

Security Audit

Unternehmensnetzwerke sind in den letzten Jahren gewachsen und mit Ihnen die Anforderungen an IT-Sicherheit und deren Lösungen. Wichtig ist, dass Sie immer den Status der IT-Security in Ihrem Unternehmen kennen und Sie sicherstellen können, dass die Vereinbarungen Ihrer Security Policy tatsächlich umgesetzt werden.

Diese Fragen beantwortet ein Security Audit.

Ziel ist ein dokumentierter Status des gelebten IT-Sicherheitsniveaus, das Aufspüren von Mängeln und Sicherheitslücken sowie die Beurteilung durch eine Überprüfung der bestehenden Sicherheitsmaßnahmen im technischen und organisatorischen Bereich. Neben einer Schwachstellenanalyse findet auch eine Bestätigung der IT-Sicherheit durch einen unabhängigen Dritten statt.

Bei einem Audit wird entweder der Ist-Zustand analysiert oder aber ein Vergleich der ursprünglichen Zielsetzung mit den tatsächlich erreichten Zielen ermittelt. Oft soll ein Audit auch dazu dienen, allgemeine Probleme oder einen Verbesserungsbedarf aufzuspüren.

Während der Ist-Analyse, die die Basis eines Audits darstellt, werden die Systemumgebung und die Schutzmaßnahmen erfasst. Diese Situation, die eventuellen Sicherheitslücken und Verbesserungsvorschläge werden dokumentiert. Anschließend wird es den Systemverantwortlichen und Administratoren präsentiert und das weitere Vorgehen mit ihnen diskutiert.

Audits haben eine Controlling-Funktion in Ihrem Unternehmen und dienen als Entscheidungsgrundlage für das weitere Vorgehen zur Verbesserung der IT-Security. Wir zeigen Ihnen, wo Handlungsbedarf besteht, damit Sie Ihre Investitionen zielgerichtet planen können.

>>>

BDG unterscheidet verschiedene Audittypen:

Netzwerkaudit

Bei dem Netzwerkaudit findet ein Scan über das Netzwerk statt. Ein Schwachstellenscan (Vulnerability Scan) findet in der Regel nur bekannte Schwachstellen. Bei einem Sicherheitsscan durch BDG werden die Testergebnisse des Schwachstellenscans durch eine manuelle Verifikation von Fehlalarmen (false positives) bereinigt, klassifiziert und priorisiert sowie konkrete Vorschläge zur Beseitigung von Schwachstellen gegeben.

Bei einem externen Netzwerkaudit wird eine Überprüfung "von außen" über das Internet durchgeführt. Gegenstand der Untersuchung sind die über das Internet erreichbaren Server und die mit ihnen in Verbindung stehenden Dienste. Der BDG-Sicherheitsberater erhält in der Regel – mit Ausnahme der Zieladresse – keine Informationen über die Systemumgebung (Black-Box).

Das interne Netzwerkaudit unterscheidet sich von der äußeren Untersuchung dadurch, dass dieser im Access Bereich (Firewallumgebung) beim Auftraggeber vor Ort stattfindet. Bei dieser Untersuchung werden die Systeme direkt in der DMZ oder im LAN überprüft, ein vorhandener Perimeterschutz wird dadurch umgangen. Dieser Test deckt Schwachstellen bei Systemen auf, die zum Beispiel durch den Schutz einer Firewall oder eines Intrusion Prevention Systems (IDP) nicht erkennbar wären, jedoch möglicherweise indirekt durch einen Angreifer oder Innentäter ausgenutzt werden könnten.

Systemaudit

Bei einem Systemaudit erfolgt die Überprüfung durch den direkten Zugriff auf ausgesuchte Systeme mit privilegierten Zugriffsrechten. Auf diese Weise können Schwachstellen aufgedeckt werden, die bei einer externen Überprüfung unbemerkt bleiben können. Der direkte Zugriff ist dann sinnvoll, wenn es sich um besonders kritische Systeme handelt.

Penetrationstest

Bei einem Penetrationstest versucht BDG mit entsprechenden Programmen oder Methoden in ein System einzudringen und dabei identifizierte Schwachstellen tatsächlich auszunutzen.

Webapplikation Audit

Webserver müssen von außen erreichbar sein und unterliegen somit erhöhten Sicherheitsanforderungen. Firewalls erlauben Zugriffe über HTTP und HTTPS und sind für applikationsspezifische Angriffe wie beispielsweise Cross Site Scripting oder SQL Injection „blind“. Oft stehen auch Funktionsaspekte im Design einer Web-Applikation im Vordergrund. Groß ist das Risiko, dass konzeptionelle und technische Sicherheitsanforderungen nicht konsequent umgesetzt werden oder Test-Stände in Produktion gehen.

Hauptaspekt des Webapplikation Audit ist das Aufspüren von Fehlern und Sicherheitslücken in einer Web-Anwendung selbst und eine Überprüfung des Webservers auf Betriebssystemebene. Die Schutzfunktion durch Sicherheitssysteme wie Firewalls, Web Application Gateways oder Intrusion Prevention Systeme wird in die Überprüfung mit einbezogen. Bei der Untersuchung werden statische und dynamische Prüfmethode angewendet.

Compliance-Audit

Sie haben neben betriebswirtschaftlichen Risiken eine Fülle von Gesetzen, Normen und Verordnungen zu beachten. Werden diese Anforderungen nicht ernst genommen, so ist eine persönliche Haftung Ihrer leitenden Mitarbeiter nicht auszuschließen.

Mit einem Soll-/Ist-Vergleich werden Abweichungen durch eine Delta-Analyse von allgemein anerkannten Sicherheitsregeln (BSI GSHB, ISO 27001, ISO 17799, etc.) erkannt und gegebenenfalls Vorschläge für eine Verbesserung unterbreitet. Neben einschlägigen Sicherheitsstandards in der IT können auch relevante Gesetze, wie zum Beispiel das Bundesdatenschutzgesetz (BDSG) und das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) oder Richtlinien wie Basel II und der Sarbanes-Oxley Act (SOA bzw. SOX) Gegenstand einer Untersuchung sein. Konkrete Maßnahmen oder Anforderungen zur Informationssicherheit werden in Gesetzen und Verordnungen in der Regel nicht eindeutig beschrieben. Sie sind daher in der Umsetzung mehr oder weniger auf sich selbst gestellt. Im Bereich der Technical Due Diligence werden von BDG relevante gesetzliche Verpflichtungen identifiziert und sinnvolle Maßnahmen abgeleitet.

Organisatorisches Audit

Dieses Audit überprüft, ob Sicherheitsrichtlinien vorhanden sind und eingehalten werden. Außerdem zeigt die Praxis, dass informelle Prozesse existieren, die nicht dokumentiert sind. Im Rahmen des organisatorischen Audits wird anhand eines standardisierten Interviews Ihr formales und gelebtes Sicherheitskonzept überprüft. Die Untersuchung erstreckt sich auch auf die Akzeptanz und Einhaltung Ihrer organisatorischen Sicherheitsvorgaben, Zuständigkeiten und Eskalationsverfahren.

Neben logischen und betrieblichen Schutzmaßnahmen können auch physische Maßnahmen in der IT berücksichtigt werden. Die Prüfung erfolgt auf Grundlage Ihrer vorhandenen Dokumentation, durch Gespräche mit den beteiligten Verantwortlichen und anhand von Checklisten zur Überprüfung der Einhaltung von Standards und Gesetzen. Dieses Audit soll Ihrem Management dabei helfen, Stärken und Schwachpunkte des Sicherheitszustandes der IT zu erkennen. Es liefert eine Aussage darüber, ob die getroffenen Maßnahmen den Anforderungen, insbesondere auch im Hinblick auf gesetzliche und betriebliche Vorschriften, angemessen sind.