



Wie man einen Security Audit für DB2 z/OS einführt

– Eine Entwurfsvorlage für DBAs

Von Dave Beulke
Aus dem Amerikanischen von Rüdiger Kurtz

Datensicherheit ist heute das beherrschende Thema. Neuere Studien von Verizon, FireEye und Anderen haben ergeben, dass durch Hacking und Informationsdiebstahl im letzten Jahr mehr als eine halbe Milliarde Datensätze aus Dateien 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?

Als Daten-Scientist, Datenbank-Administrator oder als Manager ist Ihnen bewusst, dass eine positive Wahrnehmung Ihres Unternehmens und seines Markennamens in der heutigen Zeit der Schlüssel zum Erfolg ist. Datensicherheit ist hier das kritische Kernstück dieser Wahrnehmung. Kundenvertrauen und gesellschaftlicher Ruf hängen von der Transparenz Ihres Unternehmens ab, und auch davon, inwieweit Sie die sich ständig ändernden und restriktiver werdenden PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, NIST oder andere Industrie-Compliance-Standards befolgen. Klar definierte Sicherheitsstandards, Audit Prozesse und deren wirkungsvolle Verarbeitung sind das Fundament, auf dem der Erfolg Ihres Unternehmens langfristig basiert.

“Klar definierte Sicherheitsstandards, Audit Prozesse und deren wirkungsvolle Verarbeitung sind das Fundament, auf dem der Erfolg Ihres Unternehmens langfristig basiert.”



Die Sicherheits-Audit Denkweise

Aufgrund meiner Berater-Tätigkeit weiß ich, dass die Analyse von Systemen, Datenbanken und Anwendungen im Zuge von Sicherheits-Audits viele Herausforderungen stellt, da jedes Unternehmens einzigartig ist und besondere Anforderungen an die Datensicherheit stellt. Die folgenden Kategorien und Überlegungen stellen die vielen Felder heraus, die evaluiert werden müssen, wenn es darum geht, Security-Audits aufzusetzen, die unterschiedlichen Aspekte von Datensicherheits-Compliance-Audits zu betrachten und eine langfristige Überwachungslösung gegen Hackerangriffe mittels einer umfassenden Sicherheits-Audit-Strategie zu implementieren.

Aufgrund seines Industriezweigs, der IT-Landschaft, dem Nebeneinander von eigenentwickelter und gekaufter Software und unterschiedlicher Programmiersprachen und Schnittstellen zu den Daten hat jedes Unternehmen spezielle Anforderungen an Datensicherheit und Compliance. Diese unterschiedlichen, einzigartigen Gebiete stellen gewaltige Herausforderungen dar, vergleichbar mit den umfangreichen und ebenso einzigartigen Disaster Recovery Prozeduren, die von Ihren engagierten Mitarbeitern beständig überwacht werden müssen, um den Geschäftsbetrieb zu gewährleisten. Um die Datensicherheit zu gewährleisten ist der gleiche Aufwand an Ressourcen für Sicherheit und Compliance erforderlich. Der Umfang unternehmenskritischer Faktoren ist in beiden Fällen ähnlich, und das Top-Management muss fest hinter der geforderten Zeit, den geforderten Ressourcen und Tools stehen, um Ihr Unternehmen und seine Produkte zu schützen.

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 kosten Zeit und binden Ressourcen, die dann aber fehlen, wenn es um die Erreichung der wirklich profitablen Unternehmensziele geht.

“Audit und Verwaltung dieser Umgebungen sind zeitaufwändig und ein wiederkehrender Kalvarienweg.”

Benutzerfreundliche Implementierung und Anwendung

Die heutigen dynamischen und unterbrechungsfreien Systeme, Datenbank- und Anwendungsumgebungen erfordern, dass Sicherheits- und Auditprozeduren und entsprechende Werkzeuge extrem leicht zu implementieren und zu benutzen sind. Die Dauer der Implementierung, standardisierte Audit-Prozeduren, Interfaces, die schnell Ergebnisse liefern und ein stabiles Berichtswesen sind entscheidend, um den Anforderungen an komplexe dynamische Sicherheitsumgebungen zu begegnen.

Die seitens der Industrie angebotenen Sicherheits- und Audittools bieten viele Optionen und Implementierungsstrategien. Spezielle Definitionen von Sicherheits- und Auditinfrastruktur sind mühsam zu implementieren, zu warten und zu erweitern. Die beste Lösung alle Sicherheits- und Auditaspekte abzudecken ist, die mit der vorhandenen Datenbank ausgelieferten Werkzeuge, das Logging und die vorhandenen Schnittstellen zu nutzen, um die Nutzung der Daten und die Infrastruktur der Datenbank zu überwachen. Diese in der Datenbank integrierten Werkzeuge, das Logging und die anderen Schnittstellen zu Sicherheits- und Auditaktivitäten zu nutzen gewährleistet am sichersten den gesamten Überblick. Die eingebauten Möglichkeiten liefern alle Informationen über Zugriffe, können dynamisch alarmieren und geben Einzelinformationen, um Ihre Daten proaktiv zu schützen.

So komplex die Umgebungen und die Datenhaltung auch immer sein mögen, die Implementierung von Sicherheits- und Auditfeatures muss schnell und leicht anhand von vorgegebenen Beispielen, Templates und vordefinierten Konfigurationen sein. Diese Konfigurationen müssen im Anschluss anzupassen sein, um die Zusammenarbeit mit Auditoren zu erleichtern und detaillierte Informationen für mögliche Gefahren und Sicherheitslücken bereitzustellen.

Dynamische Sicherheitsaudits sind unabdingbar

Oft bürdet man Sicherheitsaudits und Compliance-Anforderungen dem Sicherheitsteam auf, das, obschon unterbesetzt und überbelastet, gewöhnlich schon mit dem Tagesgeschäft und neuen Projekten ausgelastet ist. Dort werden dann nur in regelmäßigen Abständen Sicherheitsaudits und Compliance-Aktivitäten durchgeführt und die letztlich immer gleichen Audit-Definitionen setzen die System- und Datenbanksicherheit den neuesten Hacking-Methoden aus. In der heutigen sich dynamisch ändernden IT-Landschaft sind statische Sicherheitsaudits nicht effektiv genug für sich permanent ändernde Systeme, Anwendungen und Techniken von Hackern.

System- und Anwendungsänderungen bedürfen ständigem Sicherheitsauditing, um schnell Hackingversuche zu analysieren, zu identifizieren und vor ihnen zu schützen. Dynamische Hacking-Techniken und die ständige Suche nach System- und Datenbankschwachstellen umgehen leicht statische Sicherheitstechniken und Audit-Prozesse. Heute werden Geschäfte 24*7*365 getätigt, und Ihr Sicherheitsauditing und Ihre Sicherheitsprozesse müssen so dynamisch sein wie die permanenten Versuche, in Ihre Systeme einzudringen und sie anzugreifen.

“Wissen über Audit und Reporting und effektive Nutzung geeigneter Sicherheits- und Audit-Werkzeuge fokussieren schnell auf Compliance-Anstrengungen.”

Erfüllen Sie die aktuellen dynamischen Anforderungen

Erfahrene Berater, die die neuesten Werkzeuge anwenden und die wiederkehrenden Anforderungen an das Reporting und Geschäftssteuerung kennen sind lebensnotwendig. Diese Partner und Werkzeuge können Ihrem Unternehmen dabei helfen, umfassende multi-dimensionale Lösungen aufzusetzen, die die Anforderungen an Sicherheitsaudit und Compliance erfüllen, die Ihr Industriezweig, die speziellen Anwendungen innerhalb Ihres Unternehmens und ein Gesamtreporting für Compliance stellen. Dies kann eine äußerst komplexe Aufgabe sein, da es so viele unterschiedliche Dokumentationsanforderungen seitens Interessenvertretern von innen und von Auditoren von außen gibt. Darüber hinaus stellt Ihr Unternehmen möglicherweise spezielle Compliance-Reports für Industriekammern, für Regierungsbehörden und für andere Auditoren von außen zusammen. Um ein Werkzeug zu bekommen, das Best Practices nutzt müssen Sie Compliance Automations-Werkzeuge auf ihre Benutzerfreundlichkeit überprüfen und auf die Möglichkeit, alle Arten von äußerst detaillierten Security-Audit-Informationen ebenso bereit zu stellen wie auch zusammenfassende Berichte, die alle Arten von Reports und auch Anforderungen an den zeitlichen Rahmen abdecken.

Im Lauf der Zeit führen in Ihrem Unternehmen durchgeführte Sicherheitsaudits dazu, Sicherheitsanwendungen und ihre Compliance zu verbessern und zu verfeinern. Das Wissen über Compliance, gewonnen in unterschiedlichen Industriezweigen, und Audit-Details können die Zeit verkürzen, Compliance zu erreichen, und sie machen den entscheidenden Unterschied, wenn es darum geht, Erfolg bei der Betriebsführung und der Compliance zu haben. Wissen über Audit und Reporting und effektive Nutzung geeigneter Sicherheits- und Audit-Werkzeuge fokussieren schnell auf Compliance-Anstrengungen. Dieser Fokus hilft jedem dabei, sich darauf zu konzentrieren, einen umfassenden Blick auf Ihre Datensicherheit zu haben, darauf, wer auf Ihre Daten zugreift, welche Methode er nutzt und wie und wann zugegriffen wurde. 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, noch bevor sie sich zur Krise entwickeln.





Fit für morgen

Erweiterungsmöglichkeiten und Ausbaufähigkeit sind zwei weitere Gesichtspunkte, die es gilt im Auge zu behalten, wenn man mögliche Audit-Compliance und Automations-Werkzeuge evaluiert. Bewerten Sie, wie leicht oder wie schwer es ist, neue Sicherheitsauditbereiche und neue Anwendungen hinzuzufügen, oder neue Dokumente in die Auswahl Ihres Compliance-Reporting. Evaluieren Sie genauso die unterschiedlichen Arten von Berichten, die Ihre Werkzeuge aufgrund der zugrundeliegenden Sicherheitsaudit-Information bereitstellen können. Stellen Sie sicher, Standard Compliance-Berichte ebenso bereitstellen zu können wie auch Tabellen oder spezielle detaillierte Berichte über einzelne Sicherheitsgebiete.

Bewerten Sie auch, wie leicht es ist, Charts, Kreisdiagramme und Pivot-Tabellen Ihrer Compliance und der Sicherheitsinformationen zu erzeugen. Versuchen Sie zu Beginn Ihrer Evaluierungsbemühungen all die Sicherheitsaudit- und Compliance-Berichte zu erzeugen, von denen Sie glauben, dass Ihr Unternehmen sie regelmäßig benötigt, oder versuchen Sie die Zeit zu schätzen, die Sie benötigen, um sofort mannigfaltige Sicherheitsaudit- und Compliance-Berichte für Industriekammern, Auditoren im Innern und verschiedene Managementebenen bereitzustellen.

Sobald die Standard Sicherheits- und Compliance-Berichte evaluiert wurden versuchen Sie, diese verschiedenen Berichte dahingehend auszuweiten, andere Geschäftsfelder oder Sicherheitsaspekte zu erweitern. Entscheiden Sie, ob diese Ausweitung leicht möglich ist oder wie schwierig es ist, einen Compliance-Bericht ad-hoc zu einem Sicherheitsvorfall zu erzeugen.

Als Nächstes untersuchen Sie, wie leicht sich der Berichtszeitraum von Standard-Perioden auf einen flexiblen Zeitrahmen umstellen lässt, und wie leicht sich der Umfang der Audit-Berichte erweitern oder zusammenfassen lässt. Der Sicherheitsberichtszeitraum ist äußerst wichtig, da er jedem letztlich hilft zu verstehen, wie wichtig es ist, Änderungen am Sicherheitssystem zu befürworten, welchen Einfluss auf die Zugriffe diese Änderungen im Lauf der Zeit haben und welche Auswirkungen sie auf das System oder Anwendungen haben.

“Der Sicherheitsberichtszeitraum ist äußerst wichtig, da er jedem letztlich hilft zu verstehen, wie wichtig es ist, Änderungen am Sicherheitssystem zu befürworten, welchen Einfluss auf die Zugriffe diese Änderungen im Lauf der Zeit haben und welche Auswirkungen sie auf das System oder Anwendungen haben.”



Mehrschichtiger Ansatz

Mittels mehrerer Schichten von Zugriffsschutz und einem vollständigen Berichtswesen tragen eine Sicherheitsstrategie und ein Compliance-Berichtswesen entscheidend zum Schutz Ihrer Daten bei. Ihr Unternehmen benötigt ein vollständiges Bild der Sicherheitsanforderungen. Die beste Technik besteht darin, alle Arten von Datenzugriffen über Schnittstellen zu erfassen und aufzuzeichnen, ebenso wie die SQL-Zugriffe über Anwendungen. Um die Sicherheits- und Auditberichte vollständig zu haben müssen in ihnen auch alle ad-hoc Zugriffe auf Datenbanken und alle Utility-Läufe dokumentiert, analysiert und eingeschlossen sein.

Eine weitere Schicht für Sicherheitsaudit-Berichte sind die Sicherheitsprofile für Datenbanken und Dateien. Im Detail darzulegen, welche unterschiedlichen Nutzer und Benutzerkennungen verschiedene Lese- und/oder Schreibzugriffe auf verschiedene Datenbankobjekte und Ordner haben ist eine weitere Analyseschicht Ihrer Sicherheits- und Auditberichte. Sie müssen Objektzugriffsrechte gemeinsam mit den Informationen über Anwendungen analysieren, um herauszufinden, ob es Überschneidungen gibt, oder ob Benutzer Rechte über Datenbanken oder Anwendungen hinweg haben, die zuweilen ein Sicherheitsrisiko darstellen können.

Die Historie von Berechtigungen, Sicherheitseinstellungen und vergangene Sicherheits- Compliance darzustellen kann jedes Audit-Tool und jeden Compliance Auditor vor erhebliche Probleme stellen. Um den Audit zu verschlanken und seine Kosten zu minimieren ist es hilfreich, ein Werkzeug und einen Partner zu haben, der die Anforderungen des Reporting versteht und der weitreichendes Hintergrundwissen besitzt. Mitarbeiter und Auditoren müssen Compliance Templates wirksam einsetzen, um ein Repository aufzubauen, in dem alle Sicherheits-Compliance Einstellungen über die Zeit hinweg gespeichert werden, um alle möglichen Sicherheits-Profil-Berichte, abhängig von der Zeit, zu erzeugen.

Einige Sicherheits- und Audittools sind umständlich zu bedienen und haben einen massiven Overhead, der sich negativ auf die Performance beim Monitoring der Sicherheits-Compliance niederschlagen kann. Leicht zu nutzende Methoden, um schnelle Antworten und Compliance-Lösungen zu erhalten sind für das normale Reporting vorrangig und bei weitreichenden Untersuchungen von Unregelmäßigkeiten und Ausnahmen unabdingbar. Unsere Sicherheits-Audit-Tools haben nahezu keinen Overhead, erleichtern die Implementierung und Anwendung für permanentes Monitoring, Reporting und zum Schutz Ihrer wertvollen Daten.

Sicherheitsmessungen, Analyse- und Verbesserungsprozeduren

Wenn man einen Sicherheitsaudit in Angriff nimmt, ist es unabdingbar, einen Rundum-Blick auf das Sicherheitsumfeld innerhalb Ihrer Organisation zu implementieren, auf seine Systeme, Anwendungen und auch das Personal. Gewöhnlich ist es ein guter Ausgangspunkt, die grundlegenden Sicherheitsanforderungen für die aktivste und profitabelste Anwendung zu entwickeln. Die allgemeinen Sicherheits- und Auditanforderungen zu sammeln, und dann alle datenbank- und personenbezogenen Aktivitäten zu erfassen bringt Licht ins Dunkel für alle Beteiligten aus der Technik und dem Management.

Diese erste Sicherheitsdatensammlung ist die Baseline und der Anfang des Sicherheitsaudits und des Berichtswesens. Hoffentlich ist niemand überrascht von der großen Anzahl unterschiedlicher Zugriffe und Nutzer, die ermittelt wird. Diese Zugriffstypen zu gruppieren und die Nutzer zu klassifizieren ist der erste Schritt, wenn es darum geht, einen Sicherheitszaun um die unterschiedliche Nutzung von System, Datenbanken, Anwendungen und zugehörige Nutzung von Files zu ziehen.

Als nächster Schritt kommt die Monitoring- und Messphase, in der die Sicherheitsgruppierungen und Zahlen, die in der Analyse festgestellt wurden, validiert werden. Ändern sich die Usertypen, die Anzahl der Zugriffe im Laufe des Tages, oder ändert sich das Zugriffsverhalten? Wenn es Fluktuationen in der Nutzung gibt, lassen sich bessere Sicherheitseinstellungen oder Sicherheitsgruppierungen innerhalb vernünftiger Toleranzgrenzen finden, die deren Management erleichtern? Diese Sicherheits- und Auditfragen sind zuallererst zu beantworten für die wichtigsten PII, HIPPA und geheimer Daten, die letztlich die Sicherheits- und Auditaktivitäten überhaupt rechtfertigen, und dann für alle nicht so wichtigen Datenobjekte in anderen Systemen, Datenbanken und Anwendungen.

Daraufhin muss die in der Baseline festgestellte Nutzung den Geschäftsprozessen gegenübergestellt werden, die Abweichungen in der Anzahl der Zugriffe und die unterschiedlichen Benutzeranforderungen sind zu beurteilen. Weicht die Anzahl oder der Typus der Benutzer von der vernünftigerweise zu erwartenden Nutzung ab, oder taucht ein einzelner, unerwarteter Benutzer auf ist das möglicherweise ein Hinweis auf einen Hackerversuch auf Ihr System, ihre Datenbanken oder Ihre Anwendungen. Abhängig von den Sicherheitsaudit-Ergebnissen kann im schlimmsten Fall die Reaktion darauf sein, das gesamte System, die

“Wenn man einen Sicherheitsaudit in Angriff nimmt, ist es unabdingbar, einen Rundum-Blick auf das Sicherheitsumfeld innerhalb Ihrer Organisation zu implementieren.”

Datenbanken und Anwendungen herunterzufahren oder vielleicht einfach auch nur darin bestehen, den Endnutzern ein paar allgemeine Fragen zu stellen. Ein Monitoring der Datenzugriffe, die Überarbeitung von Sicherheitsprofilen oder Meldungen an das Management über auftretende Anomalien müssen in die Standard-Eskalations-Prozesse eingearbeitet werden, die für die unterschiedlichen Sicherheitsszenarien bestehen.

Diese Anomalien können auch zu einer Vielzahl von Diskussion über die internen Auditergebnisse führen. Der Schlüssel hierbei ist es, die Sicherheitslandschaft Ihres Systems, Ihrer Datenbanken und Anwendungen zu evaluieren und dann festzulegen, wie misstrauisch, skeptisch und neugierig man sein will, um den berechtigten Zugriff von böartigen Versuchen zu trennen, die jemand unternimmt, um einen Trojaner in Ihre Systemarchitektur einzuschleusen.

Weiterhin muss bei der internen Audit-Evaluierung festgelegt werden, mit welcher Toleranz und welchen Mitteln man diesen unterschiedlichen Situationen begegnet, unabhängig davon, wie groß oder klein diese Sicherheitsanomalie in Ihrer Sicherheitslandschaft ist. Welche Sicherheitskontrolle rechtfertigt jede einzelne dieser Situationen im Gesamtzusammenhang des Schutzes und der Sicherheit Ihrer Daten? Wie gehen die Geschäftsprozesse mit diesen Kontrollen um, ohne weiteren Zugriff auf andere Unternehmensdaten zu gewähren? Diese Überlegungen können große Bedenken und weitreichende Sicherheitsfragen aufwerfen, wenn man die Millionen Dollar berücksichtigt, die bei einer möglichen Lücke bei den PII und anderen kritischen Daten in Ihrem Unternehmen auf dem Spiel stehen.

Schließlich sind Präventiv- und Korrekturmaßnahmen zu etablieren, die ein geordnetes Vorgehen erlauben wenn es darum geht, alle Systeme, Datenbanken und Anwendungen zu kontrollieren, zu korrigieren und für zukünftige Sicherheitsfragen und Audits zu standardisieren. Die ursprünglichen Ziele, nämlich den bestmöglichen Zugriff bei bestmöglicher Sicherheit auf die richtigen Geschäftsprozesse zu gewähren sind entscheidend für Ihr Geschäft. Maßnahmen, die Sicherheit zu verschärfen und die Diskussionen darüber müssen sich auf die Anomalien und die Korrekturmaßnahmen konzentrieren, um vertrauenswürdige Nutzungen von den Anomalien zu trennen, um diese dann genauer zu untersuchen, bis die Verifizierung aller Nutzer und ihres Zugriffs vollständig abgeschlossen ist.

All diese Sicherheitsaudit-Maßnahmen und Prozeduren sind nur der erste Schritt in einem fortschreitenden Prozess, der jeden Tag, jede Woche und jedes Quartal für sich ändernde Datenbanken und Anwendungen innerhalb Ihres Unternehmens wiederholt werden muss. Sicherheitseinstellungen und Nutzer stellen immer wieder neue und interessante Anforderungen an Ihre Fähigkeit, Sicherheits- und Auditaktivitäten, Analysen und Korrekturmaßnahmen an alle Geschäftsanforderungen anzupassen und dabei Ihre Daten zu schützen.



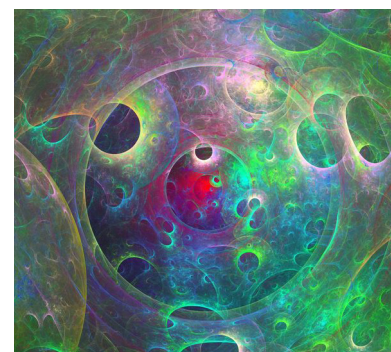
Helfen Sie Ihrem Team

Eine weitere Anforderung besteht darin einen Partner zu haben, der Ihre Mitarbeiter unterstützt, sich im Sicherheitsumfeld zurecht zu finden, es zu verstehen und aufrecht zu erhalten. Darüber hinaus ist es von Vorteil, einfache und leicht zu verstehende GUI-Interfaces einzusetzen. Werkzeuge, die leicht zu nutzen sind, die schnelle Antworten auf Fragen geben, und die eine leichtverständliche Architektur bieten, die schnell Compliance-Berichte zulassen, die Dokumentation von Zugriffsrechten erleichtern, und Sicherheitsprofile verstehen helfen stellen einen großen Nutzen dar und lassen Sie ruhig schlafen, da Sie wissen, dass Ihre Daten sicher sind. Jeder Nutzer, gleich ob technischer und Anwendungsbenutzer, versteht die Sicherheits-Compliance-Überlegungen anhand einfacher GUI-Interfaces und Datenschnittstellen, die die Erstellung von Charts, Tabellen und anderer Geschäftsberichte unterstützen.

Werkzeuge, die ein Repository besitzen, das die Vergangenheit widerspiegelt können ebenfalls von großem Nutzen sein, wenn es darum geht, Sicherheitsaudit-Informationen zeitbezogen darzustellen. Ein Repository für SQL-Zugriffe ist vielfältig einsetzbar; es kann helfen vergangene Datenbank-Zugriffe erfassen und im Detail analysieren, die Zugriffe für Compliance-Berichte zu aggregieren, Zugriffsmuster herauszufinden, Sicherheit oder Audit-Metriken darzustellen. Mittels des historischen SQL-Zugriff-Repositorys ist es möglich, alle Arten von Sicherheitsfragen über jeden denkbaren Zeitraum für Compliance zu dokumentieren. Ein SQL-Zugriffs-Repository gibt dem Auditor effektiv und problemlos tiefe Einblicke in die Sicherheit, die es ihm ermöglichen, alle Anforderungen an das Compliance-Berichtswesen zu erfüllen. Untersuchen Sie alle Sicherheits-Compliance-Aspekte für heute, für den letzten Monat oder irgendeinen anderen Zeitraum in der Vergangenheit, indem Sie rasch auf das SQL-Zugriffsrepository zugreifen. Die Fähigkeit, Sicherheits-Compliance historisch zu untersuchen ermöglicht es den Sicherheits- und Compliance-Auditoren, dynamisch Berichte zu erstellen, die ihre speziellen Sicherheitsaudits erweitern helfen.

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 die vielen Jahre, in denen ich Audits durchgeführt habe, verstehe ich diese Sicherheitsanforderungen, diese Möglichkeiten zum Compliance-Berichtswesen und die Details bei den Audit-Funktionalitäten. Es spart Ihnen Zeit und Geld, wenn Ihre Erfahrung und die Fähigkeit in die umfassende Lösung einfließen, ihre Daten zu sichern und heute Compliance-Berichte für die Herausforderungen von Morgen zu erstellen.



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

“ In der digitalen Weltwirtschaft sind Daten das wertvollste Gut Ihres Unternehmens und deren Sicherheit ist die Basis Ihres Unternehmens. ”

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.

© 2016 SOFTWARE ENGINEERING and SEGUS Inc.

