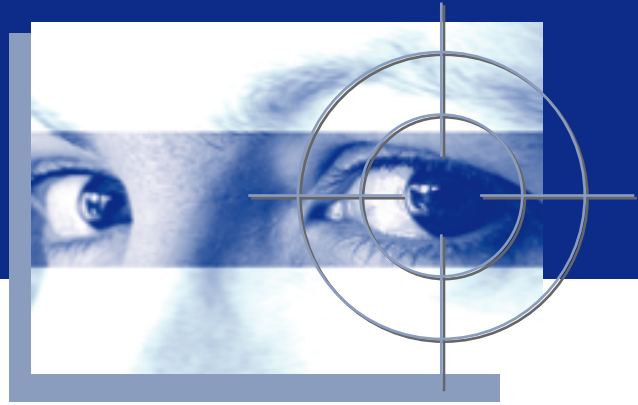


IT Security Audits



IT Security Audits

Networkers ist eines der in Deutschland führenden Unternehmen für die Planung, den Aufbau und den Betrieb von sicheren und leistungsfähigen Applikations- und Netzwerkinfrastrukturen. Unternehmen und Organisationen bieten wir ein breites Spektrum an Services - zuverlässig, kompetent und herstellerneutral.



Warum IT Security?

Falsche oder nicht ausreichende IT Security ist nicht nur ein existenzbedrohendes Wettbewerbsrisiko, sondern kann unter Umständen auch finanzielle wie strafrechtliche Haftungsrisiken nach sich ziehen - bis hin zur persönlichen Haftung von Vorstand oder Geschäftsführung.

Insbesondere deshalb kommt es für Unternehmen und Organisationen entscheidend darauf an, geeignete und angemessene Präventivmaßnahmen zu ergreifen, um die *Verfügbarkeit*, *Vertraulichkeit* und *Integrität* von Daten in einem sinnvoll definierten Umfang gewährleisten zu können.



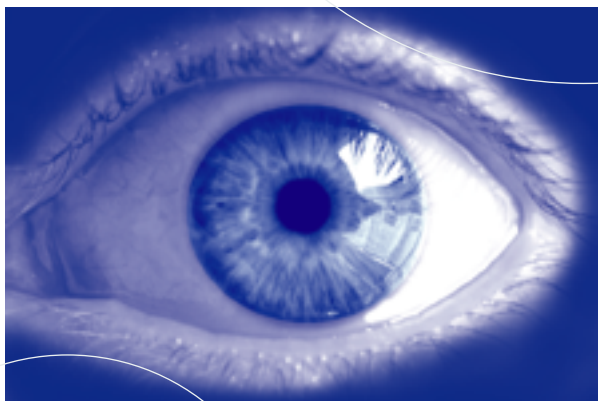
IT Security Audits

Vertrauen ist gut - Kontrolle ist besser: IT Security Audits

Ein heute als sicher geltendes System kann schon morgen gravierende Sicherheitslücken aufweisen. Die Praxis zeigt:

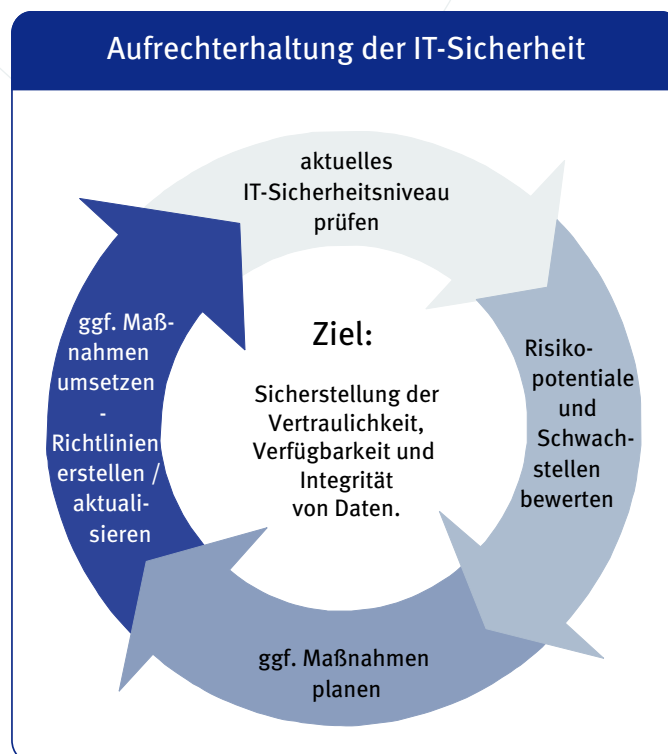
- IT- Systeme werden ständig komplexer. Damit steigt die Wahrscheinlichkeit, die Systeme nicht mehr bis ins Detail zu beherrschen.
- Immer mehr Komponenten innerhalb von IT-Infrastrukturen sind nicht ausreichend sicher konfiguriert.
- Das Wissen und die Möglichkeiten potentieller Angreifer wachsen stetig.
- Immer neue Schwachstellen werden bekannt. Attacken erfolgen in der Regel umgehend.

Nachhaltige IT Security erfordert daher periodische Überprüfungen in Form von IT Security Audits. So können Sicherheitslücken gefunden und abgestellt werden, bevor andere diese ausnutzen.



IT Security Audits: Ziele

Das Ziel von IT Security Audits geht über die Entdeckung von Schwachstellen und Sicherheitslücken weit hinaus. IT Security Audits stellen eine Bestandsaufnahme des gegenwärtigen IT-Sicherheitsniveaus dar. Deshalb beschränken sich IT Security Audits nicht isoliert auf die Aufdeckung von technisch bedingten Risiken: Sie beziehen darüber hinaus auch organisatorische, personelle und infrastrukturelle Aspekte mit ein, durch deren Betrachtung Defizite des Betriebskonzeptes erkannt werden können. Eine Bewertung der Ergebnisse kann gegen ein angestrebtes Sicherheitskonzept (z. B. BSI, ISO 17799) oder auch gegen „Best Practice“ erfolgen.



IT Security Audits

IT Security Audits brauchen Methode

IT Security mit Nachhaltigkeitsgarantie verlangt immer konsequent methodisches Vorgehen. Das bezieht sich sowohl auf die Herleitung und Herstellung angemessener und ausreichender IT Security (z.B. nach den Empfehlungen des BSI oder nach der ISO-Norm 17799), sowie auch auf die periodischen Überprüfungen des IT-Sicherheitszustandes.

So sind die für die Überprüfung zur Verfügung stehenden Sicherheitsanalysen nicht etwa willkürlich einsetzbar: White Box Audits, Black Box Audits sowie Penetrationstests behandeln jeweils spezifische Schwerpunkte. Sie besitzen jedoch modularen Charakter, so dass sie je nach Zielsetzung der Sicherheitsüberprüfung untereinander kombiniert werden können.

IT Security Audits: Sinnvolle Kombinationen von Sicherheitsanalysen zur Überprüfung der IT Security



White Box Audit
Black Box Audit
Penetrationstest

	Komponententest	Komponententest + Systemtest	Komponententest + Beweisführung	Systemtest	Systemtest + Beweisführung	komplettes Audit
White Box Audit	X	X	X			X
Black Box Audit		X		X	X	X
Penetrationstest			X		X	X

White Box Audit

Komponentenanalyse mit dem Ziel, Schwachstellen zu identifizieren. Die Sicherheitsanalyse erfolgt auf Grundlage spezifischer Insiderinformationen, bei der aus Sicht eines internen Revisors detaillierte Überprüfungen von Zielsystemen vorgenommen werden. Dazu zählen z.B. Analysen von Topologiedaten, Produktdaten, Konfigurationsinformationen, Prozessen, Richtlinien, Sicherheitsmaßnahmen etc.



Black Box Audit

Systemanalyse mit dem Ziel, Schwachstellen zu identifizieren. Die Sicherheitsanalyse erfolgt in Form einer authentischen Ausspähung mit den Mitteln eines externen Angreifers, dem keine internen Informationen (Netzpläne, Konfigurationsdaten, etc.) zur Verfügung stehen. Dabei wird das Zusammenspiel eingesetzter Schutzmaßnahmen hinsichtlich ihrer Wirkung analysiert.



Penetrationstest

Zielt darauf ab, die Existenz identifizierter Schwachstellen nachzuweisen. Die Sicherheitsanalyse erfolgt in Form realer und gezielter Angriffe auf ausgewählte und zuvor mit dem Auftraggeber festgelegte Ziele.



IT Security Audits

IT Security Audits brauchen geeignete Werkzeuge

Zur Durchführung von IT Security Audits sind Diagnosetools (Scanner) unverzichtbar. Sie liefern wertvolle Ergebnisse und verschaffen auch arbeitsökonomische Vorteile. Doch Vorsicht: Diagnosetools verfügen über gravierende Unterschiede, z.B. im Hinblick auf:

- ihre Wirkungsprinzipien
- ihren technischen sowie thematischen Fokus
- ihre Qualität der Schwachstellenidentifizierung und -analyse

Zudem bieten sie definitiv keine allumfassende Lösung. Zur Durchführung effektiver IT Security Audits sind erfahrene Experten notwendig, um nicht nur sämtliche Schwachstellen aufzuspüren, sondern diese darüber hinaus auch bewerten und durch Empfehlungen geeigneter Gegenmaßnahmen effizient beseitigen zu können.

Scanner analysieren z.B. folgende sicherheitskritischen Aspekte

- Backdoor Programme (BackOrifice2000, Netbus, ...)
- Browser (Konfiguration, Java, JavaScript, ActiveX Checks, Cookies), Brute Force-Angriffe auf Passwörter
- Denial-of-Service Angriffe (DoS-Attacken)
- Protocol Spoofing Checks
- Web-Server-Tests (Check auf Sicherheitslücken in CGI Scripts und Web-Applikationen, Test auf Betriebssystem-Version und Bugs)
- Firewall Checks (Konfiguration, Denial of Service Tests)
- Windows NT Checks: Patches, Rechtevergabe im System, Registry-Einträge, Überprüfung von Accountinformationen, Passwörter, Dienste
- FTP, TFTP Checks: Anonymous FTP, FTP bugs enabled
- Network Device Checks (Router/ Switch)
- Email Checks (Check auf eingesetzte Mail- Systeme und potentielle Sicherheitsprobleme)
- RPC Checks, NFS Checks, NIS Checks, DNS Checks
- LDAP Checks
- X Windows Checks

IT Security Audits brauchen geeignete Werkzeuge: Beispiele

Networkers setzt je nach individuellen Anforderungen und Zielen von IT Security Audits unterschiedliche Tools und Werkzeuge nach dem "Best of Breed"-Prinzip ein. Neben Eigenentwicklungen zählen unter anderem folgende Tools und Werkzeuge zu unserem Standardportfolio:

Unterstützende Tools und Werkzeuge zur Durchführung von White Box Audits

- Für Logfile-Auswertungen: "Log Analyzer" und "Reporting Center" von Webtrends
- Für Regelsatzüberprüfungen: "eTrust Policy Compliance" von Computer Associates
- Für Richtlinienüberprüfungen von Betriebssystemen: "Hyena" (Shareware), "Intrust" / "Opalis" von Enterprise International

Unterstützende Tools und Werkzeuge zur Durchführung von Black Box Audits

- Für Port- und Vulnerability-Scans: "Internet Security Scanner" von ISS, "NetRecon" von Symantec sowie "Nessus", "SATAN", "SAINT", "SARA", jeweils Open Source sowie "BV-Control" von BindView und "Retina" von eEye
- Für reine Port-Analysen: "nmap", Open Source
- Für Datenbank-Analysen: "Internet Database-Scanner" von ISS
- Für CGI-Vulnerability-Analysen: "Nikto", "Stealth", jeweils Open Source

Unterstützende Tools und Werkzeuge zur Durchführung von Penetrationstests

- Diverse Hacker- und Angriffstools

IT Security Audits

IT Security Audits brauchen Kompetenz

Umfassendes Expertenwissen im gesamten Bereich der Netzwerk- und Systemtechnik ist eine der grundlegenden Voraussetzungen zur Durchführung von effektiven IT Security Audits. Einerseits ist tiefgehendes Verständnis im Bereich der Sicherung von IT-Infrastrukturen gefordert, andererseits auch tiefgehendes Verständnis über Mittel und Wege, welche IT-Schutzmaßnahmen wie ausgeschaltet bzw. umgangen werden können.

Angriff

- So muss etwa die gesamte Bandbreite der diversen Angriffstechniken perfekt beherrscht werden. Nur mit diesen Kenntnissen sind im Rahmen von Black Box Audits und Penetrationstests stichhaltige Ergebnisse zu erzielen, die realitätskonform und mit denen von versierten Hackern vergleichbar sind.
- Darüber hinaus sind detaillierte Kenntnisse z.B. in den Bereichen Betriebssysteme, Netzwerkkomponenten, Netzwerkprotokolle und Applikationen zwingend erforderlich. Nur mit diesem Know-how lassen sich Sicherheitslücken identifizieren und sachgemäß bewerten.

Verteidigung

- Zudem ist fundiertes Expertenwissen im gesamten Bereich der IT Security unerlässlich. IT Security Audits sind nur dann tatsächlich konstruktiv, wenn der Auditor nicht nur sämtliche IT-Sicherheitslücken identifiziert und bewertet, sondern darüber hinaus auch die exakt angemessenen und ausreichenden Lösungen empfehlen sowie wirkungsvoll umsetzen kann.

- *Virusscanning*
- *Malicious Code Blocking*
- *Content Filtering*
- *URL-Blocking*
- *Spam Prevention*
- *Public Key Infrastructure*
- *Authentifizierungen*
- *Verschlüsselungen*
- *Signaturen*
- *Zertifikate*
- *Firewalls*
- *Intrusion Detection*
- *Intrusion Prevention*
- *Virtual Private Networks*
- *Secure Remote Access*
- *Secure WLAN*
- *Secure Mobile Devices*
- *Hochverfügbare Systeme*
- *Hochverfügbare Anbindungen*
- *Sicherheitskonzepte*
- *Hochverfügbarkeitskonzepte*
- *White Box Audits*
- *Black Box Audits*
- *Penetrationstests*
- *Logfile Analysen*
- *Digitale Forensik*
- *Projektmanagement*
- *Schulungen / Workshops*
- *Service Level Agreements*
- *Open Source Support*

Networkers bietet professionelle IT Security Audits sowie zuverlässige Umsetzungen von Maßnahmen

Als Spezialist in den Bereichen Netzwerktechnik und Netzwerksicherheit analysiert und bewertet Networkers den aktuellen Stand Ihrer Informationssicherheit - zuverlässig, kompetent, herstellerneutral und kostengünstig.

In Ihrem Hause präsentieren wir Ihnen anschließend die ermittelten Stärken und Schwächen des Sicherheitszustandes ihrer IT-Infrastruktur. Zudem erhalten Sie eine umfangreiche Dokumentation über die aufgedeckten Risikopotentiale inklusive detaillierter Bewertungen. Darüber hinaus erhalten Sie zu jeder identifizierten Sicherheitslücke Empfehlungen konkreter Maßnahmen zur Beseitigung bzw. Minimierung der daraus resultierenden Bedrohungen.

Des Weiteren stehen wir Ihnen auch gerne bei der Umsetzung der Maßnahmen kompetent zur Seite. Selbstverständlich umfasst dies auch fokussierte Schulungen und Workshops für Ihre Mitarbeiter.

Service Level Agreements (SLA) für einen reibungslosen Betrieb Ihrer IT-Infrastruktur runden unser Portfolio ab.





Networkers AG
Bandstahlstraße 2
58093 Hagen

fon: 0 23 31 . 80 95 0
fax: 0 23 31 . 80 95 499

email: info@networkers.de
web: www.networkers.de