Trust in, and value from, information systems

Nr. 01 | März 2017 | www.isaca.ch

Switzerland Chapter NEWSLETTER

ISACA-SVIR Fachtagung
Rückblick auf die gemeinsame Konferenz von SVIR und ISACA am 19. Januar 2017 in Zürich
Seite 69

Security Innovation
Aktuelle Bedrohungen durch Cyber-Kriminalität. Neue Risiken erfordern technische Innovationen Seite 70

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder Seite 72

ISACA-SVIR-Fachtagung «Cybersecurity – ein Fall für Revisoren?»

Dieser Frage widmete sich die gemeinsame Fachtagung von ISACA-CH und SVIR, die am 19. Januar im Hotel Four Points in Zürich stattfand.

Die voll ausgebuchte Konferenz zeugte von einem nach wie vor sehr aktiven Interesse am ausgeschriebenen Thema. Revisoren und Security-Experten aus verschiedensten Branchen setzten sich an diesem Tag mit ganz unterschiedlichen Facetten zu diesem Thema auseinander.

Zu Beginn bot **Thomas Ribi** (NZZ) den Anwesenden eine philosophische Annäherung an die zunehmende Digitalisierung, deren Konsequenzen für die Privatsphäre und wie manche Menschen nur noch mit Mühe die Grenze zwischen der natürlichen und virtuellen Welt zu ziehen vermögen. Eine überraschend spannende philosophische Auseinandersetzung für die anwesenden Techniker und Praktiker.

Die strategischen Konsequenzen der zunehmenden Digitalisierung wurde im Referat von **Dr. Daniel Diemers** (PWC) beleuchtet: Neue technologische Möglichkeiten schüren innovative Ideen und lassen neue Geschäftsmodelle entstehen. Mit einem entsprechenden Balance-Akt gilt es, diese innovativen Pflänzchen nicht mit regulatorischen Druck zu ersticken und dennoch ein adäquates Mass von Guideline und Governance zu definieren.

Dr. Lukas Ruf (Consecom AG) analysierte in seinem Referat zwei grössere Cyberattacken und legte den Fokus insbesondere auf die Schilderung wie die beiden betroffenen Firmen in dieser Situation reagierten: War innert nützlicher Frist der Schadenumfang bekannt und konnten die betroffenen Kunden und die Öffentlichkeit zeitnah informiert werden? Vorbereitende Schutzmassnahmen und Szenario basierte Reaktionspläne helfen einer Unternehmung sich auf solche Situationen vorzubereiten.

Wie sich Cyberangriffe auf Energieunternehmen über die letzten Jahre zunehmend häuften schilderte **Reto Amsler** (swissgrid) in seiner Ausführung. Die zunehmende Digitalisierung im Energiebereich erzeugt neue Angriffsflächen für Cyberattacken. Neben der Implementierung entsprechender Abwehrmassnahmen sieht Reto Amsler aber auch eine Notwendigkeit, dass europaweite Cyber-Sicherheitsvorgaben für die Energiebranche etabliert werden.

Seinen Vortrag zu «IT Grundschutz vs. Cyber Security» fasste **Luc M. Pelfini**

(BDO) zusammen mit dem Zitat: «Erst die Pflicht, dann die Kür». Ein engagiertes Plädoyer, dass die schon lange bekannten Grundschutzmechanismen konsequent angewendet werden. Bevor im Detail über Cyberangriffe diskutiert wird, soll eine angemessene und wirksame Informationssicherheit und ein stabiler und sicherer IT-Betrieb implementiert sein.

Dr. Carin Gantenbein (Zurich Insurance Group) referierte über die zunehmende Nachfrage von Versicherungsmodellen zum Schutz von Cyberrisiken. Massgeschneiderte Versicherungslösungen die einerseits risikobasierend gewichtet und anderseits eine Vielzahl von unternehmensspezifischer Faktoren berücksichtigen sind gefragt. Eines der key takeaways des Referats betont die aktuelle Realität für Unternehmen: If you're online, you're a target.

Die Fachtagung wurde abgerundet mit einem Erfahrungsbericht von **Dr. Peter Weiss** (Swiss Re) über die Prüfung der Cyber Security Governance. Erläuterungen zum Vorgehen, Bezugnahme auf Standards und den definierten Kontrollzielen wurden geschildert. Eine umfassende Liste von Erfahrungswerten zu den Stakeholder im Audit, dem Scoping (Umfang) des Audits und den Resultaten rundete dieses Referat und die Tagung ab.

Am Ende des Tages waren sich alle Teilnehmer einig: Cybersecurity ist definitiv ein Fall für Revisoren. Der Tagesmoderator, Ulrich Engler fasst die Tagung folgendermassen zusammen: *«Sehr aufmerksam haben die Teilnehmenden den Ausführungen der hochkarätigen Referenten zugehört. Das Thema ‹Cybersecurity – ein Fall für Revisoren› hat offenbar den Nerv der Zeit getroffen. Ja, Cybersecurity ist ein Fall für Revisoren, wir sollten uns tatsächlich an der Diskussion beteiligen.»* Daniela Gschwend, die Präsidentin von ISACA CH kommentiert ergänzend, dass sie neben den Referaten auch das Networking mit den Gästen bereichernd erlebt hat und fühlt sich angespornt, weitere Veranstaltungen in dieser Form zu planen.

Nach einer mehrjährigen Pause war diese Fachtagung wieder die Erste, die in Zusammenarbeit von SVIR und ISACA geplant, inhaltlich strukturiert und durchgeführt wurde. Der ISACA-Vorstand erachtet diesen Anlass als Erfolg, da diese Form eine hervorragende Gelegenheit bietet, aktuelle Themen umfassender zu betrachten und nicht nur IT-fokussiert zu diskutieren. Mitorganisatoren für zukünftige Anlässe können sich direkt bei president@isaca.ch melden.

DER AUTOR

Peter Marti, CISA, im Vorstand des ISACA Switzerland Chapters. Seit 18 Jahren in der Informatik in verschiedensten operativen und strategischen Funktionen. Heute interner IT-Auditor bei der Bank Julius Baer.

Aktuelle Bedrohungen durch Cyber-Kriminalität

Weltweit wächst die Bedrohung durch Cyber-Kriminalität für Unternehmen aller Branchen und Grössen. Im vergangenen Jahr wurden mehr als 36 Prozent aller Unternehmen weltweit Opfer von Cyber-Kriminalität.[1)] Cyber-Kriminalität steht damit in den Statistiken auf Platz 2 der häufigsten Arten von Wirtschaftskriminalität – Tendenz steigend.[2)] Weltweite Vernetzung, Digitalisierung und virtuelle Zusammenarbeit sowie Industrie 4.0 bieten Cyber-Kriminellen neue Angriffsflächen.[3)] Die Produktion wird digitalisiert und Maschinen werden über das Internet vernetzt, wodurch neue Möglichkeiten und Angriffsformen der Cyber-Kriminalität entstehen.

Cyber-Kriminalität verursacht bei einem einzelnen Angriff im betroffenen Unternehmen einen sehr hohen Schaden. Neben den primären Kosten zur Abwehr des Angriffs und der akuten Schadensbehebung kommen häufig hohe Folgekosten auf die betroffenen Unternehmen zu. Der deutsche Digitalverband Bitkom beziffert, basierend auf einer unter mehr als 500 Unternehmen in 2016 durchgeführten Umfrage, einen Schaden von rund 350 Milliarden Euro pro Jahr für die globale Wirtschaft.[4)]

Studien zeigen, dass der Grossteil von Cyber-Angriffen nicht veröffentlicht wird, dennoch gelangen in den vergangenen Jahren immer mehr Cyber-Angriffe in die Medien.

Im Jahr 2014 kam es beispielsweise zu einem der bis heute grössten Diebstähle von Zugangsdaten zu E-Mail-Konten, bei welchem rund 18 Millionen Nutzer betroffen waren. Kriminelle wendeten dabei die Vorgehensweise des Phishings an. Dabei werden Nutzer auf manipulierte Webseiten gelockt und dort aufgefordert, Daten einzugeben. Alternativ wird häufig Schadsoftware eingeschleust, welche entsprechende Informationen ausspioniert (bspw. beim Online-Banking oder Einkauf).[5)] Da als Schwachstelle hier in

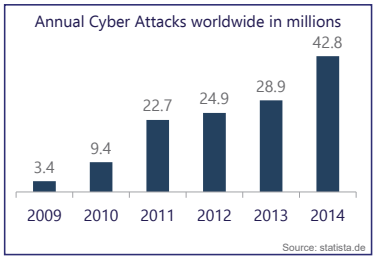
1) Global Economic Crime Survey 2016, PWC, http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html
2) Ebd.
3) Bitkom, 2016, https://www.bitkom.org/Presse/Presseinformation/Industrie-im-Visier-von-Cyberkriminellen-und-Nachrichtendiensten.html
4) http://www.internetworld.de/technik/cybercrime/cyberattacken-verursachen-milliardenschaeden-909741.html
5) Handelsblatt, 2014, http://www.handelsblatt.com/technik/vernetzt/cyberkriminalitaet-schneller-gegen-den-datenklau/9728412.html

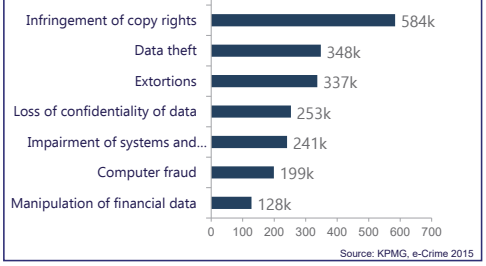
der Regel E-Mail-Accounts eine Rolle spielen, ist jedes Unternehmen dieser Gefahr ausgesetzt. Auch ein internationaler Logistik Dienstleister wurde im Sommer 2016 Opfer eines Phishing-Angriffs, bei welchem E-Mails mit gefälschtem Absender an Kunden des Dienstleisters versendet wurden. Im Anhang dieser gefälschten Mails versteckte sich ein Virus, mit dem Kriminelle an Kundendaten gelangen wollten.[6)]

Ein weiteres Beispiel der aktuellen Cyber-Kriminalität zeigt eine Reihe von DDoS (Distributed Denial of Service)-Attacken, die im März 2016 auf Schweizer Unternehmen durchgeführt wurden. Eine DDoS-Attacke stellt einen Angriff dar, bei dem die Verfügbarkeit eines Computers, Servers oder einer Webseite ausser Kraft gesetzt werden soll. Der Angriff erfolgt dabei von einer grossen Anzahl verteilter Rechner, bspw. durch die Zusendung enormer Mengen fehlerhafter IP-Pakete – solange, bis der attackierte Dienst aufgrund von Überlastung nicht mehr funktionsfähig ist.

Neben DDoS-Attacken kam es vor allem zu Datendiebstählen. Beim grössten Fall in 2016 sollen über 30 Millionen Kunden-Accounts gehackt worden sein.[7)]

"Cybercrime is a fast-growing area of crime." (Interpol, 2016)





Security Innovation – Lösungsansätze

Um durch Digitalisierung und Vernetzung neu entstandene Sicherheitslücken zu schliessen und um immer ausgefeilter agierende Cyber-Kriminelle abzuwehren sind an vielen Stellen Neuerungen in der Cyber Security gefragt. Neue Risiken erfordern technische Innovationen, die häufig sehr spezifische Sicherheitslücken in den IT-Systemen der Unternehmen schützen sollen.

Viele nationale und internationale Firmen haben bereits erkannt, dass innovative Security-Lösungen in Israel aktuell stark wachsen. Bedingt durch die von Militär und Forschung geprägte Kultur bietet Israel ein dichtes Netzwerk von Cyber Security Experten.

Generell können die folgenden sieben Handlungsfelder der Cyber Security abgegrenzt werden, in denen nach aktuellem Entwicklungs- und Forschungsstand innovative Lösungen verfügbar sind:

1. **Mobile Security:** Ziel ist es, die Geräte vor den aktuellen Gefahren, die mit Mobile und Wireless Computing in Zusammenhang stehen zu schützen, z.B. durch Anwendungen zum Lost Device Management und Tools zur proaktiven Mobile Protection. Start-Ups im Bereich Mobile Security bieten innovative Lösungen zum Schutz für Mobile Devices sowie die Aufdeckung von Cyber-Attacken in Echtzeit.[8)]
2. **Data and Information Security:** In der Praxis basieren Lösungsansätze zum Schutz von digitalen Daten gegen unautorisierten Zugriff häufig auf Anwendungen zur Data Leakage Prevention und Encryption Tools.
3. **Network Security:** Mit Fokus auf Mobile Devices und Transaktionen bieten z.B. Authentication as a Service (AaaS) Anwendungen, häufig ergänzt um Key Management Solutions, Schutz vor unautorisierten Zugriffen auf das jeweilige Unternehmensnetzwerk. AaaS Anwendungen werden sowohl als Cloud-Lösungen sowie auch als On-Premise-Anwendungen.
4. **Cloud Security:** Um unbefugten Zugriff und somit Missbrauch einer Cloud zu verhindern kommen häufig Single-Sign-On Lösungen zum Einsatz, unterstützt durch Analytics Tools, die widerrechtliche Zugriffe frühzeitig erkennen können. Innovative Lösungen, basieren auf einer Cloud Access Security Plattform, die verschiedene relevante Security Tools miteinander kombiniert.[9)]
5. **Identity and Fraud Security:** Der Fokus in diesem Bereich liegt auf der Authentifizierung der Identitäten, die auf ein System zugreifen, häufig ergänzt um Monitoring-Anwendungen zur frühzeitigen Erkennung und zur Vorbeugung von Fraud. Beispielsweise kommen dazu Anwendungen der Detection Analysis und Security Tokens zum Einsatz sowie umfassende End-to-End Fraud Prevention Lösungen, die z.B. Transaktionen, Bestellungen, Workflows und Prozesse kontrollieren und prüfen.
6. **Penetration Monitoring and Reporting:** Mit Hilfe von Penetration Tests werden Schwachstellen eines Systems aufgedeckt, oder im Falle eines bereits erfolgten Hacker-Angriffs dieser forensisch rekonstruiert. Varianten des Testings sind z.B. external und internal Testing sowie Blind Testing, bei dem im Vorfeld nur sehr wenige Informationen über das System zur Verfügung gestellt werden um einen möglichst realistischen Angriff zu simulieren.
7. **Infrastructure and Industrial Security:** Lösungsansätze zum Schutz von kritischen Infrastrukturen kombinieren in der Regel verschiedene andere Bereiche um umfangreichen Schutz zu erzeugen, z.B. Access Controls und Network Security Anwendungen. Aktuell gibt es u.a. Lösungen für ICS und SCADA Umgebungen an. Dabei werden einzelne Bestandteile der Umgebung mit einem Schutzschild versehen, das automatisierte Ausrollen von Security-Policies wird dadurch effizienter gestaltet.[10)]

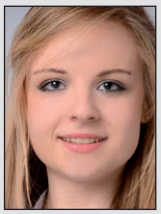
Jährlich exportiert Israel Cyber Security Services, Knowledge und Solutions im Wert von rund 3 Milliarden US-Dol-

6) SRF, Juni 2016, http://www.srf.ch/news/schweiz/phishing-angriff-mit-malware-auf-post-kunden
7) Der Westen, Juni 2016, http://www.derwesten.de/wirtschaft/digital/hack-von-twitter-daten-legt-riesigen-daten-diebstahl-nahe-id11901389.html
8) Skycure, https://www.skycure.com/skycure-for-citrix/
9) Adallom, https://techcrunch.com/2015/09/08/microsoft-confirms-purchase-of-cloud-security-firm-adallom/
10) NextNine, https://nextnine.com/solutions/ics-shield/

lar. Grosse internationale Konzerne wie bspw. die Deutsche Telekom, Cisco und IBM betreiben Research Center, sogenannte Cyber R&D Center, in Israel um sich in der Forschung zu innovativen Security Lösungen einzubringen. Diese Entwicklung wird sich in den kommenden Jahren verstärken. Für Unternehmen, die im Kampf gegen Cyber Security Risiken neue Lösungsansätze suchen ist daher ein Blick in Richtung Israel lohnenswert.

DIE AUTOREN

Andrea Tribelhorn, Senior Security Specialist und seit über 6 Jahren im Security-Bereich der Detecon (Schweiz) AG mit Projektleitungsrollen in verschiedenen Security-Projekten, u.a. zu den Themen Cyber Security, IoT, Data Analytics, Anonymisierung und Pseudonymisierung.



Annika Sophie Schewior, seit über 2 Jahren bei Detecon (Schweiz) AG im Bereich Security, Compliance & Risk Management. Dort befasst sie sich mit den Themen Cyber Security und Security Innovation in verschiedenen Publikationen und Projekteinsätzen.

Matthias Gruber, Leiter des Bereichs Security und Compliance Management bei der Detecon (Schweiz) AG mit verschiedenen Projektleitungs- und Steuerungsmandaten zu den Themen Cyber Security, Business Resilienz und Informationsschutz nach ISO27001.

ISACA AFTER HOURS SEMINARE

Donnerstag, 16. März 2017, 16:30–17:30 Uhr
(in Anschluss an die Vereinsversammlung)

Thema: Cyber Incident Response – The Last Line of Defense
This presentation looks at a sample of cyber incidents whose resolution we supported and draws conclusions on processes, tools, lessons learned and pitfalls when designing a cyber incident response capability.

Referent: Dr. Klaus Julisch, Deloitte

Die weiteren Termine 2017

- 4. April 2017, 16.40 Uhr in Bern
- 6. Juni 2017, 16.40 Uhr in Zürich

➤ Die detaillierten Ausschreibungen aktualisieren wir laufend auf unserer Webseite

ISACA-TRAINING

Datum	Hauptthema – Kurstitel
1.2.*; 12.–29.06.2017	CISA Vertiefungskurs: 10 Tage
11.–14.10.2017	CISA Repetitionsblock / Prüfungstraining: 4 Tage
1.2.*; 12.–29.06.2017	CISM Vertiefungskurs:10 Tage
19.–21.10.2017	CISM Repetitionsblock / Prüfungstraining: 3 Tage
1.2.*; 12.–29.06.2017	CRISC Vertiefungskurs: 9 Tage
05.–07.10.2017	CRISC Repetitionsblock / Prüfungstraining: 3 Tage
1.2.*; 12.–29.06.2017	CGEIT Vertiefungskurs: 9 Tage
28.–30.09.2017	Repetitionsblock / Prüfungstraining CGEIT: 3 Tage
www.itacs.ch / * Strukturiertes Selbststudium; Selbststudium ab 01.02.2017	
14.–17.03.2017	CISA 4-day exam preparation course (Module 2) (E/F)
02.–05.05.2017	CISA 4-day exam preparation course (Module 2) (E/F)
22.–24.03.2017	CISM 3-day exam preparation course (Module 2) (E/F)
10.–12.05.2017	CISM 3-day exam preparation course (Module 2) (E/F)
29.–31.03.2017	CGEIT 3-day exam preparation course (Module 2) (E/F)
17.–19.05.2017	CGEIT 3-day exam preparation course (Module 2) (E/F)
29.–31.03.2017	CRISC 3-day exam preparation course (Module 2) (E/F)
www.actagis.ch	
03.–05.04.2017 und 08.05.2017*	CGEIT, 3 Tage Prüfungsvorbereitung P-CGEIT4
20.–22.03.2017	COBIT5 Foundation, 3 Tage, P-COF3
17.–19.07.2017	COBIT5 Foundation, 3 Tage, P-COF4
03.–05.04.2017	COBIT5 Implementation, 3 Tage, P-COI3
18.–20.04.2017	COBIT5 Assessor, 3 Tage, P-COA3
22.–24.05.2017	Implementation of NIST Cybersecurity Framework with COBIT5, 3 days, P-CON3
10.–12.04.2017	Cybersecurity Fundamentals on the basis of NIST, 3 days, P-CSFU4
13.–15.03.2017	RESILIA - Cyber Resilience Foundation, 3 days, P-CRFO3
www.glenfis.ch / * Vorbereitung Juni-Prüfung 2017	

ISACA MEMBER ADVANTAGE

JUST ASK about the value of ISACA membership, and you'll learn about the ever-growing **Access**, **Savings** and **Knowledge** ISACA members receive. As an ISACA member, you'll be a key part of a global professional organization dedicated to advancing your career, helping your organization innovate, and advocating for your profession.

ACCESS

- **9 INDUSTRY-LEADING GLOBAL CONFERENCES** with access to thought leaders and networking opportunities
- **500+ JOBS** in the ISACA Career Centre
- Members-only **ONLINE JOB FAIRS**
- **1,200 VOLUNTEERS** and more than 50 types of volunteer opportunities in 2016
- **140,000 ISACA PROFESSIONALS** to network with locally and globally
- **20,000+ GLOBAL PROFESSIONALS** in ISACA's online communities
- **ADVOCACY** for the profession and industry
- **210+ ISACA CHAPTERS** offering local networking and events
- **IT AUDIT LEADERS FORUM**
- **CISO FORUMS**
- **CONNECTING WOMEN LEADERS IN TECHNOLOGY** program, including networking and content opportunities
- **CAREER TOOLS** and resources

SAVINGS

- **30% DISCOUNT** on CISA, CISM, CRISC, CGEIT and CSX exam registrations
- **UP TO 30% DISCOUNT** on exam preparation materials
- **$0: COST OF ISACA WEBINARS**
- **DISCOUNTS ON ISACA PUBLICATIONS AND RESEARCH**
- **72 HOURS OF FREE CPE**
- Discounts to ISACA's **20 TRAINING WEEK** options
- **US $45 SAVINGS** on every audit/assurance program—ISACA members have free access
- **CONFERENCE AND WORKSHOP DISCOUNTS**
- **UP TO 25% DISCOUNT** on hotel and travel
- **UP TO 40% DISCOUNT** on shipping
- **DISCOUNTS ON ONLINE COURSES**

KNOWLEDGE

- **6 ISSUES** of the *ISACA Journal* per year and 52 weekly online exclusive *Journal* articles
- **40+ WEBINARS PER YEAR**
- **475 TITLES AND VIDEOS** available from ISACA's eLibrary
- **20+ NEW WHITE PAPERS** and publications coming this year
- **80 AUDIT/ASSURANCE PROGRAMS**
- **26 ISSUES** of the @ISACA e-newsletter
- **12 EDITIONS** of the COBIT Focus e-newsletter
- **10+ COBIT 5 PUBLICATIONS** and professional guides
- **2 CYBERSECURITY NEXUS (CSX) TOOLS**
- **35 IS AUDITING AND ASSURANCE** standards and guidelines
- **11 ONLINE, ON-DEMAND COURSES**
- **60+ CASE STUDIES**
- **6 GLOBAL SURVEY REPORTS**
- **24 WORKSHOPS**

ISACA

GET ANSWERS AND JOIN TODAY AT ***www.isaca.org/ASK***

IMPRESSUM ISACA NEWS

ISACA

Herausgeber, Redaktion:	**ISACA Switzerland Chapter**
Adresse:	**Sekretariat ISACA Switzerland Chapter, c/o BDO AG, Biberiststrasse 16, 4501 Solothurn**
Erscheinungsweise:	**4× 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**