DuD
Datenschutz und Datensicherheit

Security Audits

Stefan Gora

Hintergrund

Kontrolle und Auditierung getroffener Sicherheitsmaßnahmen sind wichtige Bestandteile eines Sicherheitsmanagements, um eine Aussage über das erreichte Maß an Sicherheit treffen zu können. Dabei kann festgestellt werden, ob Maßnahmen nicht ausreichend wirksam sind oder fehlen.

Schritt 1: Festlegung des Audit-Gegenstands

Auch wenn die Fragestellung einfach anmutet, ist eine eindeutige Definition und Abgrenzung des Untersuchungsgegenstands oft gar nicht so einfach. Daher sollte im Detail der Gegenstand und auch der Umfang der Analysen bzw. im Umkehrschluss die Abgrenzung, was nicht untersucht werden soll, festgelegt werden.

Schritt 2: Dokumentation der Ziele des Audits

Die Ziele des Audits sollten zu Beginn dokumentiert und noch einmal kritisch überprüft werden. Geht es um eine Statusbestimmung oder einen Vergleich mit anderen Unternehmen und Institutionen? Wird mittel- oder langfristig eine Zertifizierung, z. B. nach IT-Grundschutz oder ISO 27001 angestrebt? Wer ist der Initiator des Audits und welcher Zielgruppe sollen die Ergebnisse präsentiert werden? Für wen sollen die Ergebnisse eine Entscheidungshilfe sein – und bei welcher Fragestellung?

Schritt 3: Methodik und Vorgehensweise

Soll eine reine Black-Box Analyse, d. h. eine technische Analyse (Penetrationstest) ohne Kenntnisse der Sicherheitsmechanismen aus Sicht eines internen oder externen Angreifers durchgeführt werden? Oder ist eine White-Box Analyse, d. h. ein Audit unter Mitwirkung der Systembetreiber in Form von Interviews und Konfigurations- und Architekturprüfungen, zielführender?

Grundsätzlich ist zu empfehlen, beide Methoden anzuwenden, da sie unterschiedliche Vorteile besitzen und sich gut ergänzen. Eine Black-Box Analyse beispielsweise besitzt nur Aussagekraft für den Zeitpunkt der Überprüfung; über Sicherheits-Prozesse wie Aktualisierung von Systemen, Monitoring und Alerting können damit keine oder nur begrenzt Aussagen getroffen werden. White-Box Analysen können andererseits aufwendig und umfangreich werden. Eine geeignete Mischung ermöglicht es, Ressourcen zu optimieren und effektiv Ergebnisse zu erzielen.

Schritt 4: Definition der Prüftiefe

Der für eine Analyse erforderliche Aufwand hängt maßgeblich von der Prüftiefe ab. Ein einfacher automatisierter Scan (Penetrationstest ohne manuelle Untersuchungen) auch von mehreren Dutzend Servergruppen kann inklusive Auswertung in wenigen Tagen durchgeführt werden. Aufwand entsteht hauptsächlich bei der Auswertung und Verifikation der Schwachstellen – und hängt damit im Wesentlichen von der Anzahl und Komplexität der festgestellten Schwachstellen ab.

Eine individuelle Analyse auch nur von einer Anwendung kann dagegen, abhängig von den gewählten Angreifermodellen und dem Umfang der gewählten Angriffsszenarien, durchaus Wochen erfordern.

Durch eine angemessene Prüftiefe sollte das für aussagekräftige Ergebnisse erforderliche Minimum an Ressourcen festgelegt werden. Durch sinnvolle Stichproben können andererseits Ressourcen eingespart werden.

Schritt 5: Festlegung des Audit-Zeitpunkts

Die Abstimmung geeigneter Zeitpunkte für die Durchführung eines Audits ist in Anbetracht gestiegener Verfügbarkeitsanforderungen und oftmals weltweitem Schichtbetrieb von Produktivsystemen insbesondere bei Penetrationstests sehr wichtig und häufig nicht einfach.

Schritt 6: Erstellung des Auditplans

Der Auditplan sollte mindestens die Details der Vorgehensweise, (Teil-) Aufgaben, eine Liste der Prüfungspunkte und den Terminplan beinhalten. Zusätzlich sollten auch geeignete Vorsichtsmaßnahmen zur Vermeidung/Verminderung von Störungen diskutiert und festgelegt werden.

Schritt 7: Durchführung des Audits

Details zur Durchführung für die Ansätze Black-Box, White-Box oder Audits auf Basis von Standards wie ISO 17799/27001 und IT-Grundschutz können [Gora_07] entnommen werden.

Schritt 8: Auswertung der Audit-Ergebnisse

Die Auswertung sollte eine Vergleichbarkeit der Ergebnisse und ggf. sogar ein Benchmarking ermöglichen. Sie sollte daher nachvollziehbar sein und sich an ggf. eigenen Standards orientieren.

Schritt 9: Dokumentation

Die Ergebnisse sollten aussagekräftig für die jeweilige Zielgruppe Technik/Organisation/Management aufbereitet werden.

Schritt 10: Ableitung von Maßnahmen

Bei der Ableitung von Maßnahmen aus den gefundenen Ergebnissen sollten nicht nur die vorhandenen, sondern auch bereits geplante Sicherheitsmaßnahmen berücksichtigt werden. Die mit den Verantwortlichen abgestimmten Maßnahmenvorschläge sollten priorisiert und um eine Kostenschätzung ergänzt werden, damit sie sich als Entscheidungsvorlage eignen.

Literatur

[Gora_07] Gora, Stefan: *Security Audits*. Secorvo White Paper, 17.01.2007. http://www.secorvo.de/whitepapers