



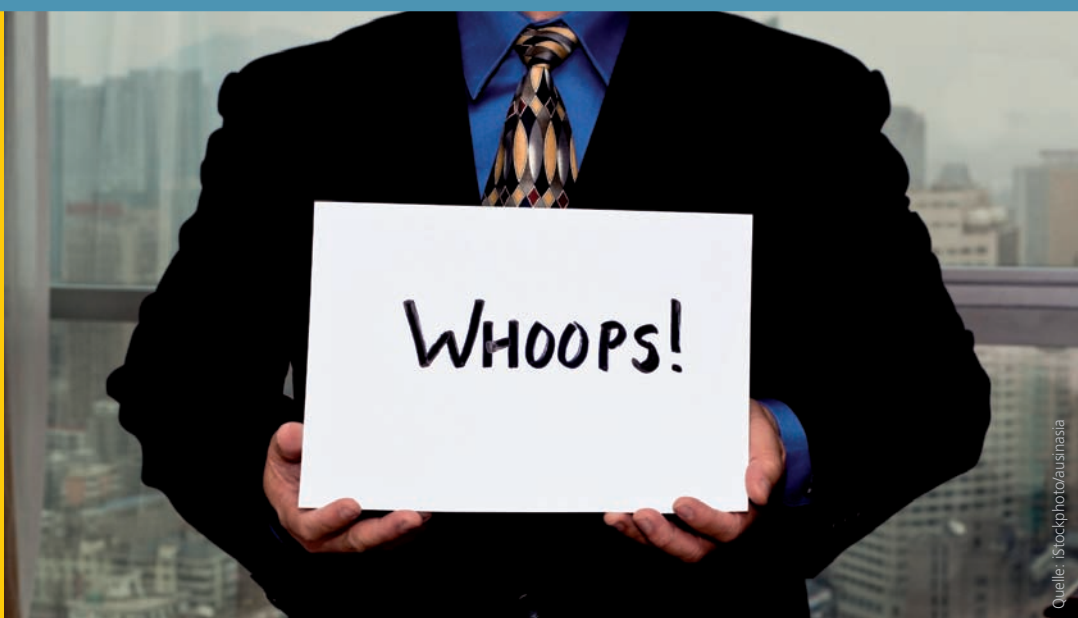
IT-Grundschutz

Informationsdienst

Workshops

Friendly Fire durch den Virens Scanner

Seite 3



Quelle: iStockphoto/ausinasia

NEWS

**„Mariposa“-Schöpfer
in Slowenien fest-
genommen** Seite 2

**Call for Papers
12. Deutscher IT-Sicher-
heitskongress** Seite 2

**Compliance-Officer
unter Zugzwang** Seite 2

Rubriken

Editorial Seite 2

Impressum Seite 15

IT und Recht

Haftungsfragen bei der Verbreitung von Schadsoftware Seite 11

Workshops

Friendly Fire durch den Virens Scanner Seite 3

Distributed Denial of Service-Angriffe nehmen zu Seite 8

Praxis und Anwendungen

Objektschutz für die Steuerberatungskanzlei Seite 14



Von Viren und anderen neuzeitlichen Krankheiten

Haftungsfragen bei der Verbreitung von Schadsoftware

Jan Schneider, Rechtsanwalt und Fachanwalt für Informationstechnologierecht

Die Bedrohung unternehmensinterner Computersysteme durch Viren, Trojaner und andere Schadprogramme ist allgegenwärtig. Häufig über E-Mail verbreitet, sorgen die kleinen, aber effektiven Programme beim Adressaten im besten Fall für Unmut, richten nicht selten aber einen handfesten Schaden im Unternehmen an. Ein Haftungsrisiko besteht auch für denjenigen, der unwissentlich bei der Verbreitung solcher Schadsoftware mitwirkt.

Die Verbreitung von Schadsoftware ist schon lange in einen bizarren Wettkampf ausgeartet: Jeden Tag gehen neue Varianten an den Start, während die Hersteller von Sicherheitssoftware mit neuen Abwehrsignaturen kontern. Neben dem klassischen Schadprogramm Computervirus sind auch Würmer und trojanische Pferde, kurz „Trojaner“ für schädliche Aktionen verantwortlich. Die Verbreitung von Viren und Würmern erfolgt häufig via E-Mail, entweder als Anhang oder selbstständig, indem sie ein vorhandenes Mailprogramm auf dem Computer mit den darin gespeicherten Adressen ausnutzen. Trojaner sind auch dafür bekannt, weitere schädliche Programme wie Backdoor-Software, unbemerkt vom Benutzer zu installieren. Es gibt zahlreiche Mischformen der drei vorgenannten Schadprogramme, weshalb die Begrifflichkeiten nicht völlig trennscharf sind. Gut abgrenzbar ist allerdings der Begriff des Phishing. Er fasst diverse Vorgehensweisen zusammen, deren Ziel sämtlich die Erlangung vertraulicher Daten, insbesondere Passwörter, PIN und TAN-Nummern oder Kreditkarteninformationen ist. Eine häufige Vorgehensweise ist die Fälschung von Webseiten, wie den Internet-Zugang einer Bank, um dort die Nutzer zur Eingabe der vertraulichen Daten zu bewegen. Die Hyperlinks zu den gefälschten Webseiten werden zumeist per E-Mail verschickt. Werden Nutzer dagegen durch die

Manipulation von DNS-Anfragen auf eine gefälschte Webseite umgeleitet, spricht man auch von Pharming. Allerdings können auch Würmer zum Ausspionieren von Passwörtern, Bankzugangsdaten und Ähnlichem eingesetzt werden, indem mithilfe eines sogenannten Keyloggers die Tastatureingaben aufgezeichnet und an den Versender des Wurms übermittelt werden.

Absichtliche Verbreitung von Schadsoftware

Dass die willentliche und gezielte Verbreitung von Schadsoftware und die Ausspähung vertraulicher Daten rechtliche Konsequenzen nach sich ziehen können, dürfte auf der Hand liegen. Die Herstellung von Schadsoftware ist, im Gegensatz zu anderen Ländern wie beispielsweise Großbritannien, unter deutschem Recht allerdings nicht strafbar. Erst wenn der Täter die selbst erstellte oder von einem Dritten beschaffte Schadsoftware absichtlich in Umlauf bringt, weiterleitet oder sonstwie verbreitet, liegt eine strafrechtlich relevante Handlung nahe. So kann sich eine Strafbarkeit beispielsweise aus § 303a StGB (Datenveränderung) bzw. § 303b StGB (Computersabotage) ergeben, wenn der schadhafte Code andere Dateien infiziert oder die Datenverarbeitung des Unternehmens nachteilig beeinflusst. Der Einsatz von Trojanern

und das Phishing können insbesondere ein strafbares Ausspähen von Daten nach § 202a StGB, einen Computerbetrug nach § 263a StGB oder auch einen herkömmlichen Betrug nach § 263 StGB (ggf. in Form einer gewerbs- oder bandenmäßigen Begehung) darstellen. Phishing ist ggf. auch nach § 269 StGB strafbar, weil beweiserhebliche Daten gefälscht werden.

Neben der strafrechtlichen Verfolgbarkeit bestehen in aller Regel zivilrechtliche Ansprüche des Geschädigten gegen den Täter und etwaige Mittäter, insbesondere auf Ersatz des entstandenen Schadens. Allerdings erfolgen Angriffe mit Schadsoftware häufig aus dem Ausland heraus, was eine strafrechtliche Verfolgung mitunter ebenso erschwert oder gar vereitelt, wie die Durchsetzung zivilrechtlicher Ansprüche. Der optimale Schutz gegen derartige Angriffe kann daher nur die Prävention sein. Dazu gehört der Einsatz aktueller Anti-Viren-Programme, Firewalls und anderer üblicher und wirkungsvoller technischer Maßnahmen.

Die absichtliche Infizierung eines EDV-Systems durch einen Mitarbeiter und sogar bereits der berechtigte Verdacht einer solchen Handlung rechtfertigt in der Regel die fristlose Kündigung des betreffenden Arbeitnehmers (LAG Saarbrücken, Urt. v. 1.12.1992, Az. 2 Sa 154/92). Auch die Androhung schadhafter Handlungen kann bereits Anlass zu einer rechtmäßigen Kündigung geben.

Haftung auch ohne Vorsatz möglich!

Deutlich vielschichtiger stellt sich die rechtliche Situation dar, soweit Schadsoftware unabsichtlich verbreitet wird. In aller Regel weiß der betreffende Mitarbeiter, Geschäftsführer, Selbstständige oder Freiberufler gar nicht, dass er zur Verbreitung der Schadsoftware beiträgt, zum Beispiel indem er eine Software aus dem Internet herunterlädt oder eine vermeintlich harmlose E-Mail an einen Geschäftspartner weiterleitet.

Auch aus derartigen Fällen kann jedoch eine Verantwortlichkeit resultieren. Wer ohne wirksame und aktuelle technische Schutzvorkehrungen sorglos Anhänge von E-Mails ihm unbekannter Adressaten öffnet oder derartige E-Mails weiterleitet und damit an der Verbreitung von Viren oder anderer Schadsoftware mitwirkt, handelt womöglich zumindest fahrlässig. Dies kann beispielsweise dann der Fall sein, wenn er aufgrund seiner Position als IT-Verantwortlicher oder aufgrund anderweitiger Sorgfaltspflichten mit dem Risiko eines Virenangriffs hätte rechnen und entsprechende Maßnahmen ergreifen müssen.

Auch eine etwaig zwischen den Parteien bestehende (vor-)vertragliche Beziehung verpflichtet den Versender einer E-Mail zu einer erhöhten Sorgfalt, die unter Umständen zu einer Verantwortlichkeit des Senders einer schadsoftwarebehafteten E-Mail führen kann (vgl. Landgericht Köln, Urte. v. 21.7.1999, Az. 20 S 5/99).

Mitverschulden und Zurechenbarkeit

Wer nach diesen Grundsätzen zumindest fahrlässig gehandelt hat, schuldet in der Regel den Ersatz eines etwaig entstandenen Schadens. Häufig wird man allerdings ein Mitverschulden des Empfängers annehmen müssen, wenn dieser nicht seinerseits wirksame und aktuelle Sicherheitsmaßnahmen ergriffen hat. Je nach konkreten Umständen des Einzelfalls wird der Mitverschuldensanteil regelmäßig im Bereich zwischen 25% und 50% liegen.

Auch das Unterlassen der gebotenen Datensicherung führt mindestens zu einem Mitverschulden des geschädigten Unternehmens (LG Köln, Urte. v. 21.7.1999), unter Umständen gar zu einer vollständigen Verneinung der Schuld des Schädigers. Das Gleiche kann gelten, wenn der Geschäftspartner seine handelsrechtlichen Untersuchungs- und Rügepflichten vernachlässigt, also beispielsweise vom Lieferanten erhaltene und für den Weitervertrieb bestimmte Datenträger nicht zumindest stichprobenartig mittels üblicher Methoden auf Virenfreiheit untersucht (LG Kleve, Urte. v. 18.5.1995, Az. 7 O 17/95).

Die Schadenverursachende Handlung eines Angestellten kann unter dem Aspekt des sogenannten Organisationsverschuldens auch dem Arbeitgeber zuzurechnen sein. Denn dieser ist zu einer sorgfältigen Auswahl seiner Angestellten und zu deren ausreichender Schulung und Instruktion im Umgang mit Internetrisiken verpflichtet. Des Weiteren muss er ausreichende technische Maßnahmen zur Sicherung der unternehmensinternen EDV-Systeme treffen. Das beinhaltet wiederum den Einsatz einer wirksamen Firewall und aktueller - und aktuell zu haltender! - Anti-Viren-Software. Weitergehende Anforderungen an die innerorganisatorische IT-Sicherheit ergeben sich beispielsweise aus dem KonTraG und dem Bundesdatenschutzgesetz. Die nicht ausreichende Beachtung dieser Anforderungen kann zu einer Verantwortlichkeit des Unternehmens oder gar zu einer persönlichen Haftung der Unternehmensleitung führen.

Besondere Haftungsrisiken für IT/TK-Dienstleister und -Anbieter

Erhebliche Bedeutung hat die Haftungsthematik für die gewerblichen Anbieter von IT-Produkten und -Dienstleistungen sowie für TK-Provider. Denn zum einen besteht je nach Art der konkreten Tätigkeit gegebenenfalls eine gesteigerte Gefahr der fahrlässigen Schädigung von Kunden bzw. Geschäftspartnern. Zum Anderen stellt die Rechtsprechung an IT-Fachunternehmen hinsichtlich der Sorgfaltspflichten erhöhte Anforderungen.

Wer eine Software gewerblich vertreibt, die ohne sein Wissen schadhafte Code enthält, haftet den Erwerbern gegenüber bereits im Rahmen der gesetzlichen Mängelhaftung, weil sich der schadhafte Code innerhalb der Software als Sachmangel derselben darstellt. Dabei ist für das Vorliegen eines Mangels unerheblich, ob und welches

4. Forum
E-Discovery 2010

EDV-gestützte Verfahrenstechniken
in Europa – Elektronische
Beweismittelbeschaffung und der
Beschäftigtendatenschutz – Records
Management & E-Mail Retention

13. – 15. September 2010
Dorint Hotel Sanssouci
Berlin-Potsdam

Besuchen Sie unser Download Center
für kostenfreie Whitepaper, Artikel
und vieles mehr!
www.ediscovery-konferenz.de/it



Jan Schneider, Fachanwalt für IT-Recht und Partner des Düsseldorfer Büros der Sozietät SKW Schwarz Rechtsanwälte, beschäftigt sich seit rund 10 Jahren mit rechtlichen Fragestellungen der Informationstechnologie.

Schädigungspotenzial der Schadcode hat, womit auch Scherz- und Demoviren erfasst werden. Neben möglichen Schadensersatzansprüchen des Erwerbers ist der Lieferant zur Behebung des Mangels, das heißt in der Regel zur Lieferung einer virenfreien Software, verpflichtet. Diese Mangelbehebungspflicht gilt unabhängig davon, ob er schuldhaft gehandelt hat oder nicht. Schlägt die Mangelbehebung fehl, ist der Erwerber zur Minderung der Lizenzgebühr oder zum Rücktritt vom Erwerb berechtigt. Der Hersteller der Software haftet zudem, ebenfalls verschuldensunabhängig, nach den Grundsätzen der Produkthaftung.

Erleidet ein Kunde aufgrund eines Fehlverhaltens des IT-Dienstleisters einen Datenverlust, so handelt es sich nach Auffassung des Bundesgerichtshofs (Urt. v. 02.07.1996, Az. X ZR 64/96) um einen so genannten entfernten Mangelfolgeschaden. Das hat die Konsequenz, dass die Ansprüche des Geschädigten der 30-jährigen Verjährungsfrist unterliegen. Aufgrund des erhöhten Haftungsrisikos ist für IT-Dienstleister und -Anbieter die Etablierung und Verwendung der bekannten technischen Schutzmaßnahmen absolut unverzichtbar. Je nach konkretem Tätigkeitsfeld wird gegebenenfalls ein deutlich kürzerer als nur wöchentlicher Aktualisierungszyklus der Anti-Viren-Dateien erforderlich sein. Soweit ein IT-Dienstleister im Unternehmen des

Kunden vor Ort tätig ist, kann der aktive Einsatz von Schutzsoftware erforderlich sein.

TK-Provider müssen selbstverständlich ihre Systeme gegen Hackerangriffe, Viren und Ähnliches wirksam schützen. Für schadsoftwarebehaftete E-Mails, die sie lediglich vom Versender zum Adressaten weiterleiten, sind sie allerdings nach den Grundsätzen des Telemediengesetzes in der Regel nicht, jedenfalls erheblich eingeschränkt verantwortlich.

Die Beschränkung der Haftung für durch Schadsoftware entstandene Schäden ist in allgemeinen Geschäftsbedingungen nur sehr eingeschränkt erlaubt. Viele der hierzu in Providerverträgen oder in den AGB von IT-Dienstleistern häufig anzutreffenden Klauseln sind unzulässig und können den Dienstleister oder Provider vor der Verantwortung für von ihm verursachte Schäden nicht bewahren.

Auch das vollständige Abbedingen der handelsrechtlichen Untersuchungs- und Rügepflichten in standardisierten Einkaufsbedingungen ist nach höchstrichterlicher Rechtsprechung unzulässig.

Gefahrenbereich Online-Banking

In kaum einem Bereich werden softwarebasierte Schadtechniken derart kriminell und zielgerichtet eingesetzt, wie im Online-Banking. Täglich kommen zahllose neue Varianten von Phishing-E-Mails in Umlauf, entstehen zahllose neue Phishing-Webseiten, mithilfe derer die Täter Zugangsdaten der Bankkunden auspähen und hiernach deren Konten plündern. Der Schaden liegt Schätzungen zufolge weltweit im Milliardenbereich.

Die aktuelle Rechtsprechung tendiert überwiegend dazu, das Risiko für die Fälschung von Online-Überweisungsaufträgen und den hierdurch entstehenden Schaden grundsätzlich der kontoführenden Bank aufzuerlegen, soweit dem Bankkunden kein Mitverschulden vorgeworfen werden

kann. So war das Landgericht Berlin im letzten Jahr der Auffassung, dass die Bank 90% des dem Kunden entstandenen Schadens zu tragen hat (LG Berlin, Urt. v. 11.8.2009, Az. 37 O 4/09). Die Entscheidung ist allerdings noch nicht rechtskräftig, die Parteien streiten in zweiter Instanz. Das LG Köln hat dem Bankkunden darüber hinaus einen Anspruch gegen einen „Geldkurier“ zuerkannt, der einen, aufgrund einer Phishing-Attacke bei ihm eingegangenen Geldbetrag, ohne vollständige Kenntnis der Umstände leichtfertig an den Täter weitergeleitet hatte (Urt. v. 5.12.2007, Az. 9 S 195/07. Dieser hatte sich nach Auffassung des Gerichts der so genannten leichtfertigen Geldwäsche nach § 261 Abs. 2, 5 StGB strafbar gemacht.

Was ein mögliches Mitverschulden des Online-Bankkunden betrifft, so begründet der bloße Umstand, dass von den Tätern zutreffende Legitimationsdaten verwendet wurden, keinen Anschein für eine Sorgfaltspflichtverletzung des Bankkunden (LG Mannheim, Urt. v. 16.5.2008, Az. 1 S 189/07). Die Bank wird in der Regel auch keine allzu hohen Anforderungen an die Sorgfaltspflichten ihres Online-Bankkunden stellen dürfen, der für eine Nutzung seines PCs in aller Regel ja keine ernst zunehmenden Fachkenntnisse besitzen muss (vgl. AG Wiesloch, Urt. v. 20.6.2008, Az. 4 C 57/08).

Allerdings muss der Kunde Warnungen der Bank und deutlich erkennbare Hinweise auf gefälschte E-Mails beachten. Derartige Hinweise können sich beispielsweise aus sprachlichen Auffälligkeiten ergeben, aus offensichtlich falschen Internet-Adressen und - so das LG Köln - sogar aus dem Fehlen des „https://“-Protokolls bzw. des Schlüsselsymbols in der Statusleiste. Was ebenfalls vom Bankkunden erwartet werden darf, ist wiederum der Einsatz einer marktüblichen und regelmäßig aktualisierten Sicherheitssoftware (LG Köln, Urt. v. 5.12.2007). Hierauf muss die Bank nicht ausdrücklich hinweisen (LG Nürnberg-Fürth, Urt. v. 28.4.2008, Az. 10 O 11391/07).■