



# Audits und Penetrationstests

ISMS-LEAD-AUDITOREN  
ANGRIFFE  
AUDITS  
INTRUSION-PREVENTION  
SECURITY  
VERWUNDBARKEITSMANAGEMENT  
TRAININGS

SICHERHEITSMANAGEMENT  
SICHERHEITSMANAGEMENT  
SICHERHEITSMANAGEMENT  
WLAN  
COMPLIANCE-ANFORDERUNGEN

IT-GRUNDSCHEIT  
DATA LOSS PREVENTION  
PENETRATIONSTEST  
IT-FORENSIK  
MOBILE/WIRELESS SICHERHEIT  
SICHERHEIT SENSIBLER DATEN  
APPLIKATIONS-SICHERHEIT  
NETZWERKSICHERHEIT  
INTERNET SICHERHEIT  
GATEWAY  
ISO/IEC 27001  
DENIAL OF SERVICE PROTECTION  
QUARANTANE-NETZWERKE

# Professionelle Audits und Penetrationstests

## cirosec steht für professionelle Audits und Penetrationstests.

Sicherheit ist kein dauerhafter Zustand. Daher muss die Effektivität der Sicherheitsmaßnahmen und der Managementsysteme regelmäßig hinterfragt werden.

Sicherheit wird durch Änderungen in Abläufen, Anwendungen und an Komponenten wie Firewalls, durch die Inbetriebnahme neuer Dienste sowie durch immer wieder neu entstehende Bedrohungen stets infrage gestellt.

Wir beraten Sie, wie Sie Ihre IT- und Informationssicherheit effektiv und effizient überprüfen und hinterfragen können.

Durch die Fokussierung auf Sicherheitsüberprüfungen und aufgrund der Größe unseres Prüferteams, der Erfahrung und Kompetenz der einzelnen Prüfer sowie der kontinuierlichen Verbesserung unserer Prüfmethoden und Werkzeuge gewährleisten wir Ihnen eine erfolgreiche und professionelle Durchführung.

Mit unseren zielgruppenspezifischen und hochwertigen Auditberichten sowie unseren internen Qualitätssicherungs- und Qualitätsmanagementprozessen bieten wir Ihnen Audits auf höchstem Niveau.

# UNSERE LEISTUNGEN IM ÜBERBLICK



Neben detaillierten Kenntnissen der aktuellen Angriffstechniken und -methoden verfügen wir über langjährige Erfahrung im Bereich von Audits und Penetrationstests. Dadurch ist es uns möglich, Ihre IT-Lösungen nicht nur auf der konzeptionellen Ebene auf potenzielle Sicherheitsrisiken hin zu untersuchen: Wir finden und bewerten auch tatsächlich vorhandene technische und organisatorische Schwachstellen.

Sicherheitsüberprüfungen sind ein sehr individuelles Thema, für das es keine Universalrezepte gibt. Deshalb müssen vor jeder Sicherheitsüberprüfung der Rahmen und der Fokus der Untersuchung abgestimmt werden.

Wir beraten Sie bereits im Vorfeld darüber, welche Bereiche und Prüfungen im Einzelfall für Sie sinnvoll sind. Beispielsweise gehören hierzu folgende Fragestellungen:

- Was ist der Schwerpunkt der Überprüfung?
- Welche Aspekte der Sicherheit sind zu beachten?
- Mit welchen Methoden darf/soll geprüft werden?
- Auf welchen Ebenen werden die Komponenten untersucht?
- Von welchen Zugängen aus sollen Prüfungen durchgeführt werden?

# UNSERE LEISTUNGEN IM DETAIL



Wir bieten Ihnen umfassende technische, konzeptionelle bzw. organisatorische Untersuchungen der Sicherheit Ihrer Anwendungen, Systeme, Infrastrukturen oder Prozesse.

Die technischen Untersuchungen können sich sowohl auf Bestandteile der Infrastruktur (z. B. Server, Netzwerkkomponenten, Firewalls, VPNs oder IDS) und Endgeräte als auch auf Anwendungen und deren Komponenten (z. B. Web Application Server) erstrecken.

Das Spektrum reicht von Social Engineering, Applikationsuntersuchungen, Quellcodeprüfungen und Konfigurationsanalysen bis hin zu Reverse Engineering.

Auch auf der organisatorischen Ebene der Informationssicherheit ist immer wieder zu überprüfen, ob das Informationssicherheitsmanagementsystem (ISMS), das Risikomanagement, die vorhandenen Richtlinien zur Informationssicherheit oder die sicherheitsrelevanten Betriebsprozesse (z. B. Security Incident Handling, Berechtigungsvergabe, Schwachstellenmanagement) noch den Anforderungen entsprechen und der Bedrohungslage angemessen sind.

Unsere langjährige Erfahrung, die Orientierung an relevanten Standards und unsere eigenen Qualitätsziele sorgen dafür, dass die Ergebnisse verständlich, nachvollziehbar und für das Management verwertbar dargestellt werden.



# UNSERE VORGEHENSWEISE



## Der Ablauf einer Sicherheitsüberprüfung lässt sich in drei Phasen gliedern.

### 1 Vorbereitung und Abstimmung der Vorgehensweise

In der ersten Phase werden die eventuell vorhandenen Risiken für den laufenden Betrieb diskutiert. Darüber hinaus besprechen wir mit Ihnen, welche Komponenten in welchem Zeitfenster zu prüfen sind. Diese Phase der Prüfung definiert die Basis für alle weiteren Schritte.

### 2 Durchführung der Prüfung

Die Durchführung der Prüfung erfolgt anhand der festgelegten Vorgehensweise. Technische, organisatorische und physische Prüfungen können sequenziell oder auch parallel vorgenommen werden. Dies findet selbstverständlich in enger Abstimmung mit Ihnen statt. Auf Wunsch werden Ihnen schwerwiegende Befunde bereits während der Prüfung gemeldet.

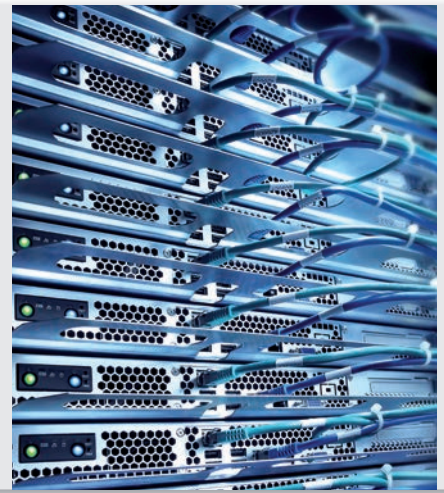
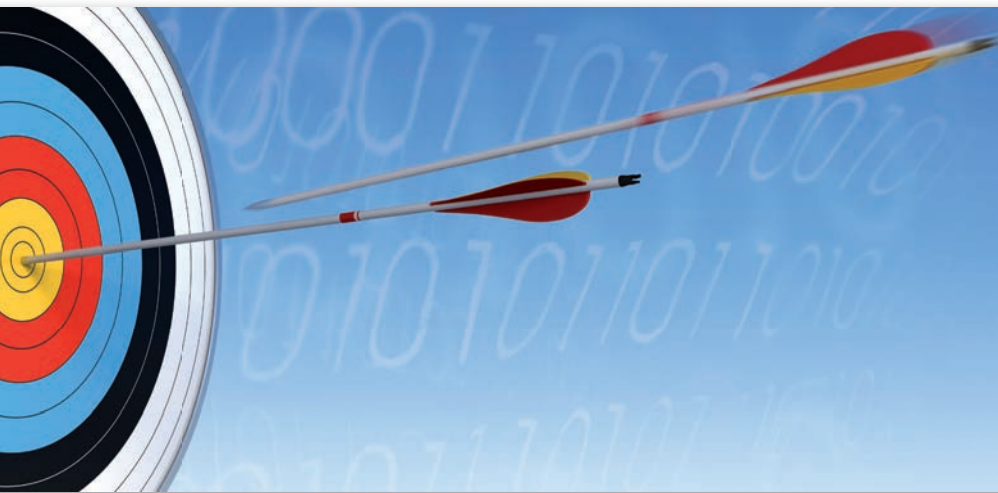
### 3 Dokumentation und Präsentation der Ergebnisse

Nach Abschluss der Überprüfung werden die Ergebnisse für die jeweiligen Zielgruppen aufbereitet und auf Wunsch präsentiert.

Entscheidend für erfolgreiche Audits und Penetrationstests ist einerseits eine kompetente und professionelle Durchführung und andererseits eine angemessene Bewertung und Präsentation der Ergebnisse für die jeweilige Zielgruppe. Für beide Aspekte ist cirosec bekannt.

Gern diskutieren wir mit Ihnen auch die Umsetzung nachhaltiger Gegenmaßnahmen und unterstützen Sie bei der Realisierung.

# BEISPIELE



## Ausgewählte Beispiele für Module von IT-Sicherheitsüberprüfungen, Penetrationstests & Audits

- Untersuchung von Web-Applikationen bezüglich Manipulations- und Einbruchmöglichkeiten auf Anwendungsebene
- Betrachtung der Sicherheit von mobilen Arbeitsplätzen, Smartphones oder Tablets
- Sicherheits- und Risikobewertung von Apps für Smartphones oder Tablets
- Überprüfung von Datenbanken bezüglich Access Control und Manipulationsmöglichkeiten
- Technische Überprüfung erreichbarer Systeme mithilfe automatisierter Scanner und manueller Methoden auf Netzwerkebene
- Red Team Exercises
- Überprüfung von ICS-Umgebungen
- Manuelle technische Überprüfung definierter Systeme hinsichtlich ihrer Konfiguration und Härting auf Systemebene
- Suche nach unbekanntem externen Verbindungen (Internet, Telefoneinwahl, WLAN)
- Überprüfung von Telefon- und Videokonferenzsystemen
- Überprüfung von Bürogeräten mit Netzwerkanschluss (beispielsweise Multifunktionsdrucker, die ins Netzwerk eingebunden sind)
- Manuelle technische Prüfung von Sicherheitskomponenten hinsichtlich ihrer korrekten und vollständigen Konfiguration bzw. Möglichkeiten zur Umgehung
- Überprüfung der Sicherheit von Anwendungen, Diensten und Daten in der Cloud
- Konzeptionelle Überprüfung der strukturellen Sicherheit einzelner Bereiche (beispielsweise Angemessenheit der Wahl von Netzwerkzonen)
- Betrachtung der Sensibilisierung und Kooperation der Mitarbeiter in Bezug auf IT-Sicherheit (Awareness)
- Überprüfung von Zugangskontrollsystemen, der Verkabelung und anderen physikalischen Aspekten
- Reverse Engineering zum Auffinden von Schwachstellen in Softwareprodukten oder Embedded-Geräten
- Innentäter- bzw. Insider-Threat-Analysen
- Überprüfung der WLAN-Infrastruktur
- Technische und konzeptionelle Überprüfung von IoT-Lösungen



cirosec GmbH  
Heilbronn | Deutschland  
T +49 7131 59455-0 | F +49 7131 59455-99 | [www.cirosec.de](http://www.cirosec.de)

