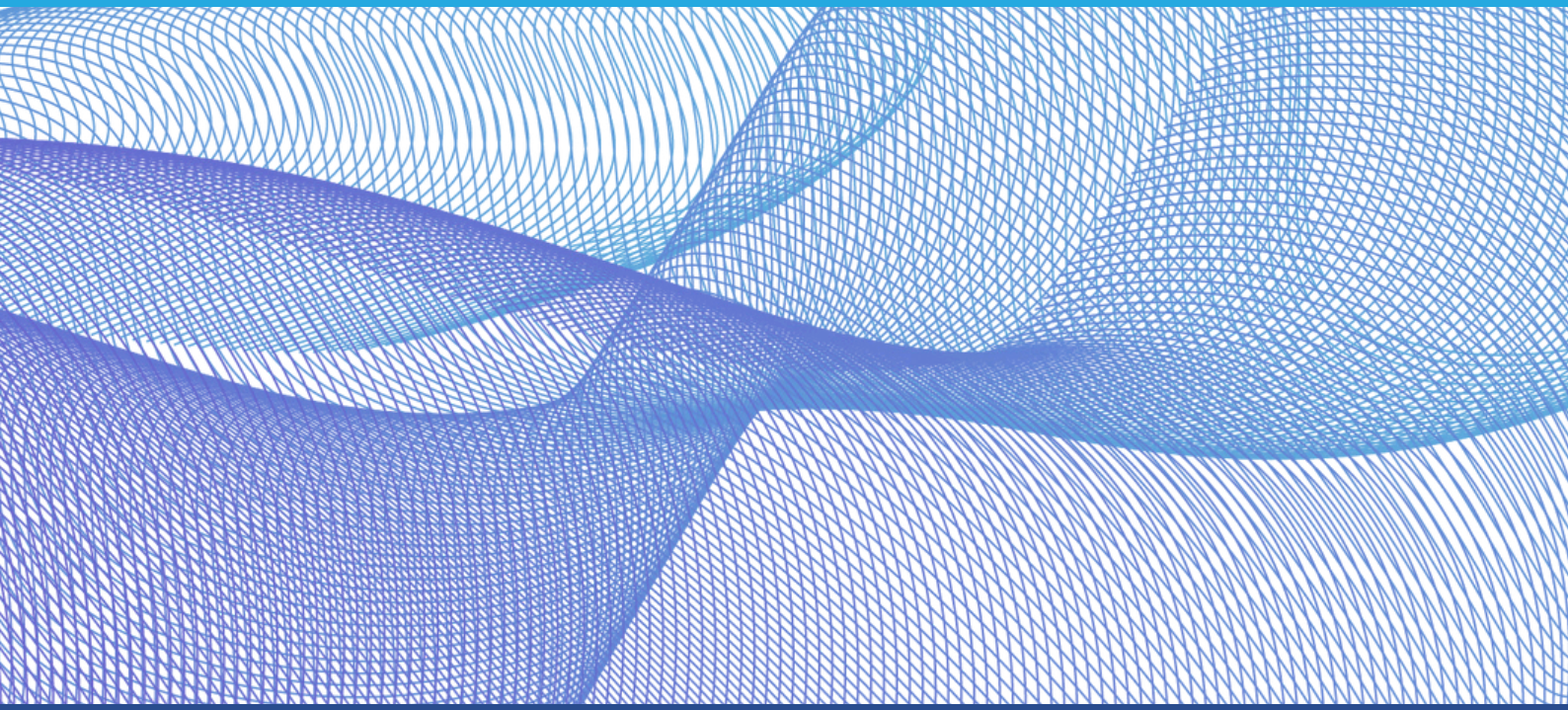


360-GRAD-SICHERHEITSANALYSE

Neutrale Bestandsaufnahme und Aufzeigen von Handlungsfeldern

cirosec

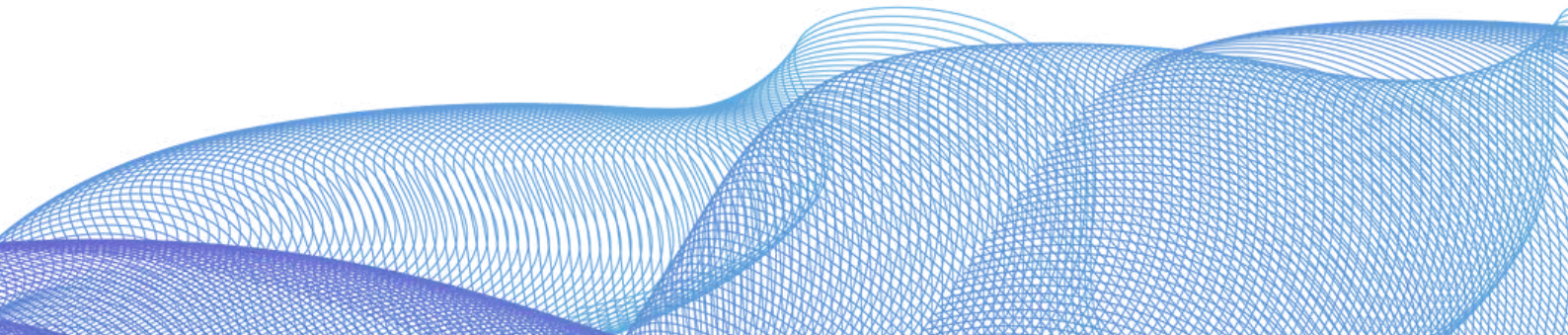
360-Grad-Sicherheitsanalyse

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 konkreten IT-Landschaft und der heutigen Bedrohungslage 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 Handlungsbedarf gegeben ist bzw. wo Optimierungsmöglichkeiten bestehen.



Bei einer 360-Grad-Analyse werden folgende Fragestellungen ausführlich beantwortet:

- Wie ist das Unternehmen aus Sicht eines unabhängigen Dritten im Bereich IT- und Informations-sicherheit aufgestellt?

- Bieten die vorhandenen Maßnahmen und Prozesse einen ausreichenden Schutz gegen die typischen modernen Bedrohungen? Ist das Sicherheitskonzept im Gesamtbild stimmig und sind die Geschäfts-anwendungen und informations-technischen „Kronjuwelen“ ausreichend geschützt?

- 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?

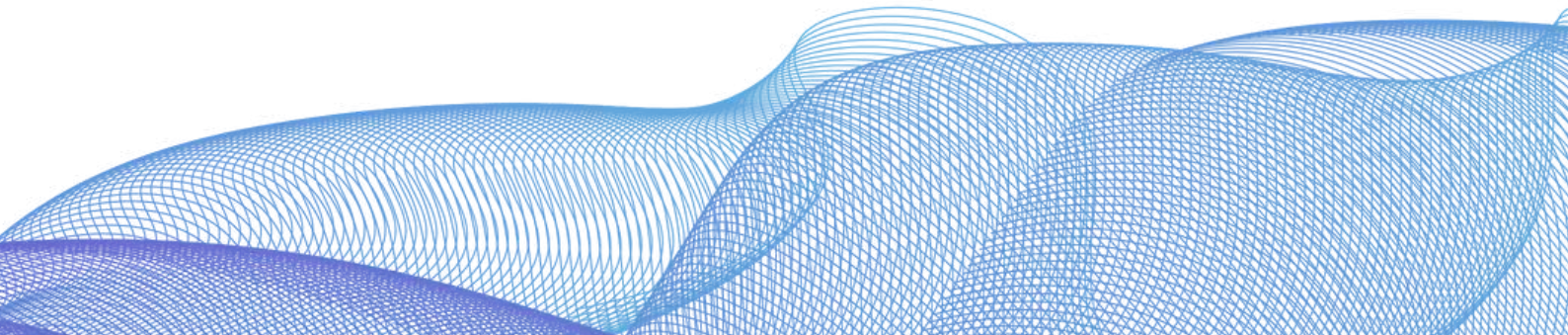
Ablauf der Analyse

Wenn Sie Ihr aktuelles Sicherheitskonzept ganzheitlich von externen, unabhängigen Experten bewerten lassen möchten, bietet eine 360-Grad-Analyse 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 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 vor moderner Malware
- Schutz geschäftskritischer Anwendungen
- Netzwerksicherheit
- Sicherheit im Produktionsumfeld
- Sicherheit bei Nutzung der Cloud
- Sicherheit der verschiedenen Geräteklassen (Clients, Server, Smartphones, Drucker etc.)



- Sicherer IT-Betrieb (Berechtigungsvergabe, Backup-Konzept, Schwachstellen- und Patchmanagement, Security Monitoring, Administrationskonzept/ Tiering etc.)
- Informationsschutz
- Security Management (ISMS, Risikomanagement, Dienstleistersteuerung, Richtlinien etc.)
- Sichere Softwareentwicklung
- Physische Sicherheit

Die 360-Grad-Analyse 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, ausführlich beschrieben sowie in einem halbtägigen Abschlussworkshop mit Ihnen besprochen.

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

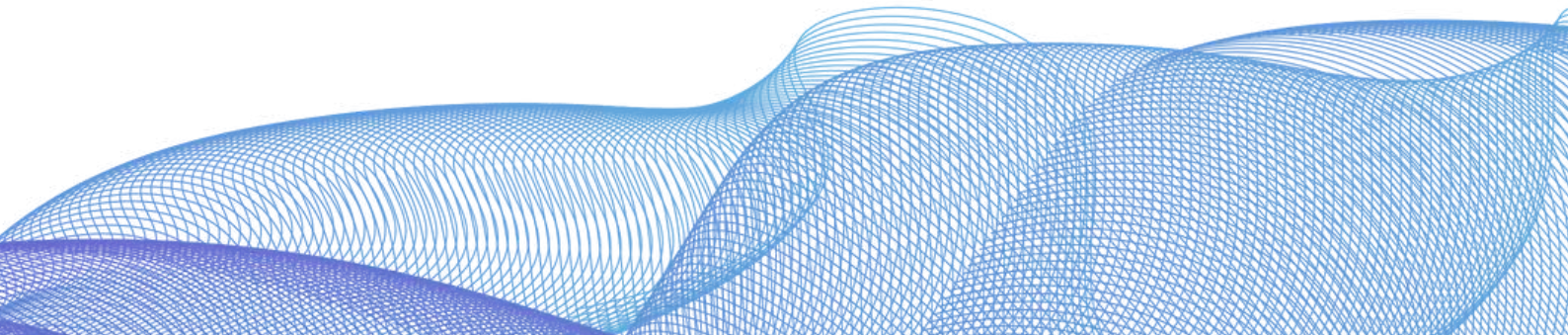
Neben detaillierten Kenntnissen der aktuellen Angriffstechniken und -methoden verfügen wir über langjährige Erfahrung im Bereich von Penetrationstests. Dadurch ist es uns möglich, Ihre IT-Lösungen nicht nur auf der konzeptionellen Ebene auf potenzielle Sicherheitsrisiken hin zu untersuchen: Wir finden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