

## Statements - qSkills Security Summit 2011

„Wirtschaftsspionage ist ein Phänomen, das in Zeiten der Globalisierung Großunternehmen und exportorientierte, innovative Mittelstandsunternehmen gleichermaßen bedroht. In Zeiten von Stuxnet und Co. reichen hier aber die klassischen IT-Sicherheitsmaßnahmen - und seien sie noch so gut implementiert - nicht aus, um das Risiko eines Informationsabflusses durch nachrichtendienstliche Angriffen auf die wichtigsten Geschäftsgeheimnisse wirksam zu reduzieren. Hier helfen nur maßgeschneiderte, auf die jeweiligen Geschäftsgeheimnisse angepasste Sicherheitslösungen, die sowohl die Technik als auch den Menschen als mögliche Schwachstelle und Angriffsziel wirksam schützen.“

*Thomas Königshofen, Konzern-Sicherheitsbevollmächtigter, Deutsche Telekom AG*

„Den PCI DSS umsetzen zu müssen bedeutet für betroffene Unternehmen einen erheblichen Aufwand. Betrachtet man den PCI DSS genauer, lassen sich Gemeinsamkeiten mit der ISO27001 sowie den Anforderungen des BDSG erkennen. Der Vortrag zeigt auf, welche Synergien sich bei einer gleichzeitigen Umsetzung der Anforderung sowohl des PCI DSS als auch des ISO27001 und des BDSG ergeben.“

*Randolf Skerka, Bereichsleiter, SRC Security Research & Consulting GmbH*

„Die Gemeinsamkeiten des Risiko-, Compliance- und Qualitätsmanagements sind unübersehbar. Gerade für kleine und mittelständische Unternehmen kann nur ein integrierter Ansatz die richtige Wahl sein, um sich in diesen Bereichen erfolgreich aufzustellen. Hier ist der prozessorientierte Qualitätsmanager angesprochen.“

*Jan Birkert, Qualitätsmanagement-Beauftragter, Oerlikon Leybold Vacuum GmbH*

„Die Biometrie feiert immer größere Erfolge mit täglich Millionen von Nutzern - nur leider nicht in Deutschland. Damit sich das ändert, wird im Vortrag gezeigt, dass Biometrie mittlerweile eine sehr sichere Angelegenheit ist, sie nicht nur Sicherheit, sondern weiteren Zusatznutzen stiftet und auch für den Massenkundenverkehr in der Kreditwirtschaft taugt.“

*Dr. Waldemar Grudzien, Direktor, Bundesverband deutscher Banken e. V.*

„Sicherheit lässt sich schon lange nicht mehr isoliert betrachten als reine Risikomanagement- oder als rein technische Disziplin. Eine Synthese aus beidem ist gefordert, zusammen mit einem tiefen Verständnis des Schutzbedarfes und der Schutzmöglichkeiten unserer Daten - gerade in Zeiten, wo wir immer weniger Kontrolle über die Informationsflüsse haben.“

*Martin Freiss, Geschäftsführer, secunomic GmbH*

## Statements – qSkills Security Summit 2011

„Sicherheitsaspekte werden häufig vergleichbar zu anderen nichtfunktionalen Anforderungen wie Performance erst relativ am Ende einer Projektverlaufes betrachtet. Vielfach hängt es am Wissen einzelner Projekt-Mitarbeiter, ob Security-Aspekte ausreichend in den frühen Phasen berücksichtigt wurden. Die planmäßige "Konstruktion" von Sicherheit erfordert aber eine Betrachtung des Themas über den gesamten Projektverlauf hinweg. Der Vortrag stellt ein projektbegleitendes Modell vor und zeigt einen Ansatz, wie es sich in ein ganzheitliches Sicherheitsrisikomanagement integrieren lässt.“

*Dr. Jörg Spilker, Leiter IT-Security, DATEV eG*

„Der Etablierung eines Business Continuity Managements (BCM) liegt der Gedanke der Wahrung elementarer Unternehmenswerte zugrunde. Ziel ist es das Leben der Mitarbeiter zu schützen sowie die Vermögenswerte und die Existenz des Unternehmens so weit als möglich sicherzustellen. Damit ist die zentrale Frage nicht ob, sondern wie denn ein BCM zu etablieren ist. Angepasst an die unternehmensindividuellen Gegebenheiten sind Lösungen zu entwickeln, die ein nachhaltiges BCM - sowohl in der Einführung als auch im Betrieb - ermöglichen. Schlantheit, Effizienz und Angemessenheit der BCM-Lösungen unter Berücksichtigung des unternehmensindividuellen Risikoprofils ist die Devise.“

*Bernd Malakowski, Operational Risk Officer & BCM-Koordinator, Swiss Life AG - Niederlassung für Deutschland*

„Für heutige Unternehmen sind Informationen der sensibelste Besitz, auf deren Basis die kritischen Geschäftsprozesse ablaufen. Daher muss die Geheimhaltung, Integrität und Verfügbarkeit dieser Informationen zu jeder Zeit gewährleistet werden. Die Informationen sind allerdings bereits bei ihrem Entstehen sehr vielfältig. Aus Geschäftssicht muss es möglich sein, unterschiedliche Sicherheitsstufen, basierend auf dem Geschäftswert und dem Sicherheitsrisiko der Informationen zu definieren. Die Daten hinter diesen Informationen sollten daher über spezielle IT-Sicherheitsmechanismen immer in Verbindung zu den Geschäftsprozessen klassifiziert und geschützt werden. Die Praxis zeigt, dass reine Data Lost Prevention Produkte nicht die Anforderungen an die heutige Informationssicherheit erfüllen und dass eine neue Lösung gefunden werden muss, um Daten und dadurch Informationen klassifizieren zu können und über Ihren Lebenszyklus hinaus zu verwalten.“

*Alina Mot, Leiterin des Competence Centers IT-Security, Empalis GmbH*

„Daten werden gespeichert um diese im Falle eines Desasters wiederherzustellen zu können. Dabei sollten diese Informationen verschlüsselt werden, um diese Daten vor Angriffen zu schützen und um rechtlichen Vorgaben zu genügen. Ein einheitliches, auditierbares und sicheres Schlüssel-Management für Unternehmen ist daher unverzichtbar. Verschiedene Standards entstanden um proprietäre Lösungen abzulösen.“

*Simon Taylor, Sales Manager Storage Solutions EMEA, THALES Information Systems Security*

## Statements - qSkills Security Summit 2011

„Entscheider sollten heute die Ressourcen auf das ernsthafte Nachdenken über die wesentlichen kritischen Zukunftsszenarien und Risiken lenken - und weniger in einer vergangenheitsorientierten Risikobuchhaltung verharren. Dies erfordert ein breites Verständnis interdisziplinärer Zusammenarbeit und auch andere Methoden, beispielsweise szenariobasierte Ansätze.“

*Frank Romeike, Geschäftsführer, RiskNET GmbH - The Risk Management Network*

„Sicherheitstechnik kann Benutzer nicht vor ihrem eigenen Verhalten schützen. Social Engineering nutzt das aus. Benutzer müssen lernen, sich richtig zu verhalten. Das ist schwer. Aber es ist möglich, wenn man es richtig macht.“

*Dr. Werner Degenhardt, Ludwig-Maximilians-Universität München, Fakultät Psychologie und Pädagogik, und Christian Steinkampf, Geschäftsführer Core-Competence GmbH*