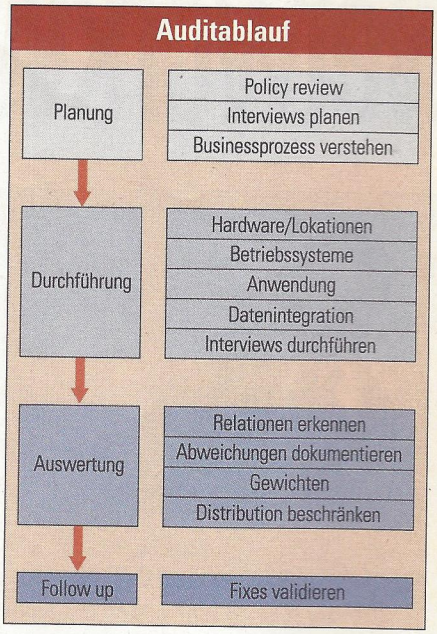
Schwachstellen identifizieren

Das Thema IT-Sicherheit ist momentan in aller Munde. Doch es reicht nicht aus, nur Sicherheitstechnologien einzukaufen. Mit internen Sicherheits-Audits können Unternehmen IT-Systeme und Prozesse prüfen und die Risiken minimieren.

FELIX LINDNER, ANTON KASKA



Umfassende Sicherheit benötigt verbindliche Richtlinien und eine entsprechende Bewusstseinsbildung bei den Mitarbeitern. Computersysteme und Netzwerke, die in Geschäftsprozesse eingebunden sind, bergen viele Risiken: Unerlaubter Zugriff auf vertrauliche Daten, Missbrauch von Computersystemen und fehlerhafte Berechnungen sind nur einige davon. Ein internes Sicherheits-Audit informiert das Management über Qualität sowie mögliche Probleme und macht Verbesserungsvorschläge. Es umfasst im Wesentlichen vier Schritte: Planung, Untersuchung und Bewertung, Ergebnis-Report, Follow-up.

Zunächst legt der Auftraggeber, in der Regel das Management, den Leistungsumfang (Scope) der Untersuchung fest. Er beschreibt, was auditiert werden soll. Mögliche Scopes sind das Evaluieren der Plattform einer Applikation oder der System- und Applikationssicherheit. Auch die Integrität von Schnittstellen und der Betrieb einer Applikation lassen sich durch ein Audit überprüfen. Danach wählt der Auftraggeber einen geeigneten Auditor, der möglichst nicht aus der Systemadministration kommt.

Dieser Auditor sollte einen Teil des Audits auf die Anwendungssicherheit legen und prüfen, ob nur berechtigte Personen Zugriff auf die Daten haben. Im nächsten Schritt trägt er alle relevanten Informationen zusammen. Dazu gehören die Sicherheitsrichtlinien für Betriebssysteme und Anwendungen, Namen von beispielhaften Nutzern sowie Organisationsdiagramme zur Dokumentation von Relationen. Der Prüfer muss sich zudem die schriftliche Genehmigung für den Test der Applikationen bei den Verantwortlichen einholen und ihnen den Zeitraum sowie mögliche Konsequenzen der Sicherheitsprüfung mitteilen. Schließlich informiert er sich über sicherheitsrelevante Log-Daten und liest Reports früherer Audits.

Die Sicherheitsrichtlinien – sowie die »system hardening procedure« für das Betriebssystem und der »installation guide« für die Applikation – haben dabei absolute Priorität. Existieren noch keine, kann das Unternehmen beispielsweise auf Basis von Dokumenten des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi.de) Richtlinien entwickeln. Dieser Schritt ist zwingend erforderlich, da sonst dem Audit jede Grundlage fehlt.

Untersuchen und bewerten

Was genau untersucht wird, hängt vom definierten Scope ab. Am Anfang stehen aber immer die Geschäftsprozesse; es folgen Hardware, Standort und Betriebssystem. Das Prüfen der Applikationen rundet den Audit-Prozess ab. Ein wichtiges Instrument ist das Befragen von System-Nutzern und -Administratoren. Außerdem verfolgt der Auditor eine bestimmte Transaktion im System durch alle Stadien und vergleicht in dieser Phase bereits Datenproben mit den Sicherheitsrichtlinien im Unternehmen. Dazu muss er den Geschäftsablauf kennen, den die Anwen-

CHECKLISTE INTERNE SICHERHEITSAUDITS

Wichtige Fragen für ein klassisches Sicherheits-Audit:

- Können nur berechtigte Personen auf die Daten zugreifen?
- Sind alle Berechtigungen nach dem Prinzip "zwingend benötigt" vergeben?
- Entsprechen Betriebssystem, Hardware und Standort den Sicherheitsbedürfnissen?
- Können Dritte die Verfügbarkeit und Zuverlässigkeit beeinflussen?

Beim Prüfen von Anwendungen sind folgende Punkte zu beachten:

- Administrationsrichtlinien für diese Anwendung
- Ist das Ändern von Konten in den Richtlinien abgedeckt?
- Umsetzung von Richtlinien in der Konfiguration
- Kontrolle der Funktionen (Menüs, Kommandos et cetera) auf Notwendigkeit
- Benutzerkonten müssen momentan Angestellte des Unternehmens sein
- Gehören alle privilegierten Konten natürlichen Personen und sind diese entsprechend informiert?
- Sind Anwendungs-Logs vorhanden?
- Werden nur unterstützte Benutzerschnittstellen verwendet?

dung unterstützt, die Art der Informationen, die das System verarbeitet, die Anzahl der Nutzer sowie die Art der übertragenen Daten.

Beim internen Sicherheits-Audit muss das Unternehmen besonderes Augenmerk auf die generelle Kompatibilität von Hardware und Software legen. Das gilt auch für die Peripherie. Der Auditor identifiziert Risikoquellen und prüft die Verfügbarkeit der Hardware. Auch die Umgebung, in der sich das System befindet, sollte er hinterfragen. Gerade Klimaanlagen oder eine nicht geprüfte unterbrechungsfreie Stromversorgung führen oft zu unangenehmen Überraschungen.

Nachdem die physische Umgebung der kritischen Elemente untersucht ist, beschäftigt sich der Auditor mit Netzwerkkomponenten und dem Betriebssystem. Benutzt das Unternehmen keine kryptographischen Protokolle, muss der Auditor die einzelnen Netzwerkkomponenten besonders gründlich testen: Kein Nutzer oder Administrator darf die Datenwege beeinflussen können, um an die Daten anderer zu gelangen.

Beim Betriebssystem spielen die Log-Daten eine entscheidende Rolle. In ihnen müssen alle sicherheitsrelevanten Informationen gespeichert sein. Sie können bei einem Hacker-Angriff von außen oder innen als Beweismittel vor Gericht dienen. Das Unternehmen muss sie deshalb besonders gut vor unzulässigen Zugriffen schützen.

Prozessabläufe sichern

Sind Hardware, Software und Umgebung getestet, gilt es die Anwendung selbst auf Sicherheitslücken zu überprüfen. Dabei muss der Auditor die »Notwendigkeit zur Erfüllung der Aufgaben« als Grundprinzip voraussetzen. Es besagt, dass Mitarbeiter ausschließlich auf die Daten zugreifen können, die sie zum Erfüllen ihrer Aufgaben benötigen. Einen weiteren Sicherheitsfaktor stellt die Verfügbarkeit einer Anwendung dar. Nicht verfügbare Applikationen stören Prozessabläufe und führen oft zu direkten finanziellen Verlusten.

Zu guter Letzt steht das Management der Applikation auf dem Programm. Fehlererhebungs-, Operations-, und Disaster-Recovery-Prozeduren müssen den einzelnen Teilorganisationen im Unternehmen bereit gestellt werden. System-Backup, Anwender-Support und Pflege der technischen Dokumentation runden die Liste der Funktionen ab, die der Auftraggeber im Rahmen des internen Sicherheitsaudits prüfen lassen sollte.

Reportage ohne Kopie

Am Ende des internen Sicherheits-Audits steht der Report. Er enthält alle Informationen und Ergebnisse, die der Auditor gesammelt hat und sollte sich in seiner Struktur an der Vorgehensweise orientieren. Nach Abteilung oder Verantwortlichen lässt sich dieser Report kaum gliedern. Der einzig legitime Empfänger dieses Dokuments ist der Auftraggeber. Der Auditor darf den am Audit beteiligten Personen auf keinen Fall eine Kopie aushändigen. Nach größeren Untersuchungen sollte er für das Management in einer Präsentation die wichtigsten Ergebnisse zusammenfassen.

ZUR PERSON

FELIX LINDNER
und
ANTON KASKA
sind Security Consultants bei n.runs in Oberursel.