

6. Information-Security-Symposium, WIEN 2010

6. Information-Security-Symposium, WIEN 2010: 14.04.2010, 13.30-19.00 / Open End / Kursalon Am Parkring, Johannesgasse 33, 1010 Wien

14.20 Effizienz mit System: Implementierung von Informationssicherheit nach ISO 27001

Die Carrier Netze der „LINZ AG TELEKOM“ betreiben seit Juli 2009 ein nach ISO 27001 zertifiziertes InformationsSicherheitsManagementsystem (ISMS). Die Beweggründe dazu waren einerseits der Wunsch der Kunden, als auch die Entscheidung der strategische Ausrichtung. Die Marke „LINZ AG Telekom“ ist als professioneller TK Dienstleister positioniert. Die Randbedingungen forderten eine straffe und effektive ISMS Organisation. Der Vortrag gibt Einblicke in Organisation und Aufbau des ISMS sowie in die Implementierung des aus unserer Sicht gesehenen „Hauptprozesses“: Das risikogesteuerte Maßnahmenmanagement. Durch die strukturierte und dokumentierte Abarbeitung gibt es Vorteile für die Mitarbeiter, die Assetverantwortlichen als auch für die Geschäftsführung. Die Managementsysteme nach ISO 9001 (QM), OHSAS 18001 (Arbeitsschutz) und ISO 27001 (ISMS) sind harmonisch im IMS (Integriertes Management System) zusammengefasst.



Berthold Haberler, Information Security Officer, Linz AG Telekom

14.40 ISO-Trends: Neue Subnormen der 27x-Reihe als Hilfsinstrumentarium

Von 0 bis 37 in 15 Minuten. Das ist nicht das Resultat eines Autotests, sondern der Rahmen für diesen ISO-27k-„Newsflash“: Ein Bukett von branchen- und themenspezifischen Subnormen hat sich um den Zertifizierungsstandard ISO 27001 herausgebildet – einige sind bereits veröffentlicht, weitere befinden sich noch in Entwicklung. Die International Organization for Standardization bietet damit ein umfassendes Hilfsinstrumentarium für die wirksame Umsetzung und Weiterentwicklung von Informationssicherheitsmanagementsystemen (ISMS). Die unterschiedlichsten Schwerpunkte der ISO-27k-Reihe begegnen auch neuen, hochaktuellen Anforderungen zur Stabilisierung des „Spannungsbogens Informationssicherheit“.



Dipl.-Ing. Herfried Geyer, CIS-Auditor und Trainer für ISO 27001

15.05 Lebendige Sicherheit: Entwicklung von „Secure Software“ im dynamischen Umfeld

Das Security Engineering stellt Methoden und Werkzeuge bereit, um das Qualitätsziel Informationssicherheit im Software-Lebenszyklus systematisch und durchgängig umzusetzen. Dies reicht von der Erhebung von Sicherheitsanforderungen und -risiken über den Entwurf von Sicherheitsarchitekturen bis zur statischen Codeanalyse und zum Security-Test. Durch die zunehmende Offenheit und Vernetzung von IT-Systemen auf der einen Seite und deren ständige Weiterentwicklung auf der anderen Seite ist das Security Engineering heute mit großen Herausforderungen konfrontiert. In diesem Spannungsfeld stellt der Vortrag Prinzipien „Lebendiger Sicherheit“ vor, die das kontinuierliche Security Engineering von der Compliance über den Entwurf bis zum Betrieb von IT-Diensten zum Ziel haben und stellt einen Bezug zu den ISO-2700x-Standards her.



Prof. Dr. Ruth Breu, Institut für Informatik, Universität Innsbruck

15.35 Solutions Section / 16.00 Pause: Info-Cubes & Snacks

6. Information-Security-Symposium, WIEN 2010

6. Information-Security-Symposium, WIEN 2010: 14.04.2010, 13.30-19.00 / Open End / Kursalon Am Parkring, Johannesgasse 33, 1010 Wien

16.45 Zivil- und strafrechtliche Verantwortlichkeit des CIO – eine neue Judikatur?

Der Vortrag wird drei große Trends behandeln: Zum Einen bejaht eine aktuelle Entscheidung des deutschen Bundesgerichtshofs eine strafrechtliche Verantwortlichkeit des Compliance Officers für Rechtsverstöße im Unternehmen, was auch in Österreich relevant werden könnte. Zweitens zeichnet sich unter dem Stichwort „Cloud Computing“ ein eindeutiger Trend zum Outsourcing von IT-Dienstleistungen ab, was naturgemäß die Kontrolle der Datensicherheit erschwert. Auch komplexe Fragen des Datenschutzes spielen hier eine Rolle, insbesondere wenn die Daten außerhalb Österreichs übermittelt werden sollen. Die datenschutzrechtliche Beurteilung hat dabei, drittens, vor dem Hintergrund der aktuellen DSGVO-Novelle zu erfolgen. Darauf aufbauend wird dargelegt, mit welchen Maßnahmen im Unternehmen bestmöglich auf die juristischen Herausforderungen reagiert werden kann. Dies auch in Bezug auf die rechtliche Bedeutung einer Zertifizierung nach ISO 27001 für Informationssicherheit.



Prof. Dr. Nikolaus Forgó, Institut für Rechtsinformatik, Leibniz Universität Hannover

17.20 Sichere Webapplikationen mit ISO 27001: Secure Coding Policy

Angriffe auf die Datenbestände eines Unternehmens erfolgen nach aktuellen Sicherheitsanalysen zum überwiegenden Teil direkt über die Applikationen. Die Norm ISO 27001 gibt die Grundsätze der Maßnahmen zur Sicherheit bei Entwicklungs- und Supportprozessen, zur Abwehr von Schadsoftware und zur korrekten Verarbeitung von Informationen vor. Die Einführung von „Secure Coding“ ist eine wirksame und schlanke Maßnahme, um die Sicherheit von Webanwendungen deutlich zu verbessern. Die Umsetzung einer solchen Policy in einem großen Rechenzentrum, wie dem BRZ beginnt mit der Awareness der Entwickler und der Erstellung verbindlicher Regeln. Schulung und ein strukturierter Erfahrungsaustausch über sicheren Code begleiten die Softwareentwicklung. Die Prüfung der erfolgreichen Umsetzung gewährleistet damit die Sicherheit der Anwendungen.



Ing. Johannes Mariel, Information Security Officer, BRZ GmbH

17.45 Perfekte Integration: ISO 20000 auf ISO 9001 – Qualität im IT Service Management

IT-Dienstleister werden mit zunehmendem Kosten- und Optimierungsdruck, anspruchsvollen Service Levels und vielfältigen Zusatzanforderungen hinsichtlich Compliance und neuer Normen konfrontiert. Die manchmal als „bürokratisch“ klassifizierten Qualitäts-, IT- und Servicestandards sind jedoch – bei pragmatischer Anwendung – ein Wegbereiter für wirksame IT-Governance, Kundenorientierung und schlanke Prozesse. Im Vortrag wird der integrative QM-Ansatz des IT-Bereichs der Oesterreichischen Nationalbank (OeNB) vorgestellt, der seit 9 Jahren nach ISO 9001 zertifiziert ist und derzeit um ISO-20000-Elemente erweitert wird. Dabei ergeben sich wesentliche Synergieeffekte in der Managementsteuerung, bei internen und externen Audits sowie in der Systemdokumentation.



Ing. Hermann Litschauer, IT Qualitätsmanagement, OeNB

18.05 Fragen & Antworten

18.20 Info-Cubes & Buffet / Ausklang mit Open End

COMPUTERWELT

**CONNECT
INFORMUNITY**

SIEMENS

Deloitte.

avedos
business solutions gmbh

SECURDATA

Siemens IT Solutions and Services



Dr. Starke
Managementsysteme®



CRISAM
DECISION ENGINEERING

ITSMPARTNER

