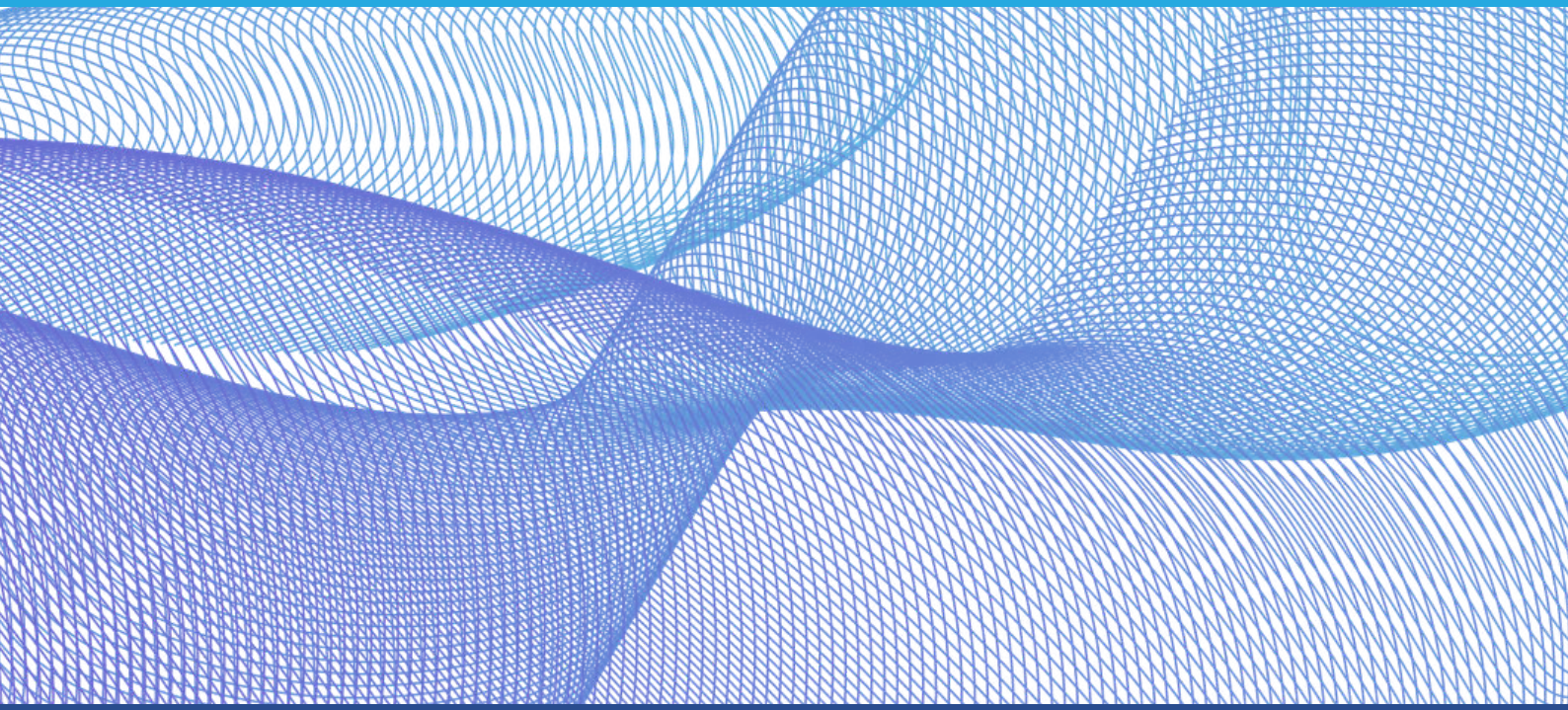


# INCIDENT RESPONSE UND FORENSIK

**Garantierte 24/7-Erreichbarkeit, Incident Handling, Forensik, Konzepte und Übungen**

cirosec

# Incident Response und Forensik

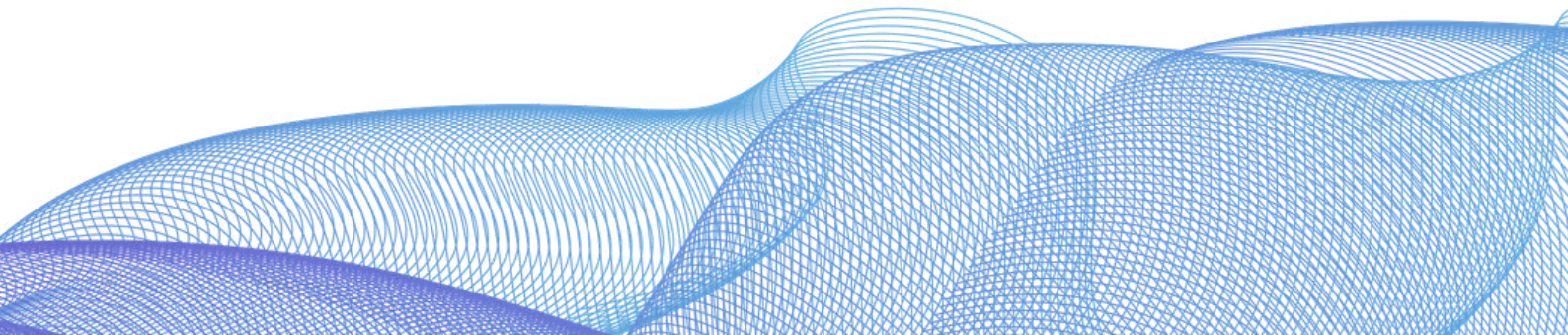
Wir bieten unseren Kunden deutschlandweit eine 24/7-Erreichbarkeit unserer Experten für Incident Response und Forensik mit garantierten Reaktionszeiten sowie einen umfassenden Leistungskatalog zur Bewältigung gezielter Angriffe und anderer IT-Sicherheitsvorfälle.

Bei einem Angriff von Hackern oder einer Infektion mit Ransomware beraten, handeln und unterstützen unsere Experten Sie bei der:

- Auswahl geeigneter Sofortmaßnahmen
- Auf- und Nachbereitung
- Wiederherstellung

Dadurch kann zeitnah richtig reagiert, der Vorfall möglichst schnell eingegrenzt und anschließend bearbeitet werden, damit der Schaden so gering wie möglich ausfällt.

Aufgrund unserer Expertise hat das BSI uns als qualifizierten APT-Response-Dienstleister gelistet.



# Detaillierte Untersuchung und Forensik

Unsere Spezialisten für Forensik untersuchen Vorfälle, betroffene Systeme, Geräte und Netzwerke sowie vorgefundene Malware mit professionellen Werkzeugen vor Ort und in unserem Forensik- bzw. Malwarelabor.

Auf diese Weise werden Tathergang und Angriffsweg rekonstruiert und die für den jeweiligen Angriff typischen Spuren („Indicators of Compromise“) aufgenommen, Hinweise auf weitere betroffene Systeme, Benutzerkonten und Daten ermittelt sowie ein eventueller Datenabfluss untersucht. Auch Informationen zur möglichen Herkunft des Angriffs wird nachgegangen.

Typische Vorgehensweisen können beispielsweise sein:

- Rekonstruktion des Tathergangs oder des Infektionswegs über die Analyse von Protokollen, Festplatten- und Hauptspeicherabbildern
- Gezielte Suche nach Dateien und Inhalten auf Endgeräten und Datenträgern bei Verdacht auf unautorisierten Datenabfluss
- Ermittlung der ursächlichen Schwachstellen für den erfolgreichen Angriff
- Live-Analyse von Systemen, um weitere Spuren zu sammeln oder den Umfang eines Vorfalls zu ermitteln
- Malwareanalyse von Dateien und Programmen

# Übungen zur richtigen Reaktion

Bei einem konkreten Sicherheitsvorfall müssen der externe Dienstleister oder das interne Incident-Response-Team im Unternehmen mit den entsprechenden internen Fachexperten für die jeweiligen IT-Systeme zusammenarbeiten.

Für diese Zusammenarbeit definiert man im Vorfeld die nötigen Rollen und Prozesse beziehungsweise Abläufe.

Um festzustellen, ob diese Pläne auch in der Praxis funktionieren, und um die notwendige Routine bei der Vorfallsbehandlung aufzubauen, sind regelmäßige Übungen unerlässlich.

Nur so wissen alle Beteiligten, wie sie im Ernstfall schnell und richtig zusammenarbeiten können.

Übungen können theoretisch simulierte Situationen sein, bei denen alle Beteiligten an einem Tisch sitzen, oder praktische Übungen, bei denen beispielsweise technische Alarme ausgelöst werden und gemeinsam bearbeitet werden müssen.

Wir unterstützen Sie bei der Vorbereitung wie zum Beispiel der Erarbeitung des Drehbuchs und auch bei der Durchführung der Übung. Dazu gehören die Moderation, die Simulation von Angreifern, die Beobachtung der Handlungen der an der Übung beteiligten Rollen und vieles mehr.

Auch die Nachbereitung von Übungen, gemeinsame Lessons-Learned-Workshops, Empfehlungen zur Verbesserung und Weiteres können wir Ihnen anbieten.

# Beratung und Erarbeitung von Incident-Handling-Konzepten

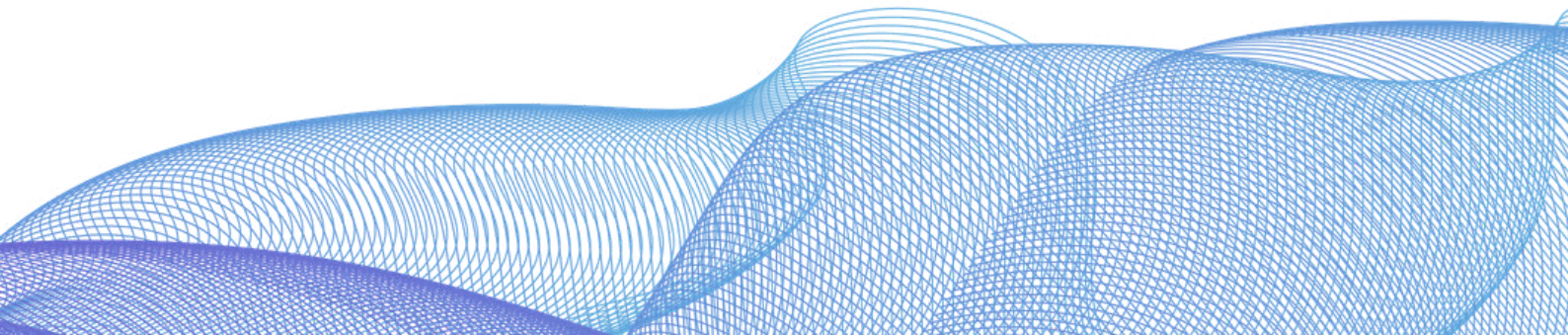
Egal ob Sie sich bei Vorfällen auf cirosec als Incident-Response-Dienstleister verlassen wollen oder ein eigenes Incident-Response-Team, CERT, CSIRT oder sogar SOC aufbauen, in jedem Fall müssen Verantwortlichkeiten, Prozesse und Reaktionspläne erstellt werden.

Wir beraten und unterstützen Sie dabei umfassend, damit Sie optimal vorbereitet sind und im Ernstfall Ruhe bewahren und zielgerichtet reagieren können.

Unsere erfahrenen Berater erarbeiten in enger Abstimmung mit Ihnen Konzepte und vorbereitende Maßnahmen.

Wir unterstützen Sie bei der Gestaltung von Prozessen, bei der Auswahl von Werkzeugen sowie bei der Festlegung von Verantwortlichkeiten und Handlungsanweisungen.

Selbstverständlich orientieren wir uns an den anerkannten Standards.



# Training Incident Handling & Response

In diesem ganztägigen Seminar werden aktuelle Methoden des Incident Handling und der Incident Response als Vorbereitung auf mögliche zukünftige Vorfälle behandelt.

### Erkennung

Zunächst gehen wir darauf ein, wie sich ein Sicherheitsvorfall erkennen lässt. Dabei werden sowohl technische Möglichkeiten zur Erkennung etwaiger Sicherheitsvorfälle auf Endgeräten und im Netzwerk erörtert als auch organisatorische Maßnahmen dargestellt.

### Standards

Anschließend zeigen wir, wie sich beispielsweise mithilfe des ISO-27035-Standards eine systematische Vorgehensweise bei der Bearbeitung eines Vorfalls gewährleisten lässt. Dabei betrachten wir ebenfalls, welche ergänzenden Anforderungen für KRITIS-relevante Unternehmen bestehen.

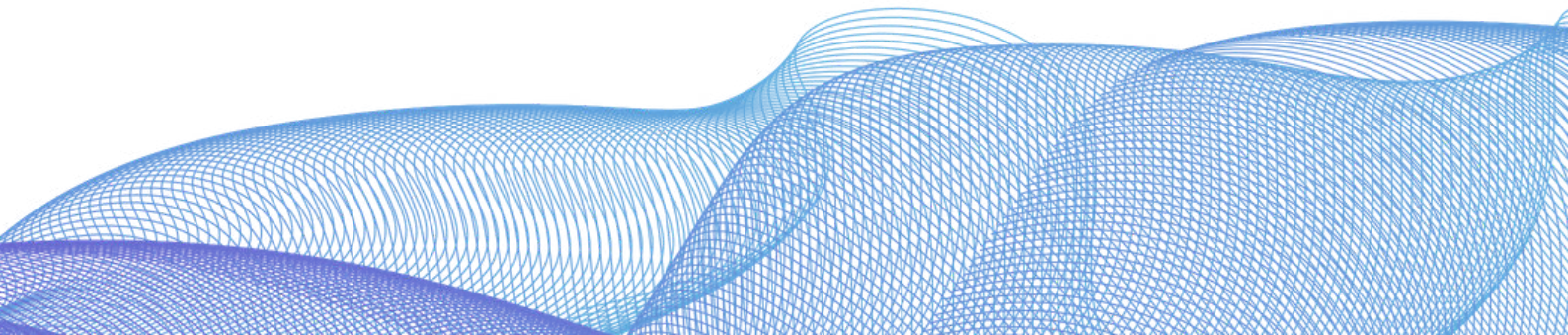
## Fallbeispiele

Darauf aufbauend erörtern wir anhand von Fallbeispielen exemplarisch das richtige Vorgehen bei einem Verdacht auf einen Hackerangriff, auf Datenmissbrauch, Datendiebstahl, Datenlöschung oder auch bei unberechtigter Nutzung firmeneigener Kommunikationsmöglichkeiten.

## Ziel

Nach Abschluss des Seminars wissen die Teilnehmer nicht nur, wie sie einen Incident-Response-Prozess im Unternehmen etablieren und weiterentwickeln können, sondern auch, welche Anforderungen an die Sammlung, Speicherung und Auswertung digitaler Spuren als Beweismittel zu erfüllen sind.

Weitere Informationen, Termine und eine Anmeldemöglichkeit finden Sie hier



# Training IR-Sofortmaßnahmen

Im Rahmen der eintägigen Schulung, die bei Ihnen vor Ort als Inhouse-Training oder auch via Microsoft Teams stattfinden kann, vermitteln wir Ihren zuständigen Mitarbeitern Grundlagen der Incident Response und forensischer Analysen, sodass diese im Falle eines Sicherheitsvorfalls in kurzer Zeit selbstständig die richtigen Sofortmaßnahmen einleiten können.

### Erkennung

Vor der eigentlichen Reaktion auf einen Vorfall und einer forensischen Untersuchung steht zunächst die Erkennung eines Vorfalls sowie die Bewertung, ob es sich dabei überhaupt um einen IT-Sicherheitsvorfall handelt, bei dem externe Unterstützung benötigt wird. Beim Hinzuziehen externer Spezialisten vergeht weitere Zeit, bis diese aktiv werden oder vor Ort sein können.

### Erste Maßnahmen

Während dieser Zeit ist es sinnvoll, bereits mit eigenem Personal erste Maßnahmen zu ergreifen, um Spuren zu sichern oder eine weitere Ausbreitung des Vorfalls zu stoppen.

## Vorbereitung

Zudem sind für die effektive Analyse, Bearbeitung und Eindämmung eines Vorfalls zahlreiche Vorbereitungen Ihrerseits notwendig, damit die erforderlichen Informationen bei Bedarf überhaupt zur Verfügung stehen und nötige Eingriffe in die IT-Infrastruktur schnell erfolgen können.

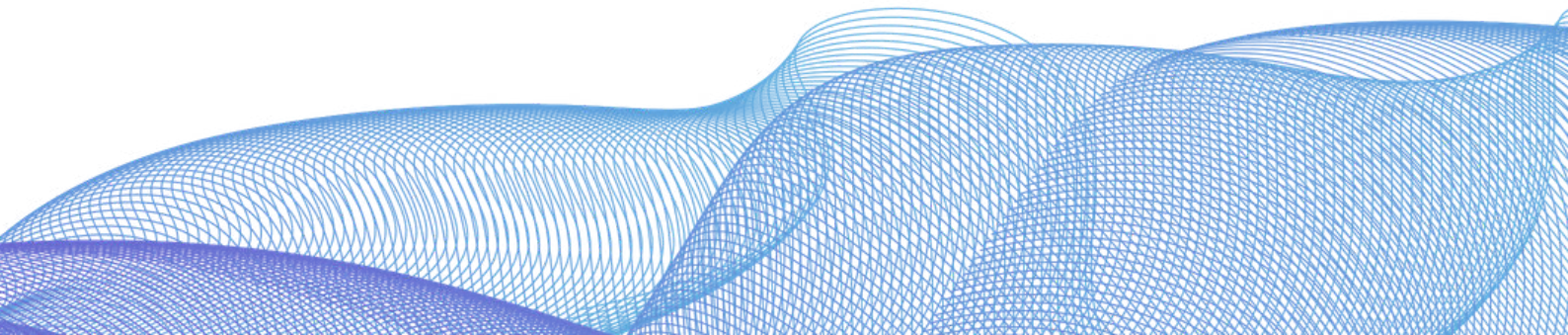
Auch die erfolgreiche Wiederherstellung von IT-Systemen nach einem Vorfall hängt stark von einer guten Vorbereitung ab.

## Zusammenfassung

Ziel ist es, Ihren Mitarbeiter die Grundlagen von IR und Forensik zu vermitteln:

- Richtige Durchführung erster Maßnahmen
- Bewertung verschiedener Situationen und passende Reaktionen
- Hilfe zur Selbsthilfe
- Übungen zur praktischen Vorgehensweise

Weitere Informationen



# 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 Sicherheitsumgebungen.

Detailliertere Informationen

- **Incident Response und Forensik**
  Wir bieten unseren Kunden deutschlandweit 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