

HELPDESK

So gleisen Sie Security Audits effizient auf

Unsere Geschäftsleitung fordert die erstmalige Durchführung einer Sicherheitsüberprüfung der IT-Infrastruktur. Welche Testtypen sind dabei für welche Anforderungen geeignet?

Sicherheitsüberprüfungen lassen sich grob in zwei Gruppen gliedern: Erstens die Checklisten-basierten, sogenannten «konzeptionellen» Security Audits, zweitens die «explorativen» Security Audits.

In die erste Kategorie fallen alle ISO/IEC 27001-orientierten Audits. Hierbei wird anhand strukturierter Interviews und ausgewählter Stichproben das Sicherheitsniveau erhoben. So können die möglichen, respektive geforderten Verbesserungsmaßnahmen eruiert werden. Fokussiert werden dabei neben technischen vor allem auch organisatorische und juristische Aspekte.

Bei explorativen Sicherheitstests wird hingegen mit geeigneten Tools (Programmen) und Techniken mehr oder weniger systematisch nach Sicherheitslücken gesucht. Dabei werden allerdings, im Sinn einer Momentaufnahme, überwiegend technische Aspekte beleuchtet und hauptsächlich Konfigurations-

mängel und mangelhafte Patchlevel aufgedeckt. Die so gewonnenen Informationen lassen daher höchstens indirekte Schlüsse auf die effektiv «gelebte» Sicherheitsorganisation zu.

Kein Audit ist allumfassend

Beide Audit-Typen haben Vor- und Nachteile. So hängt beim Interview-basierten Audit die Qualität der Erhebung direkt vom Wahrheitsgehalt der Ant-

«Es empfiehlt sich, Checklisten-basierte und explorative Security Audits clever zu kombinieren.»

worten der Interviewpartner ab. Zumal meist die Zeit fehlt, die Antworten zu verifizieren. Andererseits werden damit, sofern die Interviewfragen einem anerkannten Standard entsprechend formuliert und strukturiert sind, alle relevanten Bereiche abgedeckt. Damit eignet sich ein solches Audit, um den ersten Schritt in Richtung Zer-



ILLUSTRATION: COWTHU

tifizierung zu machen. Ein Qualitätsmerkmal, selbst wenn diese Option nicht eingelöst wird.

Explorative Audits, wie etwa Penetration Tests, bergen ebenfalls Fallstricke: Ist der Zeitrahmen zu eng, können Tests nicht seriös durchgeführt werden. Oder es mangelt den Testern am nötigen Fachwissen. Häufig werden auch – um Zeit oder Geld zu sparen – nicht alle Systeme untersucht. Oder der Ansatz ist eher chaotisch als methodisch.

Ein weiteres Problem ist die zu geringe Dokumentations-tiefe, welche die Nachvollziehbarkeit des Projekts, der Methode und vor allem der Ergebnisse vereitelt. Fatalerweise wird dies oft erst bei der nächsten IT-Revision erkannt.

Doch explorative Audits haben auch eine enorme Stärke: Ihre Resultate beruhen auf harten Fakten, lassen also weniger Raum für Fehlinterpretationen.

Audits sind zu kombinieren

Somit wird klar: Für die regelmässige Durchführung von Security-Überprüfungen sollten Checklisten-basierte und explorative Security Audits idealerweise kombiniert werden.

Mit einem verhältnismässig einfach möglichen, Checklisten-basierten Audit verschafft man sich einen Überblick («Big Picture») über das ungefähre Sicherheitsniveau der Organisation.

Geht es indes darum, klar abgegrenzte Objekte zu untersuchen (etwa die Systeme in der Demilitarisierten Zone (DMZ) oder im LAN) oder sollen Sicherheitslücken und Konfigurationsmängel einzelner Applikationen aufgespürt werden, kommen explorative Security Audits zum Zug.

Soll auch für deren Durchführung ein Standard angewendet werden, empfiehlt sich OSSTMM (Open Source Security Testing Methodology Manual). Dieser De-facto-Standard ist einerseits kompatibel zu den gängigen Normen, Gesetzen und Regularien. Andererseits erfreut sich das seit 2001 verfügbare, kostenlos einsetzbare OSSTMM stetig wachsender, internationaler Beliebtheit. So wird es etwa vom BSI (Deutsches Bundesamt für Sicherheit in der Informationstechnik) explizit für die Durchführung technischer Audits empfohlen. ■

 **Archiv aller Helpdeskartikel:**
www.computerworld.ch



Der Autor
Christoph Baumgartner ist CEO der Sicherheitsberaterin One Consult, Thalwil.
www.oneconsult.com

Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:

Haben Sie Fragen rund ums Thema IT-Sicherheit?

Schreiben Sie uns:
it-security@computerworld.ch