An Economic Damage Model for Large-Scale Internet Attacks

Thomas Dübendorfer*, Arno Wagner*, Bernhard Plattner
Computer Engineering and Networks Laboratory (TIK)
Swiss Federal Institute of Technology, ETH-Zentrum, CH-8092 Zurich
{*duebendorfer, wagner, plattner*}*@tik.ee.ethz.ch*

Abstract

Companies that rely on the Internet for their daily business are challenged by uncontrolled massive worm spreading and the lurking threat of large-scale distributed denial of service attacks. We present a new model and methodology, which allows a company to qualitatively and quantitatively estimate possible financial losses due to partial or complete interruption of Internet connectivity. Our systems engineering approach is based on an in-depth analysis of the Internet dependence of different types of enterprises and on interviews with Swiss telcos, backbone and Internet service providers. A discussion of sample scenarios illustrates the flexibility and applicability of our model.

1. Introduction

Reliability and availability of Internet services can be degraded significantly within minutes. This became apparent during the massive worm spreading incidents encountered in 2003, namely SQL Slammer [8], W32/Blaster [9], and Sobig.F [10] as well as the distributed denial of service (DDoS) attack on the root domain name servers [16] in October 2002. These worms had a negative impact on the Internet primarily due to their fast and aggressive spreading behaviour and not because of malicious code that could be used to, e.g., launch a massive DDoS attack. We can only conjecture the impact of destructive and well engineered worms on Internet service quality. Flooding of critical connections and vital services with attack traffic could result in total loss of Internet connectivity.

Companies relying on the Internet for their daily business will inevitably sustain substantial financial damage by such a large-scale attack. On the one hand direct damage (such as e.g. revenue loss during the attack), on the other hand indirect damage (such as e.g. customer loss due to degraded reputation) will be suffered.

Various general risk assessment frameworks such as CMU's OCTAVE [2] or NIST's "Federal IT Security Assessment Framework" [17] exist. They help to define a risk management strategy based on a security policy and can be used to identify vulnerabilities and valuable assets. However, their versatility is also their biggest drawback if applied to an Internet interruption attack scenario. Such frameworks give only general guidelines without concrete loss calculations and an explicit system model.

There are other published estimates of DDoS damage, especially for the United States [13]. It is very hard to evaluate their merit since the methodology usually was not published. D.A. Patterson gives in [18] a simple model for roughly estimating downtime cost including degraded employee productivity. An overview of Internet risk insurance coverage is given in [15].

For a thorough risk analysis, a transparent and comprehensive model and methodology for qualitatively and quantitatively estimating an enterprise's financial loss caused by massive Internet attacks is indispensable. The model we present in this paper could be used to optimise investment into safeguards and preventive measures, and to asses a "cyber risk" insurance policy.

This work is part of the research project DDoSVax [12] that investigates attacks in the SWITCH [19] Internet backbone. Many thanks to our students Jürg Schmid and Peter Weigel for collecting economic data and elaborating on the loss model in their semester thesis.

2. System Model

To assure that our model is built in a systematic and scientific way, we based it on the systems engineering [22] approach. After a conceptual system analysis of the current Internet infrastructure, we categorised loss into various types. Then, we identified and specified relevant elements and their dependences. Finally, in a conceptual synthesis, qualitative and quantitative sample scenarios were established and validated against our model. A well-received industry seminar about our loss model at a large Swiss re-

*Partially funded by the Swiss National Science Foundation under grant 200021-102026/1 and the Swiss Academic Research Network.

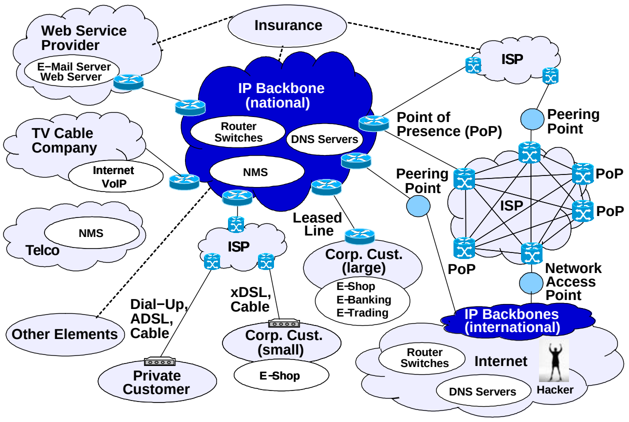

Figure 1. Internet System Model

insurance company Swiss Re [20] helped to cross-check our model and sample scenarios.

2.1. The Internet

Our system analysis resulted in the "Internet System Model" in Figure 1, that shows the relevant system elements and their relationships. The figure gives elements in and out of scope of our model. In order to deal with the complexity of todays Internet infrastructure, it had to be abstracted to a conceptual level. This allowed us to investigate the dependences that are relevant for estimating direct and indirect financial damage caused by attacks on that infrastructure and sustained by the individual elements.

Core elements of the Internet infrastructure are vital services (e.g. Domain Name Service DNS) and networking devices, mainly routers. A national Internet backbone service provider (BSP) typically hosts only large corporate customers and directly connects them to its high-bandwidth communication infrastructure. Usually, a BSP has several peering points to other national and international BSPs and to smaller Internet service providers (ISPs). Small and medium-sized corporate customers, as well as private customers, are commonly connected to one of these ISPs, which are themselves redundantly interconnected to other ISP peers. Many TV cable network companies also provide Internet connectivity and some of them also offer voice over IP (VoIP) services to their customers. In these cases, they also rely on a BSP connection. Traditional telcos typically have their own voice and data communication infrastructure. Their network management system (NMS) is commonly X.25- or IP-based and runs on a dedicated management network. In some cases gateways from the NMS to the Internet exist, however today a telephone company is typically not directly affected by a disruption of Internet connectivity.

2.2. Threat Model and User Impact

Anyone of todays 666 million [1] Internet users is a potential attacker. Many poorly secured computers can be misused by a remote hacker for an attack. In our threat model, we assume that the attacker directly or indirectly attacks a large national Internet backbone service provider with a massive distributed denial of service attack. Degradation of backbone bandwidth up to the complete interruption of Internet connectivity is suffered by the BSP's customers. We assume that the actual attack stops or is stopped after a relatively short time (hours to days). Due to the various dependences of the elements in our system model, such an attack results in massive damage to the BSP and many other elements – from smaller companies up to entire nations.

3. Methodology

Since the effects of a DDoS attack are complex, we took several steps in order to analyse interdependences involved and financial loss incurred by this type of attack. Specifically, we used graphical plots representing damage versus time in a qualitative fashion, mathematical formulae that can be used to calculate the financial loss for the different types of damage, and example scenarios that demonstrate how to calculate financial loss for concrete settings.

Estimating the probability of different types of DDoS attacks is very hard. Estimating the time needed to stop such an attack, if the attacker has designed the attack system in a way that the attack is robust against basic traffic filtering, is currently pure guesswork. Cleanup-durations in the range of several weeks seem possible for sophisticated malicious Internet worms.

The main aim of our model and methodology is to provide a universal tool that can be used to calculate the expected financial loss for a wide variety of concrete scenarios involving Internet DDoS attacks. We will not elaborate on when to transfer the risk by getting insurance.

3.1. Damage vs. Time

Financial loss is an expected effect of any significant degradation of Internet performance. Furthermore financial loss changes over time. Economic damage usually has not the same characteristics over time as technical problems have. Economic damage can still grow when technical problems have been resolved and the attack has stopped. It is therefore reasonable to evaluate damage for the time $t \longrightarrow \infty$ as a first approach. Several examples can be found in Section 5 and Figure 2. We set $t = t_0$ as the time at which the attack starts and $t = t_1$ as the time at which the attack has been completely stopped. The time interval $[t_1, t_2]$ represents the time shortly after the attack, while $t > t_2$ refers to the time period a longer time after the incident. Times $t > t_2$ may e.g. be weeks to months later. We do not model the case that the technical problems cannot be solved for a longer time or cannot be solved at all.

3.2. Types of damage

We subdivide financial damage (as the result of the interruption of Internet services) into four categories:

Downtime Loss The downtime costs can be split further into *productivity loss* (employees can no longer do “business as usual” and have to use less efficient ways to fulfil their duties; certain tasks can only be done later) and *revenue loss* (lost transactions by customers that cannot access a service or due to the inability of a company to fulfil customer requests).

Disaster Recovery Costs of the time that employees and external staff have to spend on recovery from an incident. Additionally, material costs can arise.

Liability Many companies offer service level agreements (SLAs) to their customers. In case that their service quality deviates from an SLA, the customer can claim compensation payments. Liability related losses can be partially insured and typically arise several days after the incident.

Customer Loss Customers being dissatisfied by degraded service quality might terminate their contract. The rate of new customers joining a service can substantially drop if the reputation of a company suffers. These opportunity costs arise typically weeks to months after an incident.

4. Calculating Financial Loss

Financial loss has to be quantified. While the mathematics used is relatively basic, there are many factors to be considered. The factors present in our formulae stem from the synthesis of our interviews with Internet dependent enterprises ([7], [14], [21]). The calculations are only approximations. However, they can serve as a basis to estimate how much investment into improved infrastructure robustness and faster disaster recovery is justified. The following subsections describe the details for each type of loss. The legend for the symbols used in the formulae can be found in Table 1.

4.1. Downtime

Total downtime related loss is the sum of productivity and revenue loss. This type of loss is incurred during the actual downtime interval $[t_0, t_1]$. We get

$$L_D = \frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o$$

4.2. Disaster Recovery

The loss due to disaster recovery is the sum of the cost for work and material to get the system up and running again. It arises during the downtime $[t_0, t_1]$. We get

$$L_r = E_r \cdot E_{ch} \cdot d_r + M_c$$

4.3. Liability

This loss class describes cost incurred because contracts with third parties cannot be fulfilled and these third parties demand financial compensation. The loss is incurred during $[t_1, \infty]$ and equals the sum of all demands:

$$L_C = \sum C_c + \sum C_l$$

If a claim is in dispute, substantial legal costs may arise in addition. Notice that this type of loss can often only be quantified when the affected third parties make their claims known. It is hard to estimate how much an affected third party was actually damaged by the outage without asking it. ISPs typically reimburse their customers for the time they were unable to provide service.

4.4. Customer Loss

If a service is unavailable for some time, customers might move to another service provider or no longer use the service. This type of loss is incurred over a very long time $[t_2, \infty]$ and also includes loss of potential new customers. We get

$$L_{CL} = [C_A(\Delta t) + C_P(\Delta t)] \cdot R_C(\Delta t)$$

If the revenue per customer varies significantly, the above expression is inaccurate and should be replaced by a detailed analysis focused on the most important customers.

5. Sample Scenarios

In the following we discuss some sample scenarios that illustrate the qualitative loss expectancy for different types of enterprises. For each scenario we plot the cumulative financial loss over time in Figure 2.

0	Factor	Symbol	Unit	BSP	WSP	Swiss National Scenarios	
Outage parameters							
	Outage time		h	24	168	24	168
	Working hours overlapping outage time	d_o	h	8	40	8	40
	Service operation time affected by outage	ds_o	h	24	168	24	168
	Degree of service degradation	S_o		100%	100%	100%	100%
Downtime Loss							
	Degraded Productivity						
1	Annual cost per employee	E_{ca}	CHF/yr	98,075	98,075	98,075	98,075
2	Working time per employee and year	d_a	h/yr	1,880	1,880	1,880	1,880
3	Employees affected by outage	E_{no}		3,500	4	1,038,228	1,730,380
4	Productivity degradation during outage	E_{po}		20%	20%	20%	50%
5	**SUM**		**CHF**	**292,128**	**1,669**	**86,658,903**	**1,805,393,814**
	Loss of Revenue						
6	Total annual revenue	R_a	CHF/yr	2,815,000,000	1,000,000	482,000,000,000	482,000,000,000
7	Service operating hours per year	ds_a	h	8,760	8,760	8,760	8,760
8	Part of the revenue affected by full outage	R_o		0%	0%	15%	40%
9	**SUM**		**CHF**	**0**	**0**	**198,082,192**	**3,697,534,247**
10	**SUM for Downtime**	L_D	**CHF**	**292,128**	**1,669**	**284,741,095**	**5,502,928,061**
Disaster Recovery							
10	Number of employees in the recovery team	E_r		1,750 (50%)	0	10,382 (1%)	17,304 (1%)
11	Cost per hour for a recovery team member	E_{ch}	CHF	150	150	150	150
12	Recovery work hours outside office hours	d_r	h	16	0	16	128
13	Cost of material needed	M_c	CHF	1,000,000	0	0	0
14	**SUM for Recovery**	L_r	**CHF**	**5,200,000**	**0**	**24,917,472**	**332,232,960**
Liability							
15	Claims from contractual penalties	C_c	CHF	15,000,000	0	0	0
16	Claims from other liabilities	C_l	CHF	0	0	0	0
17	**SUM for Liability**	L_C	**CHF**	**15,000,000**	**0**	**0**	**0**
Customer Loss							
18	Time interval	Δt	yrs	1	1	0	0
19	Number of actual customers lost	C_A		20	100	0	0
20	Number of potential customers lost	C_P		5	30	0	0
21	Average revenue per customer	R_C	CHF/yr	500,000	1,300	0	0
22	**SUM for Customer Loss**	L_{CL}	**CHF**	**12,500,000**	**169,000**	**0**	**0**
	Total Economic Loss		**CHF**	**32,992,138**	**170,669**	**309,658,567**	**5,835,161,021**

Comments:

0	BSP: Backbone Service Provider; WSP: Web Service Provider
1	Source: Swiss federal office for statistics [5, 6]
2	40 hours week and 5 weeks of vacations per year
4	Computer based work limited, no e-mail, no Internet
6	WSP: 6 employees, 800 customers, 2500 domains, CHF 1 mill. annual revenue
6	National Scenarios: Source: Swiss federal office for statistics [4], Credit Suisse [11]
9	WSP: Assumes a flat rate for the data volume
10	WSP: Recovery is not a responsibility of the WSP
17	National Scenarios: Claims only within Switzerland
22	National Scenarios: No customers are lost

Table 1. Example Scenarios

In order to demonstrate the flexibility and applicability of our model and methodology, Table 1 shows sample calculations of four concrete scenarios. Monetary unit is Swiss Francs (CHF). At the time of writing 1 CHF = 0.65 EUR = 0.77 USD.

5.1. Backbone and Internet Service Providers

During the downtime $[t_0, t_1]$ employee productivity is low, as Internet related services such as e-mail and web based communication are no longer available. Branch offices connected through virtual private networks (VPNs) are disconnected. In case that a BSP or ISP offers hosting or interconnection with pricing based on data transfer volume or if it earns revenue for commercials shown on, e.g., a portal web site, a financial loss will be suffered. Having customers paying a flat fee is advantageous in this event. Productivity and revenue loss sum up to the *downtime loss*, which grows linearly with the length of the downtime. *Disaster recovery* mainly consists of additional work hours of network operators and grows linearly as well.

BSPs are hit stronger by *liability* claims than ISPs as unsatisfied customers of a BSP can often refer to an SLA and claim compensation. Best-effort guarantees common in ISPs help to reduce such claims. However, a partial reimbursement of paid flat fees might be needed.

As unhappy customers cannot immediately cancel a contract, the damage resulting from *customer loss* might occur weeks or even months after the actual technical incident. A sudden surge of customers terminating their contracts is likely to happen at the end of the current service period.

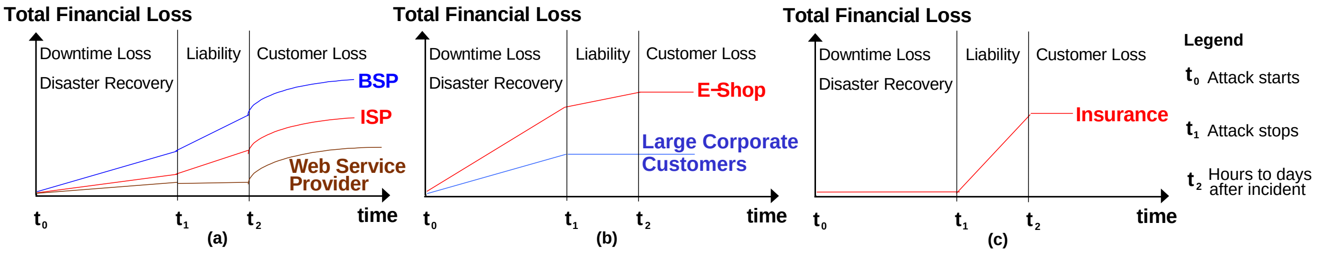

Figure 2. Cumulative financial loss of various Internet dependent enterprises

The backbone service provider (BSP) scenario in Table 1 assumes complete interruption of Internet dependent services for 24 hours. The figures are chosen such as to match a BSP of the size of Swisscom Fixnet Wholesale (SFW). Productivity degradation is estimated at 20% as most employees can do other pending work unrelated to the Internet. Total estimated loss is about CHF 33 mill., which corresponds to 1.2% of SFW's annual income.

5.2. Corporate Customers

For large corporate customers of a BSP/ISP the *productivity loss* is similar to the BSP/ISP scenario discussed in Subsection 5.1 An e-shop that sells only over the Internet also suffers severe *revenue loss* as e-shop customers that cannot connect to this online shop can easily shop in another one, which is currently available. Large companies and conglomerates typically sell over various channels and hence suffer a lot less *revenue loss* in case of Internet interruption. The resulting *downtime cost* grows linearly. *Disaster recovery* costs are rather small as the prevalent technical problems are typically solved by the ISP or BSP.

Liability claims are rare to occur for short business interruptions as is shown in the diagram. For long-term interruptions such claims can become a major issue. The same is true regarding *customer loss*.

5.3. Web Service Provider

Web service providers often charge customers for their data transfer volume like ISPs do. The total loss due to *downtime*, *disaster recovery*, and *liability* is analogous in its characteristics to the ISP scenario in Section 5.1.

The damage due to *customer loss* depends heavily on the type of SLAs with hosted customers. Infrequent and short interruptions will rarely be noticed by private customers, whereas e-shops can suffer a significant loss. A worst case would occur, if the web service provider's servers get broken into due to a lack of security, which would unsettle many customers.

The web service provider (WSP) scenario assumes a one week complete interruption of Internet dependent services. Our sample WSP with 6 employees hosting 2500 domains of 800 customers and having CHF 1 mill. in annual revenue suffers an estimated loss of CHF 0.17 mill. for the assumptions listed in Table 1.

5.4. Insurance Companies

Use of modern communication technology such as the Internet to enhance a company's productivity are inevitable. However, many companies just slowly become aware that their financial success heavily depends on an "always-on" Internet. Traditional insurance policies such as corporate liability policies [3] are not adequate to protect a company from business interruptions, productivity degradation and financial loss caused by Internet attacks.

The Swiss insurance company Zurich offers an "eRisk protection program" since mid-2000. This novel service includes consulting for risk analysis, legal advice, and optimisations to Internet related security. Business interruption, data, software, and public relations cost, and liability claims in case of service interruptions can be covered. The re-insurance company Swiss Re offers consulting and solutions for non-physical damage business interruptions, cyber liability, and revenue protection.

However, the details of such risk analyses and policy calculations are proprietary and confidential and hence difficult to compare. However, most BSPs and ISPs still refrain from obtaining insurance coverage for Internet related cyber risks.

The damage suffered by insurance companies in the event of a large-scale Internet attack is mainly the sum of *liability* claims from insurance policies. The diagram does not show the comparably small *productivity loss* incurred.

5.5. Telcos

As telephone networks, which generate the biggest part of the revenue for a telco, are usually separate from the Internet infrastructure, a telco suffers primarily from *productivity loss* of its employees that can no longer use the Internet during an attack. It is possible that a telco generates additional revenue during an attack due to people calling others by phone instead of sending e-mails.

5.6. TV Cable Companies

If a TV cable company only provides television broadcast services, the scenario is comparable to the one for a telco as just described. In case that broadband Internet is offered over the TV cable, the loss characteristics are similar to the ISP scenario discussed in Subsection 5.1.

5.7. Swiss National Scenarios

Table 1 gives two Swiss national scenarios. According to [11] 48.2% of all 3,590,000 employees [6] working in Switzerland do an IT intense job, which results in 1,730,380 affected employees during an one week (168 hours) Internet outage. For an outage of a single day in our Swiss national scenario, we assumed that only 60% respectively 1,038,228 (i.e. all large enterprises and a part of the SMEs) of all employees in IT intense jobs are affected. In addition, the Swiss national scenarios do not show liability claims and loss of customers since it is assumed that liability is within Switzerland and no customers are lost.

6. Conclusions and Outlook

The threat potential of a massive DDoS attack on critical Internet infrastructure elements can no longer be ignored. The possible direct and indirect financial loss for many Internet dependent companies must be considered in each complete business risk analysis. Our model and methodology provides a basis for transparent financial damage estimations in a qualitative and a quantitative way. The sample scenarios show that our model and methodology are applicable to real world situations and that the calculations involved are straight-forward.

As possible extensions to our model we propose to consider preventive measures and new kinds of threats that involve different loss characteristics over time. The underlying Internet system model could be enlarged to encompass the stock market, company reorganisations due to incidents and other indirectly affected systems.

For a comprehensive risk analysis, models that allow assessing the probability of specific incidents and their impact on business processes relevant for a company or organisation have to be developed.

References

[1] Computer industry almanac. http://www.c-i-a.com/pr1202.htm, December 2000.

[2] C. Alberts, S. Behrens, R. Pethia, and W. Wilson. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0. http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr017.pdf, 1999.

[3] U. Baumeister. Ein Versicherungsfall mit neuer Dimension: Deckung von Internet-Risiken als heikle Angelegenheit. http://www.nzz.ch/netzstoff/2002/2002.09.24-wi-article8DKDJ.html, April 2003.

[4] Ein steuerbarer Umsatz von über 500 Mio. Franken. http://www.statistik.admin.ch/news/archiv97/dp97080.htm, 1997. Schweizer Bundesamt für Statistik.

[5] Statistik Schweiz: Eckdaten. http://www.statistik.admin.ch/stat_ch/ber00/dkan_ch.html, 2003. Schweizer Bundesamt für Statistik, Press Release.

[6] Swiss Statistics: Keydata: Economic and Financial Data for Switzerland. http://www.statistik.admin.ch/stat_ch/ber00/imf.htm, 2003. Schweizer Bundesamt für Statistik.

[7] S. Burschka, H. Straumann, and M. Semling. Interview mit Swisscom Innovations, Security and Service Management, Bern. 17.4.2003.

[8] CERT. Advisory CA-2003-04 MS-SQL Server Worm. http://www.cert.org/advisories/CA-2003-04.html, 2003.

[9] CERT. Advisory CA-2003-20 W32/Blaster worm. http://www.cert.org/advisories/CA-2003-20.html, 2003.

[10] CERT. Incident Note IN-2003-03 W32/Sobig.F. http://www.cert.org/incident_notes/IN-2003-03.html, 2003.

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

[12] DDoSVax - In Search of a Vaccine against DDoS Attacks. http://www.tik.ee.ethz.ch/˜ddosvax/.

[13] D. Denning. Cyber Attacks. http://www.cs.georgetown.edu/˜denning/cosc511/fall01/cyber-attack.ppt, 2001.

[14] R. Ehrensperger. Interview mit Swisscom Fixnet, Network Operations, Plattform Management, Zürich. 22.4.2003.

[15] L. Haldemann. Versicherung von Internet-Risiken. http://www.ifi.unizh.ch/ikm/Vorlesungen/inf_recht/2001/Haldemann.pdf, 2001.

[16] Backbone DDoS [on DNS] (2.10.2002). http://www.internettrafficreport.com/event/2.htm. Internet Traffic Report.

[17] NIST. Federal Information Technology Security Assessment Framework. http://csrc.nist.gov/organizations/guidance/framework-final.pdf, 2000.

[18] D. A. Patterson. A simple way to estimate the cost of downtime. http://roc/cs.berkeley.edu/papers/Cost_Downtime_LISA.pdf, 2002.

[19] http://www.switch.ch.

[20] P. Weigel, J. Schmid, B. Plattner, and T. Dübendorfer. Knowledge Flow Vortrag: Wirtschaftlicher Schaden von Internet-Würmern. 31.10.2003.

[21] P. Widmer. Interview mit Bluewin, Business-Line Access, Zürich. 19.5.2003.

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