



von Brigitte Kasper

**G**egen Datenmissbrauch oder Datenklau ist niemand gefeit. Umso erstaunlicher ist, dass laut einer aktuellen Studie von Brocade, zu der europäische IT-Entscheidungsträger befragt wurden, in nur rund 50 Prozent der Fälle die nötigen Sicherheitsmaßnahmen durch Management und IT-Abteilungen eingehalten wurden. Überdies sind in 80 Prozent der Datenzentren keine Technologien zur Datenverschlüsselung im Einsatz. Einzige Ausnahme bilden laut Studie diejenigen Unternehmen, bei denen die Einhaltung der Vorschriften durch das Top-Management oder aufgrund

verbindlicher Compliance-Vorschriften gefordert wird. Auf Nummer Sicher gehen zum Beispiel Unternehmen, die für eine umfassende Sicherheit einen ganzheitlichen GRC-Ansatz (Governance, Risk Management, Compliance) verfolgen. Hierzu bietet die econet AG einen vierstufigen Lösungsansatz, bei dem nach dem Audit der bestehenden Berechtigungsstrukturen zunächst ein sauberes Datei- und Rechtestruktursystem erstellt, danach ein sicheres File-service-Management und schließlich ein Identity und Service Management implementiert werden. Beispielsweise hat das Amt

für Informationsverarbeitung der Stadtverwaltung Köln die IT-Prozesse auf Basis der econet-Lösung so standardisiert, dass sämtliche Änderungen mit Hilfe von über 200 definierten Regeln automatisch in den zehn Zielsystemen umgesetzt werden. Das Ergebnis: Die Durchlaufzeiten für Änderungsaufträge konnten von vier Stunden auf 15 Minuten verkürzt sowie die Missbrauchs- und Angriffsmöglichkeiten reduziert werden. Weiterer Vorteil: die revisionsichere Protokollierung aller Prozesse.

Unternehmen, die sich mit dem Gedanken der Implementierung einer Identity- ▶

# Der Feind im Netzwerk

**DATENSCHUTZ** Auf Nummer sicher im Unternehmen gehen – Gefahr erkannt, Gefahr gebannt.

## SOFTWARE



**SENSIBILISIERUNG** „Die Gefahren im Internet sowohl in Quantität als auch in Qualität nehmen zu“, warnt Dr. Udo Helmbrecht, Präsident des BSI.

▶ Management-Lösung tragen, unterstützt die xTigo AG mit einer Matrix zur Analyse des Handlungsbedarfs. Dazu erhalten sie einerseits aktuelle Informationen darüber, welche Probleme sie bei der Verwaltung von Identitäten und Benutzerrechten überwinden müssen. Andererseits werden die An-

forderungen an eine effiziente Benutzerverwaltung ausführlich beschrieben sowie zusätzliche Hilfestellungen für eine Analyse des individuellen Handlungsbedarfs im jeweiligen Unternehmen gegeben.

Anregungen für die Network Access Control (NAC) kann man sich auch vom Best Practice Guide holen, den Enterasys Networks Interessenten zum Download zur Verfügung stellt. Er geht – herstellerunabhängig – auf die verschiedenen Phasen der Implementierung der Technologie ein, stellt die unterschiedlichen Ansätze vor und weist auf die regulatorischen Vorgaben (Compliance) hin. „Sicherheit muss an allen Standorten im Unternehmen sowie für alle Nutzer außerhalb des Unternehmens gewährleistet werden, die bei ihrer Arbeit extern auf die Systeme zugreifen“, hebt auch Dr. Anton Grashion, Security Strategist bei Juniper Networks, hervor.

**MIT DER ZAHL** der in ein Unternehmensnetzwerk eingebundenen Geräte, insbesondere der mobilen, sowie der Installation drahtloser Netze steigen die Anforderungen, die an die IT- und Datensicherheit sowohl bei

der Nutzung als auch bei der Übertragung der Daten gestellt werden. Unternehmen, für die der Schutz geschäftlicher Dokumente von grundsätzlicher Bedeutung ist und die gesetzlichen Datenschutzanforderungen unterliegen, ermöglicht die webbasierte Secure-Data-Exchange-Lösung FileBox der Compass Security AG den komfortablen und sicheren Dokumentenaustausch über das Internet. Benötigt werden hierzu ein Mobiltelefon und ein PC mit Webbrowser, authentifiziert wird per SMS. Der Nutzer kann die Dokumente über das Internet in verschiedene FileBoxen hochladen und jedem Kommunikationspartner individuelle Zugriffsrechte erteilen.