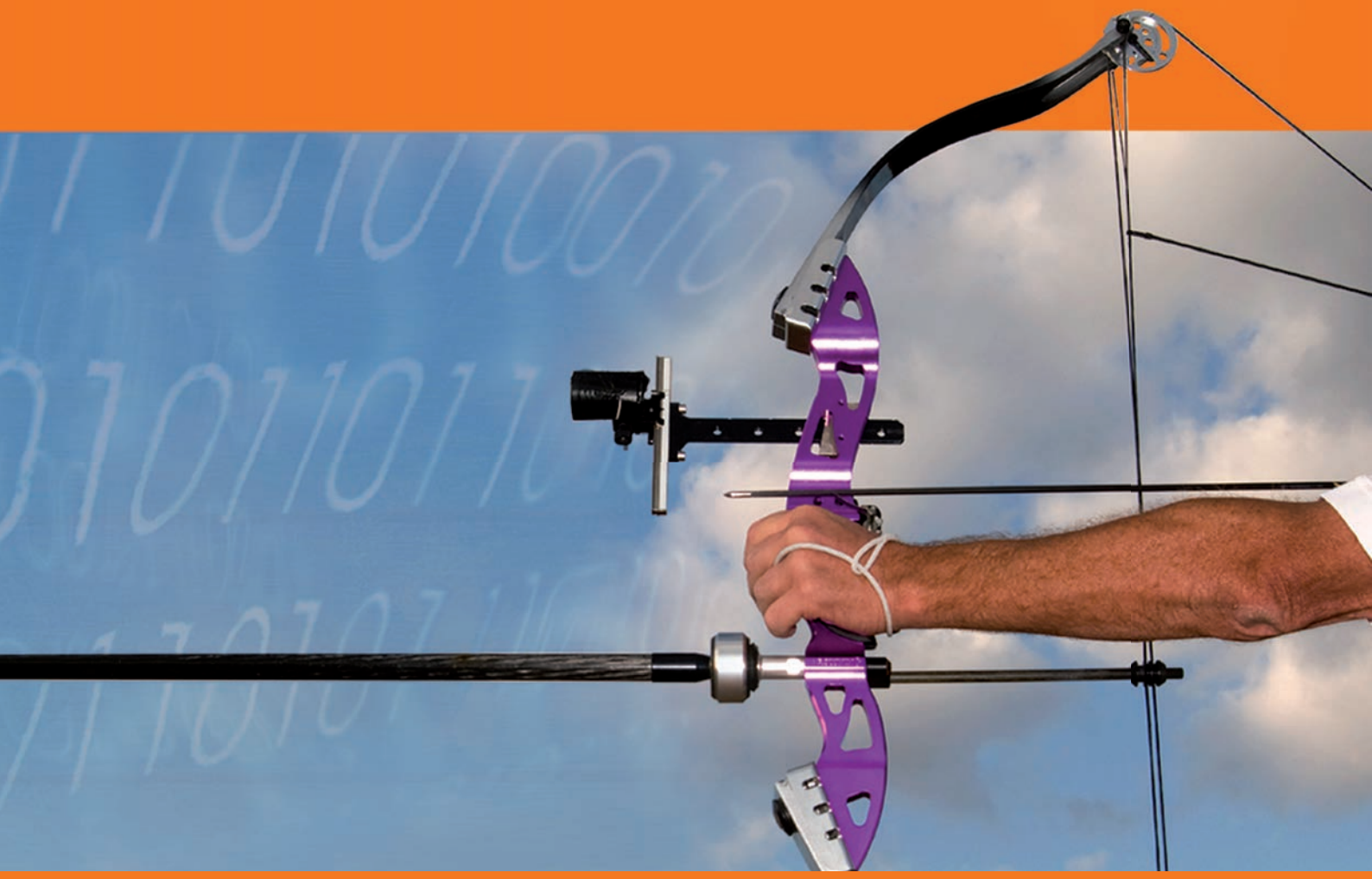


Penetrationstests und Red Teaming

cirosec

Penetrationstests und Red Teaming

cirosec steht für Penetrationstests, Red Team Exercises und professionelle Sicherheitsüberprüfungen

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

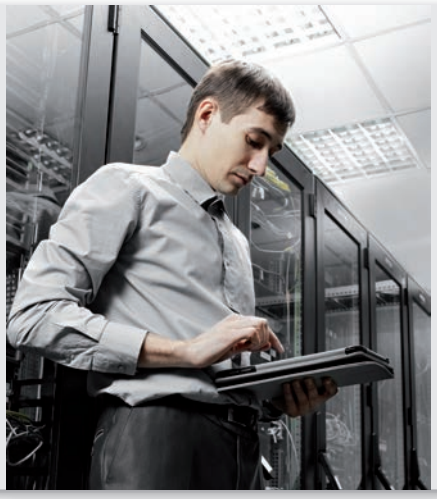
Sicherheit wird durch Änderungen in Abläufen, Anwendungen und an Komponenten wie Firewalls, durch die Inbetriebnahme neuer Dienste sowie durch immer wieder neu entstehende Bedrohungen stets infrage gestellt.

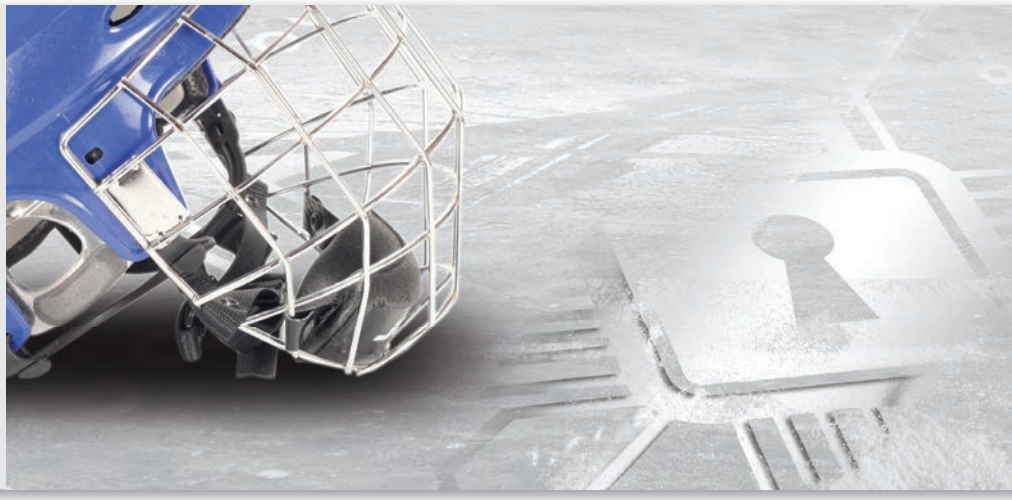
Wir beraten Sie, wie Sie Ihre IT- und Informationssicherheit effektiv und effizient überprüfen und hinterfragen können.

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 Prüfungen auf höchstem Niveau.

UNSERE LEISTUNGEN IM ÜBERBLICK





Neben detaillierten Kenntnissen der aktuellen Angriffstechniken und -methoden verfügen wir über langjährige Erfahrung im Bereich von Audits, Penetrationstests und Red Teaming. 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 sowie der Effektivität Ihrer Sicherheitsmaßnahmen.

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

Das Spektrum reicht von Red Teaming inklusive 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 Konzepte 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 Rahmenbedingungen und Ziele sowie 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

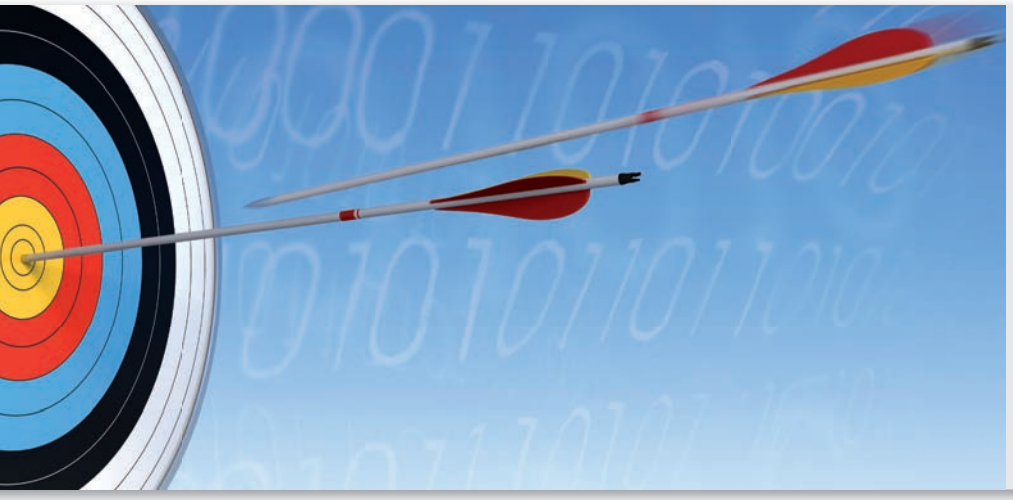
Dokumentation und Präsentation der Ergebnisse

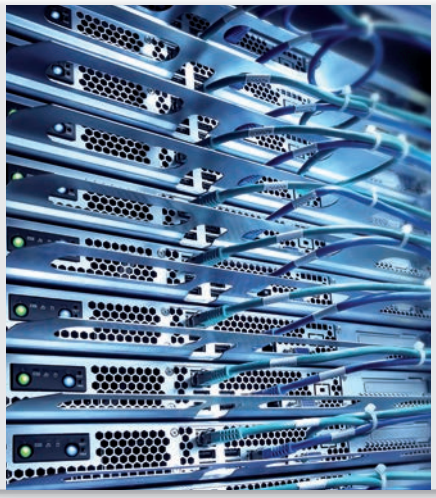
Nach Abschluss der Überprüfung werden die Ergebnisse für die jeweiligen Zielgruppen aufbereitet und auf Wunsch präsentiert.

Entscheidend für erfolgreiche Audits, Penetrationstests und Red Teaming 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 Einbruchsmöglichkeiten 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
- Prüfung der Wirksamkeit von Malwareschutzmaßnahmen, Erkennungstechniken und Reaktionsprozessen
- Überprüfung von ICS-Umgebungen
- Manuelle technische Überprüfung defi nierter Systeme hinsichtlich ihrer Konfi guration und Härtung auf Systemebene
- Suche nach unbekannten 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 Konfi guration 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 – IHR PARTNER IN DER IT-SICHERHEIT

cirosec GmbH — spezialisiert auf IT- und Informationssicherheit

Unsere erfahrenen IT-Sicherheitsspezialisten prüfen die IT-Landschaft unserer Kunden, beraten sie herstellerneutral und setzen Lösungen kompetent um.

Das cirosec-Team zeichnet sich durch seine zahlreichen Experten aus, die als Buchautoren oder Referenten bekannt sind und die Kunden mit technischem und strategischem Sachverstand individuell beraten.

Darüber hinaus verfügt das Team über langjährige Erfahrung in der Konzeption und Integration von Sicherheitsprodukten in komplexen Umgebungen.

Das Angebotsspektrum umfasst:

- Konzepte, Reviews und Analysen
- Durchführung von Audits und Penetrationstests
- Incident Response und Forensik
- Konzeption, neutrale Evaluationen und Implementierung von Produkten und Lösungen

Wir sind ein innovatives Unternehmen mit Fokus auf Informationssicherheit.

Bei technischen Lösungen liegen die Schwerpunkte in folgenden Bereichen:

- Schutz vor gezielten Angriffen (APTs) und moderner Malware
- Sicherheit im internen Netzwerk und in der Cloud
- Sicherheit für IoT und Industrie 4.0
- Verwundbarkeits- und Risikomanagement
- Nachvollziehbarkeit und Kontrolle administrativer Zugriffe
- Sicherheit von (mobilen) Endgeräten, Apps, Web-Applikationen, Portalen und Web Services

Darüber hinaus bieten wir unseren Kunden individuell gestaltete Schulungen, die von erfahrenen Beratern durchgeführt werden. Sie zeichnen sich durch einen aktuellen Praxisbezug und eine lösungsorientierte Vorgehensweise aus.

Im Rahmen unserer Hacking-Extrem-Trainings ermöglichen wir ein tiefes Eintauchen in die Sichtweise der Angreifer nach dem Prinzip „Know your Enemy“.

Bei vielen Trainings steht jedem Teilnehmer ein Notebook zur Durchführung praxisnaher Übungsaufgaben zur Verfügung.

v03CRS-18-1925-DE181022 · Bildquellen: istockphoto, shutterstock

cirosec GmbH
Heilbronn | Deutschland
T +49 7131 59455-0 | F +49 7131 59455-99 | www.cirosec.de

cirosec