Drei Banken, ein Sicherheitsmodell

Dynamisches Audit garantiert Compliance-konformes Arbeiten

Frank Zscheile, freier Journalist.

Die Einführung des Beta 96 Enterprise Compliance Auditors bedeutete für die 3 Banken EDV Gesellschaft m.b.H. (3BEG) aus Linz den Einstieg in ein dynamisches Audit. Die 3 Banken Gruppe realisierte ein zentrales Sicherheitskonzept mit Verwendung vorgefertigter z/OS Control Procedures zur exakten Umsetzung von BSI-, ISO- und CobiT Vorgaben.

Für Datensicherheit zu sorgen, ist heute eines der wichtigsten Kriterien jedes Finanzinstitutes. Ein zu sorgloser Umgang mit Nutzerrechten und Zugriffsmöglichkeiten auf sensible Informationen entscheidet unter Umständen nicht nur über Aufstieg oder Fall eines Bankhauses – das Ansehen eines ganzen Landes als zuverlässiger Bankstandort kann so in Misskredit geraten. Auch in der Bewertung durch Wirtschaftsprüfungsgesellschaften nehmen Sicherheitsthemen heute einen immer größeren Stellenwert ein. Aspekte, die sich letztlich im Rating niederschlagen.

Das ist nichts Neues für die 3-Banken-Gruppe, einen losen, 1997 entstandenen Zusammenschluss von drei österreichischen Kreditinstituten: der Bank für Tirol und Vorarlberg (BTV), der BKS Bank AG und der Oberbank. Sie beschäftigen rund 3.300 Mitarbeiter, die gemeinsame Bilanzsumme betrug 2006 ca. 25,8 Mrd. Euro. Die Banken sind gegenseitig am Kapital der jeweils anderen Banken beteiligt und nutzen ein gemeinsames Corporate Design, sind aber dennoch voll eigenständig. Bereits 1991 intensivierten die drei Regionalbanken ihre langjährige Zusammenarbeit im Bereich Organisation und EDV. Die Rechenzentren wurden ausgegliedert und in der neuen 3 Banken EDV Gesellschaft m.b.H, kurz: 3BEG, zusammengelegt.

Dipl. Ing. Anton Scheiber und Dipl. Ing. Robert Fleischer

Druck auf die EDV-Abteilungen

In den letzten Jahren erhöhte sich durch schärfere Gesetze und Richtlinien der Druck auf die EDV-Abteilung der 3 Banken Gruppe, ihre IT-Sicherheit und das Berichtswesen weiter zu optimieren. Ausgangspunkt waren die 8. EU-Richtlinie (EuroSox) und Basel II als gesetzesnahe Komponenten. Dazu kommt speziell in Österreich das Aktiengesetz. „Diese gesetzlichen Vorgaben enthalten jedoch keine, direkt in die IT übernehmbaren Formulierungen“, erklärt Dipl.-Ing. Robert Fleischer, Abteilungsleiter Systemtechnik und Produktion bei der 3BEG. Wir orientieren uns daher an den BSI IT-Grundschutzkatalogen, der ISO 27001 sowie CobiT 4.0.“ Vor allem CobiT (Control Objectives for Information and Related Technology), ein internationales Modell zur Überwachung der gesamten IT-Prozesse, ist in der österreichischen Bankenlandschaft stark verankert. Das Rahmenwerk wurde von der Information Systems Audit and Control Foundation (ISACF) entwickelt, dem Forschungsinstitut der Information Systems Audit and Control Association (ISACA). Es besteht aus gängigen Praktiken, kurz als „IT Governance“ bezeichnet, die sicherstellen, dass die IT-Prozesse die Geschäftsziele abdecken und Risiken angemessen überwacht werden. CobiT enthält konkrete Ziele, nach denen sowohl interne als auch externe Prüfer in Österreich und in zahlreichen weiteren Ländern vorgehen.

Die dort enthaltenen Maßnahmen gilt es, in konkrete Auswertungsvorschriften oder Control Procedures umzuwandeln. Zum Beispiel müssen die maximale Anzahl ungültiger Anmeldeversuche, die Anzahl der Tage bis zur Sperrung inaktiver Benutzer oder die Anzahl der Notuser mit den Ist-Werten abgeglichen werden. Neben diesen Einstellungen lassen sich auch Ereignisse aus IBMs Resource Access Control Facility (RACF) integrieren. Dabei handelt es sich um IBMs Implementation der Sicherheitschnittstelle SAF (System Authorization Facility) des Betriebssystems z/OS. Zu den unterstützten Ereignissen zählen Änderungen an den globalen RACF-Optionen (SETROPTS), mehrfach zurückgesetzte Kennwörter oder ungültige Anmeldeversuche.

Lösung gesucht

Das Unternehmen suchte eine Lösung für den dynamischen Audit im z/OS Bereich, die alle erforderlichen Maßnahmen aus BSI, ISO 27001 sowie CobiT abdeckt und dadurch die Einhaltung von Compliance-Vorschriften garantiert. Diese Maßnahmen kombinierte das IT-Team der 3 Banken Gruppe mit eigenen Vorstellungen zur IT-Sicherheit. Daraus wurde ein Anforderungskatalog zusammengestellt und mit der internen Revision abgestimmt. Mit den passenden Vorgaben ausgestattet, begab sich die 3BEG auf die Suche nach einem passenden Anbieter. „Wir starteten eine Marktbeobachtung: Welcher Anbieter kann für RACF-Audits und Compliance-Themen eine unterstützende Lösung anbieten“, erklärt Dipl.-Ing. Anton Scheiber, verantwortlich für Systemtechnik und Produktion bei der 3BEG. „Drei Produkte kamen in die engere Auswahl und wurden von uns getestet, darunter auch der Beta 96 Compliance Editor von Beta Systems.“

Mit dem deutschen Hersteller Beta Systems verband die 3 Banken Gruppe eine langjährige Partnerschaft. Schon 2003 unterstützte Beta Systems die 3BEG bei der

Eckdaten

Kunde: 3BEG
Gründungsjahr: 1991
Mitarbeiter/Innen: 175
Zentrale: Linz
Geschäftsführung: Dipl.-Ing. Günter Buchmayr, Mag. Bernd Geiger
Umsatz (2007): 38,83 Mio. €
Geschäftsstellen: 210
Konten: ca. 1,5 Mio.

Zusammenlegung von drei RACF-Datenbanken. Zudem waren Beta 92 und Beta 93 bereits im Zuge der Konsolidierung eingeführt worden. So ist es wenig verwunderlich, dass die Wahl für das Audit-Tool ebenfalls auf Beta Systems fiel. „Wir wollten mit der Audit-Software klare z/OS-Control Procedures an die Hand bekommen, um die geltenden Compliance-Vorschriften zu erfüllen. Unserer Ansicht nach waren diese bei Beta Systems am besten ausgeprägt, dokumentiert und zugleich am besten ausbaubar“, so Dipl.-Ing. Scheiber.

Gerhard Juri, verantwortlich für IT-Security und Projektkontrolle

Für die Anpassung an die Anforderungen der 3 Banken Gruppe wurden 35 konkrete Daten-Auswertungsvorschriften aus den vorgegebenen BSI-, ISO- und CobiT-Maßnahmen abgeleitet und innerhalb von Beta 96 in konkrete Control Procedures umgewandelt. Wichtig war dem IT-Team vor allem die Auswertbarkeit. Output und Bedienbarkeit sollten sich nicht an den Erfordernissen von RACF-Systemprogrammierern orientieren, sondern auch für Nicht-Techniker nutzbar sein.

Daten konsolidiert

Besonders schätzt das IT-Team der 3BEG die Offenheit des Audit-Tools. Gerhard Juri, verantwortlich für IT-Security und Projektcontrolling: „Wenn wir einen Bedarf für weitere Control Procedures sehen, können wir diese entweder selbst oder mit Hilfe des Herstellers umsetzen.“ Ein wichtiges K.O.-Kriterium bei der Produktauswahl war auch die Möglichkeit zur flexiblen Erweiterung. Unter Beweis gestellt wurde sie schon während der drei Einführungsworkshops von je drei Tagen Dauer: Ein 3BEG-Team erstellte dort eigenständig eine ISO-Auswertungsvorschrift und fügte sie den bestehenden Control Procedures in Beta 96 hinzu. Insgesamt war das IT-Team etwa drei Monate mit der Implementierung des Tools beschäftigt. Nach einem halben Jahr Praxisbetrieb war die Zahl der Auswertungsvorschriften bereits auf 50 gestiegen.

Die Ist-Daten für den Control Procedure-Abgleich entstammen verschiedensten Datenquellen: den globalen RACF-Einstellungen, der RACF-Datenbank, den SMF-Sätzen sowie den z/OS Systemeinstellungen. Die Datenextraktion wird über z/OS-Jobs angestoßen; damit nur solche Daten betrachtet werden, die für die Auswertung der Control Procedures benötigt werden. Die Daten werden gefiltert und in so genannte Result Data Sets abgelegt.

Impressum

Informationsdienst IT-Grundschutz

4. Jahrgang – ISSN 1862-4375

Herausgeber
Nina Malchus

Redaktion
Elmar Török, Fachjournalist
(verantw. für den redaktionellen Teil)
Auf dem Rain 2, 86150 Augsburg
Tel.: +49 821 4981635
E-Mail: redaktion@grundschutz.info

Verlag
SecuMedia Verlags-GmbH
Lise-Meitner-Str. 4, 55435 Gau-Algesheim
www.secumedia.de

Beteiligungsverhältnisse (Angabe gem. §9, Abs.4 Landesmediengesetz RLP) Gesellschafter zu je 1/6 sind Gerlinde Hohl, Klaus-Peter Hohl, Peter Hohl (GF), Veronika Laufersweiler (GF), Nina Malchus (GF), Stefanie Petersen.
Registereintragung: Handelsregister Mainz B 22282
Umsatzsteuer-Identifikationsnummer: DE 148266233

Abo-Service
Veronika Leuschner
Tel.: +49 6725 9304-25
Fax: +49 6725 5994
E-Mail: aboservice@secumedia.de
www.grundschutz.info

Anzeigenleitung
Stefanie Cutuk
(verantw. für den Anzeigenteil)
Tel.: +49 6725 9304-15
E-Mail: anzeigenleitung@secumedia.de
Mediadaten unter: www.grundschutz.info

Bezugspreise/Bestellungen/Kündigung
Erscheinungsweise 10 Mal jährlich
(2 Doppelausgaben)

Jahresabopreis für die Printausgabe:
98,00 € inkl. MwSt. u. Vers.k. (Inland) /
116,10 € inkl. MwSt. u. Vers.k. (Ausland).
Einzelheft: 9,50 € inkl. MwSt.u. Vers.k. (Inland) /
11,00 € inkl. MwSt. u. Vers.k. (Ausland).

Eine Kündigung ist jederzeit zur nächsten noch nicht gelieferten Ausgabe möglich. Überzahlte Beträge werden rückerstattet.

Preis im Koppelabonnement mit den Zeitschriften <kes> oder WIK:
Jahresabopreis: 76,00 € inkl. (Inland) / 84,53 € (Ausland) inkl. MwSt. und Versandkosten 130,00 SFr. (Schweiz)

Vertriebskennzeichen: ZKZ 78871

Satz/Druckvorstufe
BLACKART Werbestudio Schnaas und Schweitzer, Stromberger Str. 47, 55413 Weiler

Druck
Silber Druck oHG,
Am Waldstrauch 1, 34266 Niestetal

Diese Result Data Sets werden dann gemeinsam mit den Target Data Sets im Beta 92 Logfile-Archiv abgelegt. Damit ist die Paarung von Soll- und Ist-Werten, beispielsweise über die erlaubte und die tatsächliche Anzahl von Anmeldeversuchen eines Nutzers an einem Tag, vollzogen. Aus Beta 92 transferiert der Beta Systems Data Mover die Sets anschließend in die Windows-Umgebung von Beta 96. dort wird anhand von SQL-Abfragen der Vergleich der Werte angestellt und auf mögliche Abweichungen von der Control Procedure untersucht. Damit lassen sich auch große Mengen an Systeminformationen wie beispielsweise Config-Logs oder Event-Logs analysieren. Das Ergebnis ist ein Audit-Report, der als PDF, als E-Mail oder im CSV-Format auf einem Server der 3BEG abgelegt ist.

Kritische Vorgänge aufdecken

Gerhard Juri von der IT-Security der 3BEG erläutert das Berichtswesen: „Wir fahren unser Berichtswesen im Rahmen des IT-bezogenen internen Kontrollsystems. Es gibt einen täglichen und einen monatlichen Ablauf. Anhand von Summary Reports können wir zunächst überblicken, ob Abweichungen vorliegen – falls ja, gehen wir in den Detail-Report." Beta 96 liefert der IT-Security-Abteilung automatisch Reports mit Abweichungen von den Control Procedures. So wird täglich eine Liste aller falschen Login-Versuche jedes der landesweit 3.500 Bank-Mitarbeiter erstellt. Die Audit Reports gehen an den Abteilungsleiter, der zusammen mit der IT-Abteilung diskutiert, was im Produktionsablauf geändert werden muss.

Durch dieses dynamische Auditing ist die 3BEG in der Lage, kritische Zustände und Ereignisse in ihren IT-Systemen sofort aufzudecken und eine kontinuierliche und dokumentierte Überwachung sicher zu stellen. Die Problembereiche wurden auch früher ausgewertet, doch lief dies größtenteils manuell ab. Durch die Automatisierung mit Beta 96 können sich die Administratoren heute anderen Aufgaben widmen. „Vor allem hatten wir früher nicht solch umfangreiche Compliance-Anforderungen zu erfüllen und mussten daraus resultierend auch nicht permanent bestimmte Control Procedures überprüfen", sagt Dipl.-Ing. Robert Fleischer. „Heute hingegen sind wir verpflichtet, uns regelmäßig mit der Audit-Erstellung zu befassen und können diesen gestiegenen Aufwand dank Beta 96 mit derselben Personaldecke bewältigen."

Veranstaltungen

Messen Kongresse

DatacenterDynamics Conferences 2009
Datacenter Dynamics Limited
06.08.2009, Seattle
www.datacenterdynamics.com

Sommerakademie
Datenschutzakademie in der Nordsee
Akademie Leck
31.08.2009, Kiel
www.nordsee-akademie.de

Seminare

IT-Sicherheit am Arbeitplatz - Awareness-Training
CBT Training & Consulting GmbH
27.07.2009, Hamburg, Köln
www.cbt-training.de

Risikoanalyse in der IT-Sicherheit
Integrata AG
27. - 28.07.2009, Hamburg
www.integrata.de

Der IT-Risikomanager
Management Circle AG
27. - 28.07.2009, Frankfurt a. Main
www.managementcircle.de

Security-Hacking-Training
Profindis GmbH
27. - 31.07.2009, Ettlingen/Karlsruhe
www.profindis.de

GSTOOL - das BSI Tool zum IT-Grundschutz
BSP. SECURITY
30. - 31.07.2009, Regensburg
www.bsp-security.de

Ausbildung zum geprüften, betrieblichen Datenschutzbeauftragten
Filges IT Beratung
03. - 07.08.2009, Oberhausen (Ruhrgebiet)
www.filges.de

Der Datenschutzbeauftragte
iKR GmbH
03. - 04.08.2009, Mannheim
www.ikr.de

VPN Virtual Private Networks
SMLAN – SoftwareTraining
10. - 11.08.2009, Berlin
www.smlan.de

Security Certification Seminar (SCS)
Lanworks AG
24. - 28.08.2009, Neuss
www.lanworks.de

Mobile Security
CAST e.V. Competence Center f. Applied Security Technology
27.08.2009, Darmstadt
www.castforum.de

Round-Table Storage
Synectico GmbH
27.08.2009, Krefeld
www.synectico.de

Datenschutz in medizinischen Einrichtungen
TÜV Rheinland Akademie GmbH
27. - 28.08.2009, Kaiserslautern
www.tuev-akademie.com

Haftungsrecht und IT-Sicherheit
Bechtle GmbH & Co. KG
31.08 - 01.09.2009, Dresden
www.bechtle.com