Presse-Information vom 17. Juni 2010

Wer haftet für Schäden durch mangelnde IT-Sicherheit?

IT-Manager stehen mit einem Bein im Knast, wenn sie sorglos mit IT-Sicherheit umgehen. Was das konkret bedeutet, konnten 50 IT-Manager während einer kürzlich durchgeführten Veranstaltung der Firma MODCOMP am eigenen Leib erfahren. Der IT-Security Workshop fand in den Räumen der JVA Köln statt und bot – neben Fachvorträgen – Einblicke in den Alltag einer Justizvollzugsanstalt.

Der sorglose Umgang mit IT kann zu Schäden in erheblichem Ausmaß führen, beispielsweise bei Datenverlust, Urheberrechtsverletzungen, durch Computerviren oder gezieltes Hacking. Der Bundesgerichtshof hat beispielsweise in seinem Urteil vom 17.07.2009 die strafrechtliche Verantwortung des so genannten Compliance Officers bestätigt, also desjenigen im Unternehmen der für die Rechtssicherheit verantwortlich ist. Danach kann sich dieser selbst wegen einer Beihilfe durch Unterlassen zu betriebsbezogenen Delikten strafbar machen, sofern er trotz Kenntnis des strafbaren Verhaltens nicht die notwendigen Maßnahmen zur Verhinderung ergreift. Prof. Dr. Dirk-Michael Barton, Inhaber des Lehrstuhls für Wirtschafts- und Medienrecht an der Universität Paderborn, rät jedem IT-Manager dazu, seinen Kompetenzbereich im Arbeitsvertrag eindeutig zu formulieren und zu konkretisieren. Als Beispiel führt Prof. Barton die Durchführung von E-Mail Kontrollen in Unternehmen an. Falls ein Unternehmen nicht die private Nutzung von E-Mails verbietet, kommt das Fernmeldegeheimnis zum Tragen. Selbst wenn ein begründeter Verdacht vorliegt, verbietet das Telekommunikationsgesetz jegliche Kontrollen der E-Mails. In diesem Fall kann ein IT-Manager als Täter oder Gehilfe strafrechtlich zur Verantwortung gezogen werden, falls er unzulässige Kontrollen von E-Mail Inhalten durchführt oder duldet.

In seiner Jugendzeit war Gunnar Porada selbst Hacker, bis er mit 19 Jahren die Seiten wechselte. Seit Anfang der 90er Jahre ist er Unternehmensberater, überprüft die IT-

Sicherheit in Wirtschaft und Behörden auf der ganzen Welt und zeigt Verbesserungsmöglichkeiten auf. Im Rahmen eines Live-Hackings demonstrierte Porada die Schwachstellen des elektronischen Reisepasses und der darauf gespeicherten Fingerabdrücke. Anhand eines Angriffs auf Online Banking erläuterte er, wie Kriminelle sich selber Geld überweisen. Mahnend verwies Porada auf die Statistiken der IT-Sicherheitsfirmen, wonach 70% aller Web 2.0 Applikationen angreifbar sein sollen. Dadurch wird den betroffenen Betreibern und Unternehmen nicht nur direkter Schaden zugefügt, sondern die Server werden auch noch als Virenschleudern missbraucht. Solch manipulierte Webserver verbreiten dann ihre Schädlinge beim einfachen Ansurfen durch Schwachstellen im Webbrowser. Der normale Besuch einer Webseite reicht mittlerweile schon aus, um sich im Internet zu infizieren.

Wilfried Karden ist im Innenministerium NRW zuständig für die Abwehr von Wirtschaftsspionage. Wenn ein Unternehmen einen Verdacht auf Wirtschaftsspionage hat, ist der Verfassungsschutz zunächst der richtige Ansprechpartner, da Arbeitsergebnisse nicht veröffentlicht werden müssen. Dringt beispielsweise ein Fremder in ein Firmennetzwerk ein, kann der Verfassungsschutz ermitteln, ohne – wie die Polizei – gleich alle Computer mitzunehmen und ein Ermittlungsverfahren einzuleiten. Häufig steht der Vertrieb im Fokus der Kriminellen, da hier Informationen über Produkte, Kunden und aktuelle Angebote zusammenlaufen. Nach Meinung von Karden sind max. 5 % der Daten eines Unternehmens sicherheitskritisch und verlangen einen besonderen Schutz. Das erfordert technische Maßnahmen, aber auch Anforderungen an das Personal, z.B. dass in diesen sicherheitskritischen Bereichen externes Personal nur nach Überprüfung und in Anwesenheit eines Mitarbeiters eingesetzt wird.

Das Unternehmen CheckPoint Software Technologies –eines der führenden Unternehmen im Bereich Internetsicherheit – präsentierte schließlich seine Secure Virtuel Networking Architektur (SVN) als Basis für eine zuverlässige und vertrauliche Kommunikation im Internet. SVN gewährleistet sichere Business-to-Business

Verbindungen in Intranets, Extranets und dem Internet sowie zwischen Netzen, Systemen, Applikationen und Anwendern. Im vergangenen Monat veröffentlichte Check Point eine neue, netzwerkbasierte Data Loss Prevention (DLP)-Lösung. Sie soll für den präventiven Schutz sensitiver Informationen sorgen - wie z. B. regulativer, vertraulicher oder geheimer Daten. Auf Basis der Benutzerprofile und des Know-hows über mehr als 4.500 Applikationen meldet sich das System, wenn ein Verdacht auf Missbrauch vorliegt.

Auch wenn Frau Watzlaw von der Anstaltsleitung der JVA Köln zugeben musste, dass unter den 1.100 Gefangenen in Köln nur wenige Personen aufgrund von Online Verbrechen inhaftiert sind, verließen alle Teilnehmer mit einer neuen Sensibilität für Haftungsrisiken das Gebäude. Das Fazit des Tages: „IT-Security ist ein wichtiges Thema, welches kontinuierlich Aufmerksamkeit und Investitionen erfordert und notwendig ist, um Schaden für das Unternehmen und die Mitarbeiter zu verhindern.“ Denn der IT-Security Beauftragte muss im Ernstfall nachweisen, dass immer der technisch neueste Stand von Schutzmaßnahmen im Einsatz ist.

Initiator der Veranstaltung war der Kölner Systemintegrator MODCOMP. Das Unternehmen unterstützt seine Kunden von der Planung bis zur Inbetriebnahme und Überwachung von zuverlässigen und umfassenden IT-Securitylösungen. Unternehmen können einen Risk- und Compliance Service von MODCOMP buchen, der ihnen einen Überblick über das aktuelle Sicherheitsniveau ihrer IT-Systeme gibt, Schwachstellen bzw. Verstöße gegen Konfigurationsrichtlinien aufdeckt und Optimierungen vorschlägt.

Prof. Dr. Dirk-Michael Barton: Multimediarecht:
Kohlhammer Verlag, ISBN: 978-3170209329

Leitfaden IT-Sicherheit:
Kostenloser Download unter **www.bsi.bund.de**

Wirtschaftsspionage: Information und Prävention:

Kostenloser Download unter **www.im.nrw.de/wirtschaftsspionage**

Weitere Informationen zu IT-Sicherheitslösungen:
Ulrich Wickers, **ulrich.wickers@modcomp.de**, Tel: 0170/8425871

Über MODCOMP

Die MODOMP Gruppe ist als Systemhaus und -integrator seit mehr als 30 Jahren am deutschen Markt präsent. Weltweit gehört das Unternehmen mit Schwesterfirmen in Großbritannien und den USA zum Konzern CSP Inc. Zu den langjährigen Kunden zählen bedeutende Unternehmen aus der Industrie, den Branchen Telekommunikation, Energieversorgung, Banken und Versicherungen. MODCOMP-Kunden profitieren von vielfältigen Managed Services, die auf den individuellen Bedarf eines Unternehmens hin angepasst werden.

www.modcomp.de

Redaktionskontakt:

Modular Computer Systems GmbH
Ulrich Wickers
Business Development Manager
Oskar-Jäger-Straße 50
50825 Köln
Phone +49 (0) 221 954466-57
Fax +49 (0) 221 954466-99
Mobile +49 (0) 170 8425871
ulrich.wickers@modcomp.de