Artikel Cyber-Risiken & Audit im dynamischen Umfeld

Die Audit-Methodik und der Prüfungsumfang müssen laufend den neusten technologischen Veränderungen angepasst und erweitert werden, um die effektive Cyber-Sicherheit beim zu prüfenden Unternehmen wirksam beurteilen zu können.

Hier kommt die Frage des „Wie", da zurzeit keine Cyber-Gesetze oder Regulationen existieren.
Für den Auditor stellt dies eine sehr grosse Herausforderung dar, denn er muss die mit den enormen Veränderungen in der IT Entwicklung verbundenen Cyber-Risiken und Herausforderungen beim Vorgehen im Audit berücksichtigen. Obwohl die Auditing Standards ISA 315 (*International Standard on Auditing*, Dez 2013) die Ausgangsschritte für das Vorgehen aufzeigen, muss der Auditor in der Lage sein, die technische Vielfalt der Angriffsmöglichkeiten, die neuen Methoden zur Erkennung der Angriffe, sowie die Verantwortlichen im Unternehmen (Management, Verwaltungsrat) in seinen Audit mit einzubeziehen.

Das Cyber-Audit Vorgehen basiert auf dem Austausch von Erfahrungen und Empfehlungen von Fachleuten im Bereich Audit und IT Audit sowie auf den angelehnten Prozessbeschreibungen, bspw. dem *Cybersecurity Framework NIST* (*National Institute of Standards and Technology*, Feb 2014).

Der sich laufend ausweitende Einsatz des Cloud-Computings hat die Cyber-Risiken nochmals zusätzlich massiv verstärkt.

1. Entwicklung in der IT und Geschäftsvorteile

Die Entwicklungen in der IT im letzten Jahrzehnt haben ein schnelles Tempo erreicht: Mobile-Wireless und Netz-Technologie, Cloud-Computing, vernetzte und virtualisierte Plattformen oder Big-Data Anwendungen. Die Fortschritte ermöglichen strukturierte Veränderungen der IT Umgebung, wie Einführung alternativer Sourcing-Strukturen, Hosting oder Cloud-Computing. Diese Veränderungen haben für die Unternehmen grosse Kostenvorteile gebracht: Sie können ihre Anbindungen an die Dritt-Lieferanten und Kunden verbessern. Ein Beispiel dafür ist die Cloud-Lösung, welche wesentliche Kosteneinsparungen gegenüber der Verwaltung der Daten im eigenen Rechenzentrum bietet:

- Aus der strategischen Sicht ist das Unternehmen effizienter, dynamischer und unabhängiger von der IT-Investition.
- Aus der ökonomischen Sicht werden die globalen operativen Kosten reduziert, die Verfügbarkeit und Kapazität der Daten erhöht und der Einsatz neuer effektiverer IT-Produkte oder IT-Dienstleistungen ermöglicht.

Folglich fragt **das Management *„Wie schnell und wie kann vom Cloud-Einsatz profitiert werden?"***
Der Auditor sollte aber die Frage stellen: *„Wie sicher ist die Geschäftsleitung, dass mit Ihren Cloud Plänen die Vorteile erreicht werden?"* Konkret sollte der Auditor das Management mit folgenden Fragen konfrontieren:

- Wie ist die strategische Geschäftsausrichtung mit der Informatik synchronisiert?
- Wie unterstützt die Informatik das Geschäft?
- Basieren die IT-Investment-Entscheide auf den Business-Anforderungen?
- Bleibt die Verantwortung für die Daten innerhalb der Firma, auch wenn sie von der Sicherheit der externen Systeme ausserhalb der Firma abhängig ist?

1.1 Verändertes Geschäftsumfeld generiert neue Bedrohung

Der Drang nach Geschäftsvorteilen aus der Entwicklung von neuen Informatik- und Telekommunikationstechnologien ist gross, können jedoch auch erhebliche Risiken und Governance-Herausforderungen mit sich bringen.
Zwar bringen diese Technologien viele Annehmlichkeiten bei der täglichen Arbeit mit der Informatik, gleichzeitig aber eröffnen sie Hackern, Betrügern und Virenprogrammierern unzählige Möglichkeiten, um Computersysteme anzugreifen und – für den Benutzer nicht erkennbar – dabei die Vollkontrolle des Computers zu übernehmen. Für das Unternehmen entsteht eine neue Bedrohung - *die Cyber-Kriminalität*.

2 Cyber-Kriminalität – die globale Bedrohung

Bei den Cyber-Attacken können Kriminelle oder auch andere Interessengruppen (Konkurrenten, staatliche und private Organisationen, etc.) die bestehenden Schutzmassnahmen häufig einfach umgehen. Die existierenden Sicherheitsmassnahmen bspw. die Absicherung der logischen Schichten durch Firewalls mit Policies (Internet, Applikation-Server, Datenbank, Server) genügen nicht mehr um solche Angriffe mit Erfolg abzuwenden. Das bedeutet, dass sich das Cyber-Risiko auch auf die Unternehmen bezieht, welche keinen Einsatz neuer Technologien planen. Durch die weltweite Vernetzung praktisch aller Informatik-Systeme über das Internet haben Angreifer weltweit innerhalb von Bruchteilen von Sekunden Zugriff auf alle am Internet angeschlossenen Systeme. Dabei können unsere traditionellen Rechtssysteme praktisch beliebig umgangen werden.

«Immer mehr Kriminelle nutzen die Geschwindigkeit, Gelegenheit und Anonymität des Internets, um unterschiedliche kriminelle Aktivitäten zu begehen, welche keine physischen oder virtuellen Grenzen kennen» ***(Quelle: Interpol)***

Als Reaktion haben bereits 44 Staaten die Konvention über Cyber-Kriminalität ratifiziert und 9 Staaten unterzeichnet. Cyber-Kriminalität hat drei Bereiche: i) Attacke gegen Computer HW oder SW, Netzwerke, ii) Finanzdelikte iii) Personen und Firmen-Schädigung.

2.1 Situation in der Schweiz

«Eines der grössten Probleme im Zusammenhang mit der Nutzung des Internets ist heute die Datensicherheit», erklärt Markus Martinides, Cyber-Experte von der im Bereich Sicherheitsanalysen spezialisierten *Firma SUA Telenet GmbH*. *«Insbesondere für Firmen, die über vertrauliche Daten verfügen, aber auch für Private ist es wichtig, kontrollieren zu können, wer bzw was auf interne Daten zugreift und ob diese unerlaubt verändert oder sogar gelöscht werden*.» Aus diesem Grund sind in der Schweiz nicht nur die grossen Institutionen wie Versicherungen, Banken oder Industrieunternehmen sondern auch KMU Betriebe wie Arztpraxen und Anwaltskanzleien ebenso wie Spitäler, Gemeinden und Kantone bedroht.

Die gängigen Firewalls bieten dabei immer weniger Schutz. Denn sogenannte *Zombies* (Codes, die sich via Internet auf dem System installieren und dann Daten vom System nach aussen schicken), können sich oft völlig unbemerkt installieren und bleiben von Antivirenprogrammen und Firewalls vollkommen unerkannt. «*Oftmals sind solche Programme lange Zeit aktiv und spionieren das Netzwerk aus, bevor sie bemerkt werden*», so Markus Martinides. Tür und Tor werden Viren und Hackern beispielsweise durch die Verwendung von z.B. nicht überprüfter USB-Sticks geöffnet. Ein weiteres Problem ist, dass immer mehr Angriffe über sehr komplexe Technologien wie Javascripts laufen die verstärkt im Bereich der Internet-Browser zum Einsatz gelangen.

3 Cyber-Governance ist Management Aufgabe

„Cyber-Kriminalität wächst und ist auf dem 4.Platz aller kriminellen Taten. Cyber-Kriminalität ist nicht das Technologie Problem, es ist das Business- und das Strategie-Problem". Quelle: *PWC 2014 Crime-Survey*

Aus der Spezifikation der Management Aufgaben geht hervor, dass die Verantwortung für die Daten auf der Top-Ebene des Unternehmens bleibt:

„*Die primäre Verantwortung des Verwaltungsrats und des Managements ist die Absicherung der Zukunft des Unternehmens. Dabei müssen neben offensichtlichen Ereignissen auch verstecke Ereignisse eines Cyber-Angriffs, die auf Grund fehlender Warnsysteme gar nicht erkannt werden können, berücksichtigt werden. In der Praxis wird ein schwerwiegender Datenverlust oft zu spät erkannt und hinterlässt dann bleibende wirtschaftliche Schäden am Unternehmen".*

Der Verwaltungsrat sollte sich deshalb bewusst sein, dass es Cyber-Risiken gibt. Konsequenterweise ist die Cyber-Kriminalität ein Geschäftsthema, welches im Audit an Verwaltungsrat oder Management adressiert werden soll, z.B. mit der Frage: „*Wie wird die Cyber-Kriminalität im Unternehmen wahrgenommen?"* Dabei gibt es keinen Unterschied zwischen externem oder internem Audit, da das Ziel gleich ist, d.h. die Erkennung der Risiken und die Übernahme der Verantwortung.

3.1 Prinzipien für Corporate Governance

Die Verbesserung der Aufsicht über die Cyber-Risiken kann in folgenden Schritten erzielt werden:

1. Der Verwaltungsrat soll das Vorgehen bei Cyber-Sicherheit als **unternehmensweites Risk-Management positionieren – nicht nur als IT-Risiko.**
2. Der Verwaltungsrat soll die juristischen Konsequenzen der Cyber-Risiken verstehen, da sie sich auf unternehmens-spezifische Umstände beziehen.
3. Der Verwaltungsrat soll ausreichenden Zugriff zur Cyber-Sicherheit Expertise haben und die Diskussionen über Cyber-Risiko-Management sollten ausreichende Zeit auf seiner Agenda bekommen.
4. Der Verwaltungsrat sollte eine Richtlinie an das obere Management herausgeben, dass ein unternehmensweites Cyber-Risiko-Management-Framework aufgebaut wird mit genügend Personal und Budget.
5. Cyber-Risiken können nicht einfach durch den Abschluss einer Daten-Verlustversicherung gelöst werden.
6. Die Diskussion zwischen VR und Management sollte die Identifikation der tatsächlichen Cyber-Risiken und deren effektiven Abwehr durch organisatorische und technische Massnahmen beinhalten.

3.2 Audit Fragen an Verwaltungsräte

Der Auditor soll folgende Fragen an die Verwaltungsräte stellen können:

1 Wendet das Unternehmen ein Sicherheitsframework an?
2 Welche sind die Top fünf Risiken im Unternehmen, welche auf Cyber-Sicherheit bezogen sind?
3 Wie sind sich die Angestellten bewusst über ihre Rolle in Bezug auf Cyber-Sicherheit?
4 Sind die externen und internen Bedrohungen bei der Planung des Cyber-Sicherheit Programms beachtet worden?
5 Wie ist die Sicherheits-Governance innerhalb des Unternehmens geregelt?

6 Gibt es einen konkreten Notfallplan im Falle einer Cyber-Attacke?

4 Cyber-Risiken

4.1 Neue Risiko Quellen verursachen grössere Cyber-Angriffsflächen

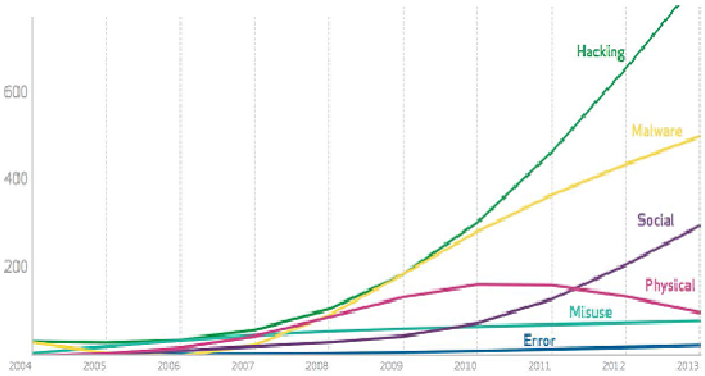
Die Cyber-Kriminalität „profitiert" von den, durch IT-Fortschritt erzeugten, neuen Risiko Quellen, welche vor allem mit dem Cloud-Computing Einsatz, mit Konzepten wie „Bring-Your-Own-Device" (BYOD) mobilen Geräten und Applikationen sowie mit der Auslagerung der für Business kritischen IT-Bereichen, entstanden sind. Die neuen Risiko Quellen haben die Cyber-Angriffsflächen vergrössert: i) Schwachstellen in den Applikationen, ii) Remote-Zugriffe, iii) Nicht effektives Änderungs-Management, iv) Schwach implementierte Netzwerksicherheit, v) mangelnde kontinuierliche Echtzeit Überwachung, vi) Schwachstellen/Risiken bei Drittfirmen vii) Fehlende Datenaufbewahrungs-Richtlinien.

4.3 Cyber-Risiken und Folgen

Die Risiken der Cyber-Kriminalität sind: i) Datenverlust, ii) Bedrohungen im Datenschutz-Bereich, iii) Verlust der Kontrolle über Zugriff auf die Daten iv) Verlust der Verfügbarkeit der Daten im Betrieb.
Die Folgen der Cyber-Attacke können dem Unternehmen weitreichenden Schaden zufügen wie: i) Verlust der Wettbewerbsfähigkeit, ii) grosse Gewinnverluste, iii) Verlust der Reputation, iv) Ruf Schädigung, v) Compliance-Probleme.

4.4 Cyber-Situation

Die Cyber-Bedrohung wird kritisch, da die Hacker sich auf den Missbrauch sensitiver oder finanziell wertvoller Information oder auf die Störung der wichtigen operativen Bereiche fokussieren. Dabei ist der Anstieg von Attacken dramatisch, da die Hacker-Bedrohungen und Sicherheits-Einbrüche nicht nur in der Anzahl exponentiell wachsen (siehe Bild 1), sondern ihre Methoden haben sich kontinuierlich weiterentwickelt und sind ausgeklügelter konstruiert.



Quelle: Verizon 2014 Data Breach Investigation Report

Bild 1: Wachsende Anzahl der Hacker Angriffe

Weiterhin ist die heutige Lage in Bezug auf die Erkennung von Hacker-Attacken sehr schwierig:

„Es dauert durchschnittlich 229 Tage bis eine erfolgreiche Hacker-Attacke auf dem Netzwerk entdeckt wird".
Quelle: Mandiant, IT-Sicherheitsunternehmen – veröffentlicht im 2013 Bericht, indem China im direkten Zusammenhang mit Cyber-Spionage gestellt wurde.

Sehr viele Daten können in dieser Zeit vom Unternehmen unbemerkt ausgeforscht, verändert und gelöscht werden. Viele Angreifer richten sich einen versteckten Remote-Zugang ein, der es ermöglicht Informationen erst bei „Bedarf" als bezahlte Dienstleistung gegenüber Ihren Auftraggebern hochzuladen.

4.5 Massnahmen

Die Massnahmen, mit welchen sich das Unternehmen gegen Cyber-Angriffe wehren kann, beziehen sich nicht nur auf die Einführung von technischen Abwehrmechanismen sondern beinhalten auch organisatorische und strukturelle Schritte:
Aus der technischen Sicht müssen zuerst die geschäftskritischen und schutzrelevanten Daten von den Verantwortlichen klassifiziert werden, die IT Spezialisten können danach die Verarbeitung, Aufbewahrung sowie die Flüsse dieser Daten identifizieren. *„Welches sind wirklich die wichtigsten und wertvollsten Daten?"* Die Informationen mit Preisen, Verkaufszahlen, Kunden Datenbanken, Herstellverfahren etc sind sehr oft weniger geschützt als Salär Daten. Mit der Identifikation und Klassifizierung der Daten wird erst die effektive Einführung der technischen Schutzmassnahmen (Sicherheit –Tools, Netzwerk-Absicherung) ermöglicht. Auf der organisatorischen Seite müssen die Richtlinien sowie das Sensibilisierungs-Programm auf die neue Situation angepasst und eingeführt werden. Die Einführung der Schutz und Kontroll-Massnahmen sind mit dem Aufbau von Überwachungs-Methoden, Erweiterung der Organisation und der Kompetenzen verbunden. Die Recherchen bei den Sicherheitsorganisationen sind dabei sehr hilfreich.

Folge für Audit und Revision: *Das Audit Vorgehen und der Prüfungsumfang müssen erweitert werden, um die Cyber-Sicherheit bei Unternehmen beurteilen zu können. Da stellt sich die Frage „Wie?“, da zurzeit keine Cyber-Gesetze oder Regulationen existieren.*

5 Cyber-Audit & Vorgehens-Methodik

5.1 Cyber-Audit Aufbau

Der Auditor muss mit der Analyse der Situation beginnen. Um die Themen und Aufgaben planen zu können, muss er dazu seine Experten-Kenntnisse ausbauen. Um die Rolle der Revision wahrnehmen zu können muss der Auditor ein komplettes Bild über das IT-Umfeld bekommen, d.h. welche Bereiche in den Audit Umfang gehören. Als Ausgangs-Basis dienen die bestehenden Audit-Standards und Vorgehens-Methoden, welche die internen Kontrollen und Risiken spezifizieren.

6.2 Themen & Aufgaben

Der Audit der Cyber-Risiken erweitert sich um die Themen i) IT Governance und Assurance, ii) IT Sicherheitsstrategie inkl. Richtlinien und Vorgaben, iii) Implementierungen iv) Projekt Risk-Management. Zu den Aufgaben des Auditors gehören Beurteilung der Cyber-Bedrohungen und Risiken, der Kontrollprozesse inkl. ihrer Maturität und IST-SOLL Analyse sowie der Kommunikation mit Verwaltungsrat, Management, Geschäfts und IT Verantwortlichen.

6.3 Cyber-Sicherheit – Assurance Expertise

Welche Expertise muss erlangt werden um die Cyber-Risiken beurteilen zu können? In der Tabelle unten werden die erforderlichen Kenntnisse zusammenerfasst:

Expertise und Forschung Bereiche für die Cyber Security Assurance	
Risk Assessment und Management	Beurteilung der Netzwerk Sicherheit
Entwicklung der Sicherheits- und Zugriff-Management-Politiken	Implementation der Einbruchmelde-Systeme, forensische- und Notfall-Prozesse
Entwicklung der Sicherheit-Bewusstsein innerhalb der Organisation und Empfehlung der Prozesse	Schutz des Privates und erhöhte Sensibilisierung
Implementierung und Integration der Sicherheits-Tools und Anwendungen	Implementierung zeitgemässen Infrastrukturen und Anwendungen
Beurteilung der Software und IT-Architektur für Sicherheit	Erkennung der neuen Richtungen Einbezug der Auffassung der Spezialisten

Bild 2: Erforderliche Kenntnisse

6.4 Cyber und Interne Kontrollen

Die Ausgangbasis für den Cyber Audit ist bereits in den *Auditing Standards ISA 315 International Standard on Auditing, Dezember 15, 2013, der International Federation of Accountants (IFAC)* vorhanden, wo klares Verständnis für Business und Interne Kontrollen spezifiziert ist:

Absatz	Thema
A21	«Verständnis über Unternehmens Kontroll-Aktivitäten: Wie das Unternehmen auf die durch IT initiierte Risiken reagiert»
A39	«IT Betrieb – Potenzial der Risiken für Business»
A103	«Einsatz von IT beeinflusst Implementierung der Kontrollen. Aus der Sicht des Auditors, Effektivität der Systeme hängt von Effektivität der IT Kontrollen»
Appendix 2	Risiko Indikatoren «Inkonsistenz zwischen IT-Strategie und Business Strategie»

Bild 3: ISA 325 Standards

6.5 IT und interne Kontrollen – Nutzen und Risiken

IT hat grossen Nutzen für die internen Kontrollen indem es zuverlässige Resultate gewährleisten kann, erweitert die Basis an Informationen und ermöglicht die Verkleinerung der Kontroll-Risiken:

ISA 315 Absatz 62 – Risk Assessment Prozeduren
Konsistente Anwendung vordefinierter Geschäftsregeln
Erweiterte Aktualität, Verfügbarkeit und Richtigkeit
Behandlung zusatz-Analysen der Information
Erweiterte Fähigkeit zur Überwachung der Performanz der Aktivitäten, Politiken und Prozeduren
Reduzieren die Risiken der ineffizienten Kontrollen
Erweiterung der Fähigkeit der effektiven Aufgabetrennung durch Implementierung der Sicherheitskontrollen in IT.

Bild 4: IT Einsatz und Interne Kontrollen

Auf der anderen Seite stellt IT für die internen Kontrollen grosse Risiken dar:

ISA 315 Absatz 63 – Risk Assessment Prozeduren
Anhängigkeit von Systemen und Programme mit fehlerhafter Datenverarbeitung, Verarbeitung fehlerhafter Daten
Unautorisierter Zugriff auf Daten: Zerstörung, Beschädigung
Zugriff Behandlung zusatz-Analysen der Information
Umgehen der Zugangsrechte, Bruch der Aufgabentrennung
Unautorisierte Veränderung der Daten
Fehler bei System, Programm Anpassungen
Ungeeignete manuelle Intervention
Verlust der Daten oder der Zugriffe

Bild 5: Interne Kontrollen und Risiken

5.7 IT-Cyber relevante IT-Umgebung

Der Auditor muss sich zuerst eine Übersicht verschaffen im Unternehmen betreffend: IT-Organisation, IT-Infrastruktur und den assoziierten Risiken, wie die IT-Prozesse und Applikation gemanagt sind und welche Dienstleistungen aktuell an Drittfirmen ausgelagert sind. Dabei muss er in seinem Bericht die Risiken nachweisen und beurteilen können.
Die Cyber relevante Umgebung hat folgende Bereiche

- Personen und Organisation
- Applikationen, Infrastruktur und IT-Prozesse
- Verständnis der IT Umgebung und der geplanten Änderungen
- Rolle der IT im Business
- Compliance Regeln und Verordnungen

Für den Aufbau der Cyber-Sicherheit ist wichtig das Gesamtbild in einem Framework darzustellen, welche die Situation, Prozesse sowie Profile umfasst, damit das Vorgehen beim Audit mit dem Kunden festgelegt werden kann.

5.8 Cyber-Sicherheits-Framework

Das Cybersecurity Framework NIST (*National Institute of Standards and Technology, Feb 2014*) hilft dem Auditor die Situation abgestimmt und transparent in Quervergleichen beurteilen zu können. Das Framework besteht aus drei Bereichen: 1. Basis Framework, 2. Implementierung in Schichten, 3. Framework Profile:

1. **Basis Framework** -beinhaltet Funktionen, Aktivitäten, Resultate und Referenzen, welche die Priorisierung der Cyber Sicherheit relevanten Entscheide ermöglichen. Im Basis Framework wird der Aufbau der Cyber Sicherheit als ein kontinuierlicher Prozess mit fünf Funktionen definiert:

Funktionen	Kategorie	Aktivität
1. Identifikation	Organisation	Aufbau der Prozesse für das Management der Cyber Risiken und der technischen Fähigkeit: Überwachung
2. Schutz	Organisation Technologie	Implementierung der organisatorischen und technologischen Schutzmassnahmen: Zugriffskontrolle
3. Detektieren	Technologie	Implementierung der Mechanismen zur Aufdeckung der Cyber Ereignisse: DDOS, Logging, Monitoring
4. Reagieren	Organisation	Einführung der Aktivitäten zur Bekämpfung der Cyber Ereignisse: Isolierung, Entfernung, Forensic, Gesetz
5. Recovery	Organisation Technologie	Wiederherstellung der Systeme: Planung und Implementierung der Massnahmen um die betroffene Systeme zurück in Betrieb zu nehmen

Bild 6: Kontinuierlich laufende Funktionen im Basis Framework

2. **Implementierung in Schichten** – beinhaltet vorhandene Cyber-Sicherheit Messwerte, mit welchen die Tiefe der erfüllten Vorgaben der Sicherheitsprozesse (Maturität) beurteilt werden kann:

Bild 7: Schichten vermitteln die Qualität der Sicherheitsprozesse

3. **Framework Profile** - beinhaltet die Beurteilung der existierenden Position sowie die Spezifikation der zu erreichenden Ziele der Cyber-Sicherheit und somit wird die Erfüllung der Prioritäten und Festlegung der Roadmap ermöglicht:

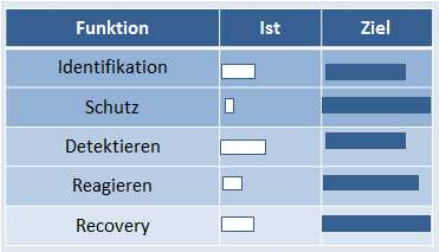


Bild 8: Roadmap für die Beurteilung der Fortschritte

Der vollständige Artikel inkl. des Vorgehens beim Aufbau der Cyber-Sicherheit und mit dem Beispiel des Cyber Audits beim Cloud Einsatz kann aus den Web Seiten www.acons.ch und www.sua-tele.net heruntergeladen werden.

Zusammenfassung

Wichtige Schlüsse für den Audit der Cyber-Risiken:

1 Cyber-Governance & Assurance hat Business-kritische Bedeutung
2 Jede Organisation kann von Cyber-Attacken betroffen werden
3 Management muss wissen, wo die Business-Risiken bei der Wertschöpfung der IT-Prozesse liegen.
4 Audit und Risk-Management Pläne müssen Cyber-Themen beinhalten.
5 Cloud-Computing ist mit der Business Strategie verbunden.

Literatur

- Cybersecurity Framework NIST (National Institute of Standards and Technology, Feb 2014)
- Cybersecurity What the Board of Directors Needs to Ask, 2014, IIARF Research Report
- Auditing Standards ISA 315 International Standard on Auditing, Dezember 15, 2013, der International Federation of Accountants (IFAC
- Transforming cybersecurity using COBIT5, 2013, ISACA
- US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey, PWC
- PwC's 2014 Global Economic Crime Survey
- Interpol and National Cyber Crime Investigation & Research
- Responding to Targeted Cyberattacks, 2014, ISACA & EY
- ISACA Journal, Volume 1, 2015
- IIA POSITION PAPER: „The three lines of defence in effective risk management and control"

Jiri Cejka, Senior Manager, Acons Governance & Audit AG
IT-Governance Spezialist
E-Mail: jiri.cejka@acons.ch
Tel: +41 44 224 3030
Homepage: www.acons.ch

Studium: Dipl. El.-Ing, Fach technische Kybernetik, CISA, Quality Auditor ISO9000

Bereiche: GRC, BCM, IT and Cyber Sicherheit, IT Risikomanagement
Fachkompetenzen: IT, IT Audit, Programm Management
Seit 2007 bei ISACA prüft Jiri weltweit das Lernprogramm *„IS Audit and Control"* an den Universitäten

Markus Martinides, CEO der im Bereich ICT-Sicherheit tätigen Firma SUA Telenet GmbH (seit 2001)
Unabhängiger IT-Sicherheitsexperte
E-Mail: info@sua-tele.net
Tel: +41 52 647 4141
Homepage: www.sua-tele.net
Security Portal: www.sec-check.net

Studium: ETH Zürich Nachrichten- und Informationstechnologien (1986)
Bereiche: Informatik, Mobil-, Richtfunk-, Daten- und Sprachkommunikation. Fachkompetenzen: IT-Sicherheit, Projektmanagement
Fokus: Übergreifende Plattformanalysen, d.h. Netzwerk-, Client- und Serversicherheit von Multivendor-Betriebssystemen und Cloud Architektur.
Mitglied bei: ISACA seit 2007 www.isaca.ch und ISSS Information Security Society Switzerland (ISSS) www.isss.ch sowie Dozent an der UZH MedLAW (Medizin - Ethik - Recht)