

Incident Handling & Response

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

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

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 detailliert erörtert.

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.

Zielgruppe: Sicherheitsverantwortliche, CERTs, betriebliche Ermittler

Voraussetzung: Grundlegende Kenntnisse in der IT; von Vorteil sind Kenntnisse von Angriffsmöglichkeiten und der Vorgehensweise von Hackern.

Beginn:

Donnerstag, 15. Juni 2023, 09:00 Uhr

Ende:

Donnerstag, 15. Juni 2023, 18:00 Uhr

Veranstaltungsort:

Köln

Deutschland

Website & Anmeldung:

Email nadine.eimuellner@cirosec.de

<http://www.cirosec.de/trainings/incident-handling-response>