Intensivkurs

IT-Sicherheitsgesetz

Management der IT-Sicherheit und der Business Continuity

14. und 15. Juni 2016, Frankfurt am Main
15. und 16. November 2016, Düsseldorf

vereon.ch

vereon
know-how for your success

Ihre Referenten

RA Hans-Joachim Hess

Dr. Heinrich Kersten

Dr. Gerhard Klett

Bringen Sie Ihre bestehenden Infrastrukturen, Vorgaben und Regelungen in Einklang mit den Anforderungen des Gesetzes:

- Aktueller Stand der Gesetzgebung und der Rechtsprechung
- Sicherheitsmanagement nach Stand der Technik
- Anwendung von IT-Grundschutz oder ISO 27001
- Übersicht der Pflichten, denen Sie sich gegenübersehen
- Effektive Vorbereitung und Durchführung von Audits
- Einsatz von Branchenkatalogen am Beispiel Energiewirtschaft
- Integration von Cloud Services und mobiler IT unter Berücksichtigung des IT-Sicherheitsgesetzes

Konkrete Anforderungen aus juristischer Sicht und Umsetzung in der Praxis

ABSTRAKT

Seit dem 24.07.2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, kurz IT-Sicherheitsgesetz, durch die Veröffentlichung im Bundesgesetzblatt rechtskräftig.

Bereits ein erster Blick auf die neu getroffenen Regelungen wirft Fragen auf, wie die Anforderungen des Gesetzes mit bestehenden Infrastrukturen, Vorgaben und Regelungen in Einklang zu bringen sind. Die Betreiber Kritischer Infrastrukturen (KRITIS) werden durch den Artikel 1 des IT-Sicherheitsgesetzes verpflichtet, den „Stand der Technik“ für den Schutz ihrer IT-Systeme anzuwenden – womit die bestehende Regelung des §9 BDSG zum technischen Schutz personenbezogener Daten auf die Sicherheit von IT-Systemen in Kritischen Infrastrukturen übertragen wird.

Die Bewertung der IT-Sicherheit beruht auf einer Risikoanalyse und -bewertung, wobei die betroffenen Unternehmen alle 2 Jahre durch ein Audit nachweisen müssen, dass sie die aus der Risikobewertung abgeleiteten Anforderungen erfüllen. Damit dürfte der Einsatz eines "Informationssicherheitsmanagementsystems" (ISMS), etwa auf der Basis der ISO27001 oder des IT-Grundschutzes, zwingend erforderlich werden.

Davon unabhängig sind auch Sicherheitskataloge zugrundezulegen, die von den Branchenverbänden und anderen Stellen herausgegeben werden und Mindestanforderungen an die Sicherheit beinhalten. Ein solcher Katalog existiert bereits für den Bereich der Energiewirtschaft.

Der bisher, beispielsweise im Bundesdatenschutzgesetz, geforderte „Stand der Technik“ berücksichtigt zwar die Veränderungen in der Informationstechnik, ist aber statisch im Vergleich zu einer Risikobewertung nach ISO27001/27005. Diese analysiert im Detail für jeden Anwendungsfall die Eintrittswahrscheinlichkeit und die Schadenshöhe eines Ereignisses und definiert daraus ein zu behandelndes Risiko.

Dabei ändern sich Risiken mit jeder neuen IT-Sicherheitslücke. Zudem beinhaltet die Bewertung der Risiken einen hochdynamischen und stetig zu aktualisierenden Analyseprozess, dessen Komplexität in modernen IT-Umgebungen erheblich sein kann.

AGENDA TAG 1

Das neue IT-Sicherheitsgesetz: Was sind die konkreten Anforderungen und was müssen Sie tun?

- Was fordert das neue Gesetz?
- Welche neuen Pflichten ergeben sich für die Unternehmen?
- Wie kann das neue Gesetz mit anderen gesetzlichen Anforderungen in Einklang gebracht werden?
- Wie können die Anforderungen konkret im Unternehmen umgesetzt werden?
- Warum ist ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 das Mittel der Wahl?
- Welche Sicherheitsvorfälle sind meldepflichtig?
- Wie sieht das Meldeverfahren aus?
- Wie detailliert muss die Untersuchung des Vorfalls erfolgen?

Hans-Joachim Hess

Praktische Umsetzung des IT-Sicherheitsgesetzes - Übersicht

Sicherheitsmanagement nach Stand der Technik

- Einrichtung und Betrieb eines ISMS nach der neuen ISO 27001
- Leitlinien und Richtlinien mit Anwendungsbeispielen
- Praxis-Beispiele für die Risikoanalyse und -bewertung
- Effektive Vorbereitung und Durchführung von Audits
- Alternative Vorgehensweise nach dem IT-Grundschutz

Aufrechterhaltung wesentlicher Geschäftsprozesse

- Grundlagen Business Continuity Management
- Praktische Durchführung einer Business Impact Analysis
- Notfall- und Wiederanlaufpläne

Integration von sog. Branchenkatalogen

- Grundsätzliches im Überblick
- Beispiel der Energiewirtschaft

AGENDA TAG 2

Erweiterung des Risikomanagements in Verbindung mit dem IT-Sicherheitsgesetz

Umsetzung der Schutz-Maßnahmen aus den Sicherheitskatalogen und dem ISMS:

Praxisbeispiele zu:

- Sicherheitsrichtlinien (statische, dynamische und mobile Komponenten)
- Organisation der Informationssicherheit
- Zugriffskontrolle
- Schutz vor physischem Zugang
- Betriebssicherheit
- Sicherheit in der Kommunikation
- Management und Meldung von Sicherheitsvorfällen
- Informationssicherheitsaspekte des Business Continuity Management (BCM)

Erweiterungen für Cloud Services und mobile Infrastrukturen

- Governance und Compliance bei der Integration von Cloud Services und Mobile IT in die IT-Infrastruktur unter Berücksichtigung des IT-Sicherheitsgesetzes, BDSG und EU-GVO
- Cloud Access Security Brokerage (CASB)

ZEITSCHEMA

08:30	Empfang und Ausgabe der Unterlagen
09:00	Beginn des Intensivkurses an Tag 1 und 2
10:30 – 11:00	Kaffeepause
12:30 – 13:30	Gemeinsames Mittagessen
15:00 – 15:15	Kaffeepause
17:00	Ende des Intensivkurses an Tag 1 und 2

ZIELGRUPPE

- IT-Leitung und IT-Verantwortliche
- IT-Sicherheitsbeauftragte
- Auditoren
- Revisoren
- IT-Sicherheitsberater

vor allem aus den Bereichen Energie, Information/Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen.

IHRE REFERENTEN

Hans-Joachim Hess ist Seniorpartner der Kanzlei Hess&Partner Rechtsanwälte in Küsnacht/ZH und Konsulent der Kanzlei Passarge Prudentino & Rhein in Hamburg/D. Zudem leitet er seit 1991 das EBDI, Institut für technische Sicherheitsberatung in Küsnacht. Schon während seiner Tätigkeit bei der EU-Kommission 1985-1986 (Rechtsdienst) hat er sich intensiv mit Fragen der europäischen Produktsicherheit und Produkthaftung befasst. Heute berät er als Spezialist für Schweizer und europäisches Haftpflichtrecht zahlreiche Unternehmen im In- und Ausland. Seine Beratungsschwerpunkte: Produktehaftung und –sicherheit, CE-Kennzeichnung, Krisenmanagement und Notfallplan, Normenwesen, Technische Dokumentation, Qualitätsmanagement. Neben seinen zahlreichen Publikationen in der Schweiz und Deutschland ist er Verfasser der Gesetzeskommentare zum Schweizer Produktehaftpflichtgesetz und zum Schweizer Produktesicherheitsgesetz. Zudem ist er als Referent und Schulungsleiter tätig.

Dr. Heinrich Kersten war Leiter der Zertifizierungsstellen bei debis (DaimlerChrysler) und der T-Systems. Er hat viele 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. Dr. Kersten ist erfolgreicher Fachbuchautor zu Themen der IT-Sicherheit.

Dipl.Ing. Dr. Gerhard Klett war Senior Security Consultant und Compliance Manager bei BASF SE und BASF IT Services. Im Rahmen dieser Tätigkeit leitete er das Department "IT Security Solutions" mit den Schwerpunkten Aufbau und Betrieb interner Kontrollsysteme, Compliance Management zu ISO27001 und Sarbanes-Oxley Act sowie Security Policies und Risiko-Management. Er ist Fachbuchautor und veröffentlichte zahlreiche Artikel zur IT-Sicherheit.

Anmeldung «IT-Sicherheitsgesetz»

Ja, hiermit melde ich mich für folgenden Termin an:

- ☐ 14. und 15. Juni 2016, Frankfurt am Main
- ☐ 15. und 16. November 2016, Düsseldorf

Die Teilnahmegebühr beträgt pro Person und Termin EUR 2'195 zzgl. 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

☐ Ich möchte mit Kreditkarte bezahlen. Bitte senden Sie mir den Zahlungslink mit der Anmeldebestätigung per E-Mail zu.

KONTAKTIEREN SIE UNS

Web	vereon.ch
E-Mail	anmeldung@vereon.ch
Fax	+41 71 677 8701
Post	Vereon AG Postfach 2232 8280 Kreuzlingen 1 Schweiz

VERANSTALTUNGSORT

Details zu den jeweiligen Veranstaltungshotels erhalten Sie mit Ihrer Anmeldebestätigung 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 sind urheberrechtlich geschützt. Vervielfältigungen und anderweitige Nutzung sind schriftlich durch Vereon AG zu genehmigen. Sie dürfen Aufnahmegeräte ausschliesslich für private Zwecke nutzen. Professionelle Fotografier- und sonstige Aufnahmetechnik sind nicht gestattet. Durch Ihre Teilnahme stimmen Sie zu, dass Sie fotografiert, gefilmt und aufgenommen werden können. Falls nicht anderweitig mit Vereon AG vereinbart, stimmen Sie zu, dass Vereon AG und Dritte Bild- und weitere Aufnahmen von Ihnen zur weiteren Verwendung und Veröffentlichung ohne Vergütung verwenden dürfen.

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 E-Mail an: adressen@vereon.ch.

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

vereon
know-how for your success

Jetzt anmelden: www.vereon.ch/isg