Unternehmer- und Aufsichtsratshaftung

Fachkonferenz des Münchner Kreises, 18. September 2003

Rolf v. Rössing

Übersicht

- Klassische Unternehmer- und Aufsichtsratshaftung
- Der Bezug zu Risiken in der Informationssicherheit
- Fallbeispiele
- Konsequenzen und Lösungen
- Ausblick

Klassische Haftung

- Unternehmer bzw. Vorstand / Geschäftsführung haften ggü. Dritten
- Aufsichtsrat leistet „good corporate governance“
- KonTraG 1998 führte verpflichtend „Früherkennungssystem“ ein
- IT-Risiken formal eher unterrepräsentiert
- Rechtsprechung sehr unterschiedlich ausgeprägt – Vorhersagbarkeit bisweilen nicht gegeben

Der Bezug zu Risiken in der Informationssicherheit

- in der Praxis: keiner !
- IT-Risiken werden häufig sachlich nicht verstanden
- Kostendruck in der IT begünstigt übermäßig hohe Risiken in der Informationssicherheit
- Haftung erstreckt sich jedoch umfassend und zwingend auf die Informationssicherheit
- Normen und “best practices” werden nur ansatzweise umgesetzt

Bezug zu Risiken in der Informationssicherheit (2)

- Information ist „Kernstück“ der unternehmerischen Tätigkeit
- Sicherheit der Information beginnt auf der Infrastrukturebene und endet bei der personellen Sicherheit
- Entstehende Risiken und Haftungsfragen gelten sinngemäß zu „normalen“ Risiken

Bezug zu Risiken in der Informationssicherheit (3)

- Verletzungen der Informationssicherheit führen immer häufiger zu Ansprüchen (Mitarbeiter, Dritte) an das Unternehmen
- Haftung des Fachverantwortlichen ist beschränkt: Schaden kann durch „symbolische Pfändung“ selten abgewendet werden
- Mittelbar greift die Vorstands- / Geschäftsführerhaftung (AktG/GmbHG - kaufm. Sorgfalt, Pflicht zur Voraussicht, Pflicht zur Schadensabwendung), in Deutschland sogar mit Beweislastumkehr bei Vorständen
- „Schuldhaftes Unterlassen geeigneter Absicherungsmaßnahmen...“ ? „...wider besseres Wissen“ (Vorsatz) ?? „... ohne sich rechtzeitig informiert zu haben“ (grobe Fahrlässigkeit) ???

Fallbeispiele

- Internet-Präsenz:
  - Marken, Verlinkung und Download-Angebote sind Zielgebiet
  - Interne oder externe Angriffe können unmittelbar Haftung auslösen (z. B. Defacements)
  - Unbeabsichtigte Offenlegung datenschutzrelevanter Informationen kann Probleme verursachen
- Drahtlose Netzwerke (WLAN):
  - nahezu vollständige Offenheit unterläuft anderweitig getroffene Sicherheitsmaßnahmen
  - “kein Schutzwille erkennbar” entlastet Täter und bedeutet Haftung
  - Unwissenheit schützt nicht vor Strafe

Fallbeispiele (2)

- Social Engineering:
  - „Sekretariatsrisiko“ ?
  - Schlüsselpersonen
  - Haftung auch nach Ende eines Arbeitsverhältnisses
- Spam:
  - Haftung bei „nigerianischen Geschäften“ ?
  - Erlaubte / unerlaubte Techniken des Vertriebs ?
  - Pornographie und politische Äußerungen ?
- Technik:
  - was sind „zumutbare“ Absicherungsmaßnahmen ?
  - was ist „menschenmöglich“ ?
  - wie oft sind Maßnahmen zu aktualisieren, um haftungserleichternd oder haftungsbefreiend zu wirken ?

Konsequenzen und Lösungen

- Rechtlich ist die Situation weitgehend klar – praktisch keineswegs
- Der Einzelfall ist – bei hoher technischer Komplexität in der Informationssicherheit – noch immer das Maß aller Dinge
- Optimierung und Automatisierung (Zeit ist Geld) bedeuten Anfälligkeit für humanintelligente Angriffe
- Die Haftungslage ändert sich nicht, aber das technische und praktische Umfeld

Konsequenzen und Lösungen (2)

- Normen (ohne Gesetzeskraft) können helfen, ein einheitliches Verständnis zu erzielen
- Hinterfragen des herrschenden Denkens in bezug auf die IT ist unabdingbar – Kostensenkung / Risikoerhöhung ?!
- IT-Durchdringung des (längst nicht mehr traditionellen) Geschäfts ist als Faktum festzuschreiben:
  - wachsende Informationsmengen bedeuten zunehmenden Aufwand für deren Sicherheit
  - Angriffsziele und –methoden werden vielfältiger
  - “Information Warfare” ist längst Realität
  - klassische Haftungsmuster werden zunehmend durch Fragen des Informationsverlusts / -gewinns ersetzt

Ausblick

- Rechtsprechung wird Unternehmer- und Aufsichtsratshaftung zunehmend auf die Informationssicherheit beziehen
- Heutige Lage zeigt Handlungsbedarf: die Möglichkeiten und Bedrohungen der IT und des „Information Warfare“ haben sich schnell entwickelt
- „Virtuelle Unternehmen“ heute und in Zukunft werden noch stärker von der Informationssicherheit abhängen – und dafür haften