

zwecks Aufbaus der Fachkunde der ernannten Datenschutzverantwortlichen bietet die Swiss Infosec AG neu den Lehrgang **Betrieblicher Datenschutzverantwortlicher** an. **Hier erfahren Sie weitere Details.**

Wir unterstützen Sie. Möchten Sie einen Ressourcenengpass überbrücken? Unsere Spezialisten stehen Ihnen schnell, kompetent und flexibel zur Seite. **Hier erfahren Sie mehr.** Für unsere zahlreichen, interessanten Aufgaben und Mandate suchen wir motivierte und gut ausgebildete Fachspezialisten. **Hier geht es weiter zu den Stellenangeboten der Swiss Infosec AG.**

Swiss Infosec AG präsentiert Ihnen folgende **Special Events** in den nächsten Monaten:

16.-17.09.2008 Olten	Intensivseminar mit Beat Lehmann , Jurist Revision Datenschutzgesetz DSG: Wie kann Datenschutz heute optimal umgesetzt werden? Weitere Informationen
29.-30.10.2008 Olten	Intensivseminar mit Beat Lehmann , Jurist Sicherheitsüberprüfungen von IT-Systemen, Ethical Hacking und Social Engineering Rechtliche Grundlagen und Hürden Weitere Informationen
11.-12.11.2008 Thalwil	Intensivseminar mit Frank Roselieb , Vorstandsmitglied der Deutschen Gesellschaft für Krisenmanager e.V. Krisen erkennen, bewältigen und erfolgreich meistern Wie sich Schweizer Unternehmen und Behörden auf den Ernstfall vorbereiten können Krisensimulation, Fallbeispiele und Empfehlungen Weitere Informationen
18.11.2008 Thalwil	Intensivseminar mit Prof. Dr. Sachar Paulus , ehemaliger Senior Vice President für Produktsicherheit bei SAP SAP-Sicherheit: Trends, Tipps und Tricks für den Umgang mit Risiken Wie Sie Ihre wichtigsten Daten erfolgreich schützen können Weitere Informationen
15.-16.12.2008 Thalwil	Intensivseminar mit Detlev Sachse , SAP-Berater Sicherheit und Auditing eines SAP-Systems für Auditoren, Sicherheitsbeauftragte und Interessierte Weitere Informationen
02.04.2009 Thalwil	Intensivseminar mit Dr. Ulrich Zwygart , Global Head Learning and Development der Deutschen Bank in London Wie trifft man Entscheidungen in schwierigen Situationen? Erfolgsfaktoren in der Entscheidungsfindung Weitere Informationen

Sie erhalten bereits seit einiger Zeit unsere Internet Infosec News als Abonnent. Die Internet Infosec News behandeln seit 1995 aktuelle Themen und Sicherheitsvorkommnisse im Bereich der Informations- und IT-Sicherheit.

CONSULTING



+ **aktuelle Ressourcenengpässe überbrücken**

- + Auditing
- + SCADA Security
- + Social Engineering
- + Security Management
- + Penetration Testing

AUSBILDUNG



+ **Elektronische Archivierung**

- + eLearning
- + Security Edutainments
- + ISO 27001 Lead Auditor
- + Datenschutzverantwortlicher
- + IT-SIBE
- + Integraler Sicherheitsmanager

INFOS



+ **Informationen anfordern**

Swiss Infosec AG
Centralstrasse 8A
CH-6210 Sursee

Maulbeerstrasse 10
CH-3001 Bern

Steinstrasse 21
CH-8036 Zürich

Fon +41 (0)41 984 12 12
Fax +41 (0)41 984 12 24
www.infosec.ch

Es ist uns ein grosses Anliegen, dass unsere News nur dort ankommen, wo diese erwünscht sind. Sollten Sie unseren Newsletter zukünftig nicht mehr wünschen, so können Sie diesen jederzeit entweder durch Betätigen des entsprechenden Links am Ende dieses E-Mails oder durch persönliche oder telefonische Kontaktnahme, Telefon +41 (0)41 984 12 12, abbestellen.

infosec@infosec.ch

THEMENÜBERSICHT



AKTUELLE MELDUNGEN

- Die Laptops der US-Regierung sind immer noch unverschlüsselt
- US-Grenzbeamte schnüffeln ohne Verdacht
- Security-Policies gegen Datenverlust noch Mangelware
- Qualität der BCM-Krisenpläne lässt zu wünschen übrig
- Mobility kann eine Gefahr für die Firma sein
- Grossteil der Unternehmen verwundbar
- eDiscovery und Sanktionen der US-Gerichte
- Was ist Compliance?
- Risiken beim IT-Outsourcing
- Sind die Datenschutzgesetze europaweit veraltet?
- Schnelltest für Euro-SOX-Compliance
- Das deutsche Bundeskabinett verabschiedet Gesetz zum biometrischen Personalausweis



EVENTS

- Jetzt anmelden! Einladung zur **ISMS Tool Box Roadshow** vom 11.09.2008
- Special Event mit **Beat Lehmann** am 16. - 17.09.2008: Revision Datenschutzgesetz DSG: Wie kann Datenschutz heute optimal umgesetzt werden?
- Special Event mit **Beat Lehmann** am 29. - 30.10.2008: Sicherheitsüberprüfungen von IT-Systemen
- Special Event mit **Frank Roselieb** am 11. - 12.11.2008: Krisen erkennen, bewältigen und erfolgreich meistern
- Special Event mit **Prof. Dr. Sachar Paulus** am 18.11.2008: SAP-Sicherheit: Trends, Tipps und Tricks für den Umgang mit Risiken
- Special Event mit **Detlev Sachse** am 15. - 16.12.2008: Sicherheit und Auditing eines SAP-Systems
- Special Event mit **Dr. Ulrich Zwygart** am 02.04.2009: Wie trifft man Entscheidungen in schwierigen Situationen?

	<h3>AUSBILDUNG</h3> <ul style="list-style-type: none">■ Wir schulen Sie – auch firmenindividuell■ eLearning: Jetzt Wissenslücken effizient und gezielt schliessen!■ IT-SIBE■ IT-SIBE Vertiefung■ *NEU* Betrieblicher Datenschutzverantwortlicher■ Technische Sicherheit■ ISO 27001 Lead Auditor■ *NEU* Sicherheit am Arbeitsplatz■ *NEU* Professioneller Umgang mit Bedrohungen und Gewalt im Arbeitsalltag■ ITIL Security Management■ Upgrade Lead Auditor BS 7799■ *NEU* Integraler Sicherheitsmanager■ *NEU* ITIL Version 3 Foundation■ *NEU* ITIL Version 3 Foundation Bridge	
	<h3>CONSULTING</h3> <ul style="list-style-type: none">■ ISO 27001 / ISO 27002■ Wir unterstützen Sie: Überbrückung von Ressourcen- oder Kompetenzengpässen■ Security Edutainments – mit Spass & Freude Security verstehen und lernen!■ Informationssicherheit, dank der ISMS Tool Box	
	<h3>PUBLIKATIONEN</h3> <ul style="list-style-type: none">■ Neuerscheinungen: Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security■ Neuerscheinungen: Informationssicherheit und die Politik■ Neuerscheinungen: Records Management	





AKTUELLE MELDUNGEN

Die Laptops der US-Regierung sind immer noch unverschlüsselt: Vorgaben sehen es eigentlich anders vor

Ein Bericht legt katastrophale Sicherheitslücken in der IT der amerikanischen Regierung offen. So sollen 70 Prozent aller mobilen Geräte, darunter auch Laptops, ohne jegliche Verschlüsselungs- oder Sicherheits-Software betrieben werden.

Das ist das erstaunliche Ergebnis eines Reports des amerikanischen Government Accountability Office (GOA). Offenbar wurde die Bush-Administration nichts dazu gelernt. Im Jahr 2006 wurde ein Laptop aus dem Amt für Veteranen entwendet und damit auch gleichzeitig die Daten von 26 Millionen Veteranen. Dieser Vorfall gilt bis heute als zweitgrösster bekannter Datenverlust.

Über 24 verschiedene grössere Regierungsämter wurden für den Report untersucht. Dabei stellte die Prüfbehörde fest, dass auf 70 Prozent der Mobilgeräte, Laptops und Notebooks, die in den Ämtern verwendet wurden, keinerlei Schutzvorrichtungen vorhanden waren.

"Eine Folge davon ist, dass Informationen über und von der Regierung ein erhöhtes Risiko von unerlaubtem Zugriff, Verlust oder Modifikation haben", heisst es in dem Report. Zudem verstossen die Ämter gegen eine geltende Regelung, dass sämtliche Daten auf mobilen Geräten, die Informationen über die Ämter tragen, nach einem staatlich geprüften Standard zu schützen sind.

Quelle: Silicon.de; Martin Schindler; 31.7.08

[< zu den Themen](#)

US-Grenzbeamte schnüffeln ohne Verdacht: Überlegen Sie sich, wie Sie dieses Problem umgehen könnten

US-Grenzbeamte behändigen ohne richterlichen Befehl Computer von Geschäftsleuten bei der Einreise. Jetzt regt sich Widerstand gegen diese Praxis.

Die Kontrolle läuft laut dem Anwalt eines Betroffenen so ab: «Bitte schalten Sie Ihren Computer an. Wir möchten ihn durchsuchen.» Wird ein Passwort aufgerufen, so muss der Einreisewillige es aushändigen. Ist er nicht bereit dazu, kann er zurückgehalten werden. Wonach genau gesucht wird, weiss der Betroffene nicht. «Wir führen eine Zufallskontrolle durch», wird ihm beschieden. Später: «Wir werden den Computer zwecks Sicherung des Inhalts zurückbehalten.» Er werde ihn zu gegebener Zeit zurückerhalten. «Dabei wird oft die ganze Festplatte kopiert, einschliesslich gelöschter Dateien», sagt Susan Gurley von Acte, dem Verein für Geschäftsreisende in Führungspositionen (www.acte.org). Betroffen waren sogar schon Anwälte – trotz Recht auf Berufsgeheimnis. Bekannt sind auch Fälle von eingezogenen Handys und Handhelds.

In einer Umfrage unter 2500 Vereinsmitgliedern, darunter auch Schweizern, wollte Gurley wissen, «ob Mitarbeiter Ihrer Firma in den letzten drei Jahren von einer Durchsuchung oder einer Beschlagnahmung elektronischer Geräte betroffen waren». Vor drei Wochen publizierte sie die Ergebnisse: Sieben von hundert Chefs bestätigten einen Vorfall im eigenen Unternehmen. Die Geräte wurden eine Woche bis drei Monate zurückbehalten, in Einzelfällen mehr als ein Jahr lang. Fast allen Fällen gemein ist, dass die Geschäftsleute weder erfahren, «warum sie durchsucht wurden, wo ihre Daten gespeichert sind und ob die Daten nach erfolgloser Durchsuchung gelöscht wurden», kritisiert Gurley. Die US-Regierung nehme keine Stellung.

In den USA regt sich mittlerweile heftiger Widerstand. Ende Juni 2008 gab es vor dem Rechtsausschuss des Senats eine Anhörung dazu. Die «The New York Times» forderte, die Grenzbeamten seien in die Schranken zu weisen. Politiker und Bürgerrechtler behaupten, dass eine auf Inhalte von Computern ausgeweitete Zollfahndung gegen die Verfassung verstosse. Denn auch in den USA gilt der Grundsatz: Keine Durchsuchung oder Beschlagnahmung ohne richterliche Erlaubnis.

Konkrete Hinweise, dass Schweizer Unternehmen betroffen sind, liegen nicht vor. Der Leiter der schweizerisch-amerikanischen Handelskammer, Martin Naville, sagt, er habe von Fällen gehört, aber einen Betroffenen kenne er nicht. Eine Umfrage unter internationalen Firmen zeigt ein widersprüchliches Bild. Für die ABB sind die Grenzkontrollen «kein Problem». Nestlé schreibt, ihr seien «keine Durchsuchungen von Nestlé-Laptops durch US-Grenzbeamte bekannt». Die Grossbanken CS und UBS wollen die Kontrollen nicht kommentieren. Das IT-Unternehmen IBM spricht unverbindlich von «eventuellen Zwischenfällen, bei denen IBM eng mit den jeweiligen Behörden zusammenarbeitet». Nur das Beratungsunternehmen KPMG bestätigt die Gefahr. «Die Durchsuchungen von Laptops an US-Grenzen sind bei den von uns beratenen Firmen definitiv ein Thema», sagt Matthias Bosshardt, Experte für Datensicherheit bei KPMG.

Damit Geschäftsdaten nicht in falsche Hände gelangen, nennt er drei Strategien.

Erstens: mit so wenig Daten wie möglich reisen und benötigte Daten nach Grenzübertritt online über sichere Verbindungen beziehen. Zweitens: Die Daten verschlüsselt auf einem unauffälligen Speichermedium transportieren, beispielsweise auf der Speicherkarte einer digitalen Fotokamera.

Und drittens: Dateien so gründlich verstecken, dass selbst Spezialisten, sogenannte IT-Forensiker, sie nicht aufspüren.

Dafür gibt es Programme. «Forensiker sehen dann nur zufällige Daten ohne Struktur, die keinen Rückschluss auf das Vorhandensein von vertraulichen Informationen zulassen», sagt Bosshardt.

Quelle: Tagesanzeiger.ch; Andreas Valda; 23.7.08

[< zu den Themen](#)

Security-Policies gegen Datenverlust noch Mangelware: Wie ist gegen Data Leakage vorzugehen?

Obwohl der Verlust sensibler Daten aus Unternehmenssicht mittlerweile zu den grössten Bedrohungen zählt, hält gut die Hälfte der Firmen entsprechende Sicherheitsrichtlinien offenbar noch für überflüssig. Das ergab eine von Trend Micro initiierte Studie. Unternehmen stufen den unerwünschten Abfluss sensibler Informationen mittlerweile als zweitgrösstes Risiko am Arbeitsplatz ein - gleich hinter Viren und noch vor der Gefährdung durch Spam, Spyware und Phishing. Das ermittelte der Security-Anbieter Trend Micro¹ in einer Untersuchung, für die 1600 Firmenanwender in Deutschland, Grossbritannien, Japan und den USA zu ihren Erfahrungen mit Sicherheitsbedrohungen befragt wurden. Sich selbst sehen die Anwender dabei offenbar weniger als Problem: Nur sechs Prozent der Befragten gaben an, einmal für einen Datenverlust verantwortlich gewesen zu sein. Deutsche, britische und amerikanische Endanwender waren im Vergleich zu Befragten aus Japan laut Studie allerdings eher bereit einzugestehen, schon einmal ein Datenleck verursacht zu haben. Den Studienergebnissen zufolge haben 46 Prozent der befragten Unternehmen aktuell keine Sicherheitsrichtlinien zur Verhinderung von Datenlecks implementiert. Dabei sind deutsche und japanische Firmen diesbezüglich etwas weiter als Firmen in Grossbritannien. Grundsätzlich, so der Bericht, sind Anti-Data-Leakage-Policies häufiger in grossen als in kleinen Organisationen zu finden. Was das Training im Umgang mit sensiblem Datengut betrifft, haben die Vereinigten Staaten offenbar die Nase vorn. So sollen in US-amerikanischen Unternehmen, die über Sicherheitsrichtlinien zur Verhinderung von Datenlecks verfügen, nahezu 70 Prozent der befragten Anwender dahin gehend geschult worden sein. In Grossbritannien hingegen haben nur 57 Prozent der Befragten Nachhilfe in Sachen Datenvertraulichkeit erhalten. Als in den untersuchten Ländern primär angewandte Methode zum Schutz vor unerwünschtem Datenabfluss ermittelte Trend Micro den Einsatz von Sicherheitslösungen. "Die Mehrzahl aller Datenlecks wird intern verursacht - entweder unabsichtlich oder absichtlich durch legitime Anwender mit Zugriff auf Daten im Unternehmensnetz", meint Glen Kosaka, Director Marketing Data Leakage Prevention bei Trend Micro. Zu einem anderen Ergebnis kommt eine kürzlich veröffentlichte Langzeitanalyse von Verizon Business. Demnach ging die überwiegende Mehrheit der in Datenverlusten resultierenden Verstösse in den vergangenen drei Jahren nicht etwa von Insidern wie Mitarbeitern oder IT-Administratoren (18 Prozent), sondern von externen Quellen (73 Prozent) wie etwa Geschäftspartnern aus

Quelle: computerwoche.de; 8.7.08

[< zu den Themen](#)

Qualität der BCM-Krisenpläne lässt zu wünschen übrig: Nicht ständig aktualisierte Notfallpläne sind wertlos

Eine Umfrage unter den Teilnehmern eines Security Leadership Seminars der Sicherheitsorganisation (ISC)² zeigt, dass zwar in fast allen grossen Unternehmen ein Krisenplan vorhanden ist, doch wird er nicht an die Geschäftsdynamik angepasst. Die befragten Risiko- und Sicherheitsmanager nannten die Implementierung, das Training und die laufende Aktualisierung der Notfallpläne als grösste Herausforderung.

☐ Es reicht nicht, einen BCM-Plan in der Schublade zu haben. Die Kontinuitätsplanung muss laufend an die zentralen Geschäftsprozesse angepasst werden, sonst nutzt die ganze Arbeit reichlich wenig☐, erklärte Ralf Binzen, der Leiter des Seminars.

☐ Es zeigt sich immer wieder, dass zwar BCM-Pläne erstellt werden, aber für die Aktualisierung und laufende Anpassung keine Budgets zur Verfügung gestellt werden.☐

In fast einem Drittel der deutschen Unternehmen obliegt die Erstellung eines BCM-Plans der Geschäftsführung und nur in 14 Prozent ist die IT-Leitung verantwortlich. Fast 40 Prozent der Unternehmen aktualisieren laut dieser Umfrage den Krisenplan einmal pro Jahr und 18 Prozent alle zwei Jahre. Keines der Unternehmen bringt den Plan mehr als einmal im Jahr auf den neuesten Stand, obwohl sich Geschäftsprozesse durchaus öfter verändern können. Auch die Prozesse des BCM-Plans werden bei 36 Prozent der Unternehmen nur einmal im Jahr trainiert, beziehungsweise in 18 Prozent der Fälle alle zwei Jahre. 7 Prozent der Unternehmen trainieren alle

sechs Monate.

Die Qualität des vorhandenen BCM-Plans wurde von einem Drittel der Befragten als mittelmässig und von 18 Prozent als niedrig eingestuft. Immerhin finden ein Fünftel der Teilnehmer die Qualität des aktuellen Krisenplans ihres Unternehmens gut. In rund 30 Prozent der Unternehmen trat zum Glück innerhalb der letzten drei Jahre keine kritische Situation auf. Mit einer kritischen Situation mussten sich 18 Prozent auseinandersetzen. Zwei beziehungsweise drei kritische Situationen in den letzten drei Jahren haben jeweils 7 Prozent der Befragten erlebt und genauso viele haben vier und mehr Situationen erlebt, in denen ein Notfallplan zum Einsatz kam.

Quelle: Computerzeitung.de; Susanne Franke; 10.7.2008

[< zu den Themen](#)

Mobility kann eine Gefahr für die Firma sein: Zu Hause und unterwegs arbeiten lassen oder nicht?

Sicherheitsbedenken sind immer noch die grösste Hürde, wenn es um die Einführung und Umsetzung von mobilen Strategien geht. Der Erfolg von Apples iPhone hat dazu beigetragen, die Weigerung der IT-Manager zu verstärken. Sie sind es, die den immer mehr wuchernden Zoo an Geräten managen müssen. Anbieter begegnen dem mit Device-Security.

"Wir beobachten immer öfter, dass die Firmen ihre Scheu vor Wireless LAN fallen lassen", sagte Dagmar Schneider, Sales Manager Deutschland, Österreich, Schweiz (DACH) bei dem WLAN-Anbieter iPass, im Gespräch mit silicon.de. "Dennoch ist das Thema der Mobility vor allem aus Security-Sicht sehr sensibel. Die Frage nach der Sicherheit wird uns von Kunden und Interessierten tatsächlich am häufigsten gestellt."

"Gerade die Hotspot-Nutzung ist dabei oft erklärungsbedürftig, vor allem weil die Kunden Risiken befürchten", sagte sie. Theoretisch wissen alle Geschäftsanwender um die Unsicherheit von öffentlichen Netzen, praktisch wollen sie aber alle 'nur mal schnell' irgendetwas versenden oder empfangen.

Wie eine aktuelle Studie des Marktforschers Datamonitor feststellte, sind derzeit Mobility-Lösungen im Wert von 6 Milliarden Dollar in Unternehmen verbaut. Bis zum Jahr 2012 sollen es Geräte und Lösungen im Wert von 17 Milliarden Dollar sein. Um diese Menge zu bewältigen, müssen die Beauftragten und Admins zum einen ihre Scheu vor den Geräten ablegen. Zum anderen müssen sie in Einklang mit der Unternehmenspolitik und den Gepflogenheiten in der jeweiligen Branche eine durchsetzbare Security-Strategie für den Wildwuchs mobiler Geräte haben und pflegen.

Zum dritten und das ist vielleicht das Schwierigste müssen sie die Nutzer erziehen und deren Sensibilität für Sicherheitsfragen in der Mobility entfachen. "Unternehmen kämpfen eine aussichtslose Schlacht gegen mobile Geräte", weiss Daniel Okubo, Technology Analyst bei Datamonitor. Statt sie alle zu verbieten, riet er dazu, lieber eine begrenzte Anzahl an Geräten offiziell zuzulassen und mit entsprechender Sicherheit und Policies auszustatten. 467 IT-Manager und CIOs haben an der Umfrage teilgenommen und die Mehrheit von ihnen leidet demnach unter dem, was Okubo die "Angst vor dem Unbekannten" nennt. Er sieht die Anbieter in der Pflicht, um die Druckpunkte der Kunden gebührend anzugehen und ihnen diese Angst zu nehmen.

Die Kunden, wie auch die Anbieter kommen dem Analysten zufolge nicht mehr an der Frage vorbei, wie ihr Device Management aussehen soll und wie es in die allgemeine IT-Strategie eingepasst wird. Und sie sollten nicht unterschätzen, wie hoch die Anwenderzufriedenheit und die damit verbundene Produktivität auch abseits des Schreibtisches werden kann, wenn die Nutzer "ihr" Gerät behalten dürfen. Sie sollten der Angst nicht die Kontrolle überlassen, riet der Analyst.

Quelle: Silicon.de; Kathrin Schmitt; 1.7.08

[< zu den Themen](#)

Grossteil der Unternehmen verwundbar: Der Fortschritt könnte schneller sein

Über 80 Prozent aller Unternehmen kämpfen täglich mit Angriffen von Hackern. Zudem haben die meisten Organisationen Sicherheitslücken, die den Verantwortlichen bekannt sind.

Viele der IT-Fachkräfte, die das Unternehmen Fortify auf dem Sicherheitskongress Infosecurity Europe 2008 befragt hat, seien äusserst besorgt über die Sicherheit der Anwendungen in ihrem Unternehmen. Damit ist das Thema Anwendungssicherheit für viele auch das vorrangigste Sicherheitsthema.

Etwa ein Drittel der Befragten berichtete zudem, dass täglich versucht werde, unberechtigt auf das Unternehmensnetz zuzugreifen. 17 Prozent dieser Angriffe seien zudem erfolgreich. Als Gegenmassnahme greifen 98 Prozent der Befragten auf eine Firewall zurück. 67 Prozent nutzen daneben Pentest und 41 Prozent erweitern die Firewall mit einer Static-Analysis-Software.

Weniger vorsichtig sind Unternehmen offenbar bei anderen Sicherheitsaspekten. Etwa ein Viertel der Unternehmen lassen Anwendungen ausser Haus entwickeln. Dabei legen sie wieder Sicherheitsprozesse fest, noch stellen Technologien die Sicherheit der extern entwickelten Anwendungen sicher, so die Studie.

Dabei waren über 60 Prozent der IT-Fachkräfte, die vorrangig für Unternehmen mit mehr als 1000 Angestellten tätig sind, überzeugt, dass das Outsourcen der Entwicklung das Sicherheitsrisiko steigert. Als positiv bewerteten die Sicherheitsexperten den Einfluss von gesetzlichen Vorgaben wie Basel II. Diese würden nicht nur für ein gesteigertes Bewusstsein, sondern auch für grössere Budgets für Sicherheitstechnologien sorgen.

Quelle: Silicon.de; Martin Schindler; 30.6.08

[< zu den Themen](#)

eDiscovery und Sanktionen der US-Gerichte: Auch in der Schweiz wird man sich damit vertieft befassen müssen

Jedes ausländische Unternehmen mit Geschäftstätigkeit in den USA muss spätestens bei gerichtlichen Auseinandersetzungen damit rechnen, seine elektronischen Daten als Beweismittel offenlegen zu müssen. Denn aufgrund von "Electronic Discovery"-Regelungen können Unternehmen verpflichtet werden, elektronisch gespeicherte Informationen zu reproduzieren, wenn diese als Beweismittel in einem Gerichtsverfahren in Betracht kommen.

Die Rechts- und IT Abteilungen vieler Firmen werden aber nicht nur durch diese in einigen Rechtsordnungen verankerten eDiscovery-Bestimmungen vor grosse Herausforderungen gestellt. Vielmehr ist eine Reproduktion digitaler Informationen oft auch im Rahmen einer "Post Merger"-Untersuchung oder etwa bei der Aufklärung von Unregelmässigkeiten im Unternehmen und somit anlässlich einer internen Revision notwendig.

eDiscovery (in Grossbritannien "eDisclosure" genannt) ist die in den Prozessordnungen mancher Länder vorgesehene Beweissammlung von elektronisch gespeicherten Informationen. Dieses Verfahren ist damit vor allem für Parteien relevant, die beispielsweise in den USA ansässig sind, denn dort erlaubt Abschnitt V der "Federal Rules of Civil Procedure (FRCP)" in Zivil-, Verwaltungs- und Strafverfahren den Zugriff auf elektronisch gespeicherte Daten des Unternehmens. Auch schweizerische Gesellschaften, die entweder direkt oder mittelbar über ein Konzernunternehmen in den USA tätig sind, müssen aber damit rechnen, neben den allgemein geltenden Anforderungen von IT-Compliance mit den Auswirkungen von eDiscovery konfrontiert zu werden.

eDiscovery-Erfordernisse an die Herausgabe digitaler Informationen

Nach US-amerikanischem Recht sind neben E-Mails auch beweisrelevante Zeichnungen, Grafiken, Tabellen, Fotos, Sprachnachrichten, Tonbandaufzeichnungen und andere Datensammlungen einschliesslich elektronisch gespeicherter Informationen grundsätzlich herausgabepflichtig. Auch Entwürfe, Anmerkungen und Notizen zu diesen Dokumenten sowie gegebenenfalls unterschiedliche Bearbeiterversionen dieser Dokumente sind vom Umfang der eDiscovery umfasst. Zu den elektronisch gespeicherten Informationen gehören schliesslich auch die Metadaten, also alle Zusatzinformationen zu den Dokumenten wie Name des Bearbeiters, Datum der Erstellung und der letzten Änderung, etc.

Die prozessuale Pflicht zur Offenlegung relevanter Dokumente und elektronischer Daten betrifft zunächst allein diejenigen Informationen, die sich im Besitz der in den USA verklagten Parteien befinden. Dennoch kann sich diese Offenlegungspflicht auch auf solche Dokumente erstrecken, die sich im Besitz einer Konzerngesellschaft befinden, selbst wenn diese gar nicht Partei des Verfahrens ist.

Die US-amerikanischen Gerichte haben nicht nur ein weitreichendes Verständnis bei der Annahme der US-amerikanischen "Jurisdiction" und dem Begriff "Dokumente", sondern sind auch bei der Auslegung des Tatbestandsmerkmals "Control" grosszügig. Über diese "Kontrollmöglichkeit" wird von den US-Gerichten oftmals eine Herausgabepflicht auch nicht am Prozess beteiligter ausländischer Gesellschaften hergeleitet, sofern eine rein tatsächliche Kontrollmöglichkeit bezüglich dieser Daten besteht. Dies gilt auch dann, wenn dieser faktischen Kontrollmöglichkeit geltendes (Datenschutz-)Recht entgegen steht.

Der Prozesspartei in den USA (und zwar auch bei der Weigerung einer europäischen Konzerngesellschaft, bei dem Auskunftsverlangen mitzuwirken) können neben dem Ausschluss eigener Beweismittel und einer Art Beweislastumkehr bei absichtlicher Vorenthaltung von Beweisen ein Unterliegen im Rechtsstreit in den USA oder finanzielle Sanktionen wegen "Contempt of Court" drohen. Zumindest mittelbar können sich daher die Vorschriften rund um eDiscovery auch auf in der Schweiz ansässige Unternehmen auswirken.

Handlungsbedarf für Unternehmen auch in der Schweiz

Um solche Sanktionen der eDiscovery zu vermeiden, aber auch um auf eine interne "Post Merger"-Untersuchung oder eine IT-gestützte "Internal Investigation" vorbereitet zu sein, müssen die in den USA tätigen Unternehmen einschliesslich ihrer im Ausland ansässigen Konzerngesellschaften entsprechende Prozesse einführen, um eine vollständige Aufbewahrung relevanter Dokumente (einschliesslich deren Entwürfe und Metadaten) sicherzustellen.

Zudem muss gewährleistet sein, dass die Vernichtung von relevanten Unterlagen und die Löschung elektronischer Daten konzernweit geregelt ist und spätestens dann ausgesetzt wird, sobald ein Rechtsstreit vorhersehbar wird oder diese Daten anderweitig benötigt werden. Ein solcher "Evidence and Disclosure Management"-Prozess kann aber vor allem auch bei einer rein unternehmensinternen Aufklärung von Sachverhalten oder einer EDV-gestützten Überprüfung nach einer Unternehmensfusion überaus hilfreich sein.

Unternehmen sind daher nicht zuletzt auch unter dem Blickwinkel von IT-Compliance gut beraten, die bei der digitalen Archivierung und fristgebundenen Vernichtung von Geschäftsunterlagen geltenden Verfahren in enger Abstimmung zwischen Rechts- und IT Abteilung auch im Hinblick IT auf die Anforderungen von eDiscovery und eine etwaige unternehmensinterne Revision zu überprüfen. Anschliessend müssen diese Prozesse unter Einschaltung der verantwortlichen internen Funktionen in einer Unternehmens-Richtlinie verbindlich festgelegt und im Konzern einheitlich umgesetzt werden.

Quelle: Compliancemagazin.de; 28.7.08

[< zu den Themen](#)

Was ist Compliance?: Erläuterungen zu einem Begriff, der in fast aller Leute Munde ist

Bei "Compliance" geht es um die "Erfüllung", "Entsprechung" bzw. "Konformität" mit staatlichen Gesetzen sowie mit Regeln und Spezifikationen, mit Grundsätzen (ethische und moralische) und Verfahren sowie mit Standards (z.B. ISO) und Konventionen, die klar definiert worden sind. Die Erfüllung der Compliance kann sowohl auf Zwang (z.B. durch Gesetze) als auch auf Freiwilligkeit (z.B.

Einhaltung von Standards) beruhen.

Die Compliance richtet sich an Unternehmen und Institutionen ebenso wie an staatliche / behördliche Einrichtungen. Streng genommen ist jeder Mensch - sei es als unabhängiges Einzelindividuum oder als Mitglied einer Gruppe, Organisation oder eines Unternehmens in irgendeiner Form Compliance-pflichtig bzw. muss seine Compliance-Fähigkeit unter Beweis stellen, muss sich compliant verhalten.

Sogar Länder können sich in diesem Sinn compliant verhalten, z.B. durch die Übernahme von übergeordneten Gesetzen in innerstaatliche gesetzliche Regelungen (z.B. innerhalb der EU) oder auf internationaler Ebene durch die Einhaltung von Konventionen (UN-Konventionen) oder Beschlüsse internationaler Gremien (z.B. OECD-Beschluss).

Das Nicht-Einhalten von Regeln, Gesetzen, Standards etc. wird als Non-Compliance bezeichnet. Unternehmen, Institutionen, staatliche und behördliche Einrichtungen bzw. Personen, die sich nicht an entsprechende Vorgaben halten, handeln dementsprechend non-compliant. Non-Compliance (Nicht-Konformität) kann sanktioniert / bestraft werden, sei es durch die staatliche Gewalt (z.B. Bussgeld) oder auch durch unternehmensinterne Strafmassnahmen (z.B. Abmahnung) bzw. vereinsinterne oder organisationsinterne Sanktionen (z.B. Ausschluss).

Die Verantwortung für Compliance innerhalb der Unternehmen ist derzeit in den verschiedensten Bereichen angesiedelt: In neu gegründeten Compliance-Abteilungen, in Legal Departments (Rechtsabteilungen), beim Controlling, bei der Internen Revision, bei den Datenschutzabteilungen, beim Personalwesen und nicht zuletzt häufig auch im Bereich der IT (Security-Abteilungen oder bei der Rechenzentrumsleitung bzw. bei der Gesamtverantwortung für die IT).

Compliance ist heute ein wesentlicher Bestandteil der Corporate Governance, bei der es um die "gute", ordnungsgemässe Unternehmensführung geht (das Erlassen und Einhalten von Verhaltensregeln - Codes of Conduct). In diesem Sinn stellt die Corporate Governance heute die Visitenkarte eines Unternehmens dar.

Was bedeutet IT-Compliance?

Unternehmen müssen Regel-/Gesetzeskonformität herstellen. Gleichzeitig werden zunehmend in den Unternehmen Geschäftsprozesse digital abgebildet. Die Informationstechnologie (IT) hat erkannt, dass früher oder später sämtliche digitale Prozessketten (= durch IT abgebildete Geschäftsabläufe) lückenlos nachweisbar sein müssen (z.B. für Kontrollen staatlicher Organe □ Steuer, Zoll, etc. bzw. für Gerichte, Wirtschaftsprüfer etc.).

Die IT-Industrie (mit ihren Software-, Hardware- und Kommunikationsangeboten) muss sich ebenfalls an ihrer Compliance-Fähigkeit messen lassen. Die Produkte müssen ihre Compliance-Fähigkeit unter Beweis stellen. Einen grossen Beitrag zur IT-Compliance leistet innerhalb der Informationstechnologie die IT-Sicherheit. Sie ist heute zwingend notwendig, eine Vernachlässigung erzeugt Haftungsfallen für Geschäftsführer und Vorstände. Die IT-Sicherheit hat grossen Einfluss z.B. auf Basel II-Regelungen; Regelungen z.B. der Kreditkartenindustrie (PCI DSS-Compliance) fordern signifikante Investitionen in IT-Security-Produkte.

Quelle: Compliancemagazin.de; download 20.7.08

[< zu den Themen](#)

Risiken beim IT-Outsourcing: Sicherheitsaspekte bei vielen IT-Outsourcing-Projekten zu wenig berücksichtigt

Obwohl Outsourcing- und Offshoring-Projekte für viele Unternehmen eine attraktive Alternative gegenüber intern gehosteten Systemen darstellt, sollte man die damit verbundenen Risiken für die Informationssicherheit nicht unterschätzen. Zu diesem Ergebnis kommt eine Studie des Information Security Forums.

Laut dem Information Security Forum (ISF), einem internationalem Verband mit 300 Mitgliedsunternehmen, gibt es zahlreiche

dokumentierte Fälle, in denen Daten beim Outsourcing verloren gingen oder gestohlen wurden. Dennoch unterschätzen einige Unternehmen das Gefährdungspotenzial, bis es dafür zu spät ist.

So zeigt die ISF-Studie auf, dass die Risiken für die Informationssicherheit oft erst im Nachhinein erkannt und Sicherheitsfachleute meist zu spät in die Projekte miteinbezogen werden. Einen Grund hierfür sehen die Security-Experten im mangelnden Risikobewusstsein insbesondere in der Führungsebene.

Eine weitere Erklärung für diesen Missstand ist das fehlende Verständnis für die Wichtigkeit eines Informations-Risikomanagements in allen Phasen des Outsourcing-Projekts.

¶ Wenn Sicherheitsspezialisten nicht vom Start weg in das Projekt eingebunden werden, nehmen die Bedrohungen für das Unternehmen ständig zu. Sei es durch Datendiebstahl, Datenverluste oder durch Auseinandersetzungen, die beispielsweise durch ungeklärte Urheberrechtsfragen entstehen¶, beschreibt Simone Seth, die Autorin der ISF-Studie, das Problem.

IT-Manager sollten deswegen zunächst sämtliche ausgelagerten Prozesse, Abläufe und Technologien unter die Lupe nehmen und geschäftskritische Grenzen für alle vier Schritte eines Outsourcing-Projekts festlegen: Für die Vorbereitung ebenso wie für die Implementierung, die Umsetzung und das Review. Der Verantwortliche für das Informations-Risikomanagement sollte zudem vertragliche Vereinbarungen treffen, welche die Anforderungen an die Informationssicherheit und die dazugehörigen Vorschriften und Regelungen berücksichtigen, um so auch rechtliche Sicherheit zu schaffen.

Hierfür müssen auch die jeweiligen regionalen Compliance-Anforderungen und gesetzlichen Regelungen beim Outsourcing-Partner vor Ort beachtet werden. Das betrifft insbesondere auch die Sprachregelung einzelner Vertragsvereinbarungen. Auf diese Weise lassen sich mögliche Konflikte zu Urheberrechtsfragen oder zur Datenübermittlung von vornherein vermeiden.

Quelle: Searchdatacenter.de; Florian Karlstetter; 11.7.08

[< zu den Themen](#)

Sind die Datenschutzgesetze europaweit veraltet?: Eine Studie soll Licht ins Dunkel bringen

Die für den Datenschutz verantwortliche höchste britische Aufsichtsbehörde "Information Commissioners Office" hat nun eine Untersuchung in Auftrag gegeben, welche klären soll, ob die anwendbaren EU-Datenschutzgesetze überhaupt noch zeitgemäss sind. Das beauftragte Forschungsinstitut RAND soll die Analyse durchführen und feststellen, ob gegenwärtige Standards beim Datenschutz überhaupt noch sinnvoll angewendet werden können, oder ob eine weit reichende Reform notwendig wäre. Falls Letzteres der Fall ist, lautet der Auftrag ausserdem, mögliche Optionen für solch eine Veränderung zu ermitteln und zu konkretisieren.

Dabei wäre dies nicht die erste Studie mit diesem Themengebiet. Auch die Europäische Kommission hatte bereits eine solche Analyse in Auftrag gegeben, wenngleich die Motivationsgründe hier wohl eher darin begründet lagen, dass man klare Richtlinien beim internationalen Datenaustausch schaffen wollte, welcher insbesondere für Probleme zwischen der EU sowie den USA gesorgt hatten. Eine Einigung hierüber soll in naher Zukunft erreicht werden.

"Das europäische Datenschutzgesetz ist zunehmend überaltert, bürokratisch und äusserst vorschreibend," so Commissioner Thomas auf einer Rechtskonferenz. "Es zeigt sein wahres Alter und scheitert zunehmend an den Herausforderungen, die die Privatsphäre ihm stellt, wie etwa beim Transfer von persönlichen Daten über Landesgrenzen hinaus sowie der zunehmenden Zahl an persönlichen Informationen, die online verfügbar sind."

Eine Reform des Datenschutzgesetzes darf europaweit als durchaus heikel betrachtet werden, da mitunter eine Lockerung erwartet werden kann, damit der Datenaustausch zwischen den Ländern zur allgegenwärtigen Terrorismusbekämpfung erleichtert werden kann. Nur mit viel Glück kann eine Stärkung des Datenschutzgesetzes erwartet werden, sofern sich die Politik der eigentlichen Aufgabe besinnt, für das Volk zu arbeiten. Die Justiz in Frankreich hat es kürzlich vorgemacht, was es heisst, auch die Daten von Filesharern zu schützen, da eine IP-Adresse deren Meinung nach in den persönlichen Lebensbereich gehört. Die Schweiz kann hier

ebenfalls gleichziehen, mit dem Eidgenössischen Datenschutzbund, der gegenwärtig ebenfalls versucht, das Sammeln von IP-Adressen durch Anti-Piracy Firmen zu unterbinden. Die sind Ansätze in die richtige Richtung, die hoffentlich bald weit reichend umgesetzt werden.

Quelle: *Gulli.com*; 8.7.08

[< zu den Themen](#)

Schnelltest für Euro-SOX-Compliance: Zwölf Fragen zeigen möglichen Handlungsbedarf auf

Nach einer Studie der Unternehmensberatung exagon haben sich die Unternehmen bislang erst sehr zurückhaltend mit der seit Ende Juni 2008 gültigen Richtlinie zu Euro-SOX (sog. 8. EU-Richtlinie) beschäftigt. Sie soll dazu dienen, durch eine höhere Transparenz wichtiger Unternehmensinformationen Finanzskandale wie in der Vergangenheit zu vermeiden. Ein EuroSOX-Schnelltest soll Unternehmen für das Problem EuroSOX sensibilisieren.

Euro-SOX betrifft alle Firmen mit einer Bilanzsumme von mehr als knapp 90 Mio. Euro. Um die Unternehmen für eine offensivere Beschäftigung mit den Erfordernissen zu sensibilisieren, hat exagon einen Euro-SOX-Schnelltest entwickelt. "Er gibt einen tendenziellen Aufschluss darüber, wie dringend und umfangreich der Handlungsbedarf ist", erklärt exagon-Geschäftsführer Joachim Fremmer:

1. Kennen Sie die genauen Anforderungen von Euro-SOX und ihre Gültigkeit für Ihr Unternehmen?
2. Besteht eine interne Projektgruppe für Euro-SOX zur Planung und Realisierung der Euro-SOX-konformen Finanzberichtsprozesse?
3. Sind die bestehenden Revisionsverfahren ausreichend für die Anforderungen von Euro-SOX?
4. Besteht innerhalb der IT ein ausreichendes Verständnis der internen Kontrollverfahren und der Prozesse zur Finanzberichtserstattung?
5. Sind Ihre IT-Organisation und die IT-Prozesse ausreichend transparent, damit wirksame Kontrollen implementiert werden können?
6. Sind die gesamten IT-Systeme identifiziert, die für Euro-SOX von Bedeutung sind? 7. Besteht eine ausreichende Risikoanalyse dieser IT-Systeme?
8. Wissen Sie genau, wo Sie in der IT die verschiedenen Controls für die verschiedenen Kontrollebenen (General IT-Controls, Application Controls, Company-Level-Controls) setzen müssen?
9. Sind die Controls inhaltlich anforderungsgerecht definiert?
10. Liegen konkrete Planungen hinsichtlich der Zuständigkeit und Qualifizierung von Mitarbeitern für die Kontrollen vor?
11. Bestehen präzise Verfahren zur Dokumentation und zum Testing der gesamten Controls?
12. Sind die Controls hinsichtlich ihrer Lokalisierung, Wirksamkeit und Dokumentation detailliert mit dem Wirtschaftsprüfer abgestimmt?

Fremmer schränkt allerdings ein, dass der exagon-Schnelltest für Euro-SOX nur eine initiale Bedeutung haben kann und nicht als ein ausreichend umfassendes Bewertungsraster missverstanden werden darf. Vielmehr könne sich hinter jedem dieser Aspekte ein umfassender Gestaltungsbedarf verbergen, damit sie den rechtlichen Bedingungen gerecht werden. "Dieser Test dient den Verantwortlichen allerdings dazu, intern oder auch gegenüber den Wirtschaftsprüfern die erforderlichen Fragen zu stellen, um gezielt den Erfüllungsgrad der Euro-SOX-Anforderungen zu beleuchten."

Quelle: *Compliancemagazin.de*; 4.7.08

[< zu den Themen](#)

Das deutsche Bundeskabinett verabschiedet Gesetz zum biometrischen Personalausweis: Früher oder später wird er kommen

Die deutsche Bundesregierung hat den umstrittenen Entwurf für die Novelle des Personalausweisgesetzes beschlossen. Gemäss dem Vorhaben und dem bislang allein vorliegenden Grobkonzept zur Umsetzung soll der elektronische, mit einem kontaktlos auslesbaren RFID-Chip ausgerüstete Personalausweis künftig ein digitales Photo sowie eine Reihe freiwilliger Zusatzfunktionen enthalten. So können sich die Bürger etwa dafür entscheiden, auch zwei Fingerabdrücke mit aufnehmen zu lassen.

Darüber hinaus kann sich der Antragsteller für eine Freischaltung eines Zertifikats für eine einfache elektronische Signatur zur Identifizierung gegenüber Behörden und Unternehmen übers Internet entscheiden. Das Aufspielen eines weiteren Zertifikats für eine qualifizierte digitale "Unterschrift" gemäss Signaturgesetz soll dagegen extra kosten.

Laut Schäuble gehört mit dem E-Perso die Zeit, in der elektronische Formulare zwar am PC ausgefüllt, aber am Ende doch manuell unterschrieben und versandt werden müssten, der Vergangenheit an: "Der elektronische Ausweis spart damit allen Beteiligten Papier, Druck-, Porto-, Transportkosten und vor allem Zeit", erklärte der Minister nach dem Kabinettsbeschluss. Das neue Dokument mache den elektronischen Geschäftsverkehr sicherer und einfacher für Bürger, Wirtschaft und Verwaltung und habe ein enormes Potenzial Bürokratiekosten einzusparen. Ein Anbieter, der den elektronischen Identitätsnachweis als "vertrauenswürdige Infrastruktur" in seine Dienste einbinden wolle, müsse vorher bei einer staatlichen Stelle ein Berechtigungszertifikat beantragen.

Schäuble rechnet damit, dass im parlamentarischen Raum eine zügige Verabschiedung des Entwurfs bis spätestens Anfang 2009 möglich ist. Der neue Ausweis könne dann vom 1. November 2010 an ausgegeben werden, nachdem vorab noch Tests durchgeführt und Anwendungen für den "Internetausweis" wie etwa die Eröffnung eines Bankkontos durch ein rein elektronisches Antragverfahren gemeinsam mit Branchenverbänden vorbereitet worden seien. Einen späteren Zwang zur Erfassung von Fingerabdrücken schloss Schäuble nicht aus, wenn es eine entsprechende EU-weite Regelung gäbe.

Die Opposition sieht das Konzept sehr kritisch. Die innenpolitische Sprecherin der Grünen im Bundestag, Silke Stokar, warnte die Bürger vor einer "gefährlichen Gutgläubigkeit". Sie sagte der Braunschweiger Zeitung, der neue Ausweis bringe keinen Sicherheitsgewinn, aber eine Reihe von Risiken und Gefahren. Besonders bedenklich findet die Grüne die vorgesehene freiwillige Speicherung des Fingerabdrucks, vor allem mit Blick auf Missbrauchsmöglichkeiten im Ausland. "Der Fingerabdruck hat im Personalausweis nichts zu suchen", meint auch der Innenexperte der Linken, Jan Korte. Er hege den Verdacht, dass die Fingerabdruckdaten eines Tages doch noch zentral gespeichert werden könnten.

Der neue Ausweis ist weiterhin für alle Deutschen über 16 Jahren Pflicht, wenn sie sich nicht per Reisepass ausweisen können. Das Dokument soll wie das alte eine Gültigkeit von zehn Jahren haben. Die zum Einsatz kommenden kryptographischen Verfahren seien vom Bundesamt für Sicherheit in der Informationstechnik entsprechend robust ausgewählt worden, heisst es dazu im Innenministerium. Geplant ist eine rund um die Uhr erreichbare Telefon-Hotline, damit Bürger bei einem Verlust oder Diebstahl die PIN für die Signaturfunktionen sperren lassen können. Fürs Ummelden ist ein Gang zum Amt weiterhin erforderlich. Wohnortwechsel werden zum einen elektronisch auf dem Chip vermerkt. Zum anderen wird die neue Adresse im Personalausweis wie bisher ganz traditionell überklebt.

Quelle: Heise.de; Stefan Krempl; 23.7.08

[< zu den Themen](#)

EVENTS

Jetzt anmelden!

Einladung zur ISMS Tool Box Roadshow vom 11.09.2008:



Informationsveranstaltung

Neu mit Workshops

Möchten auch Sie ein Information Security Management System (ISMS) vollumfänglich intranetbasiert und toolgestützt aufbauen und verwalten? Lernen Sie den unentbehrlichen Werkzeugkasten an der diesjährigen **ISMS Tool Box Roadshow** kennen.

Zeit: **13.30 - 16.30 Uhr**

Ort: **Radisson SAS Hotel, Zürich Flughafen**

13.30	Begrüssung und Kurzvorstellung ISMS Tool Box, Andre Jacomet	
13.45	Ein Beispiel aus der Praxis, Gastreferent	
14.00	Erläuterung zu den Parallelstreams, Andre Jacomet	
14.10	Workshop A Nachhaltige und pragmatische Umsetzung von Regelwerken wie ISO 27002 und IT-Grundschutz-Katalogen Matthias Grütter, Cornel Furrer	Workshop B Praxisgerechte Risikoanalysen und Audits planen, durchführen und nachbearbeiten Andre Jacomet, Reto Zbinden
14.55	Pause	
15.10	Workshop C Alle Ihre Schutzobjekte zentral inventarisieren, klassifizieren und verwalten ☐ und den Überblick behalten Matthias Grütter, Cornel Furrer	Workshop D Security Incident Management ☐ einfach und kostengünstig zur prozessgeführte Verwaltung Ihrer Incidents Andre Jacomet, Reto Zbinden
16.00	Learnings aus den Workshops, Andre Jacomet	

16.30 Apéro

Melden Sie sich **jetzt gleich an** und sichern Sie sich so Ihren Platz an der diesjährigen **ISMS Tool Box Roadshow** in Zürich Flughafen.

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Special Event mit Beat Lehmann
am 16. - 17.09.2008: Revision Datenschutzgesetz DSG: Wie kann Datenschutz heute optimal umgesetzt werden?:



Intensivseminar mit **Beat Lehmann**, Fürsprecher

Revision Datenschutzgesetz DSG: Wie kann Datenschutz heute optimal umgesetzt werden?

Sie sind herzlich eingeladen, am zweitägigen Intensivseminar zur **Revision des Datenschutzgesetzes** teilzunehmen.

Ihr nächster Termin in Olten: 16. - 17. September 2008

[Hier finden Sie weitere Informationen und Anmeldeöglichkeiten](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Special Event mit Beat Lehmann
am 29. - 30.10.2008: Sicherheitsüberprüfungen von IT-Systemen:



Intensivseminar mit **Beat Lehmann**, Fürsprecher

Sicherheitsüberprüfungen von IT-Systemen
Ethical Hacking und Social Engineering
Rechtliche Grundlagen und Hürden

Sie sind herzlich eingeladen, am zweitägigen Intensivseminar "Sicherheitsüberprüfungen von IT-Systemen unter spezieller Berücksichtigung von Ethical Hacking und Social Engineering" teilzunehmen.

Ihr nächster Termin in Olten: 29. - 30. Oktober 2008

[Hier finden Sie weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Special Event mit Frank Roselieb
am 11. - 12.11.2008: Krisen erkennen, bewältigen und erfolgreich meistern:



Intensivseminar mit **Frank Roselieb**, Vorstandsmitglied der Deutschen Gesellschaft für Krisenmanager e.V.

Krisen erkennen, bewältigen und erfolgreich meistern
Wie sich Schweizer Unternehmen und Behörden auf den Ernstfall vorbereiten können.
Krisensimulation, Fallbeispiele und Empfehlungen

Krisensituationen erfordern Ruhe, Beherrschung und die Nase für das Richtige im richtigen Zeitpunkt, in der richtigen Art und Weise zu tun. Dieses trifft insbesondere auf Führungskräfte zu, die in Krisenzeiten erst recht im Rampenlicht der Öffentlichkeit stehen. Sie müssen in der Unternehmung Leitbild sein und eine Persönlichkeit darstellen, die lange vor der Krisensituation zu einer solchen geworden ist.

Ihr nächster Termin in Thalwil: 11. - 12. November 2008

[Hier finden Sie weitere Informationen und Anmelde-möglichkeiten](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Special Event mit Prof. Dr. Sachar Paulus
am 18.11.2008: SAP-Sicherheit: Trends, Tipps und Tricks für den Umgang mit Risiken:



Intensivseminar mit Prof. Dr. Sachar Paulus, ehemaliger Senior Vice President für Produktsicherheit bei SAP

SAP-Sicherheit: Trends, Tipps und Tricks für den Umgang mit Risiken
Wie Sie Ihre wichtigsten Daten erfolgreich schützen können

Ihr nächster Termin in Thalwil: 18. November 2008

[Hier finden Sie weitere Informationen und Anmelde-möglichkeiten](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Special Event mit Detlev Sachse
am 15. - 16.12.2008: Sicherheit und Auditing eines SAP-Systems:



Intensivseminar mit Detlev Sachse, SAP-Berater

Sicherheit und Auditing eines SAP-Systems

Für Auditoren, Sicherheitsbeauftragte und Interessierte

Ihr nächster Termin in Thalwil: 15. - 16. Dezember 2008

[Hier finden Sie weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Special Event mit Dr. Ulrich Zwygart
am 02.04.2009: Wie trifft man Entscheidungen in schwierigen Situationen?:



Intensivseminar mit Dr. Ulrich Zwygart, ehemaliger Divisionär und Kommandant der Höheren Kaderausbildung der Schweizer Armee, Global Head Learning and Development der Deutschen Bank in London

Wie trifft man Entscheidungen in schwierigen Situationen?
Erfolgsfaktoren in der Entscheidungsfindung

Ihr nächster Termin in Thalwil: 2. April 2009

[Hier finden Sie weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

AUSBILDUNG

Wir schulen Sie  auch firmenindividuell: Firmenindividuelle Durchführung von Swiss Infosec-Themenkurse und -Lehrgänge



Beliebte firmenindividuelle Themen sind bspw. ISO 27001/27002 für IT-Mitarbeitende oder interne Auditoren, Archivierung, Datenschutz, Sicherheit am Arbeitsplatz, Umgang mit Bedrohungen, Krisen- und Evakuationsübungen.

Gerne führen wir die Themenkurse und Lehrgänge auch direkt bei Ihnen im Unternehmen durch. Bei firmenindividuellen Schulungen profitieren Sie, nebst der optimaleren Atmosphäre und Organisation, kostenmässig bereits ab vier Teilnehmenden.

Ihre Vorteile

- + Zeit- und Kostenreduktion
- + Vertraulichkeit
- + Steigerung der Effizienz
- + Auf Wunsch abgestimmt auf Ihre spezifischen Anforderungen

[Hier erfahren Sie mehr](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

eLearning: Jetzt Wissenslücken effizient und gezielt schliessen!



Wir bieten Ihnen gerne bereits ausgearbeitete oder auf Ihre individuellen Bedürfnisse angepasste eLearning-Systeme und -Module zu den Themen Informationssicherheit, IT-Sicherheit und Datenschutz an.

Das Swiss Infosec eLearning-Angebot ergänzt Ihre Aktivitäten im Bereich der Sensibilisierung und Ausbildung optimal und kosteneffizient.

Ihre Vorteile

- + Kosteneffizient: Keine Systeminvestitionen notwendig, tiefe Kosten pro Mitarbeitendem
- + Schneller, gezielter und effizienter Wissenstransfer
- + Idealer Bestandteil einer umfassenden Awareness-Kampagne

[Hier erfahren Sie mehr](#)

Quelle: *Swiss Infosec AG in Bern, Sursee, Zürich*

[< zu den Themen](#)

IT-SIBE: Lehrgang für Informations- und IT-Sicherheitsbeauftragte



Aus der Praxis für die Praxis!

Wir führen Sie umfassend in die Grundlagen der Informations- und IT-Sicherheit ein. Diesen Lehrgang führen wir seit fast 20 Jahren erfolgreich durch laufend aktualisiert und auf den neuesten Stand gebracht profitieren auch Sie vom geballten Wissen jahrelanger Erfahrung.

Nächster Lehrgang: 13. - 17. 10. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: *Ausbildungsprogramm 4-2008, Swiss Infosec AG*

[< zu den Themen](#)

IT-SIBE Vertiefung: Praktischer Vertiefungslehrgang für Informations- und IT-Sicherheitsbeauftragte



Sichern und erweitern Sie sich Ihr Fachwissen!

In praktischen Arbeiten und Diskussionen erarbeiten Sie gemeinsam unter fachkundiger Anleitung u.a. eine Sicherheitspolitik,

Sicherheitskonzepte und exemplarische Weisungen und Konzepte eines Unternehmens in den verschiedenen Bereichen der Integralen Sicherheit. Die Vielzahl praktischer Umsetzungshinweise ist eine echte Überlebenshilfe für jeden IT-SIBE.

Nächster Lehrgang: 10. - 14. 11. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

***NEU* Betrieblicher Datenschutzverantwortlicher: Lehrgang für Datenschutzverantwortliche gemäss revidiertem Datenschutzgesetz der Schweiz**



In diesem Lehrgang werden Sie umfassend in die Aufgaben des Datenschutzverantwortlichen eingeführt. Sie lernen die gesetzlichen Anforderungen an die Tätigkeit kennen und können innerhalb Ihres Unternehmens den verantwortlichen Funktionen im Datenschutzbereich fachlich und kompetent zur Seite stehen.

Nächster Lehrgang: 20. - 24. 10. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

Technische Sicherheit: Lehrgang technische Grundlagen der IT-Sicherheit



Mehr Sicherheit dank sicherer Technik!

Die Teilnehmenden erlernen die technischen Grundlagen der IT-Sicherheit. Den Kursteilnehmenden werden die Risiken von Netzwerkinfrastrukturen aufgezeigt und mit praxisbezogenen Mitteln veranschaulicht. Durch das Ausführen von Attacken gegen Testsysteme lernen Sie auch die Vorgehensweise eines Angreifers und die notwendigen technischen Schutzmassnahmen praktisch kennen und verstehen.

Nächster Lehrgang: 22. - 25. 09. 2008

[Weitere Informationen und Anmeldeöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

ISO 27001 Lead Auditor: IRCA-akkreditierter Lehrgang mit offizieller Zertifizierung



Wissen und Know-how zu ISO 27001

Dieser Lehrgang führt Sie umfassend in das Auditing bezüglich ISO 27001 und ISO 27002 ein. Am Ende des Lehrganges erfolgt die Zertifizierung als ISO 27001 Lead Auditor. Dies ist ein IRCA-akkreditierter Lehrgang.

Nächster Lehrgang: 08. - 12. 09. 2008

[Weitere Informationen und Anmeldeöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

***NEU* Sicherheit am Arbeitsplatz: Grundlagen der IT-Sicherheit, sicherer Einsatz von IT-Mitteln, Schutz vor Social Engineering-Angriffen**



Lernen Sie sicher mit Ihren IT-Ressourcen zu arbeiten

Lernen Sie die Ihnen zur Verfügung stehenden IT-Mittel als Benutzer sicher einzusetzen und sich vor Social Engineering-Attacken zu schützen. Des weiteren lernen Sie Gefahren am Arbeitsplatz zu erkennen und aktive Notfallvorsorge zu betreiben. Zudem erhalten Sie alle Antworten auf die Frage [Was habe ich zu tun bei einem Brand, bei einem Unfall oder bei einer Gebäudeevakuatio[n]?]. Im Vorfeld haben Sie Zugriff auf ein eLearning-Modul zur Kursvorbereitung.

Nächster Themenkurs: 24. 09. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

***NEU* Professioneller Umgang mit Bedrohungen und Gewalt im Arbeitsalltag: Gefahrensituationen erkennen und Konflikte bewältigen**



Gehen Sie mit Bedrohungen und Gewalt in Ihrem Arbeitsalltag professionell um

Mit der zunehmenden verbalen oder körperlichen Gewaltbereitschaft einzelner Mitglieder unserer Gesellschaft gelangen wir immer häufiger in unangenehme, teilweise gefährliche Konfliktsituationen. Besonders bedroht sind Mitarbeitende, die direkten Kontakt mit gestressten, unzufriedenen oder sich falsch verstanden fühlenden, teilweise gewaltbereiten Kunden haben. Wir vermitteln Ihnen praxisorientiert sowie mit den erforderlichen Hintergrundinformationen und eindrücklichen Rollenspielen den sinnvollen Umgang mit verbalen Attacken wie Drohungen bei einem Kundengespräch oder beim Empfang, den Umgang mit einer telefonischen Bomben- oder Morddrohung gegenüber Entscheidern, Beratern, Managern usw. und das situationsgerechte Verhalten bei einer Geiselnahme oder körperlichen Auseinandersetzungen.

Nächster Themenkurs: 30. 10. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

ITIL Security Management: Grundlagen, praktische Umsetzung eines effizienten ITIL-konformen Security Managements



Security Management in einer ITIL-orientierten IT-Organisation

Sie erhalten Kenntnis von den Inhalten und Strukturen einer "Best Practice"-Informationssicherheit, und praktische Hilfsmittel zur qualitativen und quantitativen Einordnung des Themas Sicherheit in anderen ITIL-Disziplinen.

Nächster Themenkurs: 06. - 07. 11. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

Upgrade Lead Auditor BS 7799: Konvertierungskurs BS 7799 Lead Auditor zu ISO 27001 Lead Auditor



Wenn Sie den Lehrgang «BS 7799 Lead Auditor» besucht und erfolgreich bestanden haben, haben Sie die Möglichkeit, Ihren Titel in «ISO 27001 Lead Auditor» umzuwandeln. Dieser Konvertierungskurs informiert Sie über die wichtigsten Änderungen und Neuerungen des ISO 27001.

Nächster Konvertierungskurs: 22. 11. 2008

[Weitere Informationen und Anmeldemöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

***NEU* Integraler Sicherheitsmanager: Lehrgang für Sicherheitsbeauftragte mit offizieller SAQ-Zertifizierung**

Sicherheit ganzheitlich betrachtet! Mit der fünftägigen Ausbildung zum Integralen Sicherheitsmanager lernen Sie alles über die Einführung und Anwendung aus organisatorischen, rechtlichen, versicherungstechnischen, physischen, umweltspezifischen, IT-technischen, personellen, arbeitssicherheits- und gesundheitstechnischen Aspekten der Integralen Sicherheit. Sicherheit: umfassendes und praxisorientiertes Rüstzeug als Grundlage oder facettenreiche Repetition für einen Sicherheitsbeauftragten.

Nächster Lehrgang: 04.-06.05./15.-16.06.2009

[Weitere Informationen und Anmeldeöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

***NEU* ITIL Version 3 Foundation: Lehrgang mit offizieller Zertifizierung**

ITIL ® ist die allgemein anerkannte Grundlage für IT Service Management. Die mögliche Zertifizierung von IT-Organisationen nach ISO 20000 belegt dies eindrücklich. Die Teilnehmenden dieses Lehrganges sollen die Methodik von ITIL in seinen Grundzügen verstehen und anwenden können. Das Ziel ist die Erlangung des international anerkannten Zertifikats [ITIL Foundation].

Nächster Lehrgang: 15. - 17. 10. 2008

[Weitere Informationen und Anmeldeöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

***NEU* ITIL Version 3 Foundation Bridge: Konvertierungskurs ITIL ® Version 2 zu Version 3 mit offizieller Zertifizierung**

ITIL ® ist die allgemein anerkannte Grundlage für IT Service Management. Die mögliche Zertifizierung von IT-Organisationen nach ISO 20000 belegt dies eindrücklich. Die Teilnehmenden dieses Themenkurses sollen die neuen Ziele und Prozesse aus ITIL V3 kennen lernen und den Service Lifecycle-Gedanken erfassen können. Das Ziel ist die Erlangung des international anerkannten Zertifikats [ITIL V3 Foundation].

Nächster Themenkurs: 13. - 14. 11. 2008

[Weitere Informationen und Anmeldeöglichkeiten](#)

Quelle: Ausbildungsprogramm 4-2008, Swiss Infosec AG

[< zu den Themen](#)

BERATUNG

ISO 27001 / ISO 27002:



Führendes Know-how und über 19 Jahre Erfahrung machen die Swiss Infosec AG zu Ihrem Ansprechpartner Nummer 1

Die rasante Entwicklung sowie die fortschreitende Globalisierung im Bereich der Informationstechnologien stellen immer höhere Ansprüche an Mensch und Maschine. Integrität und Verfügbarkeit der Daten gewinnen weiter an Bedeutung. Die Anforderungen an IT-Systeme [eigene wie fremde] steigen stetig. Eine Möglichkeit um Transparenz hinsichtlich der Sicherheitseigenschaften von IT-Produkten zu schaffen, ist die Prüfung und Bewertung von IT-Produkten und -Systemen nach einheitlichen Kriterien durch unabhängige Stellen.

Der ISO 27002 beschreibt ein System, mit dem sichergestellt wird, dass bei der Entwicklung und Anwendung von IT-Systemen definierte Sicherheitsaspekte berücksichtigt werden. Zudem können IT-Systeme nach ISO 27001 auditiert und zertifiziert werden. Die Norm ist international anerkannt und unterstützt Unternehmen bei der Definition und Umsetzung einer optimalen Sicherheitsstrategie.

Mit ISO 27001 wird der Aufbau eines Informationssicherheitsmanagements (ISMS) beschrieben. Die Norm ISO 27001 hilft mittels

Empfehlungen und einfach formulierten Regeln – sog. Controls – dabei, die Informationssicherheit zu erhöhen und dabei den wirtschaftlichen, rechtlichen und unternehmerischen Ansprüchen gerecht zu werden. Informationen sind kritische Erfolgsfaktoren, die es dauernd und angemessen zu schützen gilt. Der Aufbau eines Informationssicherheitssystems ist hier die Antwort.

Profitieren Sie von über 19 Jahren Erfahrung und dem führenden Know-how der Swiss Infosec AG. Unsere Berater – einige davon lizenzierte ISO 27001 Lead Auditoren und IT-Grundschutz-Auditoren nach BSI – helfen Ihnen gerne weiter!

Beispiele rund um ISO 27001 und 27002:

- Erarbeitung und Umsetzung ISO 27001-konformer Security Frameworks
- Durchführung von ISO 27001-Sicherheitsaudits
- Vorbereitung einer Zertifizierung nach ISO 27001
- Toolunterstützung bei der Umsetzung von ISO 27001-Anforderungen
- Ausbildungen zu ISO 27001 und ISO 27002

Nicht Sicherheit um jeden Preis, sondern angemessene Sicherheit ist das Ziel.

Um dieses Ziel zu erreichen, erarbeiten unsere Berater zusammen mit Ihnen individuelle Lösungsansätze, zugeschnitten auf Ihre Bedürfnisse.

Erarbeitung eines Security Frameworks

Die Swiss Infosec AG erarbeitet zusammen mit den Kunden das Security Framework – eine umfassende, stufenweise aufzubauende und modulare Lösung, die sich u.a. aus folgenden Dokumenten zusammensetzt und vollumfänglich konform ist mit ISO 27001 und ISO 27002:

- die Security Policy als oberstes Strategiepapier
- das Security Concept mit den Anforderungen und der Sicherheitsorganisation
- das Security Regelwerk (Regelkatalog) mit Sicherheitsregeln

Durchführung von Sicherheitsaudits

Audits dienen dem Offenlegen von Schwachstellen und Sicherheitsmängeln sowie der Kontrolle der Wirksamkeit von Massnahmen. Sicherheitsaudits werden dazu benutzt, die praktische Umsetzung und Einhaltung von Sicherheitsmassnahmen innerhalb des Unternehmens zu kontrollieren sowie die Einhaltung und Tauglichkeit der Massnahmen durch jeden einzelnen Mitarbeiter zu überprüfen.

Beratung im Vorfeld einer Zertifizierung

Die Swiss Infosec AG unterstützt Sie bei der Vorbereitung einer Zertifizierung im Bereich ISO 27001.

Unterstützung durch ISMS Tool Box

Die Weiterentwicklung des bekannten Baseline Tool zur ISMS Tool Box bietet Ihnen die Möglichkeit zum Aufbau eines kostengünstigen ISMS inkl. Sicherstellung der Legal Compliance. Profitieren Sie darüberhinaus von der Erfahrung von über 40 Mitgliedern im ISMS Praxis Forum.

www.ismstoolbox.com

Ausbildung zu ISO 27001 und ISO 27002

Nur Swiss Infosec AG bietet Ihnen Beratung und Ausbildung aus einer Hand. Das ISO 27001- und ISO 27002-Ausbildungsangebot:

- **Einführung ISO 27001/27002:** Grundlagen und Überblick über die Normen und Standards im Bereich Informationssicherheit
- **Vertiefung ISO 27001/27002:** Praktische Anwendung und Nutzung der Normen und Standards im Bereich Informationssicherheit

- ▣ **ISO 27001 Lead Auditor:** IRCA-akkreditierter Lehrgang mit offizieller Zertifizierung
- ▣ **Upgrade Lead Auditor BS 7799:** Konvertierungskurs BS 7799 Lead Auditor zu ISO 27001 Lead Auditor

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Wir unterstützen Sie: Überbrückung von Ressourcen- oder Kompetenzengpässen: Kompetent, unkompliziert und flexibel



*Möchten Sie einen aktuellen Ressourcen- oder Kompetenzmangel überbrücken?
Möchten Sie Engpässe bei unternehmensinternen Projekten entschärfen?*

Die Swiss Infosec AG bietet Ihren Kunden projekterfahrene Spezialisten und Projektleiter an, die unkompliziert und kompetent Engpässe in einem Unternehmen überbrücken können. Unsere Spezialisten übernehmen Aufgaben und Projekte, setzen diese um und bringen sie erfolgreich zum Abschluss.

Kompetenz, Erfahrung und Erfolg. Swiss Infosec AG verfügt für Projekte im Bereich der Integralen Sicherheit sowie der Informations- und IT-Sicherheit über Spezialisten mit Know-how und Erfahrung. Die Swiss Infosec AG zählt organisatorische, konzeptionelle, rechtliche, ökonomische, psychologische, technische und physische Aspekte der Integralen Sicherheit, Informations- und IT-Sicherheit zu ihren Kompetenzen.

Wir unterstützen Sie. Seit 1989 bringt Swiss Infosec AG erfahrene Projektleiter und -mitarbeitende sowie Experten im In- und Ausland erfolgreich zum Einsatz. Aus dem Pool der Swiss Infosec AG werden Projektleitende mit mehrjähriger Projektleitungserfahrung eingesetzt:

- + zur Überbrückung von Kapazitäts- und Know-how-Engpässen
- + zur Verstärkung Ihrer Projektteams
- + zur Beschleunigung von Projekten
- + für den Know-how-Transfer.

Persönlich und flexibel. Unsere Spezialisten helfen Ihnen, Spitzenbelastungen erfolgreich abzudecken. Neben einer externen und neuen Sichtweise, die eine mögliche Betriebsblindheit kompensieren hilft, führt eine externe Unterstützung auch zu einem Know-how-Transfer.

Die von Ihnen ausgewählten Spezialisten können auftreten als Linien-/Stabsmitarbeiter, Projektleiter oder als Projektmitarbeiter: unsere Spezialisten in **Wort und Bild**.

Unsere Fachleute zeichnen sich aus durch ihre Motivation, Organisationsvermögen und Eigendisziplin sowie ihre Erfahrung in den Bereichen Projektleitung und haben Interesse an einer lösungsorientierten Zusammenarbeit mit direktem Kundenkontakt. Sprachen in Wort und Schrift: Deutsch, Englisch, Französisch.

Sie entscheiden wo und wann. Der Einsatz kann von Ihnen frei definiert werden. Wir unterscheiden zwischen frei einteilbarer Arbeitszeit und einzelnen Fixterminen bei Ihnen vor Ort oder fixem Einsatz vor Ort. Der Spezialist kann von Ihnen wie ein eigener Mitarbeiter eingesetzt werden. Der Umfang des Einsatzes kann wöchentlich/monatlich flexibel festgelegt werden. Das Mandat kann unkompliziert verlängert oder aufgelöst werden.

Jederzeit genau Ihrer Situation entsprechend und somit für jede Situation geeignet. **Einsatz nach Mass! Genau so lange und genau so, wie Sie es wünschen.**

Gerne stehen wir Ihnen für ein unverbindliches Gespräch zur Verfügung.
E-Mail infosec@infosec.ch; Telefon +41 (0)41 984 12 12.

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

Security Edutainments  mit Spass & Freude Security verstehen und lernen!:



Was mit Freude, unterhaltsam und anschaulich gelernt werden kann, hinterlässt einen grösseren Eindruck und motiviert Ihre Mitarbeitenden, die Inhalte näher kennen und verstehen zu lernen!

Anlässlich von 30- bis 120-minütigen Security Edutainments schult das Swiss Infosec-Team jeweils 5 bis 250 Mitarbeitende auf sehr unterhaltsame und nachweislich nachhaltige Art und Weise.

Ihre Vorteile

- + Innovative, beliebte und nachhaltige Form der Ausbildung: ein Erlebnis!
- + Kosteneffizienz aufgrund hoher Teilnehmeranzahl
- + Sowohl als Teil einer übergeordneten Awareness-Kampagne oder als selbstständige Massnahme durchführbar

[Hier erfahren Sie mehr](#)

Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

< zu den Themen

Informationssicherheit, dank der ISMS Tool Box: Das unentbehrliche Werkzeug für Sicherheitsbeauftragte!



Weshalb das Rad neu erfinden?

Effiziente und effektive Werkzeuge für Sicherheitsbeauftragte

Die ISMS Tool Box bietet vielfältige und praxisorientierte **Funktionalitäten und Inhalte** für den Aufbau, Betrieb und Unterhalt eines Information Security Management System (ISMS).

Die ISMS Tool Box ermöglicht Ihnen den Einsatz der einzelnen Tools in Ihren Bedürfnissen und Anforderungen entsprechend.

Als Lizenznehmer der ISMS Tool Box sind Sie gleichzeitig Mitglied des ISMS Praxis Forums.

Die ISMS Tool Box erlaubt Ihnen, **Regelwerke** schnell und einfach zu erarbeiten und diese **mehrsprachig intranetbasiert** zu kommunizieren. Vorbestehende Regelwerke seitens des Kunden können effizient und schlüsselfertig aufgenommen werden. Die Regelwerke können in einer Arbeitsgruppe elektronisch **reviewt und validiert** werden, die Umsetzung geplant und laufend überprüft werden.



Die ISMS Tool Box unterstützt neben dem **Ownership-Modell die Inventarisierung und Klassifizierung** von Schutzobjekten. Die für die Schutzobjekte verantwortlichen Funktionen können übersichtlich dargestellt werden. Business Continuity-Aktivitäten können mittels des Tools effizient und effektiv unterstützt werden.

Neben der Möglichkeit, ein **Glossar** und eine **Linksammlung** intranetbasiert zu führen, kann mittels des Tools auch ein **Security Incident Management** aufgebaut werden. Daneben existieren Instrumente für die Durchführung von **Risikoanalysen und Audits**. Dezentrale Stellen können mittels einer Self Assessment-Funktion in die Aufrechterhaltung und laufende Verbesserung des ISMS eingebunden werden.

Das Tool erlaubt den direkten intranetbasierten Zugriff

auf die aktuellsten Versionen ISO 27001/ISO 27002, COBIT, BSI-Grundschriftbuch und den **ISO Plus-Katalog der Swiss Infosec AG** jeweils **deutsch und englisch**. Der ISO Plus-Katalog ergänzt ISO 27002 mit konkreten, praxisorientierten Controls und enthält direkte Verknüpfungen zu unzähligen Musterlösungen des Standardwerkes der Swiss Infosec AG.

Mandantenfähigkeit, LDAP-Kompatibilität, Import- und Exportfunktionen, Reportgeneratoren und vieles andere mehr komplettieren die ISMS Tool Box. Daneben bietet Ihnen die ISMS Tool Box die Möglichkeit, innerhalb des ISMS Praxis Forums viermal jährlich Erfahrungen in einer geschlossenen Benutzergruppe auszutauschen.

Als Mitglied des ISMS Praxis Forums haben Sie exklusiven **Online-Zugriff auf die ISMS Tool Box Community**. Der ISO Plus-Katalog der Swiss Infosec AG wird innerhalb der Community laufend kommentiert und weiter entwickelt. Die ISMS Tool Box Community ermöglicht Ihnen neben der laufenden **Replikation der Reportinginstrumente** auch den direkten Zugriff auf das Release Management und die aktuellsten Programmversionen der ISMS Tool Box.

Erfahren Sie mehr über die umfassenden Funktionalitäten und wie Sie einfach und effizient Ihre Sicherheit organisieren.
www.ismstoolbox.com

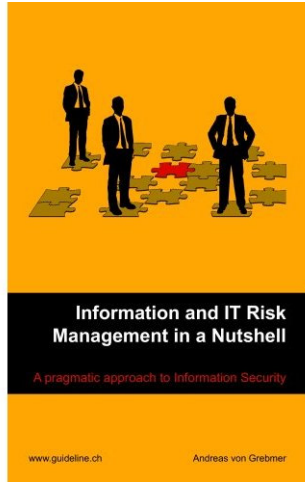
Quelle: Swiss Infosec AG in Bern, Sursee, Zürich

[< zu den Themen](#)

PUBLIKATIONEN

Neuerscheinungen: Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security: Andreas von Grebmer

Andreas von Grebmer



Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security

ISBN: 3833496584

[bestellen](#)

Quelle: www.amazon.de

[< zu den Themen](#)

Neuerscheinungen: Informationssicherheit und die Politik: Burak Gucer

Burak Gucer

Informationssicherheit und die Politik

ISBN: 1409203662

[bestellen](#)



Quelle: www.amazon.de

[< zu den Themen](#)

Neuerscheinungen: Records Management: Peter Toebak

Peter Toebak

Records Management

ISBN: 3039190598

[bestellen](#)



Quelle: www.amazon.de

[< zu den Themen](#)

Die Swiss Infosec AG ist seit 1989 das führende unabhängige Consulting- und Ausbildungsunternehmen der Schweiz im Bereich der Informations- und IT-Sicherheit sowie der Integralen Sicherheit.

Swiss Infosec AG unterstützt Sie bei

- Erarbeitung und Umsetzung umfassender Security Frameworks
- Vorbereitung und Zertifizierung nach ISO 27001
- Aufbau eines Information Security Management System (ISMS)
- Ereignis- und Krisenvorsorge inkl. Business Continuity Planning (BCP)
- Durchführung von Social Engineering Audits
- Durchführung von Audits in organisatorischen, rechtlichen und technischen Bereichen
- Konzeption und Umsetzung von Awarenesskampagnen
- Unterstützung und Überbrückung von Ressourcenengpässen

Die erfolgreiche Lösung von Aufgaben im Bereich der Informations- und IT-Sicherheit erfordert die interdisziplinäre Zusammenarbeit diverser Fachleute: 30 Sicherheitsspezialisten stehen Ihnen zur Seite und unterstützen Sie in der Funktion als Coach des Managements, IT-Leitung, IT-SIBE, als temporärer externer Security Officer, als Psychologe, Konfliktmanager und Mediator, als Auditor, Kursleiter oder externer Krisenmanager, als Begutachter, Jurist oder forensischer Experte, als neutrale Stelle und noch vieles mehr.

Sie möchten sich an- oder abmelden?

Sie erhalten dieses Mail als Abonnent der Internet Infosec News.

Möchten Sie die Internet Infosec News neu in Englisch erhalten, klicken Sie hier: **[News in Englisch](#)**

Möchten Sie die News zukünftig in TXT-Format erhalten, klicken Sie hier: **[News in TXT-Format](#)**

Möchten Sie eine andere E-Mail-Adresse anmelden, so klicken Sie bitte hier: **[Andere E-Mail-Adresse anmelden](#)**

Möchten Sie Informationen zur Swiss Infosec AG erhalten, klicken Sie bitte hier: **[Informationen bestellen](#)**

Möchten Sie zukünftig keine News mehr erhalten, so klicken Sie bitte hier: **[E-Mail-Adresse abmelden](#)**

Sollten Sie weitere Fragen und Anregungen haben, dann schicken Sie uns doch bitte ein Mail an: **infosec@infosec.ch**

SWISS INFOSEC

