

Tipps gegen Sicherheitsbedrohungen von innen

Gerhard Beeker (CA Deutschland GmbH)

Externe Sicherheitsgefahren sind hinlänglich bekannt. Über interne Sicherheitslücken und Sicherheitsbedrohungen durch Mitarbeiter, ehemalige Mitarbeitern und Beauftragte wird jedoch nur selten berichtet. Doch Angriffe von Internen nehmen immer mehr zu und sind durch den besseren Zugriff auf kritische und nützliche Informationen kostspieliger als Angriffe von außen. Festzuhalten ist:

- US-Behörden haben herausgefunden, dass durch externe Angriffe Kosten in Höhe von 56.000 US-Dollar, bei internen von zwei Millionen US-Dollar entstehen. (Quelle: US National Reconnaissance Office)
- 72 Prozent aller Unternehmen schätzen interne Sicherheitsbedrohungen genauso schwerwiegend ein wie externe. (The InfoPro's Information Security Study, 2006)
- Unternehmen sehen die Befolgung von Sicherheitsrichtlinien durch Mitarbeiter an zweiter Stelle der anstehenden Herausforderungen in den nächsten zwölf Monaten.

Wie können Unternehmen also dieser kostenspieligen und wachsenden Sicherheitsbedrohungen Herr werden? CA hat die wichtigsten Tipps für Sie zusammengestellt.

1. Richten Sie Sicherheitsrichtlinien für Dokumente und Prozesse ein und setzen sie diese automatisiert um. Nur so

sehen Sie, wie die Prozesse funktionieren und können Sie später weiterentwickeln.

2. Stellen Sie in Absprache mit Ihrer Personalabteilung sicher, dass „alte“ Nutzerkonten sofort gesperrt und gelöscht werden. Mitarbeiter und Beauftragte sollten keinen Zugriff auf interne Informationen mehr erhalten, sobald sie das Unternehmen verlassen.
3. Überprüfen Sie quartalsweise die Zugriffsrechte. Der automatische Ablauf der Nutzungsrechte vereinfacht es, die wechselnden Verantwortlichkeiten und Nutzungsrechte entsprechend umzusetzen.
4. Gewährleisten Sie, dass die Mitarbeiter in den Sicherheitsrichtlinien geschult werden und sich der Auswirkungen der Nichtbefolgung bewusst sind. Passwörter sollten beispielsweise nie notiert, noch gemeinsam genutzt werden.
5. Räumen Sie den Nutzern im Rahmen ihrer Tätigkeit so wenig Rechte wie nötig ein. Finanz- und Kundeninformationen sollten beispielsweise nur wenigen zugänglich sein. Diese Rechte müssen regelmäßig überprüft werden und an die Funktionen und Arbeitstätigkeiten angepasst werden.
6. Setzen Sie Regelungen für wirksame Passwörter ein. Leicht zu erratende Passwörter sollten vermieden werden und wenn möglich, strengere Formen der Authentifizierung wie etwa Token oder Smartcards zum Zug kommen.

7. Lassen Sie niemals gemeinschaftliche Administrator-Passwörter zu. Nur einzelne dürfen Administratorrechte für bestimmte Systeme erhalten. Wechselt oder verlässt der Systemadministrator das Unternehmen muss das Konto sofort gesperrt werden.
8. Führen Sie eine gegenseitige Kontrolle über Berechtigungen für das IT-System ein. Trennen Sie die Zuständigkeiten für die Sicherheitsrichtlinien. Derjenige, der Änderungen genehmigt, sollte diese beispielsweise nicht im System umsetzen dürfen.
9. Ihr Sicherheitssystem sollte prüfbar sein. Im Problemfall können Sie so über das Protokoll ersehen, wer ihr System gefährdet. Protokollieren Sie alle administrativen Änderungen und bewahren Sie diese so auf, dass Systemadministratoren sie nicht ändern können.
10. Richten Sie einen einzigen und zentralen Blick auf den Status ihres Sicherheitssystems ein. Manchmal sind Sicherheitsprobleme nicht ohne die gegenseitige Abhängigkeit der vielfachen Systeme ersichtbar.
11. Belasten Sie Ihre Nutzer nicht unnötig mit komplexen Sicherheitsverfahren. Weder mehrere Dutzend Passwörter noch permanente Änderungen der Passwörter sind nötig. So verleiten Sie die Mitarbeiter, Sicherheitsverfahren zu umgehen.