



Foto: Bildenbox

WINFRIED LAMBERTZ

Wer haftet bei Netzwerk-Attacken?

IT-Manager wissen oft nicht, dass ihre Verantwortung mit großen persönlichen Risiken verbunden ist. Risiken, die im Ernstfall gravierende Folgen mit sich bringen können. Wie entstehen solche Risiken und wie können sich IT-Verantwortliche dagegen schützen? Diese Fragen standen auf der Tagesordnung des „CIO-Kongresses“, der auf Einladung der Used Soft GmbH im Oktober in München stattfand.

► Die Informationsverarbeitung nimmt heute in nahezu allen Unternehmen eine Schlüsselrolle ein. Alle strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik maßgeblich unterstützt. Ein Ausfall von IT-Systemen kann gravierende Folgen für die Aufrechterhaltung des Geschäftsbetriebs haben, wenn es nicht gelingt, die Störung kurzfristig zu kompensieren. „Die Kernkompetenz des Managements muss in der Sicherung der IT-Anlagen liegen“, unterstreicht der auf IT-Recht spezialisierte Münchner Anwalt Wilfried Reiners die Bedeutung der IT-Security für ein Unternehmen. „Gefordert wird der Schutz der Infor-

TO-DO-LISTE

Haftungsrisiken ausblenden

- Machen Sie IT-Sicherheit zur Chefsache
- Bestellen Sie einen Verantwortlichen für die IT-Sicherheit
- Holen Sie sich professionelle Beratung ins Haus
- Befreien Sie sich von der Haftung durch rechtliche Absicherung

Quelle: PRW, München

mationen vor unberechtigtem Zugriff, vor unerlaubter Änderung und vor Zerstörung.“

Die IT ist also so zu managen, dass sie sicher ist. Kommt ein für IT verantwortlicher Geschäftsführer oder Vorstand seinen „Sorgfaltspflichten eines ordentlich handelnden Kaufmanns“ nicht nach, dann haftet er oder sie ganz persönlich. Und das ist schnell geschehen. „Jede Version oder jedes Upgrade einer Anwendung oder eines Betriebssystems birgt neue Sicherheitslücken“, warnt Hans-Joachim Diedrich vom Sicherheitsdienstleister F-Secure. Die größten Gefahrenquellen aber entstehen im Zusammenhang mit der Nutzung des Internets einschließlich E-Mail. Die Firmenpräsenz im Netz kann zum Angriffsziel von Hacker-Attacken werden. Der Datenaustausch mit Kunden, Filialen und Lieferanten über ein Extranet stellt eine ebenso kritische IT-Sicherheitsumgebung dar wie lokale Firmennetzwerke.

In Anbetracht dieses großen Risikopotenzials kann die Sicherung der Informationstechnik nur Chefsache sein. Die Praxis sieht allerdings anders aus. Ein Problem ist vor allem die mangelnde Sachkenntnis von Geschäftsführern in Fragen der IT-Sicherheit. Jede Aktiengesellschaft ist zum Beispiel verpflichtet, ein Risiko-

management im Schadensfall schriftlich nachzuweisen. Wenn Hacker- oder Virenangriffe in einem Unternehmen offene Türen vorfindet, weil sich der Geschäftsleiter nicht um die IT-Sicherheit gekümmert hat, dann ist er für die Folgen haftbar. Keine Versicherung wird Schäden ersetzen, wenn sie erfährt, dass der Schaden hätte vermieden werden können.

Wo sind nun die einschlägigen Rechtsvorschriften zu finden, die das Thema IT-Sicherheit abbilden und dem Unternehmer Orientierungshilfen geben? „Ein spezielles IT-Sicherheitsgesetz, in dem alles geregelt ist, gibt es nicht“, klärt Wilfried Reiners auf. Die relevanten Vorschriften sind vielmehr weit verstreut und finden sich in unterschiedlichen Gesetzen. Im Haftungsgefüge ist zunächst zwischen einer zivilrechtlichen Haftung, einer öffentlich-rechtlichen Verpflichtung – zum Beispiel Datenschutz – und einer strafrechtlichen Verantwortung zu unterscheiden.

Strikt untersagt ist es, Daten zu verändern. Über die Konsequenzen informiert der Paragraph 303a des Strafgesetzbuches: „Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.“ Zugriffe auf E-Mails

INTERVIEW

Privates Surfen und E-Mails verbieten

Rechtsanwalt Wilfried Reiners empfiehlt, Gefahrenquellen für die IT-Sicherheit eines Unternehmens im betrieblichen Umfeld auszuschalten.



Wilfried Reiners



**Rechtsanwalt und Managing Partner,
Kanzlei PRW, München**

rt: Hacker-Angriffe und Viren-Attacken können in den Netzwerken von Handelsunternehmen schwere Schäden anrichten. Wer im Unternehmen ist vor dem Gesetz für die Konsequenzen haftbar? Kann der Geschäftsführer die Verantwortung an den IT-Chef delegieren?

REINERS: Hier ist zunächst zu unterscheiden zwischen einer strafrechtlichen Verantwortlichkeit und einer zivilrechtlichen Haftung. Strafrechtliche Verantwortung lässt sich niemals delegieren. Aber auch zivilrechtliche Verantwortung lässt sich nur begrenzt weitergeben. Stark verkürzt lässt sich Ihre Frage so beantworten: Ist die EDV wichtig für das Unternehmen? Wenn ja, lässt sich die Managementhaftung nicht mehr weg delegieren. Die Funktion des IT-Chefs ist dann allein über das Arbeitsverhältnis definiert.

rt: Viren, Trojaner und andere Schädlinge gelangen nicht selten durch unachtsames Verhalten der Mitarbeiter in die Firmennetzwerke. Inwieweit kann sich der für die IT-Sicherheit Verantwortliche von der Haftung befreien, wenn der Schaden beispielsweise durch privates Surfen oder E-Mails der Mitarbeiter verursacht wurde? Ist eine rechtliche Absicherung möglich?

REINERS: Hier gibt es nur eine Lösung: Das private Surfen und E-Mails muss strikt verboten werden. Andernfalls verletzt die Geschäfts-

leitung durch den Einsatz von Anti-Spam- oder Anti-Viren-Software das Post- und Fernmeldegeheimnis gemäß Paragraph 206 des Strafgesetzbuches. Die echten Gefahren für das Management liegen aber in der praktischen Umsetzung. Wenn der IT-Leiter beispielsweise feststellt, dass sich auf dem Firmen-Server verbotenes pornographisches Material befindet, dann würde nach einer Anzeige eine Beschlagnahme des Servers durch die Staatsanwaltschaft erfolgen. Wieviele Unternehmen kennen Sie, die problemlos weiter arbeiten können, wenn ihr Server beschlagnahmt wird?

rt: Nicht viele. Heißt das, dass solche oder ähnliche Straftaten besser nicht angezeigt werden sollten?

REINERS: Im Gegenteil. In der digitalen Welt müssen die gleichen Grundsätze angewendet werden wie sonst auch. Es sind jedoch die praktischen Auswirkungen der Umsetzungen zu beachten. Dabei sind vor allem die technischen Gegebenheiten der IT-Infrastruktur zu berücksichtigen.

rt: Durch professionelle Beratung lassen sich Risiken eingrenzen. Welche Informationsquellen können Sie dem Handel hier empfehlen?

REINERS: Inzwischen hat sich das Beratungsangebot erweitert. Nach meiner Einschätzung steht an erster Stelle nicht das Beratungsunternehmen, sondern der Beschluss des Handelsunternehmens, das sicher werden möchte. Alle Berater würden zunächst prüfen, wie sicher oder unsicher eine IT-Infrastruktur ist, bevor sie weitere Maßnahmen vorschlagen würden. Wer sich mit dem Thema intensiver auseinandersetzen möchte, sollte einmal unter dem Suchbegriff IT-Sicherheit im Internet surfen. Gute Informationen gibt es auch beim Bundesamt für Sicherheit in der Informationstechnik im Internet surfen. ●

der Mitarbeiter sind ebensowenig erlaubt wie die Unterdrückung eingehender Nachrichten. Selbst dann, wenn der dringende Verdacht besteht, dass die E-Mail eines Mitarbeiters mit Viren verseucht sind, sind dem Unternehmensleiter die Hände gebunden, will er nicht Gefahr laufen, das Post- und Fernmeldegeheimnis zu verletzen. „Das Tatbestandsmerkmal des Unterdrückens im Sinne von Paragraph 206 des Strafgesetzbuches (Verletzung des Post- und Fernmeldegeheimnisses, A. d. Red.) wird durch das Ausfiltern von E-Mails erfüllt“, warnt Reiners und verweist auf ein Urteil des OLG Karlsruhe vom 10.1.2005 (1 WS 152/04). Gibt es einen Rechtfertigungsgrund, dennoch zu filtern? Reiners: „Theoretisch ja, praktisch nein“. Was so viel bedeutet wie: Gesetze alleine schützen nicht.

Schnelle Reaktion

Der Unternehmer kann sich nur dann von der Haftung befreien, wenn er das private Surfen und E-Mails in seinem Betrieb strikt verboten hat, beispielsweise durch eine E-Mail-Nutzungsvorschrift. Die Einhaltung dieser Vorschrift muss regelmäßig kontrolliert werden.

Um das Firmennetzwerk gegen die ständigen Angriffe von Hackern zu schützen, ist die Investition in eine wirksame Software-Lösung zum Schutz vor Viren und anderen Bedrohungen aus dem Internet für jedes Unternehmen Pflicht. Rund 60 Anbieter gibt es allein im Bereich Antivirus. Zu den renommierten Anbietern zählen neben F-Secure u.a. die Software-Produkte von McAfee, Norman, Sophos oder Symantec.

Was die Anbieter im Wesentlichen voneinander unterscheidet, ist die Reaktionszeit bei neu aufgetretenen Bedrohungen. Auf maximal fünf bis sechs Stunden grenzt Hans-Joachim Diedrich die Zeitspanne ein, in der ein Gegenmittel gegen einen neu entdeckten Virus im Firmennetzwerk stehen muss.

Unabhängige Testinstitute helfen, die Investitionsentscheidung für die Sicherheits-Software abzusichern (z. B. www.av-test.org). Die zunehmende Aufklärung und Wachsamkeit der Nutzer habe das Sicherheits-Level erhöht, so Diedrich: „Die Bedrohungslage ist zwar weiterhin akut, aber nicht mehr mit der Situation von 2003/2004 vergleichbar.“ Auch die bei Windows XP im Leistungsumfang enthaltene Firewall-Komponente habe die Gefahr eingedämmt. Bestandteil einer jeden Sicherheitslösung sollte unbedingt eine Anti-Spyware sein, welche das Firmennetzwerk gegen kriminelle Spionageattacken schützt.

„Das offensichtliche Vorhandensein von Angreifern und Angriffsmöglichkeiten fordert von den IT-Verantwortlichen das Ablegen von Sorglosigkeit. Wer sorglos ist, haftet, und zwar immer“, so die klare Aussage von Rechtsanwalt Reiners. Der Nicht-Einsatz von Antiviren-Software kann für den CIO haftungs- und strafrechtliche Konsequenzen nach sich ziehen, wie das Landesgericht Hamburg in einem Fall urteilte (401 O 63/00 vom 18.7.2001). Wer auf den Einsatz entsprechender Software verzichtet, handelt grob fahrlässig.

Die beste Verteidigung gegen Computerschädlinge bleibt allerdings nutzlos, wenn die Mitarbeiter das Firmennetzwerk für illegale Aktivitäten missbrauchen. Die möglichen Konsequenzen veranschaulicht Wilfried Reiners an folgendem Beispiel: Ein IT-Leiter stellt im Rahmen einer routinemäßigen Kontrolle fest, dass sich

INTERVIEW

Lokale Absicherung in den Filialen

Hans-Joachim Diedrich, Geschäftsführer Deutschland der F-Secure GmbH in München, erklärt, welche Sicherheitsvorkehrungen ein Handelsunternehmen zum Schutz vor Viren und anderen Bedrohungen aus dem Internet treffen sollte.

rt: Firmennetzwerke sind ständig neuen Angriffen aus dem Internet ausgesetzt. Die Investition in eine verlässliche Sicherheits-Software ist auch für Handelsunternehmen unumgänglich. Welche Komponenten sollte diese Software unbedingt umfassen?

DIEDRICH: Neben der Absicherung der Firmen-Infrastruktur durch eine Firewall sollte für die E-Mail-Server und Desktop- bzw. Notebook-Arbeitsplätze Virenschutz, Spyware und Spamfilter zum Einsatz kommen.

rt: Große Handelsunternehmen betreiben oft mehrere Hundert Filialen. Reicht hier die zentrale Verwaltung der IT-Sicherheit aus, um den Schutz der IT-Systeme in den Filialen zu gewährleisten, oder empfehlen Sie zusätzliche individuelle Sicherheitsmaßnahmen auf Filialebene?

DIEDRICH: Wir empfehlen in jedem Fall auch die lokale Absicherung der Arbeitsplätze in den Märkten, da diese Systeme jederzeit durch Disketten, USB-Sticks, lokale DSL-Verbindungen etc. kompromittiert werden können. In den seltensten Fällen ist die Netzwerk-Infrastruktur so gestaltet, dass eine zentrale Überwachung als alleiniges Mittel ausreicht.



Hans-Joachim Diedrich



**Geschäftsführer Deutschland
F-Secure GmbH, München**

rt: Wie hoch schätzen Sie die Gefahr ein, dass sich die aus dem PC-Bereich bekannten Schädlinge auch auf intelligente Mobiltelefone verbreiten?

DIEDRICH: Es gibt auffallende Parallelen zwischen der historischen Entwicklung der Virenverbreitung auf PCs und der aufkommenden Verbreitung auf intelligenten Handy (Smartphones). F-Secure geht davon aus, dass es mittel- bis langfristig zu Infektionen auch auf Mobiltelefonen kommen wird. Im Moment ist das Risiko, dass das Handy von einem Virus befallen wird, jedoch äußerst gering – wenn auch nicht ausgeschlossen. ●

auf dem Firmen-Server illegale MP3-Files befinden. Er weiß um den Straftatbestand und informiert umgehend seine Geschäftsleitung. In Kenntnis des Paragraphen 106 des Urhebergesetzes („Unerlaubte Verwertung urheberrechtlich geschützter Werke“) beschließt die Geschäftsleitung, dem gesetzwidrigen Tun ein Ende zu bereiten und schaltet die Staatsanwaltschaft ein. Diese erkennt die Schwere der Tat und handelt im Rahmen ihrer gesetzlichen Verpflichtungen. Zunächst wendet sie Paragraph 94 der Strafprozessordnung („Sicherstellung von Beweisgegenständen“) an und beschlagnahmt den Beweisgegenstand – im Beispielfall der Server. Er verbleibt unter Verschluss bis zum Beginn der Verhandlung.

Da die Mühlen der Justiz bekanntlich langsam mahlen, wird das Unternehmen viele Monate auf den Server verzichten müssen. Das Beispiel macht deutlich, wo für das Management die echten Gefahren liegen. Nämlich weniger in den Straftatbeständen, sondern vielmehr in der praktischen Umsetzung.

Managementfehler Unterlizenzierung

Eine in der praktischen Auswirkung ähnliche Situation würde sich ergeben, wenn die Staatsanwaltschaft bei einem Unternehmen den Tatbestand der Unterlizenzierung feststellt. „Viele CIOs halten es für vom Risiko her vertretbar, wenn sie nur mit 80-prozentiger Lizenzierung der Unternehmens-Software arbeiten, um Lizenzkosten zu sparen“, warnt Reiners vor einem Trugschluss. Es ist auch kein Geheimnis, dass die Anzahl der berechtigt genutzten Lizenzen geringer ist als die Anzahl der tatsächlich genutzten Lizenzen.

Fliegt die Unterlizenzierung auf, ist die Staatsanwaltschaft nicht mehr wahlfrei. Sie muss handeln nach Paragraph 94 STPO, und das bedeutet konkret: Beschlagnahme des Servers. Die handelsrechtliche Haftung des Unternehmers wird darüber hinaus noch durch weitere Gesetze begründet. So schließt die Verpflichtung zur ordnungsgemäßen Unternehmensführung die Lizenzkonformität ein. Die Unterlizenzierung erfüllt nicht die Anforderungen an eine Unternehmensführung „mit der Sorgfalt eines ordentlichen Kaufmanns“. Die zivilrechtliche Haftung schließt bei Unterlizenzierung eine verschuldensunabhängige Mithaftung des Unternehmensinhabers ein (Paragraph 100 UrhG). Der Anspruch geht auf Unterlassung, Beseitigung und Schadensersatz.

Ein legitimes Mittel, bei den Lizenzkosten Geld zu sparen, ist der Erwerb gebrauchter Software-Lizenzen. Darauf wies Peter Schneider, Geschäftsführer der Usedsoft GmbH und Gastgeber des CIO-Kongresses hin: „Software-Lizenzen bleiben immer neu und ohne Abnutzung – wie am ersten Tag.“ Das Münchner Unternehmer handelt mit Software-Lizenzen, die zuvor mindestens einmal von Herstellern oder Händlern an Anwender verkauft worden sind, dort aber nicht mehr zum Einsatz kommen. Usedsoft zählt auch namhafte Handelsunternehmen zu seinen Kunden wie Dohle, Edeka Rhein-Ruhr, Markant oder Rewe. •

.....
Kontakt:
redaktion@ehi.org

EuroCIS

Internationale Fachmesse
Kommunikations-, Informations-
und Sicherheitstechnik im Handel

14. - 16. 2. 2006

Düsseldorf, Germany

www.eurocis.com

InfoTel: 0211/4560-176

Europas führende IT-Messe
für den Handel und seine Partner

- Mit umfangreichem Rahmenprogramm:
 - **NEU:** Global Retail Technology Forum
 - Innovationstag Handel
 - Exhibitor Forum in Halle 2

Kooperationspartner/
Co-operation partner:

EHI
Retail Network

Tel.: +49(0)221/5 79 93-23
www.ehi.org

Messe Düsseldorf GmbH
Postfach 10 10 06

40001 Düsseldorf
Germany
Tel. +49 (0)211/4560-01
Fax +49 (0)211/4560-668
www.messe-duesseldorf.de


Messe
Düsseldorf