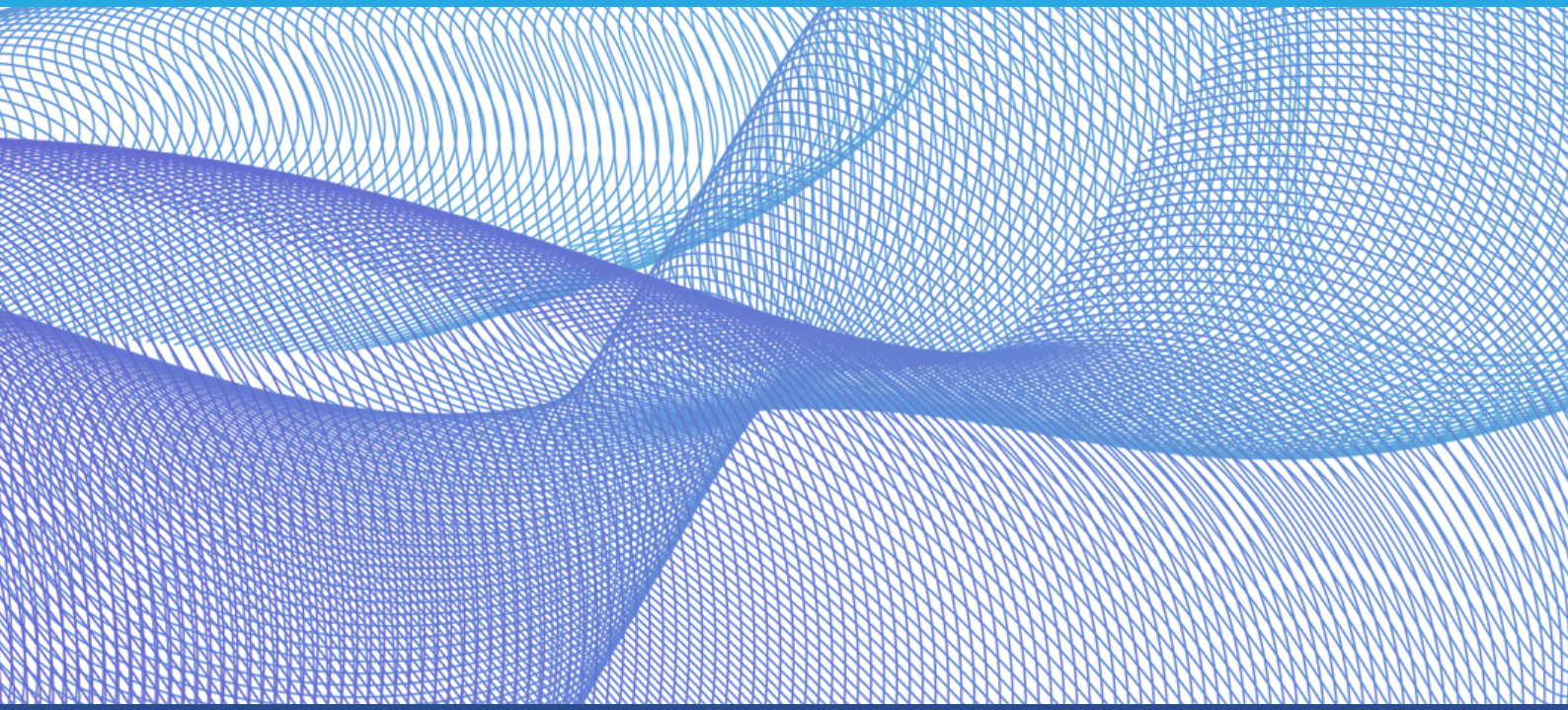


PENETRATIONSTESTS UND RED TEAMING

Technische und organisatorische Sicherheitsüberprüfungen sowie Red-Team-Assessements

cirosec

Penetrationstests und Red Teaming

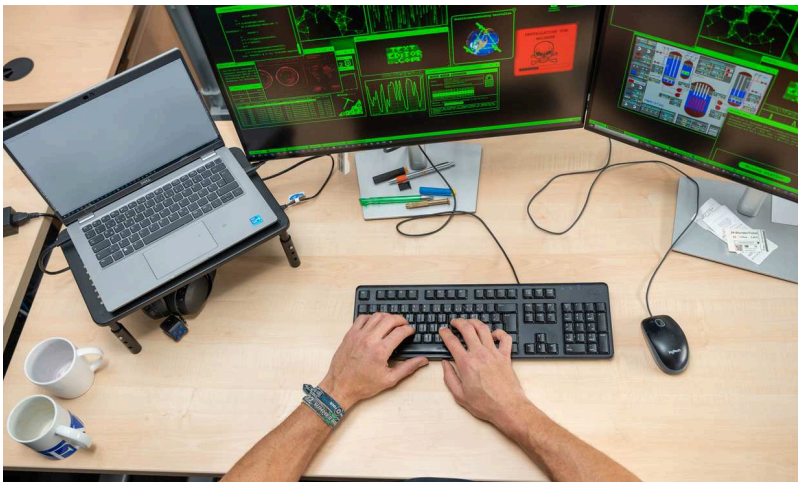
Sicherheit ist kein dauerhafter Zustand. Daher muss die Effektivität der Sicherheitsmaßnahmen, Prozesse und Managementsysteme regelmäßig hinterfragt werden.

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 Prüfberichten 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 kein Universalrezept gibt. Deshalb müssen vor jeder Sicherheitsüberprüfung der Rahmen und der Fokus der Untersuchung abgestimmt werden.

Wir beraten Sie bereits im Vorfeld, 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?

Wir bieten Ihnen umfassende technische, konzeptionelle und 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 erstrecken als auch auf Anwendungen und deren Komponenten (z. B. Webapplikationsserver).

Das Spektrum reicht von Red Teaming inklusive Social Engineering, Applikationsuntersuchungen, Quellcodeüberprüfungen 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 und Richtlinien zur Informationssicherheit sowie 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.

Der Ablauf einer Sicherheitsüberprüfung lässt sich in drei Phasen gliedern.

1

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.

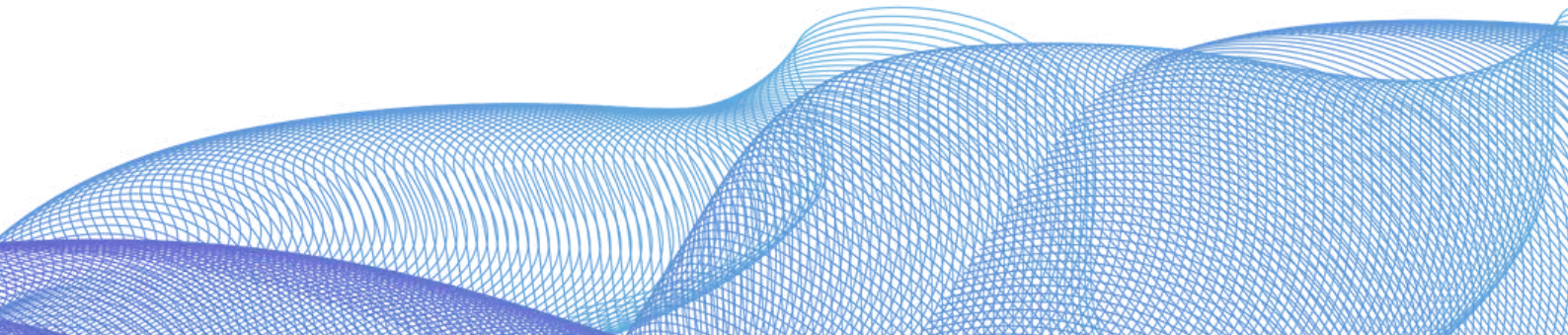
Diese Phase der Prüfung definiert die Basis für alle weiteren Schritte.

2

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.



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

Entscheidend für erfolgreiche Audits, Penetrationstests und Red Teamings ist sowohl eine kompetente und professionelle Durchführung als auch eine angemessene Bewertung und Präsentation der Ergebnisse für die jeweilige Zielgruppe.

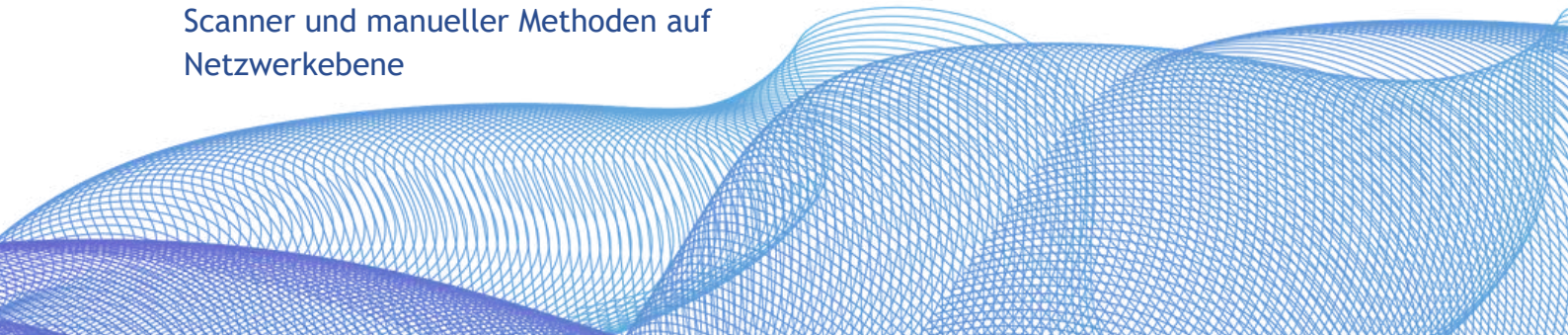
Für all diese Aspekte ist cirosec bekannt.

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

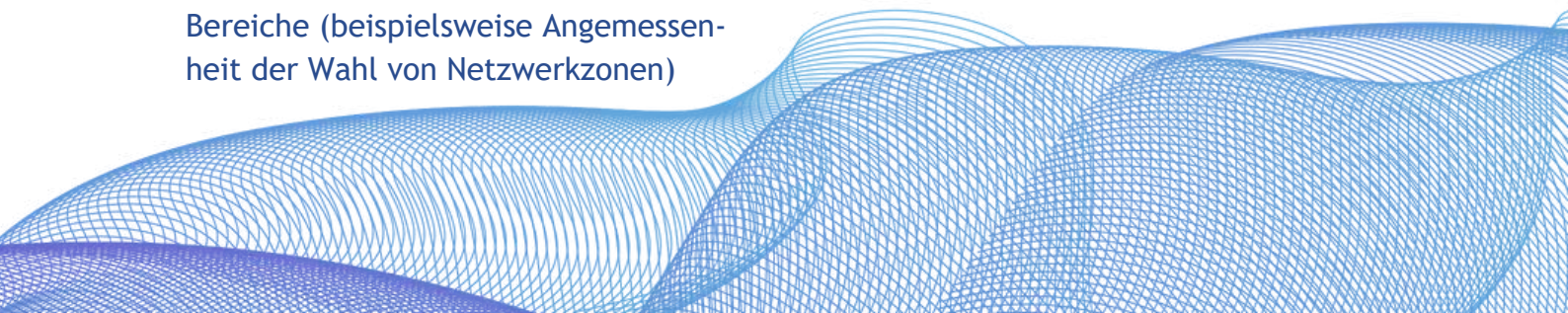
Weitere Informationen finden Sie hier

Beispiele für Penetrationstests und IT-Sicherheitsüberprüfungen

- Untersuchung von Webapplikationen bezüglich Manipulations- und Angriffsmöglichkeiten auf Anwendungsebene
- Betrachtung der Sicherheit mobiler Arbeitsplätze, von Smartphones oder Tablets
- Sicherheits- und Risikobewertung von Apps für Smartphones oder Tablets
- Überprüfung von Datenbanken bezüglich Zugangskontrolle 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 OT-Umgebungen
- Manuelle technische Überprüfung definierter Systeme hinsichtlich ihrer Konfiguration 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 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 physischen Aspekten
- Reverse Engineering zum Auffinden von Schwachstellen in Softwareprodukten oder Embedded-Geräten
- Innentäteranalysen
- Überprüfung der WLAN-Infrastruktur
- Technische und konzeptionelle Überprüfung von IoT-Lösungen



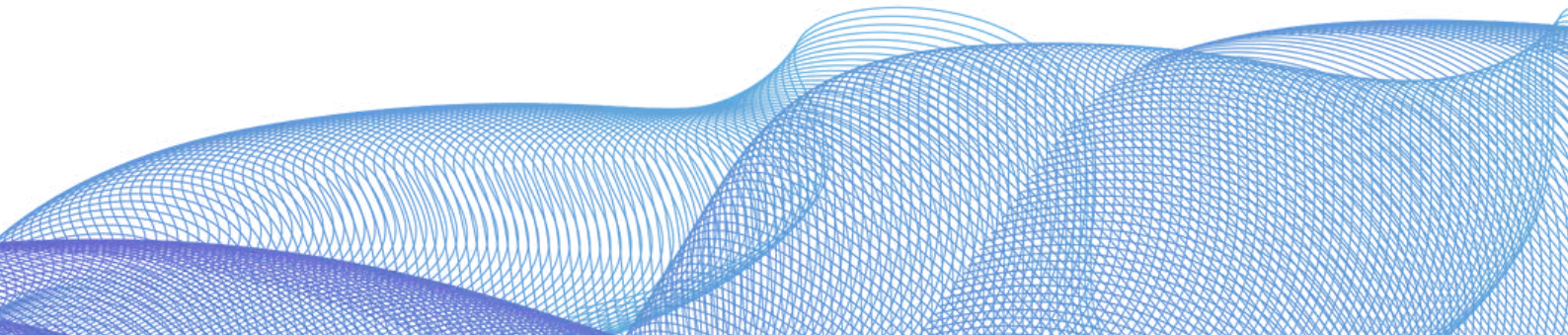
Red-Team-Assessments

Ein Red-Team-Assessment unterscheidet sich von einem klassischen Penetrationstest in mehreren Punkten.

Der größte Unterschied besteht darin, dass nicht eine Anwendung oder ein System, sondern alle Assets eines Unternehmens gleichermaßen im Fokus stehen. Dabei spielt es keine Rolle, ob es sich hierbei um ein IT-System, einen Mitarbeiter, einen Standort oder auch um ein Unternehmen in der Holding-Struktur handelt.

Stattdessen steht die Simulation realer Angriffstechniken und -taktiken im Vordergrund. Dazu werden in aller Regel konkrete Ziele definiert, die das Red-Team erreichen soll. Dies kann beispielsweise der Zugriff auf ein bestimmtes System oder eine Datenbank mit sensiblen Informationen sein.

Weitere Informationen finden Sie hier



ÜBER CIROSEC

cirosec GmbH –
Ihr Partner in der IT-Sicherheit

Wir sind ein spezialisiertes Unternehmen mit Fokus auf Informationssicherheit, führen Penetrationstests durch, unterstützen unsere Kunden bei der Incident Response und beraten sie im deutschsprachigen Raum bei Fragen der Informations- und IT-Sicherheit.

Wir sind vor allem in folgenden Bereichen tätig:

- **IT-Sicherheitsberatung, Konzepte, Reviews, Analysen und ISMS**
  Wir verfügen über langjährige Erfahrung in der Beratung, Konzeption und Analyse komplexer Sicherheits-umgebungen.

Detailliertere Informationen

- **Incident Response und Forensik**
  Wir bieten unseren Kunden deutschland-weit eine 24/7-Erreichbarkeit unserer Experten für Incident Response und Forensik mit garantierten Reaktionszeiten sowie einen umfassenden Leistungskatalog zur Bewältigung gezielter Angriffe und anderer IT-Sicherheitsvorfälle.

Mehr dazu finden Sie auf unserer Website

Penetrationstests

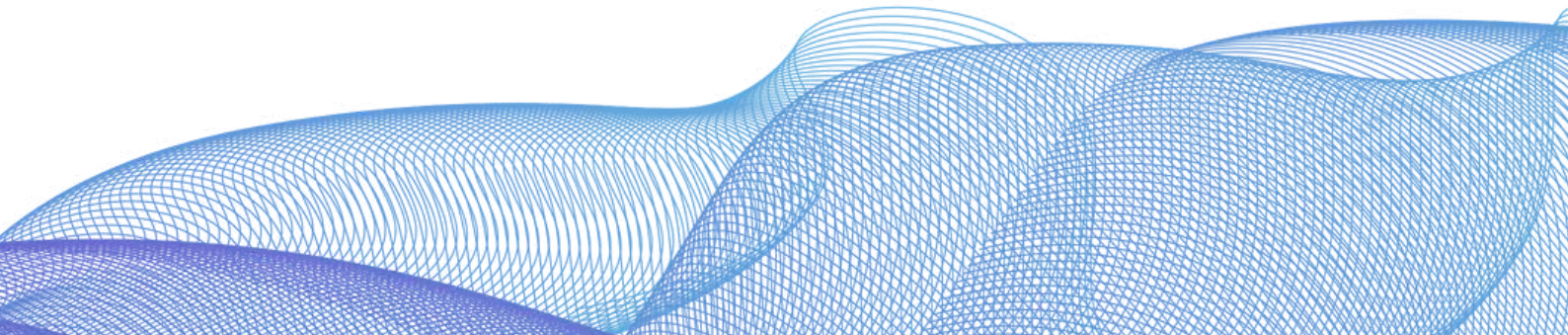
Neben detaillierten Kenntnissen der aktuellen Angriffstechniken und -methoden verfügen wir über langjährige Erfahrung im Bereich von Penetrationstests. Dadurch ist es uns möglich, Ihre IT-Lösungen nicht nur auf der konzeptionellen Ebene auf potenzielle Sicherheitsrisiken hin zu untersuchen: Wir finden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

Zu unseren Schwerpunkten

Red-Team-Assessments

Ein Red-Team-Assessment unterscheidet sich von einem klassischen Penetrationstest in mehreren Punkten. Der größte Unterschied besteht darin, dass nicht eine Anwendung oder ein System, sondern alle Assets eines Unternehmens gleichermaßen im Fokus stehen. Dabei spielt es keine Rolle, ob es sich hierbei um ein IT-System, einen Mitarbeiter, einen Standort oder auch um ein Unternehmen in der Holding-Struktur handelt.

Zu den verschiedenen Varianten



- **Auswahl & Implementierung von Produkten und Lösungen**
  Technische Sicherheitsmaßnahmen sind oft an kommerzielle Produkte oder Werkzeuge gekoppelt. Durch unsere langjährige Erfahrung und Herstellerunabhängigkeit garantieren wir nicht nur kompetente Unterstützung bei der Produktauswahl, sondern auch eine stressfreie Umsetzung und Konfiguration in Ihrer Umgebung.

Zu unserer Vorgehensweise

- **IT-Security-Trainings und Awareness**
  Wir bieten Ihnen individuell gestaltete Seminare und Trainings, in denen Ihnen unsere langjährig erfahrenen Berater den richtigen Umgang mit modernen Technologien und neuen Sicherheitsthemen vermitteln.

Zur Übersicht

cirosec GmbH | Ferdinand-Braun-Straße 4
74074 | Heilbronn | Deutschland
T +49 7131 59455-0 | www.cirosec.de

cirosec