Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Institut für Technische Informatik
und Kommunikationsnetze
Computer Engineering and
Networks Laboratory

Wirtschaftliche Auswirkungen von DDoS Attacken auf Backbone-Provider

Semesterarbeit SA-2003.27

D-BEPR

Jürg Schmid (schmijue@student.ethz.ch)
Peter Weigel (peter@weigel.us)

Eidgenössische Technische Hochschule (ETH)
Departement Informationstechnologie und Elektrotechnik
Institut für Technische Informatik und Kommunikationsnetze
Fachgruppe Kommunikationssysteme
Zürich, Schweiz

Zürich, 04. Juli 2003

Dozent:	Prof. Dr. B. Plattner
Betreuer:	T. Dübendorfer
	A. Wagner

ABSTRAKT

Ein infolge von Distributed Denial of Service (DDoS) Attacken gestörtes Backbone-Netz ist nicht mehr in der Lage, seine Aufgaben und Funktionen vollumfänglich zu erfüllen. Für den Backbone-Provider entsteht durch die Beeinträchtigung des Netzes und der Wiederherstellung der vollständigen Funktionsfähigkeit wirtschaftlicher Schaden. Betroffen sind durch eine solche Störung auch Internet Service Provider, Webhoster, Behörden, Universitäten und Unternehmen. Die Erfassung des wirtschaftlichen Schadens ist Ziel dieser Arbeit.

Die Aufgabenanalyse (Kapitel 1) sorgt für Begriffsklarheit. Die Problematik der Aufgabe wird erarbeitet und Ziele werden fixiert.

Die Situationsanalyse (Kapitel 2) umfasst das systematische Durchleuchten der momentanen Situation. Zu diesem Zweck wird zuerst das System definiert. Im Rahmen der Systemabgrenzung wird der Untersuchungsbereich abgesteckt, indem die für die Problemstellung relevanten (System) von den nicht relevanten Elementen abgegrenzt werden. Im Zentrum liegt ein exemplarischer IP-Backbone in der Schweiz. Relevante Elemente sind Kommunikationsnetze, Webhoster, Internet Service Provider sowie Privat- und Firmenkunden. Im zweiten Teil der Situationsanalyse werden das System und die das System bildenden Elemente beschrieben und deren Zusammenwirken erläutert.

Das Lösungskonzept (Kapitel 3) gibt einen Ausblick auf die Vorgehensweise bei der Erarbeitung des wirtschaftlichen Schadens infolge einer DDoS Attacke auf Backbone-Provider. Die Dimensionen Kosten, Zeit und Eintrittswahrscheinlichkeit und deren Einfluss aufeinander werden besprochen.

Kapitel 4 beinhaltet die Darstellung der wirtschaftlichen Auswirkungen einer DDoS Attacke auf Backbone-Provider. Zuerst werden die verschiedenen wirtschaflichen Schadensarten aufgelistet und beschrieben und den einzelnen Systemelementen zugewiesen. Im Weiteren wird der Schadensverlauf als Funktion der Zeit grafisch dargestellt. Wirtschaftlicher Schaden kann mittels Berechnungsansätzen geschätzt werden. Voraussetzung dafür ist die Erhebung von Inputgrössen wie Kosten, Arbeitszeiten, etc. Diese analytische Betrachtung ergänzt die vorangehende grafische Darstellung. Konkrete Beispiele schaffen ein Gespür für die Dimensionen und Grössenordnungen, um die es sich bei einem wirtschaftlichen Schaden infolge einer DDoS Attacke handeln kann. Vergangene Ereignisse und Schadensfälle werden beschrieben und das Schadenspotential bei möglichen Opfern wird aufgezeigt. Schliesslich werden zwei Szenarien einer Störung infolge einer DDoS Attacke auf Backbone-Provider aufgestellt. Aufgrund dieser Szenarien werden konkrete Schadensfälle gerechnet. Es folgt eine Schätzung des Gesamtschadens. Grundlage sind die entwickelten Formeln und grafischen Verläufe.

Zürich, 04. Juli 2003

Jürg Schmid Peter Weigel

ABSTRACT

A backbone network that has been disrupted by a Distributed Denial of Service (DDoS) attack is not able any more to fulfill its tasks and functions completely. Network failure and rebuilding its functionality causes economic harm. Such an incident affects as well Internet service providers, web hosters, public authorities, universities and companies. Objective of the thesis is to evaluate the appropriate economic harm.

In chapter 1 (task analysis) terms are clarified. Major problems are worked out. Objectives are set.

In chapter 2 (situation analysis) a close look at the current situation is taken in a systematic way. For this purpose the system is defined first. Doing this, the problem relevant elements (system) and those that are not, are defined. Showcase is an IP backbone in Switzerland. Relevant elements are communication networks, web hosters, internet service providers and private and corporate clients. The second part of this chapter describes the elements that build up the system and explains how they work together.

The solution concept (chapter 3) gives an outlook over the proceedings of evaluating the economic harm due to a DDoS attack on backbone providers. The dimensions like cost, time and occurrence probability are pointed out.

Chapter 4 evaluates the economic impact of a DDoS attack on backbone providers. The various kinds of economic harm are listed and described, and finally assigned to the system elements. Harm characteristics in function of the time are plotted. It is possible to estimate the dimensions of economic harm caused by backbone failure when inputs like cost, working hours, etc. are known. This rather analytical consideration completes the charts. Concrete examples provide a sense for dimensions of economic harm due to DDoS attacks on backbone providers. To get a deeper insight, past incidents are depicted, followed by an outline of the potential for harm. Finally two scenarios of a disruption due to a DDoS attack on backbone providers are designed. On this basis, calculations for some special cases and for the entire harm are made. They are based on the formulas and the characteristics developed above.

AUFGABENSTELLUNG

Ausgangslage

Mit Distributed Denial of Service (DDoS) Attacken (Dienstunterbindungsattacken mit hoher Angreiferzahl) wird versucht, Server oder Teile der Netzwerkinfrastruktur z.B. durch Überlasten vorübergehend unbenutzbar zu machen. Werden eine grosse Anzahl von Rechnern in einer DDoS Attacke eingesetzt, geraten auch leistungsfähige Infrastrukturen von Backbone-Providern in Gefahr.

Bei Attacken dieses Typs bricht der Angreifer im Vorfeld in eine Vielzahl von Servern ein, um dort ein ferngesteuertes Programm zu installieren, einen sogenannten Trojaner bzw. ein Backdoor-Programm. Diese Rechner werden dann Daemons genannt. Auf ein zentrales Kommando des Angreifers hin beginnen die infizierten Server gleichzeitig die angegriffenen Server mit Datenmüll in Form sinnloser Requests (Abfragen) zu bombardieren, bis die Kapazität der Server ausgelastet ist und sie schliesslich unter dem Ansturm zusammenbrechen. Da die Attacke aus vielen Richtungen gleichzeitig erfolgt, gestaltet sich die Abwehr solcher Angriffe sehr schwierig.

Andere Formen von DDoS Attacken basieren darauf, eine Interaktion zwischen dem Opfer und dem Daemon zu starten und das Opfer dann auf die Reaktion des Daemons warten zu lassen, was - genügend Daemons vorausgesetzt - ebenfalls schnell die Ressourcen des Opfers erschöpfen kann.

Problemstellung

Ein infolge von DDoS Attacken überlastetes Backbone-Netz ist nicht mehr in der Lage, seine Aufgaben und Funktionen vollumfänglich zu erfüllen. Für den Backbone-Provider entsteht durch den Ausfall oder die Beeinträchtigung des Netzes und der Wiederherstellung der vollen Funktionstüchtigkeit wirtschaftlicher Schaden. Betroffen sind durch einen DDoS bedingten Backbone-Ausfall insbesondere ISPs, Webhoster, Behörden, Universitäten und private Firmen. Die Nichterfüllung von in Verträgen mit Kunden festgehaltenen Leistungen (z.B. Netzverfügbarkeit) kann Kosten (z.B. Konventionalstrafen) zur Folge haben.

Ziel

Resultat dieser Semesterarbeit ist ein Überblick über den verursachten wirtschaftlichen Schaden und die diesen Schaden verursachenden Faktoren. Dabei wird von einem prototypischen Szenario einer DDoS Attacke auf Backbone-Provider ausgegangen.

Legitimation

Durch die Betrachtung des wirtschaftlichen Schadens einer DDoS Attacke auf Backbone-Provider lässt sich die wirtschaftliche Bedeutung eines solchen Vorfalls abschätzen. Darauf basierend kann eine fundierte Beurteilung erstellt werden, welcher präventive Aufwand zu deren Verhinderung und Abwehr betrieben werden darf. Hinsichtlich einer möglichen Versicherung solcher Schadensfälle macht eine Erhebung des wirtschaftlichen Schadens Sinn.

Vorgehen

Die Vorgehensweise ist systematisch und wissenschaftlich abgesichert nach den Grundlagen des Systems Engineering.

Situationsanalyse

Im ersten Schritt erfolgt die Einarbeitung in die Thematik von DDoS Attacken auf Backbone-Provider und den daraus entstehenden Schaden auf das Backbone-Netz und das relevante Umfeld. Ein Arbeitsplan mit Zwischenzielen wird erstellt, Informationen gesammelt und Begriffsklarheit geschaffen.

In einem zweiten Schritt wird der IST-Zustand analysiert. Das Backbone-Netz und Umfeld werden abgegrenzt und analysiert. Die kritischen Punkte und Beziehungen werden aufgezeigt.

Im dritten Schritt, der Zukunftsanalyse, werden die zu erwartenden Entwicklungen analysiert, um die zukünftigen, langfristigen Konsequenzen auf das gesamte System zu ermitteln resp. abzuschätzen und um Zukunftsperspektiven aufzuzeigen.

Die Situationsanalyse beschränkt sich auf die Schweiz. Mittels Interviews und Befragungen werden relevante Informationen gesammelt.

Zielformulierung

Ziele aus der Aufgabenstellung werden für die Darstellung des wirtschaftlichen Schadens einer DDoS Attacke auf Backbone-Provider präzisiert und in einem Katalog festgehalten.

Konzeptsynthese

Der wirtschaftliche Schaden von DDoS Attacken auf Backbone-Provider wird dargestellt und anhand des Zielkatalogs validiert.

Termine

Arbeitsbeginn: 31. März 2003
Abgabetermin: 04. Juli 2003

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

ADSL	*Asymmetric Digital Subscriber Line*
ATM	*Asynchronous Transfer Mode*
AUP	*Acceptable Use Policy*
B2B	*Business to Business*
B2C	*Business to Customer*
BNN	*Betriebs Netz Netze*
BSP	*Backbone Service Provider*
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DSL	*Digital SubscriberLine*
FTP	*File Transfer Protocol*
HTTP	*Hyper Text Transfer Protocol*
IP	*Internet Protocol*
ISDN	*Integrated Services Digital Network*
ISP	*Internet Service Provider*
KMU	*Kleinere und mittlere Unternehmen*
LAN	*Local Area Network*
NAP	*Network Access Point*
NMS	*Network Management System*
PoP	*Point of Presence*
QoS	*Quality of Service*
SDH	*Synchronous Digital Hierarchy*
SDSL	*Symmetric Digital Subscriber Line*
SLA	*Service Level Agreement*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
WWW	*World Wide Web*

1 AUFGABENANALYSE

1.1 Begriffsklarheit

1.1.1 DDoS Attacke

Mit Distributed Denial of Service (DDoS) Attacken (verteilte Dienstunterbindungsattacken) wird versucht, Server oder Teile der Netzwerkinfrastruktur durch Überlasten unbenutzbar zu machen. Werden eine grosse Anzahl von Rechnern in einer DDoS Attacke eingesetzt, geraten auch leistungsfähige Infrastrukturen von Backbone Service Providern (BSP) in Gefahr.

Bei einer Variante von DDoS Attacken bricht der Angreifer z.B. im Vorfeld in eine Vielzahl von Rechnern ein, um dort ein ferngesteuertes Programm zu installieren, einen sogenannten Trojaner bzw. ein Backdoor-Programm. Auf ein zentrales Kommando des Angreifers hin beginnen die infizierten Rechner gleichzeitig die angegriffenen Server mit Datenmüll in Form sinnloser Abfragen zu bombardieren, bis die Kapazität der Server ausgelastet ist und sie schliesslich unter dem Ansturm zusammenbrechen. Da die Attacke aus vielen Richtungen gleichzeitig erfolgt, gestaltet sich die Abwehr solcher Angriffe sehr schwierig. Beim Angriffsnetzwerk wird zwischen Master- und Daemon-Systemen unterschieden. Die Master-Systeme werden direkt vom Initianten des Angriffs gesteuert, währenddem die Daemons von den Masters aktiviert werden und das Zielsystem attackieren.

Andere Formen von DDoS Attacken basieren darauf, eine Interaktion zwischen dem Opfer und den Daemons zu starten und das Opfer dann auf die Reaktion der Daemons warten zu lassen, was - genügend Daemons vorausgesetzt - ebenfalls schnell die Ressourcen des Opfers erschöpfen kann.

Der Angriff kann beispielsweise in folgenden Schritten erfolgen:

- Der Angreifer verschafft sich einen gestohlenen Account auf einem Rechnersystem. Es handelt sich dabei meistens um ein System mit vielen Usern und hoher Bandbreite. Somit kann er seine Anwesenheit verdecken. Dieser Account dient als Speicher für die Angriffs-Werkzeuge wie Master- und Daemonprogramme, Scanning-Programme, etc. Der Angreifer kann auch mehrere solcher Speicher besitzen, so dass bei Entdecken eines Speichers auf einen anderen Speicher zurückgegriffen werden kann.

- Mittels eines Scanning-Programms aus dem Speicher wird ein Scan grosser Netzteile zur Identifizierung von Schwachstellen durchgeführt. Es werden Systeme gesucht, die Dienste anbieten, über die der Angreifer zum Beispiel durch Ausnutzung von Implementationsfehlern an Administrator-Rechte gelangt.

- Nachdem bekannt ist, auf welchen Systemen welche Sicherheitslücken vorliegen, generiert der Angreifer ein Script, welches diese Lücken angreift. Somit gelangt er effektiv an eine Vielzahl von Rechnersystemen, wo er Administrator-Rechte besitzt.

- Nun wird das Angriffsnetzwerk festgelegt. Der Angreifer bestimmt Daemon- und Mastersysteme.

- Der Angreifer führt ein Script aus, welches die Liste der „in Besitz genommenen“ Rechner benutzt und ein weiteres Script erzeugt, das den Installationsprozess automatisiert als Hintergrundprozess durchführt. Diese Automatisierung erlaubt den Aufbau eines weit verbreiteten Denial of Service Netzes ohne Wissen der eigentlichen Besitzer der Systeme. Es werden die Daeomonprogramme installiert.

- Die Masterprogramme werden vor allem auf Systemen installiert, die über eine grosse Anzahl von Netzwerkverbindungen verfügen. Weiter findet von bzw. zu solchen Systemen meist ein grosser Netzwerkverkehr statt. Dies verdeckt die Aktivitäten bzw. den Netzwerkverkehr der Master. Des Weiteren werden solche Systeme selbst bei Verdacht auf Distributed Denial of Service Attacken nicht so schnell aus dem Netz genommen, da ihre Bedeutung für das eigene Netz zu gross ist.

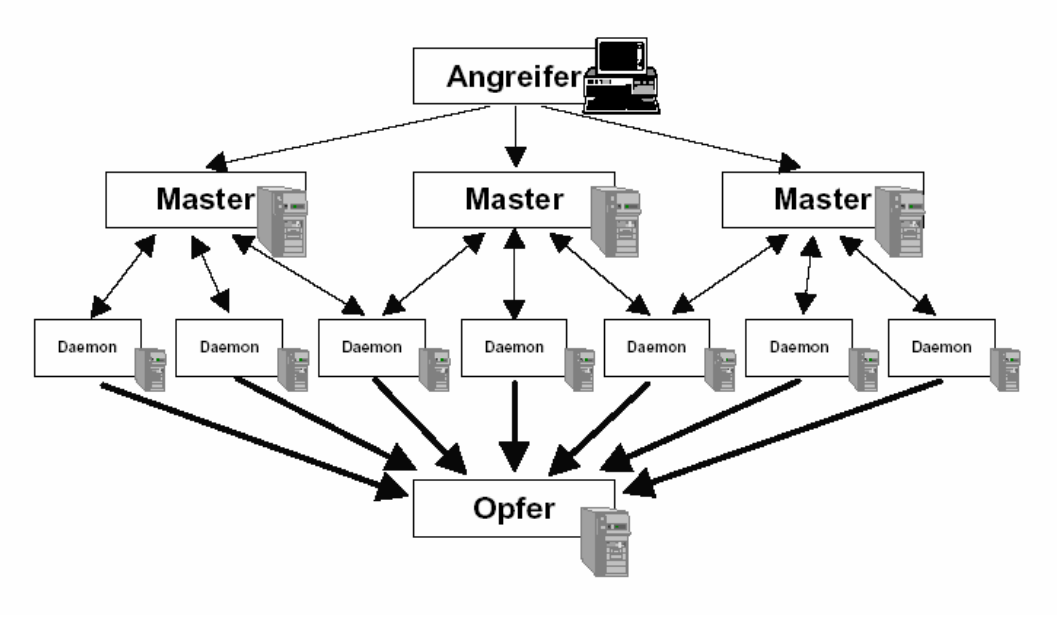

Abbildung 1-1: DDoS Netzwerk [MV00]

Die Vorbereitungen für einen Angriff sind abgeschlossen. Das Angriffsnetzwerk ist aufgebaut, und der eigentliche Angriff kann ausgeführt werden. Der Angreifer kommuniziert z.B. über eine Telnet-Verbindung mit den verschiedenen Mastern. An diese schickt er den Befehl, ein bestimmtes System anzugreifen. Dies ist der einzige Verkehr, der vom Angreifer ausgeht. Danach übernehmen die Master die weitere Steuerung und Koordinierung des Angriffs. Jeder Master steuert dabei eine grosse Anzahl von Daemons. Diese befinden sich auf anderen Systemen und können sich weit verstreut im Netz verteilen. Erst die Daemonsysteme führen auf Anweisung eines Masters den eigentlichen Angriff aus [MV00].

1.1.2 Backbone

Der Backbone ist das Rückgrat in Datennetzwerken - egal, ob es sich um ein internes Firmennetz (LAN-Backbone) oder ein Weitverkehrsnetz (WAN-Backbone) handelt.

Backbones spielen im Internet eine wichtige Rolle. Der Internet-Backbone verbindet über leistungsstarke Leitungen grosse Verkehrssammelpunkte weltweit. Er verfügt über eine weitaus höhere Übertragungskapazität als die angeschlossenen Netze.

Allerdings gibt es nicht *den* Internet-Backbone, da grosse Carrier wie z.B. Swisscom oder WorldCom in der Schweiz oder AT&T oder Cable&Wireless in den USA eigene Backbone-Netze betreiben, an deren zentrale Knoten wiederum Internet Service Provider (ISP) angeschlossen sind. Grosse Internet-Austauschknoten bringen die Backbone-Betreiber zusammen.

1.1.3 Schaden

Schaden beeinflusst die Wirtschaftlichkeit des geschädigten Unternehmens. Wir unterscheiden zwischen direktem wirtschaftlichem Schaden (z.B. Umsatzausfall) und indirektem wirtschaftlichem Schaden (z.B. Imageverlust).

1.2 Problematik und Ziel der Arbeit

Das Internet ist ein weltweites, denzentrales Rechnernetz, das verschiedene Netzwerke untereinander verbindet. Mittlerweile sind rund 30 Mio. Rechner daran angeschlossen [IL03]. Alle am Internet beteiligten Knotenrechner sind gleichberechtigte Partner. Es existiert keine Netzleitstation. Ohne geeignete und auf entsprechende Bedrohungen ausgerichtete Schutzmassnahmen ist das Internet ein unsicheres System. Die Hauptgefahren der Internetbenützung sind [BZ96]:

- Unberechtigte Beschaffung von schützenswerten Daten und Informationen
- Nicht autorisierter Zugriff auf Systeme und Anwendungen
- Verlust der Integrität
- Verhinderung des ordnungsgemässen Netzbetriebs

Werden wichtige Elemente des Internets, wie z.B. Backbone-Leitungen oder Domain Name Server (DNS-Server) angegriffen und in ihrer Kapazität beeinträchtigt, so ist ein grosser Teil des Netzverkehrs betroffen. Es entsteht Schaden, dessen Quantifizierung anspruchsvoll ist. Sicher ist, dass immer mehr Firmen einen Teil oder alle ihre Einnahmen über das Internet oder in elektronischen Märkten erwirtschaften und somit permanent der Gefahr solcher Schadensfälle ausgesetzt sind. Im Hinblick auf eine Versicherung von „Internet-Risiken“, aber auch auf eine Evaluation von sinnvollen Präventivmassnahmen ist es von Vorteil, den wirtschaftlichen Schaden abschätzen zu können.

Ziel dieser Semesterarbeit ist, die Wirkungszusammenhänge und Schadensfolgen im wirtschaftlichen Sinn bei einer DDoS Attacke auf Backbone-Provider aufzuzeigen.

1.3 Bestehende Arbeiten

Wir haben keine veröffentlichten Arbeiten in der Schweiz gefunden, die sich mit dem Problem, wirtschaftlichen Schaden aufgrund einer DDoS Attacke auf Backbone-Provider zu erheben, auseinandersetzen. Natürlich machen Unternehmen, deren Geschäftstätigkeit stark vom Funktionieren der Kommunikationsmittel wie Internet abhängen, Risikoanalysen und –abschätzungen. Diese sind jedoch in der Regel vertraulich und somit nicht öffentlich zugänglich.

Dennoch findet man Schätzungen über Schadensgrössen infolge von DDoS Attacken, vor allem in den USA [DD01]. Diese Schätzungen sind jedoch in den wenigsten Fällen nachvollziehbar, da nicht beschrieben wird, wie sie zustande kommen. Sie vermitteln aber ein Gespür für die Grössenordnung, um die es sich bei solchen Vorfällen handeln kann.

David A. Patterson von der Computer Science Division der University of California in Berkeley hat in dem Papier “A Simple Way to Estimate the Cost of Downtime” [PA02] versucht, eine einfache und nützliche Abschätzung der Kosten infolge der Nichtverfügbarkeit eines Computernetzes zu machen. Zentrale Idee in seiner Arbeit ist, nicht nur die Kosten infolge von Umsatzausfällen zu betrachten, sondern auch die verringerte Produktivität von Mitarbeitern, deren Tätigkeiten durch die Störung eines Kommunikationsneztes gestört sind, in die Rechnung miteinzubeziehen.

„Versicherung von Internet-Risiken“ [LH01] gibt einen Überblick über bestehende Internet-Risiken und deren Versicherbarkeit in der Schweiz.

2 SITUATIONSANALYSE

2.1 Systemabgrenzung

Die zweckmässige Erfassung und Abgrenzung des bearbeiteten Problems ist eine wesentliche Voraussetzung für eine erfolgreiche Problemlösung. Zur Darstellung der wirtschaftlichen Auswirkungen einer DDoS Attacke müssen die betroffenen Elemente und die Beziehungen dieser Elemente untereinander bekannt sein. Weiter wird im Rahmen der Systemabgrenzung der Untersuchungsbereich abgesteckt, indem die für die Problemlösung relevanten (System) von den nicht relevanten Elementen abgegrenzt werden [ZU99].

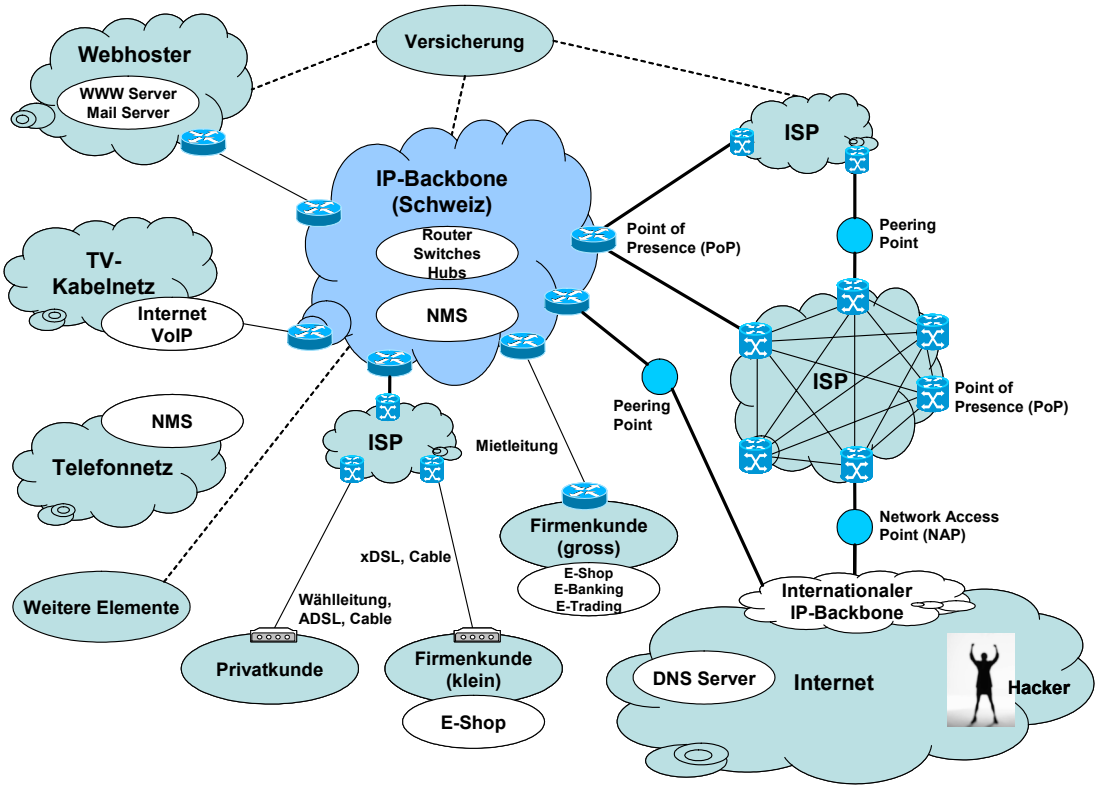

Abbildung 2-1: Betrachtetes System

Die obige Abbildung zeigt den gesamten Problembereich: Entsprechend der Aufgabenstellung wird angenommen, dass ein BSP direkt oder indirekt Opfer einer DDoS Attacke wird. Es wird davon ausgegangen, dass der angreifende Hacker anonym aus dem Internet agiert. Im Zentrum der Betrachtung steht der Betreiber eines exemplarischen IP-Backbone-Netzwerks in der Schweiz. Da dieser Backbone im Wortsinn das Rückgrat einer Reihe von Diensten bildet, hat dessen Störung besonders weitreichende Konsequenzen. Zum einen sind natürlich Verbindungen mit dem Internet betroffen. Zum anderen basieren aber auch andere Dienste, welche noch genauer spezifiziert werden, auf der Infrastruktur dieses Backbones. Um den gesamten wirtschaftlichen Schaden abschätzen zu können, der bei einer Störung des Backbones entsteht, müssen alle Elemente aufgezeigt werden, welche Abhängigkeiten zum Backbone-Netzwerk aufweisen und bei einer Störung dieses Netzwerks ebenfalls einen wirtschaftlichen Schaden verursachen bzw. erleiden.

Diese Elemente werden nun im weiteren Verlauf dieser Arbeit detaillierter betrachtet und beschrieben.

2.2 Internet

2.2.1 Hacker

Hacker war ursprünglich die Bezeichnung für einen Software-Entwickler. Heute wird der Ausdruck vor allem für Personen benutzt, die sich unerlaubt Zugang zu Computersystemen verschaffen.

Die Begriffe Hacker und Cracker werden heute meist synonym verwendet. Manche wollen jedoch zwischen Hackern und Crackern nach dem Maß ihrer kriminellen Energie unterscheiden: Hacker dringen demnach eher aus sportlichem Ehrgeiz in fremde Computersystem ein und richten dort keine dauerhaften Schäden an, während Cracker aus kriminellen Motiven in fremde Netze eindringen und sich dort nicht auf das Ausspähen fremder Daten beschränken, sondern z.B. auch Daten verfälschen [IL03].

Hacker können einzeln oder in Gruppen agieren. Bei einer DDoS Attacke ist es möglich, dass der Angriff von einer einzelnen Person ausgeht, die sich mehrerer Rechner im Internet bemächtigt hat und diese für ihre Absichten nutzt. Die Ressourcen, über die ein Hacker persönlich verfügen muss, um Angriffe zu unternehmen, sind klein. Meist genügt ein normaler Rechner mit Anbindung ans Internet. Wichtig ist das Wissen, wie eine Attacke durchgeführt werden muss und welche Mittel dabei eingesetzt werden können.

Hacker müssen jedoch nicht zwangsläufig von aussen gegen ein Ziel agieren. Es ist vorstellbar, dass ein Mitarbeiter gegen seine Firma von intern „hackt“. Dabei ist das Schadenspotential für die Firma oft grösser, da der Hacker über vertrauliche interne Informationen verfügt, die er für seine Absichten einsetzen kann. Es muss aber unterschieden werden, ob Schaden bewusst oder unbewusst sozusagen durch menschliches Versagen angerichtet wird [BU03].

Die Möglichkeit, in Rechnernetze und –systeme einzudringen, Daten zu lesen oder zu manipulieren und das System somit zu stören wird auch in Zukunft immer mehr an Bedeutung gewinnen. Eine Bedrohung erwächst aus der Möglichkeit des Cyber-Terrorismus. Es ist denkbar, dass die Steuerung lebenswichtiger Infrastrukturen (z.B. Wasserversorgung) durch DDoS Attacken gestört wird.

2.2.2 Globales Internet

Mehr als 600 Mio. Benutzer zählte das Internet weltweit im September 2002 [NUA03a]. Etwa 36 Mio. davon sind mit einer Digital Subscriber Line (DSL) Verbindung daran angeschlossen [NUA03b]. Dies zeigt das enorme Potential an Rechnern, welche in einer DDoS Attacke als Daemon eingesetzt werden könnten.

Am 22. Oktober 2002 kam es zur bisher grössten DDoS Attacke auf die Root Server des Internets. Alle 13 Domain Name System (DNS) Root Server wurden attackiert, 9 davon waren in der Folge nicht mehr funktionsfähig. Alle BSPs in den USA erlitten massive Paketverluste auf ihren Netzen. Dennoch konnten die verbleibenden 4 DNS Root Server die höhere Last problemlos verkraften [ITR02]. Dass es zu keinen weitreichenden Ausfällen im Internet kam, war primär der DNS-Struktur des Internets zu verdanken: Erstens sind die Name Server auf allen Ebenen jeweils redundant vorhanden, zweitens werden Informationen zwischengespeichert (Cache), weshalb nicht bei jeder Anfrage auf die Root Server zugegriffen werden muss [PE00]. Dies ist auch der Grund, weshalb die Auswirkungen der DDoS Attacke auf den weltweiten Internetverkehr gering waren. Die Attacke zeigte jedoch, dass die zur Verfügung stehenden Ressourcen bereits heute ausreichen, um wichtige Elemente der Internet-Infrastruktur lahm zu legen.

Im Rahmen dieser Arbeit wird die Situation in der Schweiz betrachtet. Eine Attacke auf DNS Root Server liegt deshalb ausserhalb des Untersuchungsbereichs. Die weltweiten Abhängigkeiten im Internet zeigen jedoch, dass eine Betrachtung der Situation in der Schweiz nicht vollständig isoliert erfolgen darf.

2.2.3 Marktsituation in der Schweiz

Das Internet ist in der Schweiz nach wie vor auf dem Vormarsch. Im März 2003 nutzten in der Schweiz 3,475 Mio. Menschen das Internet, das sind 61,4% der Schweizer Bevölkerung [IR03]. Gegen 100 ISPs sind auf dem Schweizer Markt tätig [CA02], wobei Bluewin als grösster Provider einen Marktanteil von 47% hält (Stand September 2002) [BW02]. Die nach wie vor steigende Bedeutung und Beliebtheit des Internets wird auch in der Nachfrage nach Breitband-Internet-Anbindungen sichtbar: Gegen 500'000 Breitband-Internet-Anschlüsse waren in der Schweiz Ende 2002 aktiv, wovon mehr als 200'000 auf Asymmetric Digital Subscriber Line (ADSL) und über 260'000 auf Kabel-Internet entfallen [SC03a, CM03]. Nicht nur Privatkunden nutzen diese Art der Internet-Anbindungen, sondern zunehmend auch kleinere Firmen als preisgünstige Alternative zu teuren Mietleitungen. Aus diesem Grund bietet z.B. Bluewin speziell für Firmenkunden auch symmetrische DSL (SDSL) Verbindungen mit jeweils 512 kbit/s Up- und Down-Stream und statischer IP-Adresse an [BW03a]. Der Betrieb eines eigenen Web-Servers ist daher so einfach und günstig wie nie zuvor.

Aus diesen Zahlen wird ersichtlich, wie weit das Internet bereits in der Bevölkerung und in der täglichen Kommunikation von Privaten und Firmen verankert ist. Die grosse Verbreitung des Internets macht zum einen die Abhängigkeit vieler Privatpersonen und Firmen von diesem Medium deutlich, zum anderen ergeben sich genau durch diese grosse Verbreitung und die damit verbundene grosse Anzahl an Servern und Clients neue Angriffspunkte für Hacker.

2.3 IP-Backbone

Die Betrachtungen beziehen sich auf ein IP-Backbone-Netzwerk in der Schweiz.

2.3.1 Aufbau

Points of Presence (PoP) sind Anschlusspunkte für den Zugang zum IP-Backbone. Sie sind je nach Datenverkehrsaufkommen geografisch verteilt und bestehen in erster Linie aus Routern, die den IP-Verkehr durch den Backbone leiten. Glasfaser- oder Kupferleitungen verbinden die PoPs untereinander. Im Gegensatz zu den normalen elektromagnetischen Übertragungen auf Kabeln oder metallischen Leitern, die im Bereich der Mega- und Gigahertz-Frequenzen stattfinden, bewegt sich die Übertragung von Licht in der Grössenordnung von Terahertz-Frequenzen. In diesen hohen Frequenzen ist die verfügbare Bandbreite sehr gross und erlaubt die Übermittlung von grossen Datenmengen [NZZ00]. Zur Zeit werden in der Praxis in Glasfasernetzen Datenübertragungsraten von 2,5 Gbit/s je Faser erreicht. Unter Laborbedingungen sind Bandbreiten bis zu 10 Gbit/s möglich [IL03]. Im Internet sind digitale Daten, welche auf Servern irgendwo auf der Welt abgespeichert sind, meist weit entfernt vom Ort, wo der Internet-User den Zugriff darauf sucht. Folglich findet ein zunehmender Anteil des Datenverkehrs auf Fernnetzen und damit auf Glasfaser-Backbones statt [NZZ00]. Aus Sicherheitsgründen werden die Backbones mit Redundanz ausgestattet. So besteht jeder PoP aus mehreren Routern, die untereinander verbunden sind und im Notfall die Funktionsfähigkeit des PoP alleine aufrechterhalten können. Des Weiteren sind die wichtigsten Verbindungen zwischen den PoPs redundant ausgelegt.

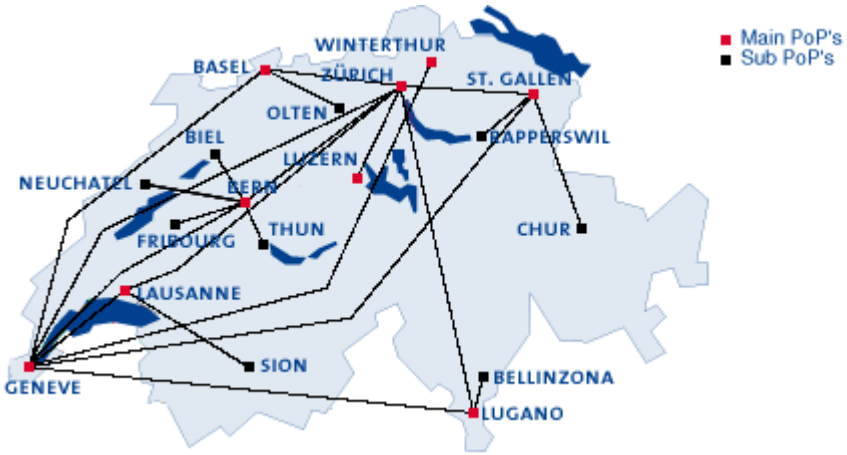

Abbildung 2-2: Swisscom IP-Backbone [IP03]

Auf den unteren zwei Ebenen des OSI-Modells (physical, data link) agiert das Backbone-Netz als reines Transportnetz mit wenig Intelligenz, weshalb es hier auf Störungen nicht sehr anfällig ist. Die Angriffsziele für DDoS Attacken sind jedoch auf den darüber liegenden Ebenen (network, transport, application) zu suchen, deren Dienste von einem reinen Transportnetz nicht bereitgestellt werden [EP03].

Die Anbindung ans globale Internet erfolgt via ISP oder via Internet Exchange Points mit anderen Backbone-Providern, u.a. durch Verbindungen zu den führenden internationalen Anbietern (Global Providers).

Die Bandbreiten der Backbones sind gross. Sunrise z.B. bietet einen Backbone, der national über eine Bandbreite von n x 2,5 Gbit/s verfügt. Die Peering-Kapazität von Sunrise innerhalb der Schweiz beläuft sich auf > 1,2 Gbit/s [SR03]. Dank dieser grossen Bandbreiten ist die Auslastung bei normalem Verkehrsaufkommen verhältnismässig klein. Der Quality of Service (QoS) Level kann durch die Reserve an Bandbreite gewährleistet werden. Einzig in Ballungszentren, wo die Konzentration von ISPs und PoPs zunimmt, werden Grenzen der Auslastung der Netzelemente erreicht. Ab 80% Auslastung kann der Verlust von Datenpaketen infolge zu geringer Kapazitäten der Bufferspeicher signifikant zunehmen [EP03].

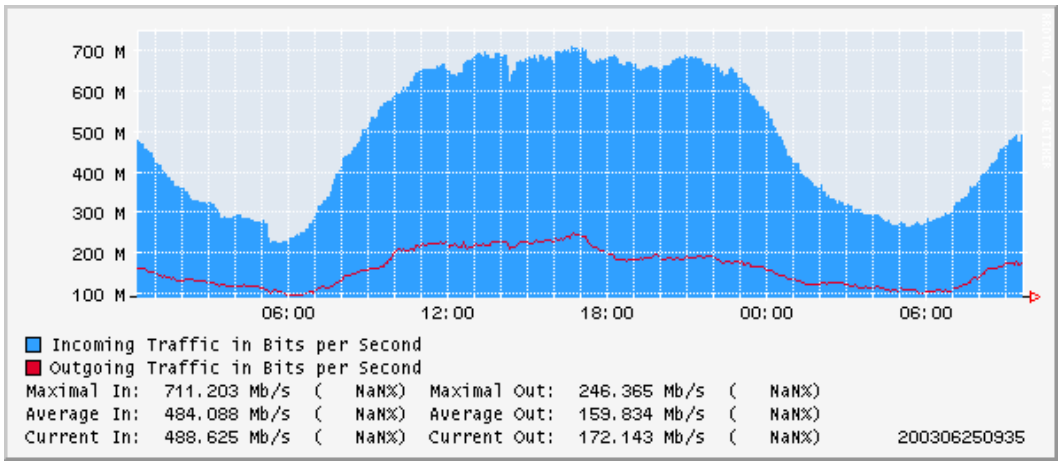

Abbildung 2-3: Datenverkehr zwischen Zürich und Genf (Swisscom IP-Backbone) [IP03]

2.3.2 Anbindung der ISPs

Endkunden sind via Backbone über ihren Internet Service Provider (ISP) mit dem Internet verbunden. Die BSPs führen sogenannte Acceptable Use Policies (AUP). Diese regeln die rechtlichen Verhältnisse zwischen dem BSP und dessen Kunden. So behält sich zum Beispiel IP-Plus, der BSP von Swisscom, das Recht vor, bei Bedrohung der Sicherheit des eigenen Netzes oder des Netzes eines Kunden, diese Gefahr mit geeigneten Massnahmen zu bekämpfen. Die Massnahmen reichen von der Abkopplung von Kunden-Sites, von welchen solche Tätigkeiten ausgehen, über Unterbruch des Datenverkehrs zum Geschädigten bis zur vollständigen Abkopplung des Kundennetzes [IP03].

Aus Sicherheitsgründen verfügt ein ISP in der Regel über mehrere Leitungen zu einem oder mehreren Backbones.

2.3.3 Sicherheitsmassnahmen

Die Sicherheitsmassnahmen bei einem BSP lassen sich in Präventiv- und Sofortmassnahmen unterteilen.

Zu den präventiven Massnahmen gehört die Netzüberwachung. Dabei kann sowohl das Verkehrsaufkommen als auch die Charakteristik der gesendeten Datenpakete untersucht werden. Kritische Netzelemente werden redundant gehalten, so dass ein Funktionsausfall aufgefangen werden kann. Das Network Management System (NMS) wird örtlich verteilt, so dass in einem Schadensfall, der sich auf einen geografischen Ort beschränkt, die Steuerung aufrecht erhalten werden kann. Firewalls regeln den Datenverkehr zwischen dem Backbone und anderen Rechnern und Netzwerken. Ein weiteres Mittel zur Sicherung des Datenverkehrs ist der Einsatz von abgeschotteten Netzen. In einem Virtual Private Network (VPN) werden die Leitungen des Backbones in einer Weise genutzt, als wären sie Teil eines privaten Leitungsnetzes. Für zusätzliche Sicherheit können die zu einem VPN gehörenden Rechner ihre Daten auch in verschlüsselter Form austauschen. Mit Hilfe dieser besonders gesicherten Leitungen werden zum Beispiel die LAN eines Unternehmens mit mehreren Standorten bei Bedarf untereinander zu einer Art Extranet verbunden (siehe Kapitel 2.5.2) [EP03, IL03].

Durch präventiven Schutz wird versucht, das Risiko eines Schadensfalls zu minimieren. Da sich die Bedrohungsformen jedoch sehr schnell ändern, lässt sich ein Restrisiko nicht ausschliessen. Mittels Plänen für Sofortmassnahmen kann auf eintretende Gefahren schnell reagiert werden.

2.3.4 DDoS Attacken

Kritische Elemente eines Backbones bezüglich DDoS Attacken sind hauptsächlich Router und Switches. Sie sind zuständig für das Weiterleiten der Datenpakete an die im Paket spezifizierte Zieladresse. Deshalb sind diese Geräte in hohem Masse redundant im Netz. Im Allgemeinen sind diejenigen Elemente des Backbone-Netzes bezüglich DDoS Attacken anfällig, welche Daten verarbeiten. Diese können durch einen Überlauf ihres internen Buffers den betroffenen Rechner lähmen oder sogar zum Absturz bringen.

Mittels Tunneling werden VPN gebildet. Tunneling dient dazu, Daten über ein unsicheres öffentliches Netz, wie das Internet, zwischen einem zentralen VPN Gateway und einem Remote VPN Client zu transportieren. Dabei wird zwischen den Endpunkten eine virtuelle Verbindung aufgebaut. Ein Tunnel wird dadurch aufgebaut, indem jedes Datenpaket einen zusätzlichen IP-Header erhält, darüber hinaus ein oder mehrere spezielle Kopffelder. Der Anfangspunkt des Tunnels ist dort, wo der IP-Header hinzugefügt wird, der Endpunkt, wo dieser wieder entfernt wird. Die eigentlichen Nutzdaten können zusätzlich auch verschlüsselt übertragen werden [SI03]. Diese Methode kann auch innerhalb des IP-Backbones angewandt werden. Datenpakete, die den Backbone betreten, werden in ein IP-Paket verpackt und so durch den Backbone zur Zieladresse geschleust. Ein Ausbrechen aus dem VPN ist deshalb nicht möglich.

Sehr kritisch ist der Angriff auf Elemente des NMS. Es handelt sich dabei um Schlüsselelemente. Denkbar ist ein Angriff auf den Server, der für die Authentifizierung der Kunden zuständig ist. Ist dieser nicht mehr verfügbar, so können sich die Kunden nicht mehr einloggen. Die Elemente des NMS sind jedoch aus dem Internet nicht erreichbar.

Die Manipulation von Routing-Tabellen bzw. von Parametern der Routing-Protokolle kann zur Überlastung einzelner Verbindungen im Backbone führen. Um Netzelemente zu rekonfigurieren ist jedoch Insiderwissen notwendig. Passwörter müssen bekannt sein [EP03].

Es existieren wenige Mittel, um von Profis durchgeführte DDoS Attacken zu verhindern. Die Herkunft der Angreifer ist infolge von Verschleierungsmechanismen und durch die grosse Anzahl involvierter Rechner und Verbindungen kaum feststellbar. Durch den Einsatz von Bandbreiten-Limiter kann lediglich das Überschreiten einer bestimmten Auslastung verhindert werden. Diese Geräte sind teuer, die maximale Bandbreite der Verbindung muss de facto erhöht und der Limiter darf nicht selber Opfer einer DDoS Attacke werden. Nicht vernachlässigt werden darf die Möglichkeit des Angriffs auf das Backbone-Netzwerk von innen. Sind Sicherheitsmechanismen und Passwörter bekannt, besteht die Möglichkeit, das Backbone-Netz zu stören [BU03].

2.4 Internet Service Provider

2.4.1 Verbindungsglied zum Internet

Die ISPs stellen für die Endkunden die Angliederung zum eigentlichen Internet dar: Sie sind mit den europäischen bzw. internationalen Backbones verbunden, zu welchen es z.B. in Zürich und Genf Zugangspunkte (Network Access Points, NAP) gibt [EP03]. Kritische Netzelemente werden redundant gehalten und Kapazitäten grosszügig ausgelegt.

Ein ISP bietet Internetzugang vor allem für Privatkunden und kleine Firmenkunden (KMU) an. Via Anschlusszentrale und ISP werden die Kunden mit dem Netz des BSP verbunden, welcher wiederum Anbindung an das globale Internet sicherstellt. Viele Kleinfirmen benutzen ihren privaten Internetzugang für ihr Geschäft (verdeckte Firmenkunden) [WI03]. Es ist daher schwierig abzuschätzen, wie die Kundenstruktur eines ISP genau aussieht und wie gross und bedeutend die Abhängigkeiten der einzelnen Kunden vom Funktionieren des Zugangsdienstes sind.

Viele ISPs bieten neben dem Zugangsdienst noch zusätzliche Dienste an. Unter anderem funktionieren sie auch als Hosting-Provider (siehe Kapitel 2.6). Bluewin, der grösster ISP in der Schweiz, zählt auch zu den grössten Hosting-Providern [WI03].

Es gibt verschiedene Präventivmassnahmen zur Verhinderung von Schadensfällen, die Kunden betreffen. Host- und Netzwerk-Sicherheit kümmert sich z.B. darum, dass die Adressen der Netzelemente aus dem Internet nicht sichtbar sind und dass das NMS von der Umwelt abgeschottet wird. Mittels angemessener Skalie-

rung werden ausreichend grosse Kapazitäten zur Verfügung gestellt, die Reserven beinhalten. Ein weiteres probates Mittel bildet die Prüfung der eigenen Netzsicherheit durch externe Spezialisten. Dadurch werden Sicherheitslecks vorzeitig aufgedeckt und behoben [WI03].

2.4.2 DDoS Attacken in der Vergangenheit

Am 15. Februar 2002 wurde der ISP TIC (The Internet Company) mit Sitz in Kriens Opfer einer DDoS Attacke. Da durch den massiv erhöhten Datenverkehr das interne Routing bei TIC zum Erliegen kam, war auch die Anbindung an den Backbone (im Beispiel IP-Plus) nicht mehr gegeben [TIC02]. Dieses Beispiel zeigt, dass die ISPs besonders exponiert sind. Der in diesem Fall involvierte BSP war lediglich an den Schnittstellen zum ISP betroffen, die restliche Infrastruktur wurde jedoch nicht tangiert. Es wird hier also sichtbar, dass eine koordinierte Attacke über Kunden mehrerer ISPs gleichzeitig erfolgen muss, um die Funktion eines Backbones ernsthaft bedrohen zu können.

2.5 Endkunden

2.5.1 Privatkunden

Nach wie vor verbinden sich die meisten Kunden von Zuhause aus über ein Analogmodem oder über Integrated Services Digital Network (ISDN) mit dem Internet. Die Verbreitung von Breitband-Anschlüssen wächst aber rasant (siehe Kapitel 2.2.3). Die ständige Anbindung ans Internet birgt neben dem Komfort einer Standleitung aber auch Gefahren: Besonders private Computer sind oftmals schlecht gewartet, haben viele Sicherheitslücken und sind somit ideale Angriffspunkte für Hacker. Einerseits ist die Gefahr gross, dass persönliche Daten von einem solchen Computer gestohlen werden, andererseits macht die relativ grosse verfügbare Bandbreite diese Computer auch attraktiv als Daemons in DDoS Attacken (siehe Kapitel 1.1.1) [NUA00].

Die Breitband-Internet-Zugänge für Privatpersonen, welche z.B. Bluewin oder Cablecom anbieten, sind nichts desto trotz nicht vergleichbar mit der Mietleitung einer Firma. Zum einen garantieren die Anbieter von ADSL oder Kabel-Internet keinerlei QoS, lediglich ein „Best Effort“ wird geboten. Weder die Bandbreite noch die Verfügbarkeit der Anbindung wird den Privatkunden zugesichert. Zum anderen basieren auch die Service-Leistungen dieser Anschlüsse auf dem gleichen Prinzip. Eine sofortige Fehlerbehebung oder auch Konventionalstrafen bei Nichterfüllen der Verträge sind daher nicht vorgesehen [BW03b].

2.5.2 Firmenkunden

Firmenkunden haben vielfältige Ansprüche an das Backbone-Netzwerk: Zum einen dient es als Verbindung zu einem ISP und somit zum Internet, zum anderen werden bei grossen Firmen auch verschiedene Firmenstandorte darüber vernetzt. Swisscom bietet für Firmenkunden zum Beispiel das Produkt „LAN-I“ (LAN In-

terconnect Service) an, welches als VPN aufgefasst werden kann. Ein vergleichbares Produkt für kleine Firmen nennt sich „Office Connex“ [SCES03a]. Der LAN-I Service läuft entweder über Frame Relay oder über den IP-Backbone von Swisscom (IPSS). Hier zeigt sich, wie abhängig die interne Kommunikation vieler Firmen von einem funktionierenden IP-Backbone ist. Neben vielen Grossfirmen, Banken und der Börse sind auch zahlreiche KMU auf dieses Kommunikationsmittel angewiesen [BU03]. Anders als bei den Privatkunden sind z.B. bei LAN-I verschiedene SLAs erhältlich. Auch Konventionalstrafen sind explizit vorgesehen [SCES03b]. Kleine Firmen jedoch, welche auf einen günstigen ADSL-Anschluss ausweichen, kommen nicht in den Genuss besonderer Service-Leistungen. Sie werden z.B. bei Bluewin gleich behandelt wie alle anderen Kunden auch und erhalten keinerlei Garantien bezüglich QoS oder Verfügbarkeit [BW03b].

Immer mehr Unternehmen erwirtschaften einen Teil ihres Umsatzes über das World Wide Web (WWW). Sie profitieren dabei vor allem von tieferen Transaktionskosten. Die auf den Versandhandel von Hardware, Software und EDV-Zubehör spezialisierte Arp-Datacon-Gruppe mit Sitz im zugerischen Rotkreuz erwirtschaftet zum Beispiel bereits 40% ihres Umsatzes mit dem Online-Shop, wobei 33% über den Internet-Shop und 7% durch Business-to-Business-Transaktionen anfallen. Die Firma eröffnete 1999 einen auf SAP/R3 basierenden Online-Shop. Dank einer integrierten Prozesskette von der Lagerbewirtschaftung über das Rechnungswesen bis zur Kundenverwaltung profitierte Arp Datacon letzes Jahr von einer Kostenersparnis von rund 50% gegenüber konventioneller Bestellung [NZZ02a].

Doch das Geschäft mit E-Commerce ist nicht ohne Risiken. Die Abhängkeit von der Technologie nimmt zu. Der Umsatz ist abhängig von der Verfügbarkeit des Internet-Dienstes. Vor allem reine Online-Shops sind durch die sogenannten E-Risiken besonders bedroht, währenddem Unternehmen, die ihre Produkte auch über konventionelle Kanäle verkaufen, über eine gewisse Redundanz verfügen.

Ebenfalls zu erwähnen ist die steigende Bedeutung des elektronischen Zahlungsverkehrs: E-Banking gehört mittlerweile zum Standardangebot der Grossbanken und wird sowohl von Firmenkunden als auch von Privatkunden genutzt. Ein Ausfall bzw. eine Beeinträchtigung dieser Services hätte weitreichende Konsequenzen. Zahlungen könnten nicht mehr (oder nur noch verzögert) ausgeführt werden. Neben dem eigentlichen Internetzugang ist allenfalls auch die Interkonnektion der Banken sowie die Verbindung zu den Bankomaten etc. gestört (siehe Kapitel 2.9). Ein Ausweichen auf die telefonischen Dienste der Banken oder auch auf die „klassischen“ Einzahlungsscheine wäre also in vielen Fällen auch nicht möglich.

2.6 Webhoster

Am Internet angeschlossene Rechner sind Server oder Client. Server bieten im Internet Dienste an. Clients machen von diesen Diensten Gebrauch. Es gibt unter anderem Web Server, E-Mail Server oder File Transfer Protocol (FTP) Server. Jeder Server macht seine Dienste im Internet über nummerierte Ports verfügbar. Eine Portnummer steht für einen verfügbaren Dienst. Wenn ein Rechner als Web Server konfiguriert ist, ist dieser Dienst auf Port 80 verfügbar. Ein FTP Server ist

auf Port 21 ansprechbar. Falls ein Server Verbindungen auf einem Port von extern, also aus dem Internet, erlaubt und keine Firewall den Zugang schützt, kann jeder Teilnehmer im Internet über diesen Port vom angebotenen Dienst Gebrauch machen. Clients verbinden sich mit einem Dienstanbieter über eine spezifische IP-Adresse auf einem spezifischen Port. Besteht die Verbindung zwischen Client und Server auf einem Port, so greift der Client über ein spezielles Protokoll auf den Dienst zu. Wird eine Website abgerufen, handelt es sich um das Hypertext Transfer Protocol (HTTP).

Für unsere Betrachtungen ist die Konfiguration eines Rechners als Web Server von besonderem Interesse. Über eine Website, die im ganzen Internet abrufbar ist, können Produkte oder Dienstleistungen angeboten, vertrieben und bezahlt werden. Beim E-Commerce handelt es sich um über Datennetze abgewickelten Geschäftsverkehr.

Jeder Rechner kann mit entsprechender Software als Web Server konfiguriert werden. Eine Anbindung ans Internet ermöglicht weltweiten Zugriff auf die darauf abgelegten Websites. Webhoster verfügen über eine Anzahl leistungsfähiger WWW Server, konzentriert an einer Lokalität (Hostfarmen), deren Speicherplatz sie Unternehmen zum Betrieb ihrer Websites vermieten. Durch Unterhalt und Wartung wird der Service erweitert. Der Aufbau und die Gestaltung der Website ist Sache des Unternehmens, das ins Online-Geschäft einsteigen will. Die Webhoster sind über ISP und IP-Backbone mit dem Internet verbunden und somit verantwortlich, dass die auf ihrem Speicher abgelegten Websites mit genügend grosser Bandbreite und somit Verfügbarkeit abgerufen werden können. Der QoS ist Gegenstand des Vertrags zwischen Webhoster und dem Unternehmen, das eine Website unterhält.

2.7 Versicherungen

Immer mehr Unternehmen sind auf dem Internet präsent und erwirtschaften Teile ihres Umsatzes über das Internet oder auf elektronischen Märkten. Neben den traditionellen Risiken entstehen somit neue Risiken, die bisher unbekannt waren - E-Risiken.

DDoS Attacken zielen auf die Störung der Verfügbarkeit von Dienstanbietern ab. Es ist z.B. möglich, dass infolge einer DDoS Attacke Homepages von Unternehmen für eine gewisse Zeit vom Internet verschwinden, da der entsprechende Web Server seinen Dienst nicht mehr erfüllen kann oder durch aufgebrauchte Bandbreite aus dem Internet nicht mehr erreichbar ist. Umsatzausfälle des betroffenen Unternehmens sind die Folge. Betriebsunterbrechungsversicherungen sind deshalb von besonderem Interesse für Unternehmen, die ihre Waren oder Dienstleistungen zumindest teilweise über das Internet absetzen. Weitere Risiken bestehen im Anfallen von Kosten durch Wiederherstellung des ursprünglichen Zustands des attackierten und geschädigten Netzes und der Geräte, Imageverlust und Haftpflichtansprüche von Dritten [LH01].

Traditionelle Versicherungskonzepte sind für eine Industrie entwickelt worden, die in keinen lebenswichtigen Abhängigkeiten von IT-Systemen stand. Die neuen

Gefährdungspotentiale aus dem Internet werden von den bekannten Versicherungsdeckungen nur ungenügend erfasst. Typischerweise verwirklichen sich diese Risiken eben nicht als Körperschäden oder Schäden an materiellen Sachen, sondern als reine Vermögensschäden, die von der Haftpflichtversicherung eines Unternehmens üblicherweise nicht abgedeckt sind [UB02].

Risiken sind nur vernünftig versicherbar, wenn sie sich einschätzen lassen. Im Internet ist dies sehr schwierig. Dies hat verschiedene Gründe. Auf der einen Seite existieren wenige Erfahrungswerte aus der Vergangenheit. Anderseits wandelt sich das Internet so schnell, dass es schwierig ist, Standards zu erarbeiten. Des Weiteren sind immaterielle Schäden schwer quantifizierbar. Immaterieller Schaden wie z.B. Imageverlust muss in messbare Kriterien wie Kundenabgang aufgeschlüsselt werden. Infolge dieser Unsicherheit sind die Versicherungen noch immer sehr teuer. Das Geschäftspotenzial für immer mehr Versicherungsanbieter ist aber zu gross, um es zu ignorieren [DR00].

In der Schweiz bietet die Zürich-Versicherungs-Gesellschaft mit Partnern die Marktleistung „eRisk protection program“ seit Ende Mai 2000 als ganzheitliche Lösung mit diversen Dienstleistungen wie Risikoanalyse, Rechtsberatung und Optimierung der Internet-Security an. Die Versicherungslösung umfasst frei kombinierbare Deckungen: Betriebsunterbrechung, Daten und/oder Software, Public Relations-Kosten, Haftung bei Unterbrechung sowie Haftung bei elektronischer Veröffentlichung. Diese Art von Versicherungen wendet sich in erster Linie an Dienstanbieter wie ISPs, BSPs oder Webhoster. Sie alle wollen sich gegenüber Forderungen ihrer Kunden, die aus einem Dienstunterbruch und somit Nichteinhaltung von in Verträgen festgelegten Leistungen erwachsen, finanziell absichern.

Es ist davon auszugehen, dass die meisten BSPs Konventionalstrafen ablehnen und somit dahingehend kein Versicherungsschutz besteht, da die Prämien zu hoch sind. Es bestehen Best-Effort-Verträge. Hingegen können sich Betreiber für materielle Schäden und Arbeitsstunden infolge von Betriebsunterbrüchen versichern [BU03].

2.8 Andere Netzwerke

2.8.1 Telefonnetz

Das klassische Telefonnetz, basierend auf der Synchronous Digital Hierarchy (SDH), hat auf den ersten Blick keine Beziehungen zu einem IP-Netzwerk [KE97]. Die Kommunikation zwischen NMS und den Netzelementen des Telefonnetzes (Switches) läuft meistens über X.25 und nur in wenigen Fällen über IP. Bei Swisscom wird z.B. über IP kommuniziert, wenn Konfigurationen direkt aus den Call-Centers vorgenommen werden. Der gesamte Verkehr des NMS läuft bei Swisscom jedoch über das separate Betriebs-Netz-Netze (BNN), auch bei Konfigurationen über IP. Das BNN hat wohl Übergänge (via Firewall) zum Intranet, aber keine direkte Verbindung zum IP-Backbone. Das Telefonnetz wird dementsprechend nicht durch Störungen des IP-Backbones tangiert [BU03, EP03].

2.8.2 TV-Kabelnetz

Mit einer steigenden Anzahl an neuen Diensten, welche auf den Netzen der Kabelfernseh-Betreiber angeboten werden, können auch die Beziehungen zu den IP-Backbone-Netzwerken immer enger werden: Neben dem Kabelinternet, welches zwangsläufig auf die bestehende Infrastruktur von BSP und ISP zurückgreift, ist auch ein Telefoniedienst, welcher auf „Voice over Internet Protocol“ (VoIP) basiert, darauf angewiesen. Der Telefoniedienst von Cablecom basiert jedoch auf dem Asynchronous Transfer Mode (ATM) und fällt daher nicht in diese Kategorie [CC03a].

Neben den Angeboten für Privatkunden bieten TV-Kabelnetz-Betreiber aber in zunehmendem Masse auch Produkte für Firmenkunden an. So profitiert Cablecom vom eigenen Backbone-Netzwerk und offeriert eine Vielzahl an Diensten für Firmenkunden wie z.B. Standort übergreifende Firmennetzwerke und Internet Zugänge [CC03b, CC03c].

2.9 Weitere Elemente

Um ein ganzheitliches Bild zu erhalten, müssen weitere Elemente betrachtet werden, welche ebenfalls auf ein funktionierendes Backbone-Netzwerk angewiesen sind. Hier sind insbesondere Services und Applikationen zu nennen, welche elektronisch kommunizieren und so für den Anwender einen Dienst zur Verfügung stellen, z.B.:

- Bankomaten, Kreditkartenleser
- Börse
- Lotto, Sport-Toto
- Interne Bestellabläufe bei Migros und Coop
- Interne Kommunikation SBB
- Interkonnektion der Banken
- Steuerung von Wasser- und Stromversorgung

Ein Ausfall des Backbones beeinflusst diverse Dienste des täglichen Lebens. Nicht nur Privat- sondern auch Firmenkunden sind davon betroffen [BU03].

Bei Kommunikation von Maschinen untereinander (Beispiel EC-System) wäre bei einem Unterbruch des Backbone-Netzwerks mit einem Totalausfall zu rechnen. EC-Transaktionen wären nicht mehr möglich, solange die Hosts von Banken von der Attacke betroffen sind. Beispiel hierfür ist der Absturz des Telekurs-Hosts am letzten verkaufsoffenen Samstag vor Weihnachten 2001. Bankomaten hingegen funktionieren auch offline, jedoch mit eingeschränkter Funktionalität. Die Auswirkungen und Konsequenzen einer Störung hängen hier sehr stark davon ab, wie lange die Banknetze autonom funktionieren können [EP03].

Bei anderen Applikationen ist ein Ausweichen auf alternative Übermittlungsmethoden besser möglich. So können z.B. die internen Bestellabläufe der Grossverteiler in eingeschränktem Masse auch via Telefon und Fax erledigt werden, wobei es auch hier mit zunehmender Dauer der Störung zu Problemen und Personalengpässen durch die „manuellen“ Bestellabläufe kommen dürfte.

3 LÖSUNGSKONZEPT

3.1 Ziele der Lösung

Die Darstellung der Wirkungszusammenhänge und Schadensfolgen bei einer DDoS Attacke (siehe Kapitel 1.2) muss aufgrund der Komplexität des betrachteten Systems in mehreren Schritten erfolgen. Folgende Punkte sollen daher im weiteren Verlauf erarbeitet werden:

- Grafische Darstellung des Schadens über die Zeit
- Formeln zur Berechnung der verschiedenen Schadensarten
- Szenariobildung zur Berechnung exemplarischer monetärer Werte

Die erarbeiteten Instrumente sollen es dem Leser ermöglichen, eigene Berechnungen durchführen zu können. Die Berechnungsformeln müssen in unterschiedlichen Fällen angewandt werden können.

3.2 Vorgehen

Wirtschaftlicher Schaden kann infolge einer technischen Störung des Backbone-Netzwerkes auftreten. Er ist kostenwirksam und schlägt sich in der Erfolgsrechnung einer Unternehmung nieder.

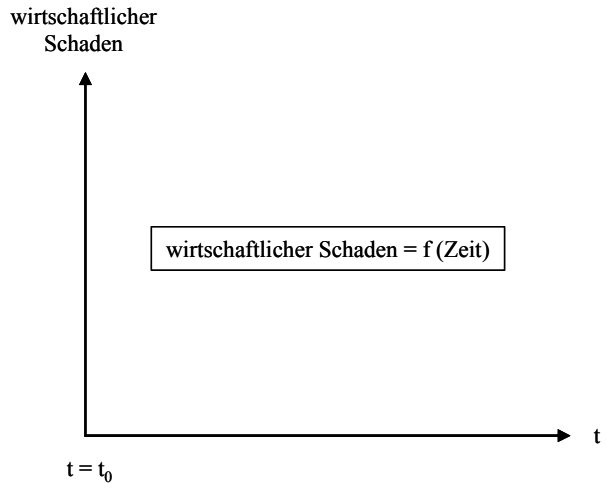

Abbildung 3-1: Schaden als Funktion der Zeit

Wirtschaftlicher Schaden ist eine Funktion der Zeit. Der zeitliche Verlauf der technischen Störung des Backbone-Netzes ist nicht gleich demjenigen des wirtschaftlichen Schadens. Es macht deswegen Sinn, in einer ersten Phase die wirtschaftlichen Schadensarten für $t \rightarrow \infty$ zu betrachten, bevor wir in einer zweiten Phase ein konkretes Schadensszenario annehmen und somit die Störungszeit und das Störungsausmass des Backbones festsetzen. Bei $t = t_0$ tritt die technische Störung ein.

3.3 Eintrittswahrscheinlichkeit

Die Betrachtung des wirtschaftlichen Schadens in Abhängigkeit von der Zeit bildet die Grundlage für weitere Abschätzungen innerhalb dieser Arbeit. Ein finanzieller Wert ist aber für sich alleine wenig aussagekräftig. Vielmehr muss dieser in

Relation zur Eintrittswahrscheinlichkeit eines Schadens gesetzt werden. Ein hoher finanzieller Schaden wird durch eine extrem kleine Eintrittswahrscheinlichkeit deutlich relativiert. Diese umfassende Betrachtung muss z.B. auch angestellt werden, wenn der präventive Aufwand, der zur Verhinderung dieses Schadens betrieben werden darf, abgeschätzt werden soll. Es macht einen deutlichen Unterschied, ob ein Schaden regelmässig jeden Monat oder jedes Jahr auftritt, oder ob er nach heutigem Ermessen eigentlich gar nicht auftreten kann. Folgende Punkte müssen also beachtet werden:

- Wirtschaftlicher Schaden
- Eintrittswahrscheinlichkeit
- Zeitdauer der Störung

Der Begriff des Schadens wurde in Kapitel 1.1.3 genauer umschrieben. In der Aufgabenstellung wird davon ausgegangen, dass dieser Schaden durch eine DDoS Attacke auf einen BSP verursacht wird. Es muss hier unterschieden werden zwischen indirekten und direkten (siehe auch Kapitel 2.3.4): Eine indirekte Attacke kann z.B. via verschiedene ISPs erfolgen. Durch Überlasten der Netzwerk-Architektur wird hier der Backbone oder Teile davon unbenutzbar gemacht. Eine direkte Attacke auf den Backbone erfolgt z.B. auf das NMS oder auf die Authentifizierungsserver im Netzwerk. Dabei wird der Backbone nicht überlastet, sondern erfüllt seine Funktion nicht mehr bzw. ist für die Kunden nicht mehr erreichbar.

Für die Betrachtung des wirtschaftlichen Schadens ist es in weiten Bereichen irrelevant, wie ein Schaden genau zu Stande kommt. Sobald die Funktionsfähigkeit des Backbones gestört ist, kann Schaden entstehen. Lediglich in Bereichen, welche eng mit den technischen Aspekten verknüpft sind, ergeben sich allenfalls Unterschiede im wirtschaftlichen Schaden (z.B. bei den Wiederherstellungskosten). Ein weiterer Unterschied liegt allenfalls auch in der Schadensdauer. Mutwillig veränderte Routing Tables in einem Backbone-Netz stellen einen tatsächlichen physischen Schaden dar (siehe auch Kapitel 2.3.4). Das Reparieren bzw. das Erstellen vollständig neuer Routing Tables im Backbone dauert je nach Umfang mehrere Tage, wogegen eine DDoS Attacke basierend auf Überlastung eventuell nach einer Stunde bereits keine Auswirkungen mehr zeigt [BU03].

DDoS Attacken stellen lediglich einen Teil eines weiten Spektrums an Bedrohungen für einen BSP dar. Es ist hier wichtig zu sehen, dass diese Bedrohungen jeweils zwar verschiedene technische Auswirkungen haben, der wirtschaftliche Schaden in weiten Bereichen aber ähnlich ist. Die Eintrittswahrscheinlichkeiten dieser Schadensfälle unterscheiden sich voneinander, obwohl sie in der Regel alle sehr klein sind.

Im Verlauf dieser Arbeit wird die Betrachtung entsprechend der Aufgabenstellung auf ein prototypisches Szenario beschränkt. Es wird dabei angenommen, dass zum Zeitpunkt $t_0=0$ bereits ein Schaden eingetreten ist, welcher das Backbone-Netzwerk stört. Die Eintrittswahrscheinlichkeit eines Schadens wird nicht weiter betrachtet. Beim Angriff handelt es sich um eine DDoS Attacke.

4 WIRTSCHAFTLICHE AUSWIRKUNGEN

4.1 Schadensarten

Schadensart / Element	Produktivitätsverlust	Entgangener Umsatz	Wiederherstellung des Betriebs	Forderungen von Dritten	Kundenverlust
Backbone Service Provider	X	(X)	X	X	X
Internet Service Provider	X	(X)	X	X	X
Privatkunden					
Firmenkunden					
E-Shop	X	X			X
KMU	X	X			
Grosskonzern	X	X	(X)		
Webhoster	X	(X)	X	X	X
Versicherung	X			X	
Andere Netzwerkbetreiber					
Telefongesellschaft	X				
Kabelfernsehgesellschaft	X	(X)	X	(X)	(X)
Weitere					
Bankautomaten, Kartenleser		(X)	X		
Börse	X		X	X	
Lotto, Sport-Toto		X			
Migros, Coop	X	(X)			X
Banken	X	X	X	(X)	X

Tabelle 4-1: Elemente und Schadensarten

Der betrachtete Schaden infolge einer DDoS Attacke auf einen BSP ist kostenwirksam. Kosten können unmittelbar z.B. durch erhöhten Arbeitseinsatz zur Wiederherstellung des Netzbetriebes anfallen. Opportunitätskosten sind die entgangenen Nutzen, die man bei Nichteintreten einer Störung hätte erzielen können (z.B. entgangener Umsatz). Auch sie sind zu berücksichtigen, beeinflussen sie doch die Ertragslage einer Unternehmung.

Produktivitätsverlust	Durch Störung eines Dienstes sind Mitarbeiter unter Umständen nicht mehr in der Lage, ihre Arbeiten vollumfänglich zu erledigen. Das Unternehmen büsst Produktivität ein.
Entgangener Umsatz	Umsatzausfall entsteht durch entgangene Transaktionen (Verkauf, Vermietung, etc.), sei dies weil die Verbindung zum Kunden nicht mehr steht oder interne Firmenabläufe (z.B. Bestellwesen) nicht mehr funktionieren. Kundenabgang ist hier nicht berücksichtigt. Er wird separat betrachtet. Bei Umsatzausfall handelt es sich um direkte Opportunitätskosten.
Wiederherstellung des Betriebs	Zur Wiederherstellung des Betriebs eines geschädigten oder gestörten Netzes oder Dienstes müssen Arbeitsstuden aufgewendet werden (technische Instandsetzung, Kundendienst). Des Weiteren können Materialkosten anfallen. Diese sind jedoch in vielen Fällen gegenüber den Personalkosten vernachlässigbar, da sie aus Kulanz oft vom Hersteller (von Netzelementen etc.) übernommen werden [BU03]. Bei den Wiederherstellungskosten handelt es sich um direkte Kosten. Sie fallen unmittelbar nach Eintreten einer Störung an.
Forderung von Dritten	Je nach Vertragslage von Erbringern eines Dienstes zum Kunden können im Störungsfall Haftpflichtansprüche des Kunden geltend gemacht werden oder Konventionalstrafen eintreten. Diese Kosten können unter Umständen teilweise abgewälzt werden (z.B. durch Versicherung des Schadensfalls). Es handelt sich um direkte Kosten, die jedoch meistens mit einer gewissen zeitlichen Verzögerung gegenüber der Störung anfallen.
Kundenverlust	Verlust von Kunden tritt in allen Fristigkeiten auf, wobei sich der Abgang mit zunehmender Störung bzw. zunehmender Häufigkeit von Störfällen erhöht. Bestehen mindestens gleichwertige Alternativen, nimmt die Kundentreue ab. Gehen Kunden verloren oder nimmt die Anzahl der Neukunden pro Zeit ab, so schlägt sich das im Umsatz nieder (Opportunität). Kundentreue, Kundenzugang und Kundenabgang sind Messgrössen für die Kundenzufriedenheit.
Sonstige Schäden	Handelt es sich bei der von der Störung betroffenen Firma um ein börsenkotiertes Unternehmen, so kann der Anleger und Aktionär (im weiteren Sinn auch das Unternehmen selber – nämlich wenn es eigene Aktien hält) einen finanziellen Schaden erleiden (Wertverlust). Dieser Schaden aufgrund einer DDoS Attacke ist

	jedoch kaum rational fassbar. Er sei der Vollständigkeit halber hier erwähnt, wird jedoch nicht weiter verfolgt. Eine Dienststörung kann einen Imageschaden bewirken. Dieser wird sich negativ auf den Kundenzugang auswirken. Ausbleibender Umsatz ist die Folge.

Tabelle 4-2: Beschreibung der Schadensarten

4.2 Eintretender Schaden

4.2.1 Darstellung

Zur Abschätzung der wirtschaftlichen Auswirkungen wird der Schaden pro Systemelement beschrieben und grafisch in Abhängigkeit der Zeit dargestellt. Die folgenden Grafiken zeigen jeweils qualitativ den kumulierten wirtschaftlichen Schaden über die Zeit. Der Kurvenverlauf stellt dabei eine mögliche Schadensabfolge dar.

Zum Zeitpunkt $t=t_0$ tritt die Störung infolge einer DDoS Attacke auf einen BSP ein. Diese Störung ist zu $t=t_1$ vollständig behoben. Somit können drei Intervalle betrachtet werden. Die Zeit während der Störung (to<=t<t1) und die Zeiten kurzfristig (t_1<=t<t_2) bzw. langfristig (t>=t_2) nach der Störung. Eine Überlagerung der einzelnen Kurvenabschnitte ist denkbar. Der Übersichtlichkeit und Verständlichkeit halber wird bei dieser Darstellung jedoch darauf verzichtet.

Um den gesamten Schaden der DDoS Attacke abschätzen zu können, muss von einem Zeitpunkt >>t2 ausgegangen werden, an dem der kumulierte Schaden nicht weiter zunimmt. Ausgehend von diesem Punkt können dann für alle Schadensarten die entsprechenden Gesamtkosten eruiert werden.

4.2.2 BSP und ISP

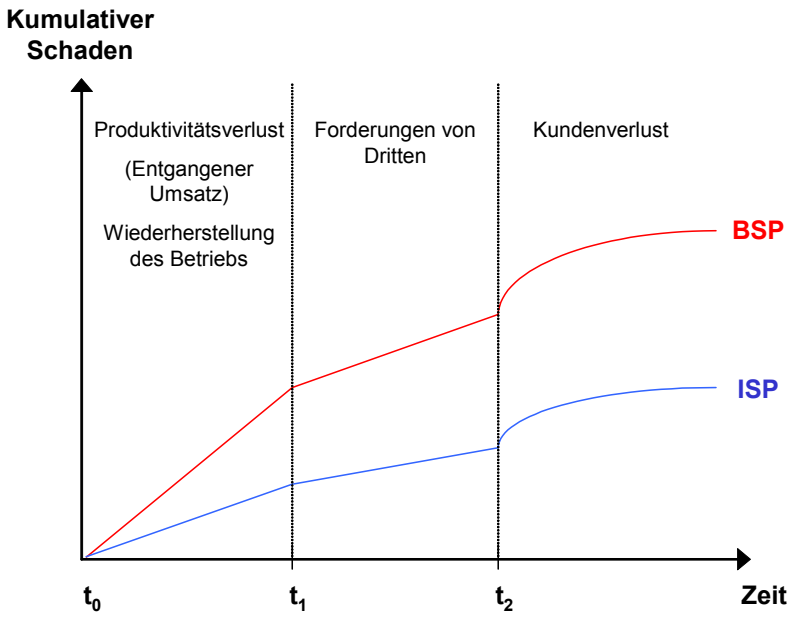

Abbildung 4-1: Kumulativer Schaden bei BSP und ISP

Produktivitätsverlust. Eine Störung des IP-Backbones tangiert die Produktivität der Mitarbeiter aller betroffenen Firmen, also auch der BSPs und ISPs. Falls ein Zugriff auf standortübergreifende Firmennetzwerke nicht mehr möglich ist, wird die Arbeit am Computer erschwert oder sogar verunmöglicht. Neben dem eingeschränkten oder fehlenden Zugang zu den eigenen Daten ist auch der Zugriff auf Internet und E-Mail betroffen, was mit zunehmender Dauer der Störung die Produktivität verringert. Der Gegenwert, den die betroffenen Firmen hier für ihre Lohnkosten erhalten, sinkt also mit zunehmender Dauer der Störung.

Entgangener Umsatz. Beim BSP wird der Umsatz von einer Störung des Netzwerks nicht unmittelbar tangiert, da dieser in der Regel keine zeitabhängigen Gebühren für die Benutzung seiner Infrastruktur erhebt. Allenfalls sind datenmengenabhängige Gebühren denkbar. Eine gewisse Umsatzeinbusse (z.B. ein Verlust von Provisionen) ist auch beim ISP denkbar. So wird z.B. ein Teil des Bluewin-Portals über Werbung und über Partner E-Shops finanziert (siehe auch Kapitel 4.4.3).

Wiederherstellung des Betriebs. Für den BSP als von der DDoS Attacke direkt Betroffenen stellen die Wiederherstellungskosten einen grossen Teil des gesamten wirtschaftlichen Schadens dar. Diese Kosten bestehen in erster Linie aus Personalkosten und in zweiter Linie aus Materialkosten. Wie in Kapitel 4.1 erwähnt, können Materialkosten oft vernachlässigt werden. Es sei denn, es fallen z.B. durch entstandene Sicherheitslücken Updates in Hardware (neue Geräte) oder Software (Lizenzkosten) an. Wie in Tabelle 4-2 erwähnt, werden diese Kosten aber oft vom Hersteller übernommen. Beim ISP verhält sich die Situation ähnlich wie beim BSP. Falls der ISP von der DDoS Attacke nicht direkt

betroffen ist, fällt der Anteil der Wiederherstellungskosten jedoch kleiner aus als beim BSP.

Forderung von Dritten. Je nach Vertrags-Bedingungen treten bei einer Störung des Netzes Konventionalstrafen in Kraft. BSPs haben mit Firmenkunden oft umfangreiche SLAs, welche im Störungsfall zum Tragen kommen (siehe Kapitel 2.5.2). Der BSP wird in diesem Fall unter Umständen auch von den ISPs direkt behaftet. Die ISPs selbst haben sich gegenüber den Privatkunden gut abgesichert. Da lediglich ein Best Effort garantiert wird, sind im Störungsfall keine Forderungen seitens dieser Kunden zu befürchten (siehe Kapitel 2.5.1). Es ist dennoch denkbar, dass Verträge mit Firmenkunden oder Webhostern bestehen, welche Konventionalstrafen vorsehen. Es wird angenommen, dass der Schaden gemessen am Umsatz beim BSP durch die Forderungen von Dritten deutlich höher ist als beim ISP, da ein BSP viele Verträge mit Firmenkunden (und entsprechenden SLAs) hat, welche solche Forderungen zulassen.

Kundenverlust. Die Auswirkungen eines Kundenverlustes werden erst nach einer gewissen Zeit spürbar. In der Regel sind Abonnemente bei einem ISP oder Mietleitungen bei einem BSP nicht per sofort kündbar. Sie müssen aber beim nächst möglichen Termin nicht mehr erneuert werden, wenn die Kunden in den entsprechenden ISP oder BSP das Vertrauen verloren haben. Es ist davon auszugehen, dass diese Kündigungen gehäuft (z.B. am Ende eines Monats nach einer Störung) eintreffen, danach aber nur noch sporadisch. Dies hat unter Anderem damit zu tun, dass ein Störungsfall bei den Kunden oft rasch wieder in Vergessenheit gerät, solange er nicht wiederholt auftritt. Die Wahrscheinlichkeit eines Wechsels von Firmenkunden zu einem anderen Anbieter wird im einmaligen Schadensfall als gering angesehen, da die Wechselkosten für den Kunden hoch sind (insbesondere bei kundenspezifischen Mietleitungen). Zudem bestehen entsprechende Verträge, welche bei solchen Schadensfällen zum tragen kommen. Anstelle eines Kundenverlusts ist daher eher eine Anpassung dieser Verträge zu Ungunsten des BSP denkbar.

4.2.3 Firmenkunden

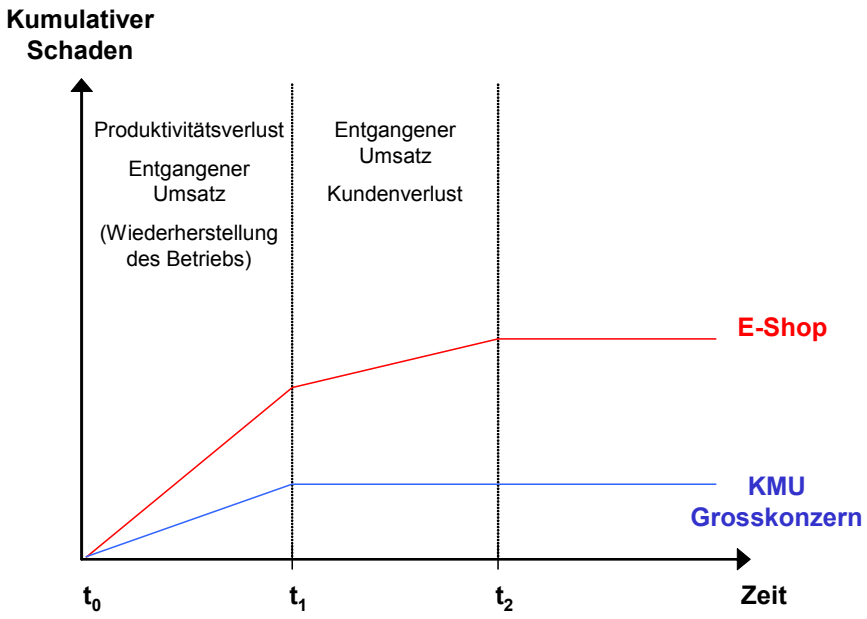

Abbildung 4-2: Kumulativer Schaden bei Firmenkunden

Produktivitätsverlust. (Siehe Ausführungen in Kapitel 4.2.2)

Entgangener Umsatz. Bei einem E-Shop, welcher seine Produkte ausschliesslich über das Internet vertreibt, fällt der Umsatzverlust am gravierendsten aus. Jede Minute, in welcher die Website des E-Shops nicht erreichbar ist, bedeutet einen Ausfall an Einnahmen. Bei einer KMU oder bei einem Grosskonzern, bei welchem das Internet nur einer von vielen Verkaufskanälen ist, fällt der Ausfall prozentual am Gesamtumsatz deutlich geringer aus. Viele Kunden werden auf funktionierende Alternativen - wie Telefon oder Fax - ausweichen. Insbesondere bei Projektgeschäften mit anderen Firmen ist hier kein Umsatzausfall oder Kundenverlust zu befürchten, da die Rahmenbedingungen mit denen eines E-Shops nicht vergleichbar sind.

Wiederherstellung des Betriebs. Die Wiederherstellungskosten werden für Firmenkunden allgemein als klein angesehen, da die betroffenen Services oft von Dritten betrieben werden, welche auch für den Unterhalt verantwortlich sind. Insbesondere ein E-Shop wird kaum Kosten zur Wiederherstellung seines Dienstes haben, da meist ein Webhoster diese Arbeit übernimmt. Bei Grosskonzernen werden die Wiederherstellungskosten hingegen eher ins Gewicht fallen, insbesondere bei Standort übergreifenden Netzwerken.

Kundenverlust. Ein Verlust von Kunden wird bei E-Shops bereits früher eintreten als z.B. bei den ISPs. Grund dafür ist der Unterschied im Charakter der Geschäftsbeziehung zu den Kunden: Ist ein E-Shop einige Zeit nicht erreichbar, werden die Kunden bei lukrativen Alternativen zur Konkurrenz wechseln und bis auf weiteres dort bleiben. Obwohl also ein E-Shop wieder online ist, wird der Umsatz- und Kundenverlust weiter leicht zunehmen.

4.2.4 Webhoster

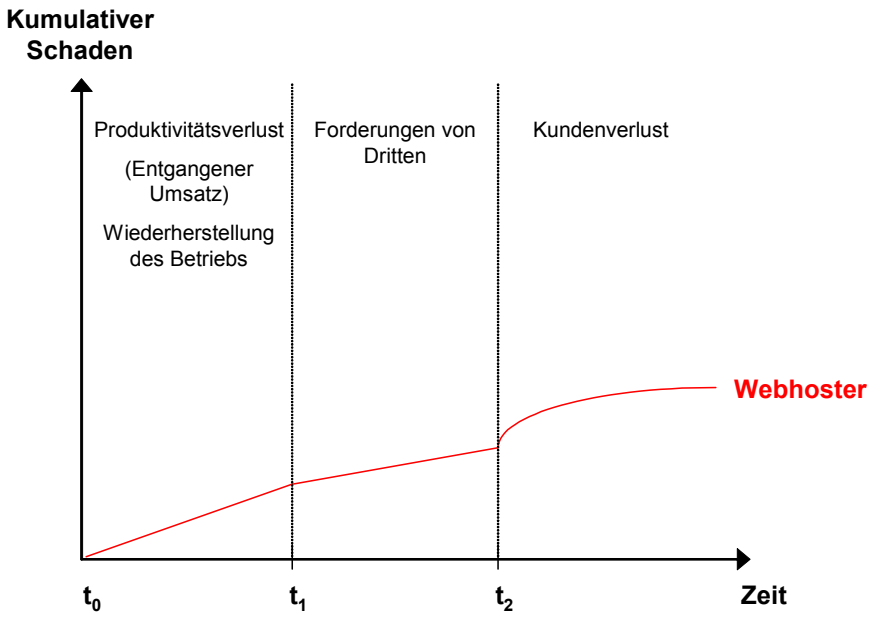

Abbildung 4-3: Kumulativer Schaden bei Webhostern

Produktivitätsverlust. (Siehe Ausführungen in Kapitel 4.2.2)

Entgangener Umsatz. Ist in den Abonnementen des Webhosters eine Begrenzung der übertragenen Datenmenge vorgesehen, so wird zusätzlicher Datenverkehr separat verrechnet. Damit kann weiterer Umsatz generiert werden.

Wiederherstellung des Betriebs. Bei einer Störung des IP-Backbones kann die Konnektivität des Webhosters zum Internet beeinträchtigt werden. Beim Webhoster entstehen ähnlich wie beim ISP dann Kosten, wenn manuelle Eingriffe an der eigenen Infrastruktur notwendig sind, um deren Funktionalität wiederherzustellen.

Forderungen von Dritten. Abhängig von den Verträgen, welche ein Webhoster mit seinen Kunden hat, kommen nach einem Störungsfall Forderungen auf ihn zu. Bei Privatkunden, welche lediglich ihre Homepage auf einem Server hosten lassen, haben die Webhoster in der Regel sämtliche Schadenersatzansprüche der Kunden wegbedungen. Allenfalls wird den Kunden ein sofortiger Rücktritt vom Vertrag zugestanden [FF03a]. Bei Firmenkunden muss jedoch davon ausgegangen werden, dass SLAs bestehen und der Webhoster im Störungsfall auch zahlungspflichtig wird. Insbesondere grosse Firmen betreiben aber ihre Server oft in Eigenregie und sind somit nicht von einem Webhoster abhängig.

Kundenverlust. Der Ausfall der eigenen Website während einiger Stunden wird vielen Privatkunden gar nicht auffallen. Firmenkunden verlieren aber eventuell einen Teil ihres Umsatzes. Ebenfalls ist eine nicht erreichbare Firmenwebsite keine gute Visitenkarte und kann dem Image schaden (siehe Tabelle 4-2). Es ist unklar, wie viele Firmen oder Privatkunden nach einem grösseren Störungsfall ihren Webhoster tatsächlich wechseln werden (sofern sie ihre Server nicht

ohnehin selbst betreiben). Insbesondere bei kleineren Websites stellt ein solcher Wechsel kein grosses Hindernis dar. Auch hier wird angenommen, dass die Kündigungen gehäuft auftreten (z.B. Ende des Monats, vgl. auch Ausführungen beim ISP). Bei der Störung eines Backbone-Netzwerks sind mehrere Webhoster gleichermassen betroffen, was den Imageverlust für den Einzelnen relativiert. Bei Attacken direkt auf die Server des Webhosters und bei damit verbundenen Schäden, kann der Kundenverlust aber deutlich höher ausfallen. Insbesondere dann, wenn den Webhoster selbst eine eindeutige Schuld trifft, kann der Imageverlust immens sein (siehe dazu das Beispiel von Tiscali, Kapitel 4.4.5). Der Kundenverlust ist also stark abhängig von der Art der Störung und vom entsprechenden Vertrauensverlust bei den Kunden.

4.2.5 Versicherungen

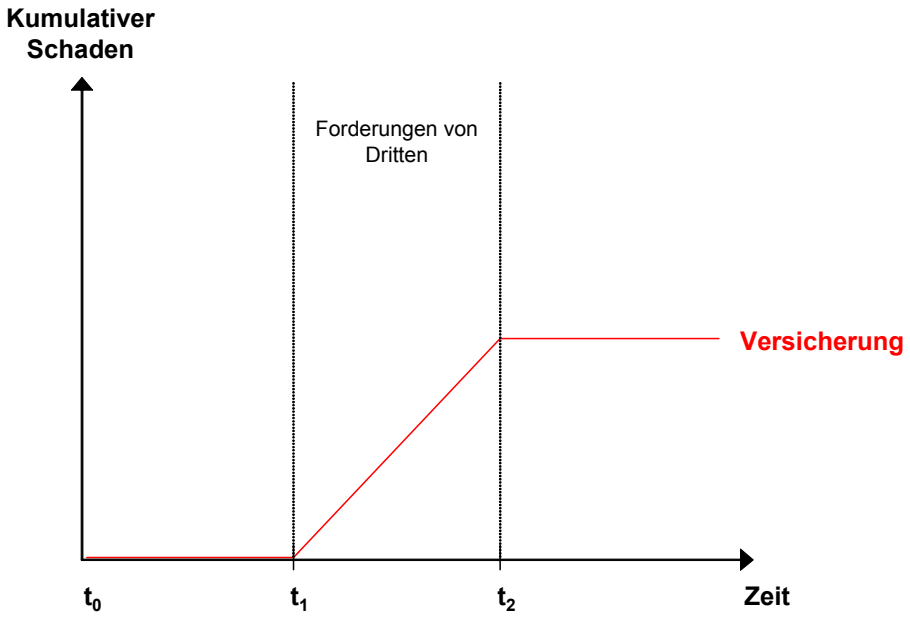

Abbildung 4-4: Kumulativer Schaden bei Versicherungen

Produktivitätsverlust. Wie bei jeder anderen betroffenen Unternehmung werden auch bei den Versicherungen Produktivitätsverluste durch die Störung der IT-Systeme auftreten. Der Übersichtlichkeit halber wird dies in der Grafik jedoch nicht gezeigt, da der Fokus klar auf den Forderungen der Versicherten liegt.

Forderung von Dritten. Wie in Kapitel 4.2.1 beschrieben, treffen Forderungen zeitverzögert nach Behebung des Schadens ein. Insbesondere Wiederherstellungskosten und Umsatzverluste werden hier von den Versicherten angemeldet, zusätzlich können auch weitere Schäden (siehe Kapitel 2.7) von der Versicherung abgedeckt werden.

4.2.6 Telefonnetz-Betreiber

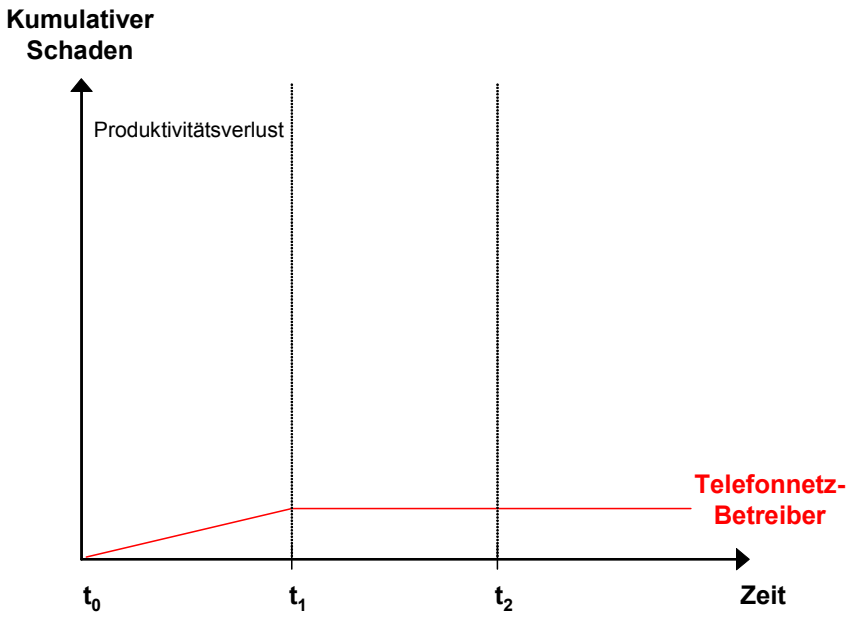

Abbildung 4-5: Kumulativer Schaden bei Telefonnetz-Betreibern

Produktivitätsverlust. (Siehe Ausführungen in Kapitel 4.2.2)

Entgangener Umsatz. Da das klassische Telefonnetz keine Verbindung zum IP-Backbone besitzt, ist hier auch mit keiner Störung zu rechnen. Ein Umsatzverlust bei den Gesprächsminuten ist also nicht zu befürchten. Bietet der Telefonnetz-Betreiber zusätzliche Dienste wie z.B. Internetzugang an, so gelten die Überlegungen für einen ISP (siehe Kapitel 4.2.2).

4.2.7 TV-Kabelnetz-Betreiber

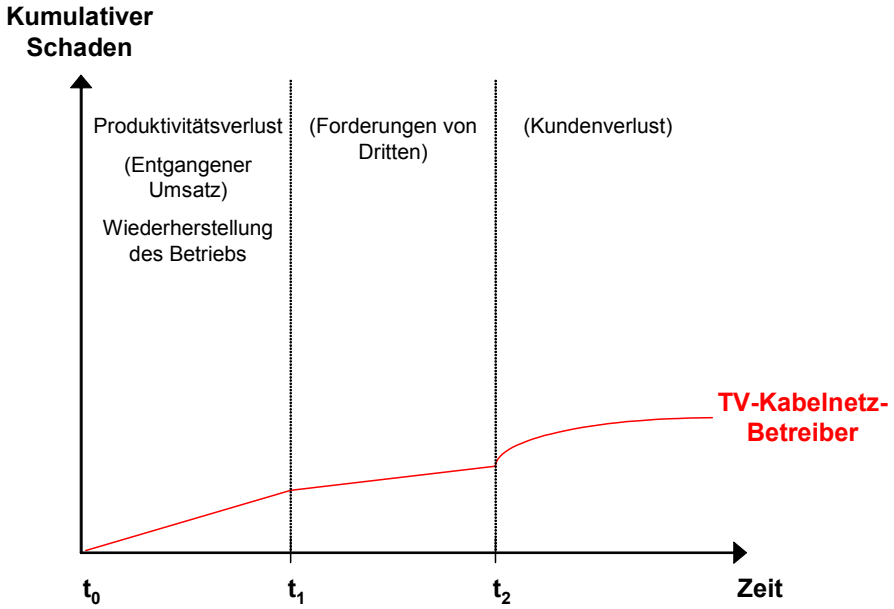

Abbildung 4-6: Kumulativer Schaden bei TV-Kabelnetz-Betreibern

Produktivitätsverlust. (Siehe Ausführungen in Kapitel 4.2.2)

Entgangener Umsatz. Das TV-Kabelnetz steht je länger je mehr ebenfalls mit IP-Backbones in Verbindung (siehe Kapitel 2.8.2). Mit zunehmender Verbreitung von Telefoniediensten über IP und Kabelinternet steigt die Bedeutung einer funktionierenden Anbindung an einen IP-Backbone. Da die meisten TV-Kabelnetz-Betreiber in der Schweiz mittlerweile keine Abonnemente für Kabelinternet mehr anbieten, bei denen die Preise von der Datenmenge abhängen, kann bei einem Ausfall des IP-Backbones im Bereich von Stunden auch nicht von einem eigentlichen Umsatzverlust gesprochen werden.[1] Lediglich bei den Telefoniediensten ist ein Umsatzausfall denkbar. Ebenso bei den Pay-Per-View-Angeboten, welche über ein Modem in der Set-Top-Box bestellt werden können. Die Bestellung via Telefon steht hier aber als Alternative offen. Aufgrund der momentan noch geringen Verbreitung dieser Angebote wird der Umsatzausfall für den TV-Kabelnetz Betreiber gemessen am Gesamtumsatz jedoch als gering angenommen.

Wiederherstellung des Betriebs. Je nach dem, ob der TV-Kabelnetz-Betreiber ein eigenes IP-Backbone-Netzwerk betreibt oder nicht, fallen auch die Wiederherstellungskosten unterschiedlich hoch aus. Beim grössten TV-Kabelnetz-Betreiber der Schweiz (Cablecom), welcher ein eigenes IP-Backbone-Netzwerk betreibt, fallen diese Kosten also massgeblich ins Gewicht, da er selbst für die Wiederherstellung verantwortlich ist.

[1] Insbesondere Cablecom hat von Beginn an nur Kabelinternet-Abonnemente ohne Begrenzung der Datenmenge angeboten. Eine Ausnahme bildet z.B. noch die GGA Reinach [GGA03]. Der Trend geht aber (auch bei ADSL) eindeutig hin zu Flat-Rates.

Forderungen von Dritten. Auch beim TV-Kabelnetz-Betreiber sind von Seiten der Privatkunden keine Forderungen zu erwarten. Bietet der Betreiber aber auch für Firmenkunden umfangreiche Dienstleistungen mit spezifischen SLAs an, so können Forderungen entstehen (siehe Beispiel Cablecom, Kapitel 2.8.2).

Kundenverlust. Ein Wechsel des Anbieters eines Breitband-Internet-Zugangs ist für Privatkunden einfach. Meistens stellt ADSL eine Alternative zum Kabelinternet dar. Dasselbe gilt auch für die Telefonie. Aufgrund des Monopols der TV-Kabelnetz-Betreiber in den jeweiligen Regionen ist ein Wechsel zu einem anderen Anbieter aber nicht möglich. Lediglich der Wechsel zum Satellitenfernsehen wäre eine Alternative. Bei den Firmenkunden gelten die gleichen Überlegungen wie bei den BSPs und ISPs: Der Verlust von Firmenkunden bei einem einmaligen Störfall ist aufgrund der hohen Wechselkosten für die Kunden gering.

4.2.8 Überblick

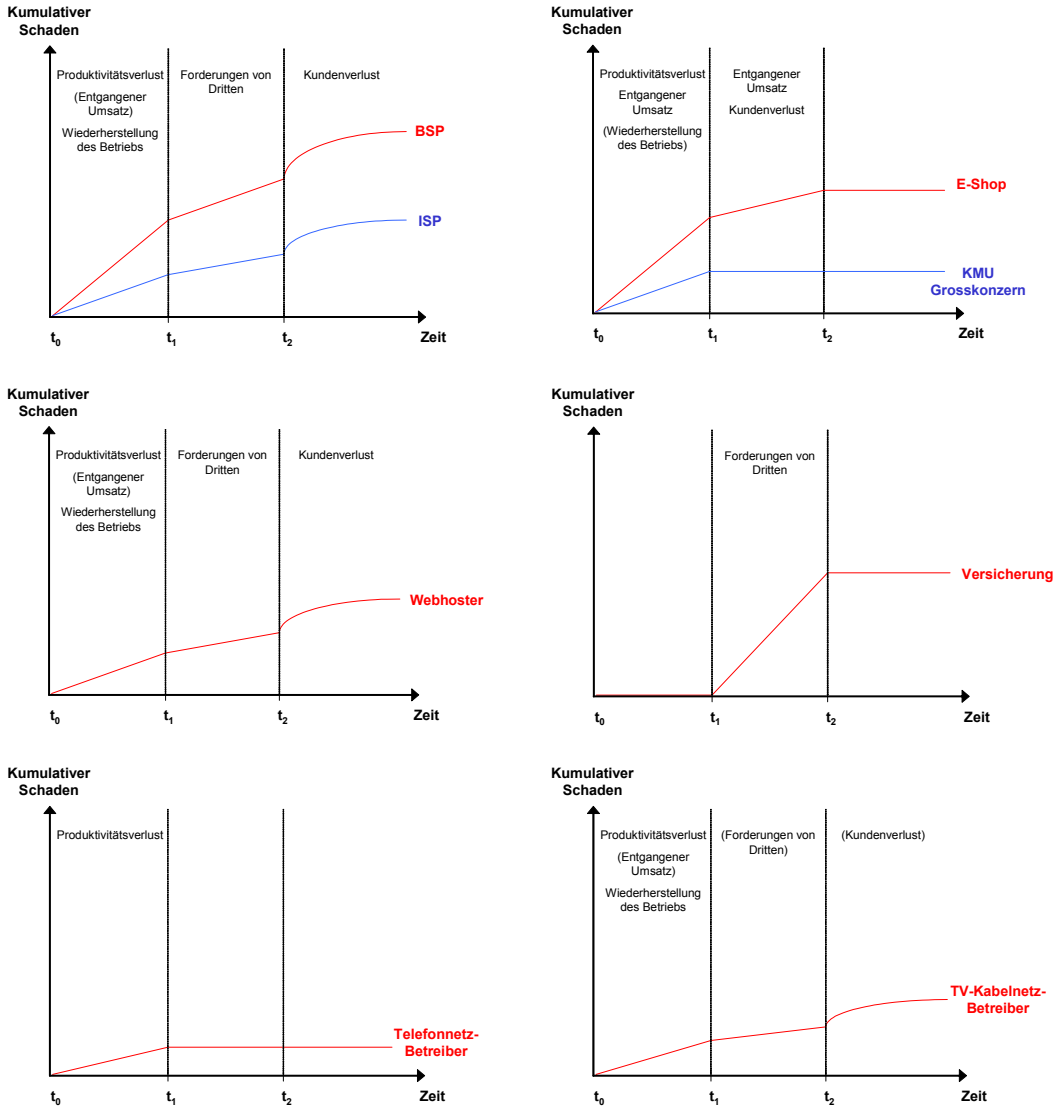

Abbildung 4-7: Überblick Schadensverläufe

4.3 Eigene Berechnungsansätze

Die Erhebung des Schadens und somit der Kosten erfolgt nach Behebung der technischen Störung zu einem Zeitpunkt >>t_2 (siehe Kapitel 4.2.1). Die nachfolgenden Formeln sind abhängig von der Störungsdauer ($d_s=t_1-t_0$) und bestimmen die Gesamtkosten für die vorgefallene Störung.

4.3.1 Downtime-Kosten

$$DK(d_A, d_{AS}, d_B, d_{BS}) = \left[\frac{MK}{d_A} \cdot d_{AS} \cdot AM \cdot b + \frac{U}{d_B} \cdot d_{BS} \cdot AU \right] \cdot a \qquad \text{CHF}$$

DK: Downtime-Kosten (CHF)

d_A : Anzahl Mitarbeiter-Arbeitsstunden pro Jahr (h)

d_{AS} : Mitarbeiter-Arbeitszeit während der Störung (h)

d_B : Anzahl Betriebsstunden pro Jahr, Dienstverfügbarkeit (h)

d_{BS} : von der Störung betroffene Dienstbetriebszeit (h)

MK: Produktivitätskosten pro Mitarbeiter und Jahr, Gehälter und Boni (CHF)

AM: Anzahl der Mitarbeiter, die von der Störung betroffen sind (#)

U: Ø Umsatz pro Jahr (CHF)

AU: Anteil des Gesamtumsatzes, der von der Störung betroffen ist (%)

a: Ausfallgrad des gestörten Dienstes (%)

b: Verringerung der Produktivität der Mitarbeiter (%)

Beachte:

- d_{AS} und d_{BS} sind abhängig von der Dauer der Störung des Dienstes. Die Störung muss weder zeitgleich mit den Mitarbeiter-Arbeitszeiten noch mit der Dienstverfügbarkeit sein.
- d_{BS} : Gehen wir davon aus, dass ein E-Shop seine Produkte nur in den normalen Geschäftsöffnungszeiten verkauft und die Störung in der Nacht eintritt, so ist die von der Störung betroffene Dienstbetriebszeit gleich Null.
- Die Downtime-Kosten setzen sich aus Kosten, die durch den Ausfall von Umsatz entstehen, und solchen infolge eines Produktivitätsverlustes zusammen [PA02]. Sind Mitarbeiter in besonderem Masse abhängig vom Funktionieren

eines Computernetzes, so können diese bei Störung eines Dienstes ihre volle Leistung nicht mehr erbringen.

- Umsatzausfall hat zwei mögliche Ursachen: Ist die Website eines Unternehmens, das E-Commerce betreibt, nicht online, so können keine Verkäufe getätigt werden. Durch den Ausfall eines Computernetzes wie ein Backbone-Netz können firmeninterne Kommunikationskanäle (z.B. Bestellwesen) gestört sein, was wiederum Umsatzausfall zur Folge haben kann.

- Downtime ist definiert durch die Dauer der technischen Störung. Sie muss nicht unbedingt zu Umsatzausfall führen. Im Falle von E-Commerce können Kunden warten und später bestellen. Produktivitätsverlust ist nicht zwingend. Mitarbeiter, deren Betriebsmittel gestört sind, können andere produktive Arbeiten ausführen.

- Umsatz ist Schwankungen unterworfen. Somit wird es kritisch, Jahresumsätze auf die relativ kurze Störungsdauer hinunterzubrechen. Eine Lotterie-Gesellschaft kann z.B. in den Stunden vor Eingabeschluss einen Umsatzsprung erleben.

4.3.2 Wiederherstellung des Betriebs

$$WK(d_S) = IT \cdot SS \cdot d_U + MK \qquad \text{CHF}$$

WK: Wiederherstellungskosten (CHF)

d_U: Überstunden (h)

IT: Instandsetzungs-Team (Anzahl Mitarbeiter)

SS: Stundensatz Instandsetzungs-Team (CHF)

MK: Materialkosten (CHF)

Beachte:

- Die Wiederherstellung des gestörten Dienstes beginnt unmittelbar nach Eintritt der Störung.

- Das Instandsetzungs-Team verursacht nur zusätzliche Kosten, wenn es Überstunden machen muss.

4.3.3 Forderungen von Dritten

$$FD = \sum (KS + HA) \qquad \text{CHF}$$

FD: Forderungen von Dritten (CHF)

KS: Konventionalstrafen (CHF)

HA: Haftpflichansprüche (CHF)

Beachte:

- Diese Forderungen werden nicht alle gleichzeitig geltend gemacht. Sie werden aktuell, wenn in Verträgen fixierte Leistungen nicht erbracht werden oder Abmachungen nicht eingehalten werden können.
- Oft stehen diese Ansprüche erst nach Feststellen des Schadensausmasses fest.

4.3.4 Kundenverlust

$$KV(\Delta t) = [AK(\Delta t) + PK(\Delta t)] \cdot UK(\Delta t) \qquad \text{CHF}$$

KV: Kundenverlust (CHF)

AK: Verlust an bestehenden Kunden (Anzahl abgehende Kunden)

PK: Verlust an zukünftigen potentiellen Kunden (Anzahl potentielle Kunden)

UK: Ø Umsatz pro Kunde (CHF)

Δt: betrachtetes Zeitintervall ab Eintritt Störung

Beachte:

- Die Kosten infolge eines Kundenverlustes können nur durch Angabe eines Zeitintervalls quantifiziert werden. Deshalb sind alle Elemente der obigen Formel in Abhängigkeit dieses Zeitintervalls Δt.

4.4 Konkrete Beispiele

4.4.1 Einführende Bemerkungen

Konkrete Zahlen für eingetretene Schäden sind sehr schwierig in Erfahrung zu bringen. Es handelt sich dabei um Daten, die vertraulich behandelt und von den Unternehmen nicht veröffentlicht werden. Es handelt sich oft um Schätzungen. Im Zentrum folgender Beispiele sind deshalb Umsatzzahlen. Diese sind bei börsenko-

tierten Unternehmen veröffentlicht und bei nicht börsenkotierten Unternehmen immerhin aufgrund von verschiedenen Marktdaten recht zuverlässig schätzbar.

Von Interesse ist der entgangene Umsatz pro Zeiteinheit. Dies ist immer eine Schätzgrösse und ein Durchschnittswert. Natürlich fällt der Umsatz nicht regelmässig über das Jahr verteilt an. Dennoch schaffen diese Zahlen ein Gespür für die Grössenordnung, um die es sich bei Umsatzausfällen handeln kann.

4.4.2 Wachstumsmarkt E-Commerce

Der Schweizer Umsatz im Business-to-Business-Bereich (B2B), dem Geschäft zwischen Produktions- und Handelsunternehmen, hat sich seit 2000 jährlich verdoppelt und lag im vergangenen Jahr bei CHF 21 bis 25 Mrd. Franken [FO03]. Gemäss dem Marktforschungsunternehmen Forrester sollen in der Schweiz im Jahr 2004 im B2B-Markt bereits CHF 100-120 Mrd. umgesetzt werden. Die Chemieunternehmen mit einem elektronischen Umsatzvolumen von CHF 27 Mrd. sollen den Spitzenplatz einnehmen, gefolgt von Finanzdienstleistern (CHF 24 Mrd.) und der IT-Industrie (CHF 20 Mrd.) [EN02].

Vergleichsweise klein ist dagegen das elektronische Business-to-Consumer-Geschäft (B2C): Die Umsatzschätzungen schwanken hier zwischen CHF 0,5 und 1,5 Mrd. Franken. Doch immerhin kommt dies einem gesamtschweizerischen stündlichen Umsatz von über CHF 100'000 pro Stunde gleich, wenn man davon ausgeht, dass E-Shops über 24 Stunden am Tag und 365 Tage im Jahr Bestellungen entgegennehmen und bearbeiten [FO03].

4.4.3 Bluewin

Die Firma Bluewin hat per Mitte 2001 mit 1,3 Mio. registrierten Kunden CHF 68 Mio. Umsatz erwirtschaftet. Der Umsatz in den ersten drei Quartalen 2001 belief sich auf CHF 107 Mio. [BW01]. Ende 2001 waren etwa 730'000 Accesskunden aktiv [SC03b]. 90% des Umsatzes wird über das Zugangsgeschäft von Bluewin als ISP gemacht. Werbeeinnahmen und Shopping-Kommissionen machen etwas weniger als 10% aus [NZZ02b].

Bluewin macht also schätzungsweise einen Umsatz von etwa CHF 140 Mio. pro Jahr, wobei das Web-Portal um die CHF 15 Mio. ausmacht. Das Web-Portal ist jederzeit geöffnet. Wird der Gesamtumsatz auf die Stunde hinuntergebrochen, so werden im Schnitt gegen CHF 2'000 pro Stunde umgesetzt.

4.4.4 Arp Datacon

Die auf den Versandhandel von Hardware, Software und EDV-Zubehör spezialisierte Arp-Datacon-Gruppe, die in der Schweiz im zugerischen Rotkreuz beheimatet ist, setzt für das weitere Wachstum auf E-Commerce als strategischen Erfolgsfaktor. Der Umsatz im Jahre 2001 betrug CHF 103 Mio. 41 % des Umsatzes wurden über den Online-Shop generiert, wobei Internet-Shop 33% und B2B-Transaktionen 8% ausmacht. Hier wird das Geschäft über eine direkte Verbindung

zur Unternehmens-Software des Kunden abgeschlossen, zum Teil auch über elektronische Marktplätze. Als nächstes Ziel will Arp Datacon den Anteil elektronischer Bestellungen von 40 auf 50 Prozent erhöhen. [NZZ02a] . Da der Online-Shop tagtäglich rund um die Uhr in Betrieb ist, entsteht durch dessen Ausfall eine durchschnittliche Umsatzeinbusse von etwa CHF 5'000 pro Stunde.

4.4.5 Tiscali

Der ISP und Webhoster Tiscali wurde am 3. März 2003 Opfer einer Hacker-Attacke, wobei der Inhalt von 899 Kunden-Websites gelöscht wurde. Tiscali wurde dabei in einer Stellungnahme von den Hackern verhöhnt, da zuvor offenbar diverse Warnungen bezüglich bestehender Sicherheitslücken ignoriert worden waren [PT03]. Je nach Webhosting-Abonnement der Kunden gehen Tiscali bei einer Kündigung so bis zu CHF 538 pro Kunde und Jahr verloren [TI03]. Sollten alle betroffenen Kunden ihr Tiscali Abonnement kündigen, würde dies einem Schaden von fast CHF 500'000 im Jahr entsprechen. Der Verlust durch Kundenabgänge wird in der Realität wohl deutlich geringer ausfallen. Dennoch könnte sich der Imageverlust weiter auf das Telefonie- und Internet-Geschäft von Tiscali auswirken und ebenfalls Kosten verursachen.

Die Abschätzung eines allfälligen Kundenverlusts nach einer solchen Attacke ist schwierig. Wie erwähnt, spielt die Art der Attacke und deren Auswirkungen eine wichtige Rolle. Bei einer DDoS Attacke auf einen IP-Backbone sind in der Regel mehrere Webhoster betroffen, weshalb der Einzelne in der Öffentlichkeit nicht besonders exponiert ist. Bei einer Attacke wie der oben erwähnten wird der Webhoster hingegen viel direkter angegriffen und somit schwindet auch das Vertrauen der Kunden in diesen betroffenen Webhoster viel mehr.

4.4.6 Swisscom Mobile

Der vollständige Ausfall des Swisscom-GSM-Netzwerks am 27. Juli 2001 gehört zu den schwerwiegendsten Zwischenfällen der letzten Jahre. Eine Systemstörung, welche zum Ausfall des Signalisierungsverkehrs geführt hat, war die Ursache des Ausfalls. Obwohl hier keine Hacker-Attacke von aussen vorlag, wird sichtbar, dass solche schwerwiegenden Auswirkungen insbesondere auch durch Fehler oder Attacken von innen verursacht werden können. Der knapp zehnstündige Ausfall hat Kosten in der Grössenordnung von CHF 30 Mio. verursacht, was für die Zeitdauer der Störung pro Stunde einen Schaden von etwa CHF 3 Mio. ausmacht. Knapp die Hälfte davon ist auf den Umsatzausfall, der Rest auf die Wiederherstellungskosten zurückzuführen. Allfällige Forderungen von Swisscom-Kunden und ein späterer Kundenverlust sind in dieser Zahl noch nicht enthalten. Eine 100prozentige Verfügbarkeit des Swisscom-GSM-Netzes wird aber in den Allgemeinen Geschäftsbedingungen auch nicht garantiert, weshalb die meisten Kunden wohl keine Forderungen stellen können. Die durchschnittliche Verfügbarkeit des Netzes liegt bei etwa 99,95%, was einer Ausfallzeit von etwas mehr als vier Stunden pro Jahr entspricht [PT01, NZZ01].

Wie in Kapitel 2.8.1 erwähnt, ist bei einer DDoS Attacke nicht mit einem Ausfall des Telefonnetzes zu rechnen. Die möglichen Auswirkungen auf Telefonnetze

werden hier aber sichtbar. Da der Trend bei der Telefonie weiter in Richtung VoIP geht, wäre ein solcher Totalausfall der Telefonnetze in Zukunft durchaus auch aufgrund eines Ausfalls der IP-Backbones denkbar. Der Schaden ist in einem solchen Fall noch um ein Vielfaches höher als oben aufgeführt, wenn sowohl die Mobil- als auch die Festnetze mehrerer Anbieter betroffen sind.

4.4.7 Gesellschaft Schweizer Zahlenlotto

Im Jahr 2001 wies Swiss Lotto einen Umsatz von gegen CHF 600 Mio. auf [ZL01]. Die Dienstverfügbarkeit – also die Öffnungszeiten der Lotto-Annahmestellen – ist begrenzt. Gehen wir von einer durchschnittlichen Öffnungszeit von 60 Stunden pro Woche aus, so macht die Lotto-Gesellschaft pro Halbtag etwa CHF 1 Mio. Umsatz. Dabei handelt es sich um eine grobe Durchschnitts-Schätzung. Der Umsatz schwankt sehr stark. Gegen Annahmeschluss und bei sehr lukrativen Gewinnchancen kann dieser richtiggehend explodieren.

Ist die Lotto-Gesellschaft infolge einer Störung der Dateneinlesung und –übertragung nicht mehr in der Lage, Lose zu verkaufen, so entstehen zumindest Opportunitätskosten. In der Realität wird sich der Grossteil des Umsatzes einfach zeitlich verschieben. Obige Umsatzzahl vermittelt einen guten Eindruck über die Grössenordnungen.

4.5 Rechenbeispiele

4.5.1 Szenarien

Szenarien spielen mögliche Ereignisse und deren Folgen durch [ZU00]. Die in Kapitel 4.2 und 4.3 erarbeiteten Schadensverläufe und Formeln werden in Rechenbeispielen angewendet. Bei den Resultaten handelt es sich um Schätzungen, denn einige Inputgrössen sind nicht analytisch berechenbar. Alle Annahmen und Schätzungen sind jedoch begründet und nachvollziehbar. Die Schadensgrössen sollen Basis für weitere Überlegungen sein und helfen, sich ein Bild über die Grössenordnung der entstehenden Schäden zu machen. Gemäss Aufgabenstellung wird die Funktion von Backbone-Netzwerken durch eine DDoS Attacke gestört. Es werden zwei Szenarien gebildet:

I	II
• Die Konnektivität des betrachteten Elements (ISP, Webhoster, etc.) zu den zur Verfügung stehenden IP-Backbones ist aufgrund einer Störung dieser Backbones nicht mehr gegeben. • Der Dienstausfall beträgt 100%.	
Die Ausfalldauer beträgt	
24 Stunden	1 Woche

Tabelle 4-3: Szenarien

Es hat sich jedoch gezeigt, dass sich mit ihnen am besten Abschätzungen über die anfallenden Schäden machen lassen. Komplexere Szenarien können von diesen

abgeleitet werden. Es werden dann zur Berechnung Inputgrössen benötigt, die nur von direkt betroffenen Firmen erhoben werden können.

Mittels eines Excel-Sheets werden für jedes Szenario Zahlenbeispiele gerechnet (siehe Appendix).

4.5.2 Backbone Service Provider

Der BSP als direkt Betroffener erleidet den grössten Schaden. Stellvertretend für andere grosse Backbone Service Provider soll das Beispiel Swisscom Fixnet Wholesale, welche die leitungsgebundene, technische Infrastruktur für andere Swisscom Gruppengesellschaften bereitstellt, betrachtet werden. Neben 150 nationalen Telekommunikationsfirmen stellt Fixnet Wholesale auch zahlreichen Firmenkunden (via Swisscom Enterprise Solutions) Daten- und Mietleitungen zur Verfügung. Zur Abschätzung des Schadens wird von Szenario I (Ausfall des IP-Backbones während 24 Stunden) ausgegangen.

Der Umsatzausfall, welcher aufgrund minutenabhängiger Tarife entsteht, kann hier vernachlässigt werden (siehe Kapitel 4.2.2) Die Wiederherstellungskosten machen für den BSP jedoch bereits einen grossen Teil des gesamten Schadens aus: Neben den zusätzlichen Lohnkosten fallen auch Kosten für Ersatzausrüstungen bzw. für Software-Updates ins Gewicht. Wie in Kapitel 4.2.2 beschrieben, werden diese Kosten jedoch oft aus Kulanzgründen von den Herstellern übernommen. Die Forderungen von Dritten hängen von den jeweiligen Verträgen mit den Kunden ab, weshalb im Beispiel lediglich eine mögliche Grössenordnung angegeben wird, welche realistisch erscheint [NZZ01, BU03, WI03]. Dasselbe gilt auch für einen allfälligen Kundenverlust. Der Produktivitätsverlust der Mitarbeiter wird in Szenario I mit 20% als relativ gering angenommen, da während eines Arbeitstags in der Regel noch Arbeit unabhängig von E-Mail und Internet verrichtet werden können.

Der Schaden für einen BSP in der Grösse von Swisscom Fixnet Wholesale kann bei einem Ausfall des gesamten Backbone-Netzwerks für 24 Stunden mit gut CHF 30 Mio. beziffert werden. Dies entspricht im Beispiel etwa 1,2% des Jahresumsatzes. Der genaue Betrag hängt aber stark von den Verträgen mit den jeweiligen Kunden und vom Verhalten und Entgegenkommen des BSP gegenüber den Kunden ab. Die angegebene Zahl berücksichtigt keine firmenspezifischen (und vertraulichen) Daten und kann somit zwischen einzelnen Firmen stark variieren.

4.5.3 Firmenkunde

Arp Datacon (siehe Kapitel 4.4.4) betreibt einen Online-Shop.

Wir gehen davon aus, dass Szenario I eintritt. Infolge einer DDoS Attacke auf den Backbone-Provider, von dem die Erreichbarkeit der Website von Arp Datacon abhängt, fällt dieser vollständig aus. Dies führt dazu, dass während 24 Stunden keine Online-Bestellung mehr gemacht werden kann.

Besonderheit dieses Beispiels ist, dass der Online-Dienst rund um die Uhr an 365 Tagen im Jahr verfügbar ist. Der Firmenumsatz wird auf die Stunden gemäss obiger Dienstverfügbarkeit hinuntergebrochen. Dabei handelt es sich um eine grobe Durchschnittsrechnung. Die Umsatzkurve während eines Tages oder innerhalb einer Woche verläuft in Realität nicht konstant. Da der Dienstausfall nur einen Tag dauert, kann davon ausgegangen werden, dass sich der Umsatzverlust in Grenzen hält, da viele Kunden bereit sind zu warten und am nächsten Tag bestellen, telefonisch bestellen oder im Laden vorbeigehen. Allenfalls entstehen Wiederherstellungskosten bei der Instandsetzung der Anbindung ans Internet. Geschieht dies ausserhalb der normalen Bürozeiten, so fallen Kosten infolge von Überstunden ins Gewicht. Es ist nicht davon auszugehen, dass Arp Datacon einen grossen Kundenverlust erleidet. Möglich ist, dass einzelne Kunden bei einen anderen E-Shop bestellen. Imageschaden bei dieser Schadensdauer ist nicht zu erwarten.

Der Schaden bei einem solchen Szenario beläuft sich gemäss unseren Überlegungen und Schätzungen auf über CHF 10'000. Ist die Wiederherstellung des Betriebs ausschliesslich Sache einer Drittfirma, so können diese Kosten massiv gesenkt werden.

4.5.4 Webhoster

Die Vielfalt an bestehenden Webhostern ist gross. Sie führt von Privatpersonen, die einen Computer als Server betreiben und einige Websites verwalten bis zu grossen Unternehmen, die Webhosting nur als Teil ihrer Geschäftstätigkeit definieren und den grössten Teil ihres Umsatzes mit anderen Diensten wie Internetzugang erwirtschaften. Die Informationspolitik ist sehr restriktiv. Es sind wenig Daten über Umsätze, Kundenstruktur und Kosten erhältlich. Deshalb schaffen wir für dieses Rechenbeispiel einen fiktiven Webhoster X. Die Zahlen und Annahmen stützen sich auf Recherchen in Internet, Literatur und auf Gespräche [WI03, KÖ03, GR03, FF03b, HC03].

Webhoster X	
Der Webhoster verdient sein Geld mit Hosting von Websites und Webdesign. In diesem Beispiel wird nur der Geschäftsteil Hosting betrachtet.	
6 Mitarbeiter	• 2 Marketing • 2 Technik • 2 Webdesign
800 Hosting-Kunden	Jeder Kunde besitzt im Durchschnitt drei Domains.
2’500 Abonnemente	Die durchschnittlichen Abonnementskosten belaufen sich auf ca. CHF 35 pro Monat.
Umsatz	Ca. CHF 1 Mio. pro Jahr (Abonnemente)

Tabelle 4-4: Beispiel eines Webhosters

Es tritt Szenario II ein. Die Websites sind während einer Woche nicht online, weil die Internetanbindung durch eine DDoS Attacke auf den für den Webhoster X kritischen Backbone vollständig gestört ist.

Beim Webhoster X handelt es sich um einen kleinen Webhoster. Es bestehen nur Best Effort Verträge mit den Kunden. Forderungen von Dritten oder Haftpflichtansprüche können von Kundenseite nicht geltend gemacht werden. Des Weiteren fallen praktisch keine Wiederherstellungskosten an, da der Webhoster selbst Kunde von einem ISP ist. Der Kundenverlust durch verspieltes Vertrauen oder Imageschaden kann jedoch schwer wiegen, auch wenn die Websites schlussendlich nicht durch Verschulden des Webhosters down sind. Schliesslich hätte er sich ja um eine bessere Anbindung ans Internet kümmern können. Somit sind bei diesem Szenario vor allem Kosten zu erwarten, die durch Kundenabgänge in der Zeit nach dem Vorfall (Nichterneuern des Abonnementes) oder durch weniger Neukunden entstehen (Opportunitäten).

In unserem Beispiel belaufen sich die Kosten auf über CHF 150'000. Dies ist bereits ein grosser Betrag, wenn man bedenkt, dass die Störung von einer Woche kostenmässig bereits gut einen Zehntel des Jahresumsatzes durch Webhosting ausmacht.

4.5.5 Telefonnetz-Betreiber

Ein Telefonnetz-Betreiber ist lediglich durch den erlittenen Produktivitätsausfall von einem Ausfall des IP-Backbones betroffen. Ein kurzer Ausfall des IP-Backbones hat noch keine gravierenden Auswirkungen. Im Beispiel wird daher das Szenario II mit einem Ausfall von einer Woche verwendet. Stellvertretend für die Vielzahl an neuen Telefonnetz-Betreibern in der Schweiz, wird im Beispiel die Firma Sunrise betrachtet.

Da das Telefonnetz selbst immer noch funktionsfähig ist, kommt es zu keinem Umsatzverlust. Aus diesem Grund sind auch keine Forderungen von Dritten zu erwarten. Sunrise ist während der Störung aber direkt von einem Produktivitätsverlust betroffen. Es wird angenommen, dass der Zugriff auf das firmeninterne Netzwerk nicht mehr funktioniert. Weiter ist auch der E-Mail-Verkehr und der Zugang zum Internet nicht mehr gegeben. Dies hat im Laufe einer Woche eine Produktivitätseinbusse von etwa 50% zur Folge.

Im Beispiel wird die Tätigkeit von Sunrise auf das Betreiben des Telefonnetzes eingeschränkt. In der Funktion eines BSP oder ISP entstehen aber natürlich weitere (weitaus grössere) Kosten, welche separat betrachtet werden müssen. Im Beispiel bewegt sich der Schaden für Sunrise im Bereich von etwa CHF 700’000 bei einer Störung von einer Woche.

4.6 Schaden für die gesamte Schweiz

4.6.1 Vorgehen

Eine Ausweitung des betrachteten Bereichs auf alle Unternehmen in der Schweiz ermöglicht eine Abschätzung des maximal möglichen Schadens (Worst Case Betrachtung). Es wird davon ausgegangen, dass entsprechend den Szenarien in Kapitel 4.5 sämtliche IP-Backbones in der Schweiz vollständig ausfallen. Aus diesem Grund werden auch allfällige redundante Anbindungen von Firmen etc. nicht betrachtet. Erneut wird eine Störungsdauer von 24 Stunden bzw. von 1 Woche angenommen.

Um den gesamtschweizerischen Schaden abschätzen zu können, müssen für alle Firmen ähnliche Überlegungen zu den Beispielen in Kapitel 4.5 gemacht werden. Sämtliche Teilschäden müssen aufsummiert werden. Aufgrund der Komplexität dieser Betrachtung wird hier jedoch ein „top down“ Vorgehen verwendet: Ausgehend von der Branchenstruktur und vom ausgewiesenen Gesamtumsatz in der Schweiz, werden anhand der Abhängigkeiten zu einer funktionierenden IT-Infrastruktur die Grössenordnungen des gesamten Schadens in der Schweiz abgeschätzt.

4.6.2 Abschätzungen

Die durchschnittlichen Mitarbeiter-Produktivitätskosten belaufen sich in der Schweiz auf CHF 98'075 pro Jahr [BS03a, BS03b]. Es wird angenommen, dass während der ersten 24 Stunden der Produktivitätsverlust der Mitarbeiter noch kleiner ist als bei einem Ausfall von einer Woche. Oftmals können während eines Tages andere Arbeiten unabhängig vom Computer ausgeführt bzw. Offline-Dateien am Computer bearbeitet werden. Nach einer Woche sinkt die Produktivität der Mitarbeiter jedoch deutlich (Annahme: 50%), da z.B. auch die Kommunikation via E-Mail nicht mehr möglich ist. Zu Beginn seien primär die Grosskonzerne betroffen, welche standortübergreifende Firmennetzwerke besitzen und somit direkt vom Ausfall der IP-Backbones betroffen sind. Kleinere Firmen betreiben oft ein kleines Netzwerk lediglich innerhalb eines Gebäudes und sind somit nicht unmittelbar vom Ausfall betroffen. Es wird jedoch angenommen, dass der Produktivitätsverlust nach einer Woche sämtliche Firmen der IT-intensiven Branche betrifft.

Mit einem ausgewiesenen Gesamtumsatz in der Schweiz von etwas mehr als 1000 Mrd. CHF [BS97] und einem Anteil der IT-intensiven Branchen von 48,2% [CS02] lässt sich der Umsatz abschätzen, welcher stark von einer funktionierenden IT-Infrastrukur abhängt. Entsprechend kann der Umsatzverlust für die Firmen abgeschätzt werden, falls die IP-Backbones nicht mehr zur Verfügung stehen.

Die Wiederherstellungskosten variieren stark zwischen den verschiedenen Unternehmen (siehe Kapitel 4.2). In der Abschätzung gehen wir davon aus, dass etwa 1% aller Arbeitskräfte in den betroffenen Firmen direkt an der Wiederherstellung der Dienste beteiligt sind.

Bei der Betrachtung aller Firmen in der Schweiz muss eine Doppelzählung vermieden werden. Entsprechend sind in den Abschätzungen keine Kundenverluste oder Forderungen von Dritten enthalten. Da alle Firmen gleichermassen betroffen sind, gibt es für die Kunden keine Veranlassung, ihren Anbieter zu wechseln. Sollten sie es trotzdem tun, entsteht bei einer gesamtschweizerischen Betrachtung aber kein Schaden, da der Verlust eines Kunden der Firma A in der Regel den Gewinn eines Neukunden für die Firma B bedeutet. Auch allfällige Forderungen aus Konventionalstrafen sind zur Vermeidung von Doppelzählungen nicht enthalten, da die Zahlung einer Strafe den Schaden für die Firma A zwar erhöht, ihn für die Firma B aber reduziert. Diese Annahmen treffen natürlich nur unter der Bedingung einer geschlossenen Schweizer Volkswirtschaft zu. Sie dienen der Reduktion der Komplexität.

Allfällige gesamtwirtschaftliche Schäden aufgrund von Verlusten an der Börse und damit verminderten Unternehmenswerten sind in der Betrachtung ausgeklammert. Deutliche Auswirkungen an der Börse werden noch nicht nach einem Ausfall von 24 Stunden erwartet, sondern erst nach mehreren Tagen [WI03]. Das Szenario eines Ausfalls sämtlicher IP-Backbones in der Schweiz für eine Woche dient der Abschätzung einer oberen Grenze des Schadens. Realistischer scheint ein Teilausfall der Netzte, weshalb die konkreten Auswirkungen auf die Börsenkurse jeweils separat für die betroffenen Firmen betrachtet werden müssten.

Der Schaden eines vollständigen Ausfalls aller IP-Backbones in der Schweiz beläuft sich entsprechend der Ausführungen im Appendix (Kapitel 7.5 und 7.6) auf etwa CHF 310 Mio. für einen Tag und auf knapp CHF 6 Mrd. für eine Woche. Wie erwähnt sind in diesen Zahlen keine Forderungen von Dritten und keine Auswirkungen eines Kundenverlusts enthalten.

Der Schaden steigt mit der Zeit mehr als linear. Grund ist der zunehmende Produktivitätsverlust bei den Mitarbeitern und die wachsende Anzahl von Unternehmen, welche direkt betroffen sind. Kommen Verluste an der Börse, Konventionalstrafen und Kundenverluste hinzu, so kann von einem exponentiellen Verlauf der Schadenshöhe für die einzelnen Firmen ausgegangen werden. Begrenzt wird dieser Schaden lediglich durch die den Unternehmenswerte an der Börse und durch die Reserven des Unternehmens. Es ist schwierig abzuschätzen, nach welcher Zeit dieser maximale Schaden erreicht sein wird, da grosse Unterschiede zwischen den einzelnen Firmen vorhanden sind. Nach einer Woche sind aber auf jeden Fall bereits deutliche Anzeigen davon sichtbar [WI03].

5 ZUSAMMENFASSUNG

Es gibt direkten und indirekten wirtschaftlichen Schaden infolge einer DDoS Attacke auf Backbone-Provider. Tritt der Schaden unmittelbar nach Eintritt einer technischen Störung eines Backbone-Netzes ein, so sprechen wir von einem direkten Schaden (z.B. Umsatzverlust). Wenn der Schaden jedoch erst nach einer gewissen Zeit eintritt, so handelt es sich um einen indirekten Schaden (z.B. Kundenverlust). Der wirtschaftliche Schaden ist eine Funktion der Zeit.

Die Bedeutung eines wirtschaftlichen Schadens ist nicht nur von dessen Ausmass und der Störungsdauer abhängig. Vielmehr muss auch die Eintrittswahrscheinlichkeit betrachtet werden. Ist das Schadenspotential gross, die Eintrittswahrscheinlichkeit jedoch sehr klein, so ist die Gefährdung dementsprechend gering. Diese Arbeit ging davon aus, dass eine Störung des Backbone-Netzes eintritt (Eintrittswahrscheinlichkeit 100%). Aufgrund dieser Störung wurde der Schaden bemessen.

Betrachtet man den wirtschaftlichen Schaden, der infolge einer DDoS Attacke auf ein Backbone-Netz eintritt, so muss man verschiedene Schadensarten unterscheiden. Entgangener Umsatz und Wiederherstellungskosten des Betriebs sind direkte Kosten. Sie fallen unmittelbar nach Eintritt der Störung an. Beim Umsatz handelt es sich um Opportunitätskosten. Potentieller Umsatz geht verloren. Auch Forderung durch Dritte, sei dies durch Haftpflichtansprüche oder Konventionalstrafen, sind direkte Kosten. Meistens fallen diese mit einer gewissen zeitlichen Verzögerung gegenüber der Störung an. Gehen bestehende oder potentielle Kunden verloren, so schlägt sich auch dies im Umsatz nieder (Opportunität). In der Regel handelt es sich dabei um indirekte Kosten. Nicht alle Schadensarten treten bei allen Geschädigten gleichzeitig auf.

Grafiken zeigen den zeitlichen Verlauf des wirtschaftlichen Schadens für einen Geschädigten. Die Relationen für verschiedene betroffene Unternehmen werden deutlich. So erleidet ein E-Shop, der all seinen Umsatz über das Internet macht, prozentual zu seinem Gesamtumsatz mehr Schaden als ein Grosskonzern, der nur einen Teil seiner Produkte online absetzt. Nicht alle Schadensarten verlaufen linear über die Zeit.

In „Schadensformeln“ werden die verschiedenen Schadensarten in Parameter (Input) zerlegt. Durch Erhebung von Inputgrössen aufgrund einer vorgefallenen Störung kann der Schaden (Output) geschätzt werden.

Konkrete Beispiele von bereits eingetretenen Schäden und das Aufzeigen von Schadenspotentialen bei Unternehmen schaffen ein Gespür für die Grössenordnungen und Dimensionen. Anhand dieser Zahlen können erarbeitete Resultate validiert werden.

Um Schadensfälle zu schätzen, wurden zwei Szenarien eingeführt. Dabei wurde davon ausgegangen, dass ein Backbone-Netz für bestimmte Zeit gestört ist und dessen Dienst vollständig zum Erliegen kommt. Mit Hilfe der grafischen Schadensverläufe und der Formeln wurde der wirtschaftliche Schaden geschätzt.

6 FAZIT

6.1 Erkenntnisse

Das Schadenspotential infolge einer DDoS Attacke auf Backbone-Provider ist beträchtlich. Es kommt vor allem durch die grossen Abhängigkeiten der einzelnen Diensterbringer, Dienste und Dienstbenutzer untereinander zustande. Die grosse Vernetztheit in der Informationstechnologie führt zu hoher Komplexität der Probleme. Um solche Probleme analysieren und lösen zu können (so zum Beispiel die Abschätzung von wirtschaftlichem Schaden), ist es zwingend, eine klare Systemabgrenzung zu machen, die Betrachtungen auf diesen Bereich zu konzentrieren und Annahmen zu treffen.

Die Erhebung von wirtschaftlichem Schaden infolge einer DDoS Attacke auf Backbone-Provider ist anspruchsvoll. Zum einen fehlen Erfahrungen aus der Vergangenheit, zum anderen lässt sich diese Art von Schaden nicht eindeutig berechnen. Es müssen Schätzungen gemacht werden, um sich der Grössenordnung und Dimensionen bewusst zu werden. Schätzungen basieren auf bekannten Grössen, aber auch auf Annahmen. Ist ein Schaden noch nicht eingetreten, so stehen nicht alle Informationen, die man zu dessen Berechnung benötigt, zur Verfügung. Die Annahmen müssen fundiert sein. Klare Argumentation ist im Sinne der Nachvollziehbarkeit der Schätzung unabdingbar. Nur so können erarbeitete Resultate in weiterführenden Betrachtungen sinnvoll verwendet werden.

6.2 Ausblick

Die Informationstechnologie entwickelt sich stetig weiter. Die Abhängigkeiten unserer Gesellschaft von der Technik steigen. Die Anzahl und vor allem die Vielfalt der Bedrohungen, die daraus erwachsen, nehmen zu. Unter der steigenden Komplexität der Systeme kann die Übersicht leiden. Es ist möglich, als einzelner Internet-User eine DDoS Attacke zu starten und dabei infolge fehlender Rückverfolgbarkeit nicht zur Rechenschaft gezogen werden zu können. Es ist immer mehr Geld im Spiel. E-Banking und E-Commerce sind im Vormarsch. Umsätze werden vermehrt durch Verbindung von Handel mit moderner Kommunikationstechnik gemacht. Unternehmen sind auf das tadellose Funktionieren der Kommunikationsnetze angewiesen, um ihre Geschäfte machen zu können.

Wirtschaftlicher Schaden infolge technischer Störung kann nie ganz ausgeschlossen werden. Es können jedoch präventiv Massnahmen getroffen werden, um die Risiken zu verkleinern. Bei der Erarbeitung von präventiven Massnahmen müssen die Aspekte Schadenspotential, Eintrittswahrscheinlichkeit und Rentabilität der Investitionen integral betrachtet werden.

7 APPENDIX

7.1 Backbone Service Provider (Kapitel 4.5.2)

	Störungsdauer	*(h)*	**24**
	davon Bürozeiten	*(h)*	**8**
	davon Betriebszeiten der technischen Infrastruktur	*(h)*	**24**
	Ausfallgrad des gestörten Dienstes	*(%)*	**100.0%**
	Downtime Kosten		
	Verringerte Produktivität		
1	Mitarbeiter-Produktivitätskosten	*(CHF/Jahr*MA)*	**98'075**
2	Arbeitszeit	*(h/Jahr)*	**1'880**
3	Anzahl Mitarbeiter von Störung betroffen	*(# Mitarbeiter)*	**3'500**
4	Verringerung der Produktivität der Mitarbeiter	*(%)*	**20.0%**
5			**CHF 292'138**
	Entgangener Umsatz		
6	Ø Umsatz	*(CHF/Jahr)*	**2'815'000'000**
7	Betriebszeit, Dienstverfügbarkeit	*(h/Jahr)*	**8'760**
8	Anteil des Umsatzes von Störung betroffen	*(%)*	**0.0%**
9	Anteil des Umsatzes, der später realisiert wird	*(%)*	**0.0%**
10			**CHF 0**
	Wiederherstellung des Betriebs		
11	Anteil der mit Instandsetzung beschäftigten MA	*(%)*	**50.0%**
12	Instandsetzungs-Team	*(# Mitarbeiter)*	**1'750**
13	Stundensatz Instandsetzungs-Team	*(CHF/h)*	**150**
14	Materialkosten	*(CHF)*	**1'000'000**
15	Arbeitszeit ausserhalb der Bürozeiten	*(h)*	**16**
16			**CHF 5'200'000**
	Forderung von Dritten		
17	Konventionalstrafen	*(CHF)*	**15'000'000**
18	Haftpflichtansprüche	*(CHF)*	**0**
19			**CHF 15'000'000**
20	**Kundenverlust**		
21	Betrachtetes Zeitintervall	*(Jahre)*	**1**
22	Verlust an bestehenden Kunden	*(#/Jahr)*	**20**
23	Verlust an potentiellen Kunden	*(#/Jahr)*	**5**
24	Ø Umsatz pro Kunde	*(CHF/Jahr)*	**500'000**
25			**CHF 12'500'000**
	Total wirtschaftlicher Schaden	***(CHF)***	**32'992'138**

1 Quelle: Bundesamt für Statistik [BS03a, BS03b]
2 Annahme: 40 Stunden pro Woche; 5 Wochen Ferien pro Jahr
3 Quelle: Swisscom Geschäftsbericht 2002 [SC02]
4 Arbeit am Computer nur noch eingeschränkt möglich
Zugriff auf Firmennetzwerk (standortübergreifend) nicht mehr möglich
E-Mail Verkehr und Internet-Zugriff nicht mehr möglich
6 Annahme: Anteil von Wholesale am Gesamtumsatz von Fixnet entspricht dem Verhältnis der Mitarbeiterzahlen
44% des Umsatzes von Fixnet fällt bei Wholesale an (Quelle: Swisscom Geschäftsbericht 2002 [SC02])
7 Annahme: Dienste 7x24h verfügbar
8 Umsatzverlust während der Störung vernachlässigt
10 Annahme: Keine datenmengenabhängigen Gebühren
11 Beinhaltet auch Zuzug von externen Fachleuten
13 Eigener Erfahrungswert
14 Durch Software-Updates, neue Hardware, etc.
Wird i.d.R. durch Hersteller des Equipments übernommen [BU03]
17 Beispiel: Bewegt sich in realistischer Grössenordnung
Konventionalstrafe deckt in der Regel Teile des Schadens ab, welcher die eigenen Kunden durch die Störung erlitten haben
Genauer Betrag muss innerhalb der entsprechenden Firma anhand der Verträge mit den Kunden ermittelt werden [WI03]
18 Keine Haftpflichtansprüche
Annahme: Es kann Wholesale keine Fahrlässigkeit nachgewiesen werden.
20 Anmerkungen:
Ansprechpartner für Firmenkunden ist in der Regel Swisscom Enterprise Solutions.
Fixnet Wholesale stellt technische Infrastruktur zur Verfügung.
22 Annahme: Wechselkosten für Kunden (Grossfirmen, Operators) hoch
Geringer Kundenverlust
Anpassung der bestehenden Verträge denkbar
23 Annahme: Wenig Alternativen zu Wholesale in der Schweiz
Geringer Verlust an potentiellen Kunden
24 Beispiel: Bewegt sich in realistischer Grössenordnung
Genauer Betrag muss innerhalb der entsprechenden Firma ermittelt werden [WI03].

Tabelle 7-1: Rechenbeispiel Backbone Service Provider

7.2 Firmenkunde (Kapitel 4.5.3)

	Störungsdauer	*(h)*	**24**
	davon Bürozeiten	*(h)*	**8**
	davon Betriebszeiten der technischen Infrastruktur	*(h)*	**24**
	Ausfallgrad des gestörten Dienstes	*(%)*	**100.0%**
	Downtime Kosten		
	Verringerte Produktivität		
1	Mitarbeiter-Produktivitätskosten	*(CHF/Jahr*MA)*	**98'075**
2	Arbeitszeit	*(h/Jahr)*	**1'880**
3	Anzahl Mitarbeiter von Störung betroffen	*(# Mitarbeiter)*	**90**
4	Verringerung der Produktivität der Mitarbeiter	*(%)*	**10.0%**
5			**CHF 3'756**
	Entgangener Umsatz		
6	Ø Umsatz	*(CHF/Jahr)*	**103'000'000**
7	Betriebszeit, Dienstverfügbarkeit	*(h/Jahr)*	**8'760**
8	Anteil des Umsatzes von Störung betroffen	*(%)*	**41.0%**
9	Anteil des Umsatzes, der später realisiert wird	*(%)*	**39.0%**
10			**CHF 5'644**
	Wiederherstellung des Betriebs		
11	Anteil der mit Instandsetzung beschäftigten MA	*(%)*	**2.0%**
12	Instandsetzungs-Team	*(# Mitarbeiter)*	**2**
13	Stundensatz Instandsetzungs-Team	*(CHF/h)*	**150**
14	Materialkosten	*(CHF)*	**0**
15	Arbeitszeit ausserhalb der Bürozeiten	*(h)*	**16**
16			**CHF 4'320**
	Forderung von Dritten		
17	Konventionalstrafen	*(CHF)*	**0**
18	Haftpflichtansprüche	*(CHF)*	**0**
19			**CHF 0**
	Kundenverlust		
20	Betrachtetes Zeitintervall	*(Jahre)*	**0**
21	Verlust an bestehenden Kunden	*(#/Jahr)*	**0**
22	Verlust an potentiellen Kunden	*(#/Jahr)*	**0**
23	Ø Umsatz pro Kunde	*(CHF/Jahr)*	**0**
24			**CHF 0**
	Total wirtschaftlicher Schaden	***(CHF)***	**13'720**

1 Quelle: Bundesamt für Statistik [BS03a, BS03b]
Volkseinkommen bezogen auf tatsächliche Arbeitskräfte
2 Annahme: 40 Stunden Woche; 5 Wochen Ferien pro Jahr
3 Quelle: Fallstudie Arp Datacon [EU03]
Annahme (gesamthaft 122 Mitarbeiter)
4 Schätzung
5 Tritt nur während Bürozeiten auf
6 Quelle: Fallstudie Arp Datacon [EU03]
7 Dienst jeden Tag rund um die Uhr verfügbar
8 Quelle: Quelle Neue Zürcher Zeitung [NZZ02a]
9 95% von 41%
10 Annahme
11 Schätzung
13 Eigener Erfahrungswert
14 vernachlässigbar
15 Nur zusätzliche Kosten für Überstunden, Nachtarbeit, etc.

Tabelle 7-2: Rechenbeispiel Firmenkunde

7.3 Webhoster (Kapitel 4.5.4)

	Störungsdauer	*(h)*	**168**
	davon Bürozeiten	*(h)*	**40**
	davon Betriebszeiten der technischen Infrastruktur	*(h)*	**168**
	Ausfallgrad des gestörten Dienstes	*(%)*	**100.0%**
	Downtime Kosten		
	Verringerte Produktivität		
1	Mitarbeiter-Produktivitätskosten	*(CHF/Jahr*MA)*	**98'075**
2	Arbeitszeit	*(h/Jahr)*	**1'880**
3	Anzahl Mitarbeiter von Störung betroffen	*(# Mitarbeiter)*	**4**
4	Verringerung der Produktivität der Mitarbeiter	*(%)*	**20.0%**
5			**CHF 1'669**
	Entgangener Umsatz		
6	Ø Umsatz	*(CHF/Jahr)*	**1'000'000**
7	Betriebszeit, Dienstverfügbarkeit	*(h/Jahr)*	**8'760**
8	Anteil des Umsatzes von Störung betroffen	*(%)*	**0.0%**
9	Anteil des Umsatzes, der später realisiert wird	*(%)*	**0.0%**
10			**CHF 0**
	Wiederherstellung des Betriebs		
11	Anteil der mit Instandsetzung beschäftigten MA	*(%)*	**0.0%**
12	Instandsetzungs-Team	*(# Mitarbeiter)*	**0**
13	Stundensatz Instandsetzungs-Team	*(CHF/h)*	**150**
14	Materialkosten	*(CHF)*	**0**
15	Arbeitszeit ausserhalb der Bürozeiten	*(h)*	**128**
16			**CHF 0**
	Forderung von Dritten		
17	Konventionalstrafen	*(CHF)*	**0**
18	Haftpflichtansprüche	*(CHF)*	**0**
19			**CHF 0**
	Kundenverlust		
20	Betrachtetes Zeitintervall	*(Jahre)*	**1**
21	Verlust an bestehenden Kunden	*(#/Jahr)*	**100**
22	Verlust an potentiellen Kunden	*(#/Jahr)*	**30**
23	Ø Umsatz pro Kunde	*(CHF/Jahr)*	**1'300**
24			**CHF 169'000**
	Total wirtschaftlicher Schaden	***(CHF)***	**170'669**

1 Quelle: Bundesamt für Statistik [BS03a, BS03b]
Volkseinkommen bezogen auf tatsächliche Arbeitskräfte
2 Annahme: 40 Stunden Woche; 5 Wochen Ferien pro Jahr
3 Annahme: nur technische Funktionen betroffen
4 Schätzung (Offline-Arbeiten möglich)
5 Tritt nur während Bürozeiten auf
6 Annahme Webhoster X
7 Websites rund um die Uhr online
8 Umsatz entspricht den Abonnementseinnahmen
9 Umsatz entspricht den Abonnementseinnahmen
10 Annahme: Keine datenmengenabhängigen Gebühren
11 Wiederherstellung nicht Sache des Webhosters
13 Eigener Erfahrungswert
14 Vernachlässigt
15 Nur zusätzliche Kosten für Überstunden, Nachtarbeit, etc.
21 Annahme Webhoster X
22 Annahme Webhoster X

Tabelle 7-3: Rechenbeispiel Webhoster

7.4 Telefonnetz-Betreiber (Kapitel 4.5.5)

	Störungsdauer	*(h)*	**168**
	davon Bürozeiten	*(h)*	**40**
	davon Betriebszeiten der technischen Infrastruktur	*(h)*	**168**
	Ausfallgrad des gestörten Dienstes	*(%)*	**100.0%**
	Downtime Kosten		
	Verringerte Produktivität		
1	Mitarbeiter-Produktivitätskosten	*(CHF/Jahr*MA)*	**98'075**
2	Arbeitszeit	*(h/Jahr)*	**1'880**
3	Anzahl Mitarbeiter von Störung betroffen	*(# Mitarbeiter)*	**700**
4	Verringerung der Produktivität der Mitarbeiter	*(%)*	**50.0%**
5			**CHF 730'346**
	Entgangener Umsatz		
6	Ø Umsatz	*(CHF/Jahr)*	**360'000'000**
7	Betriebszeit, Dienstverfügbarkeit	*(h/Jahr)*	**8'760**
8	Anteil des Umsatzes von Störung betroffen	*(%)*	**0.0%**
9	Anteil des Umsatzes, der später realisiert wird	*(%)*	**0.0%**
10			**CHF 0**
	Wiederherstellung des Betriebs		
11	Anteil der mit Instandsetzung beschäftigten MA	*(%)*	**0.0%**
12	Instandsetzungs-Team	*(# Mitarbeiter)*	**0**
13	Stundensatz Instandsetzungs-Team	*(CHF/h)*	**150**
14	Materialkosten	*(CHF)*	**0**
15	Arbeitszeit ausserhalb der Bürozeiten	*(h)*	**128**
16			**CHF 0**
	Forderung von Dritten		
17	Konventionalstrafen	*(CHF)*	**0**
18	Haftpflichtansprüche	*(CHF)*	**0**
19			**CHF 0**
	Kundenverlust		
20	Betrachtetes Zeitintervall	*(Jahre)*	**1**
21	Verlust an bestehenden Kunden	*(#/Jahr)*	**0**
22	Verlust an potentiellen Kunden	*(#/Jahr)*	**0**
23	Ø Umsatz pro Kunde	*(CHF/Jahr)*	**422**
24			**CHF 0**
	Total wirtschaftlicher Schaden	***(CHF)***	**730'346**

1 Quelle: Bundesamt für Statistik [BS03a, BS03b]
2 Annahme: 40 Stunden pro Woche; 5 Wochen Ferien pro Jahr
3 Annahme: Knapp 30% aller Mitarbeiter bei Sunrise sind im Bereich der Festnetz-Telefonie tätig.
4 Arbeit am Computer nur noch eingeschränkt möglich
Zugriff auf Firmennetzwerk (standortübergreifend) nicht mehr möglich
E-Mail Verkehr und Internet-Zugriff nicht mehr möglich
6 Annahme: 20% des Gesamt-Umsatzes stammen aus der Festnetz-Telefonie
Quelle: TDC Geschäftsbericht 2002 [TDC02], TDC Geschäftsbericht 2001 [TDC01]
7 Annahme: Dienste 7x24h verfügbar
11 Keine Wiederherstellung notwendig
13 Eigener Erfahrungswert
14 Vernachlässigt
19 Keine Forderungen von Dritten, da Telefonie-Dienste noch verfügbar sind
23 360 Mio. CHF Umsatz in der Festnetz-Telefonie mit 852'000 Kunden

Tabelle 7-4: Rechenbeispiel Telefonnetz-Betreiber

7.5 Gesamte Schweiz: Szenario I (Kapitel 4.6.2)

	Störungsdauer	*(h)*	**24**
	davon Bürozeiten	*(h)*	**8**
	davon Betriebszeiten der technischen Infrastruktur	*(h)*	**24**
	Ausfallgrad des gestörten Dienstes	*(%)*	**100.0%**
	Downtime Kosten		
	Verringerte Produktivität		
1	Mitarbeiter-Produktivitätskosten	*(CHF/Jahr*MA)*	**98'075**
2	Arbeitszeit	*(h/Jahr)*	**1'880**
3	Arbeitsplätze in der Schweiz	*(# Mitarbeiter)*	**3'590'000**
4	*davon in IT-intensiven Branchen*	*(%)*	**48.2%**
5	Arbeitsplätze in IT-intensiven Branchen	*(# Mitarbeiter)*	**1'730'380**
6	*davon direkt betroffen*	*(%)*	**60.0%**
7	Anzahl Mitarbeiter von Störung betroffen	*(# Mitarbeiter)*	**1'038'228**
8	Verringerung der Produktivität der Mitarbeiter	*(%)*	**20.0%**
9			**CHF 86'658'903**
	Entgangener Umsatz		
10	Ø Umsatz	*(CHF/Jahr)*	**484'000'000'000**
11	Betriebszeit, Dienstverfügbarkeit	*(h/Jahr)*	**8'760**
12	Anteil des Umsatzes von Störung betroffen	*(%)*	**20.0%**
13	Anteil des Umsatzes, der später realisiert wird	*(%)*	**5.0%**
14			**CHF 198'904'110**
	Wiederherstellung des Betriebs		
15	Anteil der mit Instandsetzung beschäftigten MA	*(%)*	**1.0%**
16	Instandsetzungs-Team	*(# Mitarbeiter)*	**10'382**
17	Stundensatz Instandsetzungs-Team	*(CHF/h)*	**150**
18	Materialkosten	*(CHF)*	**0**
19	Arbeitszeit ausserhalb der Bürozeiten	*(h)*	**16**
20			**CHF 24'917'472**
	Forderung von Dritten		
21	Konventionalstrafen	*(CHF)*	**0**
22	Haftpflichtansprüche	*(CHF)*	**0**
23			**CHF 0**
	Kundenverlust		
24	Betrachtetes Zeitintervall	*(Jahre)*	**0**
25	Verlust an bestehenden Kunden	*(#/Jahr)*	**0**
26	Verlust an potentiellen Kunden	*(#/Jahr)*	**0**
27	Ø Umsatz pro Kunde	*(CHF/Jahr)*	**0**
28			**CHF 0**
	Total wirtschaftlicher Schaden	***(CHF)***	**310'480'485**

1 Quelle: Bundesamt für Statistik [BS03a, BS03b]
2 Annahme: 40 Stunden pro Woche; 5 Wochen Ferien pro Jahr
3 Quelle: Bundesamt für Statistik [BS03b]
4 Quelle: Credit Suisse [CS00]
6 Grosskonzerne und Teile der KMU
8 Arbeit am Computer nur noch eingeschränkt möglich
Zugriff auf Firmennetzwerk (standortübergreifend) nicht mehr möglich
E-Mail Verkehr und Internet-Zugriff nicht mehr möglich
10 Quellen: Bundesamt für Statistik [BS97]; Credit Suisse [CS00]
11 Annahme: Dienste 7x24h verfügbar
17 Eigener Erfahrungswert
18 Vernachlässigt
23 Vermeiden von Doppelzählung bei Betrachtung aller Firmen
28 Vermeiden von Doppelzählung bei Betrachtung aller Firmen

Tabelle 7-5: Rechenbeispiel gesamte Schweiz (Szenario I)

7.6 Gesamte Schweiz: Szenario II (Kapitel 4.6.2)

	Störungsdauer	*(h)*	**168**
	davon Bürozeiten	*(h)*	**40**
	davon Betriebszeiten der technischen Infrastruktur	*(h)*	**168**
	Ausfallgrad des gestörten Dienstes	*(%)*	**100.0%**
	Downtime Kosten		
	Verringerte Produktivität		
1	Mitarbeiter-Produktivitätskosten	*(CHF/Jahr*MA)*	**98'075**
2	Arbeitszeit	*(h/Jahr)*	**1'880**
3	Arbeitsplätze in der Schweiz	*(# Mitarbeiter)*	**3'590'000**
4	*davon in IT-intensiven Branchen*	*(%)*	**48.2%**
5	Arbeitsplätze in IT-intensiven Branchen	*(# Mitarbeiter)*	**1'730'380**
6	*davon direkt betroffen*	*(%)*	**100.0%**
7	Anzahl Mitarbeiter von Störung betroffen	*(# Mitarbeiter)*	**1'730'380**
8	Verringerung der Produktivität der Mitarbeiter	*(%)*	**50.0%**
9			**CHF 1'805'393'814**
	Entgangener Umsatz		
10	Ø Umsatz	*(CHF/Jahr)*	**484'000'000'000**
11	Betriebszeit, Dienstverfügbarkeit	*(h/Jahr)*	**8'760**
12	Anteil des Umsatzes von Störung betroffen	*(%)*	**50.0%**
13	Anteil des Umsatzes, der später realisiert wird	*(%)*	**10.0%**
14			**CHF 3'712'876'712**
	Wiederherstellung des Betriebs		
15	Anteil der mit Instandsetzung beschäftigten MA	*(%)*	**1.0%**
16	Instandsetzungs-Team	*(# Mitarbeiter)*	**17'304**
17	Stundensatz Instandsetzungs-Team	*(CHF/h)*	**150**
18	Materialkosten	*(CHF)*	**0**
19	Arbeitszeit ausserhalb der Bürozeiten	*(h)*	**128**
20			**CHF 332'232'960**
	Forderung von Dritten		
21	Konventionalstrafen	*(CHF)*	**0**
22	Haftpflichtansprüche	*(CHF)*	**0**
23			**CHF 0**
	Kundenverlust		
24	Betrachtetes Zeitintervall	*(Jahre)*	**0**
25	Verlust an bestehenden Kunden	*(#/Jahr)*	**0**
26	Verlust an potentiellen Kunden	*(#/Jahr)*	**0**
27	Ø Umsatz pro Kunde	*(CHF/Jahr)*	**0**
28			**CHF 0**
	Total wirtschaftlicher Schaden	***(CHF)***	**5'850'503'486**

1 Quelle: Bundesamt für Statistik [BS03a, BS03b]
2 Annahme: 40 Stunden pro Woche; 5 Wochen Ferien pro Jahr
3 Quelle: Bundesamt für Statistik [BS03b]
4 Quelle: Credit Suisse [CS00]
6 Alle Firmen
8 Arbeit am Computer nur noch eingeschränkt möglich
Zugriff auf Firmennetzwerk (standortübergreifend) nicht mehr möglich
E-Mail Verkehr und Internet-Zugriff nicht mehr möglich
10 Quellen: Bundesamt für Statistik [BS97]; Credit Suisse [CS00]
11 Annahme: Dienste 7x24h verfügbar
17 Eigener Erfahrungswert
18 Vernachlässigt
23 Vermeiden von Doppelzählung bei Betrachtung aller Firmen
28 Vermeiden von Doppelzählung bei Betrachtung aller Firmen

Tabelle 7-6: Rechenbeispiel gesamte Schweiz (Szenario II)

LITERATURVERZEICHNIS

[BS03a] Bundesamt für Statistik (2003). Statistik Schweiz: Eckdaten. http://www.statistik.admin.ch/stat_ch/ber00/dkan_ch.htm (20.05.03).

[BS03b] Bundesamt für Statistik (2003). Swiss Statistics: Keydata: Economic and Financial Data for Switzerland (19.05.03). http://www.statistik.admin.ch/stat_ch/ber00/imf.htm (20.05.03).

[BS97] Bundesamt für Statistik (1997). Ein steuerbarer Umsatz von über 500 Mio. Franken, Pressemitteilung (16.09.97). http://www.statistik.admin.ch/news/archiv97/dp97080.htm (20.05.03).

[BW01] Bluewin (2001). Swisscom Fixnet und Bluewin: engere Zusammenarbeit, Medienmitteilung (5.10.01). http://www.bluewinag.com/cont/cont_ff_position.html (16.05.03).

[BW02] Bluewin (2002). Bluewin Marktanteil (September 2002). http://www.bluewinag.com/cont/cont_ff_position.html (14.04.03).

[BW03a] Bluewin (2003). ADSL Abos für Business. http://www2.bluewin.ch/services/zugang/adsl/abos_business_d.php (28.04.03).

[BW03b] Bluewin (2003). ADSL Vertragsbedingungen (Januar 2003). http://www2.bluewin.ch/services/zugang/adsl/vertragsbedingungen_d.php#B (29.04.03).

[BW03c] Bluewin (2003). Allgemeine Geschäftsbedingungen von Swisscom AG, geltend für Bluewin AG. http://www2.bluewin.ch/info/terms_d.html (20.05.03).

[CA02] Caccia, F. (2002). Zahlen und Fakten der Telekommunikation, S. 16. http://www.sicta.ch/deutsch/pdf/F.Caccia.pdf (16.04.03).

[CC03a] Cablecom (2003). Cablecom Digital Phone – so funktioniert's. http://www.digitalphone.ch/de/pages/sof_tec.php (28.04.03).

[CC03b] Cablecom (2003). Topnet Global IP: Der symmetrische Internet Zugang mit der garantierten Bandbreite. http://www.cablecom.ch/service_datasheet_topnet_global_ip-2.pdf (12.05.03).

[CC03c] Cablecom (2003). Business Solutions. http://www.cablecom.ch/business_solutions.htm (12.05.03).

[CM03] Cablemodem Schweiz (2003). News: Jahresrückblick, die Zahlen von 2002 (12.04.03). http://www.cablemodem.ch/news/body_news.html (28.04.03).

[CS00] Credit Suisse (2000). Electronic Commerce: (R)evolution für Wirtschaft und Gesellschaft, Economic Research (Januar 2000). http://research.credit-suisse.ch/de/publications/ecobriefing/pdf/eb15_d.pdf (20.05.03).

[DD01] Denning, D. (2001). Cyber Attacks. www.cs.georgetown.edu/~denning/cosc511/fall01/cyber-attack.ppt (27.05.03).

[DR00] Rosenthal, D. (2000). E-Commerce-Versicherungen. http://www.insider.ch/ipd/recht/kapitel3/rch3009.htm (23.04.03).

[EN02] ECommerce News (2002). http://emarkt.ch/newsletters/ecnjan02.pdf (15.03.03).

[EU03] Eugster, J. (2002). E-Procurement Lösung der ARP Datacon. Referenzbeispiel mit der Post. http://experience.fhbb.ch/cases/experience.nsf/volltext/arp (20.05.03)

[FF03a] Feelfree (2003). Allgemeine Geschäftsbedingungen. http://www.feelfree.ch/home.php4?siteAction=agb (15.05.03).

[FF03b] Feelfree (2003). http://www.feelfree.ch/home.php4 (21.05.03).

[FO03] Thissen, H. (2003). Glanz und Elend der Online-Shops. Forum, S. 44 (Ausgabe 2/2003). Forum Verlag GmbH, Konstanz.

[GGA03] Improware (2003). Internet Services im GGA Verbundnetz Reinach: Produkte. http://www.intergga.ch (16.05.03).

[GR03] green.ch (2003). http://www.green.ch (21.05.03).

[HC03] Bluewin Hostcenter (2003). http://www.hostcenter.com/de/ (21.05.03).

[IL03] Internet-Lexikon. http://www.it-group.ch/netlexikon/frame_i.htm (29.04.03).

[IP03] IP-Plus Internet Services (2003). http://www.ip-plus.net (30.04.03).

[IR03] IT Reseller Online (2003). 3,5 Mio. Schweizer nutzen das Internet (10.04.03). http://www.itreseller.ch/default.lasso?Artikel=15354 (28.04.03).

[ITR02] Internet Traffic Report (2002). Backbone DDoS (22.10.02). http://www.internettrafficreport.com/event/2.htm (08.04.03).

[KE97] Keshav, S. (1997). An Engineering Approach to Computer Networking: ATM Networks, the Internet, and the Telephone Network (4. Auflage), S. 498-505. Addison-Wesley, Massachusetts.

[KÖ03] Köthe, N. (2003). Kurzer Bericht vom Webhosting Tag 2003. http://lists.hostsharing.net/archiv/global/2003-April/007262.html (21.05.03).

[LH01] Haldemann, L. (2001). Versicherung von Internet-Risiken, S. 4. http://www.ifi.unizh.ch/ikm/Vorlesungen/inf_recht/2001/Haldemann.pdf (15.04.03).

[NUA00] NUA Internet Surveys (2000). High Speed Users at Risk from Hackers (04.07.2000). http://www.nua.com/surveys/index.cgi?f=VS&art_id=905355884&rel=true (29.04.03).

[NUA03a] NUA Internet Surveys (2003). How many online? (September 2003). http://www.nua.com/surveys/how_many_online/index.html (29.04.03).

[NUA03b] NUA Internet Surveys (2003). Over 36 million DSL lines worldwide (12.02.03). http://www.nua.com/surveys/?f=VS&art_id=905358720&rel=true (29.04.03).

[NZZ00] Neue Zürcher Zeitung (2000). Optoelektronik – einer vielversprechende Industrie (12.12.00). http://www.nzz.ch/2000/12/12/qo/page-article6XE9F.html (29.04.03).

[NZZ01] Neue Zürcher Zeitung (2001). Fragiles Lebenselixier Handy: Der Netzausfall kostet die Swisscom 30 Millionen Franken (30.07.01). http://nzz.gbi.de/NZZ.ein (13.05.03).

[NZZ02a] Neue Zürcher Zeitung (2002). Doppelstrategie mit Katalog und Internet. Online-Shop von Arp Datacon senkt die Betriebskosten (24.11.02). http://www.nzz.ch/2002/09/24/ob/page-article8E01I.html (25.04.03).

[NZZ02b] Neue Zürcher Zeitung (2002). Web-Portale mutieren zu Kundenschaltern (22.03.03). http://www.nzz.ch/netzstoff/2002/2002.03.22-em-article81TE1.html (16.03.03)

[PA02] Patterson, D.A. (2002). A simple way to estimate the Cost of Downtime. http://roc.cs.berkeley.edu/papers/Cost_Downtime_LISA.pdf (13.05.03).

[PE00] Peterson, L.; Davie, B. (2000). Computer Networks: A Systems Approach (Second Edition), S. 624-630. Morgan Kaufmann, San Francisco.

[PT01] Pressetext (2001). Verkettung zweier Fehler Ursache für Swisscom-Absturz: Mobilnetz ist nur zu 99,95 Prozent sicher (31.07.01). http://web.pressetext.ch/reframe.pl.cgi/query.php (08.05.03).

[PT03] Pressetext (2003). Hacker löschen 899 Homepages bei Tiscali Schweiz. http://www.pressetext.ch/pte.mc?pte=030303042&phrase=tiscali (15.05.03).

[SC02] Swisscom (2002). Geschäftsbericht 2002, S.18-24. http://www.swisscom.com/gb02/gb02_d/pdf/geschaeftsbericht.pdf?homepage=geschaeftsbericht2002pdf&lang=de (21.05.03).

[SC03a] Swisscom (2003). ADSL-Boom führt zu Engpässen, Medienmitteilung (24.01.03). http://www.swisscom.com/mr/content/media/index_DE.html?2003 (28.04.03).

[SC03b] Swisscom (2003). Unternehmensprofil. http://www.swisscom-fixnet.ch/fx/content/portrait/corporateprofile/index_DE.html (16.05.03).

[SCES03a] Swisscom Enterprise Solutions (2003). Produkte und Lösungen: LAN Interconnect Service. http://www.swisscom.com/es/products/intraextra/lani.htm (29.04.03).

[SCES03b] Swisscom Enterprise Solutions (2003). LAN Interconnect over IPSS© Service: Das moderne Netzwerk für Ihre unternehmensweiten Kommunikationsbedürfnisse (Januar 2003). http://www.swisscom.com/es/lan-i_over_ipss_factsheet.pdf (29.04.03).

[SEF03] Swiss Economic Forum (2003). KMU Trends 2003. http://www.swisseconomic.ch/index.cfm?FUSEACTION=OBJEKTE_DRITTE&MID=453 (20.05.03).

[SI03] Das Siemens Online Lexikon (2003). http://w3.siemens.de/solutionprovider/_online_lexikon/ (30.04.03).

[SR03] Sunrise Internet Backbone (2003). http://www.sunrise.net/business/bus_dat/bus_dat_ico/bus_ser_net.htm (29.04.03).

[TDC01] TDC Tele Danmark (2002). Annual Report 01. http://download.tdconline.dk/pub/tdc/english/investor/aarsraporter/pdf/aarsrapport_2001_uk.pdf (21.05.03).

[TDC02] TDC Tele Danmark (2003). Annual Report 02. http://download.tdconline.dk/pub/tdc/english/investor/aarsraporter/pdf/Annual_Report2002.pdf (21.05.03).

[TI03] Tiscali (2003). Tiscali Products: Web Hosting. http://products.tiscali.ch/prod-webhosting-index.htm (15.05.03).

[TIC02] TIC The Internet Company AG – Inter.net Schweiz (2002). Stellungsnahme zum Ausfall der Internet-Dienste vom Freitag 15. Februar 2002 (18.02.02). http://web.tic.ch/pressearchiv/2002.02.18.ausfall.backbonel.pdf (04.04.2003).

[UB02] Baumeister, U. (2002). Ein Versicherungsfall mit neuer Dimension: Deckung von Internet-Risiken als heikle Angelegenheit. http://www.nzz.ch/netzstoff/2002/2002.09.24-wi-article8DKDJ.html (16.04.03).

[ZL01] Gesellschaft Schweizer Zahlenlotto (2001). Geschäftsbericht 2001 http://www.sport-toto.ch/uns/gb_gsz_2001_de.pdf (16.05.03)

[ZU00] Züst, R. (2000). Einstieg ins Systems Engineering: Systematisch denken, handeln und umsetzen (2. Auflage), S. 75f. Verlag Industrielle Organisation, Zürich.

[ZU99] Züst, R. (1999). Systems Engineering - kurz und bündig (1. Auflage), S. 26. Verlag Industrielle Organisation, Zürich.

QUELLENVERZEICHNIS

[BU03] Burschka, S./ Straumann, H./ Semling, M., Interview am 17. April 2003. Swisscom Innovations, Security & Service Management, Bern.

[EP03] Ehrensperger, R., Interview am 22. April 2003. Swisscom Fixnet, Network Operations, Platform Management, Zürich.

[WI03] Widmer, P., Interview am 19. Mai 2003. Bluewin, Business-Line Access, Zürich.