

## Quantensprung

# Die Quantifizierung von Informationssicherheit



Für die meisten Mitarbeiter in Unternehmen bedeutet Sicherheit ein muskelbepackter Wachmann, eine elektronisch gesicherte Eingangstür, die das Durchziehen eines Sicherheitsausweises verlangt, oder vielleicht noch eine Firewall auf dem Arbeitsplatzrechner.

Für Prof. Dr.-Ing. Clemens Martin von der Dualen Hochschule Baden Württemberg in Mannheim bedeutet Sicherheit jedoch viel mehr. Als Experte im Bereich Betriebssysteme und Netzwerke weiss er natürlich um den Wert der auf Computern gespeicherten

Daten und sein Forschungsfeld an der DHBW dreht sich darum die Sicherheitsverfahren und Systeme zu verbessern, die die unternehmenskritischen Daten und Informationen schützen.

Als Professor der Wirtschaftsinformatik in der Fakultät für Be-

triebswirtschaft der DHBW vereint Prof.Dr.-Ing. Martin präzise akademische Arbeit mit umfangreicher Erfahrung im wirtschaftlichen Umfeld: „Informationen, die Unternehmen sammeln, neu schaffen und wieder verbreiten gehören

zu deren wertvollsten Gütern“ konstatiert Prof.Dr.-Ing. Martin.

Die Gründe Hackern und auch Wettbewerbern jeweils einen Schritt vorausbleiben zu wollen, sind klar. Allein in den USA verursachten Verletzungen der IT Sicherheit bei den Unternehmen Kosten im Durchschnitt pro Vorfall von \$234.000 (CSI Report 2009); eine Zahl, die zwar unter der des Vorjahres aber immer noch oberhalb der von 2005/2006 erhobenen Werte liegt. Spitzenreiter (mit \$770.000) sind mittlerweile Sicherheitsvorfälle, die auf Schwächen in der Wireless-Infrastruktur basieren (vor Diebstahl von mobilen Geräten mit \$710.000 und finanziellem Betrug mit \$450.000). Prozentual gesehen liegen die Vorfälle die durch Infektionen mit Schadsoftware verursacht wurden, mit 64,3 % deutlich vor den Diebstählen von Laptops und anderen mobilen Geräten(42,2%) und den in 2007 mit fast 60% noch an der Spitze liegenden „Insider“-Attacks (29.7%).

„Mein Hauptfokus liegt auf Informationssicherheitsbetrachtungen für die Unternehmensebene, nicht im Detail der technischen Infrastrukturlösungen, sondern auf den Technologien und Methoden die eine bessere Unterstützung der Geschäftsprozesse erlauben“, so Dr. Martin.

Die Ermittlung von geschäftsrelevanten Informationssicherheitsinformationen wird zunehmend wichtiger. In Folge der Finanzskandale in den USA rund um Enron und WorldCom sind dort mit der Sarbanes-Oxley Gesetzgebung von 2002 Auflagen für die Industrie geschaffen worden, die mittlerweile entsprechende oder ähnliche Maßnahmen in der gesamten industrialisierten Welt nach sich gezogen haben. Das ursprüngliche Gesetz verlangt, dass börsennotierte Unternehmen in ihren Jahresberichten über die Effektivität ihrer internen Kontrollsysteme für die finanzbuchhaltenden Systeme Auskunft geben.

„Für die Unternehmen, die Audits durchführen und Jahresabschlüsse prüfen, stellt dies eine Herausforderung dar, weil ihr Prüfungsauftrag nun so verstanden wird, dass auch die

Prozesse und Systeme zur Gewährleistung der Unverfälschtheit und zum Schutz dieser Finanzdaten mitgeprüft werden müssen“, sagt Dr. Martin. „Sicherheitsmechanismen sind notwendig um die Kompromittierung dieser Daten wirkungsvoll zu verhindern. Für das obere Management stellt sich in Folge dessen allerdings die schwierige Frage, wie genau es um die Informationssicherheit in ihren Unternehmen steht und in welcher Qualität diese gemanaged wird. Gerade im Hinblick auf unliebsame Überraschungen bei den entsprechenden Unternehmensprüfungen möchte man vorbereitet sein, um proaktiv handeln zu können.“

In seinem bereits an seiner vorigen Universität, der University of Ontario Institute of Technology (UOIT) in Kanada, in Zusammenarbeit mit Bell Canada, der größten kanadischen Telefongesellschaft, begonnenen Forschungsvorhaben versucht Dr. Martin effizientere Methoden zu entwickeln, um Unternehmen besser und schneller Auskunft über den Status der Informationssicherheit geben zu können.

„Viele informationstechnisch orientierten Überlegungen für große Systeme beschränken sich auf Fragestellungen wie ‘Woher bekomme ich welche Daten und wie verarbeite ich diese möglichst effizient?’, wie sie etwa von Security Information Management Systemen beantwortet wird. Dabei wird häufig die Frage des gesamtunternehmerischen Zusammenhangs und damit der Unterstützung der Unternehmensziele außer Acht gelassen. Seine Forschungsarbeiten konzentrieren sich daher auf die Entwicklung eines ‘Information Security Dashboards‘ für die Managementebene, um damit eine effizientere Erfolgskontrolle und Ressourcensteuerung zu ermöglichen.

Letztendliches Ziel ist es, ein Informationssicherheits-Regelungssystem zu entwerfen, das das Management bei der Auswahl geeigneter Maßnahmenpakete unterstützt.“

Kenntnis um die Bedrohungslage und die damit verbundenen Sicherheitsvorfälle ist eines der Themen mit denen er sich auch mit seiner Co-Autorin Dr. Bernadette Schell, ehemalige Dekanin der Fakultät für Business & IT an der UOIT, in zwei Büchern „Cybercrime“ und dem „Websters New World Hacker Dictionary“ intensiv beschäftigt hat.

„Die ‚Bad Guys‘ verbessern kontinuierlich ihre Kenntnisse und Methoden“, sagt er offen. „Wir müssen sicherstellen, dass die ‚Good Guys‘ nicht auf der Verliererseite landen“.

Nach der Entwicklung des ersten kanadischen Masters of IT Security hat Dr. Martin nun für die Duale Hochschule Baden Württemberg in Mannheim den MBA-Studiengang „IT Management“ entwickelt. Dieser weist als eine von drei möglichen Vertiefungsrichtungen das „Management von Informationssicherheit“ auf und wird unter Leitung von Dr. Martin ab September 2010 durch die Graduate School Rhein-Neckar, den Kooperationspartner der DHBW Mannheim für weiterführende und berufsbegleitende Studiengänge, angeboten.



„Für die Unternehmen, die Audits durchführen und Jahresabschlüsse prüfen, stellen die neuen gesetzlichen Vorgaben eine Herausforderung dar, weil ihr Prüfungsauftrag nun so verstanden wird, dass auch die Prozesse und Systeme zur Gewährleistung der Unverfälschtheit und zum Schutz dieser Finanzdaten mit geprüft werden müssen.“

Prof. Dr.-Ing. Clemens Martin