

Intensivkurs

IT-Notfallmanagement

Ein praktischer Leitfaden für effektive Notfallmassnahmen, Business Continuity und Disaster Recovery

29. und 30. September 2010 in Zürich
17. und 18. November 2010 in Zürich

vereon.ch

»« VEREON
know-how for your success

Kursleiter



Priv.-Doz. Dr. Heinrich Kersten



Dr. Gerhard Klett

Highlights aus dem Programm

- + Methoden zur Risikoanalyse und -bewertung wie Risk Analysis, Business Impact Analysis oder Kritikalitätsanalyse korrekt anwenden
- + Notfallkonzepte und Notfallhandbücher als Arbeitsanweisung für den Notfall
- + Schnittstellen zu Change-, Configuration-, Problem- und Service Level Management
- + Konkrete Massnahmen bei typischen Notfällen in der Informationsverarbeitung: Ausfall zentraler IT-Systeme, Manipulationen oder mangelnde Compliance
- + Planung und Durchführung von Übungen für Notfälle und Wiederanlaufplanung
- + Praxiserfahrungen mit Business Continuity nach ISO 27001
- + Standards für das Notfallmanagement und Sicherheitskonzepte
- + Key Performance Indicators für Reviews und Audits festlegen

1. Tag: Business Continuity

INHALTE DIESER VERANSTALTUNG

Risikoanalyse und -bewertung

Viele Organisationen haben die Sinnhaftigkeit und Vorteile eines Sicherheitsmanagements für ihre Informationsverarbeitung erkannt: Es werden mögliche Sicherheitsvorfälle nach Eintrittshäufigkeit und Schadenhöhe analysiert und daraus Risiken für die Organisation abgeleitet, klassifiziert und bewertet. Zumindest bei höheren Risiken versucht man, diese durch geeignete "präventive" Massnahmen unter eine noch akzeptable Grenze zu drücken. Weiterhin ist der Compliance-Aspekt zu beachten, der eine Beschäftigung z.B. mit ISO 27001, dem IT-Grundschutz oder weiteren Regularien erfordern kann.

Risikokategorisierung

Nimmt man sich die Ergebnisse der Risikoanalyse und -bewertung vor, so erkennt man schnell, ob es Risiken gibt, die bei ihrem Eintritt einen gravierenden oder sogar Existenz bedrohenden Schaden für die Organisation nach sich ziehen können. Ereignisse dieser Kategorie bezeichnet man als Notfälle. Massgebend ist also die mögliche Schadenhöhe im Einzelfall - weniger die Häufigkeit des Eintritts.

Typische Notfälle in der IT

Um welche Vorfälle handelt es sich üblicherweise? Dazu einige Beispiele:

- Beim Ausfall wichtiger IT-Anwendungen und IT-Systeme geht es darum, möglichst schnell wieder in einen Normalzustand zu kommen - ggf. auch mit Überbrückung durch einen Notbetrieb -, um Umsatzverluste oder Vertragsstrafen zu vermeiden.
- Ein wichtiger Service oder ein System ist in hohem Masse gestört und stellt ein Desaster dar; eine Rückkehrprozedur zum vollen Leistungsumfang ist erforderlich.
- Manipulationen an Daten und Anwendungen durch einen Innentäter sind erkannt worden; Ziel muss es sein, dessen Aktivitäten so schnell wie möglich zu unterbinden und auf einem sicheren früheren Stand der Daten und Anwendungen aufzusetzen.
- Bei Ausfall eines Dienstleisters (z.B. Netzwerk-Provider) sollen durch "Umschaltung" auf einen anderen Dienstleister Verluste und Ausfallzeiten minimiert werden.
- Wird aufgrund fehlender Compliance bei einem Rechenzentrum z.B. von einer Aufsichtsbehörde eine Betriebseinstellung verfügt, resultiert dies möglicherweise in einem massiven Umsatzverlust; hier geht es um eine kurzfristige, nachweisbare Wiederherstellung der Compliance, so dass der Betrieb fortgesetzt werden kann.

Notfallmanagement

Solche Vorfälle können bei ihrem Eintritt bereits Notfälle darstellen oder aber sich in kurzer Zeit dazu auswachsen. In diesen Fällen kommt es also darauf an, durch schnelle sachgerechte Entscheidungen und trainierte, qualitativ überwachte, Vorgehensweisen (Notfallübungen) die Auswirkungen auf die Geschäftstätigkeit und die Verluste der Organisation zu begrenzen. Dieses "reaktive" Vorgehen ist eine zentrale Aufgabe des Notfallmanagements zur Beherrschung von Notfällen.

Konkrete Massnahmen ergreifen

Einige konkrete Massnahmen im Rahmen des Notfallmanagements dienen zur rascheren Beherrschung der Situation:

- Erforderlichen Organisationsstrukturen mit ihren Rollen, Prozessen und Dokumentationen (u.a. Notfallkonzept, Notfallhandbuch) einrichten
- Schnittstellen zu bereits existierendem Change-, Configuration-, Problem- und Service Level Management definieren und betreiben
- Wesentliche Methoden (Risk Analysis, Business Impact Analysis, Kritikalitätsanalyse) anwenden
- Notfallübungen planen
- Key Performance Indicators für die Reviews und internen/externen Audits festlegen
- Massnahmen umsetzen, z.B. Notfall- und Wiederanlaufplanung

AGENDA ERSTER TAG

Leitung: Dr. Gerhard Klett

09:00

Begrüssung und Eröffnung

- Programmübersicht
- Vorstellung
- Organisatorisches

Relevanz von Business Continuity

- Zielsetzung der Business Continuity
- Compliance-Aspekte
- Grundsätzliche Erfahrungen

10.15 - 10.30 Kaffeepause

Organisation von Notfallmassnahmen

- Rollen und Zuständigkeiten
- Notfallplanung für kritische Geschäftsprozesse
- Schnittstellen zu ITIL
- Auditierung von Notfallmassnahmen

12.00 - 13.00 Gemeinsames Mittagessen

Bedeutung von Change-, Configuration- und Risk-Management

- Überbrückungsmassnahmen
- Wiederanlaufplanung / Disaster Recovery
- Notfallübungen

Unterstützung durch Tools

- TNG Advanced Helpdesk (AHD)
 - Automatisierung von Serviceprozessen
 - Zentrales Repository für Problemmangement
 - Monitoring von Serviceprozessen, Überwachung von festgelegten Bearbeitungszeiten
- BS 25999-2 Business Continuity Selfassessment Online Tool
- Business Impact Assessment Tool
- Business Continuity Checklist Tool

15.15 - 15.30 Kaffeepause

Praxiserfahrungen mit Business Continuity nach ISO 27001

- Darstellung der Controls
- Business Continuity und Zertifizierung

2. Tag: Business Impact Analysis und IT-Grundschutz

17:00 Ende erster Tag

AGENDA ZWEITER TAG

Leitung: Priv.-Doz. Dr. Heinrich Kersten

09:00

Begrüssung und Eröffnung zweiter Tag

- Programmübersicht
- Vorstellung
- Organisatorisches

Business Impact Analysis (BIA)

- Ermitteln kritischer Geschäftsprozesse
- Einführung in die Methode der BIA
- Anwendung der BIA anhand konkreter Beispiele
- Verfügbare Hilfsmittel

10.15 - 10.30 Kaffeepause

Dokumentation beim Notfallmanagement

- Notfallkonzept als Planungsgrundlage
- Notfallhandbuch als Praxisgrundlage
- Notfall- und Wiederanlaufpläne als Arbeitsanweisungen für den Notfall
- Aufzeichnungen und Auswertungen über Notfälle

12.00 - 13.00 Gemeinsames Mittagessen

Notfallmanagement nach BSI 100-4

- Inhalte und Bedeutung des IT-Grundschutz
- BSI-Standards 100-x
- Bausteinkatalog, Massnahmenkatalog, Gefährdungskatalog
- Vorgehensmodell gemäss Schutzbedarf

15.15 - 15.30 Kaffeepause

Sicherheitskonzepte nach IT-Grundschutz

- Normaler Schutzbedarf
 - IT-Verbund beschreiben
 - Schutzbedarfsermittlung
 - Massnahmenkonsolidierung und Umsetzungsplanung
- Höherer Schutzbedarf
 - Erweiterte Analyse nach BSI-Standard 100-3
 - Anwendung der Gefährdungskataloge
 - Massnahmen erweitern und validieren

Massnahmen zur Notfallprävention

- Sicherheitsleitlinien und -konzepte
- Risk Management
- Incident Management

17:00 Ende zweiter Tag

IHRE KURSLEITER

Dr. Gerhard Klett verfügt durch seine langjährige Tätigkeit als Senior Security Consultant bei der BASF SE und der BASF IT Services GmbH im Fachgebiet Informatik-Sicherheit und Netzwerke über umfangreiche Praxiserfahrung. Er leitete die Planung und den Aufbau der gesamten IT-Infrastruktur der Verwaltung der RAO Gazprom in Moskau, einer der grössten Joint-Venture Partner der BASF. Seine Arbeitsschwerpunkte als Leiter des Departments "IT Security-Solutions" bei der BASF IT Services GmbH waren Security Consulting, Risikomanagement und Compliance für ISO 27001, Zertifizierung und Sarbanes Oxley (SOX), Security für E-Commerce, sichere Kommunikation und Authentifizierung, Public Key Infrastructure (PKI), E-Mail-Sicherheit sowie Schwachstellenanalyse und Security Scans. Heute führt er die IT-Security Beratungsfirma GK IT-Security Consulting.

Priv.-Doz. Dr. Heinrich Kersten war Leiter der Zertifizierungsstelle bei der T-Systems GEI GmbH, Bonn, sowie stellvertretender Leiter des Sektorkomitees "Security" beim Akkreditierer DATECH. In seiner Tätigkeit bei T-Systems hat Dr. Kersten Unternehmen in Belangen der Informationssicherheit auditiert und zertifiziert. Weitere umfangreiche Berufserfahrung konnte Dr. Kersten unter anderem bei der Bayer AG und während seiner Tätigkeit beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Leitender Regierungsdirektor und Abteilungsleiter für "Wissenschaftliche Grundlagen und Zertifizierung" sammeln. Beim BSI war er u.a. mit der Produktzertifizierung und der Weiterentwicklung und Anwendung von Sicherheitsstandards befasst.

WER SOLLTE TEILNEHMEN?

Geschäftsführer, CIO, Leiter IT, Notfallbeauftragte, Incident Manager sowie Sicherheitsverantwortliche und Datenschutzbeauftragte. Darüber hinaus Führungskräfte und Mitarbeiter der Bereiche

- IT-Sicherheit
- IT-Risikomanagement
- IT-Revision
- Datenschutz und -sicherheit
- Betriebliche Sicherheit

AKTUELLE VERANSTALTUNGSHINWEISE

Sicherheit Mobiler Endgeräte

15. September 2010, Zürich
www.vereon.ch/sme

SEPA und SAP

15. September 2010, Zürich
www.vereon.ch/sus

Datenschutz aktuell

23. September 2010, Zürich
www.vereon.ch/dsa

SAP-Berechtigungskonzept

16. November 2010, Zürich
www.vereon.ch/sbk

IT-Notfallmanagement

Ja, hiermit melde ich mich an für:

29. und 30. September 2010, Zürich

17. und 18. November 2010, Zürich

Die Teilnahmegebühr beträgt pro Person und Termin für zwei Tage CHF 2'295.- zzgl. 7.6 % MwSt.

1. PERSON

Anrede, Titel

Name, Vorname

Position, Abteilung

E-Mail

Firma

Strasse, Nr.

Postfach

PLZ, Ort

Land

2. PERSON

Anrede, Titel

Name, Vorname

Position, Abteilung

E-Mail

RECHNUNGSDetails

Bestellreferenz

MwSt.-Nr.

Firma

Abteilung

Strasse, Nr.

PLZ, Ort

Datum, Unterschrift

Bei Zahlung per Kreditkarte bitte ausfüllen

Karteninhaber

Kartenummer

gültig bis



5 WEGE ZUR ANMELDUNG

Web vereon.ch
Telefon +41 71 677 8700
Fax +41 71 677 8701
E-Mail anmeldung@vereon.ch
Post Vereon AG
Postfach 2232
8280 Kreuzlingen
Schweiz

VERANSTALTUNGSORTE

Die Veranstaltungen finden jeweils in zentraler Lage und in gehobenem Ambiente statt. Weitere Details senden wir Ihnen rechtzeitig vor den jeweiligen Terminen per E-Mail.

TEILNAHMEBEDINGUNGEN

Geltungsbereich

Diese Teilnahmebedingungen regeln das Vertragsverhältnis zwischen dem Veranstalter und dem Teilnehmer. Der Teilnehmer erkennt mit seiner Anmeldung diese Teilnahmebedingungen an. Abweichende Allgemeine Geschäftsbedingungen des Teilnehmers haben keine Gültigkeit.

Teilnahmegebühr

Die Teilnahmegebühr beinhaltet die Teilnahme für eine Person. Sie versteht sich inklusive schriftlicher Unterlagen, Mittagessen und Tagungsgetränke zzgl. MwSt. Nach Eingang Ihrer Anmeldung erhalten Sie eine Anmeldebestätigung und eine Rechnung. Diese ist direkt nach Erhalt, in jedem Fall vor Eintritt in die Veranstaltung fällig.

Anmeldung

Die Anmeldung kann schriftlich via Internet, E-Mail, Fax oder per Post oder mündlich per Telefon erfolgen. Sie ist, vorbehaltlich gesetzlicher Widerrufsrechte, verbindlich. Jede Anmeldung erlangt erst durch schriftliche Bestätigung seitens des Veranstalters Gültigkeit. Die Veranstaltungsteilnahme setzt die vollständige Bezahlung der Teilnahmegebühr voraus.

Urheberrecht

Alle im Rahmen der Veranstaltungen ausgegebenen Unterlagen sowie anderweitig erworbene Artikel sind urheberrechtlich geschützt. Vervielfältigungen und anderweitige Nutzung sind schriftlich durch den Veranstalter zu genehmigen.

Rücktritt des Teilnehmers

Sollte der Teilnehmer an der Teilnahme verhindert sein, so ist er berechtigt jederzeit ohne zusätzliche Kosten einen Ersatzteilnehmer zu benennen. Darüber hinaus ist eine vollständige Stornierung bis 30 Tage vor Beginn der Veranstaltung kostenlos möglich. Die Stornierung bedarf der Schriftform. Bei späterem Rücktritt oder Nichterscheinen wird die gesamte Teilnahmegebühr fällig.

Programmänderungen und Absagen

Der Veranstalter behält sich vor, Änderungen am Inhalt des Programms sowie Ersatz und Weglassen der angekündigten Referenten vorzunehmen, wenn der Gesamtcharakter der Veranstaltung gewahrt bleibt. Muss eine Veranstaltung aus wichtigem Grund oder aufgrund höherer Gewalt (kriegerische Auseinandersetzungen, Unruhen, terroristische Bedrohungen, Naturkatastrophen, politische Beschränkungen, erhebliche Beeinflussung des Transportwesens usw.) abgesagt oder verschoben werden, so wird der Veranstalter die zu diesem Zeitpunkt angemeldeten Teilnehmer umgehend schriftlich oder mündlich benachrichtigen. Bereits eingegangene Zahlungen werden für eine zukünftige Veranstaltung gutgeschrieben oder bei einer Terminverschiebung auf den neuen Termin ausgestellt. Kosten seitens des Teilnehmers, die mit der Absage einer Veranstaltung verbunden sind (z.B. Reise- und Übernachtungskosten), werden nicht erstattet.

Haftung

Alle Veranstaltungen werden sorgfältig recherchiert, aufbereitet und durchgeführt. Sollte es dennoch zu Schadensfällen kommen, so übernimmt der Veranstalter keine Haftung für die Vollständigkeit und inhaltliche Richtigkeit in Bezug auf die Vortragsinhalte und die ausgegebenen Unterlagen.

Datenschutz

Überlassene persönliche Daten behandelt der Veranstalter in Übereinstimmung mit den geltenden datenschutzrechtlichen Bestimmungen. Sie werden zum Zwecke der Leistungserbringung elektronisch gespeichert. Einblick und Löschung der gespeicherten Daten kann jederzeit gefordert werden. Anfragen bitte per Email an: info@vereon.ch.

Schlussbestimmungen

Der Vertrag unterliegt dem schweizerischen Recht. Gerichtsstand ist Kreuzlingen (Schweiz).



Jetzt anmelden www.vereon.ch/inm