Security Journal GAI Netconsult, 4/2004

Ulrich Emmert

Brandbekämpfung im Netz

Das Hauptproblem der EDV-Sicherheit ist oft die unerkannte Gefahr eines Internet-Angriffs. Die wenigsten der sicherheitsrelevanten Vorfälle wird überhaupt entdeckt (nach einer FBI-Studie ca. 1 %). Davon wiederum werden nur ca. 1% der Fälle veröffentlicht, da meist größere Imageschäden befürchtet werden.
Die technischen Gefahren werden anhand der wenigen veröffentlichten Fälle als zu vernachlässigend abgetan, während die rechtlichen Gefahren häufig komplett ignoriert werden.
Wenn es im Netzwerk “brennt”, kommt die Feuerwehr schon zu spät – um so wichtiger ist es, dass die “Brandschutzmauern” korrekt aufgebaut und die “Brandschutzvorschriften” beachtet werden. Im Internet wird häufig noch das “Floriansprinzip” angewendet: “Oh heiliger St. Florian, verschon mein Netz, zünd´ andere an”.

Nur wenig bekannt ist, dass es überhaupt rechtliche Verpflichtungen gibt, Firewalls aufzubauen und regelmäßig zu warten. Am 1.7.2004 sind diesbezüglich einige Änderungen in Kraft getreten, die aber in der Öffentlichkeit kaum wahrgenommen wurden. Es gibt kein einziges Gesetz, das sich direkt mit Internet-Sicherheit beschäftigt, sondern es gibt völlig verstreut in der Rechtsordnung Ansatzpunkte, die auf die zwingende Verwendung von Security Software wie Antivirus-Software, Firewall- und Intrusion Detection Software hindeuten.
Deshalb gibt es weder einheitliche Anwendungsbereiche noch einheitliche Sicherheitsvorschriften für die verschiedenen nachfolgend besprochenen Rechtsgrundlagen.

Vorschriften für Kapitalgesellschaften (AG, GmbH)

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet alle Kapitalgesellschaften mit Ausnahme der kleinen

Kapitalgesellschaften (§ 267 Abs. 1 HGB) zur Aufstellung eines Lageberichts nach § 264 des Handelsgesetzbuches (HGB).
In § 289 HGB neuer Fassung wird nunmehr auch verlangt, dass die Risiken zukünftiger Entwicklungen detailliert beschrieben werden.

Die Risiken dieser Entwicklungen erstrecken sich in zunehmendem Maße auch auf die IT-Sicherheit. In einem Unternehmen, welches über keinerlei Backup-System verfügt, gibt es wahrscheinlich mit Ausnahme eines Gebäudebrandes keinen größeren Schaden als bei einem Headcrash der Serverfestplatte. Im Internet-Zeitalter muß der Totalverlust der Daten aber nicht immer auf Hardwarefehler zurückzuführen sein, sondern kann auch durch Liebesbriefe oder einen Melissa-Geist ausgelöst werden. Im schlimmsten Fall transportieren Trojanische Pferde unbemerkt die Daten aus dem Unternehmen hinaus.
Wesentliche Gefahren des Unternehmens sind nicht korrekt bewertet, wenn nur Marktanalysen oder Konjunkturprognosen als Grundlage einer Risikovorschau herangezogen werden.
Eine zutreffende Risikoanalyse im Bereich IT-Sicherheit kann im Gegensatz zu anderen Bereichen auch nicht durch eine bloße Fortschreibung vergangener Risikobewertungen erfolgen.
Durch das Bekanntwerden immer neuer Sicherheitslöcher können sich die Aussagen einer solchen Risikobewertung als extrem irreführend herausstellen. Das HGB verlangt jedoch einen Lagebericht, der zum Zeitpunkt der Abgabe nach bestem Wissen und Gewissen eine richtige Aussage trifft. Durch die Pflicht zur gewissenhaften Erstellung der Buchführung aus § 240 HGB und der Überprüfung durch den Abschlussprüfer nach § 317 Abs. 2 Satz 2 HGB ist es hier für den Geschäftsführer der GmbH bzw. Vorstand und Aufsichtsrat der AG nicht möglich, sich aus der Verantwortung zu stehlen.
Eine bewusste oder fahrlässig falsche Bewertung in einem Lagebericht kann auch zu persönlicher Haftung der Verantwortlichen nach § 823 ff. des Bürgerlichen Gesetzbuches (BGB) führen.

Vorschriften für Behörden und Freiberufler

Im Bereich der freien Berufe sowie des öffentlichen Dienstes sind zudem die Vorschriften des § 203 des Strafgesetzbuchs (StGB) ernst zu nehmen, um der dort angedrohten Strafe - bis zu einem Jahr Freiheitsstrafe - zu entgehen. Die Angehörigen der dort in Absatz 1 genannten Berufe müssen die Geheimnisse, welche ihnen in Ausübung ihres Berufes mitgeteilt wurden, bewahren. Dazu gehört natürlich auch, dass die Geheimnisse aus dem Internet nicht erreichbar sein dürfen. Auch ist es nicht erlaubt, ohne Einverständnis der Kunden Daten unverschlüsselt über das Internet zu übertragen.
Wenn allerdings die Kunden, zu deren Schutz das Berufsgeheimnis besteht, unverschlüsselt Fragen über das Internet stellen, ist der Berufsträger aus dem Gesichtspunkt des mutmaßlichen Einverständnisses berechtigt, die Antwort ebenfalls unverschlüsselt zu übertragen.
In der Regel werden auch die eMails der Kunden mehr tatsächliche Angaben enthalten als die Antwort des Berufsträgers der freien Berufe.
Entsprechendes gilt nach § 203 Absatz 2 StGB für das Amtsgeheimnis im öffentlichen Dienst.

Vorschriften für alle Unternehmen

Ohne besonderen Schutz der Daten gibt es auch keine Möglichkeit, einen Datenspion überhaupt zu verfolgen. In § 202a StGB werden nur gegen Einsichtnahme besonders gesicherte Daten dem Schutz des Strafrechts unterstellt.
Mangels strafrechtlichem Schutz ist in der Regel jedoch keine Verfolgung möglich,
weil es den Providern aus datenschutzrechtlichen Gründen nicht möglich ist, die zur Enttarnung des Hackers notwendigen Angaben zu liefern.

Betriebsgeheimnisse – Haftungsverteilung intern

Schließlich ist der Systemadministrator auch gegenüber seinem Arbeitgeber verpflichtet, gemäß der Aufgabenstellung im Arbeitsvertrag die Daten des Unternehmens vor dem Zugriff von außen bestmöglich zu schützen. Der Systemadministrator könnte bei fehlenden Sicherheitsvorschriften auch wegen Verletzung von Betriebsgeheimnissen durch Unterlassen nach § 17 des neuen

Gesetzes gegen unlauteren Wettbewerb (UWG) vom 3.7.2004 Ärger mit dem Staatsanwalt bekommen.

Wenn der Systemadministrator die notwendigen Maßnahmen von der Geschäftsleitung nicht genehmigt bekommt, könnten Gesellschafter auch diese zur Verantwortung ziehen. Arbeitsrechtlich gehört eine Sicherheitsüberprüfung zu seinen wichtigsten Aufgaben, die er gewissenhaft zu erfüllen hat. Macht der Systemadministrator aufgrund leichter Fahrlässigkeit

Fehler bei der Konfiguration, so kann der Arbeitgeber jedoch nicht den Schaden seinem Angestellten aufbürden. Der Arbeitsbereich des Systemadministrators ist extrem gefährlich, was die mögliche Haftung betrifft. Danach ist es dem Arbeitgeber, der seinen Angestellten mit einem riskanten Job betraut, nicht möglich, ihn wegen leichter Fahrlässigkeit in die Haftung zu nehmen oder bei mittlerer Fahrlässigkeit mehr als die Hälfte im Wege des Regresses einzufordern.

I

Datenschutz

Geheimschutz- und Organisationsregelungen, die alle Unternehmen betreffen, enthalten die Datenschutzgesetze.

Kaum jemand kennt die umfangreichen Vorgaben für alle Unternehmensnetzwerke, die sich aus § 9 des Bundesdatenschutzgesetzes sowie dem zugehörigen Anhang ergeben. Dort werden gezielt einzelne Maßnahmen gefordert, die den unbefugten Zugriff auf personenbezogene Daten verhindern sollen. Dies gilt aber nicht nur für den Zugriff von außen, sondern es wird hier auch explizit der innerbetriebliche und innerbehördliche Datenschutz angesprochen. Die Schutzmaßnahmen müssen natürlich der Unternehmensgröße und der Schutzwürdigkeit der Daten angemessen sein, weshalb größere Unternehmen wesentlich mehr Sicherheitsmaßnahmen ergreifen müssen als 2- oder 3-Mann-Betriebe.

Dort werden konkrete Sicherheitsmaßnahmen gefordert, wie z.B. die Zutrittskontrolle nicht nur zu Serverräumen, sondern auch zu allen Räumen, in denen Clients stehen, an denen personenbezogene Daten genutzt werden, die Zugangskontrolle zu den Daten gegen unberechtigte Nutzung, die Kontrolle der Zugriffsberechtigungen und der abgespeicherten Daten, der Schutz der Daten bei Transport und Weitergabe, die eindeutige Authentifizierung desjenigen der personenbezogene Daten in PCs eingibt usw. Es darf also nicht reichen, einen blauen Mantel anzuziehen und einen

Putzeimer in die Hand zu nehmen, um Zutritt zu den Räumen zu bekommen oder telefonisch ein neues Passwort zu erfragen.
Wer die Einhaltung dieser Regelungen organisatorisch nicht im Griff hat, riskiert einiges: Erstens gibt es Schadensersatzregelungen ohne Betragsobergrenze, die auch noch mit einer Beweislastumkehr versehen sind, d.h. wenn Daten das Unternehmen unbefugt verlassen, wird das Verschulden des Unternehmens erst einmal vermutet und es muss sich erst selbst entlasten, was die Vorschrift extrem gefährlich macht.
Zweitens gibt es hier eine Strafvorschrift – § 43 des Bundesdatenschutzgesetzes – mit einer Bußgelddrohung von bis zu 250.000 Euro, bei Bereicherungs- oder Schädigungsabsicht sogar Freiheitsstrafe bis zu zwei Jahren. Das sollte beides Anlass dazu geben, die übliche Einstufung von Datenschutzvergehen als Kavaliersdelikte gründlich zu überdenken.
Im Internet sind besonders die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) sowie der §§ 91 des neuen Telekommunikationsgesetzes vom 1.7.2004 (TKG) zu beachten, welche die Übermittlung von personenbezogenen Daten an Dritte untersagen, sofern diese nicht zur Abrechnung der übertragenen Daten eingeschaltet werden. Daraus ergibt sich, dass bei Anschluss des eigenen Netzwerkes an das Internet dafür Sorge getragen werden muss, dass die Daten vor dem Zugriff aus dem Internet besonders gesichert sind.

Notwendigkeit von ergänzenden organisatorischen Maßnahmen

Oft wird eine Firewall als Black Box betrachtet, die bereits alle Sicherheitsanforderungen erfüllt. Die Firewall sollte jedoch nur Teil eines umfassenden technischen und rechtlich-organisatorischen Sicherheitskonzeptes sein.

Angriffsrichtung von innen

Nicht immer greift der “Brand” von außen auf das eigene Unternehmen über. Die meisten Angriffe im Unternehmensnetzwerk erfolgen von innen durch eigene Mitarbeiter. Ebenso wie in den Landesbauordnungen müssen “Brandschutzmauern” auch innerhalb des Unternehmens in Betracht gezogen werden, nicht nur an der

Grenze zum Nachbarn, vor allem dann, wenn unterschiedliche Sicherheitsbedürfnisse im Unternehmen bestehen.
Wichtig sind daneben auch organisatorische Maßnahmen, damit z.B. die eigenen Mitarbeiter nicht “Brandschutztüren” offen stehen lassen, indem sie sich mit Modems um die Firewall herum ins Internet verbinden oder “selbstentzündliches Material” (Trojaner) mit ins Unternehmen bringen.

Haftung nach außen durch Angriffe eigener Mitarbeiter

Ein weiterer Aspekt ist die Aufgabe des Unternehmens, den Mitarbeitern die “Zündhölzer” wegzunehmen, mit denen sie über das Internet andere Unternehmen “anzünden” können. Wenn dies nicht vollständig gelingt und sich die Mitarbeiter z.B. im Supermarkt neue “Zündhölzer” beschaffen, ist darauf zu achten, dass die “Streichholzschachtel”, die am Tatort gefunden wird, wenigstens nicht den Schriftzug des eigenen Unternehmens trägt. Mit anderen Worten sollten die rechtlichen Haftungsbedingungen so ausgestaltet sein, dass das Unternehmen nicht für das Fehlverhalten der Mitarbeiter herangezogen werden kann und damit das Image der Firma beeinträchtigt wird.

Haftung durch Kenntnis von illegalen Inhalten

Seit 21.12.2001 sind die Haftungsrisiken für Unternehmen erheblich gestiegen, weil den Unternehmen nach dem Elektronischen Geschäftsverkehrsgesetz inzwischen bei der Speicherung von illegalen Inhalten auf eigenen Rechnern nicht mehr nur die Kenntnis der zuständigen Mitarbeiter, sondern aller Mitarbeiter zugerechnet wird, für die sie Informationen speichern.

Fazit

“Feuerlöscher” werden aller Erfahrung nach nur dann angeschafft, wenn dies entweder Vorschrift ist oder die Versicherung damit droht, ansonsten nicht zu zahlen. Es gibt zwar keine direkte Vorschrift zur Installation von Security Software, aber ohne diese Software sind die zahlreichen genannten Vorschriften nur dann zu erfüllen, wenn das eigene Unternehmen nicht an das Internet angeschlossen ist.

“Feuerlöscher” bringen aber nur dann etwas, wenn jeder weiß, wie man sie bedient und deren Funktion regelmäßig kontrolliert wird. Auf das Internet übertragen heißt das: Nur mit einem technischen und rechtlich-organisatorischen Sicherheitskonzept kann man die Gefahren von innen und außen in den Griff bekommen, insbesondere nach der Haftungserweiterung durch das Elektronische Geschäftsverkehrsgesetz und den seit 1.1.2002 erheblich erweiterten Gewährleistungsfristen nach der Schuldrechtsreform.

Zu einem qualifizierten Sicherheitskonzept gehört auch die Verpflichtung (Nutzungsbedingungen/Ergänzung Arbeitsvertrag) und Ausbildung der Mitarbeiter in diesem Bereich sowie die regelmäßige Funktionskontrolle (Firewall-Check).

Unsere Kanzlei bietet sowohl Risk Management Schulungen als auch Workshops zur Erstellung von Security Konzepten (in Anlehnung an das BSI Grundschutzhandbuch und den ISO 17799 Standard aber im rechtlichen Bereich weit darüber hinaus) an.

Kontakt

ulrich.emmert@kanzlei.de
www.kanzlei.de