# 360-Grad-Sicherheitsanalyse



cirosec

# 360-Grad-Sicherheitsanalyse

## Neutrale Bestandsaufnahme und Aufzeigen von Handlungsfeldern

Die IT- und Informationssicherheit im Unternehmen muss laufend an die sich verändernde Bedrohungslage und an sonstige Rahmenbedingungen im Unternehmen angepasst werden.

Dabei den Überblick zu behalten und die passenden Sicherheitsmaßnahmen auszuwählen ist nicht einfach, zumal die eigenen Strukturen im IT-Sicherheitsbereich oft über Jahre gewachsen sind.

Entscheidend bei der Auswahl von Sicherheitsmaßnahmen ist, sich nicht von Hypes leiten zu lassen, die insbesondere der Produktmarkt hervorbringt, sondern sich an den individuellen Bedürfnissen und Risiken zu orientieren.

Unter Berücksichtigung der zu schützenden Werte, der Bedrohungslage und der bereits vorhandenen technischen und organisatorischen Maßnahmen erhalten Unternehmen im Rahmen einer 360-Grad-Analyse eine ausführliche Betrachtung, wie der Stand der IT- und Informationssicherheit in ihrem Unternehmen zu bewerten ist und wo der größte Handlungsbedarf gegeben ist bzw. wo Optimierungsmöglichkeiten bestehen.

Somit werden mit einer 360-Grad-Analyse folgende Fragestellungen beantwortet:

- Wie ist das Unternehmen aus Sicht eines unabhängigen Dritten im Bereich IT- und Informationssicherheit aufgestellt?
- Bieten die vorhandenen Maßnahmen einen ausreichenden Schutz gegen die typischen modernen Bedrohungen? Ist das Sicherheitskonzept im Gesamtbild stimmig?
- Welches sind die notwendigen Handlungsfelder im Bereich IT- und Informationssicherheit in den nächsten Monaten und Jahren und mit welcher Priorität sollte man die Themen jeweils angehen?

## Ablauf der Analyse

Wenn Sie Ihr aktuelles Sicherheitsniveau ganzheitlich von externen, unabhängigen Experten bewerten lassen möchten, sind Sie bei uns genau richtig. Eine 360-Grad-Analyse bietet hierfür einen idealen Rahmen. Sie besteht aus einem eintägigen Workshop mit anschließender Analyse und Dokumentation.

Ziel der 360-Grad-Analyse ist es, die vorhandenen Anwendungen, die IT-Infrastruktur, die getroffenen Schutzvorkehrungen sowie die IT-sicherheitsrelevanten Prozesse im Gesamtbild zu erfassen, um mögliche Angriffspunkte und Schwachstellen zu identifizieren und zu bewerten.

In Anlehnung an gängige Standards werden beispielsweise die folgenden Themengebiete betrachtet:

- Schutz geschäftskritischer Anwendungen
- Netzwerksicherheit
- Sicherheit im Produktionsumfeld
- Sicherheit von Endgeräten wie Clients, Server, Smartphones oder Drucker etc.
- Schutz vor Malware
- Sicherer IT-Betrieb (Administrationskonzept, Berechtigungsvergabe, Schwachstellen- und Patchmanagement, Security Monitoring etc.)
- Sicherheit bei Nutzung der Cloud
- Security Management (ISMS, Richtlinien, Risikomanagement, Dienstleistersteuerung etc.)
- Informationsschutz
- Sichere Entwicklung
- Physische Sicherheit

Der 360-Grad-Workshop folgt keinem starren Raster. Gerne gehen unsere Berater vertiefend auch auf Ihre aktuellen Schwerpunktthemen und Fragestellungen ein.

Sämtliche Befunde werden priorisiert, technische und organisatorische Empfehlungen für Maßnahmen ermittelt und ausführlich beschrieben.

Auf Wunsch können die Ergebnisse darüber hinaus in einer vertiefenden strukturierten Bedrohungs- und Risikoanalyse weiterverarbeitet werden.

Die Ergebnisse der 360-Grad-Analyse zeigen Sicherheitsverantwortlichen mögliche Handlungsfelder priorisiert auf.

# cirosec GmbH

## Kompetente IT-Security-Beratung, Pentests und Incident Response

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.

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
- Penetrationstests und Red Teaming
- 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 für die Cloud und aus der Cloud, SASE/SSE, CASB etc.
- Verwundbarkeits- und Risikomanagement
- Zero Trust
- EDR und XDR
- Sicherheit von Smartphones, Tablets und Apps
- Schutz von Web-Applikationen, Portalen und Web Services
- ISO 27001, Risikomanagement, Prozesse, Policies, Richtlinien
- Nachvollziehbarkeit und Kontrolle administrativer Zugriffe
- IoT und Industrie 4.0

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.

Dazu gehören beispielsweise:

- Hacking Extrem
- Hacking Extrem Web-Applikationen
- Incident Handling & Response
- Crashkurs IT- und Informationssicherheit
- Sicherheit in MS Office 365
- Malware & Rasomware – Hintergründe, Erkennung, Schutz
- Sicherheit von Windows 10/11 im Unternehmen

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.



cirosec GmbH
Ferdinand-Braun-Straße 4 | 74074 Heilbronn | Deutschland
T +49 7131 59455-0 | F +49 7131 59455-99 | www.cirosec.de

cirosec