10. Information-Security-Symposium, WIEN 2014

Kundenvertrauen stärken – Sicherheit mit System: 04. Juni 2014, 13.00-18.30 / Open End / Kursalon Parkring, Johannesgasse 33, 1010 Wien

13.45 Eröffnung der Vorträge durch Erich Scheiber, CIS-Geschäftsführung

13.55 Schutz ISO 27001 für das Internet: ISMS-Implementierung bei Registry nic.at

Die nic.at GmbH ist die Österreichische Domain Registry und betreibt die Top Level Domain „.at" sowie mehrere generic TLDs. Das Funktionieren dieser Systeme und insbesondere des Domain Name Services ist essenziell für unseren täglichen digitalen Alltag. Um die Informationssicherheit nachhaltig sicherzustellen und kontinuierlich zu verbessern entschied sich nic.at ein Informationssicherheits-Managementsystem nach ISO/IEC 27001:2013 aufzubauen. Bei der Unternehmensgröße eines KMU gibt es spezifische Anforderungen bei der Einführung eines ISMS. So muss z.B. das meist nur rudimentäre Prozessmanagement Skaleneffekte unterstützen und die Flexibilität erhalten. Ein angemessenes Risikomanagement muss Sicherheitsmaßnahmen unterstützen und mit angemessenem Aufwand erlauben. Sicherheit als Selbstzweck ist ein absolutes „No-Go". Unser Ziel war und ist die Unterstützung des Kerngeschäfts der nic.at. Erfahrungen und Erkenntnisse sollen im Zuge des Vortrags erläutert werden.
Christian Proschinger, CISO, nic.at GmbH

14.25 Neun Jahre 27001-Zertifizierung: Eine Bilanz in Anlehnung an das BRZ-Reifegradmodell

Der Wandel der Sicherheitskultur vom Compliance-Anspruch zum alltäglich im Unternehmen gelebten Sicherheitsbewusstsein prägte die Zeit von der ersten Zertifizierung bis zum heutigen Tag. Die Veränderung der Rolle des CISO vom „Dr. No" zum Partner bei der Bewältigung der Sicherheitsfragen beschreibt diesen Wandel. Die kategorische Auflistung von Sicherheitsmaßnahmen ohne Wenn und Aber ist einem risikobasierten Ansatz des bewussten Umgangs mit der Informationssicherheit gewichen. Die Skepsis mancher Kunden gegen eine aufwändige Sicherheitsbürokratie ist dem in Verträgen manifestierten Wunsch nach einem Dienstleiter mit Sicherheitszertifikat gewichen. Wären alle diese Veränderungen auch ohne Verpflichtung zu einem ISMS nach ISO 27001 möglich gewesen? Haben sich die Erwartungshaltungen von Kunden und Geschäftsführung an diese Ausrichtung erfüllt? Steht der Mehrwert eines Zertifikats in einem guten Verhältnis zum Aufwand? Und wie kann die Akzeptanz der Mitarbeiter und des Managements aufrecht erhalten werden, nachdem der Reiz des Neuen verflogen ist? Die Antworten auf diese Fragen hören sie im Bericht über die Bilanz nach vier Sicherheitszertifikaten in neun Jahren.
Ing. Johannes Mariel, Abteilungsleiter G-SQ, Bundesrechenzentrum

14.55 Zeichen setzen: Vorbereitung auf die Data Center Zertifizierung nach ANSI/TIA 942

Als einer der ersten IKT-Service-Provider in Österreich plant die Energie AG OÖ Data GmbH eine Zertifizierung des Rechenzentrums nach ANSI/TIA 942. Der Vortragende berichtet über die wesentlichen Inhalte und Anforderungen der RZ-Norm mit ihren vier Infrastrukturbereichen Telecommunications (Phys. IT-Netz, passive Komponenten), Electrical (Energieversorgung und -verteilung), Architectural (Architektonik und physische Sicherheit), Mechanical (Klimatisierung, HKLS) sowie über die Herausforderungen bei der Implementierung. Synergien der Rechenzentrumszertifizierung mit ISO 27001 und die Vorbereitung zur Zertifizierung mit Hilfe eines Stage Reviews zwecks Statusbestimmung werden aufgezeigt. Die aus dem Stage Review gewonnenen Erkenntnisse werden beleuchtet und dargestellt. Die Anforderungen aus Sicht eines sicheren Rechenzentrums sind in manchen Bereichen strenger als in der Informationssicherheit. Als Beispiel sei genannt, dass der RZ-Standard nach TIA-Level 3 Zutrittsschleusen für Einzelpersonen mit Kameraauthentifizierung fordert. Die Einteilung erfolgt in vier Ratingstufen, wobei Ratingstufe 3 als Grundforderung eine korrigierende Instandhaltung ausweist.
DI (FH) Matthias Tischlinger, CISO, Energie AG OÖ Data GmbH

15.25 Solution Section // 15.40 Pause: Info-Cubes & Snacks

10. Information-Security-Symposium, WIEN 2014

Kundenvertrauen stärken – Sicherheit mit System: 04. Juni 2014, 13.00-18.30 / Open End / Kursalon Parkring, Johannesgasse 33, 1010 Wien

16.30 Risikoanalyse-Methoden für kritische Infrastrukturen und komplexe Abhängigkeiten

Durch Arbeitsteilung und Globalisierung stehen Wertschöpfungsprozesse unter zunehmendem Einfluss komplexer Wechselwirkungen. Neben steigenden Abhängigkeiten zwischen Informationen, Prozessen und IT-Systemen rücken vielfältige Angriffspunkte durch Störungen von Lieferketten, Versorgungsnetzen und strategisch wichtigen Unternehmen immer weiter in den Mittelpunkt der Medien. Der Vortrag gibt einen Überblick über grundsätzliche Anforderungen komplexer Informationssicherheits-Risikomanagementansätze und stellt unterschiedliche Risikoanalysemethoden für die Betrachtung von kritischen Infrastrukturen und komplexen Interdependenzen dar. Anhand einer beispielhaften Modellierungsbasis werden Anforderungen an Steuerung, Modellierung, Analyse, Kollaboration und Kontinuität aufgezeigt und Lösungswege beschrieben. Darauf aufbauend werden unterschiedliche Analysemethoden unter Anwendung von funktionalen Beziehungen, Bayes'schen Entscheidungsnetzen und Fuzzy Logic, Sozialer Netzwerkanalyse, Petrinetzen u.a. dargestellt und deren Vor- und Nachteile aufgezeigt.
Stefan Schiebeck Msc, Scientific Researcher, Austrian Institute of Technology GmbH

17.00 Intelligente Unternehmen – stabile Systeme, Fähigkeit zum schnellen Wandel

Systemmanagement-Normen haben sich bewährt und bestens etabliert. Über 1,1 Mio. nach ISO 9001 zertifizierte Organisationen weltweit und mehr als 300.000 ISO-14001-Zertifikate sprechen für sich. In der Informationssicherheit ist die ISO 27001 mir mehr als 20.000 Zertifizierungen und gut 2.000 Neuzugängen pro Jahr führend. Anforderungen nehmen zu, die Komplexität wächst, Know-how potenziert sich. Wie rüsten sich intelligente Unternehmen für die Zukunft? Welche Chancen und Perspektiven erkennen und nutzen sie? Warum wird die Kompetenz der Integration immer wichtiger? Welche Eigenschaften sind hier besonders gefordert? Wie könnte der Revisionsprozess von ISO 9001 & Co intelligente Unternehmen unterstützen? Wie kann Integration erfolgreich gemanagt werden? Wie können die möglichen Anforderungen der ISO 9001:2015 für den Erfolg von morgen schon heute genutzt werden?
DI Axel Dick, MSc Environmental Management, Prokurist, Quality Austria

17.25 Legal Compliance: Big Data – Herausforderungen aus datenschutzrechtlicher Sicht

Durch neue Systeme und immer leistungsfähigere Anwendungen ergeben sich immer neue Möglichkeiten, aber nicht alles was möglich ist, ist auch legal. Insbesondere im Bereich „Big Data" ergeben sich Spannungsverhältnisse mit dem Recht der Betroffenen auf Datenschutz. Mit einigen Beispielen aus der Praxis soll erläutert werden, wie derzeit die *worst Practice* bei Facebook und anderen Anlassfällen aussieht und was man daraus lernen kann. Die Grundsätze des Datenschutzes werden erläutert und besonders relevante Probleme bei „Big Data" Anwendungen (z.B. rechtlich gültige Zustimmung, Zweckbindung, Löschungsverpflichtungen oder Informationsverpflichtungen) herausgearbeitet. Neben der heutigen Praxis und der Durchsetzungspraxis in den EU-Mitgliedsstaaten wird abschließend auch die derzeit in Verhandlung befindliche EU-Datenschutzreform kurz erläutert, welche sich als wegweisende Veränderung in der heutigen Datenschutzlandschaft erweisen könnte.
Mag. Maximilian Schrems, Jurist, europe-v-facebook.org

18.00 Info-Cubes & Buffet – Band - Open End