UNIVERSITÄTSLEHRGANG
FÜR INFORMATIONSRECHT UND RECHTSINFORMATION
AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

Einbruch im Webshop

Verantwortlichkeit und Risikotragung

MASTERTHESIS

zur Erlangung des akademischen Grades

Master of Advanced Studies (MAS)

Begutachter:

DI DrDr Walter J Jaburek

Mag Ralf Blaha

im September 2001

Inhaltsverzeichnis

1 EINLEITUNG 4

1.1 Sachverhalt, Ziel dieser Arbeit 7

2 DER WEBSHOP 8

3 EINBRUCH IM WEBSHOP 10

3.1 Die Sicherheitslücke 10

3.1.1 Falsche Konfiguration 10

3.1.2 Systemfehler 11

3.1.3 Ungenügende Schulung 12

3.2 Der Angreifer 13

3.2.1 Hacker (im engeren Sinn) 13

3.2.2 Cracker 13

3.2.3 Krimineller Einzeltäter 13

3.2.4 Insider 14

3.2.5 Wirtschaftsspionage 14

3.2.6 Organisierte Kriminalität 14

3.3 Der Angriff 15

3.3.1 Ausspionieren der Zugangsdaten 15

3.3.2 Ausnutzen von Systemfehlern 17

3.3.3 Vorgehensweise nach erlangtem Zugang 18

3.4 Denial of Service (DoS) 20

3.5 Viren 21

3.6 Würmer 22

3.7 Konsequenzen 23

3.7.1 Verlust der Vertraulichkeit 23

3.7.2 Verlust der Verfügbarkeit 24

3.7.3 Verlust der Integrität 24

3.7.4 Fazit 24

4 ZIVILRECHTLICHE KONSEQUENZEN 25

4.1 Anspruch des geschädigten Unternehmens gegenüber dem Angreifer.... 25

4.1.1 Anspruchsgrundlage 25

4.1.2 Rechtsdurchsetzung 26

4.1.3 Abteilungen für Computerkriminalität bei Sicherheitsbehörden 27

4.2 Anspruch des geschädigten Unternehmens gegenüber dem Provider 28

4.2.1 Vertragstypus 28

4.2.2 Gewährleistung 29

4.2.3 Schadenersatz 32

4.2.4 Verschulden 36

4.2.5 Umfang der Ersatzpflicht 38

4.3 Webhostingverträge in der Praxis 39

4.3.1 Vertragstypus/Hauptleistungspflichten 39

4.3.2 Wahrung von Integrität und Verfügbarkeit (Safety) 40

4.3.3 Wahrung der Vertraulichkeit (Security) 41

5 GEGENMAßNAHMEN 44

5.1 Organisatorische Maßnahmen 44

5.1.1 IT-Sicherheitskonzept 44

5.1.2 IT-Sicherheit im laufenden Betrieb 45

5.1.3 IT-Sicherheitsbewusstsein 46

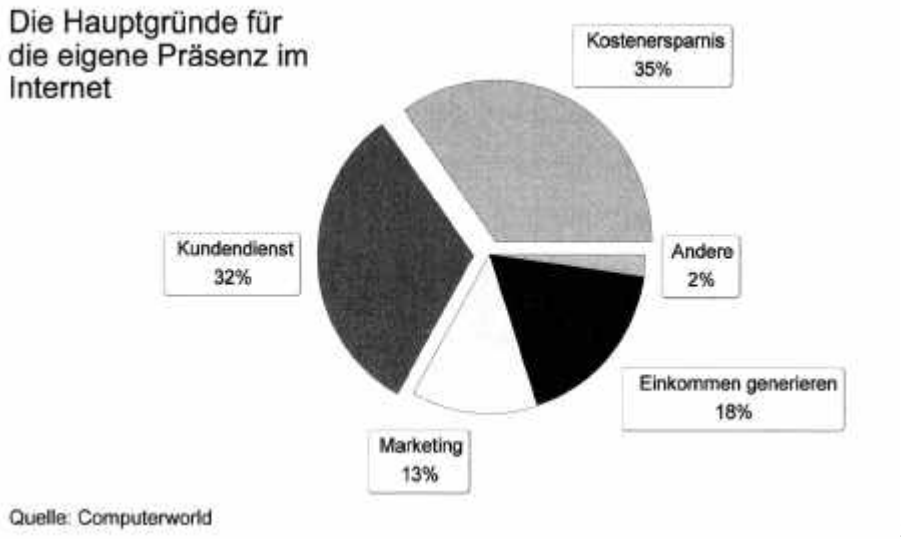
5.2 Technische Maßnahmen 47

6 CONCLUSIO 48

7 LITERATURVERZEICHNIS 49

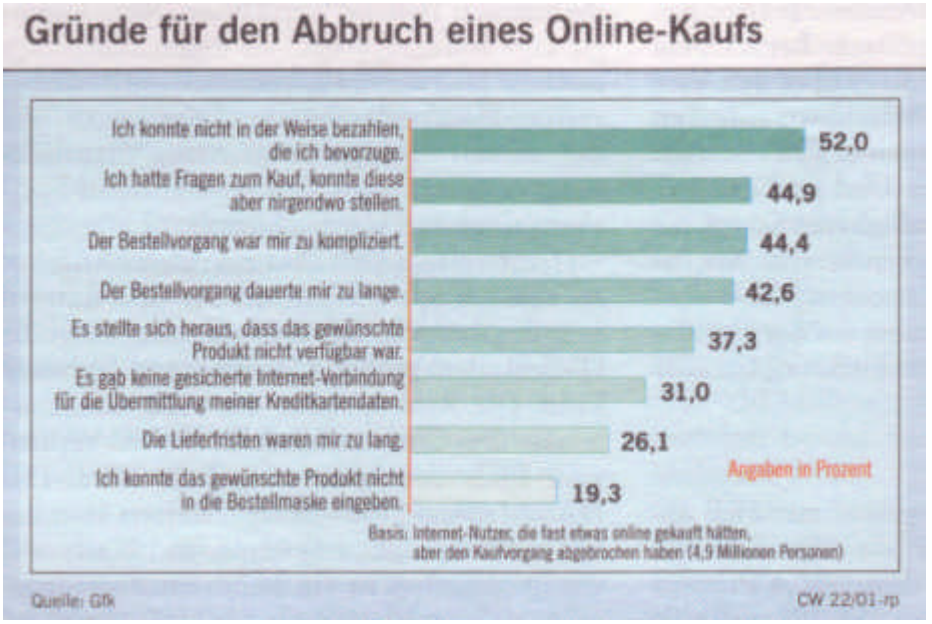
1 Einleitung

Der elektronische Handel bietet der Wirtschaft ungeahnte Chancen, die von dieser trotz der derzeit vorherrschenden Katerstimmung auch wahrgenommen werden. Mittlerweile glaubt kaum jemand, es sich leisten zu können, nicht im World Wide Web präsent zu sein.



1

Doch der Absatz im Internet wächst trotz des großen Angebotes nicht so stark, wie er könnte. Das hat verschiedene Ursachen, angefangen von der oft umständlichen Bedienung bis zu den Zahlungsmodalitäten.



Eine Ursache liegt in den Sicherheitsrisiken, die regelmäßig durch spektakuläre Fälle in das Bewusstsein der Öffentlichkeit treten, aber nicht wirklich fassbar sind und sowohl den potentiellen Kunden als auch den Unternehmer verunsichern. Laut einer Studie von Gartner machen sich 86% von 7000 befragten Amerikanern große Sorgen über die Sicherheit ihrer Daten im Netz.[2] Auslöser dafür sind einerseits die Flut der Computerviren, andererseits spektakuläre Einbrüche in Server. Das sind zwar verschiedene Sicherheitsprobleme, die meisten Surfer haben aber Schwierigkeiten, zwischen Virenproblematik und Datendiebstahl zu unterscheiden.

Nach den Erkenntnissen der Gartner-Studie ist den Menschen der Schutz ihrer Kreditkartendaten und der Zugangsdaten für das Onlinebanking am wichtigsten. Danach folgt das Bedürfnis, die eigene Adresse oder Telephonnummer vor Fremden geheim zu halten. Am wenigsten berührt die Menschen ihr Online-Profil und e-Mail-Adresse.

Die Folge dieser Angst ist, dass nur rund die Hälfte aller surfenden Amerikaner derzeit das Web nützt, um finanzielle Transaktionen zu tätigen.

Spektakuläre Fälle von Computerkriminalität, die einem das Einkaufen über das Internet verleiden, gibt es genug[3]

- Ende 1999 stahl ein Hacker[4] mehr als 485000 Kreditkartendatensätze von einer E-Commerce-Website und hat diese dann heimlich auf der Website einer US-Bundesbehörde gespeichert.
- Im Jänner 2000 veröffentlichte ein Hacker mit dem Deckname Maxim 25000 erbeutete Kreditkartendaten im Internet.

---

[1] Aus: *Krause*, Electronic Commerce, Berlin 1998, S. 21

[2] Computerwoche 33/2001 S. 7

[3] Beispiele aus: *Power*: Attacken im Web, München 2001, S. 118ff

[4] Ich bin mir bewusst, dass Computerfreaks diese pauschale Verwendung des Begriffes „Hackers“ nicht billigen, verwende in meiner Arbeit diesen Begriff jedoch als pars pro toto für jemanden, der die Sicherheit eines Systemes kompromittiert, da sich in den Medien „Hacker“ als Bezeichnung dafür eingebürgert hat.

- 1997 hackte sich Carlos Salgado (Deckname SMAK) unter Ausnützung bekannter Systemmängel in mehrere Internetfirmen, stahl Tausende Kreditkartendaten und versuchte, diese zu verkaufen. Er knackte insgesamt 86326 Kreditkartenkonten von 1214 verschiedenen Finanzinstitutionen.
- 1994 erleichterte der russische Hacker Vladimir Levin – möglicherweise mit Hilfe eines weiteren Hackers - die Citibank um zehn Mio US-$, indem er sich die fehlenden Sicherheitsvorkehrungen des öffentlichen Telephonnetzes zunutze machte, über das die Kunden ihre Daten unverschlüsselt übertrugen.
- 1994 übernahmen eine Bande von Hackern, die sich „Phonemasters" nannten, die Kontrolle über eine Reihe von Telephonnetzen (zB AT&T Corp, British Telecommunications Inc, MCI World Com und Southwestern Bell) und drangen ua in die Datenbanken von Nexis/Lexis ein. Sie richteten durch umfangreiche Betrügereien einen geschätzten wirtschaftlichen Schaden von 1,85 Mio US-$ an.

Dazu kommt noch, daß kaum ein Unternehmen freiwillig zugibt, Opfer einer Hackerattacke geworden zu sein, da der Vertrauensverlust katastrophale Folgen haben kann, besonders für Unternehmen, für die das Vertrauen der Kunden lebenswichtig ist, wie zum Beispiel Banken und Versicherungen.

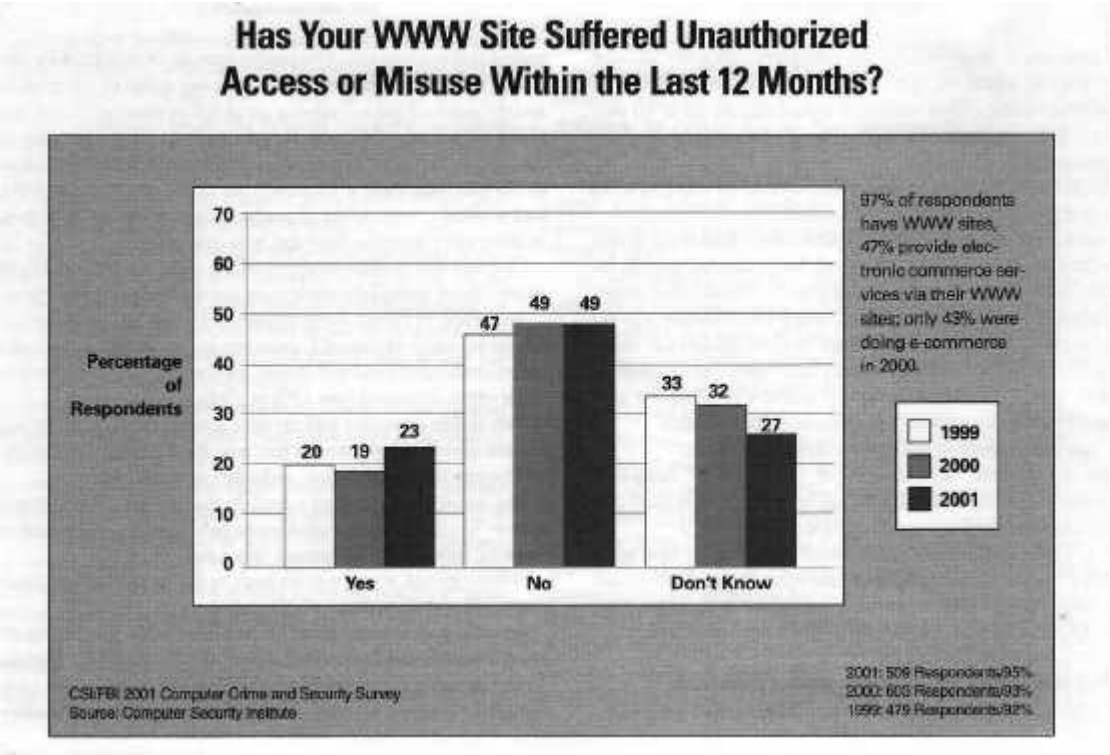
Die Computerkriminalität wächst mit dem e-Commerce und muss daher auch in die wirtschaftlichen Überlegungen miteinbezogen werden.

Ein paar Beispiele aus dem „2001 Computer Crime and Security Survey"[5], welches vom Computer Security Institute (CSI) gemeinsam mit dem FBI erstellt wurde (Diese Studie wurde in den USA mit Behörden und großen Unternehmen erstellt, ist aber aufgrund der Tatsache, dass das Internet nicht durch Staatsgrenzen beschränkt wird, auch für europäische Verhältnisse relevant)

---

[5] Computer Security Institute: 2001 CSI/FBI Computer Crime and Security Survey

- 85% der befragten Sicherheitsmanager haben in den letzten zwölf Monaten Komprimittierungen ihrer Computersicherheit festgestellt.
- 64% haben durch solche Kompromittierungen finanzielle Einbussen erlitten. Der Großteil dieser Verluste wurde durch den Verlust von proprietären Daten und Betrug verursacht.
- 70% geben ihre Schnittstelle zum Internet als regelmäßigen Eintrittspunkt für solche Kompromittierungen an (im Gegensatz zum internen Netzwerk)



Mit diesen – durch solche Untersuchungen bestätigten - Sorgen geht eine enorme Rechtsunsicherheit einher.

Nur wenn die Beteiligten die Risiken kennen, können sie sie mit einkalkulieren, und nur so kann sich Vertrauen entwickeln, welches die Grundlage jedes Wirtschaftens ist.

1.1 Sachverhalt, Ziel dieser Arbeit

Stellen Sie sich vor, Sie sind Geschäftsführer eines österreichischen Unternehmens, das Autoteile vertreibt. Sie haben beschlossen, auch das Internet als Vertriebskanal zu nutzen, haben aber aus unternehmerischen Erwägun-

gen einen Provider mit Einrichtung und Betrieb Ihres Webshops betraut. Von diesem bekommen sie eines Montag morgens einen Anruf, in dem dieser Ihnen mitteilt, dass sich am Wochenende eine unberechtigte Person Zugang zu dem Server, auf dem der Webshop läuft, verschafft hat. Diese Person konnte Daten lesen und zu verändern, und hat dafür gesorgt, dass der Webshop seit Samstag Nacht nicht mehr erreichbar ist. Man kümmere sich aber darüber und werden „in Kürze“ alles wieder unter Kontrolle haben.

Sie werden sich fragen:

- Wie konnte das passieren?
- Wer zahlt mir den Schaden?
- Was kann ich so etwas in Zukunft verhindern?

In meiner Arbeit will ich Antworten auf diese drei Fragen geben; im zivilrechtlichen Teil will ich mich auf das Verhältnis Provider zu Unternehmen beschränken, da dieses das vertragsrechtlich und auch wirtschaftlich interessanteste ist.

2 Der Webshop

Im vorliegenden Fall besteht die Annahme, daß ein mittelständisches Unternehmen seine Waren über das Internet absetzen will. Der Internetvertrieb (Webshop) soll aber von einem beauftragten Unternehmen eingerichtet und technisch betrieben werden. Die Kommunikation des Unternehmens mit dem Webshop soll über das Internet abgewickelt werden.

Diese Lösung kann für kleine und mittlerere Unternehmen kostengünstiger sein, als sich die Infrastruktur selber anzuschaffen. Weiters muß das Unternehmen keine weiteren Techniker einstellen: Die technische Umsetzung liegt beim Service Provider. Diese Lösung wird in dem Maße, wie sich die Unternehmen mehr und mehr auf ihr Kerngeschäft konzentrieren, immer beliebter.

Beim Service Provider ist – in der Regel – auch mehr Sicherheits-Know-how vorhanden, da bei diesem die technische Infrastruktur, zu der auch die Si-

cherheitslösungen zählen, zum zentralen und wichtigsten Budgetbereich seines Unternehmens gehört und er die Kosten für hochkomplexe Sicherheitslösungen auf seine Kunden umlegen wird. Weiters hat er auch eher die Kapazitäten für eine Rund-um-die-Uhr-Überwachung der Server, auch wenn er danach trachten wird, die Überwachung zu automatisieren.[6]

Hingegen ist die Kehrseite der Medaille die Tatsache, dass ein erfolgreicher Provider sicherlich ein sehr beliebtes Ziel für Hacker und dergleichen wird.

Wenn man sich eines Providers bedient, heißt das aber nicht, daß man das Thema Sicherheit damit komplett ausgelagert hat: Genauso wichtig wie ein sicherer Webshop ist nämlich auch der sichere Informationskanal zwischen Webshop und Unternehmen. Es kommt vor, daß dieser Grundsatz nicht beachtet wird, was zu dem absurden Ergebnis führen kann, daß Bestellungen von dem um viel Geld abgesicherten Webshop per unverschlüsselter e-Mail oder Fax an das Unternehmen geschickt werden. Das ist aber derzeit in vielen Fällen leider die Praxis. Fortgeschrittener ist natürlich die Übertragung der Daten über das Internet, wobei in diesem Fall ein „Virtual Private Network" verwendet werden kann. Hier wird über das Internet eine verschlüsselte, sichere Verbindung aufgebaut, die von Dritten nicht - oder nur sehr schwer – kompromittierbar ist. Physisch könnten die Datenpakete zwar noch von Dritten abgefangen werden (daher nur "virtuelles" privates Netzwerk), sie können jedoch nur mit enormen Aufwand entschlüsselt werden und sind damit in der Praxis wertlos.

Welche kritischen Daten sind nun am Webserver gespeichert?

Seitens des Unternehmens sind lediglich kommerzielle Daten wie Artikel, Preise und Lagerstände und – unter Umständen - Kundenprofile gespeichert. Von den Kunden selbst liegen aber kritische Daten auf dem Webserver auf : Angefangen von Stammdaten wie Name, Adresse, Telefonnummer und e-Mail-Adresse sind auch Kreditkartendaten vorhanden.

---

[6] vgl NetworkWorld 22.3.01 S. 34

3 Einbruch im Webshop

In diesem Kapitel werde ich zunächst auf die Ursachen von Sicherheitslücken eingehen, dann die möglichen Angreifer klassifizieren und schließlich die Arten und den Ablauf eines Angriffs beschreiben.

3.1 Die Sicherheitslücke

"Sicherheit" zunächst schließt alle Vorkehrungen und Maßnahmen in personeller, organisatorischer, baulicher und technischer Hinsicht mit ein, die dazu dienen, Personen, Daten, Verfahren, Sachen oder einen Raum vor Gefahren zu bewahren.

Hier will ich mich auf die technischen und organisatorischen Aspekte beschränken.

Für Sicherheitslücken gibt es drei wesentliche Ursachen[7]:

3.1.1 Falsche Konfiguration

Computerprogramme wie zB Betriebssysteme, Anwendungsprogramme und Netzwerksoftware bieten eine Fülle von Funktionen; viele dieser Funktionen werden von den meisten Anwendern nicht benutzt und sind ihnen unbekannt; sie können aber ein Sicherheitsrisiko darstellen, etwa allein dadurch , daß sie nicht deaktiviert sind. Falsche Konfiguration führt oft dazu, dass das System auf eine Anfrage über einen bestimmten Port[8] Zugang gewährt, obwohl es das nicht sollte. In Windows 95/98 zB wird unter Port 139 das NetBIOS-Protokoll angesprochen. Dieses Protokoll wird verwendet, um File- und Druckerserver über das Internet anzusprechen. Ist dieses Protokoll aktiviert, so können fremde Computer über das Internet auf das betreffende System

---

[7] Frei nach: *Anonymous*: Hackers Guide, München 1999, S.23ff

[8] Unter einen Port versteht man ein (logisches) Eingangstor zu einem Computer. Es gibt tausende Ports, von denen Nr 0-1023 von der IANA genormt sind. Eine Beschreibung der Ports findet sich zB unter http://www.logosec.de

zugreifen. [9] Das Problem dabei ist, dass dieses Protokoll bei vielen Usern standardmäßig aktiviert ist, diese aber nichts davon wissen.

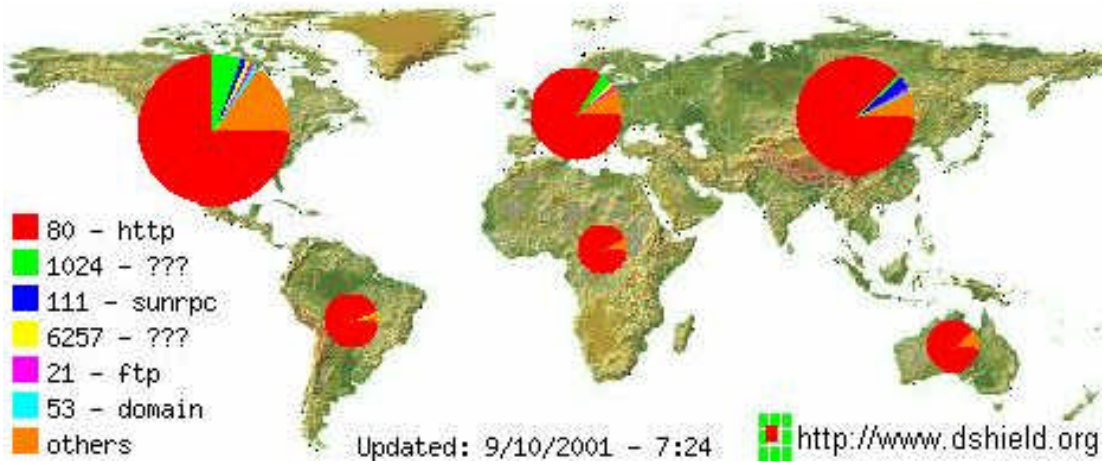


Abbildung: Geographische Verteilung der angreifenden Computer zwischen 5.9.-10.9.2001. Die Farbe bezeichnet den vom Angreifer anvisierten Port

Darüberhinaus ist es schwierig, mit der rasanten Entwicklung Schritt zu halten: Laufend werden Sicherheitslöcher bekannt, die geschlossen werden müssen; dazu gibt es dann meist Updates und Patches[10]. Diese können aber auch neue Sicherheitslöcher öffnen, insbesonders wenn eine Fehlerbehebung mit der Implementierung neuer Funktionalitäten einhergeht.

3.1.2 Systemfehler

Ein Systemfehler bzw Softwarefehler kann einerseits zu Fehlern im Arbeitsablauf führen und es andererseits Hackern ermöglichen, diese Fehler auszunutzen, um das System zu beschädigen oder Kontrolle darüber zu erlangen. Die Hersteller entwickeln zwar rasch Patches dazu, informieren aber in der Regel nicht die Öffentlichkeit darüber, da sich das nicht bezahlt macht. Und das Wissen über diese Sicherheitslücken ist wesentlich. Darüber versuchen man-

---

[9] Für eine genaue Beschreibung des NetBIOS-Angriffes siehe http://www.zerosecurity.de/article.php3

[10] "Patch" (engl f Flicken): Ein kleines Programm, das einen Softwarefehler beheben soll

che Softwarehersteller, die Anwender über geheime Funktionen der Software auszuspionieren.

Derzeit aktuellstes Beispiel dafür ist Windows XP. Dieses erfordert eine Freischaltung über Telephon oder Internet, um Softwarepiraterie zu unterbinden. Microsoft ist aber nicht bereit, Auskunft darüber zu geben, welchen Informationen über den Computer bei der Onlinefreischaltung an Microsoft übertragen werden[11]. Es ist denkbar, dass hier umfassende Informationen über die auf dem betreffenden PC verwendete Software (Raubkopien?, Konkurrenzprodukte?) versendet werden.

3.1.3 Ungenügende Schulung

Wissen ist Macht: Das gilt ganz besonders in Sicherheitsfragen. Früher wurde das Thema Sicherheit zwar vom Anwender ferngehalten, heutzutage ist es aber notwendig, dass jeder ein gewisses Basiswissen im Bereich Computersicherheit aufweist, etwa was den Umgang mit Passwörtern und mit Software aus dem Internet angeht. Denn die beste Firewall[12] ist nutzlos, wenn ein Unberechtigter über ein gültiges Konto einsteigt, dessen Passwort er ausspionieren oder erraten konnte!

Benutzer...

...verwendet Passwörter, die sich leicht aus dem Namen herleiten lassen und dementsprechend einfach geknackt werden können,

...bewahren ihre Passwörter auf einem Post-it an ihrem Monitor auf,

...verraten unbekannten Stimmen am Telefon ihre Passwörter,

...verlassen ihre angemeldeten und unbeaufsichtigten Computer,

...laden unkontrolliert e-Mail-Anhänge herunter und führen diese aus,

...und deaktivieren ihre Antiviren-Software, weil sie ihren Zugriff auf Daten verlangsamt.

---

[11] http://www.handelsblatt.com, Meldung vom 12.7.2001

[12] Rechner bzw Software, die den Datenverkehr kontrollieren und nach konfigurierbaren Bedingungen unterbinden können

Das geschieht auch bei Internet Service Providern, die es eigentlich besser wissen müssten!

3.2 Der Angreifer

Potentielle Angreifer lassen sich nach ihren Interessen und Ressourcen klassifizieren:

3.2.1 Hacker (im engeren Sinn)

„Hacker“ ist ursprünglich eine Bezeichnung für jemanden, der intensiv „in die Tastatur hackt“ und meint damit eine Person, die sich sehr gut mit Computern und Netzwerken auskennt. Heutzutage wird in den Medien jeder als Hacker bezeichnet, der ein Sicherheitsrisiko für einen Rechner darstellt. Hacker ieS haben aber keine destruktiven Absichten sondern betrachten das Überwinden von Sicherheitsbarrieren als Herausforderung und Test ihrer eigenen Kenntnisse. Außer dem Knacken des Systems an sich verfolgen Hacker in der Regel keine besonderen Ziele; oft werden publikumswirksame Nachrichten hinterlassen.[13]

3.2.2 Cracker

Ein Cracker knackt Computersysteme aus Neugier, um Aufmerksamkeit zu erregen oder um Anerkennung in der "community" zu finden. Um diese Ziele zu erreichen, versucht er meist, Schaden anzurichten, da dies das größte Medienecho erzeugt. Meist ist er kein besonderer Computerfachmann sondern verwendet dazu Crackertools, die im Internet frei zum Download angeboten werden.[14]

3.2.3 Krimineller Einzeltäter

---

[13] zB nach dem Knacken der Site der amerikanischen "Moody Air Force Base": "Don't you wish the army would password protect their sites?" (*Anonymous*, Hackers Guide, S. 104)

[14] so zB unter http://www.root-core.com

versuchen, unberechtigten Zugang zu einem System zu erlangen, um einen finanziellen Vorteil zu erlangen. im vorliegendem Falle wäre der Diebstahl von Kreditkartendaten mit darauf folgender Erpressung des anbietenden Unternehmens denkbar. Möglich wäre auch die Tätigung von Bestellungen im Internet mit diesen Daten. Hier hängt das Gefährdungspotential ganz vom individuellen Know-how des Angreifers ab.

3.2.4 Insider

Von diesen geht grundsätzlich die größte Gefahr aus, da sie in der Regel Zugangsprivilegien haben und Kenntnisse über Struktur, Sicherheitslücken und Standort von sensiblen Daten haben können. Ihre Motivation kann Rache am Arbeitgeber oder auch ein finanzielles Interesse sein.

3.2.5 Wirtschaftsspionage

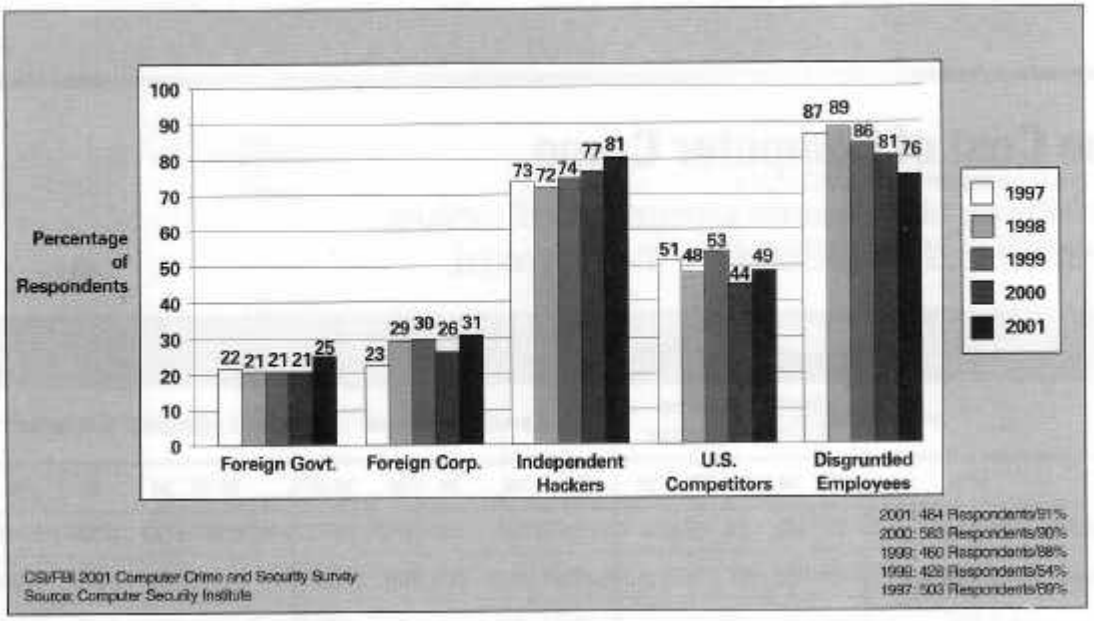
Aus diesem Bereich gibt es nur wenige offizielle Informationen, da offiziell grundsätzlich alles abgestritten wird: der wirtschaftliche Schaden für das betroffene Unternehmen würde durch das Bekanntwerden des Vorfalles nur größer. Die durch Diebstahl geistigen Eigentums verursachten Schäden sind aber enorm; laut der Internationalen Handelskammer in Wien erleidet die österreichische Wirtschaft durch Spionage jährlich Verluste in Höhe von 8 bis 14 Mrd öS.[15] ivF spielt Wirtschaftsspionage aber keine Rolle, da in unserem Webshop keine sensiblen Forschungs- und Entwicklungsdaten liegen.

3.2.6 Organisierte Kriminalität

Die organisierte Kriminalität ist technisch auf dem neuesten Stand und bedient sich intensiv der Möglichkeiten des Internets. Sie verfügt über enorme Ressourcen und stellt daher ein großes Gefahrenpotential im Netz dar, insbesonders weil "traditionelle" Geschäftsfelder wie Schutzgelderpressung leicht auf das Internet übertragen werden können.

---

[15] Quelle: *Power*, Attacken im Web, S. 207



3.3 Der Angriff

Es gibt eine Vielzahl von Möglichkeiten, in ein Computersystem einzudringen. Im Folgenden werde ich die wesentlichen Methoden beschreiben.

3.3.1 Ausspionieren der Zugangsdaten

Der Angreifer kann auf verschiedene Arten vorgehen. Die erste ist einmal, zu versuchen, sich als berechtigter User beim System anzumelden. Dazu benötigt er eine Benutzerkennung und ein Passwort. Diese Informationen herauszufinden, ist gar nicht so kompliziert, wie es erscheint; dazu unten.

Der Angreifer hat auch die Möglichkeit, ein Programm auf die Reise zu schicken, das für ihn die gewünschten Informationen aufspürt. Diese Programme - Trojanische Pferde genannt - werden vom ahnungslosen User gemeinsam mit einem anderen Programm installiert und protokollieren ohne Wissen des Benutzers Passworte und andere relevante Informationen. Diese Daten werden dann, wenn der Computer des Opfers mit dem Internet verbunden ist, "nach Hause", dh an eine vom Programmierer des Trojaners vorher definierte Internetadressse geschickt.

3.3.1.1 Die Benutzerkennung

Alle Betriebssysteme haben ab Werk Standardbenutzerkennungen wie etwa „sysadm“, „demo“ oder "guest" eingerichtet, die ein nachlässiger Systemadministrator möglicherweise nicht modifiziert oder gelöscht hat. Eine besondere Situation besteht bei Unix/Linux-Betriebssystemen: Hier gibt es standardmäßig den Zugang „root“, der alle Administratorrechte zur Verfügung stellt. Dieser Zugang kann nicht verändert oder gelöscht werden.

Viele Benutzerkennungen bestehen aus den Initialen oder dem vollen Namen des Berechtigten, was die Suche auch nicht schwerer macht.

3.3.1.2 Das Passwort

Die meisten Menschen verwenden sehr primitive Passworte wie etwa den eigenen Vornamen oder Geburtsdaten. Solche Passworte können in wenigen Versuchen ermittelt werden. Werden sicherere Passworte verwendet, sind diese meist durch eine so genannte "Wörterbuchattacke" ("dictionary attack") zu knacken. Dabei verwendet der Angreifer ein Programm, das automatisch immer wieder versucht, sich am System anzumelden und dabei jedesmal ein neues Wort aus einem elektronischen Wörterbuch als Passwort ausprobiert. Da sich die meisten Passworte in einem Wörterbuch finden lassen, ist diese Methode recht erfolgversprechend. Hier spielt - abgesehen von dem Sicherheitsbewußtsein des Berechtigten - schon die Qualität des Systems bzw die Professionalität des Systemadministrators eine Rolle:

Erlaubt das System Tausende vergebliche Anmeldeversuche oder sperrt es nach einigen Versuchen den Zugang?

Wieviel Zeit muss zwischen den Anmeldeversuchen vergehen? Wenig sichere Systeme erfordern nach einem erfolglosen Anmeldeversuch keine Wartezeit; das macht eine Wörterbuchattacke sehr effektiv, da diese dann sehr rasch zu einem Ergebnis kommen wird. Idealerweise verdoppelt das System nach jedem erfolglosen Anmeldeversuch die Wartezeit; diese Lösung wird aber sehr selten verwendet.

Protokolliert es die Vorgänge mit? Liest jemand diese Protokolle?

Schlägt das System vielleicht Alarm?

Auf der sicheren Seite ist man, wenn man nur ausgefallene Passworte verwendet, die nicht nachzuvollziehen sind, möglichst noch mit Sonderzeichen, zB gi!3&511ox. Leider sind solche Passworte sehr schwer zu merken, es ist aber möglich, sich diese nach einer Logik zu stricken, die man sich merkt.

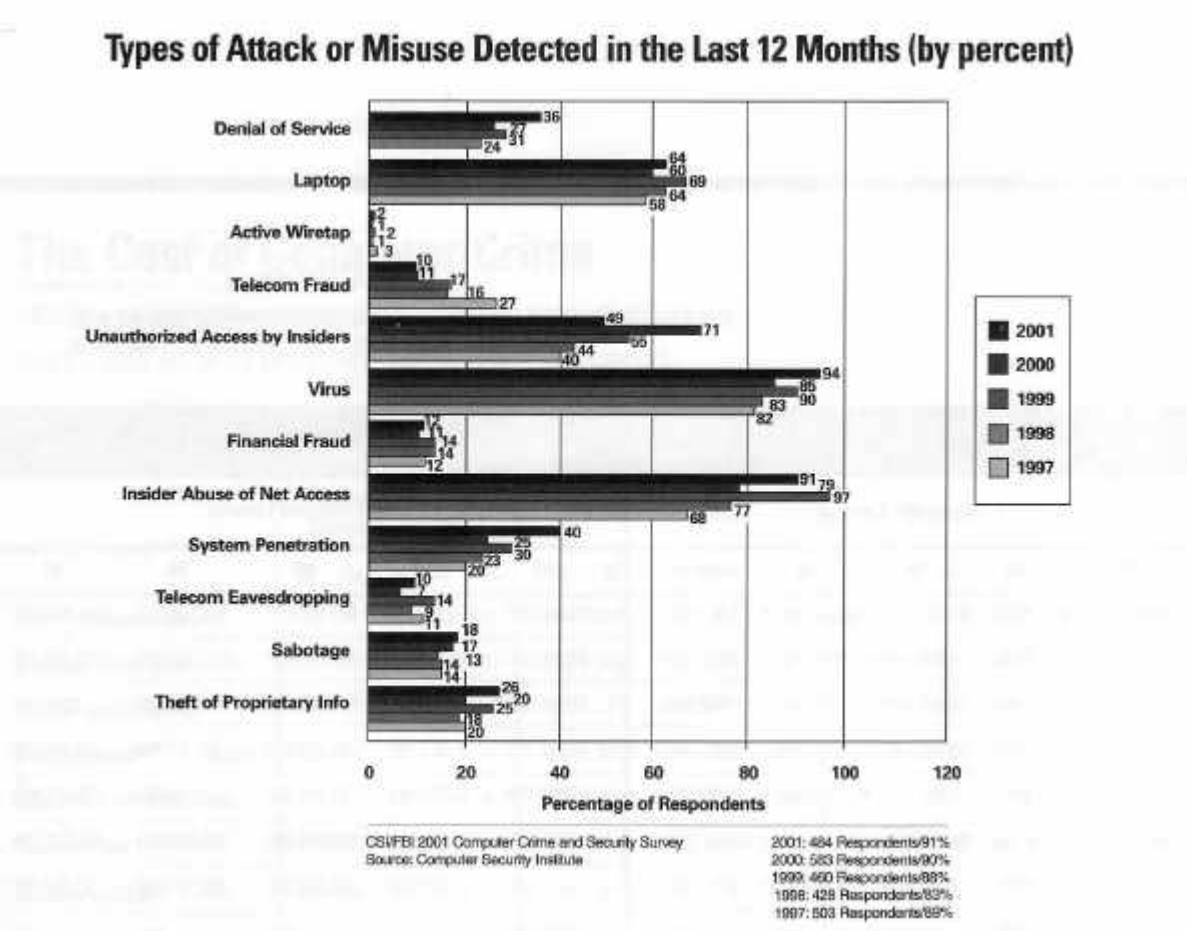
Am sichersten ist die Verwendung von lediglich einmal verwendbaren Passwörtern, diese werden aber kaum angenommen.

Eine weitere Möglichkeit, an Benutzerkennungen und Passworte zu kommen, ist das Mitprotokollieren des Anmeldevorganges zB durch sogenanntes "packet sniffing". Dabei "hängt" der Angreifer ein Tool an einen Punkt (zB Server, Router), wo Anfragen an den Zielserver durchkommen; dieses Tool "durchschnüffelt" die durchkommenden Datenpakete nach Passwörtern und protokolliert die gefundenen Informationen.

3.3.2 Ausnutzen von Systemfehlern

Bleibt der Angreifer beim Ausspionieren eines Passwortes erfolglos, so muß er sich eine "Hintertür" suchen, um in den Webshop einzubrechen. Dazu wird er zunächst einmal herausfinden, unter welches Betriebsystem und welche Serversoftware auf dem Zielsystem läuft. Wie oben schon erwähnt, können sich aufgrund der verwendeten Software, deren Versionen, der möglichen Konfigurationen und dem Zusammenspiel der Komponenten eine Unzahl an Sicherheitslöchern ergeben.

Mit dem Internet, insbesonders den Newsgroups zum Thema Sicherheit und Hacking, steht dem Angreifer ein riesiger Wissensfundus zur Verfügung, den er nach Informationen über das Zielsystem absuchen kann. Vielerorts finden sich im Internet auch sogenannte Cracker-Tools, mit denen auch ein Möchtegern-Hacker unter Ausnutzung einer bestimmten Sicherheitslücke in ein System einbrechen kann.



3.3.3 Vorgehensweise nach erlangtem Zugang

Hat der Hacker über die eine oder andere Methode Zutritt zum System erlangt, so stehen ihm unterschiedliche Möglichkeiten: Abhängig von den Privilegien des Kontos, das er verwendet, kann er Daten etwa betrachten und herunterladen oder auch diese verändern, löschen, das System umkonfigurieren, um sich für spätere "Besuche" einen Zugang einzurichten oder auch möglichst viel Schaden anrichten.

»Wenn jemand von außen in Systeme Ihrer Organisation eingedrungen ist, Sie bitte an, in welcher Weise der Eindringling aktiv geworden ist.«

Datenintegrität manipuliert	41	6,8 Prozent
Schnüffelprogramm installiert	40	6,6 Prozent
Passwortdateien gestohlen	34	5,6 Prozent
Systeme sondiert/durchsucht	88	14,6 Prozent
Trojanische Logons	35	5,8 Prozent
IP-Schwindel	29	4,8 Prozent
Virus eingeführt	64	10,6 Prozent
Nutzung von Diensten unterbunden	38	6,3 Prozent
Daten heruntergeladen	49	8,1 Prozent
Geschäftsgeheimnisse verletzt	59	9,8 Prozent
Geld gestohlen/umgeleitet	2	0,3 Prozent
E-Mails/Dokumente gelesen	76	12,6 Prozent
Das Eindringen veröffentlicht	3	0,5 Prozent
Personal belästigt	27	4,5 Prozent
Sonstiges (Beschreibung)	18	3,0 Prozent
Gesamt	603	100,0 Prozent

[16]

In unserem Falle könnte er die Homepage um witzige Meldungen "bereichern", Preise verändern, für Kunden Bestellungen tätigen, Kundendaten verändern oder herunterladen.

Das Herunterladen der Kreditkartendaten der Kunden wird für den Hacker am interessantesten sein. Mit diesen Daten kann er dann im Internet Waren und Dienstleistungen beziehen, bis sie vom Kreditkartenunternehmen gesperrt werden, was einige Zeit dauern kann. Wenn der Hacker eine große Anzahl von Kreditkartendaten ausspäht, kann er damit einen enormen Schaden anrichten, der schlussendlich auf den zurückfällt, der den Vorfall aufgrund mangelnder Sicherheitsvorkehrungen zu verantworten hat.

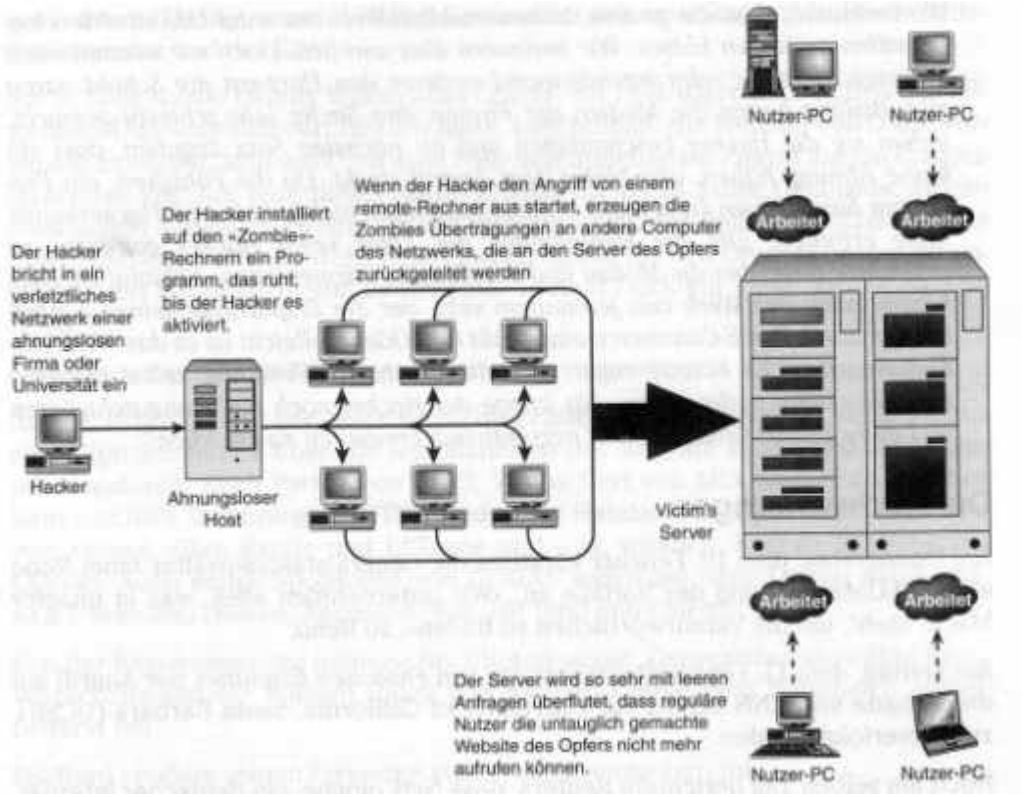
Das bringt uns zu einem wesentlichen Problem: Ein vorsichtiger Hacker kann in ein System eindringen, die von ihm gewünschten Daten kopieren und nach dem Löschen aller Spuren das System unbemerkt verlassen. Niemand erfährt je, dass der Vorfall stattgefunden hat. Wie hoch die Dunkelziffer solcher Angriffe ist, ist nicht abzuschätzen.

[16] Quelle: *Power*, Attacken im Web, S. 60

3.4 Denial of Service (DoS)

Eine Methode, ein System mit destruktiven Absichten anzugreifen, besteht in einer DoS-Attacke. Das Ziel eines solchen Angriffes ist, das Zielsystem durch Bombardierung mit einer Unzahl an Anfragen funktionsuntüchtig zu machen. Groß angelegte DoS-Attacken werden meist „verteilt“ durchgeführt; dazu bricht der Angreifer in eine Reihe von Systemen ein und installiert dort Programme. Diese Programme nehmen das Zielsystem dann auf Kommando gleichzeitig unter Beschuss und zwingen es in die Knie.

Erst kürzlich wurde eines der renommiertesten Institute für Computersicherheit, das „Computer Emergency Response Team“, Opfer eines solchen Angriffes und war drei Tage praktisch nicht zu erreichen.[17]

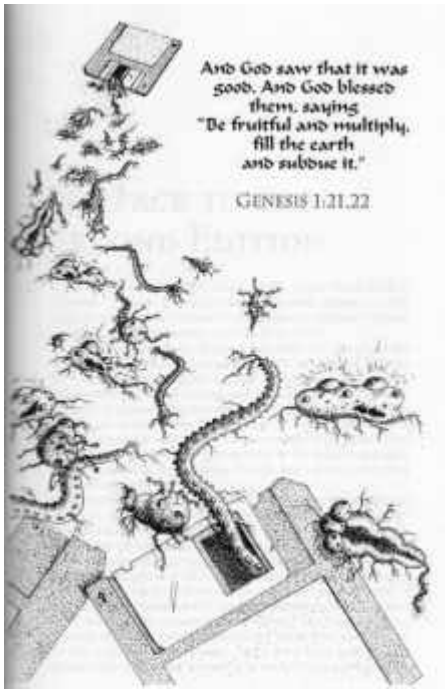


Primär ist so eine Attacke zwar eine Form von Vandalismus, sie könnte aber auch wirtschaftliche Interessen dienen; denkbar wäre ein damit verbundener Erpressungsversuch.

---

[17] Computerwoche 22/2001, S. 12

3.5 Viren



Unter einem Computervirus versteht man Programmcode , der in der Lage ist, sich selbst zu reproduzieren, indem er sich an andere Programme anhängt.

Ein Virus muss per se nicht „böse“ oder destruktiv; die Anweisungen eines Virus, die zB Dateien löschen oder Festplatten formatieren, sind „Nutzlast“. Viren könnten theoretisch auch positive Zwecke erfüllen, tatsächlich wird derzeit diskutiert, „gute“ Viren zum Aufspüren „böser“ Viren einzusetzen[18]. Die Umsetzbarkeit dieser Idee ist aber sehr umstritten. Was Viren derzeit sehr gefährlich macht, ist die starke Verbreitung von sicherheitstechnisch sehr bedenklicher Software der Firma Microsoft wie zB MS Outlook oder MS Word. Die in diesen Programmen vorhandenen Sicherheitslücken sorgen gepaart mit der Unachtsamkeit vieler Anwender dafür, dass sich Viren wie „Melissa“ heute mit astronomischer Geschwindigkeit über den Erdball verbreiten können.

Virus	Jahr	Typ	Zeitbedarf, bis er »vorherrscht«	Schäden
Jerusalem, Cascade, Form ...	1990	.exe-Datei, Bootsektor	3 Jahre	$50 Millionen für alle Viren in 5 Jahren
Concept	1995	Word-Makro	4 Monate	$50 Millionen
Melissa	1999	Word-Makro, über E-Mail verschickt	4 Tage	$93–$385 Millionen
I love you	2000	E-Mail und aktiviertes Visual Basic Script	5 Stunden	>$700 Millionen

Quelle: ICSA.net.

[18] vgl Computerwoche 30/2001, S. 22

Die immer neuen Sicherheitslücken in den Microsoft-Produkten beginnen schon, sich wirtschaftlich auf die ersten Unternehmen auszuwirken, die Windows-Systeme einsetzen: Der amerikanische Versicherer J.S. Wurzler hat eben die Versicherungsprämien seiner Anti-Hacker-Versicherungen für Kunden erhöht, die Windows-Betriebssysteme verwenden.[19]

3.6 Würmer

Würmer ähneln Viren, reproduzieren und verbreiten sich aber auf andere Weise. Sie sind eigenständige Programme, die sich selbständig über das Internet verbreiten und im Gegensatz zu Viren nicht darauf angewiesen sind, daß der Benutzer ihn durch Aufrufen einer infizierten Datei aktiviert. Wenn ein Wurm Zugriff auf ein System erlangt, speichert er dort eine Kopie von sich ab; diese Kopie sucht dann selbständig nach weiteren Rechnern und infiziert diese.

Die Designer von Würmern sind sehr kreativ:

Ein britisches Sicherheitsunternehmen berichtete vor kurzem von dem „Win32.Invalid"-Wurm, der sich als Sicherheitsupdate für den Internet Explorer ausgibt.[20]

Viel Aufsehen hat der „I love you"-Wurm erregt; vor kurzem erst hat ein Wurm namens „Code Red" für Schlagzeilen gesorgt.[21] Code Red hat unter Ausnützung einer Sicherheitslücke in Microsofts Internet Information Server innerhalb kürzester Zeit über 300.000 Webserver befallen. Bei Servern, deren Standardsprache Englisch ist, verunstaltet Code Red die Web-Seiten dieses Rechners mit dem Text „Welcome to http://www.worm.com! Hacked by chinese!" Bei Servern, deren Standardsprache nicht Englisch ist, scannt er nach verwundbaren Rechnern und verbreitet sich weiter. Von allen befallenen Rechnern startet Code Red außerdem an jedem 20. eines Monats eine ver-

---

[19] Computerwoche 23/2001, S. 5

[20] http://www.pressetext.at , 1.9.2001

[21] siehe ua Computerwoche 30/2001, S. 6

teilte DoS-Attacke auf die Webpräsenz des Weißen Hauses. Kurz nach Analyse des Wurmes durch Sicherheitsexperten erfolgte eine zweite Angriffswelle durch einen lediglich um 13 Byte geänderte Variante.

Was kann ein Unternehmen, das einen Webshop betreiben lässt, aus diesem Vorfall lernen? Die Sicherheitslücke, die sich der Wurm zunutze gemacht hatte, war bereits Mitte Juni entdeckt worden. Microsoft hatte daraufhin relativ schnell einen Patch veröffentlicht, der die Lücke schloss. Offenbar haben es aber viele Administratoren nicht für notwendig befunden, diesen Patch auf ihren Webservern zu installieren, sonst wären nicht so viele Server befallen worden.

Für diese Administratoren muss man vorbringen, dass die große Zahl der Updates und Patches für Software es schwer macht, am Ball zu bleiben. Ein sorgfältiger Administrator hat aber meines Erachtens durch regelmäßige Konsultation von Newslettern und Herstellerwebsites den Überblick zu behalten, auch wenn die Informationsflut enorm und diese Tätigkeit daher zeitaufwendig ist.

3.7 Konsequenzen

3.7.1 Verlust der Vertraulichkeit

Der Verlust der Vertraulichkeit von kritischen eigenen Daten – geistigem Eigentum - kann für ein Unternehmen enorme Verluste bedeuten.

- Die gestohlenen Daten können in die Hände interessierter Dritter, zB Konkurrenzunternehmen gelangen und diesen einen Wettbewerbsvorteil verschaffen.
- Gestohlene Daten können in manipulierter Form veröffentlicht werden.

Noch schlimmer sieht die Sache aus, wenn Kunden oder Geschäftspartner aufgrund des Diebstahls ihrer Daten Schaden erleiden.

- Dies bringt oft eine Verletzung vertraglicher Pflichten oder auch gesetzlicher Auflagen mit sich.

- Abgesehen von diesen juristischen Implikationen kann der dadurch bewirkte Vertrauensverlust der Kunden ein Unternehmen in den Ruin treiben!

3.7.2 Verlust der Verfügbarkeit

Der Verlust der Verfügbarkeit hat je nach Art des Unternehmens unterschiedlich gravierende Folgen. In unserem Fall wird das Unternehmen es verkraften, wenn der Webshop ein Wochenende offline war; wenn das ganze Unternehmensnetzwerk „steht“, steigt der Schaden bald in schwindelerregende Höhen, da heutzutage ohne Zugriff auf die elektronisch vorliegenden Daten kaum mehr gearbeitet werden kann.

Eine Bank, die über einen Zeitraum von zwei Tagen keine Geschäftsvorfälle bearbeiten kann, wäre inzwischen schon konkursreif.

3.7.3 Verlust der Integrität

Darunter versteht man das Problem, dass man nach einem Angriff nicht mehr sicher sein kann, dass die kompromittierten Daten noch richtig sind. Die Daten können beschädigt, gelöscht oder manipuliert worden sein. Eine Rücksicherung der kompromittierten Daten kann daher notwendig werden. Dies kostet Zeit und Geld und ist nur möglich, wenn man vor dem Angriff für eine regelmäßige und zuverlässige Sicherung der Daten gesorgt hat.

3.7.4 Fazit

Ein erfolgreicher Angriff hat somit weitreichende Folgen. Diese können in letzter Konsequenz zur

- Beeinträchtigung wirtschaftlicher Beziehungen,
- Verlust des Vertrauens von Kunden und Geschäftspartnern in die eigene Arbeitsqualität und zur
- Einbuße der Konkurrenzfähigkeit

führen.

Die Schadenshöhe ist nicht abschätzbar!

4 Zivilrechtliche Konsequenzen

4.1 Anspruch des geschädigten Unternehmens gegenüber dem Angreifer

4.1.1 Anspruchsgrundlage

Zuallererst denkt man natürlich an einen Anspruch gegen den Angreifer; dieser wird sich auf einen Schadenersatzanspruch nach deliktischer Haftung stützen.

Kausalität und Vorsatz liegen eindeutig vor, die Rechtswidrigkeit muss sich durch Verstoß gegen eine Schutznorm ergeben:

Hier kommen in Österreich der § 126a StGB (Datenbeschädigung) und der § 148a StGB (Betrügerischer Datenverarbeitungsmissbrauch) in Frage. Diese Strafnormen erfordern aber zumindest ein Verändern der Daten durch den Hacker, was dieser aber nicht tut, wenn er lediglich Daten kopiert und nichts manipuliert oder löscht. Weiters kommen noch die § 118ff StGB (Verletzung des Briefgeheimnisses, Verletzung des Fernmeldegeheimnisses, Missbrauch von Tonaufnahme- und Abhörgeräten, Verletzung von Berufsgeheimnissen, Verletzung eines Geschäfts- oder Betriebsgeheimnisses, Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses) in Frage.

In Verbindung mit dem § 77 UrhG (Briefschutz) und den oben genannten Normen kann man ableiten, „dass die österreichische Rechtsordnung den unbefugten Zugriff auf vertrauliche Mitteilungen grundsätzlich missbilligt“[22], was eine hinreichende Schutznorm zur Begründung einer deliktischen Haftung des Hackers darstellt, wenn er diese verletzt, indem er Daten ausspioniert.

Auch das Datenschutzgesetz(DSG) bietet eine Schutznorm: Die ausspionierten Kundendaten sind unzweifelhaft personenbezogene Daten iSd § 4 Abs.1 DSG, da sie die Identität der Kunden preisgeben. Gemäß § 1 Abs.1 hat jedermann einen Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht (Grund-

---

[22] *Gassauer-Fleissner*, Geheimhaltung, Offenbarung und Veröffentlichung von Daten in Informationsnetzwerken, ecolex 1997, 102

recht auf Datenschutz). Dieses Interesse für die Kunden besteht darin, dass Unbefugte nicht ihre Rechnung und Kosten einkaufen sollen.

Bei Ausspionierung von Informationen durch Insider kommt auch der § 11 UWG als Schutznorm in Betracht. Dieser stellt die Weitergabe von Geschäfts- und Betriebsgeheimnissen durch Bedienstete zu Zwecken des Wettbewerbs unter Strafe. Nach dem § 12 UWG begründet ein Verstoß gegen diese Bestimmung auch Schadenersatz- und Unterlassungsansprüche.

4.1.2 Rechtsdurchsetzung

Diese ist problematisch:

1. Der Angreifer muss identifiziert werden. Das ist machbar; kann aber sehr aufwendig werden, wenn der Angreifer geschickt agiert hat und über eine Reihe von – ebenfalls gehackter – Systeme unschuldiger Dritter in das Zielsystem eingedrungen ist. Man muss sich dann mit den Administratoren der betroffenen Systeme in Verbindung setzen, um die Spur zurück verfolgen zu können. Dies kann etwa bei Servern in Südamerika, Afrika oder Asien sehr kompliziert bis unmöglich werden.

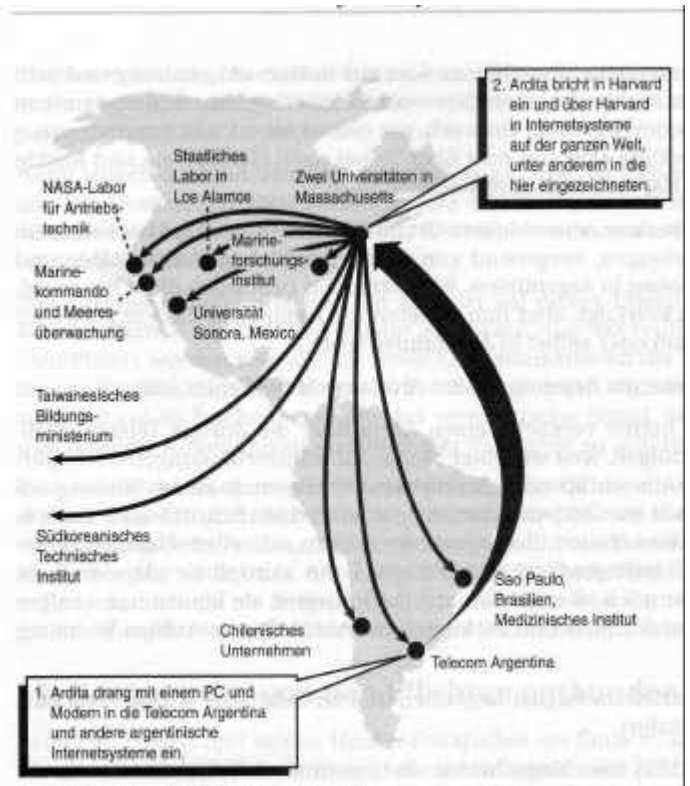


Abbildung 6.2: Der Pfad des Hackers.
Quelle: amerikanisches Justizministerium.

Schon für die Sicherheitsbehörden ist die Strafverfolgung schwierig: "Internet-Kriminelle sind gegenüber der Exekutive im Vorteil. Die E-Mail eines Kriminellen braucht zwei Minuten von Wien nach New York, der Rechtsweg zwischen Österreich und den USA benötigt zwischen acht und zwölf Monaten."[23]

2. Der Angreifer muss verklagt werden können. Wie bringt man einen koreanischen Hacker vor ein österreichisches Gericht?
3. Die Tat muss dem Angreifer nachgewiesen werden können. Dieser Beweis kann geführt werden, macht aber einen teuren Sachverständigenprozess notwendig, da Richter in der Regel nicht über das technische Verständnis verfügen, einen Hackerangriff nachzuvollziehen.
4. Nach dem gewonnenen Prozess muss man noch zu seinem Geld kommen.

Fazit: Die Erfolgsaussichten, auf diesem Wege zum Ziel zu gelangen, sind äußerst gering; der Aufwand dafür ist enorm. Sinnvoll ist es aber sicherlich, Anzeige bei den Strafverfolgungsbehörden zu erstatten, und sei es nur, um die Verwaltung dazu zu bewegen, Abteilungen für Cyberkriminalität einzurichten bzw diese auszubauen.

4.1.3 Abteilungen für Computerkriminalität bei Sicherheitsbehörden

Seit 1. August 1999 besteht im Bundesministerium für Inneres eine Zentralstelle zur Bekämpfung der Internetkriminalität: die Abteilung II/16-ITB, Informationstechnologie/Beweissicherung. In dieser Abteilung gibt es mehrere Untergruppen, zuständig für die Bereiche Beweissicherung, Netzwerkkriminalität, Verschlüsselungssysteme, Auswertung und Analyse; die Beamten sind besonders ausgebildet und werden aktiv, wenn sie von Exekutivdienststellen aus dem In- oder Ausland von einer Computerstraftat verständigt werden.

In einem Gespräch mit einem Beamten dieser Abteilung konnte der Verfasser erfahren, dass die internationale Zusammenarbeit der verschiedenen staatli-

---

[23] *Otupal* (aus der Zentralstelle im Innenministerium zur Bekämpfung der Computer- und Netzkriminalität) in: *Brenner*, IT-Kriminalität: Niemandsland für Kriminelle, Öffentliche Sicherheit, Das Magazin des Innenministeriums,Nr. 7-8/2001, http://www.bmi.gv.at

chen Sicherheitsbehörden gut funktioniert. Die offiziellen Rechtshilfeersuchen über die Interpol helfen im Bereich der Computerkriminalität aber wenig, da „das benötigte Logfile eines Proxyservers von gestern morgen schon wieder überschrieben ist, das Rechtshilfeverfahren aber sieben Monate dauern würde."

Zur Erleichterung der internationalen Zusammenarbeit hat die Interpol ein Frühwarnsystem eingerichtet, über welches die Sicherheitsbehörden Informationen über IT-Kriminalität rasch über das Internet austauschen können.[24]

In den USA wurden vom FBI ein zentrales „National Infrastructure Protection Center" und über das Land verteilte „Regional Computer Intrusion Squads" eingerichtet, die in Fällen von Computerkriminalität ermitteln.

Es ist zu erwarten, dass den Strafverfolgungsbehörden angesichts der zunehmenden Vernetzung und der immer engeren Zusammenarbeit der Behörden verschiedener Staaten in Zukunft mehr und mehr Ressourcen zur Bekämpfung von Computerkriminalität zur Verfügung stehen werden.

4.2 Anspruch des geschädigten Unternehmens gegenüber dem Provider

Interessanter ist es natürlich, den eigenen Provider zur Verantwortung zu ziehen; dieser hat in der Regel ein weitaus größeres Potential zur Zahlung von Schadenersatz.

4.2.1 Vertragstypus

Die Natur eines Webhostingvertrages ergibt sich aus dem Umfang der durch den Provider eingegangenen Verpflichtungen. Zunächst handelt es sich einmal um ein Dauerschuldverhältnis. Abhängig von der Ausgestaltung kann es Elemente eines Dienstleistungsvertrages, eines Werkvertrages oder auch eines Mietvertrages beinhalten, wie die deutsche Rechtsprechung bereits festgestellt hat. In Österreich hingegen gibt es noch keine Judikatur dazu.[25]

---

[24] *Lattacher*, Internetkriminalität: Terror aus dem Datennetz, Öffentliche Sicherheit 3-4/2001, http://www.bmi.gv.at

[25] *Jaburek*, Handbuch der EDV-Verträge[3], Wien 2000, S. 21

Bei Betrachtung des Webhostingvertrages kommt man zu dem Schluss, dass man es im wesentlichen mit einer Spielart des Rechenzentrums- bzw Outsourcingvertrages zu tun hat, den es schon seit den 70er Jahren gibt. In beiden Fällen stellt der Auftragnehmer dem Auftraggeber seine Rechner für dessen Daten zur Verfügung und erbringt darüber hinaus Dienstleistungen.

Der Rechenzentrumsvertrag erinnert aufgrund der primären Leistung, dem zur Verfügung stellen von Rechnerkapazität, ebenfalls zunächst an einen Mietvertrag, „diese Einordnung wird aber dem RZ-Vertrag nicht ganz gerecht."[26] Das diesem Vertrag innewohnende Erfolgsmoment legt einen Werkvertrag nahe.

Auch beim Webhostingvertrag stellt der Provider dem Kunden Speicherplatz auf seinen Servern zur Verfügung. Diese Leistung das deutet auf einen Mietvertrag hin. Dagegen spricht aber, dass es das Wesen der Miete ist, die Mietsache im Eigenbesitz zu haben und darüber verfügen zu können. Der Kunde kann aber in unserem Fall nicht über die Festplatten auf den Servern verfügen; das kann nur der Provider. Darüber hinaus ist das zur Verfügung stellen von Speicherplatz nicht der wesentliche Teil des Vertrages sondern erbringt darüber hinaus noch umfassende Dienstleistungen:

Die Leistung ist der Webauftritt als Ganzes und dieser wird wesentlich durch technische (zB Datenbankanbindung des Webshops) und künstlerische (Webdesign) Leistungen erbracht.

Dieses Leistungsbündel deutet auf einen Dienstleistungs- oder Werkvertrag hin.[27] Wie sich unten zeigt, ist die konkrete Einordnung in einen Vertragstypus für die konkreten Ansprüche des Kunden nicht wesentlich.

4.2.2 Gewährleistung

Gewährleistung ist das bei allen entgeltlichen Verträgen gesetzlich angeordnete Einstehenmüssen des Schuldners für Sach- und Rechtsmängel, welche die Leistung zum Zeitpunkt ihrer Erbringung aufweist. Gewährleistungsan-

---

[26] *Schneider*, Handbuch des EDV-Rechts, Köln 1997, S. 1603

[27] vgl *Schneider*: Handbuch des EDV-Rechts, S. 1701ff

sprüche sind unabhängig vom Verschulden des Auftragnehmers; sie erfordern lediglich das Vorliegen eines objektiven Mangels.

Der Auftragnehmer hat dafür einzustehen, dass seine Leistung die bedungenen oder die im Verkehr gewöhnlich vorausgesetzten Eigenschaften aufweist. Daher ist es sinnvoll, die Parameter der zu erbringenden Leistungen genau zu fixieren, und die Gewährleistungsansprüche zu definieren. Nach dem neuen, am 1.1.2002 in Kraft tretendem Gewährleistungsrecht sind auch öffentliche Äußerungen des Auftragnehmers über seine Leistungen(Werbung) für die Beurteilung der bedungenen Eigenschaften ausschlaggebend!

Wurde nichts vereinbart, so ist zu eruieren, was die im Verkehr gewöhnlich vorausgesetzten Eigenschaften von Webhostingdienstleistungen sind:

Anforderung	**Beschreibung**
Verfügbarkeit	Die Verfügbarkeit ist die kritischste Eigenschaft eines Webangebotes; ist der Webshop nicht online, existiert er für die Kunden nicht und kann keinen Umsatz generieren. Sie wird für Webangebote idR als Prozentwert über einen gewissen Zeitraum angegeben. Die gewöhnlich vorausgesetzte Verfügbarkeit hängt ganz vom Geschäftsbereich ab. Im Bankenbereich wird sie bei nahezu 100% liegen, für einen Webshop um 95%.
Reaktionszeit	Eine kurze Reaktionszeit ist bei Onlineangeboten wichtig, um die Kunden zu halten und sie nicht zu verärgern (Der durchschnittliche Surfer wartet nicht länger als sieben Sekunden auf den Aufbau einer Webseite). Sie ist im Internet aber nicht nur vom Dienstleister abhängig. In der Regel beträgt sie einige Sekunden.
Sicherheit	Gewöhnlich wird ein Sicherheitsstandard vorausgesetzt, der dem „Stand der Technik“ entspricht. (Für Details siehe unten 4.2.3.2)
Redundanz	Man setzt voraus, dass das System des Auftragnehmers so aufgebaut ist, dass es noch funktioniert, wenn einzelne Komponenten(Festplatten, Rechner, Netzwerkknoten) ausfallen.

Aktualisierung	Es wird erwartet, dass die Hardwareinfrastruktur und die Software regelmäßig aktualisiert wird; sie sollte nicht veraltet sein.
Störungsstelle	Webdienstleister bieten oft auch eine Hotline an, die zu bestimmten Zeiten besetzt, Störungsmeldungen entgegennimmt und den Anrufer bei technischen Problemen unterstützt. Man erwartet, dass eine Hotline zumindest zu den Geschäftszeiten besetzt ist.

Von Gesetzes wegen kann der Kunde bei behebbaren Mängeln zunächst einmal Verbesserung fordern. Ist der Mangel unbehebbar oder wird der vom Auftragnehmer nicht innerhalb einer angemessenen Frist behoben, so hat der Kunde das Recht auf Preisminderung, und, wenn der Mangel wesentlich ist, auf Wandlung.

Entsprechen Internetdienstleistungen zu einem gewissen Zeitpunkt nicht den vereinbarten Anforderungen, so ist dieser Mangel unbehebbar, da man zB die fehlende Verfügbarkeit der Website in der letzten Woche nicht mehr herstellen kann (Die Verbesserung ist für Zielschuldverhältnisse ausgelegt). Der Kunde kann daher sofort Preisminderung bzw Wandlung verlangen.

Bei einem Mietvertrag berechtigt der § 1117 ABGB den Mieter zur Vertragsauflösung bzw wird gemäß § 1096 ABGB der Mietzins ex lege gemindert, wenn der Vermieter seiner Pflicht zur Erhaltung der Bestandsache nicht nachkommt. „AGB der Hersteller schließen dieses Recht auf Zinsminderung in der Regel aus, was aber – zumindest bei vollständiger Unbrauchbarkeit der Mietsache – sittenwidrig und damit nichtig ist.“[28]

Somit ist bei der Gewährleistung der Vertragstypus nicht ausschlaggebend, da man jeweils zu dem selben Ergebnis gelangt.

[28] *Jaburek*, Handbuch der EDV-Verträge, S. 274

4.2.3 Schadenersatz

4.2.3.1 Kausalität

Der Provider kann durch das Nichttreffen angemessener Sicherheitsvorkehrungen kausal für einen erfolgreichen Hackerangriff werden.

Die Beweisführung ist jedoch schwierig:

Grundsätzlich liegt gemäß § 1296 ABGB die Beweislast bei der geschädigten Partei. § 1298 ABGB normiert eine Beweislastumkehr bei Verletzung von vertraglichen Verpflichtungen, hier muss der Schädiger beweisen, dass ihn kein Verschulden trifft; die Kausalität muss aber weiterhin der Geschädigte beweisen. Diese Beweislastumkehr gilt auch bei Verletzung von vertraglichen Nebenverpflichtungen[29], insbesonders auch bei der Verletzung einer vertraglichen Schutz- und Sorgfaltspflicht.[30] Voraussetzung für die Beweislastumkehr ist aber nicht die bloße Kausalität sondern auch das Vorliegen einer objektiven Obligationswidrigkeit in der Sphäre des Schädigers, die den Anschein eines Verschuldens weckt.[31]

Im Anlassfall liegt durch den Hackereinbruch und dem Stillstand des Systems diese objektive Obligationswidrigkeit zweifelsohne vor.

Für die Beweisführung ist es ratsam, den Zustand des Systems zum Zeitpunkt des Angriffes festzuhalten. Dies erfolgt am besten durch einen Beweissicherungsantrag bei Gericht, da der Provider jederzeit die Möglichkeit hat, das System zu ändern und man ihm daher gewisse Sicherheitsmängel nur mehr schwer nachweisen kann.

Es ist daher sinnvoll, möglichst rasch beim zuständigen Gericht einen Beweissicherungsantrag nach § 384 Abs.1 ZPO zu stellen. Die Beweissicherung erfolgt dann durch einen Sachverständiger vor Ort, der die Methode des Eindringens des Hackers und den Zustand des Systems festhält.

---

[29] zB OGH 30.3.1955 SZ 28/87; 6.2.1990 ZVR 1991/17

[30] zB OGH 17.1.1990 NRsp 1990/90; 3.9.1992 JBL 1993, 396

[31] *Bydlinski*, Zur Haftung der Dienstleistungsberufe in Österreich und nach dem EG-Richtlinienvorschlag, JBl 1992, 347; *Ertl*, Zivilrechtliche Haftung im Internet, CR 3/1998, 180

4.2.3.2 Rechtswidrigkeit

Hier kommt es ganz auf den Vertrag an. Für den Kunden ist es angesichts der Problematik ausgesprochen wichtig, die wesentlichen Fragen der Leistungserbringung und der Haftung im Vertrag ausdrücklich zu regeln. Unterlässt man das, so ist im Streitfall der Richter berufen, den Vertrag ergänzend auszulegen – nicht gerade die beste Voraussetzung für einen Prozesserfolg.

Wurde nichts konkretes vereinbart, dann müssen die Verpflichtungen im Zuge der ergänzenden Vertragsauslegung konkretisiert werden. Dazu muss man die von redlichen und verständigen Vertragspartnern gewöhnlich vorausgesetzten Eigenschaften von Webhostingleistungen hinsichtlich Sicherheit definieren. Diesen könnten etwa sein:

Anforderung	**(Mögliche) Umsetzung**
Verwendung von Betriebsystemen, die akzeptable Sicherheit bietet	Bewährte Betriebsysteme, die länger auf dem Markt sind, Betriebsysteme mit gutem Sicherheitskonzept (zB Unix und seine Derivate wie etwa Linux)
Sicherheitseinrichtungen auf dem neuesten Stand der Technik	Installation von Firewalls, Intrusion Detection Systems, Virenscannern, usw..., Regelmäßige Updates
Vorhandenes und gelebtes Sicherheitskonzept	Erstellung eines Sicherheitskonzepts mit Hilfe externen Beratern, Zertifizierung, Monitoring
Alle Mitarbeiter sind zur Einhaltung der Sicherheitsrichtlinien verpflichtet	Entsprechender Passus in den Arbeitsverträgen
Übertragung von sensiblen Informationen nur verschlüsselt	E-mail-Verkehr mit „Prettty Good Privacy“(PGP), http-Übertragungen mit „Secure Socket Layer“ (SSL) verschlüsseln

Wenn der Provider diesen Anforderungen nicht entsprochen hat, hat er seine Leistungspflicht objektiv verletzt, was eine Haftung aus dem Vertrag begründet.

Muss man seinen Anspruch auf deliktische Haftung stützen, so bietet sich als Schutznorm § 90 TKG:

„§ 90 (1) Die Pflicht zur Erlassung von Datensicherheitsmaßnahmen im Sinne des § 21 des Datenschutzgesetzes im Zusammenhang mit der Erbringung eines Telekommunikationsdienstes obliegt jedem Betreiber jeweils für jeden von ihm erbrachten Dienst.

(2) Unbeschadet des Abs. 1 hat der Betreiber in jenen Fällen, in denen ein besonderes Risiko der Verletzung der Vertraulichkeit besteht, die Teilnehmer über dieses Risiko und über mögliche Abhilfen einschließlich deren Kosten zu unterrichten."

Der Provider kann im weiteren Sinne als „Betreiber eines Telekommunikationsdienstes" iSd Telekommunikationsgesetzes (TKG) gesehen werden, auf jeden Fall decken sich die Aufgaben beider Dienstleister weitgehend. § 90 TKG kann daher auch für den Provider als Schutzpflichten begründen. Unterlässt er die entsprechenden Sicherheitsmaßnahmen, verstößt er gegen diese Schutznorm, handelt damit rechtswidrig und wird schadenersatzpflichtig.

Den Provider treffen auch Verpflichtungen nach dem Datenschutzgesetz(DSG), die als Schutznormen zu qualifizieren sind. Zunächst ist zu prüfen, wer als Auftraggeber iSd § 4 Z 4 DSG zu betrachten ist:

Auftraggeber ist laut dieser Bestimmung derjenige, der die Entscheidung getroffen hat, Daten für einen bestimmten Zweck zu verarbeiten. Diese Entscheidung hat das Unternehmen, das den Webshop als Vertriebskanal verwendet und damit die Kunden dazu bringt, ihre Daten in ein Webformular einzugeben, getroffen.

Der Provider könnte als Auftraggeber betrachtet werden, wenn ihm anlässlich er Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt wurde oder er über die Entscheidung über Art und Weise der Verwendung eigenverantwortlich zu treffen hat. Da das Unternehmen dem Provi-

der sehr wohl vorschreibt, was dieser mit den Kundendaten zu machen hat, er diese sehr wohl verarbeiten soll, trifft beides nicht zu; Auftraggeber iSd DSG bleibt das Unternehmen. Der Provider ist somit Dienstleister iSd § 4 Z5 DSG.

Als solcher er gemäß § 14 DSG verpflichtet, Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Er hat sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind.

$ 14 Abs.2 DSG zählt explizit Maßnahmen zur Wahrung der Datensicherheit auf, so zB

- die Belehrung der Mitarbeiter über die bestehenden Datenschutzvorschriften,
- die Regelung von Zutrittsberechtigungen zu den Räumen des Dienstleisters,
- die Regelung von Zugriffsberechtigungen auf Daten und Programme und der <u>Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte</u>
- die Führung von Protokollen zur Sicherstellung der Nachvollziehbarkeit von Verwendungsvorgängen.

Diese Maßnahmen müssen je nach Art der verwendeten Daten unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, dass den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Weiters hat der Dienstleister gemäß § 15 Abs.1 DSG die Pflicht, Daten aus Datenanwendungen, die ihm ausschließlich aufgrund seiner berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, geheim zu halten.

Verstößt der Provider gegen diese Schutznormen, handelt er ebenfalls rechtswidrig.

4.2.4 Verschulden

Die Frage, ob die oben Pflichten schuldhaft verletzt wurde, bedarf im Streitfall meist der Klärung durch Gerichtssachverständige.

Um Anhaltspunkte für die Klärung dieser Frage zu finden, will ich auf den unter 3.6 beschriebenen Fall des Systemadministrators zurückkommen, der den Patch gegen den „Code-Red"-Wurm nicht installiert:

Dieses Verhalten ist aus schadenersatzrechtlichen Gesichtspunkten höchst relevant: Handelt ein Systemadministrator leicht oder grob fahrlässig, wenn er diesen Patch nicht installiert? Dazu muss man in Betracht ziehen, dass insbesonders Microsoft-Software so voller Sicherheitslücken ist, dass ständig Patches und Sicherheitsupdates veröffentlicht werden, die sich zu einer unübersehbaren Menge anhäufen, wenn man nicht dauernd „am Ball bleibt". Ein sorgfältiger Administrator wird den Patch installieren, wenn er von der Sicherheitslücke und von der Verfügbarkeit erfährt. Diese Informationen erfährt ein sorgfältiger Administrator, der sich über einschlägige Newsletter und Websites hinsichtlich der Sicherheitsaspekte „seiner" Systeme auf dem laufenden hält.

Hält der Administrator sich nicht auf dem laufenden oder ignoriert er ihm mitgeteilte Sicherheitslücken, so handelt er daher schwer fahrlässig, da dies Fehler darstellen, die einem ordentlichen Systemadministrator nicht unterlaufen dürfen!

Es folgt eine Matrix einer Auswahl von in der Praxis auftretenden Vorfällen mit dem Vorschlag einer Qualifizierung des Verschuldens:

Sachverhalt	Verschuldden	Begründung
Keine Firewall installiert oder installierte Firewall aus Performancegründen deaktiviert	Grob fahrlässig	Ein Server ohne aktiver Firewall ist Angriffen aus dem Internet ungeschützt ausgesetzt
Firewall wurde nicht an das zu schützende System angepasst, sondern läuft mit Standardkonfiguration	Grob fahrlässig	Eine nicht sorgfältig konfigurierte Firewall ist nutzlos
Aus Kostengründen wurde eine Firewall installiert, die für das System nicht leistungsfähig genug ist	Grob fahrlässig	Eine leistungsmäßig nicht ausreichende Firewall ist lediglich Makulatur
Die ordnungsgemäß installierte Firewall weist eine bisher unbekannte Sicherheitslücke auf	Kein Verschulden	Hier liegt die Verantwortung beim Hersteller; der Administrator hat lediglich die Pflicht, sich über das Produkt zu informieren
Es werden keine sicherheitsrelevanten Patches und Sicherheitsupdates eingespielt	Grob fahrlässig	Wissen über neue Sicherheitslücken verbreitet sich sehr rasch über das Internet und wird von Hackern ausgenützt. – Das Schließen dieser Lücken mittels Herstellerpatches ist für einen sorgfältigen Administrator selbstverständlich sein
Ein allgemein bekannter Patch wurde nicht eingespielt	Grob fahrlässig	Der sorgfältige Administrator bleibt hinsichtlich seiner Systeme auf dem laufenden
Ein spezieller, relativ unbekannter Patch wurde nicht eingespielt	Leicht fahrlässig	Bei der Fülle an Patches kann auch ein sorgfältiger Administrator einen übersehen
Es gibt keine Richtlinien bez Passwörter, Passwörter werden nie geändert, Passwörter werden weitergegeben	Grob fahrlässig	Das Ausspionieren wird dadurch ausgesprochen leicht gemacht (siehe 3.3.1)
Richtlinien vorhanden, wurden ivF von Mitarbeiter aber nicht befolgt	Grob fahrlässig	Zurechnung über das Verschulden des sorglosen Mitarbeiters

Diese Anforderungen an die Computersicherheit sind selbstverständlich auch an den Kunden zu stellen. Das gilt insbesonders hinsichtlich des Umganges mit Passworten, die der Kunde vom Provider bekommt, um die Daten im Internet selbständig zu ändern.

4.2.5 Umfang der Ersatzpflicht

Der Schadenersatz umfasst grundsätzlich den positiven Schaden, die Verminderung des vorhandenen Vermögens. Zum positiven Schaden zählen auch aufgrund des Ereignisses zu tätigender Aufwand und den Geschädigten treffende Verbindlichkeiten.[32]

Dieser kann unter anderem in den Kosten der Versorgung der Kunden mit neuen Zugangsdaten und der Kosten der Wiederherstellung der gelöschten Daten bestehen, eine genaue Quantifizierung ist aber besonders im IT-Bereich schwierig (vgl 3.7).

Die Ersatzpflicht umfasst – da es ich um ein Handelsgeschäft handelt – gemäß Art 8 Nr 2 EVHGB auch bei leichter Fahrlässigkeit den entgangenen Gewinn. Entgangener Gewinn definiert sich als die „Beeinträchtigung künftiger Erwerbs- und Gewinnchancen, ohne dass bereits ein bestehendes Vermögensgut oder Recht verletzt wurde“[33], hier kann ua in den in der Zeit der Unerreichbarkeit des Webshops entgangenen Geschäfte bestehen. Wie beziffert man aber den durch den Vertrauensverlust der Kunden entstandenen Schaden?

---

[32] *Koziol/Welser*, Grundriss des bürgerlichen Rechts[10], Wien 1995, S. 444ff

[33] *Krejci*, Grundriss des Handelsrechts, Wien 1995, S. 271

4.3 Webhostingverträge in der Praxis

Wie sehen die Verträge in der Praxis aus?[34] Wesentlich sind für unsere Problemstellung die Hauptleistungspflichten und Haftungsregelungen hinsichtlich der beiden Aspekte der Datensicherheit, die im Englischen als „Safety“(Wahrung von Integrität und Verfügbarkeit) und „Security“(Wahrung der Vertraulichkeit) bezeichnet werden.

Der Provider hat naturgemäß ein Interesse daran, seine Pflichten möglichst vage zu beschreiben und im besten Falle nur ein „Bemühen“ ohne Erfolgsverbindlichkeit zu schulden; er ist im Vorteil, da er in der Regel nur auf Grundlage seiner Allgemeinen Geschäftsbedingungen abschließen will, die ihm seine Juristen in aller Ruhe ausgetüftelt haben.

Mit dem Auftragsvolumens steigt aber die Verhandlungsbereitschaft des Providers; die Bereitschaft, wegen ein paar Vertragsklauseln auf einen guten Auftrag zu verzichten, sinkt.

Es ist immer sinnvoll, nicht widerspruchslos den Standardvertrag des Dienstleisters zu unterschreiben, sondern mit klaren Vorstellungen in solche Verhandlungen zu gehen und seine eigenen Interessen hineinzureklamieren. Wenn man glaubt, aufgrund des fehlenden eigenen technischen Verständnisses nicht „mitreden“ zu können, ist es ratsam, einen Berater zuzuziehen.[35]

4.3.1 Vertragstypus/Hauptleistungspflichten

Für den Kunden ist es sinnvoll, den Vertrag in Richtung Werkvertrag zu bringen, da bei diesem die Pflichten des Auftragnehmers tendenziell am strengsten beurteilt werden und die gesetzlichen Gewährleistungsregelungen für den Kunden günstig sind.

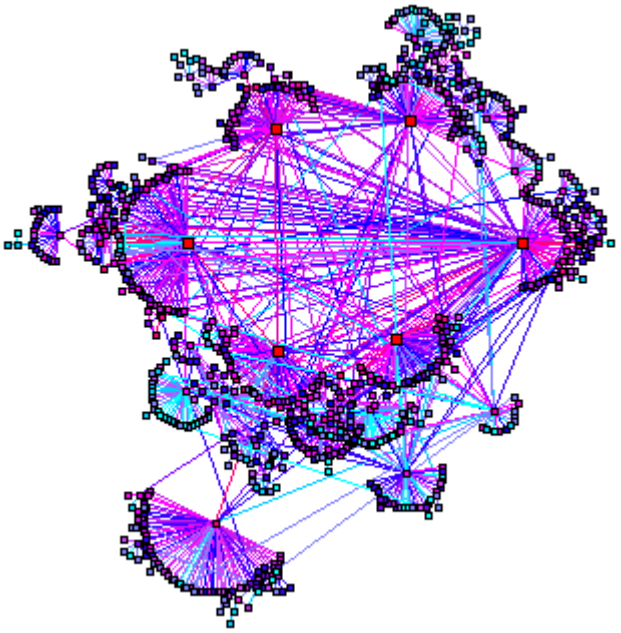
Hinsichtlich der Erbringung der Leistungen muss man sich immer bewusst sein, dass das Internet trotz seiner (ursprünglich militärischen) Konzeption als

---

[34] siehe http://www.lawfirm.de/papers/content/content2.html

[35] Ausführliche Anleitung für IT-Vertragsverhandlungen siehe *Jaburek,* Handbuch der EDV-Verträge, S. 30ff

redundantes, dezentrales Netzwerk von Interdependenzen geprägt ist. Auch im Internet gibt es neuralgische Punkte, deren Zerstörung das Internet auseinanderbrechen lässt[36].



[37]

Aber auch im lokalen Bereich ist der Provider von Dritten abhängig: Wenn deren Netzwerke zusammenbrechen, die naturgemäß außerhalb des Einflussbereiches des Providers liegen, kann die Leistung unverschuldet unmöglich werden. Auf Seiten der Provider wird in AGB immer auf die mangelnde Einflussmöglichkeit auf die Verfügbarkeit von nicht von ihm selbst betriebene Leitungswege (vis maior) hingewiesen[38].

Für den Kunden wäre in diesem Zusammenhang eine vertragliche Regelung, die dem Provider die Beweislast für das Fehlen eigenes Verschuldens bei Berufung auf höhere Gewalt aufbürdet, sinnvoll.

4.3.2 Wahrung von Integrität und Verfügbarkeit (Safety)

Die Frage, wer regelmäßige Datensicherungen vornimmt, gehört ebenfalls geklärt.

---

[36] http://www.heise.de/tp/deutsch/inhalt/co/8441/1.html

[37] Quelle: http://www.heise.de/tp/deutsch/inhalt/co/8441/1.html

[38] AGB der KPNQwest Austria, http://www.kpnqwest.at/agb/agb.php

Viele Provider wälzen die Pflicht zur Datensicherung komplett auf den Kunden ab.[39] Man findet zB Bestimmungen wie „Für Datenverlust ist die BreNet nicht haftbar“.[40]

Dabei wird vergessen, dass es teuer, unpraktikabel und daher praktisch unmöglich für den Kunden ist, täglich zig Megabytes an Daten über eine Datenleitung zu sichern. Darüber hinaus eröffnet dieser regelmäßige Datentransfer eine weitere Möglichkeit für Hacker, diese abzufangen.

Der Provider kann die Backups um einiges leichter anfertigen, da sich ja die Rechner in seinem Herrschaftsbereich befinden. Die Übertragung dieser Verpflichtung an den Provider ist daher die einzig praktikable Lösung.

In diesem Licht ist es aus der Sicht des Kunden sinnvoll, eine Klausel in den Vertrag zu reklamieren, dass der Provider dafür haftet, dass die von dem Kunden oder an den Kunden übermittelten Daten nicht in seiner Einflußsphäre beschädigt werden oder verloren gehen, und zwar idealerweise schon bei leichter Fahrlässigkeit.

Diese Haftung für Beeinträchtigung durch Viren, die in die oben genannte Haftung fallen würde, wird in der Regel von Providern nur bei Vorsatz und grober Fahrlässigkeit übernommen; eine Regelung, die für den Kunden sicherlich nachteilig ist und daher nicht akzeptiert werden sollte. (Zur Sittenwidrigkeit solcher Bestimmungen siehe nächstes Kapitel)

4.3.3 Wahrung der Vertraulichkeit (Security)

Grundsätzlich trachtet der Provider (natürlich) danach, die Haftung für eigenes Verschulden auf Fälle schwerer Fahrlässigkeit und Vorsatz zu beschränken, so auch in diesem Zusammenhang.[41]

Zunächst ist es sinnvoll, die Pflicht zur Geheimhaltung von Passwörtern und zur unverzüglichen Änderung dieser, sobald die Vermutung besteht, dass

---

[39] so zB die AGB der „Yippi-Yeah! E-Business GmbH“, http://www.speicherzentrale.de/agb.php

[40] AGB der BreNet GmbH, http://www.providerwerden.de/agb.php

[41] so zB die AGB von KPNQwest Austria, aaO

diese ausspioniert wurden, ausdrücklich festzuhalten. Die Informierung des Vertragspartners von solchen Vorfällen sollte ebenfalls geregelt werden.

Diese Regelungen sind für beide Parteien gleichermaßen wichtig.

Provider haben in ihren AGB Passagen, nach denen der Kunde das Risiko, dass Dritte die übermittelten Daten abhören, ausdrücklich in Kauf nimmt und überdies für jeden Missbrauch haftet, „der aus einer eventuell unberechtigten Verwendung des Passwortes folgt".[42]

Pauschal findet sich auch in AGB, dass der Kunde für die Sicherheit der von ihm ins Internet und auf Webservern gespeicherten Daten vollumfänglich selbst Sorge trägt.[43]

Solche Bedingungen kann man mE bereits als „wider die guten Sitten" bzw als „gröblich benachteiligend" nach § 849 Abs.3 ABGB qualifizieren, da sie das Risiko eines Schadens aufgrund des Ausspionierens der Daten durch einen Hacker vollständig auf den Kunden überwälzt. Überdies ist im österreichischen Recht nach hM Freizeichnungen für grobes Verschulden überhaupt unzulässig.[44]

Nach dem Risikoprinzip haftet der Vertragspartner, der das Risiko erhöht, für den auftretenden Schaden.

Die Sphäre des Kunden, dh das bei ihm aufliegende Passwort ist aber nicht der einzige Risikobereich. Am Server des Providers findet sich aber eine weitere, größere Risikosphäre, auf die der Kunde keinen Einfluss nehmen kann, ebenso wie auf die Art und Weise der Übertragung der Daten. [45]

---

[42] AGB der „Yippi-Yeah! E-Business GmbH", aaO; AGB der BreNet GmbH, aaO; AGB der iCar, http://www.icar.de/hp/webdesign/agb.html

[43] AGB der kambach.net, http://kambach.net/site/agb/agb.htm

[44] *Ertl*, CR 3/1998, 180

[45] vgl *Zib*, Electronic commerce und Risikozurechnung im rechtsgeschäftlichen Bereich, ecolex 1999, 230

Eine vertragliche Bestimmung, die einem Vertragspartner ein Risiko aufbürdet, das zum Großteil der andere Vertragspartner kontrolliert, verstößt gegen die guten Sitten und ist daher – auch unter Kaufleuten – gemäß § 879 Abs.1 ABGB nichtig.

Weiters wird in AGB ausdrücklich festgestellt, dass „Datenschäden, Schäden durch Datenmissbrauch oder durch kriminelles Eindringen“ nur „bis zu einem gewissen Grad“ verhindert werden können. „Die (...) kann hier aber keine Haftung übernehmen, verpflichtet sich aber die für die (...) möglichen Schutzmaßnahmen einzusetzen.“[46]

In anderen AGB findet sich die Zusicherung, angemessene Sicherheitsmaßnahmen gegen unberechtigte Serverzugriffe durch Hacker mit der nötigen Sorgfalt zu treffen, die dem „gehobenen technischen Standard entsprechen; eine Haftung für solche Fälle wird aber ausgeschlossen.“[47]

Ein derartiger, pauschaler Haftungsausschluss ist aus den oben genannten Gründen nicht zulässig. Die Pflicht, Sicherheitsmaßnahmen zu treffen, schränkt diesen Haftungsausschluss wiederum ein.

Ausgewogener dagegen die Formulierung, nachdem der Provider verpflichtet ist, „alle technisch möglichen und zumutbaren Maßnahmen“ zum Schutz der Daten zu ergreifen, jedoch nur bei Vorsatz und grober Fahrlässigkeit zu haften.[48]

In der Regel wird versucht, in AGB die Höhe der Ersatzpflicht betragsmäßig zu beschränken[49], dies ist hinsichtlich grober Fahrlässigkeit und Vorsatz – wie bei den inhaltlichen Haftungsbeschränkungen - aus den oben genannten Gründen nicht zulässig.

---

[46] AGB der BreNet GmbH, aaO

[47] AGB der iCar, http://www.icard.de/hp/webdesign/agb.html

[48] AGB der KPNQwest Austria, aaO

[49] so zB AGB der Netway Communications AG, http://home.netway.at/hp2000b/channel_netway/agb/nwyoffice_agb.php3

5 Gegenmaßnahmen

Absolute Sicherheit gibt es nicht – besonders nicht im Netz. Damit aber derartige Vorfälle selten oder auch nie auftreten, sollte man sich als Unternehmen seinen Provider genau aussuchen. Es folgt eine kurze Beschreibung der Maßnahmen, die der Provider treffen sollte, um solche Vorfälle wie den gegenständlichen zu vermeiden. Wenn ihr Provider zu diesen Themen klare Konzepte vorweisen kann, so wird Ihr Webshop Angriffen nicht schutzlos ausgeliefert sein.

5.1 Organisatorische Maßnahmen

5.1.1 IT-Sicherheitskonzept

Der erste Schritt ist die Erstellung eines Sicherheitskonzeptes. In letzter Zeit hat sich der – seine Wurzeln im amerikanischen Verteidigungsministerium habende – „IT-Sicherheitskriterien-Katalog“ entwickelt, der die Bedrohungsanalyse und Maßnahmenergreifung standardisiert:[50]

1. Stufe: Ermittlung der Schutzbedürftigkeit
    a. Erfassung der IT-Anwendungen und der zu verarbeitenden Informationen
    b. Bewertung der IT-Anwendungen und der zu verarbeitenden Informationen

    Rückkoppelung
2. Stufe: Bedrohungsanalyse
    a. Erfassung der bedrohten Objekte
    b. Bestimmung der Grundbedrohungen
    c. Bestimmung der Bedrohungen

    Rückkopplung
3. Stufe: Risikoanalyse

[50] aus *Schneider*: Handbuch des EDV-Rechts, S. 213

a. Bewertung der bedrohten Objekte

b. Bestimmung der Häufigkeit von Schäden

c. Bestimmung und Zusammenstellung der aktuellen Risiken

4. Erstellung des IT-Sicherheitskonzeptes

a. Auswahl von Maßnahmen

b. Bewertung der Maßnahmen

c. Kosten-Nutzen-/Gesamtkosten-Betrachtung

d. Restrisiko-Analyse

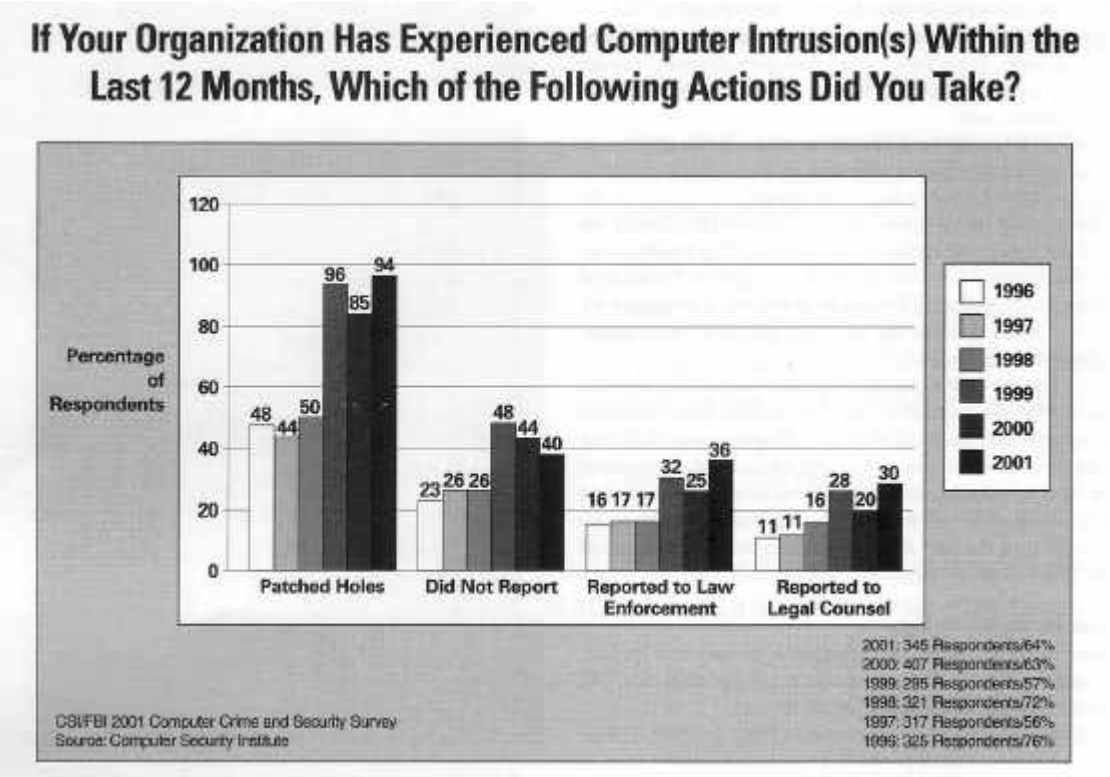
Rückkoppelung

5.1.2 IT-Sicherheit im laufenden Betrieb

- Möglichst tägliche Beobachtung verschiedener Quellen mit dem Ziel, ständig auf dem aktuellen Stand der identifizierten Bugs zu sein sowie zu entscheiden, inwieweit diese relevant für die eigenen Systeme sind und mit welchen Mitteln die angebotenen Lösungen umgesetzt werden müssen.
- Bewertung von Sicherheitsrelevanten Alarmen und Ereignissen, deren Weiterleitung und gegebenfalls die Initiierung einer Eskalation. Die Meldungen, die verarbeitet werden müssen, kommen unter anderem aus Intrustion-Detection-Systemen, Meldungen der Firewall, Netz-Logfiles und Antivirus-Alarmen. Ein wesentlicher Teil des Monitoring ist die Pflicht, die genannten Quellen stets aktuell und das Volumen an Meldungen unter Kontrolle zu halten, ohne wesentliche Informationen zu unterdrücken
- Regelmäßige und möglichst automatisierte Überprüfung der eigenen Verletzlichkeit. Diese ständigen Aktionen können keinesfalls periodische Risikobewertungen ersetzen, erhöhen jedoch das allgemeine Niveau und gewährleisten schnellere Reaktionen auf unvorhergesehene Risiken. Auch hier ist es wesentlich, die eingesetzten Tools ständig auf

dem neuesten Stand zu halten, da sonst der betriebene Aufwand zu einer trügerischen Sicherheit führt

- Formale Eskalations- und Reaktionsprozeduren für den Fall von Ereignissen. Das können Virenverbreitung, DoS-Angriffe und Hackereinbrüche sein, die dazu führen, dass Systeme heruntergefahren werden müssen, Netze überlastet sind, IP-Adressen geblockt werden, eine Wiederherstellung von Daten notwendig wird oder kriminalistische Untersuchungen eingeleitet werden müssen. Dazu ist die Definition von Rollen notwendig, damit beispielsweise entschieden werden kann, wer informiert werden muss oder wer Aktionen freigibt.[51]



5.1.3 IT-Sicherheitsbewusstsein

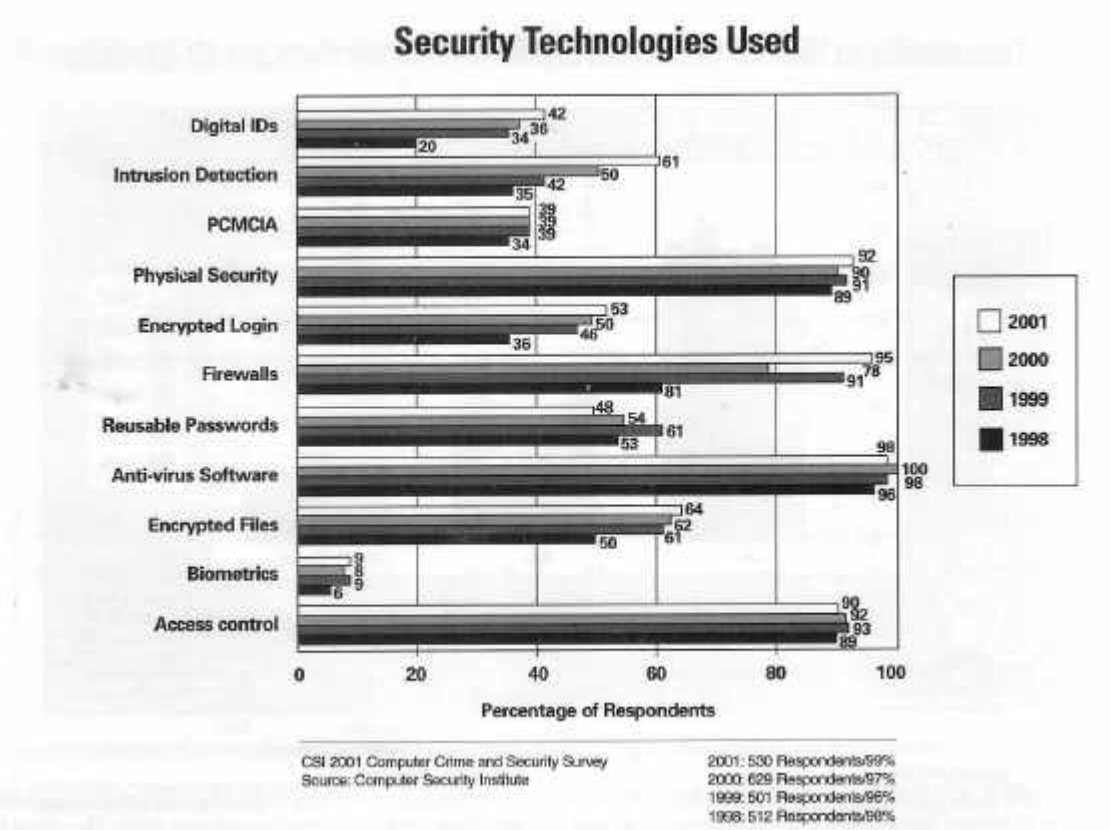
Die klaffenden Löcher, die durch mangelndes Sicherheitsbewusstsein geprägten Verhalten in die um teures Geld aufgebaute Sicherheitsphalanx reißt, können durch vielfältige Maßnahmen geschlossen werden. Wenn man das Thema ansprechend aufbereitet, nehmen es die Verantwortlichen bereitwillig auf und vermeiden die in 3.1.3 beschriebenen Verhaltensweisen: Das beginnt

[51] vgl Computerwoche 33/2001, S.40

bei Marginalien wie Mauspads mit Schlagworten der Informationssicherheit und geht über Informationsveranstaltungen bis zu regelmäßig aktualisierten Informationen im Intranet.

5.2 Technische Maßnahmen

Aus technischer Sicht gibt es eine Reihe von Maßnahmen, die man für seine Informationssicherheit ergreifen kann: Firewalls, Public Key Infrastructure, Virtual Private Networks, Intrusion Detection Systems (IDS) – eine Methode nach der anderen kommt in Mode und wird als das Allheilmittel angepriesen, bis sie von dem nächsten Wundermittel abgelöst wird. Derzeit ist der Einsatz von Intrusion Detection Systems „im Trend“: Laut dem „2001 Computer Crime Survey“ haben 1998 35% der Befragten IDS verwendet, heuer sind es 61%.



Die Sicherheitsprobleme werden daneben aber nicht weniger. Erschwerend kommt dazu, dass Sicherheitslösungen auf löchrigem Fundament gebaut werden, da etwa die Betriebssysteme von Microsoft nach und nach immer mehr Sicherheitslücken offenbaren. Welche Überraschungen sie noch für die Anwender bereit halten, ist nicht absehbar, da Microsoft die Sourcecodes aus kommerziellen Gründen geheim hält und wie einen Augapfel hütet – was a-

ber im Oktober vorigen Jahres einen Hacker nicht daran hinderte, in einen Microsoft-Server einzudringen und sich Zugang zu den Quellcodes zu verschaffen.[52]

Ein interessanter Ansatz wird derzeit von Invicta Networks realisiert: Den Angreifern soll durch ein rapides Wechseln der IP-Adressen - gleich einem bewegten Ziel – die Attacke erschwert werden.[53]

6 Conclusio

Ein Unternehmen, das im Web präsent sein will und einen Dienstleister damit betraut, hat den Problemkomplex Internetsicherheit damit **nicht** mit ausgelagert. Von der Wahl des Vertragspartners über die Vertragsverhandlungen bis zum täglichen Betrieb muss man Sicherheitsaspekte mitberücksichtigen, um die eigenen Daten und die der Kunden geschützt zu wissen. Idealerweise verfügt man selber über das erforderlich technische und juristische Know-how; ist das aber nicht der Fall, so empfiehlt es sich, die Hilfe von Experten in Anspruch zu nehmen. Dass man bei der Sicherheit an der falschen Stelle gespart hat, merkt man erst, wenn es zu spät ist.

---

[52] *Powers*: Attacken im Web, S. 14

[53] Computerwoche 22/2001, S. 10

7 Literaturverzeichnis

Kommentare und Bücher

Anonymous, Hackers Guide – Sicherheit im Internet und im lokalen Netz, München 1999

Cheswick/Bellovin**,** Firewalls and Internet Security: repelling the wily hacker, USA 1994

Dittrich/Tades, ABGB[34], Wien 1994

Jaburek, Handbuch der EDV-Verträge[3] , Wien 2000

Koziol/Welser, Grundriß des bürgerlichen Rechts I[10] , Wien 1995

Krause, Electronic Commerce, Berlin 1998

Krejci, Grundriß des Handelsrechts, Wien 1995

Ludwig, The Giant Black Book of Computer Viruses, Show Low (Arizona) 1998

Manninger/Göschka/Schwaiger, Electronic Commerce – die Technik, Berlin 2001

Power, Attacken im Web, München 2001

Redeker**,** Handbuch der IT-Verträge, Köln 2000

Schneider**,** Handbuch des EDV-Rechts, Köln 1997

Artikel in Zeitschriften und im WWW

Bydlinksi**,** Zur Haftung der Dienstleistungsberufe in Österreich und nach dem EG-Richtlinienvorschlag, JBl 1992, 347

Gassauer-Fleissner, Geheimhaltung, Offenbarung und Veröffentlichung von Daten in Informationsnetzwerken, ecolex 1997, 102

Wilhelm**,** Wieder Verwirrung um § 1298 ABGB, ecolex 1993, S.73

Zib, Electronic commerce und Risikozurechnung im rechtsgeschäftlichen Bereich, ecolex 1999, 230

Computer Security Institute, Computer Security Issues & Trends, Vol VII, No.1, 2001

Network World, München 2001

Computerwoche, München 2001

Websites

http://www.gocsi.org	Computer Security Institute
http://www.securelab.com	Ausführliche Website zum Thema Internetsicherheit mit kommerziellem Hintergrund
http://www.sicherheit-im-internet.de	Website von BRD-Behörden zur Sicherheitsproblematik
http://www.sicherheitsmanagement.de	Website eines deutschen Rechtsanwaltes zum Thema Sicherheit
http://www.techweb.com/tech/security	Ausführliche Informationen zum Thema Internetsicherheit
http://www.rechtsprobleme.at	Österreichische Website zum Internetrecht
http://www.securitynewsportal.com	Ausführliche Informationen zum Thema Internetsicherheit
http://www.dshield.org	Gibt eine Übersicht über Hackerattacken weltweit
http://cryptome.org	Website zum Thema Verschlüsselung, zivile Freiheiten und Sicherheit
http://www.infosyssec.com	Ausführliche Informationen zum Thema Internetsicherheit
http://www.root-core.com	Cracker-Website
http://www.infosecuritymag.com	Website eines Unternehmens im Bereich IT-Sicherheit
http://www.heise.de	Online-Nachrichten
http://www.handelsblatt.com	Das Handelsblatt im Internet
http://www.bmi.gv.at	Bundesministerium für Inneres