Incident Response und Forensik

cirosec

24/7-Erreichbarkeit bei einem Vorfall

Incident-Response-Service mit garantierter Reaktionszeit

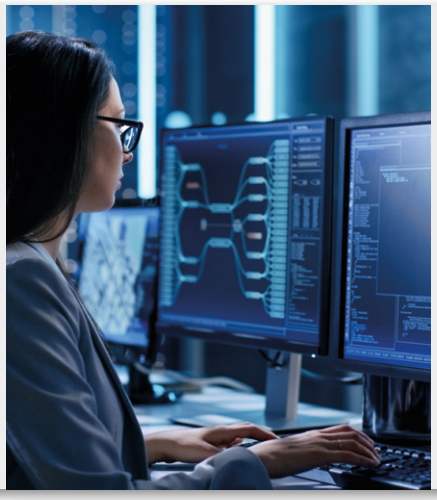
Wir bieten unseren Kunden deutschlandweit eine 24/7-Erreichbarkeit unserer Experten für Incident Response und Forensik mit garantierten Reaktionszeiten sowie einen umfassenden Leistungskatalog zur Bewältigung gezielter Angriffe und anderer IT-Sicherheitsvorfälle.

Bei einem Einbruch von Hackern oder einer Infektion mit Ransomware beraten, handeln und unterstützen unsere Experten:

- Auswahl geeigneter Sofortmaßnahmen
- Unterstützung bei der Auf- und Nachbereitung
- Unterstützung bei der Wiederherstellung

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

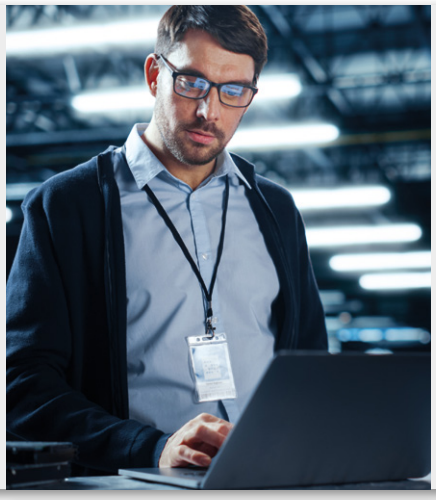
Aufgrund unserer Expertise hat das BSI uns als qualifizierten APT-Response-Dienstleister gelistet.



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. Malware-Labor.

Auf diese Weise werden der 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.



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.

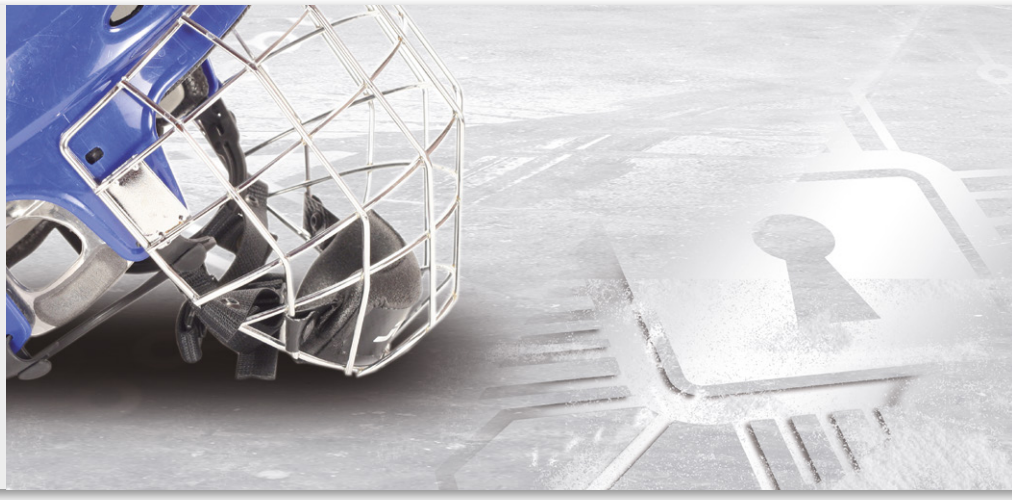
Um festzustellen, ob diese Pläne auch in der Praxis funktionieren, und um die notwendige Routine bei der Vorfallsbehandlung aufzubauen, sind regelmäßige Übungen unerlässlich. Nur so wissen alle Beteiligten, wie sie im Ernstfall schnell und richtig zusammenarbeiten können.

Verschiedene Ansätze

Übungen können theoretisch simulierte Situationen sein, bei denen alle Beteiligten an einem Tisch sitzen, oder praktische Übungen, bei denen beispielsweise technische Alarme ausgelöst 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 wird anhand von Fallbeispielen exemplarisch das richtige Vorgehen bei einem Verdacht auf Hacker-Einbruch, Datenmissbrauch, Datendiebstahl, Datenlöschung oder auch bei unberechtigter Nutzung firmeneigener Kommunikationsmöglichkeiten erörtert.

Ziel

Nach Abschluss des Seminars wissen die Teilnehmenden 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.

cirosec GmbH – Ihr Partner in der IT-Sicheheit

Die erfahrenen IT-Sicherheits-spezialisten von cirosec führen Penetrationstests durch, beraten ihre Kunden 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 cirosec-Team über langjährige Erfahrung in der Konzeption und Integration von Sicherheitsprodukten in komplexen Umgebungen.

Das Angebotsspektrum umfasst:

- Beratung, Konzepte, Reviews und Analysen
- Durchführung von Audits und Penetrationstests
- Incident Response und Forensik
- Konzeption, Evaluation und Implementierung von Lösungen
- Trainings und Awareness

Die Themenschwerpunkte von cirosec liegen auf modernen Schutzmaßnahmen für Unternehmen.

Dazu gehören zum Beispiel:

- Schutz vor gezielten Angriffen (APTs), moderner Malware und Denial-of-Service-Angriffen
- Sicherheit von (mobilen) Endgeräten, Apps, Webapplikationen, Portalen und Webservices
- Nachvollziehbarkeit und Kontrolle administrativer Zugriffe
- Informationssicherheitsmanagement (ISMS)
- Cloud Security
- Windows-10/11-Sicherheit und Office 365
- IoT und Industrie 4.0
- Verwundbarkeits- und Risikomanagement

v02CRS-22-1929-DE220818 · Bildquellen: istockphoto, shutterstock

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

cirosec