



Ist ein 339° Security Audit hinreichend?

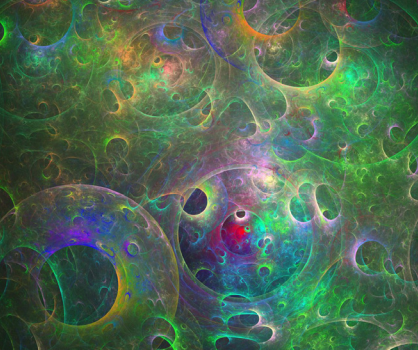
– Ein Whitepaper für CTOs und CEOs

Von Dave Beulke
Aus dem Amerikanischen von Rüdiger Kurtz

Gleichgültig ob man im Sitzungssaal oder im Wohnzimmer ist– jeder möchte wissen, ob persönliche Informationen im Unternehmen sicher sind. Hacking tritt in allen Varianten auf – als Datenklau, als Mittel, Industriegerät zu zerstören oder auch als Waffe, Regierungen zu stürzen, indem politische Geheimnisse veröffentlicht werden. Neuere Studien von Verizon (<http://www.verizonenterprise.com/DBIR/2015/>), FireEye (<http://www.fireeye.com/current-threats/threat-intelligence-reports.html>) haben ergeben, dass im letzten Jahr weltweit mehr als eine halbe Milliarde Datensätze aus Dokumenten und Datenbanken gestohlen wurden. Diese Hackerangriffe haben Unternehmen Hunderte von Millionen Dollar an Ordnungs- und Konventionalstrafen und Unternehmensverlusten gekostet. Ist auch Ihre Firma möglicherweise angreifbar?

Eine positive Wahrnehmung Ihres Unternehmens und seiner Produkte ist in der heutigen Zeit unabdingbar für Erfolg. Für diese positive Wahrnehmung ist die Datensicherheit ein kritischer Baustein. Das Kundenvertrauen und der Ruf des Unternehmens hängen davon ab, indem Sie transparent machen, wie Sie die vielen PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, NIST und andere Compliance Standards befolgen. Jeder dieser Industrie Standards gibt detaillierte Anweisungen zur Vertraulichkeit, Integrität und zum Schutz von privaten Kundendaten. Klar definierte Sicherheitsstandards, Audit Prozesse und deren wirkungsvolle Verarbeitung sind das Fundament, auf dem der Erfolg Ihres Unternehmens langfristig basiert.

“Für diese positive Wahrnehmung ist die Datensicherheit ein kritischer Baustein.”



Die Komplexität des Unternehmens steht dem Erfolg im Weg

Heterogene Altanwendungen und die ständige Entwicklung neuer Umgebungen in Einklang zu bringen ist eine komplexe Herausforderung. Audit und Verwaltung dieser Umgebungen sind zeitaufwändig und ein wiederkehrender Kalvarienweg. Standardisierte Sicherheitsrichtlinien und umfassende Sicherheitsprozesse müssen kontinuierlich auf Wirksamkeit geprüft und an Kosten angepasst werden, wenn neue Systeme online gehen, um deren Verträglichkeit sicherzustellen. Diese wiederkehrenden Ausgaben für diese Compliance-Anwendungen kosten Zeit und binden Ressourcen, die dann aber fehlen, wenn es um das Erreichen der wirklich profitablen Unternehmensziele geht.

Was macht den Unterschied der Security Audit Lösungen aus?

Zunächst brauchen Sie einen Partner mit Erfahrung, der Ihnen zur Seite steht bei der ständigen Analyse der Daten-Zugriffs Aktivitäten und den Anforderungen diverser Industrie-Standards. Heutige moderne Audit Lösungen sollten sich in die bestehende DB2 Infrastruktur integrieren, sehr schnell Datenzugriffe analysieren können und die Komplexität der Security Audit Aufgabe erleichtern. Jede Security Audit Lösung muss die ständig wiederkehrenden Anforderungen an Ihr Geschäftsmodell verstehen und schnell umsetzbar eine umfassende Lösung anbieten, die die vielen unterschiedlichen Dokumentations-Anforderungen der Interessenvertreter im Inneren und die Auditoren von außerhalb zufriedenstellt. Der Stand der Technik bei Security Audit Aktivitäten fordert eine lückenlose Dokumentation über die 3 Bereiche: System, Datenbank und Applikationen. Diese Dokumentation sollte in der Lage sein, alle Arten von granularer, detaillierter Information sowie zusammengefasstes Datenmaterial für jeden Typ von Reporting-Anforderung bereit zu stellen.

Nach vielen Jahren im Dienst unserer Kunden haben wir unsere Expertenwissen auf dem Gebiet der Compliance und des Auditing so verfeinert, so dass wir Ihre Kontrolle über Ihr Unternehmen und die Erfolge auf dem Gebiet des Auditing entscheidend beeinflussen können. Unsere Audit- und Reporting-Lösungen zielen darauf, einen umfassenden Überblick über Ihre Datensicherheit zu bieten, wer auf diese Daten zugreift, welche Mittel er einsetzt, wie er zugreift und wann. Aufgrund dieser Informationen bieten wir praktische Use Cases für die Berechtigungsprüfung an, den Daten-Workload und auch ad hoc Zugriffe innerhalb Ihrer System-Umgebung, die Sie bei Sicherheitsproblemen alarmieren, bevor sie sich zur Krise ausweiten.

Mittels mehrerer Schichten von Zugriffsschutz und einem vollständigen Reporting tragen eine Sicherheitsstrategie und auch ein Compliance-Berichtswesen entscheidend zum Schutz Ihrer Daten bei. Nur wenn man alle Zugriffe innerhalb Ihres Systems aufzeichnet, wie durch SQL innerhalb der Anwendung zugegriffen wird und welche Sicherheitsprofile verwendet werden kann man ein komplettes Bild Ihrer Datensicherheit entwerfen und Ihre Compliance-Standards an Regularien anpassen.

“Diese wiederkehrenden Ausgaben für diese Compliance-Anwendungen kosten Zeit und binden Ressourcen.”

“Die besten Tools nutzen die bestehende DB2 Infrastruktur, um alle SQL Aktivitäten und Daten Zugriff von Anwendungen zu erhalten. Derartige in die bestehende DB2 Infrastruktur eingebettete Tools erzeugen die geforderten Compliance Antworten schnell.”

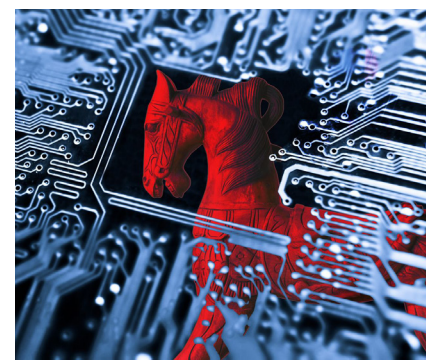
Helfen Sie Ihrem Team

Durch die Nutzung von Tools – viele mit einfach zu bedienenden, geradlinigen GUI Benutzeroberflächen – kann Ihr Team wirksamer seine Security Umgebungsgrenzen (Security Perimeter) navigieren, verstehen und warten. Security Auditoren schätzen es, ein Tool mit guter Architektur und handlichem Design zu benutzen, um rasch Compliance –Reports erstellen zu können, Security Privilegien zu dokumentieren und Profile der Security Objekte zu verstehen. Mit Hilfe einer leicht zu erlernenden GUI Oberfläche verstehen Ihre technischen und fachbezogenen Benutzer sehr schnell die vorhandenen Security Compliance Überlegungen und können sehr schnell Ihre Security Audit ID-Aktivitäten dokumentieren.

Die Auswahl von Security und Audit Tools muss ein Augenmerk auf extensiven Overhead oder schwerfällige Interfaces haben, die zu Performance-Problemen während des Security Compliance Monitorings führen können. Die besten Tools nutzen die bestehende DB2 Infrastruktur, um alle SQL Aktivitäten und Daten Zugriff von Anwendungen zu erhalten. Derartige in die bestehende DB2 Infrastruktur eingebettete Tools erzeugen die geforderten Compliance Antworten schnell für ein reguläres Reporting und stellen auch Report-Lösungen für besonders dringende Untersuchungen zu Unregelmäßigkeiten und Ausnahmen bereit. Der Stand der Technik ist heutzutage ein Sicherheits-Audit-Tool anzuschaffen, das nahezu keinen Overhead produziert, die Implementierung und Benutzung handhabbar macht für konstantes Monitoring, Reporting und Schutz Ihrer wertvollen Daten (data assets)

Die Historie von Berechtigungen, Sicherheitseinstellungen und vergangene Sicherheits- Compliance darzustellen kann jedes Audit-und Compliance-Reporting vor erhebliche Probleme stellen. Um die Kosten des Audits zu minimieren und zu verschlanken ist es hilfreich, ein Werkzeug und einen Partner zu haben, der die Anforderungen des Reporting versteht und weitreichendes Hintergrundwissen besitzt. Durch ein integriertes Security Audit Tool können Ihre Mitarbeitern und Auditoren einfach vorher entwickelten Templates folgen, die es ermöglichen, problemlos ein Repository aufzubauen, um dort Ihre Sicherheits-Compliance Informationen abzulegen – und zwar für alle Anforderungen jedweden Industrie-Standards, zum Exception-Reporting sowie zur raschen Diagnose außergewöhnlicher Security-Vorkommnisse.

Zusätzlich bieten einige Tools historische SQL Daten-Zugriffe und Security-Details, die einen vielfältigen Nutzen bieten: Sie können vergangene Zugriffe auf Ihre Datenbank erfassen und im Detail analysieren, diese Zugriffe für Compliance Reports aggregieren, wiederkehrende Muster in den Zugriffen erkennen oder Sicherheits- und Audit-Kennzahlen darstellen. Durch das SQL Zugriffs Security Repository lässt sich die gesamte Compliance über jeden Zeitraum doku-



mentieren und untersuchen, und alle Anforderungen, die Sie an Sicherheit und Audits haben, lassen sich mühelos und schnell erfüllen. Über diese Reporting-Funktion lassen sich alle Sicherheitsaspekte darstellen, gleichgültig ob für heute, für letzten Monat oder für irgendeinen anderen Zeitraum in der Vergangenheit. Die Möglichkeit, vergangene Compliance zu untersuchen ermöglicht es Sicherheits- und Compliance-Auditoren, dynamisch Berichte zu erstellen, um ihre Bemühungen zu unterstützen.

In der digitalen Weltwirtschaft sind Daten das wertvollste Gut Ihres Unternehmens und deren Sicherheit ist die Basis Ihres Unternehmens. Die Daten zu sichern, vor Zugriffen zu schützen und transparente Sicherheits- und Compliance-Reports helfen Ihren Angestellten und Kunden dabei, Sie als vertrauenswürdigen Partner zu schätzen.

Durch meine jahrelange Erfahrung mit Audits verstehe ich diese Security-Anforderungen, die geforderten Compliance Reporting Fähigkeiten und die notwendigen funktionalen Audit Details. Mit den hinreichenden Erfahrungen und Fähigkeiten einer umfassenden Lösung zur Datensicherheit und eines Compliance-Reportings sind Sie für die Herausforderungen von Morgen gut aufgestellt – und sparen schon heute Zeit und Geld.

Eine Lösung, die ich empfehlen kann ist WorkloadExpert Audit for DB2 z/OS von SOFTWARE ENGINEERING.

Sie erhalten folgende Vorteile:

- Schnell zu erlernen und leicht zu benutzen
- Äußerst geringer bis nahezu kein Overhead
- Unterstützt alle Benutzer im gewünschten Reporting-Umfang
- Umfassende Compliance-Reports für Datenzugriffe und Berechtigungen
- Workload Warehouse für jeden Compliance-Zeitraum

Über den Autor

Der unabhängige Berater Dave Beulke ist ein Systemstratege, ein Anwendungsarchitekt, Sicherheitsauditor und ein Performance-Experte, der auf Big Data, Data Warehäuser und hochverfügbare Internet Geschäftslösungen spezialisiert ist. Er ist seit 1998 IBM Gold Consultant, war einer der ersten IBM Information Champions, ist Präsident von DAMA-NCR, war IDUG-Präsident, und spricht häufig bei nationalen und internationalen Konferenzen zu über Data-Management Themen. Seine Architekturentwürfe, Audits und Tuning-Techniken unterstützen Organisationen dabei, ihr Informationskapital zu schützen und Millionen bei der Verarbeitung einzusparen.

Der Übersetzer: Rüdiger Kurtz ist Datenbankadministrator für DB2 z/OS und DB2 LUW in der Abteilung Informatik Betrieb der HUK Coburg.

