherheit von Daten und Kontoinformationen in der Finanzdienstleistungsbranche als Alleinstellungsmerkmal. In anderen Branchen wie dem Einzelhandel haben publik gewordene Datenlecks beträchtlichen finanziellen Schaden bei mehreren Firmen hinterlassen und die Unternehmen gezwungen, ihre Sicherheitsvorkehrungen öffentlich zu thematisieren.

Forrester dazu: „Eine gute Datensicherheit und -kontrolle umfasst weit mehr, als nur das Nötigste zu tun, um Schlimmes zu verhindern. Tatsächlich stellt proaktive Datensicherheit eine wahre Geschäftschance dar. Ermitteln Sie, wie das Business die Daten verwenden möchte, welche Daten benötigt werden und wie diese zu beschaffen sind.“[5]

Ein wichtiger Schritt in der Entwicklung einer Schutzstrategie: Nachdem Sie verifiziert haben, dass Probleme in den bestehenden Systemen behoben wurden, sollten Sie Ihre Datenbanken generell sicherer machen. Sie müssen also Systeme und Prozesse für das Management folgender Schlüsselbereiche entwickeln:

- **Privilegien:** Managen Sie unnötig lockere Nutzerzugangsrechte und richten Sie Prüfungen ein für Objekterstellung, Nutzerrechte, Rechteverteilung an DBAs und Nutzer sowie Rechte auf Systemebene.

- **Authentifizierung:** Prüfen Sie Passwortrichtlinien und Standardanbieterkonten und stellen Sie sicher, dass es keine leeren Kennwörter, Remoteanmeldeparameter etc. gibt.

- **Konfiguration:** Finden Sie bekannte Konfigurationsschwachstellen. Prüfen Sie plattformspezifische Variablen wie die zulässige Höchstzahl fehlgeschlagener Anmeldeversuche für DBA-Profile.

- **Version:** Verifizieren Sie, dass die richtigen Versionsnummern und Patchebenen vorliegen.

Zusätzlich zur Absichung Ihrer Datenbanken sollten folgende Schlüsselfunktionen zur Stärkung der Datensicherheit gegeben sein:

- **Echtzeitüberwachung der Datenaktivität** zur Überprüfung von Datennutzungsmustern und Umsetzung von Sicherheitsstrategien.

- **E-Discovery-Fähigkeit**, mit der Möglichkeit, Infrastrukturen auf sensible Daten/Repositorys zu scannen.

- **Data Masking und Verschlüsselung**, um die Nutzung sensibler Daten im Falle ihres Verlusts oder Diebstahls einzuschränken.

Der Nutzen, der sich aus all diesen Maßnahmen ergibt, geht weit über die reine Sicherheit hinaus. Sie tragen auch zur Einhaltung regulatorischer Vorgaben bei. Darüber hinaus erhalten Sie mehr Kontrolle über Ihre Daten und können diese in Ihrem Geschäft strategisch sinnvoller einsetzen. Ein solider, proaktiver Datenmanagementansatz kann den Grundstein für Big Data Analytics legen und somit für Innovationen, besseren Kundendienst sowie gesteigerte Rentabilität im Unternehmen sorgen.

So beginnen Sie

Die Sicherung Ihrer Datenbanken und sensiblen Daten ist eine geschäftliche Notwendigkeit. Schließlich möchte kein Unternehmen die Folgen einer weitreichenden Datenpanne ausbaden müssen. Dazu Forrester: „Es dauert nicht mehr lange, bis wir auch Datensicherheit und Datenschutz als Alleinstellungsmerkmale im Geschäft sehen werden.

Unternehmen, die diese Themen proaktiv angehen, werden in der heutigen digitalen und datenbasierten Wirtschaft einen Wettbewerbsvorteil haben."[6]

Am besten führen Sie zuerst eine Schwachstellenanalyse durch, um herauszufinden, wo Sie anfällig sind und was Sie dagegen tun können. Mit der 30-Tage-Schwachstellenanalyse von IBM steht Ihnen dafür eine simple, kostengünstige Möglichkeit zur Verfügung. Die Testversion von IBM InfoSphere **Guardium Vulnerability Assessment** bietet alle in diesem Artikel beschriebenen Funktionen und Vorteile, einschließlich:

- Durchsuchung Ihrer Datenbanken zum Auffinden sensibler Daten.
- Untersuchung von Datenbanken auf Schwachstellen: Auf Ihre Datenbanken werden Schwachstellentests angewandt.
- Schwachstellenberichte bereiten Ihre Testergebnisse auf und liefern Ihnen umsetzbare Handlungsempfehlungen.
- Das Berechtigungsmanagement sagt Ihnen, wer worauf zugreifen darf.
- Das Konfigurationsauditsystem überwacht Änderungen auf Betriebssystemebene, die Ihre Organisation für Angriffe anfällig machen.

Neben der Schwachstellenanalyse bietet IBM zahlreiche weitere Funktionen, die gewährleisten, dass Ihr proaktiver Datensicherheitsansatz auch Ihren langfristigen Bedürfnissen gerecht wird. Dazu gehören InfoSphere Discovery, eine E-Discovery-Lösung, die Infrastrukturen auf sensible Daten/Repositorys scannt; InfoSphere Guardium Data Activity Monitor zur Überwachung der Datenbankaktivität; InfoSphere Optim Data Privacy zur Anonymisierung von Daten und InfoSphere Guardium Data Encryption.

Sind Sie bereit, den ersten Schritt zur Verbesserung von Datenschutz und Datensicherheit zu machen? Dann laden Sie sich kostenlos **InfoSphere Guardium Vulnerability Assessment** herunter.

Warum IBM?

InfoSphere Guardium ist Teil des IBM Security Systems Frameworks sowie von IBM InfoSphere Information Integration and Governance (IIG), einer Kernkomponente von IBM Watson™ Foundations, der Big Data- und Analyseplattform von IBM.

InfoSphere IIG bietet ein marktführendes Funktionsspektrum für Big Data und die damit verbundenen Herausforderungen. Es unterstützt optimale Skalierbarkeit und Performance für große Datenvolumina, eine agile und korrekt dimensionierte Integration und Governance, die der zunehmenden Datengeschwindigkeit entspricht, und unterstützt und schützt zahlreiche verschiedene Datentypen und Big Data-Systeme. InfoSphere IIG trägt zum Erfolg von Big Data- und Analyseprojekten bei, indem es Geschäftsanwendern die Gewissheit gibt, auf gewonnene Erkenntnisse vertrauen und entsprechend handeln zu können.

Weitere Informationen

Wenn Sie mehr über IBM InfoSphere Guardium for Applications erfahren möchten, wenden Sie sich bitte an Ihren IBM-Vertreter oder IBM Business Partner oder besuchen Sie uns auf: ibm.com/software/data/guardium

Des Weiteren hilft Ihnen IBM Global Financing dabei, die Softwarefunktionen, die Ihr Geschäft braucht, so kostengünstig und strategisch sinnvoll wie möglich zu erwerben. Wir bieten Kunden abhängig von ihrer Bonität maßgeschneiderte Finanzierungslösungen an, die zu ihren Geschäfts- und Entwicklungszielen passen, ein effektives Cashflow-Management ermöglichen und ihre Gesamtbetriebskosten senken.

Finanzieren Sie Ihre geschäftskritischen IT-Investitionen mit IBM Global Financing und bringen Sie Ihr Unternehmen voran!

Weitere Informationen finden Sie unter: **ibm.com/financing**

IBM Corporation
Software Group
Route 100
Somers, NY 105899 USA

Produziert in den Vereinigten Staaten von Amerika
Dezember 2014

Quellen

1 „2014 Cost of Data Breach Study: Global Analysis“, Ponemon Institute LLC, Mai 2014

2 „Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis“, Ponemon Institute, 5. Mai 2014

3 „Implement a Proactive Strategy for Data Security“, Forrester Consulting, Sept. 2014

4 „2012 Data Breach Investigations Report“, Verizon RISK Team, 2012

5 Ibid, Fußnote 3

6 Ibid, Fußnote 3

Recycling – machen Sie mit!