Security-Trends

PwC Information Security® Survey 2017 – Business Continuity und Security Policy und DSGVO

CONNECT INFORMUNITY

Dienstag 12.September 2017
9.00–14.00 Uhr

PwC Österreich
1030 Wien, Erdbergstraße 200

- **Aktuelle Bedrohungsszenerien aus der Praxis von PwC – Vorstellung der Studie: Global State of Information Security® Survey 2017 von PwC**
- **Business Continuity Management in einem internationalen Reisekonzern – Fallbeispiel: Wenn das Ferienparadies zum Katastrophengebiet wird**
- **Security aus rechtlicher, organisatorischer und Management-Sicht – Die neue DSGVO 2018 in Kombination mit dem ISMS und einem eigenen Datenschutz-Management-System – dem DSMS**
- **Mit Podiumsdiskussion zur PwC-Studie und Security-Trends**
  Mit Dr. Wolfgang Prentner, Dr. Christian Kurz (PwC Österreich), Dr. Markus Frank (FrankLaw), Wolfgang Mahr (continuuuity), Dr. Peter Kieseberg (SBA Research Institute)

Referenten:
Dr. Markus Frank (FrankLaw)
Dr. Christian Kurz (PwC Österreich)
Wolfgang Mahr (continuuuity)
Dr. Wolfgang Prentner (ZT Prentner)
N.N. (CIS)

Moderation:
Dr. Peter Kieseberg (Secure Business Austria) angefragt

Bei freiem Eintritt.
Anmeldung erforderlich!

Mit freundlicher Unterstützung von:

SECURITY CIS CERTIFICATION & INFORMATION

fh st.pölten

pwc

SBA Research

ZTP IT-Ziviltechnikergesellschaft

FUTURE NETWORK

9.00 **Eröffnung der Veranstaltung**

9.10 **Aktuelle Bedrohungsszenerien aus der Praxis von PwC – Vorstellung der Studie: Global State of Information Security@ Survey 2017 von PwC**
Dr. Christian Kurz (PwC Österreich)

10.00 **Business Continuity Management in einem internationalen Reisekonzern – Fallbeispiel: Wenn das Ferienparadies zum Katastrophengebiet wird**
Wolfgang Mahr (continuuuity, Schweiz)

10.35 **Pause**

10.50 **Security aus rechtlicher, organisatorischer und Management-Sicht – Die neue DSGVO 2018 in Kombination mit dem ISMS und einem eigenen Datenschutz-Management-System – dem DSMS**
Dr. Markus Frank (FrankLaw)

11.30 **Podiumsdiskussion zur PWC-Studie und Security-Trends**
Mit Dr. Wolfgang Prentner, Dr. Christian Kurz (PwC Österreich), Dr. Markus Frank (FrankLaw), Wolfgang Mahr (continuuuity), Dr. Peter Kieseberg (SBA Research Institute)

13.00 **Business-Continuity-Zertifizierung nach ISO 22301: der Weg und das Ziel**
N.N. (CIS)

13.30 **Networking**

14.00 **Ende der Veranstaltung**

Aktuelle Trends des Security-Markts bei Gartner

Der Markt für Security-Software verändert sich dramatisch. Das IT-Research- und Beratungsunternehmen Gartner hat die vier treibenden Kräfte hinter der Umwälzung identifiziert: 1. die zunehmende Nutzung von Advanced Analytics, 2. deutlich größere IT-Ökosysteme, 3. die wachsende Akzeptanz von Software as a Service (SaaS) und 4. die Aussicht auf strengere Regulierung und drohende Strafen. Diese Faktoren bringen Unternehmen dazu, neu über ihren Bedarf an Sicherheits- und Risikomanagement-Software nachzudenken. »Der Security-Markt geht durch eine Phase der Disruption. Grund ist der schnelle Übergang zu Cloud-basierten digitalen Geschäftsmodellen und Technologien. Dadurch ändert sich der Beitrag der Risiko- und Sicherheits-Funktionen zur Wertschöpfung innerhalb einer Organisation«, sagte Deborah Kish, Principal Research Analyst bei Gartner. »Zugleich schaffen die Bedrohungsszenarien und die steigende Zahl der schwerwiegenden Security-Vorfälle Nachfrage für effektivere Sicherheits-Technologien und Innovationen.«

Zu den wichtigsten Sicherheitstechnologien zählen laut Gartner unter anderem Plattformen zur Cloud Workload Protection, Remote Browser und die Analyse des Netzwerktraffics. Die Analysten werden weitere IT-Security-Trends auf den folgenden weltweiten Gartner Security & Risk Management Summits 2017 vorstellen.

(Quelle: Gartner)

Aktuelle Bedrohungsszenarien aus der Praxis von PwC

Christian Kurz (PwC Österreich)

Cyber-Angriffe und Social-Engineering-Attacken finden in Unternehmen aller Branchen und Größenordnungen profitable Opfer. Wie die jährlich von PwC durchgeführte Umfrage GSISS zeigt, sind sich die meisten befragten Unternehmen der umfangreichen Gefahren bewusst. Kaum eine technisch-verantwortliche Stelle hat jedoch die Ressourcen und das Know-how, bezüglich der Gefahrenabwehr immer auf dem neuesten Stand zu sein, geschweige denn eine lückenlose

Global State of Information Security® Survey 2017 von PwC:

Österreichische Unternehmen hinken bei IT-Sicherheit hinterher

- Knapp zwei Drittel der Unternehmen weltweit verzeichnen Kostenanstieg für IT-Sicherheit, in Österreich sind es hingegen nur 34 %
- Phishing-Attacken sind die am häufigsten verzeichnete Sicherheitsstörung 2016
- 20 % der heimischen Unternehmen tätigen konkrete Investitionen in Sicherheitsstrategien für das Internet of Things (global 46 %)
- Nur ein Drittel führen aktive Mitarbeiterschulungen zur IT-Sicherheit durch (global 56 %)
- 33 % der heimischen Unternehmen setzen auf Cloud-Lösungen für ihre IT-Dienste (63 % global)

Aufarbeitung von Vorkommnissen zu gewährleisten. Dieser Vortrag greift praktische Erfahrungen aus der forensischen Sicht von PwC auf und leitet daraus die aktuellen Herausforderungen und Bedrohungsszenarien ab. Der Vortragende gibt einen Einblick in tatsächlich untersuchte Fälle, wie z. B. Fake President Fraud oder Immigration Fraud und die Arbeitsweise der Forensiker.

Business Continuity Management in einem internationalen Reisekonzern: wenn das Ferienparadies zum Katastrophengebiet wird

Wolfgang Mahr (continuuity)

Business Continuity Management (BCM) schützt Unternehmen vor den Auswirkungen von Betriebsunterbrechungen. Die Gründe und Auslöser können vielfältig sein und das Unternehmen ohne eigenes Verschulden treffen. Schutzwirkung wird durch methodisches Vorgehen wie z. B. die Implementation international anerkannter Normen erzielt – und dadurch die Aufrechterhaltung einer gewissen Geschäftstätigkeit erzielt.

In der Reisebranche gelten dagegen weit höhere Anforderungen: das Unternehmen hat zusätzlich die Verantwortung, sich um das Wohlergehen seiner Kunden – speziell wenn diese schon die Reise angetreten haben – zu kümmern. Dies stellt zusätzliche Anforderungen an ein BCM-Vorgehen dar: es sind im Grunde genommen zwei Projekte gleichzeitig durchzuführen, was zu weit höheren Anforderungen an alle Beteiligten führt.

Security aus organisatorischer, rechtlicher und Management-Sicht (Security Policy) (ohne Technik), insbesondere in Hinblick auf die Datenschutzgrundverordnung (DSGVO)

Markus Frank (Frank-Law)

IT-Sicherheit ist ein sehr großer Teilbereich der DSGVO-Pflichten. Dafür muss gem Art 32 DSGVO ab 25. 5. 2018 (Inkrafttreten der DSGVO) ein »Verfahren« (= Informations-Sicherheits-Management-System, ISMS) eingerichtet sein. Je nach »Gefährlichkeit« der Datenverarbeitung verlangt die DSGVO daneben oder kombiniert mit dem ISMS auch ein eigenes Daten-Schutz-Management-System, DSMS.

Wie das Sicherheits-Management-System gemäß Art. 32 DSGVO auszusehen hat, was sich gegenüber der bisherigen Verpflichtung nach DSG 2000 ändert und über die praktische Erfahrung mit den Schwierigkeiten und Unsicherheiten bei der Implementierung des neuen ISMS (allein oder in Kombination mit einem DSMS) kann ich berichten. Daneben freilich auch darüber, warum die Geschäftsleitungen der Unternehmen die Herstellung ausreichender Daten-Sicherheit in ihren Organisationen auf Grund der neuen Rechtslage ganz massiv unterstützen müssen (persönliche Organisations-Verantwortung, hohe Bußgelder für die Organisation bis zu 4 % des Jahresumsatzes / bis zu 20 Mio. €).

Standards wie z. B. ISO 27001, Entwurf ISO 29151, VdS 3473, ISIS 12 etc. sind – mit und ohne Zertifizierung – eine wichtige Orientierungshilfe bei der Einführung von ISMS und DSMS in der Praxis. Solche zertifizierte Standards können wesentliche Beweis-Erleichterungen für die Nachweispflichten der Organisationen gemäß DSGVO bringen.

Referenten

Dr. Markus Frank, *LLM, ist als Rechtsanwalt spezialisiert auf interdisziplinäre Untersuchungen von Schadenursachen bei Wirtschaftsdelikten und Vertragsverletzungen. Vor diesem Hintergrund ist er als Rechtsexperte im Beirat der Zertifizierungsorganisation CIS vertreten und fungiert im Rahmen der CIS-Zertifikatslehrgänge als Trainer für ISO 27001.*

Christian Kurz *arbeitet seit 2012 für PwC und war davor 7 Jahre in der IT-Beratung und 5 Jahre in der Forschung tätig. Parallel dazu unterrichtet er an Fachhochschule St. Pölten im Masterstudiengang Information Security. Seine fachlichen Schwerpunkte liegen in den Bereichen Computer Forensik, Electronic Discovery und Untersuchungen im Bereich Cyberforensics. Er ist Certified Cyber Forensic Professional –European Union von (ISC)2.*

Dr. Peter Kieseberg *erhielt seinen Abschuss an der TU Wien. Im Anschluss arbeitete er als Associate Consultant bei Benmark, sowie als Consultant bei NEWCON im Bereich Telekommunikation, speziell in den Bereich Interconnection Billing und DWH/BI. Set Mai 2010 ist er Research Manager und Forscher bei SBA Research, seine Spezialisierungen liegen dabei in den Bereich der digitalen*

Forensik, sowie des Fingerprintings strukturierter Daten, speziell auch im medizinischen Bereich.

Dr. Wolfgang Mahr *hat über 20 Jahre Erfahrung in der Beratung und Projektmanagement im ICT-Umfeld und hat sich während der letzten 15 Jahre auf den Bereich der Business Continuity Management spezialisiert.*

Er hat umfassende Erfahrung in IT-Governance, IT-Sicherheit, Business Management, Marketing, Account und Product Management, in der beruflichen Bildung als Autor von Lerninhalten, und als internationale Sprecher. Er hält einen Doktortitel der Eidgenössischen Technischen Hochschule in Lausanne (EPFL), den Grad eines Diplomingenieur in Elektrotechnik der TU Wien, hat einen Bachelor of Business Administration der GSBA Zürich, ist ein Certified Information Systems Auditor (CISA) und ist ein langjähriges Mitglied des Business Continuity Institute (FBCI). Er ist ein zertifizierter Trainer von BCI und PECB.

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.*

CON•ECT BUSINESS ACADEMY

Einführung Business Continuity Management (BCM)

Referent: Dr. Wolfgang Mahr
(governance & continuuuity)

Termine: 18. Oktober 2017, 22. Februar, 12. September 2018, alle Wien

Der ISO 22301 Einführungskurs ermöglicht den TeilnehmerInnen, die Grundkonzepte eines BCMS (Business Continuity Management Systems) zur verstehen. Dabei handelt es sich um ein Management-System gemäß ISO, welches jeweils die optimale Einführung einer Thematik (z. B. Qualitätsmanagement, Informationssicherheit, Umweltmanagement) beschreibt.

Business Continuity umfasst dabei die Maßnahmen, eine Organisation bzw. wesentliche Teile davon pro- und retroaktiv vor den Auswirkungen von Betriebsunterbrechungen zu schützen. Der Kurs beschreibt in diesem Zusammenhang die Wichtigkeit der vorbereitenden Maßnahmen für Unternehmen, Verwaltungseinheiten bzw. der Gesellschaft im Allgemeinen.

Teilnahmegebühr: € 850,–; Frühbucher: € 750,–
(Alle Preise + 20 % MwSt.)

CON•ECT EVENTMANAGEMENT

An
CON•ECT Eventmanagement
Kaiserstraße 14/2, 1070 Wien
Tel.: (01) 522 36 36-36 **Fax: (01) 522 36 36-10**
registration@conect.at **http://www.conect.at**

Anmeldung

- ☐ Ich melde mich zu »Security-Trends« am 12. 9. 17 kostenfrei an.
- ☐ 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: