Security, Risk- und Compliance Management

CONOECT INFORMUNITY

Dienstag, 15. September 2015
12.00 bis 18.00 Uhr

CMS Reich-Rohrwig Hainz Rechtsanwälte GmbH
1010 Wien, Gauermanngasse 2

- **PwC-Studie zum Thema Informationssicherheit**
- **Wirtschaftsspionage: Was tun als Betroffener?**
- **Aktuelle Bedrohungsszenarien**
- **Risikomanagement**
- **Prozessmodelle im Kontext von Verträgen – Nutzen & Standards**
- **Identity- und Access-Management**
- **Secure Coding**
- **End-to-End-Security**
- **Netzwerksecurity und Security mobiler Endgeräte**
- **Security aus technischer, organisatorischer, rechtlicher und Management-Sicht (Security Policy)**

Referenten: **Oliver Eckel** (Cognosec), **Claudia Gerlach** (CG Kontrakt), **Dr. Johannes Juranek** (CMS Reich-Rohrwig Hainz Rechtsanwälte) **Mag. Andreas Plamberger** (PwC Österreich), **DI Dr. Wolfgang Prentner** (ZT Prentner IT GmbH), **Christoph Schmittner, MSc.** (Austrian Institute of Technology GmbH)

Beschränkte Teilnehmerzahl!
Anmeldung erforderlich!
Bei freiem Eintritt für IT-Anwender!

Mit freundlicher Unterstützung von:

AIT Austrian Institute of Technology · SECURITY CERTIFICATION INFORMATION cis · CMS Law.Tax · cognosec A UC GROUP COMPANY · ZTP Ziviltechnikergesellschaft für Informationstechnologie · FUTURE NETWORK

AGENDA

12.00 **Registration & Networking**

12.15 **Compliance in der IT: Haftungsfragen bei Sicherheitslücken**
Dr. Johannes Juranek (CMS Reich-Rohrwig Hainz Rechtsanwälte)

12.45 **Wirtschaftsspionage: Was tun als Betroffener?**
DI Dr. Wolfgang Prentner (ZT Prentner IT GmbH)

13.15 **Fragen & Antworten**

13.35 **PwC-Studie zum Thema Informationssicherheit & Cybersecurity**
Andreas Plamberger (PwC Österreich)

14.00 **Sichere IT Infrastruktur**
Oliver Eckel (Cognosec)

14.35 **Pause**

15.15 **Best Practices**

16.15 **Prozessmodelle im Kontext von Verträgen – Nutzen & Standards**
Claudia Gerlach (CG Kontrakt)

16.35 **Pause**

16.45 **M2M Kommunikation**
Christoph Schmittner, MSc (Austrian Institute of Technology GmbH)

17.15 **Networking**

18.00 **Ende der Veranstaltung**

Compliance in der IT: Haftungsfragen bei Sicherheitslücken

Johannes Juranek
(CMS Reich-Rohrwig Hainz Rechtsanwälte)

Datendiebstahl und Schadenzufügung ist eine moderne Form der Kriminalität. Angriffe können also von außen und von Innen kommen und verursachen massive finanzielle Schäden in Unternehmen. Daher ist es wichtig, sich über die wichtigsten Quellen für den Datenverlust bewusst zu werden. Netzwerke und das Internet und Hacker sind dabei die größte Bedrohung, aber auch menschliches Versagen ist häufig ein Grund für Sicherheitslücken. Welche Verantwortung hat nun der Geschäftsführer und wofür haftet er? Rechtsanwalt Dr. Johannes Juranek informiert über die aktuelle Rechtslage und zeigt auf, welche Maßnahmen Geschäftsführer ergreifen müssen, um im Fall eines Angriffes nicht für den Schaden haften zu müssen.

Wirtschaftsspionage: Was tun als Betroffener?

Wolfgang Prentner
(ZT Prentner IT GmbH)

Die Wirtschaftsspionage und kriminellen Aktivitäten haben im Jahr 2014 um 13 % zugenommen. Wenn man sich vor Augen hält, dass 87 % der Mitarbeiter keine emotionale Bindung an das Unternehmen haben, laut einer Umfrage des Gallup Instituts und laut einer anderen Statistik 50 % der Mitarbeiter sagen »die Daten gehören auch mir da ich daran mitgearbeitet habe«, so ist klar sichtlich, dass die Hemmschwelle via Wirtschaftsdelikte speziell auch im Bereich Wirtschaftsspionage in der IT gegeben ist.

Weiter wird bemerkt, dass das Management nahezu naiv ist was das Vertrauen in die IT und deren Administratoren angeht.

Zudem wurde durch den Ankauf von Finanzdaten durch Regierungen das Berufsfeld des professionellen Datendiebes gefördert.

Was man als Betroffener tun kann, erklärt IT-Ziviltechniker Wolfgang Prentner seines Zeichens Sicherheitsspezialist, studiert und promoviert im Sicherheitsbereich an der TU Wien.

Welcher Anteil am Gesamtbudget für IT-Ausgaben steht für IT-Sicherheit in Ihrer Institution zur Verfügung?

	absolut	in Prozent
weniger als 5 %	66	25,7 %
5 % bis 10 %	40	15,6 %
10 % bis 15 %	19	7,4 %
15 % bis 20 %	7	2,7 %
20 % bis 25 %	2	0,8 %
mehr als 25 %	7	2,7 %
keine Angabe	119	45,1 %

Beantwortet durch 257 Teilnehmer
Keine Antwort automatisch als »keine Angabe« gewertet
Quelle: Ergebnisse der Cyber-Sicherheits-Umfrage 2014, SecuMedia Verlags GmbH

PwC-Studie zum Thema Informationssicherheit

- Finanzielle Schäden durch Hackerangriffe deutlich gestiegen
- Budgets werden dennoch gekürzt
- Geheimdienste werden als Bedrohung empfunden

Andreas Plamberger (PwC Österreich)

Die Zahl der Angriffe auf die IT-Sicherheit von Unternehmen ist im vergangenen Jahr sprunghaft angestiegen. Dies ist das Ergebnis des Global State of Information Security Survey, welche die Wirtschaftsprüfungs- und Beratungsgesellschaft PwC jährlich zusammen mit den Fachmagazinen CIO und CSO durchführt. Dazu wurden im Frühjahr 2014 rund 9800 IT-Verantwortliche in über 154 Ländern befragt, darunter 30 österreichische Unternehmen. Es ist die größte Umfrage ihrer Art.

Das zentrale Ergebnis: Vor 18 Monaten ist die Gesamtzahl der Angriffe auf die IT-Sicherheit von Unternehmen im Vergleich zum Vorjahr um 48 Prozent auf 42,8 Millionen angestiegen. Dies entspricht 117330 Angriffen pro Tag. Seit 2009 ist die Zahl damit sogar um 66 Prozent angestiegen. Trotz der zunehmenden Anzahl an Sicherheitsvorfällen sinken die Ausgaben für IT-Sicherheit. Zwar gaben 48 Prozent der Studienteilnehmer an, dass sie IT-Sicherheitsrisiken stärker wahrnehmen (2011: 39 %). Dennoch sanken die Ausgaben für IT-Sicherheit gegenüber dem Vorjahr um 4 Prozent.

Milliardenschaden durch Verlust von Geschäftsgeheimnis. Der Studie zufolge entstand vor 18 Monaten weltweit ein Verlust von geschätzten 2,7 Millionen Dollar pro Angriff, das ist zum Vorjahr ein Anstieg von 34 Prozent. Dabei sind große Verluste zunehmend an der Tagesordnung: Die Zahl der Fälle mit einem Verlust von mehr als 20 Millionen Dollar stieg 2013 sogar um 92 Prozent. In der Summe betrug der Schaden, der durch den Verlust von Geschäftsgeheimnissen entstand, zwischen 749 Milliarden und 2,2 Billionen Dollar. Da viele Angriffe nicht gemeldet werden, liegt die Dunkelziffer der globalen Kosten durch Cyberkriminalität jedoch wohl um einiges höher.

Falls Ihre Institution in den Jahren 2012/13/14 durch Cyberangriffe Schäden davongetragen hat: Welcher Art waren diese?

	Anzahl der Nennungen
Reputationsschaden	42
Produktionsausfall	41
Informationsabfluss z. B. von Entwicklungs-/Forschungs-/Finanzdaten (Wirtschaftsspionage)	14
Informationsabfluss z. B. Kreditkarten-Daten von Kunden o. Ä. (Cybercrime)	4
Diebstahl digitaler Identitäten (z. B. Login-Daten durch Phishing)	34
Erhebliche Kosten für die Aufklärung und Wiederherstellung der Systeme	56
Erhebliche Kosten durch Ansprüche Dritter (z. B. geschädigter Kunden)	4
Bußgelder oder andere Strafzahlungen	0

Beantwortet durch 126 Teilnehmer, Mehrfachnennungen möglich
Keine Antwort: 131 Teilnehmer

Quelle: Ergebnisse der Cyber-Sicherheits-Umfrage 2014, SecuMedia Verlags GmbH

Sichere IT Infrastruktur

Oliver Eckel (Cognosec)

Prozessmodelle im Kontext von Verträgen – Nutzen & Standards

Claudia Gerlach (CG Kontrakt)

Chancen und Risiken sind seit jeher fester Bestandteil sämtlicher Geschäftsprozesse und unternehmerischen Entscheidungen. Die bewusste Auseinandersetzung mit Chancen und Risiken ist untrennbar mit unternehmerischem Handeln verbunden.

Eine strukturierte Vorgehensweise in der Behandlung von Chancen und Risiken ist das Kernstück einer umfassenden Kontrolle der Geschäftstätigkeit.

Aber auch gesetzliche Bestimmungen zu Bilanzierung, Corporate Governance und Compliance erfordern mittlerweile ein systematischeres Vorgehen in der Risikoerkennung. Die Einführung standardisierter Prozessmodelle in Unternehmensabläufe gewährleistet die konsequente Behandlung von Chancen und Risiken unter Berücksichtigung der gesetzlichen wie auch unternehmensinterner Vorgaben. Verträgen kommt dabei eine zentrale Bedeutung zu, denn Risiken, die erst nach Vertragsabschluss erkannt werden, sind nur noch schwer zu kontrollieren.

Der einheitliche, nach ISO 31000 standardisierte Risikomanagement-Prozess, als Teil eines systematischen Vertragsmanagements, schafft die nötige Transparenz

- über die Wirtschaftlichkeit vertraglicher Vereinbarungen
- über die wichtigsten vertraglichen Inhalte und Klauseln
- in der Wahl der richtigen Vorgehensweise zur Abwehr und Minimierung von Risiken

Worldwide Security Spending Forecast (Millions of Dollars)

			2012	2013	2014	2015
Enterprise	Identity Access Management	User Provisioning (UP)	1,397	1,549	1,720	1,898
		Web Access Management (WAM)	634	678	719	766
		Other Identity Access Management	627	722	839	954
	Infrastructure Protection	Endpoint Protection Platform (Enterprise)	3,179	3,191	3,280	3,364
		Other Security Software	2,762	3,021	3,273	3,524
		Secure E-mail Gateway	1,678	1,725	1,774	1,820
		Secure Web Gateway	2,033	2,158	2,327	2,505
		Security Information and Event Management (SIEM)	1,361	1,578	1,808	2,035
		Security Testing (DAST and SAST)	416	484	561	649
		Data Loss Prevention	573	731	941	1,203
	Network Security Equipment	IPS Equipment	1,470	1,524	1,549	1,510
		SSL VPN Equipment	576	481	386	297
		VPN/Firewall Equipment	6,064	6,644	7,322	8,076
	Security Services	Consulting	10,795	11,437	12,152	12,934
		Hardware Support	1,240	1,319	1,404	1,497
		Implementation	11,981	12,737	13,585	14,526
		IT Outsourcing	10,443	12,002	13,838	16,008
Consumer	Consumer Security Software	Consumer Security Software	4,892	5,043	5,297	5,557
Grand Total			**62,120**	**67,022**	**72,774**	**79,123**

Source: Gartner (October 2013)

M2M Kommunikation

Christoph Schmittner, MSc (Austrian Institute of Technology GmbH)

Der Vortrag behandelt das Problem im Umgang und Einsatz mit Legacy-Protokollen und die zu beachtenden Auswirkungen auf die Produktionssystem unter Einbeziehung der von ihm entwickelten Safety- und Security-Co-Engineering Methoden. Es werden dabei über Erfahrungen aus einem EU-Projekt berichtet. Kritischen Geschäftsinformationen muss man jetzt auf Maschinenlevel schützen, während Safety auch im Backend eine Rolle spielt.

ReferentInnen

Oliver Eckel *ist Geschäftsführer von Cognosec, einen führenden Firma im Bereich Informationssicherheit, SCADA (Schutz kritischer Infrastruktur) und sicherem Zahlungsverkehr im Internet. Er ist darüber hinaus Mitglied im internationalen Security Risk Management Beirat von Agiliance. Zuvor war er Head of Security bei der bwin AG und Chief Security Officer der Wave Solutions/Bank Austria.*

Claudia Gerlach *unterstützt seit über 25 Jahren regionale und internationale Vertriebsteams darin, neue Prozesse und innovative Ansätze wirtschaftlich in Arbeitsabläufe zu integrieren und umzusetzen u. a. betreffend Vertragsmanagement. Sie ist Leiterin des Vertragsmanagements Service für die Regionen APAC und Europa. Als Global Contract Manager ist sie verantwortlich für die Bereiche Performance Management und Kompetenzentwicklung. Schulungen zu Risiko-, Vertragsänderungs- und Forderungsmanagement werden von ihr konzipiert und durchgeführt. Weiters hält Claudia Gerlach Vorträge zu Themen im Vertragsmanagement Coaching. Sie führt Prozesse im Vertragscontrolling ein und setzt Grundlagen um und wendet sie an. Referenzen: Siemens AG, Berlin/München, Nokia Siemens Networks GmbH & Co. KG (jetzt: Nokia Solutions and Networks), München*

ZT Dr. Wolfgang Prentner *seit 1998 IT-Ziviltechniker im Fachbereich Informationstechnologie. Geschäftsführer der ZT-PRENTNER-IT GmbH, Gerichtssachverständiger und promovierter Informatiker an der TU Wien. Als unabhängige Prüf- und Überwachungsstelle für Informatik, CyberSecurity, Datenschutz und dem INTERNET-SICHERHEITSGURT unterstützt er außerdem in ehrenamtlicher Funktion die Länderkammer, die Bundeskammer und das Bundeskomitee ›Die Freien Berufe Österreichs‹ sowie das Bundeskanzleramt seit 2004.*

Christoph Schmittner *ist wissenschaftlicher Mitarbeiter beim Austrian Institute of Technology im Bereich Safety and Security. Seine Schwerpunkte sind Safety Engineering, Road Safety, Embedded Systems, Autonomous Robotics, Automotive Systems Engineering, Computer Security and Reliability etc.*

Johannes Juranek *ist Partner bei CMS Reich-Rohrwig Hainz. Er ist einer der führenden Experten in den Bereichen Technologie-, Datenschutz- und Wirtschaftsrecht. Johannes Juranek bringt weitreichende Erfahrung beim Führen von komplexen Rechtsfällen mit sich, insbesondere für Klienten aus den Branchen Technologie und Konsumgüter. Zu seinen Klienten zählen österreichische und internationale Unternehmen, die er auch vor Gerichten und Schiedsgerichten vertritt.*

CONNECT
BUSINESS ACADEMY

Vertragsmanagement – die kommerzielle Seite Ihrer Verträge

Referentin: Claudia Gerlach
(CG Kontrakt)

Termine: 16. September 2015, 15. Oktober 2015, Wien

Es werden folgende Fragestellungen behandelt:

- Was genau ist Vertragsmanagement?
- Wie setze ich Vertragsmanagement-Prozesse in meinem Unternehmen ein?
- Wie profitiere ich von Vertragsmanagement?

Das Seminar bietet eine Einführung in die Teilbereiche des Vertragsmanagements:

- Risiko-, Vertragsänderungs- und Forderungsmanagement
- Je Teilbereich werden der Aufgabenumfang und die relevanten Prozessschritte vorgestellt sowie Kernelemente der Prozesses herausgearbeitet.

Ergänzt wird der Überblick um die erforderlichen administrativen Prozesse:

- Vertragscontrolling (Leistungsindikatoren, Genehmigungen, Verantwortlichkeiten)
- Vertragsverwaltung (Berichterstattung/Reporting, Dokumentation)

Teilnahmegebühr: € 550,– (Alle Preise + 20 % MwSt.)

CONNECT
BUSINESS ACADEMY

Information-Security-Manager

Technologieexperte/expertin mit Führungsqualitäten

Seminar mit Zertifizierungsprüfung nach ISO 27001 / ISO 27002

Referenten: Herfried Geyer (CIS-Auditor und -Trainer), **Günther Schreiber** (CIS, Quality Austria), **Markus Frank** (Rechtsanwaltskanzlei Frank-Law), **Orlin Radinsky** (Rechtsanwaltskanzlei BKP)

Termine: 14.–17. Sept., 9.–12. Nov. 2015, Wien

Information-Security-Manager nehmen jene zentrale Position im Unternehmen ein, in der Führungs- und Technologiekompetenz gleichermaßen gefragt sind. Sie betreuen den Aufbau, die Implementierung sowie die ständige Verbesserung des Informationssicherheits-Managementsystems (ISMS) und fungieren als Schnittstelle zwischen der obersten Führungsetage und den operativen Unternehmensbereichen. Dieser CIS-Lehrgang führt Sie sicher ans Ziel – er vermittelt kompakt und anwendungsorientiert die Kernelemente des internationalen Standards für Informationssicherheit ISO/IEC 27001 sowie seine korrekte Interpretation und Umsetzung. Der Lehrgang besteht aus 3 Modulen:

- Die Normen ISO/IEC 27001:2013 und ISO/IEC 27002:2013
- Psychologische Grundlagen für IS-Manager
- Rechtsgrundlagen

Teilnahmegebühr: € 3.200,–, Prüfungsgebühr; € 650,–

CONNECT
BUSINESS ACADEMY

Certified Information Systems Security Professional (CISSP)

In Zusammenarbeit mit SBA Research gGmbH

Referent: Andreas Tomek u. a. (SBA Research)

Termine: 23.–27. November 2015, 13.–17. Juni 2016, Wien

Viele Unternehmen beginnen die CISSP (Certified Information Systems Security Professional) Zertifizierung als Grundlage für Ihre Arbeit im technischen, mittleren, oder Senior Management. Mit der Erlangung des CISSP – dem weltweit angesehenen Zertifikat im Sicherheitsbereich – beweisen Sie tiefgehende Kenntnisse in Sicherheitskonzepten, Umsetzung und Methodologie. (ISC)², einer der international führenden Anbieter für Sicherheitszertifikate, setzt mit dieser hochwertigen und strengen Prüfung die Latte für Exzellenz im Sicherheitsbereich.

Teilnahmegebühr: € 3.210,–, Prüfungsgebühr; € 645,– (Alle Preise + 20 % MwSt.)

CONNECT
BUSINESS ACADEMY

Windows Hacking – Wie Hacker und Betriebsspione arbeiten

In Zusammenarbeit mit SBA Research gGmbH

Referenten: Stefan Jacoubi, Mag. Andreas Tomek, Gernot Goluch (Security Research)

Termine: 3.–4. Dezember 2015, 31. März – 1. April 2016, Wien

Der Kurs behandelt die typischen Sicherheitslücken und Angriffspunkte sowie geeignete Schutzmaßnahmen in Windows-Netzwerken. Dabei wird sowohl auf die aktuelle Betriebssystemgeneration (Windows 7 und Server 2008R2, 2012), als auch ältere (XP, Vista, Server 2000 & 2003) noch in Betrieb befindliche Versionen eingegangen.

- Sicherheitslücken und deren Absicherung bei Windows Servern
- Sicherheitslücken und deren Absicherung bei Windows Clients
- Sicherheitslücken und deren Absicherung im Netzwerk und auf mobilen Endgeräten

Teilnahmegebühr: € 1.450,–, Frühbucher: € 1.380,– (Alle Preise + 20 % MwSt.)

An
CON•ECT Eventmanagement
1070 Wien, Kaiserstraße 14/2

Tel.: +43 / 1 / 522 36 36-36
Fax: +43 / 1 / 522 36 36-10
E-Mail: registration@conect.at
http://www.conect.at

ANMELDUNG: Nach Erhalt Ihrer Anmeldung senden wir Ihnen eine Anmeldebestätigung. Diese Anmeldebestätigung ist für eine Teilnahme am Event erforderlich.

STORNIERUNG: Sollten Sie sich für die Veranstaltung anmelden und nicht teilnehmen können, bitten wir um schriftliche Stornierung bis 2 Werktage vor Veranstaltungsbeginn. Danach bzw. bei Nichterscheinen stellen wir eine Bearbeitungsgebühr in Höhe von € 50,– in Rechnung. Selbstverständlich ist die Nennung eines Ersatzteilnehmers möglich.

ADRESSÄNDERUNGEN: Wenn Sie das Unternehmen wechseln oder wenn wir Personen anschreiben, die nicht mehr in Ihrem Unternehmen tätig sind, teilen Sie uns diese Änderungen bitte mit. Nur so können wir Sie gezielt über unser Veranstaltungsprogramm informieren.

Anmeldung

CON•ECT EVENTMANAGEMENT

☐ Ich melde mich zu »Security, Risk- und Compliance Management« am 17. 9. 2015 an:
- ☐ Als IT-Anwender aus Wirtschaft und öffentlicher Verwaltung kostenfrei
- ☐ Als IT-Anbieter/-Berater zu € 390,– (zuzügl. 20 % MwSt.)

☐ Ich möchte Zugriff auf die Veranstaltungspapers zu € 99,– (+ 20 % MwSt.)

☐ Ich möchte in Zukunft weiter Veranstaltungsprogramme per E-Mail oder Post übermittelt bekommen.

Firma:

Titel: | Vorname:

Nachname:

Funktion:

Straße:

PLZ: | Ort:

Telefon: | Fax:

E-Mail:

Datum: | Unterschrift/Firmenstempel:

● Ich erkläre mich mit der elektronischen Verwaltung meiner ausgefüllten Daten und der Nennung meines Namens im Teilnehmerverzeichnis einverstanden.

● Ich bin mit der Zusendung von Veranstaltungsinformationen per E-Mail einverstanden.

(Nichtzutreffendes bitte streichen)

15070 Layout: Gerhard Krill