



22.04.2024

online

Kritische Infrastrukturen schützen am Beispiel Black Out – Regulierung und (neue) Anforderungen

KRITIS-Gesetz und KRITIS-Verordnung | EU-Regulierung | Hyperrisiko Blackout | Fallbeispiele
Krisenmanagement | Anforderungen | Workshop



Rico Kerstan

Mitgründer Deutsches Institut für Sicherheit und Krisenvorsorge (DISK)
Berater, Trainer und Auditor für die Sicherheit kritischer Infrastrukturen



Prof. Dr. André Röhl

Mitgründer Deutsches Institut für Sicherheit und Krisenvorsorge (DISK)
Professor für Sicherheitsmanagement an der Northern Business School

Kritische Infrastrukturen (KRITIS) müssen sich an zahlreiche Richtlinien und gesetzliche Vorgaben halten, da ihr Ausfall zur erheblichen Beeinträchtigung der öffentlichen Sicherheit führen kann. Daher benötigt es geeignete Strategien, Prozesse und Tools, um ihren Schutz zu gewährleisten.

In diesem eintägigen Praxisseminar erfahren Sie die aktuellen gesetzlichen Vorgaben zum Schutz der Infrastruktur und der IT-Sicherheit. Anhand von Praxisbeispielen erhalten Sie einen Eindruck vom Ist-Zustand im öffentlichen Sektor sowie den Umsetzungsstand der Handlungsaufgaben. Anhand des Beispielszenarios Blackout wird erläutert, wie kritische Infrastrukturen auf derartige Ereignisse vorbereitet werden und wie Sie ein geeignetes Bewältigungskonzept sowie Krisenresilienz in Ihrer Organisation implementieren können. Darüber hinaus wird es Empfehlungen zum Krisenmanagement geben.

Das Seminar schließt mit einem Workshop, in dem Sie ein Krisenszenario im Rahmen eines Krisenstabes durchspielen. Während und nach dem Seminar wird es ausreichend Raum für Fragen aus Ihrem Arbeitsgebiet geben.



Inhaltsübersicht

- Einführung in das Thema
- Begriffsdefinition Kritische Infrastruktur
- System des Katastrophen- und Bevölkerungsschutzes
- Inhalte der aktuellen Regulierung
- KRITIS-Gesetz und KRITIS-Verordnung
- Inhalte der Vorgaben zur IT-Sicherheit
- Zukunft NIS2, CER und KRITIS-Dachgesetz
- EU-Regulierung
- Hyperrisiko Blackout
- Eintrittswahrscheinlichkeit und Schadensausmaß
- Fallbeispiele in Deutschland
- Modell organisationaler Resilienz
- Bewältigungsfähigkeit und Widerstandskraft
- Kritische Prozesse als Ergänzung zu Kritischen Infrastrukturen
- Fokus Krisenmanagement
- Mindestanforderungen an Krisenorganisationen
- Praxisübung zur Krisenstabsarbeit



08:45

Login

09:00

Begrüßung und Vorstellungsrunde

- Gemeinsame Vorstellungsrunde
- Erwartungen und Zielsetzung für die Veranstaltung

09:15

Einführung in das Thema

- Begriffsdefinition Kritische Infrastruktur
- System des Katastrophen- und Bevölkerungsschutzes
- Vorstellung der aktuellen Sektoren- und Schwellenwertsystematik
- Akteure in der Regulierung und Kontrolle

10:00

Inhalte der aktuellen Regulierung

- KRITIS-Gesetz und KRITIS-Verordnung
- Inhalte der Vorgaben zur IT-Sicherheit
- Exkurs Störfallbetriebe und weitere regulierte Unternehmen
- Praxiserfahrungen und Bewertung des IST-Standes

10:45

Kaffeepause

11:15

Zukunft NIS2, CER und KRITIS-Dachgesetz

- EU-Regulierung
- Umsetzungsstand
- Handlungsaufgaben

12:00

Hyperrisiko Blackout

- Definition Blackout
- Digitalisierung, vernetzte Gesellschaft und Normal Accidents Theory
- Eintrittswahrscheinlichkeit und Schadensausmaß
- Fallbeispiele in Deutschland
- Auswirkungen in einer Gemeinde: Beispiel eines Hands-on-Forschungsprojekts

12:45

Mittagspause



13:45

Modell organisationaler Resilienz

- Bewältigungsfähigkeit und Widerstandskraft
- Innere Verfasstheit und Kooperation nach außen
- Bottom-up Konzept gesellschaftlicher Resilienz
- Kritische Prozesse als Ergänzung zu Kritischen Infrastrukturen

14:30

Fokus Krisenmanagement

- Definition und Abgrenzung
- Projektmanagement vs. Krisenstabsarbeit
- Mindestanforderungen an Krisenorganisationen

15:15

Kaffeepause

15:45

Workshop

- Praxisübung zur Krisenstabsarbeit
- Auswertung und Diskussion resilienzfördernder Faktoren

16:30

Ende des Seminars



Rico Kerstan

Rico Kerstan, MBA, verfügt über langjährige Erfahrung als Berater, Coach und Auditor sowie im Sicherheitsmanagement der Bundesdruckerei GmbH in Berlin. Er ist als Unternehmensberater tätig. Seine aktuellen Tätigkeitsschwerpunkte sind Krisenmanagement, Risikomanagement und Informationssicherheit. Herr Kerstan ist Träger des Hamburger Sicherheitspreises 2021/22. Sein Beitrag befasste sich mit der Frage der Zusammenarbeit unterschiedlicher Organisationen sowie staatlicher und privatwirtschaftlicher Akteure im Krisenmanagement. Herr Kerstan verfügt über einen Abschluss als Bachelor of Engineering (B. Eng.) in Gefahrenabwehr. Er ist als Lehrbeauftragter für Sicherheitsmanagement an der HWR Berlin und an der NBS Northern Business School Hamburg tätig.



Dr. André Röhl

Prof. Dr. André Röhl ist Professor und Studiengangsleiter für Sicherheitsmanagement an der NBS Northern Business School in Hamburg. Der promovierte Verwaltungswissenschaftler und Organisationspsychologe (Master) berät freiberuflich Unternehmen und Organisationen bei der Verbesserung der Sicherheitsmanagementstrukturen. Seine Schwerpunkte sind die Personalorganisation und -entwicklung sowie der Aufbau und die Entwicklung von wirksamen Sicherheitsstrukturen.

Zielgruppe – An wen richtet sich dieses Seminar?

Das Praxisseminar richtet sich an Führungskräfte, MitarbeiterInnen und SachbearbeiterInnen, für die Aspekte der Sicherheit interessant sind, beispielsweise aus den Bereichen:

- Informationssicherheit
- Datensicherheit
- Risikomanagement / Krisenprävention
- Zentrale Dienste
- Organisation
- (Digitale) Transformation
- Behördenleitung
- Amtsleitung
- Finanzen, Finanzsteuerung
- Kämmerei
- Haushalt
- u.v.m.

Die Inhalte des Seminars sind relevant für öffentliche Institutionen und öffentliche Unternehmen wie:

Städte, Landkreise, Kommunen und Verbandsgemeinden, Ministerien auf Bundes- und Landesebene, nachgeordnete Behörden und Betriebe von Bund und Ländern, Unternehmen der öffentlichen Hand und Betriebe gewerblicher Art (BgA), gemeinnützige und kirchliche Einrichtungen, Religions- und Weltanschauungsgemeinschaften, Universitäten, Universitätskliniken, Fachhochschulen sowie Forschungseinrichtungen, Finanz- und Prüfbehörden, öffentliche Versicherer, Verbände, Vereine und Stiftungen, Verbandsgemeinschaften, Kammern, Landesförderbanken, Staatskanzleien sowie Kliniken, Krankenhäuser, Rechenzentren, infrastrukturelle und weitere Einrichtungen und Organisationen der öffentlichen Hand.



Termin:

22.04.2024

online

TEILNAHMEGEBÜHR:

Online-Teilnahme: 399,- Euro zzgl. MwSt.

Details zur Anmeldung unter www.fortbildungskampagne.de/anmeldung

DIE TEILNAHMEGEBÜHR BEINHALTET:

- Schulungsunterlagen (digital)
- Teilnahmezertifikat

ANMELDUNG:

Bitte verwenden Sie zur Anmeldung unser Online-Anmeldeformular unter: www.fortbildungskampagne.de/anmeldung

KONTAKT FÜR RESERVIERUNGEN UND BUCHUNGEN:

Haben Sie Fragen zum Seminar oder zu Reservierungen und Buchungen?

Schreiben Sie uns einfach eine Email oder rufen Sie uns unter der folgenden Rufnummer an:

Email: team@fortbildungskampagne.de | Telefon: +49 (0) 30 89 56 27 16

TEILNAHME- UND STORNIERUNGSKONDITION (AUSZUG):

Die verbindliche Anmeldung erfolgt über unser Online-Anmeldeformular und wird durch Zusendung einer Anmeldebestätigung sowie der Rechnung bestätigt. Stornierungen sind bis vier Wochen vor Veranstaltungsbeginn kostenfrei, bereits gezahlte Beträge werden erstattet. Bei kurzfristiger Stornierung oder beispielsweise krankheitsbedingter Abwesenheit ist die Benennung eines Ersatzteilnehmers jederzeit möglich. Sofern sich kein Ersatzteilnehmer findet, kann nach Absprache ein Gutschein ausgestellt werden, der zur Teilnahme an einem Nachfolgetermin oder einem ähnlichen Seminar berechtigt. Bitte beachten Sie unsere AGB, die unter dem folgenden Link aufgerufen werden können:

www.fortbildungskampagne.de/agb

DATENSCHUTZHINWEISE:

Wir weisen darauf hin, dass Sie die Verwendung Ihrer Daten gemäß unserer Datenschutzbestimmungen durch eine Nachricht an datenschutz@fortbildungskampagne.de selbstverständlich jederzeit widerrufen können. Bitte beachten Sie unsere Datenschutzbestimmungen, die unter dem folgenden Link aufgerufen werden können:

www.fortbildungskampagne.de/privacy

HINWEISE ZUM DATENSCHUTZ BEI ONLINE-TEILNAHME:

Details zur technischen Umsetzung der Online-Teilnahme erhalten Sie im Anschluss an Ihre Anmeldung. Ein wirksamer Auftragsverarbeitungsvertrag mit dem technischen Dienstleister liegt vor. Durch die Fortbildungskampagne als Veranstalter erfolgt während der Online-Teilnahme keine Speicherung von schriftlichen, akustischen oder visuellen Daten der Teilnehmenden. Eine temporäre Protokollierung des Chat-Verlaufes einer Online-Veranstaltung wird binnen zwei Arbeitstagen nach der Veranstaltung gelöscht. Bitte beachten Sie, dass Sie im Rahmen Ihrer Online-Teilnahme möglicherweise unfreiwillig Daten und Informationen übertragen, etwa durch weitere Personen in Ihrem Raum. Eine mögliche Übertragung derartiger Informationen liegt in Ihrem Verantwortungsbereich.