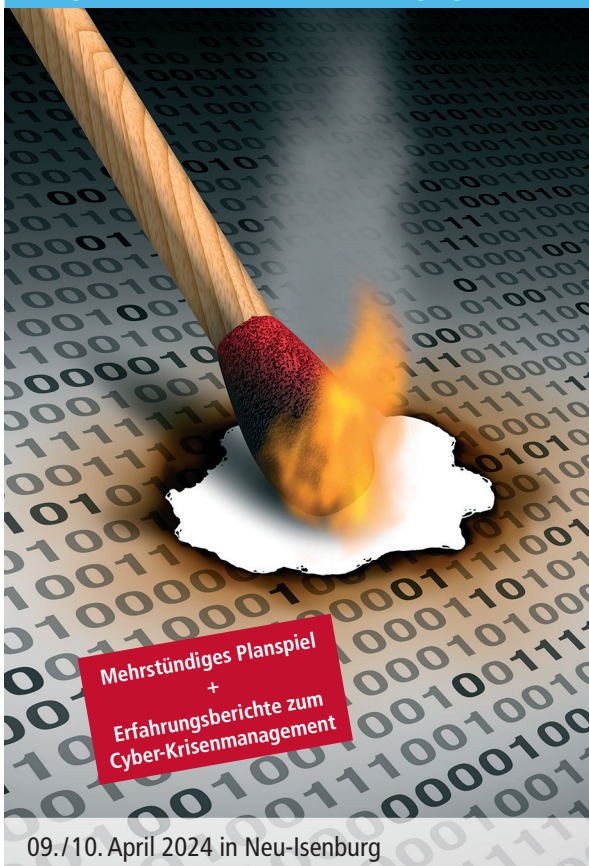


SIMEDIA-Seminar

Krisenmanagement für Cyber-Lagen

Neue Herausforderungen für das Krisenmanagement –
Erfolgsfaktoren für eine effektive Bewältigung



Mehrständiges Planspiel
+
Erfahrungsberichte zum
Cyber-Krisenmanagement

09./10. April 2024 in Neu-Isenburg

Vorwort

Trotz steigender Investitionen in IT-Sicherheitsmaßnahmen und Einbeziehung von KI-basierten Abwehrmaßnahmen finden Hacker immer neue Möglichkeiten, in Unternehmen einzudringen und enormen Schaden anzurichten. Cyberattacken auf Behörden und Unternehmen gehören längst zum Sicherheitsalltag. **Es ist heute keine Frage mehr ob, sondern wann es passiert.** Man denke nur an die erfolgreichen Angriffe auf den amerikanischen IT-Dienstleister Kaseya, auf die Supermarktkette Coop, die TU Berlin, den Landkreis Anhalt-Bitterfeld, Media Markt & Saturn, die Continental AG, den Traktorhersteller Fendt sowie DDoS-Angriffe auf die Websites mehrerer Flughäfen in Deutschland etc. etc. Die Liste ließe sich fast beliebig fortsetzen. Laut Gartner kostet eine Downtime-Stunde die Unternehmen heute zwischen 120.000 und 475.000 €.

Ein neues Ausmaß haben die Cyberangriffe durch den Angriff Russlands auf die Ukraine erhalten. Immer häufiger erfolgen gezielte Angriffe auf öffentliche Infrastrukturen, aber auch auf Unternehmen. Kürzlich registrierte man sogar eine ganze Angriffswelle auf eine mittlere dreistellige Zahl an Unternehmen. **Die Gefahr, Opfer eines Cyberangriffes in Deutschland zu werden, ist im Moment laut Lagebericht des BSI so hoch, wie noch nie.**

Prävention und Detektion reichen heute nicht mehr aus, vielmehr müssen **Strukturen** im Unternehmen **geschaffen, Verantwortlichkeiten geklärt** und **Prozesse geübt** werden, wie mit einem Cyber Angriff umzugehen ist. Richtig aufgestellt, können Betriebsunterbrechungen, Imageschäden, Haftung gegenüber Dritten und Know-How-Verluste so auf ein Minimum reduziert werden.

Cyber-Krisen stellen grundsätzlich neue Anforderungen an das Krisenmanagement. Ziel dieses SIMEDIA-Seminars ist es, die Teilnehmer optimal auf den professionellen Umgang mit CyberVorfällen vorzubereiten, theoretisch und praktisch in Form eines **realitätsbezogenen Planspiels:**

- ▶ Was lässt sich anhand von Beispielen über Angreifer, Angriffswege und Schadenswirkungen aussagen?
- ▶ Was kann man aus bisherigen Vorfällen lernen?
- ▶ Was sind die besonderen Herausforderungen im Cyber-Krisenmanagement?
- ▶ Welche neuen Erfordernisse muss der Krisenstab bewältigen?
- ▶ Welche Erfolgsfaktoren sind wesentlich für eine aussichtsreiche Cyber-Vorfall-Bewältigung?
- ▶ Wie kann man Cyber-Krisenmanagement-Strukturen erfolgreich im Unternehmen implementieren?

Zielgruppe:

Die Veranstaltung wendet sich an Krisenmanager, Mitglieder von Krisenstäben sowie die Geschäftsleitung.

Programm 09. April 2024

Seminarleiter:

Matthias Hämmerle, Hämmerle Consulting

Johannes Strümpfel, Siemens AG

- 9:00 Uhr** **Einführung und kurze Vorstellung der Teilnehmer:innen**
- 09:15 Uhr** **Die aktuelle Cyber-Bedrohungslage**
- ▶ Angreifer und Angriffswege
 - ▶ Schäden und Auswirkungen, „Impact“
- 10:15 Uhr** **Cyber-Krisenmanagement – Teil 1**
- ▶ Cyberresilienz
 - ▶ Klassisches Krisenmanagement
 - ▶ Besondere Herausforderungen im Cyber-Krisenmanagement und Unterschiede zum „klassischen Krisenmanagement“
- 11:15 Uhr** **Kaffeepause**
- 11:45 Uhr** **Cyber-Krisenmanagement – Teil 2**
- ▶ Realistisches Testen und Üben
 - ▶ Lessons Learned aus Cyber-Lagen
 - ▶ Finanzielle Schadensbewertung bei Cyber-Angriffen
 - ▶ Cyber-Versicherungen
- 13:00 Uhr** **Mittagspause**
- 14:00 Uhr** **Planspiel (1)**
- ▶ Vorstellen des Szenarios bzw. der Ausgangslage
 - ▶ Festlegen von Rollen und Prozessen
 - ▶ Gruppenarbeit (30 Minuten)
 - ▶ Ergebnispräsentation und Reflexion
- 15:30 Uhr** **Kaffeepause**
- 16:00 Uhr** **Planspiel (2)**
- ▶ Einspielung von Lageveränderungen
 - ▶ Gruppenarbeit (30 Minuten)
 - ▶ Ergebnispräsentation und Reflexion
-
- 17:30 Uhr** **Ende des ersten Veranstaltungstages**
Gemeinsames Abendessen und Erfahrungsaustausch
-

Programm

10. April 2024

08:30 Uhr **Reflexion Tag 1**

09:00 Uhr **Planspiel (3)**

- ▶ Einspielung von Lageveränderungen
- ▶ Gruppenarbeit (45 Minuten)
- ▶ Ergebnispräsentation (2x10 Minuten) und Reflexion

10:30 Uhr **Kaffeepause**

11:00 Uhr **Planspiel (4)**

- ▶ Einspielung von Lageveränderungen
- ▶ Gruppenarbeit (45 Minuten)
- ▶ Ergebnispräsentation (2x10 Minuten) und Reflexion

12:30 Uhr **Mittagessen**

13:30 Uhr **Verhandlungsführung bei Cyber-Erpressungen**

Sebastian Reis, Result Group

14:00 Uhr **Planspiel (5)**

- ▶ Verhandlungsführung
- ▶ Simulation einer Verhandlung durch die Lehrgangsteilnehmer mit anschließender Feedbackrunde
Sebastian Reis, Result Group

15:00 Uhr **Kaffeepause**

15:30 Uhr **Gesamtauswertung der Veranstaltung (Lessons Learned, Best Practice, Key Take-Aways)**

16:30 Uhr **Ende des Seminars**

Ergänzende Veranstaltungen:

Krisen- und Notfallmanager, BdSI

Strategien und Training für Unternehmens- und Sicherheitsverantwortliche

Im Zentrum einer erfolgreichen Krisenbewältigung stehen immer die verantwortlichen Akteure. Der »Faktor Mensch« mit seinen Stärken und Schwächen beim Handeln in kritischen Situationen macht die psychologische und arbeitsorganisatorische Vorbereitung im Krisen- und Notfallmanagement so relevant. Ein besonderer Schwerpunkt des Lehrgangs liegt deshalb in der Vermittlung **praxisorientierter Inhalte** mittels einer Vielzahl von Simulationsübungen und insbesondere der **computersimulierten Krisenstabsübung »MS Compass«**. Die Teilnehmer werden systematisch auf spezifische Anforderungen vorbereitet und haben die Möglichkeit, das eigene Verhalten vor dem Hintergrund erlebter Notfall- und Krisensituationen zu fühlen und zu reflektieren. **Optimierte Handlungsstrategien** können so entwickelt und internalisiert werden. Abschlussprüfung entweder am Ende des Lehrgangs Notfallmanagement oder des Aufbaulehrgangs Krisenmanagement.

Risiko Stromversorgung

Szenarien, Strategien, Fallstricke in der Notstromkonzeption

Nahezu täglich wird in den Medien über regionale bis zu mehrstündige Stromausfälle berichtet. Auch wenn Experten häufiger über den »lang anhaltenden Stromausfall« diskutieren: Das Risiko kurzer oder mehrstündiger Stromausfälle ist um ein Vielfaches höher. Die Folgen können auch hier gravierend sein.

Das SIMEDIA-Seminar beleuchtet die relevanten Aspekte eines Stromausfalls, dessen **Auswirkungen**, gibt **Handlungsempfehlungen** und zeigt **Lösungswege** auf, wie sich Unternehmen und Institutionen auf einen Stromausfall vorbereiten können. Profitieren Sie von **Quick-Check-Dokumenten** sowie einem **Orientierungsleitfaden**, um die Folgen eines Stromausfalls in Ihrem Unternehmen zu analysieren, erste Schritte einzuleiten sowie ein **Notfallkonzept** »Betrieb unter Notstromversorgung« zu entwickeln.

Business Continuity Professional, BdSI

Theorie und Praxis – Implementierung eines Business Continuity Managements

Die 6-tägige Lehrgangreihe vermittelt praxisorientiert – basierend auf international anerkannten Standards und Best Practice Methoden des Business Continuity Institutes/UK – die Anforderungen an das eigene Business Continuity Management (BCM). Im Grundlehrgang werden dabei **wesentliche Methoden** und **Herangehensweisen** vermittelt und alle Phasen des BCM-Lebenszyklus behandelt. Anhand praktischer Beispiele und Übungen werden im Aufbaulehrgang alle konzeptionellen Schritte von der **Policy** über die **Strategieentwicklung**, die Erstellung von **Notfallplänen** sowie die Test-, Maintenance- und Monitoring-Verfahren bis hin zur **Einbettung in die Unternehmenskultur** vertiefend behandelt. Mittels einer simulierten BCM-/Wiederanlaufübung wird praxisnah das Zusammenspiel von arbeitsorganisatorischer Vorbereitung sowie der Notwendigkeit von strukturierter Kommunikation und Teamarbeit erfahren.

Die Veranstaltungstermine finden Sie unter www.simedia.de

Referenten



Hämmerle, Matthias

Matthias Hämmerle, MBCI, ist selbständiger Unternehmensberater für die Themen Business Continuity Management, Informationssicherheit, IT Service Continuity Management sowie Krisenmanagement. Er berät Unternehmen sowohl bei der Prävention unternehmenskritischer Ereignisse als auch bei der Bewältigung im Krisenmanagement. Matthias Hämmerle ist Herausgeber der BCM-News (www.bcm-news.de), dem führenden deutschen Portal für Business Continuity Management. Neben seiner Beratungstätigkeit ist er als Dozent und Autor tätig, u.a. als Dozent bei der Frankfurt School of Finance & Management. Zuvor war er als Head of BCM & Krisenmanagement für einen weltweit tätigen Finanzdienstleister sowie als Berater für namhafte Unternehmensberatungen sowie Wirtschaftsprüfungsgesellschaften tätig. Er hat in seiner Tätigkeit verschiedene Lagen bewältigt, darunter Hurrican Sandy, Stromausfälle, Personalausfall durch Epidemie sowie Gebäude- und IT-Ausfälle.



Reis, Sebastian

MBA Security & Safety Management, M.A., B.A., ist Manager bei Result Group GmbH. Sein Aufgabenfeld umfasst die Beratung und operative Unterstützung von Unternehmen und Privatkunden im Bereich Risiko- und Krisenmanagement, BCM, Reisesicherheit und Compliance Risk Management. Zudem ist er von Result Group entsandter Geschäftsführer des Expertennetzwerks Unternehmensresilienz (ENUR), das sich zur Aufgabe gemacht hat, Unternehmen durch einen interdisziplinären Ansatz bei der Prävention und Bewältigung von Cyberangriffen zu unterstützen. Hierbei übernimmt er die Aufgabe des Krisenmanagements und der Verhandlungsführung mit Tätergruppen. Vor seiner Tätigkeit als Unternehmensberater war er Offizier im fliegerischen Dienst der deutschen Marine. Neben seiner fliegerischen Tätigkeit qualifizierte er sich im Bereich der spezialisierten Einsatzkräfte der Marine und im Bereich des militärischen Nachrichtenwesens und sammelte Erfahrung in diversen Auslandseinsätzen.



Strümpfel, Johannes

Dipl.-Ing. (univ.) Elektrotechnik, stellvertretender Leiter Unternehmenssicherheit der Siemens AG, Leiter der Abteilung Security Convergence. Seit 2001 für verschiedene Aufgaben und Sicherheitsthemen in der Unternehmenssicherheit der Siemens AG tätig (Sicherheitstechnik, Lauschabwehr, Know-how-Schutz, Sicherheitslage, Krisenmanagement und Sicherheitsprozesse). Davor Beamter im höheren Dienst des Bundesnachrichtendienstes (Referent Information Warfare Threat Assessment) und Offizier der Luftwaffe im Bereich Fernmeldeelektronische Aufklärung sowie als Lehr-Offizier. Vorstandsvorsitzender des Bayerischen Verbands für Sicherheit in der Wirtschaft (BVSW) und Beirat im MBA-Studiengang Strategy, Global Risk & Security Management an der Technischen Hochschule in Ingolstadt sowie im Studiengang Risiko- und Sicherheitsmanagement (RSM) an der Hochschule für Öffentliche Verwaltung Bremen (HföV).

Anmeldebedingungen

Veranstaltungsort

Mercure Neu-Isenburg, Frankfurter Straße 190, 63263 Neu-Isenburg, Tel: +49 6 102 59940, E-Mail: h5381@accor.com. Es steht ein begrenztes Zimmerkontingent **bis 4 Wochen vor** Veranstaltungsbeginn zur Verfügung. Bitte nehmen Sie die Reservierung unter Berufung auf Ihre Teilnahme an der Veranstaltung selbst vor. Stichwort: SIMEDIA.

Kosten

Die Teilnahmegebühr für das Seminar beträgt 1.240,- € (für Abonnenten des »Sicherheits-Berater« reduziert sich der Preis um 5 %) und ist nach Rechnungserhalt vor Beginn der Veranstaltung zu entrichten. Der Preis versteht sich zuzüglich Mehrwertsteuer. Darin enthalten sind eine digitale Dokumentation, Mittagessen, Erfrischungen und Pausenverpflegung sowie das gemeinsame Abendessen zwischen zwei gebuchten Veranstaltungstagen.

Anmeldung

Ihre Anmeldung und Zahlung richten Sie bitte an die SIMEDIA Akademie GmbH, Alte Heerstraße 1, 53121 Bonn. Nach Eingang Ihrer Anmeldung, die Sie telefonisch +49 228 9629370, per E-Mail anmeldung@simedia.de oder über das Internet unter www.simedia.de vornehmen können, erhalten Sie die Anmeldebestätigung und detaillierte Informationen zur gebuchten Veranstaltung sowie das Hotel. Die SIMEDIA Akademie behält sich vor, Anmeldungen ohne Angabe von Gründen abzulehnen.

Stornierung/Rücktritt

Wenn Sie bereits verbindlich zu einer Veranstaltung angemeldet sind, aber nicht teilnehmen können, stehen Ihnen folgende Möglichkeiten zur Verfügung:

Bis unmittelbar vor Beginn einer Veranstaltung können Sie einen Kollegen (Ersatzperson) benennen. Dafür entstehen Ihnen keine weiteren Kosten.

Bis 4 Wochen vor der Veranstaltung können Sie die Teilnahme kostenlos stornieren. Der Rücktritt muss immer schriftlich (per E-Mail) erfolgen.

- Erfolgt der Rücktritt zwischen 30 und 8 Tagen vor Veranstaltungsbeginn, werden wir 50% der Teilnahmegebühr berechnen
- Erfolgt der Rücktritt nach weniger als 8 Tagen vor der Veranstaltung, ist die volle Teilnahmegebühr zu entrichten

Erscheint der Teilnehmer nicht, ohne abgesagt zu haben, sind wir berechtigt, die volle Veranstaltungsgebühr in Rechnung zu stellen. Sollte die Veranstaltung seitens SIMEDIA Akademie GmbH abgesagt werden, so besteht ein Anspruch auf volle Rückerstattung der Teilnahmegebühr; Ansprüche darüber hinaus bestehen nicht.

Programmänderungen

Änderungen bleiben vorbehalten.

Wir über uns

Die SIMEDIA Akademie GmbH steht in Deutschland für hochwertige Seminare, Foren und Zertifikatslehrgänge. Ausgewählte, praxiserfahrene Referenten vermitteln umfassendes Wissen zu aktuellen Themen rund um die betriebliche Sicherheit. Darüber hinaus schätzen Nachwuchs- und Führungskräfte unsere Veranstaltungen als wertvolle Informations- und Erfahrungsbörsen. In Kooperation mit der Messe Essen konzipierte und veranstaltete die SIMEDIA Akademie GmbH den Security Kongress über 10 Jahre lang. Die SIMEDIA Akademie GmbH ist eine Schwesterfirma der VON ZUR MÜHLEN'SCHE GmbH, Sicherheitsberatung – Sicherheitsplanung, BdSI. Weitere Informationen erhalten Sie im Internet unter: www.simedia.de.