Krisenmanagement

Wir durchlaufen gemeinsam Simulationen von realitätsnahen Krisensituationen und sprechen handlungsorientierte Empfehlungen zur Lösung aus. Sie erlernen souverän auf Krisensituationen zu reagieren und gezielt unter Druck zu kommunizieren.

Was tun, wenn die Hacker kommen?

Die Bedrohungslage für Unternehmen und Behörden steigt immer weiter an: laut Bitkom waren von 2015 bis 2016 53% der Unternehmen in Deutschland direkt von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen – Tendenz steigend. Durch die zunehmende Vernetzung von Geräten und Diensten vergrößert sich die virtuelle Angriffsfläche in Organisationen. Damit wachsen auch die unmittelbaren Auswirkungen eines Cyberangriffs und die damit verbundenen Schäden innerhalb einer Organisation. Um bei Angriffen oder Notfällen eine strukturierte und zielführende Vorgehensweise zu wahren, ist ein wirkungsvolles Krisenmanagement erforderlich. Dies stellt eine komplexe Aufgabe dar, da viele verschiedene Akteure berücksichtigt werden müssen. Hinzu kommt ein geringes Risiko- und Gefahrenbewusstsein innerhalb von Organisationen.

Bei einem Notfall ist die passende Reaktion der Schlüsselpersonen entscheidend. Dazu gehört zum einen, das ideale Vorgehen zu kennen und umzusetzen, und zum anderen, in Krisensituationen richtig zu kommunizieren. Die Teilnehmenden lernen diese Komponenten nicht nur theoretisch kennen, sondern erleben im Seminar eine komplexe Krisensimulation live und in isolierter Umgebung. Hierbei müssen sie mit einer Vielzahl an Cyberangriffen umgehen, z.B. einem Social Media Shitstorm ausgelöst durch Hacker oder einem DDoS-Angriff. Für eine erfolgreiche Krisenbewältigung stehen die Seminarteilnehmenden bewusst im Mittelpunkt, denn in kritischen Situationen sind psychologische und arbeitsorganisatorische Vorbereitungen besonders relevant. Die Vorgehensweise der Teilnehmenden wird anschließend ausgewertet und sie erhalten handlungsorientierte Hinweise zur Optimierung der Prozesse in ihrer Organisation.

Informationen	Inhalte	Nutzen
Voraussetzungen Problemloser Umgang mit dem PC, Wissen über die IT-Grundprozesse des Unternehmens, IT-Grundkenntnisse z.B. Verständnis über die Funktionsweise des E-Mail-Versands **Dauer** 1 Tag Präsenz (9-17:30 Uhr) **Teilnehmerzahl** Max. 16 Personen **Veranstaltungsort** Mittweida, auch vor Ort im Unternehmen möglich **Kosten** 600 € pro Person **Experten** Prof. Dr. rer. nat. Dirk Labudde, Hochschule Mittweida Markus Straßburg, Fraunhofer Learnlab Martin Klöden, Fraunhofer Learnlab	**Session 1** Kommunikationstheorie – Überblick über verschiedene Modelle sowie die Funktionsweisen von Kommunikation **Session 2** Entscheidungsmodell und Problemlösungsprozess – Vorstellung von Stresstypen und des FORDEC-Modells (speziell zum Vorgehen im Krisenmanagement entwickelt) **Session 3** Krisensimulation – Inszenierung einer mehrstündigen Krise im Unternehmen ausgelöst durch verschiedene Cyberattacken **Session 4** Review der Simulation – Reflexion des Verhaltens der Teilnehmenden; nützliche Tipps und Best Practices	**Sie werden erkennen, wie:** • das eigene Bewusstsein für die Gefahren von Cyberangriffen bezogen auf den Einzelnen und das ganze Unternehmen geschärft werden können • Sie souverän in Krisensituationen reagieren und Ihre Kommunikation, sowie die gemeinsame Lösungsfindung verbessern können • Sie Abläufe und interne, sowie externe Prozesse in Krisensituationen besser nachvollziehen können

Zielgruppe

- Geschäftsführer und Management
- Anwender und Nerd
- Fachkräfte von Unternehmen und Behörden