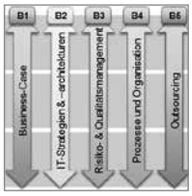
ISACA®
Trust in, and value from, information systems
Switzerland Chapter
Nr. 03 | September 2013 | www.isaca.ch
NEWSLETTER

Informationssicherheit
Heute braucht es andere Mittel, um die Informationssicherheit zu gewährleisten, sei es bei den KMU und im Bankenbereich. **Seite 69**



Data Loss Prevention
DLP als ganzheitliche Abwehrstrategie gegen den widerrechtlichen Abfluss von Daten **Seite 72**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 73**

Adieu Burg

Die IT-Sicherheitsinfrastruktur von KMU und antiquierter Burgen hatten früher eines gemeinsam. Für beide war es ausreichend das lokale Hoheitsgebiet vor Angreifern und Eindringlingen zu schützen. Die Anforderungen für KMU haben sich aber geändert, dicke Mauern allein reichen nicht mehr aus.

Von Markus Mangiapane, Berater, BSG Unternehmensberatung

Die alten Schutzmauern von Burgen hatten in der Vergangenheit nur einen Sinn, das eigene Territorium vor Angreifern zu schützen. Diese Analogie ist regelmässig bei Themen der IT-Security anzutreffen. Beim Unternehmen werden, wie bei einer Schutzmauer, Sicherheitszonen mit spezieller Hardware und Software aufgebaut, um so das eigene Netzwerk nach aussen hin abzuschotten. Doch in der heutigen Zeit reicht es nicht mehr aus, einfach nur eine dicke Mauer aufzubauen; es müssen andere Lösungen gefunden werden.

Paradigma Wechsel der Cyberattacken

In der aktuellen Fachpresse wird in letzter Zeit vermehrt von «Cyberspionage» oder «Cyberangriffen», vor allem gegen KMU berichtet. Unter dem Begriff Cyberangriff versteht man das Eindringen in fremde Computersysteme zum Zweck der Informationsgewinnung. Dabei spielt es keine Rolle, ob es sich um Geheimdienste handelt oder um einen einzelnen Angreifer, der sich einen wirtschaftlichen Vorteil verschaffen will.

Grossangelegte Angriffe, die wir aus der Vergangenheit mittels Viren und Malware kennen, hatten nur einen Zweck: Einen möglichst grossen Personenkreis zu treffen und dadurch einen grossen betriebswirtschaftlichen Schaden erzielen. Die aktuellen Cyberangriffe hingegen werden sehr individuell und konkret durchgeführt. Warum ist das so?

Das Ziel dieser Angriffe hat sich komplett verändert. Früher hatten die Angreifer das Ziel öffentliche Aufmerksamkeit zu erhalten, um auf diese Weise «Ruhm» zu erlangen. Je höher der betriebswirtschaftliche Schaden oder je wirksamer die Medienpräsenz war, desto erfolgreicher war ihr Unterfangen. Heute geht es um den Zugriff auf Informationen, welche sich weiterverkaufen lassen. Informationen wie zum Beispiel Rezepturen, Baupläne, technische Zeichnungen, Finanzzahlen eines Unternehmens, etc.

Gibt es eine Lösung für dieses Problem? Ja, es gibt einen vernünftigen und sinnvollen Lösungsansatz, um diesem Problem entgegenzuwirken.

Das Gesetz als Basis des Handelns

Die erste Frage, die es in diesem Zusammenhang zu beantworten gilt, lautet: *Gibt es rechtliche Vorgaben über die zu schützenden Daten durch den Gesetzgeber?*

Mit dem Datenschutzgesetz (DSG), dem Obligationenrecht (OR), dem Fernmeldegesetz (FMG) oder der Geschäftsbücherverordnung existieren eine ganze Reihe an rechtlich verbindlichen Vorgaben zum Thema Umgang und Schutz von Informationen. Es werden hier ganz klare Aussagen zum Schutz von Daten, dem Nachweis der Nichtveränderbarkeit, der Vertraulichkeit oder dem Postgeheimnis gemacht, die für alle Unternehmen verbindlich sind. Die rechtlichen Vorschriften nehmen die Verantwortlichen unmissverständlich in die Pflicht. Konkrete Massnahmen fehlen jedoch im Gesetzestext und müssen durch jedes Unternehmen selbst erarbeitet werden.

Wer ist innerhalb eines Unternehmens für die Daten und den Schutz derer verantwortlich?

In Bezug auf die Verantwortlichkeit ist festzuhalten, dass diese im OR ganz klar geregelt ist. Niemand anders als die Geschäftsführung ist für die Daten und dem daraus resultierenden Datenschutz verantwortlich. Diese Aufgabe kann zwar an eine Fachstelle delegiert werden, jedoch bleibt die Geschäftsleitung für die ord-

nungsgemässe Datenhaltung und den Datenschutz zuständig. Zur Geschäftsleitung gehören laut eines Urteils des Bundesgerichts alle Personen, die eine materiell leitende Position besetzen und auf das Funktionieren des Unternehmens einen massgeblichen Einfluss haben. Damit ist der Personenkreis grundsätzlich sehr weit gefasst und schliesst unter anderem den CIO mit ein.

Veränderte Anforderungen an die IT

Die Geschäftsanforderungen der KMU verändern sich. Früher hatten Unternehmen einen Standort, an dem, von der Verwaltung bis hin zur Produktion, alles vorhanden war. In der heutigen Zeit haben mittelständische Unternehmen oftmals mehrere Standorte, produzieren in verschiedenen Ländern und nutzen unterschiedlichste Infrastrukturen.

Mit diesen Geschäftsanforderungen verändern sich auch die Anforderungen an die Informatik. Sie muss die Geschäftsprozesse verstehen, sie mit IT-Mitteln unterstützen, den Betrieb sicherstellen, ihre Kosten im Griff behalten UND dabei den neuen Anforderungen Rechnung tragen. Wie sonst ist zu erklären, warum sich zum Beispiel das Thema «Bring your own device» seit geraumer Zeit immer in den Medien auftaucht. Der Wunsch, Daten immer und überall zu bearbeiten, ist omnipräsent. Auch andere Themen wie Cloud-Computing oder Unified Communication stellen die Informatik, und vor allem die Informationssicherheit, vor schier unlösbare Aufgaben. Aus den Unternehmen werden aktuell immer wieder die gleichen Forderungen laut:

- flexibles Arbeiten egal wann und wo
- Interne Daten sollen auf beliebigen Endgeräten, auch ausserhalb des Geschäftsnetzwerkes, verfügbar sein
- der Austausch von Daten mit Lieferanten, Kunden oder Dienstleistern.

Wie schafft die Informatik den Spagat zwischen den an sie gestellten Anforderungen bezüglich Leistungsfähigkeit, Flexibilität und gleichzeitig die Erfüllung der Informationssicherheits-Richtlinien bzw. den gesetzlichen Anforderungen?

Dies ist ein schwieriger Weg, der bereits in den Köpfen der Geschäftsleitung beginnen sollte. Jedoch fehlt dieser oftmals das Bewusstsein und das Verständnis für die Informatik.

Um den Handlungsbedarf einmal ganz klar aufzuzeigen, reicht es, zunächst mit folgender Fragestellung an die Informatik heranzutreten: «Wer hat alles Zugriff auf die wichtigsten Unternehmensdaten?» In der Regel ist die Antwort so erschreckend wie ausreichend, um das benötigte Verständnis zu wecken. Hier wird meistens festgestellt, dass zu den vom Dateneigner berechtigten Personen noch unzählige andere Personen auf unternehmenskritische Daten Zugriff haben.

Diese Problemstellung kann weiter vertieft werden, indem sich die Unternehmen die Frage nach den Auswirkungen bei Verlust oder Diebstahl ihrer unternehmenskritischen Daten stellen. Hier kommt die Prüfung sehr schnell zum Ergebnis, dass der Verlust wichtiger und geschäftskritischer Informationen ein hohes Risiko mit sehr grossem Schadenspotenzial darstellt.

Hier treffen wir auf «des Pudels Kern»: Die Angst, Daten gänzlich oder an Mitbewerber zu verlieren und dadurch nicht mehr wettbewerbsfähig zu sein, ist gross. Daher werden zum Teil technisch aufwendige Infrastrukturen aufgebaut, welche die gesamte Informatik wie eine antiquierte Wehrmauer schützen sollen. Dies erzeugt oftmals nur eines – eine Scheinsicherheit!

Denn: Was passiert in der Realität bei den KMU? Es werden Daten aus dem internen Netzwerk auf ungeschützte mobile Endgeräte gespeichert, Informationen in der Cloud, wie z. B. DropBox, etc. ungenügend geschützt abgelegt und eine unbestimmte Anzahl an Personen wie Mitarbeiter, Informatiker oder externe IT-Dienstleister dürfen und können auf wichtige Unternehmensdaten zugreifen. Die Devise lautet in der Regel: Bequemlichkeit und Funktionalität vor Sicherheit!

Was kann das Unternehmen konkret dagegen tun?

Die Schutzbedarfsanalyse

Eine geeignete und praktikable Möglichkeit, diese Fragestellung in den Griff zu bekommen, ist die Durchführung einer Schutzbedarfsanalyse.

Hier werden in einer ersten Phase die für das Unternehmen relevanten Business Prozesse herausgearbeitet. Anschliessend wird pro Prozess definiert, wie wichtig und widerstandsfähig dieser innerhalb des Unternehmens sein muss, um einen stabilen Betrieb zu gewährleisten. Die Informationen diesbezüglich kommen nicht von der Informatikabteilung sondern von den Prozessverantwortlichen, die beurteilen können, wie sich Schadenszenarien konkret auf die Prozesse auswirken.

In einer Schutzbedarfsanalyse werden die Fragen nach Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Arbeitsprozessen oder Daten beantwortet. Zudem können die Prozesse nach ihrer Kritikalität priorisiert werden. Diese Informationen sind die Basis für sinnvolle und praktikable Sicherheitskonzepte. Mit diesen Konzepten ist es dann wiederum möglich, die kritischen Prozesse entsprechend der Schutzbedarfsanalyse, mit allen technischen und organisatorischen Möglichkeiten, zu schützen.

Zusätzlich werden alle vorhandenen Daten und kritischen Applikationen identifiziert und anschliessend klassifiziert. So können die unternehmenskritischen Informationen von unwichtigen unterschieden werden.

Diese unternehmenskritischen Daten gilt es, mit allen technischen und organisatorischen Möglichkeiten vor unbefugtem Zugriff zu schützen. Dies kann in letzter Konsequenz auch dazu führen, dass diese Daten das interne Netzwerk nicht verlassen dürfen. Diese dürfen dann weder in einer E-Mail auf mobile Endgeräte repliziert, auf USB-Sticks oder CDs kopiert oder ausgedruckt werden.

Fazit

KMU müssen noch mehr zum Schutz der eigenen Informationen tun. Die Bedrohung durch direkte und unvermittelte Angriffe auf die Netze der Unternehmen durch hochprofessionelle Cyberkriminalität ist real. Die Zeiten, in der man sich von dicken Burgmauern schützen lassen kann, sind vorbei. Deshalb muss die Informationssicherheit einen anderen Stellenwert erhalten und mit Nachdruck angegangen werden. Denn: Hier ist noch ein erheblicher Nachholbedarf festzustellen.

Im Bereich der Informationssicherheit ist auch für die KMU angebracht, externe Unterstützung beizuziehen. Gerade bei den Themen Durchführung einer Schutzbedarfsanalyse oder der Beurteilung IT-rechtlicher Fragen sind die Spezialisten gefragt.

Jetzt gilt es mehr denn je Konzepte zu erarbeiten um das eigene Know-how vor dem Verlust durch Industriespionage in Form von Cyberangriffen zu schützen. Der Verlust eigener Informationen an einen Mitbewerber, welcher sich dadurch einen «unlauteren» Wettbewerbsvorteil verschaffen kann, stellt ein erhebliches Risiko für das gesamte Unternehmen dar.

DER AUTOR

Markus Mangiapane ist Berater bei der BSG Unternehmensberatung und dort für den Bereich Informationssicherheit und IT-Management zuständig.
Markus.mangiapane@bsg.ch; www.bsg.ch

Informationssicherheit in der Bankenbranche

Die Banken werden mit neuen Herausforderungen an die Informationssicherheit konfrontiert, einerseits aufgrund der sich stetig verändernden Gefährdungslage, andererseits auch aufgrund sich verändernder Geschäftsmodelle und neuer regulatorischer Anforderungen.

Von Tom Schmidt, Partner EY, EMEIA Financial Services Advisory

Nachdem sich die Banken in letzter Zeit intensiv mit dem Thema «Data Leakage» auseinandergesetzt haben, gewinnt nun das Thema «Cybersecurity» zunehmend an Wichtigkeit. Unter dem aktuellen Kostendruck verändern sich zudem auch die Geschäftsmodelle der Banken, einschliesslich der Frage nach der Sourcing-Strategie und mit den damit verbundenen Auswirkungen auf die Informationssicherheit. Dabei haben die Banken den zunehmenden regulatorischen Anforderungen bezüglich Informationssicherheit ebenfalls entsprechend Rechnung zu tragen.

Cybersecurity-Vorkehrungen auf verschiedenen Ebenen

Das Thema Cybersecurity hat in letzter Zeit an Bedeutung gewonnen und die Management-Ebene in vielen Unternehmen erreicht. Die Kompromittierung der Informationssicherheit durch Angriffe aus dem Internet ist grundsätzlich nicht neu. Neu ist jedoch die Intensität und Grösse der (erfolgreichen) Angriffe und die durch die Medien begünstigte öffentliche Wahrnehmung dieser. Sowohl die Angriffsmethoden als auch die Angriffswerkzeuge haben eine neue Qualität erreicht. Dass solche Angriffe nicht nur durch private, sondern auch durch staatliche Organisationen durchgeführt werden, erschwert die Situation für die betroffenen Unternehmen zusätzlich.

Die Herausforderungen für die Banken und für weitere Unternehmen, insbesondere für jene, welche einen Teil der kritischen Infrastruktur eines Landes bilden, werden über die kommenden Jahre laufend zunehmen. Es ist deshalb wichtig, dieses Thema aus gesamtheitlicher Sicht anzugehen und entsprechende Vorkehrungen auf verschiedenen Ebenen zu treffen. Aus technologischer Sicht geht es vereinfacht gesagt darum, die Systeme am Perimeter (Übergang von öffentlichen Netzwerken und unternehmensinternen Netzwerken) und die sensitiven Daten möglichst an der Quelle (data centric) angemessen zu schützen.

Informationssicherheit bei Sourcing-Vorhaben

Aufgrund des herrschenden starken Kostendrucks beschäftigen sich viele Banken mit dem Sourcing-Thema, das heisst unter anderem mit der Fragestellung, welche Systeme, Applikationen und Daten in der Wertschöpfungskette ausserhalb der Bank kostengünstiger betrieben und unterhalten werden können. Eine Auslagerung zieht Fragen zur Informationssicherheit nach sich, und insbesondere bei einer Auslagerung ins Ausland steigen die gesetzlichen und regulatorischen Anforderungen an die Informationssicherheit.

Voraussetzung für eine gesetzeskonforme Auslagerung von Systemen, Applikationen und Daten ist eine darauf ausgerichtete Architektur derselben. Grundsätzlich gilt: Sensitive Daten sollten möglichst sparsam in Applikationen, Datenbanken und Dateiablagen gespeichert werden. Dies vereinfacht einerseits den Schutz der sensitiven Daten und andererseits die Auslagerung von Systemen und Applikationen, welche keine sensitiven Daten enthalten. Die sensitiven Daten sollten möglichst an der Quelle (data centric) geschützt werden, da die Wirksamkeit des Perimeter-Schutzes durch den Einsatz von mobilen Geräten und durch die sich aufweichenden Systemgrenzen zwischen den Unternehmen zunehmend abnimmt.

Regulierung und Selbstregulierung

Die Regulierungsdichte für Finanzunternehmen hat in den letzten Jahren stark zugenommen und stösst nun vermehrt auch in den Informationssicherheits-Bereich vor. Zum einen hat die SBVg letzten Herbst ihr Positionspapier zum Thema DLP veröffentlicht. Auch wenn die SBVg selber keine regulatorischen Vorgaben für die Bankbranche erlässt, nimmt sie als Verband des Schweizer Finanzplatzes doch eine wichtige Rolle bezüglich Selbstregulierung wahr. Das DLP-Dokument umfasst zahlreiche Kontrollen, welche im Rahmen von 62 Datenabfluss-Szenarien adressiert werden. Die Szenarien decken allerdings nur einen allfälligen Abfluss von Daten aufgrund von internen Bedrohungen ab, jedoch nicht externe Bedrohungen für die Informationssicherheit, wie beispielsweise Industriespionage oder Hackerangriffe.

Zum anderen wird die FINMA demnächst eine verbindliche Vorgabe verabschieden, welche regulatorische Anforderungen bezüglich der Vertraulichkeit von Kundendaten formuliert. Die Anforderungen der FINMA werden weniger granular sein als die Kontrollen im SBVg-Dokument, adressieren aber interne und externe Gefahren.

Anforderungen von morgen schon heute berücksichtigen

Die Gewährleistung der Informationssicherheit wird für die Banken auch in Zukunft eine erhebliche Herausforderung darstellen, sowohl aus organisatorischer als auch aus technischer Sicht. Die Banken sind deshalb gut beraten, sich bereits mit den zukünftigen Veränderungen und Anforderungen zu beschäftigen und diese in aktuell laufenden Projekten entsprechend zu berücksichtigen.

DER AUTOR

Tom Schmidt
Ernst & Young AG
Partner
EMEIA Financial Services Advisory

Ernst & Young AG
Belpstrasse 23
3001 Bern

DLP: Zum Wohle Ihrer Unternehmensdaten

Der widerrechtliche Abfluss von kritischen Geschäftsdaten kann existenzbedrohend sein. Data Loss Prevention (DLP) in Verbindung mit den richtigen Prozessen ist ein wichtiger Baustein einer ganzheitlichen Abwehrstrategie.

Viele Unternehmen setzen ein breites Arsenal von Sicherheitsmassnahmen ein, um unerwünschten Datenverlust vorzubeugen. Typische Lösungen wie Firewalls und Anti-Virus Software können wirksam auf die Bedrohung von aussen reagieren. Allerdings übersieht dieser Ansatz einen wichtigen Aspekt: In der Regel stellen die eigenen Mitarbeitenden das grösste Risiko für einen schädlichen Informationsabfluss dar.

Zwei aktuelle Beispiele dazu: Der fehlgeschlagene Datendiebstahl durch einen Mitarbeitenden beim Nachrichtendienst des Bundes im Herbst 2012[1] oder die Steuersünder-CD[2] mit gestohlenen Bankkundendaten, die sogar zu einem länderübergreifenden juristischen und politischen Schlagabtausch geführt hat.

Mitarbeitende mit krimineller Energie gehen meist nach dem gleichen Muster vor: Sie entwenden vertrauliche Geschäftsdaten unbemerkt aus dem Unternehmen, indem sie diese auf einen mobilen Datenträger kopieren bzw. an eine externe, meistens private Email Adresse senden. Danach können sie die Informationen mit hohem wirtschaftlichem Wert an Dritte verkaufen oder weitergeben.

DLP als Retter in der Not

DLP-Lösungen helfen, den Datenabfluss aus dem Unternehmen zu überwachen und unerwünschten Datenverlust zu verhindern. Die Abbildung zeigt eine thematische Übersicht zu DLP.

Der Schutz von DLP-Lösungen erstreckt sich auf persistent abgelegte Daten (Data-at-Rest), aktuell bearbeitete Daten (Data-in-Use) wie auch auf Daten, welche sich in der Übertragung befinden (Data-in-Motion).

Gegenmassnahmen können sowohl passiv (Detektion), als auch aktiv (Prävention) umgesetzt werden. Detektion überwacht den ausgehenden Datenabfluss auf verdächtige Muster und schlägt beim Erreichen von festgelegten Schwellwerten Alarm. Durch das technische Unterbinden von bestimmten Operationen kann präventiv ein widerrechtlicher Informationsabfluss verhindert werden. Vorstellbar in diesem Zusammenhang ist beispielsweise das Blockieren von Drucken oder Kopieren auf mobile Speichergeräte und Versenden von sensiblen Daten.

Praxistauglichkeit

Bevor man sich für die Einführung einer DLP-Lösung entscheidet, muss im Vorfeld untersucht werden, wie DLP die im Unternehmen bestehenden Sicherheitskonzepte und -lösungen am besten unterstützt, damit ein klarer Mehrwert geschaffen werden kann.

In der Praxis hat es sich bewährt, die Arbeiten zur Initialisierung, Konzeption und Überprüfung von DLP-Lösungen in folgende Bausteine zu gliedern:

- B1: Business-Case
- B2: IT-Strategien und –architekturen
- B3: Risiko- und Qualitätsmanagement
- B4: Prozesse und Organisation
- B5: Outsourcing
- B6: Audits und Assessments inklusive Gap-, SWOT- sowie Kosten-/Nutzenanalysen

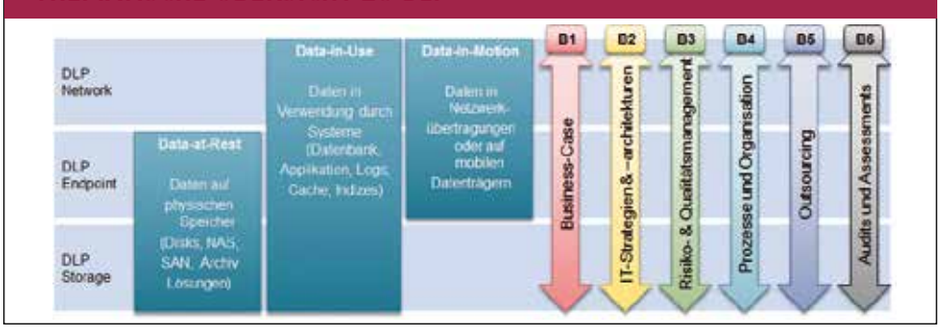
Um eine DLP-Lösung erfolgreich betreiben zu können, müssen die kritischen Daten bekannt sein. Diesem Schritt wird oftmals nicht die notwendige Aufmerksamkeit geschenkt, wodurch suboptimale Lösungen umgesetzt werden. In diesem Zusammenhang bietet der Baustein Audits und Assessments professionelle Unterstützung.

DLP ist als Teil einer sogenannten «Defense-in-Depth» (Verteidigung in der Tiefe)-Strategie zu betrachten. An dieser Stelle leisten DLP-Lösungen einen wertvollen Beitrag zum Schutz der Daten über deren gesamten Lebenszyklus hinweg, d. h. von der Erzeugung über die Bearbeitung bis hin zur Archivierung.

1) http://grundrechte.ch/CMS//medienmitteilung-vbs.html

2) http://de.wikipedia.org/wiki/Steuers%C3%BCnder-CD

THEMATISCHE ÜBERSICHT ZU DLP



DIE AUTOREN

Dr. Adrian Marti ist Leiter des Kompetenzbereichs Informationssicherheit der AWK Group adrian.marti@awk.ch, www.awk.ch/de/kompetenzen/informationssicherheit

Tarkan Bas ist Senior Consultant im Kompetenzbereich Informationssicherheit bei AWK Group

Dr. Philipp Grabher ist Consultant im Kompetenzbereich Informationssicherheit bei AWK Group

Über die AWK Group

AWK ist mit rund 140 Mitarbeitenden eines der grössten Schweizer Beratungsunternehmen für Informationstechnologie. Wir sind schweizweit tätig mit Standorten in Zürich, Bern und Basel. Unsere Dienstleistungen umfassen Consulting, Engineering und Projektmanagement.

Informationen des Verbands

Vier neue «Schweizer» Zertifikate

Cyber Security, Data Loss Prevention, IAM usw. sind eigentliche Mode-Themen, die schon vor vielen Jahren da waren und immer wieder unter neuen Begriffen auftauchen. Propagiert werden jeweils spezifische Sicherheitsmassnahmen, die oft sehr teuer sind und auch nicht unbedingt nachhaltig wirken.

Sinnvoller wäre es daher in den meisten Fällen, einerseits in stabile Managementsysteme und andererseits in eine fundierte Ausbildung der Mitarbeitenden zu investieren – dies ist in der Regel wesentlich nachhaltiger und kann die Wirkung von Investitionen in die Sicherheit vervielfältigen.

Das ISACA Switzerland Chapter bietet zwei Mal pro Jahr eine berufsbegleitende Aus- und Weiterbildung für Sicherheitsspezialisten an. Der 14tägige Kurs mit Präsenzunterricht, ausführlichen und klar strukturierten Unterlagen (und Hausaufgaben!) vermittelt ein umfassendes Fachwissen und bereitet auch auf die internationale CISM-Prüfung (Certified Information Security Officer) vor. Analoge Ausbildungen bestehen auch für CISA (Certified Information System Auditor), CGEIT (Certified in the Governance of Enterprise IT) und CRISC (Certified in Risk and Information Systems Control).

Für erfahrene Personen mit wenig Zeit offeriert das Switzerland Chapter vier neue «Schweizer» Zertifikate: AUD (Zertifiziert in IT-Revision), ISM (Zertifiziert in Informationssicherheitsmanagement), GOV (Zertifiziert in IT-Governance) und IRM (Zertifiziert in IT-Risikomanagement). Die neuen Zertifikatskurse umfassen jeweils:

- umfangreiches Skript zur Vorbereitung und als Nachschlagewerk
- vier Tage Unterricht mit Handouts aller Präsentationen, Gruppenarbeiten und Fallstudien
- Pausen- und Mittagsverpflegung an allen Kurstagen
- einfache Fallstudie mit Korrektur und Benotung sowie Lösungsvorschlag
- 3–4 kleine Online-Prüfungen als Vorbereitung
- Zertifizierung durch das ISACA Switzerland Chapter

Weitere Informationen erhalten Sie über www.isaca.ch oder unser Sekretariat.

ISACA-TRAINING

17.09.2013	SAM-VD	**Software Asset- und Lizenz-Management (SAM&SLM)**
18.09.2013	LM5-VD	**Software Asset Management - Lizenzmodelle der Top5-Hersteller aus Revisionssicht**
23.09.2013	ACC-IPG	**Wirksamer Zugriffsschutz (Access Control)**
24.09.2013	AHS	**ISACA AHS September**
30.09.2013	ISMS-KK	**ISMS gemäss ISO 27000 implementieren und verbessern** Wirkungsvolles Sicherheitsmanagementsystem in 30 Schritten
04.10.2013	STR-KK	**Strategische Ausrichung von Geschäft (Business) und Informatik (IT)**
07.10.2013	RIM-KK	**Risikoprüfung und kontinuierliche Risikoüberwachung**
08.10.2013	IKS-KK	**Design, Betrieb und Überwachung von Kontrollen**
www.itacs.ch		
23.9.-25.9.13	COB-FD	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
14.-15.10.13	COB-IG	**ISACA Implementing Governance of Enterprise Using COBIT (Deutsch)**
18.-19.11.13	COB-IG	**ISACA Implementing Governance of Enterprise Using COBIT (Deutsch)**
25.11.-27.11.13	COB-FD	**ISACA COBIT 5 Foundation Zertifikat von ISACA**
www.glenfis.ch		

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
Erscheinungsweise: 4x jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch

Copyright: © Switzerland Chapter der ISACA