

April 18, 2005 || Informationsschutz mit biometrischen Verfahren:

Weit über die Sarbanes-Oxley-Gesetzgebung hinaus

Gemäß den Vorgaben der Sarbanes-Oxley-Gesetzgebung zum Thema Informationssicherheit müssen Unternehmen dokumentieren, welcher Anwender auf welche Daten zugreift. Mit biometrischen Verfahren lassen sich mögliche Sicherheitslücken beim Passwortschutz schließen.

Jüngsten Berichten zufolge verzögern viele Unternehmen die Veröffentlichung ihres Geschäftsberichts oder versuchen trickreich die Anforderungen der Sarbanes-Oxley-Gesetzgebung (Sarbanes-Oxley Act, SOA) zu erfüllen. Doch damit werden die Unternehmen langfristig wohl nicht das Vertrauen der Anleger zurückgewinnen. Besser wäre es, das Kontrollmanagement und die Corporate Governance tatsächlich zu verbessern.

SOA fordert unter anderem eine Dokumentation des Kenntnisstands von CEO und CFO über finanztechnische Fragen rund um das Unternehmen. In Gerichtsverfahren werden hierfür in jüngerer Zeit sogar E- und Voice-Mails als Beweismittel herangezogen. SAP hat umgehend auf SOA reagiert und zusätzliche Funktionen für ihre Kunden in über 18.000 Unternehmen entwickelt. SAP Compliance Management for SOA ist in SAP R/3 integriert. Mit der Entscheidung für eine integrierte betriebswirtschaftliche Standardsoftware lassen sich Prozesse optimieren und Kosten senken. In punkto Informationssicherheit muss jedoch noch einiges über solche Standardprozesse hinaus getan werden.

Wissenschaftler der California State University Fullerton (CSUF) forschen an biometrischen Verfahren. Hierfür dient die bioLock-Lösung, die die realtime AG für SAP R/3 entwickelt hat, als Grundlage. Im März 2005 stellten Vijay Karan, Curtis Williams und Malini Krishnamurthi von der CSUF mit Thomas Neudenberger von realtime North America das bioLock-Forschungsprojekts am SAP Curriculum Congress 2005 in Atlanta, Georgia, vor. Professoren anderer Universitäten, die an der SAP University Alliance teilnehmen, haben ebenfalls Interesse an biometrischen Forschungen signalisiert.

Die Forscher der CSUF haben herausgefunden, dass SOA meist phasenweise eingeführt wird. Für den Funktionsumfang der SAP-Lösung sind in Hinblick auf die Sarbanes-Oxley-Gesetzgebung vor allem die Abschnitte 301, 302, 401, 404 und 409 von Bedeutung. Gemäß Abschnitt 301 des SOA lassen sich via SAP Whistle Blower anonymisierte E-Mails an den Prüfungsausschuss der Aktiengesellschaften verschicken. Abschnitt 302 des SOA fordert Kontrollmöglichkeiten in Hinblick auf das Berichtswesen, insbesondere den Finanzbericht. Hierzu dienen die Lösungen Management of Internal Controls (MIC), Audit Information System (AIS), SAP Business Information Warehouse (SAP BW) und SAP Strategic Enterprise Management (SAP SEM). Wie in Abschnitt 401 gefordert lassen sich alle durch Wirtschaftsprüfer vorgenommenen Korrekturen in den Finanzberichten darstellen. Externe Wirtschaftsprüfer sind Abschnitt 404 entsprechend in der Lage, komplexe interne Kontrollsysteme zu evaluieren. Künftig müssen zudem Vorfälle, die die Wertentwicklung eines Unternehmens beeinflussen, als Ad-hoc-Meldungen innerhalb von 48 Stunden veröffentlicht werden.

Viele Wege führen zum Passwort

Während Firewalls Eindringlinge davon abhalten sollen, Daten zu stehlen oder zu zerstören, verfolgt SOA im Hinblick auf Informationssicherheit andere Ziele. Passwörter allein bieten hierbei keine Sicherheit: Forscher haben über 20 verschiedene Wege ermittelt, um an das Passwort eines SAP-Anwenders zu gelangen. Der einfachste Weg ist, unter der Tastatur nachzuschauen und das dort notierte Passwort abzulesen. Aber auch freche Reset-Anfragen oder Ausspäh-Versuche wie Passwort-Sniffer und Passwort-Cracker zählen zum Standard-Repertoire. Hilft all das nichts, muss man seinem Kollegen eben einmal über die Schulter schauen. CEOs und CFOs, die für Jahresabschlüsse verantwortlich zeichnen, brauchen jedoch die Sicherheit, dass niemand in der Lage war, unzulässige Änderungen vorzunehmen.

Das bioLock-System der realtime AG geht deshalb über einen reinen Passwortschutz hinaus. Es bietet etwa die Möglichkeit, auf Ebene der Geschäfts- und Finanzleitung zu dokumentieren, wann welche Daten in SAP R/3 aufgerufen oder verändert wurden. Auch Anwender aus dem Personal- und Finanzwesen, der Entwicklung, dem Verkauf und dem Einkauf sollten via bioLock identifiziert werden. Auf diese Weise sind Wirtschaftsprüfer wie im SOA gefordert in der Lage zu prüfen, wer wann welche Aktionen in der SAP-Software ausgeführt hat. Alle Aktivitäten werden aufgezeichnet und in internen bioLock-Protokolldateien gespeichert. Diese Protokolldatei lässt sich nach Anwendern, Zugangsverweigerungen oder Aktivitäten filtern, sortieren und in verschiedenen Formaten exportieren.

Fallbeispiele

Ein Angestellter des Brevard Countys in Florida hatte sich das Passwort eines Kollegen verschafft und machte in dessen Namen vertrauliche Informationen im Unternehmen publik. Der Angestellte erhielt eine Klage, für den Brevard County hagelte es Negativ-Schlagzeilen. Für die Einführung des Fingerabdruck-Identifikationssystems erhielt der County im November 2003 den angesehenen „InfoWorld 100 Award“ für den Schutz und die Überwachung von Zugriffen nach SAP R/3.

Aus Rache hatte ein ehemaliger Angestellter der Bekleidungsfirma American Eagle Outfitters Passwörter und Anwendernamen von Kollegen sowie eine Anleitung zum Eindringen in das Netzwerk in Hacker-Chaträumen verbreitet. Die daraus resultierenden Angriffe führten zu gravierenden finanziellen Schäden im Weihnachtsgeschäft. Der ehemalige Mitarbeiter wurde identifiziert und wegen Handels mit Passwörtern und Computerkriminalität zu 18 Monaten Haft

verurteilt.

Die Beispiele zeigen, wie leicht verärgerte Angestellte oder ehemalige Mitarbeiter Schäden in Höhe von mehreren Milliarden Dollar verursachen können. Wer nicht frühzeitig in Informationssicherheit investiert, hat vielleicht das Nachsehen.

Neue Technologie, neue Anwendungsfelder

Informationssicherheit muss ständig neu erkämpft werden. Dazu dienen neu entwickelte Technologien, wie etwa Tastaturen mit Smart Cards von Cherry Electrical Products. Vor allem die Kombination von Biometrie und Smart Cards sorgt für ein wirkungsvolles Identitätsmanagement. Alle bioLock-Funktionen lassen sich sowohl mit Biometrie oder Smart Cards als auch mit beiden Verfahren schützen. Bei kritischen Funktionen wie Überweisungen oder der Anwender-Verwaltung kann das System sogar die Identifizierung von zwei Personen verlangen – vergleichbar mit zwei Unterschriften auf einem Scheck. Kombination wie Biometrie und Smart Cards finden beispielsweise auch bei der inneren Sicherheit, der Verbrechensbekämpfung oder der Strafverfolgung Verwendung.

Zu den viel versprechenden Verfahren, Informationssicherheit zu verbessern, zählen etwa Biometrie, Agenten-Technologie und Radio Frequency Identification (RFID). SAP Research, die Forschungseinrichtung der SAP, entwickelt hierzu die notwendige Infrastruktur. So lassen sich beispielsweise biometrische Verfahren hervorragend in die SAP Auto-ID Infrastructure integrieren. Forschungsschwerpunkte wie an der California State University Fullerton ergänzen diese Entwicklungsarbeit. In der Praxis müssen Unternehmensführungen, IT-Leiter und die Gesetzgebung lernen, sich dieser Technologien zu bedienen und deren Gebrauch fördern, um Bedrohungen im Bereich Informationssicherheit wirkungsvoll zu begegnen.

Artikel

Autoren



Prof. Paul Sheldon Foote