Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

VIRUS – Sicher im Netz?

2. Internationale Konferenz zur Virtuellen Bibliothek des Goethe-Instituts Brüssel

Rafael Ball, Cornelia Röpke, Willy Vanderpijpen (Hrsg.)

Bibliothek
Library

Schriften des Forschungszentrums Jülich
Reihe Bibliothek / Library Band / Volume 13

Forschungszentrum Jülich GmbH
Zentralbibliothek

VIRUS – Sicher im Netz?

2. Internationale Konferenz zur Virtuellen Bibliothek des Goethe-Instituts Brüssel

Rafael Ball, Cornelia Röpke, Willy Vanderpijpen (Hrsg.)

Organisatoren:

Goethe-Institut Brüssel, Belgien
Zentralbibliothek des Forschungszentrums Jülich, Deutschland
Bibliothèque Royale de Belgique / Koninklijke Bibliotheek van Belgie, Brüssel

In Zusammenarbeit mit:
Ambassade de France en Belgique, Botschaft der Bundesrepublik Deutschland, CICEB (eské Centrum, Det Danske Kulturinstitut, Instituto Cervantes, Istituto Italiano di Cultura, The Finnish Cultural Institute for Benelux, The Louvain Institute for Ireland in Belgium, Österreichisches Kulturforum), Information Society Technologies, ZKM (Zentrum für Kunst und Medientechnologie Karlsruhe)

Schriften des Forschungszentrums Jülich
Reihe Bibliothek / Library Band / Volume 13

ISSN 1433-5557 ISBN 3-89336-377-7

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Herausgeber und Vertrieb:	Forschungszentrum Jülich GmbH Zentralbibliothek D-52425 Jülich Telefon (02461) 61-5368 · Telefax (02461) 61-6103 e-mail: zb-publikation@fz-juelich.de Internet: http://www.fz-juelich.de/zb
Umschlaggestaltung:	Grafische Medien, Forschungszentrum Jülich GmbH
Druck:	Grafische Medien, Forschungszentrum Jülich GmbH
Copyright:	Forschungszentrum Jülich 2005

Schriften des Forschungszentrums Jülich
Reihe Bibliothek / Library Band / Volume 13

ISSN 1433-5557
ISBN 3-89336-377-7

Inhaltsverzeichnis

In Zeiten einer vernetzten Welt ist das Thema der „Netzsicherheit“ zwar zu einem banalen Allgemeinplatz der IT-Branche verkommen, bleibt aber dennoch eine der bedeutendsten Fragen in einer Umgebung, die sich zunehmend in nahezu allen Lebensbereichen von der Sicherheit und Zuverlässigkeit jener Netzwerke der Kommunikation abhängig gemacht hat. Dies trifft im besonderen Maße zu auf die Informations- und Bibliotheksbranche, deren Kommunikations- und Transportmedium schlicht das Netz geworden ist. Dieses Thema bewusst breit anzugehen, von technischen Details abzusehen und die ganze Dimension von Sicherheit zu be- und umgreifen, hatten sich die Veranstalter der Konferenz „VIRUS –Sicher im Netz“ am 2. und 3. Februar in Brüssel, die Bibliothek des Goethe-Instituts Brüssel, die Zentralbibliothek der Forschungszentrums Jülich GmbH und der Königlichen Bibliothek in Brüssel vorgenommen. Die Breite der Themen spiegelt sich im Programm wieder: Technische Aspekte neben juristischen Fragen des Copyright, ethische Diskussionen neben Berichten über Filtersoftware, Fragen zur Datenintegrität neben Industriesabotage, die Moral der Hacker neben Kunstinstallationen zur Netzwerksicherheit.

Trotz der Vielzahl der Themen, die in zwei Konferenztragen nicht ausdiskutiert, sondern durch Vorträge nur angerissen werden konnten, gelang durch die Auswahl der internationalen Referenten ein umfassender Überblick über die Aspekte der Netzwerksicherheit. Diesen Querschnitt des Denkens soll auch der vorliegende Konferenzband widerspiegeln. Er versammelt in Aufsätzen, in den Vortragspräsentationen, durch Bilder und durch Lebensläufe der Referenten und Beteiligten die Gesamtsicht auf das Thema „Sicherheit im Netz“ und versucht durch unkonventionelle grafische Gestaltung den ganzheitlichen Ansatz wiederzugeben, soweit die Medien Buch und CD dies ermöglichen.

Die Herausgeber

Eröffnungsvortrag

Eröffnungsvortrag

Prof. Dr. Ernst Pöppel, Vorstand des Instituts für Medizinische Psychologie, Vorstand des Humanwissenschaftlichen Zentrums der Ludwig Maximilian Universität München

Die Erforschung der Informationsaufnahme und -verarbeitung sowie der neuronalen Mechanismen sind elementare Voraussetzungen für die Entwicklung optimaler, an die Arbeitsweise des menschlichen Gehirns angepasster Informationstechnologien und geeigneter Mensch-Maschine-Schnittstellen.

Seit der griechische Philosoph Parmenides vor etwa zweieinhalbtausend Jahren als erster Philosoph radikal die Frage nach dem Wesen des Seins stellte, und somit Metaphysik und das formale Denken begründete, beschäftigen sich Philosophen, Psychologen, Dichter und Literaturwissenschaftler mit Fragen wie „Was ist Geist?", „Wie denken wir?", „Was ist Bewusstsein?", „Was ist unser Gedächtnis?". Diese Fragen versuchen nun die Neurowissenschaften mit moderner Hirnforschung zu beantworten.

Die enorme Bedeutung der Hirnforschung wird in erster Linie im Hinblick auf den medizinischen Aspekt und die damit verbundenen volkswirtschaftlichen Konsequenzen deutlich. So werden etwa ein Drittel der im Gesundheitssystem anfallenden Kosten durch Störungen des Nervensystems verursacht. Für die Behandlung von Krankheiten wie Alzheimer, Parkinson, Schlaganfälle, Epilepsien, Multiple Sklerose, Schizophrenien, Depressionen und Schmerz werden alleine in Deutschland jährlich etwa 80 Milliarden Euro an Aufwendungen fällig. Insbesondere vor den Problemen, die der demographische Wandel mit sich bringt, versuchen Neurowissenschaftler auch bei der Erforschung altersbedingter neurologischer Erkrankungen einen Beitrag zu leisten. Dies macht im Umkehrschluss aber gleichzeitig deutlich, dass dieser medizinische Bereich wahrscheinlich der größte Markt der Zukunft sein wird.

Ein weiteres Argument für die Relevanz der Hirnforschung betrifft den Bereich der Technologie. Hier stellt sich die Frage, wie das Gehirn Informationen verarbeitet, also Prozesse wie Sehen, Hören, Denken oder Bewerten auf neuronaler Ebene ablaufen. Ziel dieser Forschung ist dann eine intelligentere und effizientere Gestaltung von Mensch-Maschine-Schnittstellen. Der dringende Bedarf in diesem Bereich wird am Beispiel des Internet deutlich. Durch ungünstige Navigationssysteme ist das Internet noch immer eine der größten „Zeitvernichtungsmaschinen" beim Umgang mit Informationen. Hieraus ergibt sich die Herausforderung, vorhandenes Wissen möglichst anstrengungslos verfügbar zu machen. Aus biologischer Sicht ist der Mensch dazu veranlagt, möglichst anstrengungslos Informationen aufzunehmen und zu bewerten. Dabei wird deutlich, dass es enge Verknüpfungen zwischen der Hirnforschung und Informationswissenschaft gibt. Dieser enge Zusammenhang spiegelt sich auch bei vielen Entwicklungen im Softwarebereich wieder, wo Hirnforscher mittlerweile unverzichtbar geworden sind.

Auch bei der naturwissenschaftlichen Betrachtung des Themenbereichs Erziehung und Bildung liefern die Neurowissenschaften einen großen Beitrag. Hier kann die Hirnforschung dazu beitragen, neue Lehr- und Lernziele zu entwickeln. Entscheidend ist dabei die

Erkenntnis, dass der Mensch bei der Geburt mit einem Überangebot möglicher Verbindungen von Nervenzellen ausgestattet ist. Das Gehirn wird dann in den ersten zehn Lebensjahren durch Informationsverarbeitung geformt, das heißt, dass die zahlreichen Verbände von Nervenzellen und ihre genetisch angebotenen Verknüpfungen müssen tatsächlich genutzt werden. In dieser Phase werden die angeborenen, genetisch vorgegebenen Programme bestätigt, um dann die Matrix des Gehirns endgültig festzulegen. Das bedeutet, dass jeder Mensch mit Potenzialitäten, und nicht mit fest vorgegebenen Programmen zur Welt kommt.

Auf diese Weise wird auch eine genetisch vorgegebene Sprachkompetenz, z.B. die phonetische Kompetenz ausgebildet. Das bedeutet, dass das akzentfreie Sprechen einer Sprache lediglich bis zum etwa zehnten Lebensjahr erlernt werden kann. Demzufolge gibt es keinen Menschen, der eine Sprache akzentfrei sprechen kann, wenn er bis zur Pubertät nur eine Sprache gelernt hat. Vor dem Hintergrund eines zukünftigen Europas, in dem die Menschen anstrengungslos miteinander kommunizieren können angesichts der zunehmenden Globalisierung ist es also sinnvoll zu fordern, dass alle Kinder bis zur Pubertät in Europa mindestens drei Sprachen lernen. Diese Forderung wäre für das Gehirn eine völlig unproblematische Aufgabe. Um eine breite Basis phonetischer – und somit auch kultureller – Kompetenz zu schaffen, müssten sie neben ihrer Muttersprache noch Englisch und eine dritte, slawische oder romanische Sprache lernen. Um dies zu erreichen wäre es notwendig, schon im Kindergarten mit intensivem Sprachunterricht zu beginnen.

Das letzte in diesem Kontext wichtige Argument für Hirnforschung ist, dass sie einen wichtigen Beitrag bei der Untersuchung von Kommunikation leisten kann. Alleine im Bereich der wissenschaftlichen Kommunikation unter den ungefähr 40.000 Neurowissenschaftlern entstehen jährlich etwa 100.000 neue Publikationen. Dabei handelt es sich zunächst um eine Menge an Informationen, also potenzielles Wissen. Da sich in immer stärkerem Maße Wissensinseln bilden, also Personengruppen, innerhalb derer ein bestimmtes Wissen konsolidiert wird, kommt es trotz einer Explosion an Informationen insgesamt zu einem Rückgang des Wissens. Dieser Zustand macht die Entwicklung neuer Konzepte notwendig, um die weltweit vorhandenen Informationen qualitätskontrolliert verfügbar und damit zu Wissen zu machen.

Derzeit wird bei uns ein Konzept auf Basis der Hypothese entwickelt, dass wissenschaftliche Information in bestimmten Kontexten so charakterisiert werden kann, dass es durch Dreiwortsätze, also Subjekt-Objekt-Prädikat-Aussagen repräsentiert wird. Das Ziel ist es, die Information in wissenschaftlichen Texten auf dieser Grundlage mit Hilfe von Algorithmen semantisch zu extrahieren, also Dreiwortsätze zu konstruieren. Auf diese Weise wäre es möglich, dem Rechercheur Wissen über die Information durch die üblichen Schlagworte hinaus anzubieten. Somit könnte Wissen tatsächlich auf breiter Ebene verfügbar gemacht werden. Ziel solcher Algorithmen ist es, eine Komplexitätsreduktion zu erreichen, was der Physiologie des menschlichen Gehirns Rechnung trägt.

Komplexitätsreduktion ist ein grundlegendes Prinzip der Verarbeitungsprozesse im Gehirn. Wenn Menschen über einen Sachverhalt nachdenken, etwas sehen oder hören, dann geschieht dies nicht als passiver Prozess, an dem verschiedene informationsverarbeitende Systeme beteiligt sind. Am Beispiel des Internet bedeutet dies, dass die verfügbaren Informationen nicht einfach passiv aufgenommen werden. Vielmehr hat die Person immer eine bestimmte Einstellung, ein Hypothese, eine Erwartung, einen Rahmen, innerhalb dessen bestimmte Informationen aufgenommen werden. Das heißt, es erfolgt zunächst eine Selektion und Interpretation dessen, was überhaupt aufgenommen werden kann (Top-Down-Hypothese). Dies geschieht in einem für das Gehirn ökonomischen Prozess, einer Art kreativer

„Müllentsorgung". Sämtliche Informationen, die für den gegenwärtigen Seh- und Denkprozess nicht relevant, sind werden weggefiltert. Dieses neuronale System kennt keine Viren oder andere Störungen, da die Hypothese eine Wahrnehmung von randständigen oder irrelevanten Informationen gar nicht zulässt. Das Gehirn gehorcht somit dem Prinzip der maximalen Komplexitätsreduktion.

Neben diesem positiven gibt es allerdings auch einen negativen Aspekt, der sich aus dieser Arbeitsweise des Gehirns ergibt und der unter dem Begriff „Vorurteil" zusammengefasst werden kann. Das Gehirn strebt Informationen möglichst schnell zu verarbeiten und einfache Kategorien zu erstellen. „Vorurteile" dienen der möglichst einfachen Gestaltung unserer Umwelt, auch im sozialen Bereich, unter Berücksichtigung des Parameters Zeit. „Vorurteile" gehören somit zur notwendigen Grundausstattung des Menschen, um Komplexitätsreduktion zu gewährleisten. Dieser Mechanismus der Komplexitätsreduktion birgt jedoch die Gefahr einer nicht angemessenen Beurteilung von Sachverhalten.

Letztendlich ist jede sinnliche Wahrnehmung und jeder Denkprozess die Verifikation oder Falsifikation einer Hypothese, die das Gehirn in einem gegebenen Augenblick über einen bestimmten Sachverhalt erstellt. Daraus resultierend gibt es also nicht Wahrnehmung oder Reflektion als Widerspiegelung eines Sachverhalts, sondern Bestätigung oder Verwerfung dessen, was im Gehirn antizipiert wird.

Die Informationsverarbeitung im Gehirn erfolgt dezentral. So ist bekannt, dass bei verschiedenen Prozessen, wie Lesen, Zuhören oder Nachdenken, unterschiedliche Areale des Gehirns aktiv sind. Prinzipiell gibt es im Gehirn lediglich drei verschiedene Arten von Nervenzellen. Das sind zum einen Zellen, die Informationen aufnehmen und von denen es im menschlichen Gehirn ca. 500 Millionen gibt. Für die Informationsabgabe ist ein anderer Zelltyp zuständig, der für die Koordination von Bewegung verantwortlich ist, die Sprache, die Mimik und die Erregung der inneren Organe. Dabei handelt es sich um ca. 2 Millionen Zellen. Der dritte, mit bis zu einer Billion häufigste Zelltyp bildet das so genannte intermediäre Netz. In diesem findet die zentrale Informationsverarbeitung statt. Die Architektur des Gehirns unterscheidet sich prinzipiell von künstlichen Informationsverarbeitungssystemen wie Computern. Jede Nervenzelle sendet nach dem Prinzip der Konvergenz Informationen zu etwa 10.000 anderen Nervenzellen und empfängt ebenso, nach dem Prinzip der Divergenz, von 10.000 anderen Zellen Informationen. Diese Informationen werden in Form verschiedener chemischer Botenstoffe, Neurotransmitter, übertragen. Wenn eine Nervenzelle aktiv ist, dann kann sie die nächste in ihrer Aktivität erregen (Prinzip der Exzitation) oder hemmen (Prinzip der Inhibition). Das heißt, es gibt insgesamt drei Erregungszustände, neutrales, erregtes oder reduziertes Niveau, sämtlich bedingt durch chemische Botenstoffe. Die bekannten neurologischen Erkrankungen wie Epilepsie, Schizophrenie, Parkinson oder Depression, werden allesamt durch Störungen auf der chemischen Ebene bestimmter Bereiche des Gehirns, also zu wenig Erregung oder Hemmung, verursacht.

Nun stellt sich die Frage, wie viele Arbeitsschritte nötig sind, um Informationen innerhalb des Gehirns zu transferieren. In Anbetracht der riesigen Zahl an Nervenzellen vermutet man auch eine große Zahl an Zwischenschritten, in Abhängigkeit von der Entfernung der Zellen. Bei der mathematischen Betrachtung unter Berücksichtigung der Divergenz ergibt sich jedoch, dass der maximale Abstand beliebiger Elemente, die Informationen verarbeiten, lediglich vier Zwischenschritte beträgt. Diese strukturell bedingte funktionelle Nähe bedeutet in der Sprache der Datenverarbeitung, dass das Gehirn durch „massivste Parallelität" ausgezeichnet ist: Alles ist mit allem offenbar engstens verbunden. Vergleicht man das mit technischen

Ansätzen, z.B. mit der Menüführung im Internet, so wird eine völlig andere Architektur der Informationsverarbeitung offensichtlich. Die Tatsache der engsten Vernetzung im neuronalen Netzwerk hat Konsequenzen für unser Selbstverständnis und unsere Funktionsweise. Allein aus der Architektur des Gehirns leitet sich die Feststellung ab, dass ein Wahrnehmen ohne ein gleichzeitiges Erinnern und gefühlsmäßiges Bewerten, oder ein Erinnern ohne ein gefühlsmäßiges Bewerten und Wahrnehmen, oder ein Gefühl ohne einen Erinnerungsbezug und eine wahrnehmungsmäßige Repräsentation, nicht möglich ist. Nicht zuletzt aufgrund dessen ist eine Simulation menschlichen Denkens, Fühlens und Handelns in weiter Ferne.

Ein elementarer Befund der Hirnforschung ist die Erkenntnis, dass Elemente der Information im Gehirn modular repräsentiert sind. Insgesamt verfügt das Gehirn auf psychischer Ebene über vier Funktionsbereiche, nämlich der Wahrnehmungen (der Reizaufnahme), des Lernens und Gedächtnisses (der Reizbearbeitung), der Gefühle (der Reizbewertung) sowie der Handlungen, Aktionen oder Reaktionen, die spontan oder auf Reize hin auftreten. Damit Inhalte subjektiv verfügbar sein können, wir also bewusst erleben können, bedarf es weiterer Funktionen, die man als logistische Funktionen bezeichnen könnte.

Verschiedene Hirnareale sind also für unterschiedliche Prozesse verantwortlich. Am Beispiel des Lesens wird deutlich, dass verschiedene Areale auch parallel aktiv sein können. So wird beim Sehen die Information über das Auge aufgenommen und dann in mehreren gleichzeitig aktiven, Bereichen dekodiert, um Bedeutungszusammenhänge herstellen zu können. Ebenso verhält es sich beim Sprechen, auch hier sind mindestens 7 verschiedene Kompetenzen notwendig, die parallel aktiv sein müssen, damit wir miteinander reden können. Weiterhin ist ein gewisser Wortvorrat essentiell, der in Form von zwei „Lexika" im Gehirn vorliegt. Eines beinhaltet inhaltstragende Wörter, wie Verben und Nomina, das andere speichert Funktionswörter. Um diese richtig einzusetzen ist eine syntaktische Kompetenz notwendig, die Grammatik, also die Fähigkeit, Wörter nach bestimmten Mustern und Regeln zu funktionellen Einheiten zusammen zu setzen. Darüber hinaus besitzt der Mensch auch semantische Kompetenz, also die Fähigkeit, der Sprache Bedeutung zu geben. Bei Störungen in diesem Bereich wird die Sprache inhaltsleer. Der Mensch besitzt auch phonetische Kompetenz, die besonders beim Erlernen der Sprache wichtig ist. Interessant ist in diesem Zusammenhang, dass allen ca. 5000 Sprachen der Welt nur etwa 100 verschiedene Sprachlaute vorgegeben sind. Neben der phonetischen Kompetenz ist auch die prosodische Kompetenz, also die Akzentuierung oder Sprachmelodie wichtig, die beim Lesen von Texten übrigens nicht mehr vorhanden ist. Diese Fähigkeit kann durch Störungen der rechten Gehirnhälfte verloren gehen. Eine weitere Kompetenz ist die pragmatische oder kognitive Kompetenz. Diese ist notwendig, um die Sprache der gegebenen Situation anzupassen und z.B. bei Patienten die an Schizophrenie leiden stark gestört ist. Ob und wie man miteinander redet wird durch die soziale Kompetenz gesteuert. Sie hilft, die geeignete Distanz zu einem Gesprächspartner einzuschätzen und ist bei einer Sprechsprache von großer Bedeutung.

Da das Gehirn parallel auf die verschiedenen Kompetenzen zugreifen muss, um zu denken, zu sprechen oder zu planen, entsteht ein logistisches Problem und macht eine zeitliche Organisation, eine Synchronisation notwendig. Um dies zu erreichen hat das Gehirn mehrere Mechanismen entwickelt. Mit einem davon schafft sich das Gehirn Systemzustände, innerhalb derer die Komplexität reduziert wird. Diese Systemzustände schafft sich das Gehirn mittels neuronaler Konstellationen von 30 bis 40 Millisekunden, die vermutlich durch oszillatorische Prozesse in Neuronenpopulationen ermöglicht werden, innerhalb derer Elementarereignisse kontemporal, also gleichzeitig behandelt werden. Das bedeutet, es wird nicht bewertet was verarbeitet wird, sondern es wird ein Schema generiert, durch welches alles, was zu einem solchen Zeitfenster gehört als ein Systemzustand definiert wird. Die Zeit im Gehirn läuft

somit nicht kontinuierlich ab, sondern es folgen Zeitquanten im Bereich von etwa 30 Millisekunden aufeinander. Fehlen diese oszillatorischen Prozesse, zum Beispiel in der Narkose, sind damit auch nicht mehr die Voraussetzungen für eine Ereignisdefinition vorhanden, und es kommt dadurch zu einem absoluten Verlust subjektiver Zeiterfahrung. Das Gehirn schafft sich so „zeittote" Zonen außerhalb der mathematischen Zeit. Wie kann nun aber auf der Grundlage isoliert definierter Ereignisse in unserem Erleben so etwas wie erlebte Kontinuität entstehen? Es stellt sich also die Frage nach der zeitlichen Integration aufeinanderfolgender Ereignisse. Diese beruht auf einem weiteren neuralen Mechanismus. Im Prinzip gibt es zwei Möglichkeiten, wie eine Integration nacheinander definierter Ereignisse ablaufen könnte. Eine Möglichkeit wäre – und die wird von manchen Vertretern der Informatik verfochten, dass die Integration von Ereignissen semantisch abläuft. Semantische Integration setzt ein intern repräsentiertes Schema voraus, mit dem die jeweils aufgenommene Information verglichen wird. Bestätigt die Information das interne Schema, ist damit der Prozess der zeitlichen Integration abgeschlossen. Neben einer semantischen Integration ohne Zeitbegrenzungen ist jedoch auch eine präsemantische Integration denkbar, die unabhängig von einem internen Schema und vorgegebenen Reizen, die am Schema überprüft werden, abläuft. Eine solche automatische Integration im Gehirn wird durch zahlreiche Beobachtungen tatsächlich nahe gelegt. Allerdings verkettet das Gehirn nicht Perioden aus 30 bis 40 Millisekunden, sondern tatsächlich von ca. 3 Sekunden. Experimente haben gezeigt, dass es sich dabei um ein universelles Prinzip handelt, welches bei entsprechenden Verhaltensweisen in verschiedensten Kulturen festgestellt wurde. Dies zeigt sich auch in der Sprache. So bildet der Mensch Phrasen oder Aussageeinheiten von ca. 8-14 Silben, die immer 2-3 Sekunden dauern. Diese Segmentierung gilt für alle Sprachen der Welt. Das universelle neuronale Zeitfenster von 2-3 Sekunden wird auch bei intentionalen Bewegungen, dem Kurzzeitgedächtnis oder der Verweilzeit von Blicken beobachtet. Die Kontinuität menschlichen Erlebens ist also nicht eine passive Widerspiegelung der klassischen Zeit nach Newton'scher Definition, sondern das, was innerhalb eines 2-3 Sekunden Zeitfensters repräsentiert ist, wird inhaltlich miteinander verbunden. So entsteht Kontinuität und Bewusstsein.

Die hier vorgestellten Befunde, welche die Neurowissenschaften bei der Analyse der im Gehirn ablaufenden Prozesse bereits gewonnen haben und zukünftig gewinnen werden, können entscheidend zur effizienten Entwicklung und Implementierung technischer Systeme im Informations- und Kommunikationsbereich beitragen.

Curriculum Vitae

Ernst Pöppel

Dienstadressen Institut für Medizinische Psychologie,
Medizinische Fakultät der Ludwig-
Maximilians-Universität München
Goethestr. 31
D-80336 München
Tel. ++49-89-5996650
Fax ++49-89-5996615
und Humanwissenschaftliches Zentrum ,
der Ludwig-Maximilians- Universität München
Goethestr. 31
D-80336 München
Tel. ++49-89-5996651
Fax ++49-89-5996489

Geburtsdatum 29. April 1940
Geburtsort Schwessin, Pommern

Akademische Ausbildung

1976	Habilitation für Psychologie (Dr. phil. habil.) Naturwissenschaftliche Fakultät, Leopold-Franzens-Universität Innsbruck/Österreich
1974	Habilitation für Sinnesphysiologie (Dr. med. habil.) Medizinische Fakultät, Ludwig-Maximilians-Universität München
1968	Promotion zum Dr. phil. in Psychologie Leopold-Franzens-Universität Innsbruck
1962-1968	Studium der Psychologie und Zoophysiologie Universitäten Freiburg/Breisgau, München und Innsbruck
1959	Abitur, Kepler-Gymnasium Freiburg/Breisgau

Wissenschaftliche Positionen

2001	Wissenschaftlicher Ko-Direktor des Parmenides-Center für Neuroscience and Knowledge Research", München
2000	Wissenschaftlicher Leiter des „Generation Research Programs", Bad Tölz
1997	Geschäftsführender Vorstand des Humanwissenschaftlichen Zentrums der Ludwig-Maximilians-Universität München
1992-1997	Mitglied des Vorstands Forschungszentrums Jülich Zuständigkeit: Medizin, Biotechnologie, Umwelt
1976	Ordinarius für Medizinische Psychologie, Medizinische Fakultät, Ludwig-Maximilians-Universität München
1973-1976	Wissenschaftlicher Assistent Max-Planck-Institut für Psychiatrie, München
1972-1973	Staff Scientist Neuroscience Research Program, Boston, USA

1971-1973	Research Associate Massachusetts Institute of Technology, Cambridge, USA Department of Psychology and Brain Science
1969-1970	Stipendium der Volkswagen-Stiftung Max-Planck-Institut für Psychiatrie, München Abteilung Neurophysiologie
1966-1968	Stipendium der Max-Planck-Gesellschaft Max-Planck-Institut für Verhaltensphysiologie, Andechs Abteilung Aschoff (Chronobiologie)
1965-1966	NASA-Stipendium Max-Planck-Institut für Verhaltensphysiologie, Andechs

Akademische Auszeichnungen

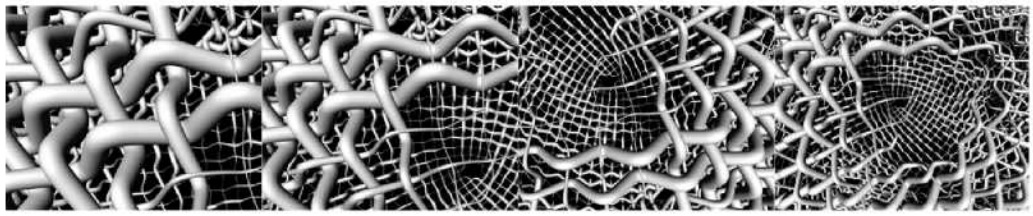
1997	Mitglied der Europäischen Akademie der Wissenschaften und Künste
1995	Exponat Deutsches Museum Bonn
1993	Mitglied der Deutschen Akademie der Naturforscher Leopoldina
1988	J.E. Purkinje Medaille der Tschechischen Medizinischen Gesellschaften
1984	Levinson Award of the American Poetry Association
1983	Preis des Kollegiums Deutscher Medizinjournalisten
1959	Scheffel-Preis

Forschungsgebiete

Neuropsychologie der visuellen Wahrnehmung („blindsight", „visual completion")
Zeitliche Organisation von Hirnprozessen und mentalen Vorgängen
Restitution von Funktionen nach Hirnverletzungen Physiologische Messung von Narkosetiefe Schmerzwahrnehmung
Tagesperiodik psychologischer und physiologischer Funktionen
Technische Entwicklung von medizinischen Meßgeräten

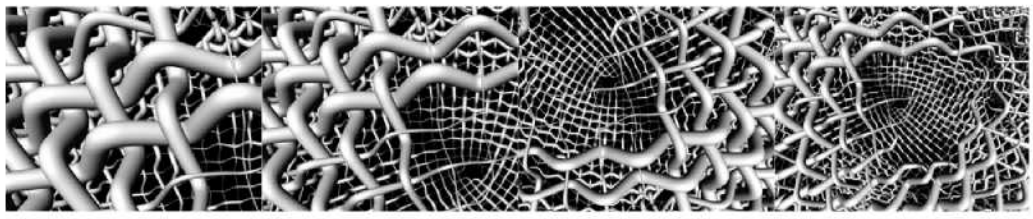
Publikationen

ca. 250 Veröffentlichungen (davon 20 Bücher als Autor/ Herausgeber)
ca. 500 Vorträge in verschiedenen Ländern



Sektion I

Informationswissenschaften und Anwendungen: Theorie und Praxis



Sicherheit und Verunsicherung im Zeitalter elektronischer Wissenschaftskommunikation

Dr. Rafael Ball, Leiter der Zentralbibliothek, Forschungszentrum Jülich

Abstract

The transition from analogue, printed to digital, electronic media for the communication of scientific information gives rise to even more intense conflicts and fields of tension between the actors in the value-added chain of scientific information than has previously been the case. Starting from the definition of the concept of security, the lecture examines security aspects of the document, the author, records systems, the user and the library. It thus becomes clear that major emphasis is not primarily placed on issues of technical security in scientific communication, but rather that our basic understanding of availability, certainty, foreseeability, predictability and durability is called into question.

1. Einleitung

Beim Übergang vom analogen, gedruckten zum digitalen, elektronischen Medium für die Verbreitung von wissenschaftlicher Information, sind die Konflikte und Spannungsfelder der Akteure in der Wertschöpfungskette der wissenschaftlichen Information noch stärker als bisher hervorgetreten. Neue Möglichkeiten der Kommunikation sind entstanden, die Möglichkeiten der technischen Vervielfältigung und weltweiten Verbreitung haben nicht nur die Geschäftsmodelle der Zeitschriftenverlage und ihre auf die Printumgebung bezogenen Exklusivrechte zunehmend in Frage gestellt, sondern auch die Sicherheitsfrage wichtig werden lassen. Vor dem Hintergrund einer stark gestiegenen Literaturproduktion (täglich produzieren 7 Millionen Wissenschaftler weltweit 30.000 Artikel, die Zahl der in den ISI-Datenbanken gelisteten Artikel hat sich im Laufe der vergangenen 20 Jahre verdoppelt[1]) und einer zunehmend elektronisch distributierten Wissenschaftsinformation ist das Massenstreaming in elektronischen Netzen zur alltäglichen (und allnächtlichen) Selbstverständlichkeit geworden. Sicherheit im Netz ist daher längst kein akademisches Thema mehr, sondern handfeste Forderung der Netznutzer. Doch kann, wer Sicherheit fordert, auch Sicherheit erwarten? Wer kann heute im Netz noch etwas „ver-sichern"? Bei der Masse der umgesetzten Daten, bei der Struktur des Netzes, bei dem Turnover der Inhalte wird „Versicherung" schwierig. So ist in der undurchdringlichen Endlosigkeit des Netzes nichts und niemand mehr seiner und seiner Dinge sicher. Und wer seiner nicht mehr sicher ist, kann schon gar nichts mehr ver-sichern. Das Medium selbst ist zur allgemeinen Verunsicherung geworden. Doch leben wir generell in einer Zeit, in der Sicherheit nicht mehr garantiert werden kann auch wenn wir noch so oft versichert werden und uns dies noch so oft versichert wird. Das gilt besonders für das Internet, wenn es als interaktives freies Medium verstanden werden will und nicht als bloßer Kanal der Massenkommunikation[2]. Hier entsteht ein Spannungsfeld zwischen dem Anspruch des freien unzensierten, kommunikativen demokratischen Mediums und der Nutzung dieses Mediums als bloßem Massenkommunikationsmittel. Wenn aber teure (wertvolle, bezahlte und unbezahlbare)

[1] www.isinet.com

[2] Münker, Stefan; Roesler, Alexander, Praxis Internet, Kulturtechniken der vernetzten Welt, Suhrkamp, 2002

Inhalte über das Netz verbreitet werden sollen (wie es in der wissenschaftlichen Kommunikation unzweifelhaft geschieht), muss die Sicherheit einen anderen Stellenwert erhalten als beim freien offenen Austausch über Netze.

2. Geschichte eines Begriffs

Ein kleiner historisch-etymologisch-semantischer Rückblick auf die Terminologie von Sicherheit hilft zu verstehen, was Sicherheit meint und was es im Netz nicht sein kann. Bei Cicero und Lukrez ist der Begriff belegt und meint einen Seelenzustand der Freiheit von Sorge und Schmerz. Dabei rekurriert „Sicherheit" auf das Lateinische *securus* bzw. *securitas*, als das es sorglos, unbesorgt, unbekümmert, sorgenfrei, heiter, sicher und gefahrlos verstanden werden kann[3]. Obwohl es nach der Phonetik doch schnell in die Nähe von *securis* dem Beil, der Axt, dem Schlag und der Wunde rückt, einer Bestimmung, die man als Netznutzer nur zu oft zu spüren bekommen, wenn „Sicherheit im Netz" einmal nicht funktioniert.
Aber auch als *salus* in der Bedeutung von Unverletztheit und Wohlbefinden bezieht sich der Terminus in seinen Anfängen auf die Bestimmtheit des Individuums.
Sicherheit zunächst also immer auf die Verfassung des Individuums bezogen, bekam erst später im Sinne einer *pax romana* im Römischen Reich einen politischen Impetus. Fast zeitgleich wurde dann auch die *Cautio*, nicht die *Securitas* zur „Sicherheit" im Sinne einer Bürgschaft, einer Sicherung, aber auch einer Vorsicht und Behutsamkeit zu einem Terminus Technicus in wirtschaftlicher und finanztechnischer Bedeutung. So wie der Sicherheitsbegriff sich vom rein individuellen Anliegen über einen Begriff im Rechtssinne hin zu einer territorial und sozial verstandenen Sicherheit entwickelte, steht der Netznutzer mit seinem Bedürfnis nach Netzsicherheit in direkter Folge einer als angeborenes Recht verstandenen Sicherheit. Und ebenso wie der Begriff der Sicherheit trotz seiner Unschärfe und Breite in ein allgemeines Grundverständnis im Alltagswissen des Menschen verankert ist und voraussetzungslos verstanden wird, gelten für die Sicherheit im Netz jene Attribute, die auch für ein allgemeines Sicherheitsverständnis in Anspruch genommen werden: Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit. Wer für die wissenschaftliche Kommunikation Netze nutzt, wird bei diesen einem allgemeinen Sicherheitsverständnis zugeordneten Attributen aufhorchen, sind es doch jene Forderungen, die heute bisweilen verbissen die Diskussion um die Zukunft der wissenschaftlichen Kommunikation bestimmen. Ich möchte jetzt auf jene Sicherheitsmerkmale zurückkommen, sie aber unter den verschiedenen Aspekten der Wissenschaftskommunikation diskutieren: Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit unter der Rücksicht des Dokuments, des Autors, der Nachweissysteme, des Benutzers und der Bibliothek.

3. Sicherheit des Dokuments

Das Dokument als veröffentlichtes Ergebnis und Zeugnis eines wissenschaftlichen Erkenntnisprozesses war lange Zeit das endgültige Endergebnis einer wissenschaftlichen Arbeit, das Dokument als Dokumentation abgesicherter Inhalt, unveränderbar vorliegend und für alle Zeit archivierbar und archiviert. Die Sicherheit der Ergebnisse als Sicherheit des Dokuments war garantiert, die Veröffentlichung als Zeitschriftenartikel oder

[3] Brockhaus 1995

monographisches Werk seinerseits der Abschluss und der Garant für die Sicherheit des Dokuments. Die Wechselwirkungen aber, die durch interaktive Nutzbarkeit von Bild-, Ton- und Textdokumenten entstehen und ihr Einfluss auf Wissenschaft und wissenschaftliches Arbeiten sowie auf den Prozess der Erkenntnisgewinnung sind noch kaum untersucht. Gerade erst beginnen wir zu begreifen, wie die Existenz von dynamischen Dokumenten grundsätzliche wissenschaftliche Ergebnisse und den Output in Form wissenschaftlicher Publikationen revolutioniert, etwa dadurch, dass Erkenntnisgewinnung und -verarbeitung sowie die Verbreitung und Diskussion von Ideen in ein „Realtime-Verhältnis" geraten sind. Statik und Gegenwärtigkeit, Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit (mithin all jene Attribute von Sicherheit), lösen sich in reine Dynamik auf. Und wie Jüngst Thomas Hettche in der FAZ schrieb, „reisen wir dabei mit beängstigend leichtem Gepäck. Denn nichts was wir aufnehmen, akkumuliert sich noch in uns. So wie wir nicht mehr satt sind, wenn wir nicht essen, sind wir dumm, wenn der Datenfluss einmal abreißt. Und so klingt es fast unglaublich. Dass Bibliothekare, - einst Bewahrer von Buch und Kultur – heute aktiv daran beteiligt sind unsere anamnetische Kultur verschwinden zu lassen"[4] Wie unglaublich wichtig die Sicherheit der Netze damit geworden ist, liegt auf der Hand.

4. Sicherheit des Autors und seiner Dokumente

Der größte Angriff auf die Sicherheit des Autors und seiner Dokumente ist heute die Open Access Bewegung[5]. Denn die Entwicklung neuer Kooperationsformen für die Produktion und Distribution wissenschaftlicher Informationen wirft mehr Fragen auf als sie lösen kann: Dabei ist der prinzipielle Ansatz der Open Access und Open Archiv Bewegung grundsätzlich zu begrüßen und sicher ehrenwert: Alle Welt soll Zugang haben zu den Erkenntnissen von Wissenschaft und Forschung, keiner soll ausgeschlossen werden und keiner soll dafür bezahlen müssen. Nicht nur *free access*, sondern *auch free of charge access* ist die Forderung derjenigen, die das etablierte System nicht mehr für bezahlbar oder bezahlwürdig halten. „Open Access meint, dass Literatur kostenfrei und öffentlich im Internet zugänglich sein sollte, ohne finanziellen, technischen oder gesetzlichen Barrieren. In allen Fragen des Copyright sollte die einzige Einschränkung darin bestehen, den Autoren das Recht zu sichern, dass ihre Arbeit angemessen anerkannt und zitiert wird"[6].
Mit der *Berlin Declaration* etwa wird die deutsche wissenschaftliche Öffentlichkeit gleichsam verpflichtet, die Prinzipien des Open Access-Publizierens anzuwenden[7].
Hat also das traditionelle Verlagssystem versagt? Haben Verleger und Verlage über Jahrhunderte dazu beigetragen, die wissenschaftlichen Erkenntnisse zu verheimlichen statt sie zu verbreiten? Klagen wir heute über eine Informationsarmut oder über einen Information overload? Gab (und gibt) es keinen Mehrwert bei der Produktion von wissenschaftlichen Journalen, Büchern und Editionen und gab (und gibt) es keine sinnvolle Arbeitsteilung zwischen denen, die wissenschaftlich arbeiten und jenen die wissenschaftlich zuarbeiten, etwa verlegen?
Im Netz soll jetzt jeder, der wissenschaftlich arbeitet verlegen, jeder der wissenschaftlich arbeitet auch produzieren und vertreiben können. Also „back to the roots", zu jenem System

[4] Thomas Hettche in der FAZ vom 23.12.2003
[5] „Open Access meint, dass Literatur kostenfrei und öffentlich im Internet zugänglich sein sollte, ohne finanzielle, technische oder gesetzliche Barrieren. In allen Fragen des Copyright sollte die einzige Einschränkung darin bestehen, den Autoren das Recht zu sichern, dass ihre Arbeit angemessen anerkannt und zitiert wird".
[6] http://www.soros.org/openaccess/g/index.shtml, http://www.soros.org/openaccess/g/read.shtml
[7] „Wir beabsichtigen, unsere Forscher und Stipendiaten dazu anzuhalten, ihre Arbeiten nach dem „Prinzip des offenen Zugangs" zu veröffentlichen" (http://www.mpg.de/pdf/openaccess/BerlinDeclaration_dt.pdf)

wie man bis zum 17. Jahrhundert vor der Gründung der ersten wissenschaftlichen Zeitschrift[8] wissenschaftlich kommuniziert hat?
Open Access und *Open Access Publishing*[9] geben keine Antworten auf jene Fragen nach Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit. Zu individuell sind die Lösungen, zu „selbstgestrickt" die Systeme, zu wenig unabhängig die Betreiber.
Ob sich nun *Open Access* langfristig als ein nennenswertes Element in der wissenschaftlichen Kommunikation durchsetzt oder als semiprofessionelle Hometechnik marginalisiert wird, ob sich die Informationsbranche nach der Bildung beeindruckender und bedrückender Monopole wieder stabilisiert, die Sicherheit in der wissenschaftlichen Kommunikation ist verschwunden und durch unbeantwortete Fragen ersetzt worden:
Wie kann wissenschaftliche Information künftig produziert werden? Was gewinnt man, wenn man die bisherigen sicheren Systeme verlässt? Wie groß ist die Sicherheit der neuen Produktionsformen? Wer garantiert die Qualität? Wer sorgt für die Integrität der Daten und wer für die Langzeitverfügbarkeit? Wer zahlt für den wissenschaftlichen Publikationsprozess?[10] Wer organisiert die Qualitätsprüfung, das Peer Reviewing? Wer leistet künftig den Vertrieb und das Marketing für ein Produkt, das es gar nicht mehr geben soll? Wer strukturiert die wissenschaftlichen Inhalte so, dass sie sinnvoll in Disziplinen und Unterdisziplinen gegliedert und auffindbar sind? Wer hat Vertrauen in all die zweifelhaften elektronischen Suchmaschinen, die als einzige Nachweismittel für wissenschaftliche Inhalte bleiben sollen?

5. Sicherheit des Nachweissysteme

Wissenschaftliche Inhalte müssen nicht nur veröffentlicht werden, sie müssen auch nachweisbar und wieder auffindbar sein. Zu diesem Zweck gab und gibt es das komplette Instrumentarium bibliothekarischer und dokumentarischer Nachweissysteme. Das waren jahrhundertelang handgeschriebene Kataloge, gedruckte Bibliographien und Referateorgane. Die Electronic Library aber begann in Bibliotheken nicht mit Volltexten, sondern bei jenen Nachweissystemen.
In ihren Anfängen war die digitale Welt also nicht für Volltexte konzipiert und die ersten Online-Informationen stellten hohe Anforderungen an die Nutzer der Soft- und Hardware. Inzwischen hat die technologische Entwicklung eine ganze Reihe von Such- und Retrievalmöglichkeiten eröffnet, deren neue Qualität mit dem bisherigen Erschließungsinstrumentarium nichts mehr gemein hat. Bereits 1965 hat der amerikanische Informationswissenschaftler Licklider darauf hingewiesen, dass es nicht das Papier an sich zu ersetzen gilt, sondern dessen begrenzte Retrievalfähigkeit[11]. Heute müssen Nutzer wissenschaftlicher Informationen mit dem Erschließungssystem der Bestände genauso wie mit den Retrievalsystemen der digitalen Daten vertraut sein. Viele elektronische Nachweissysteme suggerieren eine umfassende Prüfung aller vorhandenen Literatur, können dies aber nur selten leisten. In diesen Fällen wird der Erschließungsapparat zum Fluch und das Suchsystem zum Sicherheitsrisiko, weil es den Nutzer in der falschen Gewissheit lässt,

[8] Garvy, William D.: Communication: The Essence of Science, facilitating information exchange among librarians, scientists, engineers and students. Pergamon Press: Oxford N.Y., 1979, S. 1/2
[9] Vgl. Harnad, Stevan: Dual open-access strategy. http://www.zbmed.de/summit/PPharnad.pdf
[10] Donald W. King, University of Pittsburgh School of Information Sciences, USA, Who is Going to Pay for Open Access Publishing?, Cologne summit on open access publishing 2004;
http://www.zbmed.de/summit/PPking.pdf
[11] J.C.R.Licklider: Libraries of the future. Cambridge, MA 1965

alles gefunden zu haben. Die Relevanz und Vollständigkeit der Ergebnisse kann allerdings nur einschätzen, wer das jeweilige Suchsystem beherrscht. Die Freiheit ist genauso trügerisch wie die Suggestivkraft eines scheinbaren Generalchecks aller Literatur und Informationen.
Die digitale Netzwerkrevolution beginnt ihre Kinder dann zu fressen, wenn die Technik den Menschen nicht schlauer macht, sondern dümmer zurücklässt. Er verlernt durch ihren Einsatz den sinnvollen Umgang mit wichtigen Werkzeugen und wird abhängig von online zur Verfügung stehenden Datenströmen, die er zunehmend weniger versteht und beherrscht. Im Wirrwarr der elektronischen Angebote weiß heute ein Nutzer kaum mehr, was er in den elektronischen Systemen wirklich suchen und finden kann. Vielmehr herrscht ein unbegriffener Crossover zwischen Mensch und Maschine. Der Leser (mutiert zum Endnutzer) wird zurückverwiesen auf die Unmenge der digitalen Datenbestände und ihrer Suchmaschinen im Netz, still gestellt in der falschen Gewissheit einer vollständigen Informations- und Literaturübersicht. Somit verkehrt sich Sicherheit in ihr Gegenteil und aus Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit resultiert Konfusion.

6. Sicherheit des Benutzers

Die wissenschaftliche Kommunikation in Datennetzen stellt nicht nur für den Autor, seine Dokumente und die Nachweissysteme, sondern auch für den Rezipienten von elektronischer Information und Literatur ein Sicherheitsrisiko dar. Nicht jenes, das ein jeder eingeht, der heute die Bühne der Netzkommunikation betritt, sondern ein ganz spezifisches Sicherheitsrisiko, das mit der Integrität des Inhalts von Dokumenten verknüpft ist. Die Einmaligkeit und Authentizität von Inhalten ist heute mehr denn je fraglich geworden. Eine Überprüfung häufig nicht möglich. Und wenn Open Access die Zukunft des wissenschaftlichen Publizierens sein soll, dann werden auch für den Benutzer Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit der Inhalte zu einem Sicherheitsrisiko. Dokumente auf einem fachlichen oder institutionellen Dokumentenserver sind kein Ersatz für eine zitierfähige Publikation in einer Fachzeitschrift. Sie bieten keine fachlich gegliederte Verbreitung in der Wissenschaftscommunity (diese läuft nach wie vor über die Disziplinen und ihre Fachzeitschriften), es findet keine Primärberücksichtigung in den für die wissenschaftliche Bewertung wichtigen Produkten *Science Citation Index* und *Web of Science* statt und es existieren dadurch nationale und internationale Akzeptanzprobleme. Eine bunte Mischung verschiedenster Dokumententypen, angefangen vom Volltext über Präsentationen, Vorträge bis hin zu wissenschaftlichen Primärdaten lassen den Benutzer nicht nur jegliches Gefühl der Sicherheit vermissen, sondern das Gefühl entstehen, endgültig in der Beliebigkeit von Google verloren zu sein.

7. Sicherheit der Bibliothek

Die Bibliothek galt lange als Inbegriff jener Sicherheit, die sich in Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit manifestierte. So langweilig, wie coolen Menschen Bausparen für die Altervorsorge erscheint, so sicher waren Bücher und Zeitschriften in Bibliotheken verwahrt und beschützt, wenn auch bisweilen der Schutz vor dem Leser zu weit getrieben wurde. Die Bibliothek als Ort der Sicherheit als Rückzugsraum vor der Vergänglichkeit, beschrieben sogar als Paradies[12] hat – getrieben von einem Ökonomisierungszwang der Wissenschaft längst jenen Anspruch aufgeben müssen und

[12] Jorge Luis Borghes: „Das Paradies habe ich mir immer als eine Art Bibliothek vorgestellt."

ist zum gemischten Informationsversorgungsbetrieb mutiert. Bereits vor 60 Jahren wurde die Universalbibliothek im Handtaschenformat erdacht. Einer der engsten Berater des Präsidenten Roosevelt, der Direktor des Office of Scientific Research and Development, Vannevar Bush konzipierte seine Memex, einen „Memory Extender" eine sonderbare elektrisch-mechanische Maschine, geschaffen um Inhalte und Bilder zu verknüpfen, den modernen Netz-PC mit Hyperlink-Technik auf dem Arbeitsplatz eines jeden Wissenschaftlers, die multimediale Universalbibliothek in der handlichen Größe einer Juke-Box. Mit ihrer Hilfe sollte 1945 Amerika der entscheidende Vorsprung in Wissenschaft und Forschung gelingen. Die Memex wurde nie gebaut und so blieb es zur damaligen Zeit bei der bloßen Vision einer alles verknüpfenden Literatur- und Informationsmaschine[13].

Das Menschheitswissen ist aber heute längst nicht mehr in schwerfälligen Folianten versteckt, sondern gelangt in blitzschnellen Elektronen durch Kupfer- und jüngst als Photonen durch Glasfaserkabel selbst in jene entlegenen Winkel, in denen Bibliotheken weder bekannt sind noch jemals gebaut wurden.

Die Informationswut über die Informationsarmut ist zur Informationsflut geworden und überschwemmt die Welt mit Wissen und Informationen, die viele gar nicht bestellt haben.

War es für den gebildeten Bibliothekar des 18. Jahrhunderts noch eine Wonne, im Kreise seiner Bücher einfach zu sein, so scheint er heute verflucht im Informationsozean; längst ist er nicht mehr der Spezialist, der Bildung und Wissen ermöglicht, sondern der ein Übermaß dessen zu verhindern sucht, das er Jahrhunderte lang mühsam angesammelt hat und das ihn heute zusammen mit den Lesern und Nutzern nach der digitalen Beschleunigung geradezu in den Würgegriff genommen hat. Denn längst ist Information und Wissen nicht mehr die Basis für Wissenschaft und Erkenntnis, sondern der Feind der Intelligenz.

Denn das entscheidende Wissen heute ist, zu wissen, was man nicht zu wissen braucht. Bei mehr als 80.000 Neuerscheinungen im Jahr ist es nicht mehr möglich, zu lesen, sondern bereits ein Ausweis von Belesenheit zu wissen, was man nicht zu lesen braucht[14].

Der Weg zur Wissensgesellschaft ist digital und die digitale Bibliothek die einzig konsequente Antwort auf die digitale Welt. Dennoch scheint der Mensch das große Hindernis auf dem Weg zur endgültigen Wissensgesellschaft zu sein: Die Masse der verfügbaren Daten (längst nicht mehr nur Information oder gar Wissen) steht in einem sonderbaren Missverhältnis zu den Zeitressourcen der Menschen. Immer mehr Daten buhlen um die Aufmerksamkeit potentieller Nutzer. Der Instant-Wissenschaftler mit dem längst gesellschaftsfähigen quick-and-dirty-Prinzip wird von seiner digitalen (oder längst schon virtuellen) Bibliothek versorgt und seit Bibliotheksbenutzer Kunden heißen zählt jeder Klick als Nutzung und das Selbstbewusstsein der Bibliothekare berauscht sich an kryptischen Zugriffszahlen, die keiner zu überprüfen geschweige denn zu interpretieren vermag. Und so schließt sich der Kreislauf: Die von den Bibliothekaren so bedauerte Datenflut wird von ihnen selbst stetig verstärkt.

Kein Tag ohne neues Internetportal und so versinkt eine ganze Welt in der Datenflut, ohne Hoffnung auf jene Arche Noah, der sie so dringend bedürfte. Bleibt uns also nichts als das Zählen der Zugriffe und die viel gelobte Dienstleistung, die nur noch als Performance überlebensfähig ist, wenn nicht die gute Leistung, sondern nur noch deren Inszenierung gilt?

Auch wer heute die Bestände einer Bibliothek nach den Kriterien von Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit bewertet, wird bitter enttäuscht. Die Reduzierung von Beständen, das massive Abbestellen von Zeitschriften ist

[13] Ball, R.: Die Zukunft der Spezialbibliotheken oder die Spezialbibliothek der Zukunft. In: BuB : Forum für Bibliothek und Information, 54 (2002), 10/11, 633 - 639

[14] Norbert Bolz: „Der Mensch ist zum Flaschenhals der Informationswelt geworden – er hemmt die hemmungslose Verbreitung von Daten und ist gleichzeitig - ausgestattet mit der Kraft des Vergessens - die letzte Instanz einer organisierten Ignoranz zur Filterung der Datenflut."

geradezu zu einem Volksport für Bibliothekare geworden. Stöhnten die Erwerbungsbibliothekare noch vor Jahren über die Last der vielen Bestellungen, brechen sie heute unter der riesigen Zahl der Abbestellungen zusammen. Sicher ist in Bibliotheken heute nur noch die Abbestellung. Und dies ist ein gespenstiges Szenario, weil es die K.O.-Runde der Bibliotheken einläutet. Wer die Sicherheit der Bestände (sei es im Netz oder traditionell) nicht mehr garantieren kann, wird künftig um seine Existenz bangen müssen - Was ist geschehen?
Die massive Zunahme der Informationsmenge, manifest im dramatischen Anstieg der Literatur- und Zeitschriftenproduktion brachte die Bibliotheken, deren Etats der Zunahme der Information nicht mehr Schritt halten konnten in eine schwierige Situation. Durch die parallel stattfindende Medienrevolution konnten aber die Printmedien nicht einfach durch digitale substituiert, sondern mussten additiv um diese ergänzt werden – ein Prozess, der die Leistungsfähigkeit der allermeisten Bibliotheken überfordert hat. Anstelle der notwendigen Konzentration wurde von jedem ein wenig angeboten – zu wenig von jedem. Es unterblieb zudem der Aufbau des notwendigen Know-Hows – um die Sicherheit der Bibliothek und ihrer Dienste war es geschehen. Längst diskutieren Entscheidungsträger über viele Personalstellen in Bibliotheken, die nur noch den Mangel verwalten.
Die Preisexplosion für Bücher und Zeitschriften insbesondere des STM-Marktes (Science-Technology-Medicine)[15] zeigt weiterhin, dass der Markt keinen Wettbewerb zuließ, sondern von wenigen Monopolisten beherrscht ist – echte Substitutionsprodukte gibt es auf dem Informationsmarkt nicht. Aber auch die Umkehr der wissenschaftlichen Publikationsverhältnisse und die Etablierung von Open Access Publishing bringen keinen Zugewinn an Sicherheit für die Bibliotheken und ihre Bestände. Wer etwa garantiert den Zugriff und die Zugriffssicherheit bei kostenfreien Angeboten? Wenn alles kostenfrei in Netz verfügbar ist werden keine Verträge mehr geschlossen werden, sich aber auch niemand mehr an Zusagen gebunden fühlen. Die Kehrseite von Freiheit ist Beliebigkeit. Und damit ist niemandem im wissenschaftlichen Umfeld wirklich gedient.

8. Zusammenfassung

Ich habe versucht zu zeigen, dass jene Sicherheitsaspekte wie Verfügbarkeit, Garantiertheit, Voraussehbarkeit, Berechenbarkeit und Haltbarkeit des Dokuments, des Autors, des Lesers und der Bibliothek samt ihrer Nachweissyssteme in der elektronischen Wissenschaftskommunikation auf verschiedenste Weise und in je unterschiedlicher Qualität gefährdet sind. Der Wechsel von einer traditionellen, auf Papier gestützten Wissenschaftskommunikation hin zu einer digitalen Publikations- und Kommunikationsform erfordert in besonderem Maße Sicherheitsvorkehrungen der verschiedensten Art, deren Notwendigkeit bis heute noch nicht allen Akteuren in letzter Konsequenz klar geworden ist. Besonders problematisch ist das „Suggestivgefühl" von Sicherheit und Vollständigkeit, das vor allem bei der zunehmend an den Endnutzer delegierten Informationssuche die nahezu immer vorhandenen Treffermengen elektronischer Suchmaschinen induziert. Aber auch die digitale Welt muß aufräumen mit dem Missverständnis, eine vollständige Informationsversorgung leisten zu können, auch wenn sie noch sehr dem Traum der nun scheinbar machbaren informationellen Absolutheit entspringt.

---

[15] „...prices in *all* fields are seen to have increased since 1970 at a rate significantly greater than inflation." *(Mellon Report on University Libraries & Scholarly Communication. ARL 1992)*
„Periodicals are the primary cause of the rapid rise in the cost of library services in the academic and industrial sectors over the last 10-15 years." *Gomersall, British Library, in Serials, 1991)* Butler 1999

Curriculum Vitae

Dr. Rafael Ball studied biology, Slavonic studies and philosophy at the universities of Mainz, Warsaw and Moscow. He took his doctorate in biology and has worked in the library sector since 1994, first in the library of the University of Freiburg, Germany, and then as the head of the Central Library of Research Centre Jülich.
Since 2002 he is Teaching professor at the Institute of Library and Information Science at the Jagiellonian University in Cracow, Poland, and at the Department of Information Studies of the University of Applied Sciences in Chur, Switzerland. The major priorities of his practical and theoretical work are library management and the development of the digital library services.

Ein Blick in die Zukunft: Trends in der Entwicklung von Informationsdiensten, -methoden und -praktiken

Prof. Dr. Josef Herget, Leiter des Bereichs Information und Dokumentation, Hochschule für Technik und Wirtschaft, Chur (Schweiz)

Abstract

In diesem Beitrag wird zunächst die Sicherheitsproblematik aus einer ökonomischen Perspektive beleuchtet. Die Ausgaben für Sicherheit steigen in Organisationen aller Art und stellen neue Herausforderungen an die organisatorische Gestaltung. Die Auswirkungen dieser Problematik beeinflussen auch die Informationsarbeit, dies sowohl aus der Sicht des einzelnen Informationsproduzenten als auch aus der Sicht von Informationsorganisationen, wie zum Beispiel Bibliotheken. Die einzelnen Wertschöpfungsprozesse verändern sich und verteuern die Informationsarbeit insgesamt. Abschliessend werden Ergebnisse einer Delphi-Studie präsentiert, die Experteneinschätzungen zu Entwicklungen in der Informationswissenschaft aufzeigen.

1. Sicherheit im Netz – Technologien und ökonomische Wirkungen

Moderne Informationsinfrastrukturen bilden die Basis unserer hochvernetzten, zunehmend kollaborativ agierenden Informations- und Kommunikationsumgebungen. Ohne sie ist Information, Forschung und Kommunikation kaum mehr vorstellbar. Ein sicheres und verlässliches Funktionieren dieser Plattformen der Wissensarbeit ist Voraussetzung für effiziente Arbeitsprozesse. Investitionen in diese grundlegenden Infrastrukturen sind daher unverzichtbar. Zunehmend sind allerdings massive Angriffe auf diese Infrastrukturen festzustellen, ob unberechtigter Zugang mit Missbrauch von Daten oder Ressourcen, das Ausspionieren von Passwörtern (zum Beispiel durch das sogenannte Phishing), das Einschleusen von Viren oder Überwachungssoftware, das Verändern oder Löschen von Dateien oder auch der Missbrauch von elektronischen Adressen zu Spamzwecken. Aber auch das systematische Stehlen von Forschungsresultaten und –berichten von internen Servern als moderne Formen digitaler Spionage sind keine Seltenheit mehr. Diese Attacken verursachen mittlerweile Schäden in Milliardenhöhe in den Volkswirtschaften. Folgerichtig wird der „Sicherheit“ zunehmend eine hohe Aufmerksamkeit gewidmet. Von dieser Entwicklung sind alle Akteure im wissenschaftlichen Produktionsprozess und der Vermittlung von Informationen ebenso betroffen. Sowohl der einzelne Forscher, der externe Informationen beschafft oder Ergebnisse seiner Arbeit austauscht, oder auch beispielsweise Bibliotheken, die Zugang zu ihren Informationsressourcen der Öffentlichkeit anbieten. Mittlerweile bieten auch fast alle Bibliotheken Arbeitsplätze mit öffentlichem Internetzugang an. Gerade auch sie müssen aber sichere Arbeitsumgebungen gewährleisten, was diese angesichts der begrenzten Personalkapazitäten und der kaum vorhandenen Qualifikationen vor besondere Probleme stellt.

Das Thema der Sicherheit wird hier umfassend betrachtet, darunter fallen alle Massnahmen, die sicherstellen sollen, dass Zugang, Beschaffung, Bereitstellung, Verarbeitung, Austausch

und Speicherung von Information in allen Formen von Berechtigten in der gewünschten Art und Weise erfolgen, ohne Behinderungen oder Manipulationen der eigenen Infrastruktur und Informationsressourcen befürchten zu müssen.

Das Gebiet der Informationssicherheit mit ihren diversen Konzepten ist denn auch durch eine hohe Innovationsrate gekennzeichnet. Neue Instrumente und Anwendungen drängen permanent in den Markt, der mittlerweile eine beträchtliche Grösse erreicht hat und weiterhin noch wachsen wird. Gartner Research (2004) prognostiziert den Entwicklungspfad und die voraussichtliche Marktreife neuer Entwicklungen im sogenannten „Hype Cycle" (der Hype Cycle zeichnet die Aufmerksamkeit (Visibility), die neuen Entwicklungen zukommt (zum Beispiel in der Presse, auf Konferenzen) und deren tatsächliche Marktreife und Akzeptanz (Maturity) vor; dabei werden auch zeitliche Aussagen darüber getroffen, wann eine Marktreife und damit eine Ausbreitung einer Technologie erwartet werden kann) wie folgt:

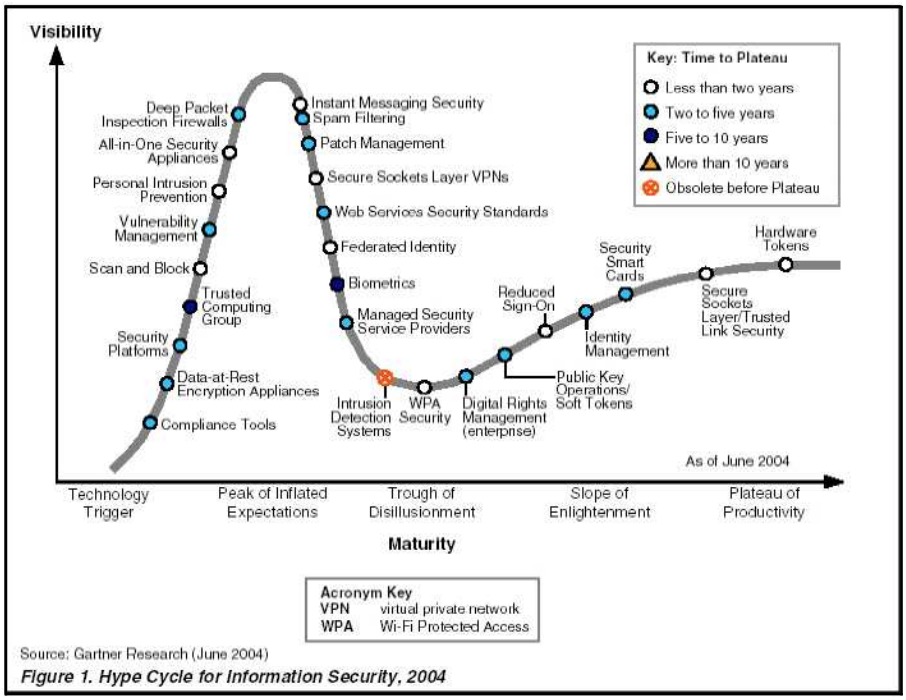


Figure 1. Hype Cycle for Information Security, 2004

Abbildung1: Hype Cycle für Informationssicherheit, 2004, Quelle: Gartner (Juni 2004)

Eine Vielzahl neuer Technologien und Anwendungen drängen auf den Markt, die Leistungsbeiträge für sicherere Arbeitsumgebungen verheissen. Deren jeweilige Beurteilung und Erprobung muss im Kontext der Anforderungen betrachtet werden. Sicherheit kostet Geld – je höher die Ansprüche an die Verfügbarkeit von Informationssystemen, um so mehr muss investiert werden:

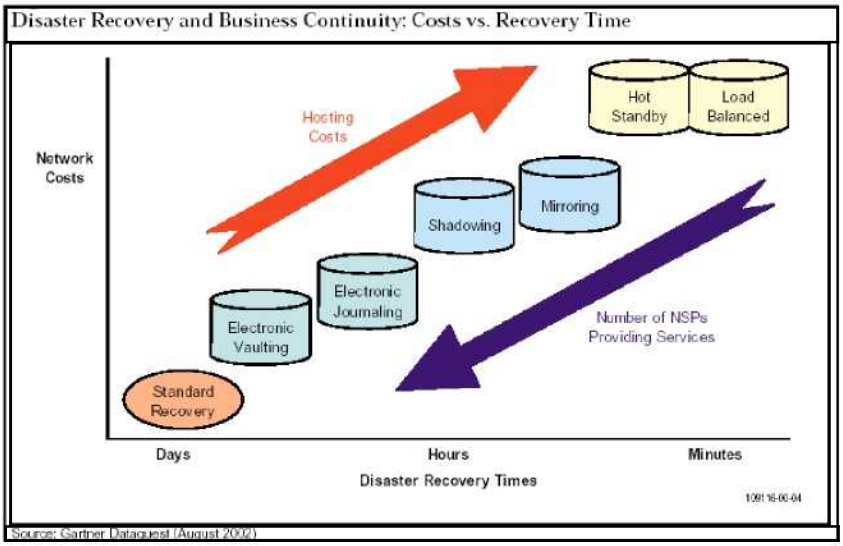


Abbildung 2: Disaster Recovery and Business Continuity; Quelle - Gartner (August 2002)

Für viele Organisationen ist eine ständige Verfügbarkeit ihrer Informationssysteme fast unverzichtbar geworden. Ein Ausfall von mehreren Tagen kann in der Regel nicht in Kauf genommen werden, folglich steigen die Kosten für entsprechende Vorsichtsmassnahmen.
Die Investitionen in Sicherheitsarchitekturen steigen seit Jahren kontinuierlich an. Die nordamerikanische Tendenz lässt sich ohne weiteres analog auf Europa übertragen. Ein immer grösserer Anteil des Investments in Informationstechnologie (IT) und IT-bezogene Dienstleistungen – die Budgets für IT sind in den letzten Jahren allenfalls moderat gestiegen - entfällt auf den Bereich der Informationssicherheit. Die Ausgaben für IT-Sicherheit-Diensleistungen haben sich innerhalb von 5 Jahren mehr als verdoppelt – ein Trend, der auch künftig anhalten dürfte.

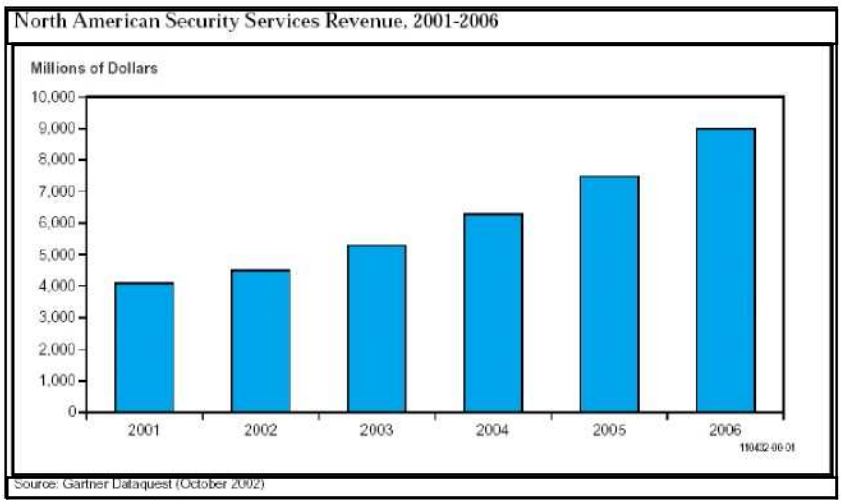


Abbildung 3: North American Security Services Revenue, 2001-2006; Quelle: Gartner (Oktober 2002)

Der grösste Anteil an den Kosten für Dienstleistungen der Informationssicherheit entfällt – folgt man der Prognose von Gartner - mittlerweile auf Beratungsleistungen.

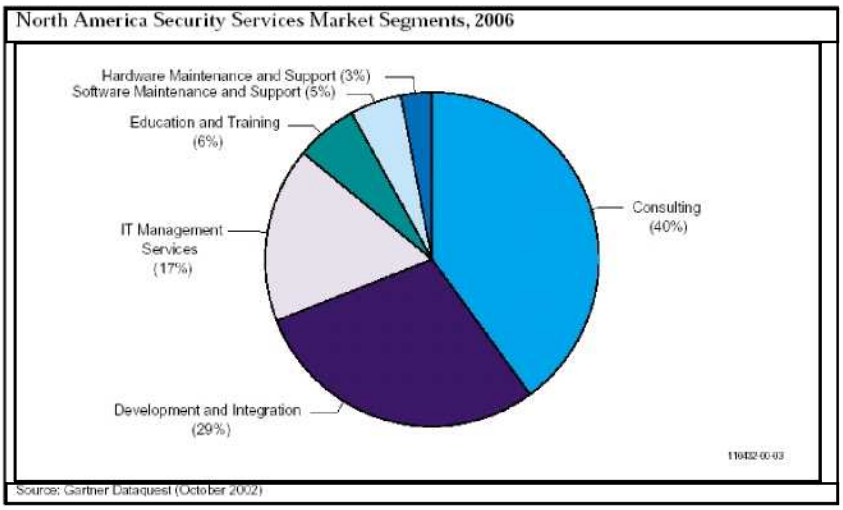


Abbildung 4: North American Security Services Market Segments, 2006; Quelle: Gartner (Oktober 2002)

Neue Technologien und Investitionen in IT-Sicherheit-Dienstleistungen umreissen jedoch nur einen Aspekt der Informationssicherheit. Bedingt durch die Durchdringung beinahe sämtlicher Geschäftsprozesse durch IT ergeben sich neue Herausforderungen ebenso für die Gestaltung der Organisation, sowohl in den Zuständigkeiten als auch den Prozessen, die verändert und häufig neu geschaffen werden müssen. Zahlreiche neue Aufgaben erfordern auch neue Qualifikationen, die zum Teil erst noch erworben werden müssen. Gerade auch die aktuelle Diskussion zur IT-Governance (Information Management-Governance wäre wohl die bessere Bezeichnung, da es vorwiegend um die Transparenz von Informationsprozessen geht), die sich aus dem US-amerikanischen Sarbanes-Oxley-Act zur Erhöhung der Transparenz in Unternehmen ergibt, aber auch aus europäischen Initiativen wie Basel II oder der 8. EU-Audit-Richtlinie, haben eine grössere Bedeutung der Informationssicherheit zur Folge und sie werden aufgrund zunehmender Regelungen insgesamt zu höheren Kosten der Informationsverarbeitung beitragen.

Aus dem dargelegten lässt sich folgende These formulieren:
These I
„Sicherheit im Netz“ führt zu neuen
- Technologien und Anwendungen,
- organisatorischen Regelungen,
- Aufgaben und
- Qualifikationsanforderungen.

Die Kosten der Informationsverarbeitung werden sich durch diese neuen Anforderungen erhöhen.

Zum Thema Informationssicherheit sind zahlreiche Informationsressourcen im Internet verfügbar, eine kleine Auswahl sei hier empfohlen:

Einige Links

- Allgemeine Informationen, Leitfäden, Downloads, Webkurs: www.bsi.bund.de/gshb/webkurs/index.htm
- IT Governance Institute: www.itgi.org
- Information Systems Audit and Control Association: www.isaca.org

2. Auswirkungen der Sicherheitsaspekte auf Prozesse der Informationsversorgung

Informationen werden in verschiedenen Kontexten beschafft, verarbeitet und distribuiert. Exemplarisch werden nachfolgend zwei typische Informationsprozesse betrachtet, einmal eine Perspektive, die an der Produktion von wissenschaftlicher Information orientiert ist, zum zweiten wird die betriebliche Perspektive betrachtet, wie sie zum Beispiel in innerbetrieblichen Informationsstellen vorzufinden ist. Analoge Überlegungen gelten für Bibliotheken und andere Institutionen der Informationsarbeit. Der informationelle Produktionsprozess lässt sich in primäre Aktivitäten, die unmittelbar wertschöpfend wirken und in sekundäre Aktivitäten, die zur Koordination der Infrastruktur und zur Sicherstellung des Ablaufs notwendig sind, unterteilen. IT-Sicherheit ist den sekundären Aktivitäten zuzuordnen. Fragen der IT-Sicherheit wirken sich auf jede einzelne Wertschöpfungsstufe aus, die Folge ist, dass damit der informationelle Produktionsprozess insgesamt mit höheren Kosten belastet wird. Als Kosten der Sicherheit sind beispielsweise bereits Aufwendungen für Virenfilter, Firewalls, Passwortverwaltung, Filtern und das Löschen von Spams, Anfertigung von Sicherheitskopien, Aufwendungen für Kryptographie und Verschlüsselung usw. zu rechnen.
Schematisch lassen sich die Auswirkungen auf den informationellen Produktionsprozess wie folgt darstellen:

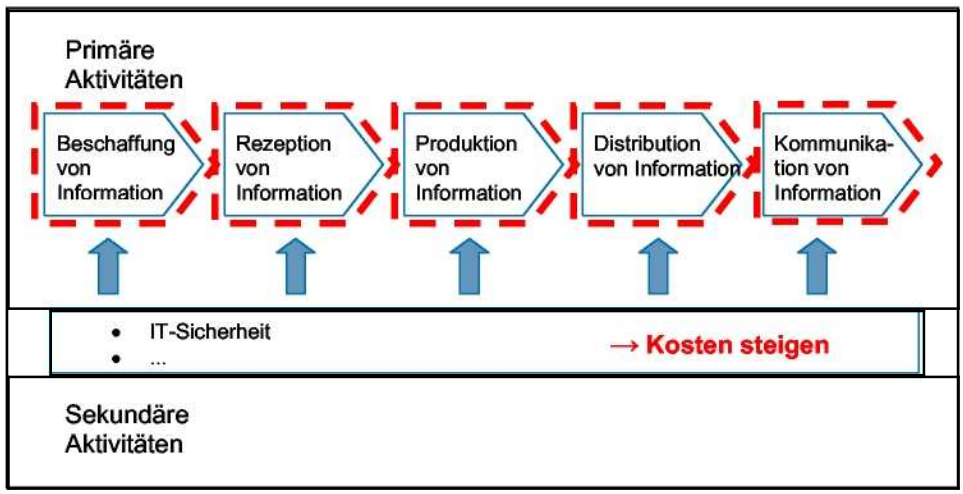


Abbildung 5: Der informationelle Produktionsprozess

Die schraffiert umrandeten Felder verdeutlichen die Erhöhung der Kosten der jeweiligen Wertschöpfungsstufen durch zusätzliche Kosten der IT-Sicherheit.

Auch die betriebliche Informationsversorgung unterliegt einem ähnlichen Phänomen mit vergleichbaren Auswirkungen. Auch die dortigen Wertschöpfungsprozesse werden von Sicherheitsaspekten durchdrungen und führen insgesamt zu einer höheren Kostenbelastung für die Informationsversorgung.

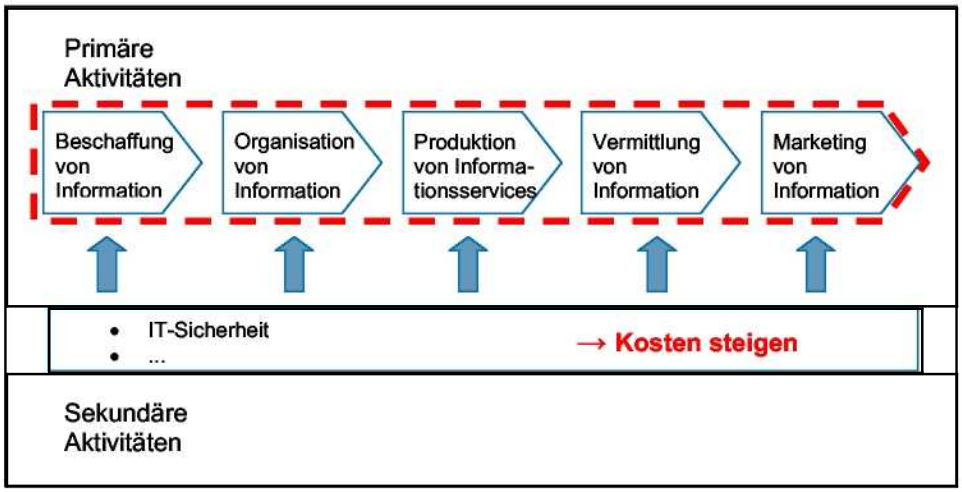


Abbildung 6: Die Informationsversorgung in der Praxis

Dies führt zur nächsten These:
These II
Der Prozess der Informationsversorgung ändert sich prinzipiell nicht, er wird allerdings „umständlicher" und teuerer.
„Sicherheit im Netz" schafft zusätzliche Kosten der Informationsversorgung, die schliesslich auf die Partizipanden der Information-Value-Chain umgewälzt werden (müssen).

3. Welche Entwicklungen erwarten die Information Professionals bis zum Jahr 2010?

Im Rahmen eines Forschungsprojektes an der HTW Chur zu zukünftigen Trends und Tendenzen der Informationswissenschaft wurde eine mehrstufige, trinationale Delphi-Studie durchgeführt. Die Delphi-Studie umfasst etwa 200 Experten (Praktiker und Wissenschaftler) aus den folgenden Berufsfeldern:

- Informationswirtschaft
- Informationsmanagement
- Archiv
- Bibliothek

Die Teilnehmer rekrutieren sich aus Deutschland, Österreich und der Schweiz. Beginn der Delphi-Studie war Herbst 2004, sie wird mit der dritten Erhebungsrunde im Sommer 2005 beendet sein.

Ziel der Delphi-Studie ist es vor allem, eine Bewertung möglicher zukünftiger Schwerpunkte informationswissenschaftlicher Forschung und Entwicklung mit einer grösseren Prognosesicherheit zu ermöglichen.

Die zu treffenden Aussagen beziehen sich auf das Jahr 2010.
Es wurde gefragt nach dem Grad der

- Wünschbarkeit
- Wichtigkeit
- Realisierbarkeit

von Ereignissen oder Aussagen.

Die Beantwortung konnte in der Intervall-Skala von 1 (nicht wünschbar/wichtig/realisierbar) - 6 (sehr wünschbar/wichtig/realisierbar) erfolgen.

Im Folgenden werden einige ausgewählte Ergebnisse nach der zweiten Befragungsrunde (Stand Januar 2005) vorgestellt.

Multimediale Datenbanksysteme
Bezüglich der Entwicklung von neuen Multimedia-Datenbanksystemen, die auch multimediale Anfragen erlauben, kann eine hohe Wünschbarkeit dieser Entwicklung festgestellt werden. Auch die Wichtigkeit wird noch als relativ hoch angesehen, die realistische Umsetzung dieser Entwicklung wird hingegen nüchterner bewertet und liegt im mittleren Bereich.

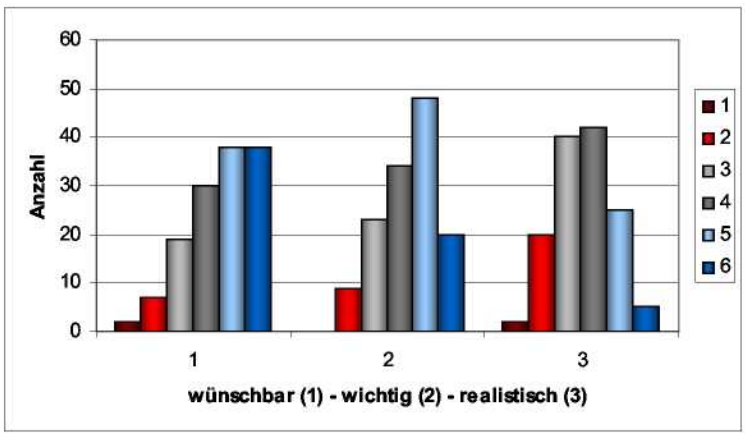


Abbildung 7: Entwicklung von neuen Multimedia-Datenbanksystemen, die auch multimediale Anfragen erlauben.

So wünschbar beispielsweise eine Anfrage nach Tönen, Bildern und anderen Multimedia-Objekten erscheint, mit einer Realisierung innerhalb der nächsten fünf Jahre wird eher nicht gerechnet.

Automatische Übersetzung
Die Mehrsprachigkeit lässt gerade in Europa den Wunsch nach einer automatischen Übersetzung in die wichtigsten europäischen Sprachen aufkommen. Trotz mittlerweile jahrzehntelanger Bemühungen entsprechen die verfügbaren Systeme immer noch nicht den oftmals gewünschten Qualitätsanforderungen. Bezogen auf automatische Übersetzungen für Datenbanken wird auch künftig die Realisierung hinter den Wünschen zurückbleiben, wie die Einschätzung der Experten ergibt.

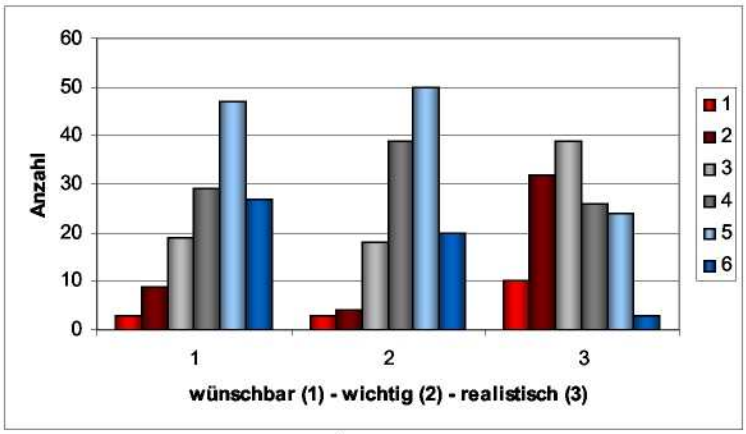


Abbildung 8: Automatische Übersetzungen zwischen den Sprachen Deutsch, Englisch, Französisch (und ggf. weiteren) werden für die wichtigen Datenbanken verfügbar sein.

Weitere Forschungsanstrengungen sind folglich auch hier zu erwarten, der Zeithorizont von fünf Jahren wird nach Ansicht der Experten nicht ausreichen, um unmittelbar professionell verwertbare Ergebnisse zu erzielen.

Selbstadaptive Suchsysteme
Als durchaus wichtig und erwünscht wird auch die Entwicklung von selbstadaptiven Suchsystemen für Endbenutzer angesehen. Die Möglichkeiten, dass sich die Informationssysteme automatisch dem Kontext des Informationsnachfragenden anpassen, werden aber auch mehrheitlich noch mit Skepsis beurteilt. Ein Durchbruch wird von der Mehrheit in den nächsten Jahren jedenfalls noch nicht erwartet.

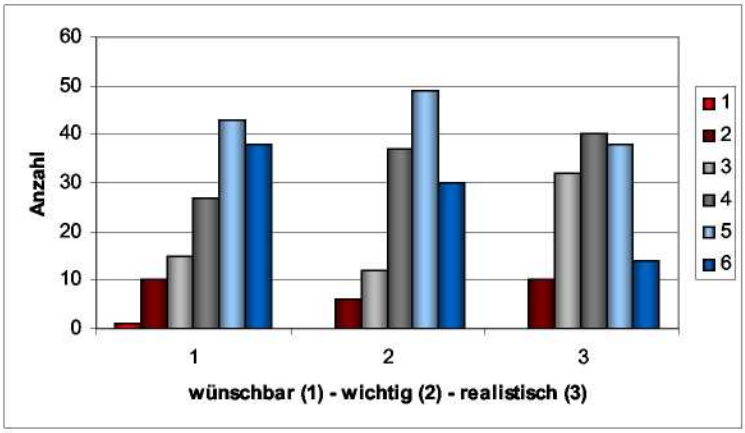


Abbildung 9: Suchsysteme für Endbenutzer werden zunehmend als selbstadaptive Systeme konzipiert werden.

Auch hier wird ein Forschungsfeld deutlich, dessen Wichtigkeit unter den Experten unbestritten ist, in dem befriedigende Resultate aber noch mehr Zeit benötigen werden.

Automatische Textzusammenfassung

Die ständig zunehmende Informationsmenge führt zum Wunsch, diese Informationsmenge zu reduzieren, ohne auf wichtige inhaltliche Aussagen verzichten zu müssen. Eine relative Zustimmung findet die Hypothese, nach der Systeme der automatischen Zusammfassung von Texten (Abstracting) an Bedeutung zunehmen werden.

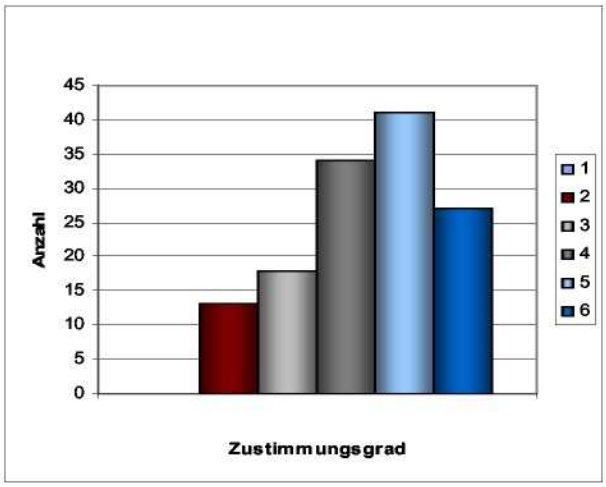


Abbildung 10: Systeme der automatischen Zusammenfassung von Texten (Abstracting) werden wegen der immer grösseren Textmengen an Bedeutung zunehmen.

Innovationspotenzial informationstechnischer Entwicklungen
Welche informationstechnischen Entwicklungen werden in den nächsten Jahren den Arbeitsbereich der befragten Experten mit innovativen Potenzialen verändern? Von den zur Beurteilung angebotenen sieben Entwicklungen, die auf eine offene Befragung nach zukunftsweisenden Entwicklungen in der ersten Runde zurückzuführen sind, messen die meisten Befragten ein grosses Potenzial der Langzeitarchivierung digitaler Daten, der automatischen Indexierung, den Suchtechnologien und dem ubiquitären Zugriff auf Informationssysteme zu. Relativ uneinheitlich ist die Beurteilung bezüglich des semantischen Webs, der Topic Maps und der Text- und Spracherkennung.

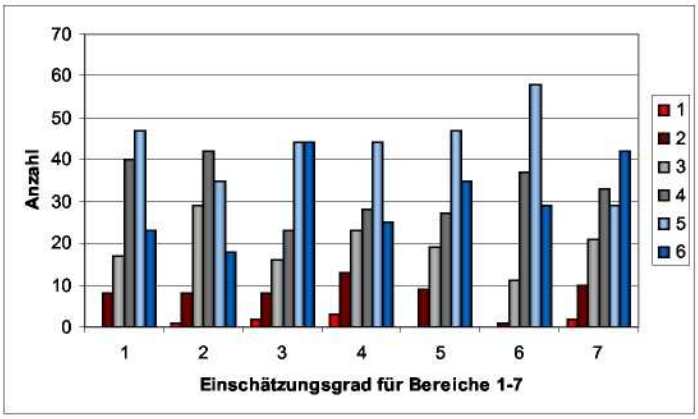


Abbildung 11: Wie schätzen Sie das Innovationspotenzial folgender informationstechnischer Entwicklungen bis zum Jahr 2010 für Ihren Arbeitsbereich ein?
1: semantische Netze / semantisches Web
2: Topic Maps / Ontologien
3: Langzeitarchivierung digitaler Daten
4: Text- und Spracherkennung
5: automatische Indexierung
6: Suchtechnologien
7: mobile Technologien / ubiquitärer Zugriff

Bedeutung von Forschungsfeldern
In welchen Gebieten wird künftig der grösste Forschungs- und Entwicklungsbedarf gesehen? Aus den angebotenen sechs Themenbereichen wird der grösste Bedarf in der Langzeitarchivierung digitaler Daten, der Informations- und Medienkompetenz und der Nutzerforschung gesehen. Rechtliche Fragen folgen mit geringem Abstand, für weniger wichtig werden Fragen zur Vermarktung von Informationen und zur Informationsgesellschaft gesehen.

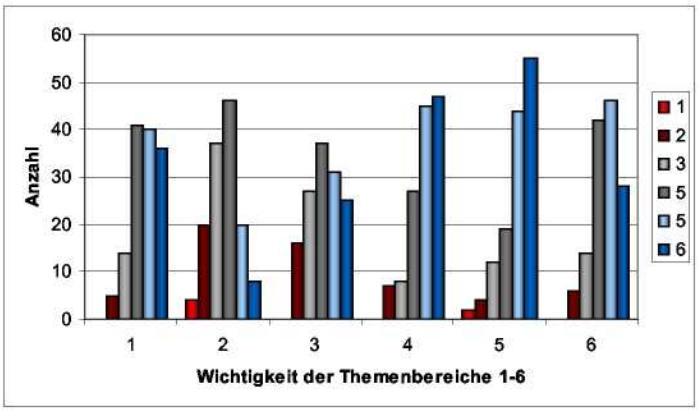


Abbildung 12: Für wie wichtig halten Sie Forschungs- und Entwicklungsarbeiten zu den folgenden Themenbereichen?
1: Nutzerforschung (Informationsbedarf und -verhalten)
2: Vermarktung von Informationen
3: Informationsgesellschaft, -ethik, -politik, -kultur
4: Informations- & Medienkompetenz / Information Literacy
5: Langzeitarchivierung digitaler Daten
6: Rechtliche Fragen (Urheber-, Informationsrecht)

Zusammenfassend und explizit bezogen auf die eingangs aufgeworfenen Fragen der Sicherheit im Netz lassen sich die Ergebnisse zu Zukunftstrends zu folgender These verdichten:

These III
Die Entwicklung neuer Methoden, Technologien und Praktiken in den nächsten Jahren in der Informationswissenschaft führt zu noch mehr digitalen und vernetzten Arbeitsformen – mit damit verbundenem grösseren Gefährdungspotential für sicheres Arbeiten.
Sicherheit im Netz wird nicht als Kernaufgabe der Informationswissenschaftler und Informationspraktiker betrachtet – es findet eine Delegation der Zuständigkeit und Verantwortung statt.

4. Fazit

Methoden, Verfahren und Techniken der Informationsarbeit unterliegen einem beständigen Innovationstempo. An dieser Dynamik wird sich auch künftig nichts ändern. Die Fragen der Sicherheit im Netz und ihren Auswirkungen auf die Informationsarbeit führt zu mannigfachen Entwicklungen, die sich folgendermaßen darstellen lassen:

- Der Komplex der Informationssicherheit wird künftig für die Informationsarbeit an Bedeutung zunehmen
- Das Risikopotential der zunehmend digitalisierten Information-Value-Chain erhöht sich weiterhin
- Verstärkte Kooperation mit IT und/oder neue Qualifikationen für die Informations-versorgung sind notwendig

- Die Kosten der Informationsarbeit für den Endnutzer steigen ohne zusätzliche informationelle Mehrwerte zu bieten
- Mehr Mittel müssen künftig für Fragen der Sicherheit im Netz ausgegeben werden – dies wird bei begrenzt steigenden Budgets tendenziell zu einer Umverteilung der Mittel führen müssen.

In der Frage der Sicherheit verlassen sich Informationswissenschaftler und -praktiker auf die Informatik. Eine enge Zusammenarbeit ist folglich Voraussetzung, um auch künftig effiziente Informationsversorgungssysteme für Wirtschaft und Gesellschaft zu gewährleisten.

Quellen

Gartner Research: NSP Opportunities Exist in Network Security and Business Continuity, 19. August 2002
Gartner Research: North America Security Services Market Forecast: 2001-2006, 9. October 2002
Gartner Research: Hype Cycle for Information Security, 2004, 3 June 2004

Curriculum Vitae

Josef Herget is Professor for Information Science at the University of Applied Sciences in Chur, Switzerland.
Previously he worked at the University of Konstanz, Germany and Marmara University, Istanbul, Turkey. He has wide experience as a consultant and was engaged in many national and European projects within the information society. His research areas are: information management, economics of information services, technology transfer and information markets.

Präsentation

Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

The most dangerous enemy sits in my chair

Dr. Tomáš Řehák, Director of the Central Public Library of Prague

Abstract

To make our data safer might be quite a cheap task. The most common security flaws are usually quite easy to identify, however sometimes very difficult to remove because they are deeply mounted to our habits and corporate culture.

Something about MLP

Municipal Library of Prague (www.mlp.cz) is the biggest public library in Czech Republic. Well, the National Library has got bigger stocks but from all other points of view we are the biggest one.
MLP started to flirt with computers quite soon. Since 1982 all the new book records have been stored into computers. We have developed our own library system called **Koniáš**, which we have been operating since 1997. We have quite strong IT division staffed with more then 14 full-time-equivalents. And they are very capable indeed with some members of the team being real stars.

Something about myself

I have been Municipal Library of Prague Managing Director since July 2002. However I have been in MLP since 1992, starting as IT specialist, then head of IT department and later deputy director. I graduated at Charles University in Prague at Faculty of Mathematics, Department of Probability and Mathematical Statistics. Because of my education my approach to IT has never been really technical and having been for few years out of IT business gives me a kind of distance. I am no longer really IT skilled man, but I still understand basic principles behind the scenes. And I have had responsibility for system security for many years. At the beginning that was administrator responsibility, nowadays it is managerial one. And all that together gives me fine point of view for my attempt to describe some general principles about system security.

Foreword

The aim of this presentation is just to share few thoughts how to make our data safer. I will give no really new bright ideas. All I will speak about are common and well known principles. May be they are so common and plain that we quite often forget to follow them…

Before we get into different dangers which jeopardize our data and before we start to discuss how to challenge those dangers, let's start with one very simple principle:

A chain is just as strong as its weakest link. Simple enough? Too obvious to mention it here? Okay, let's have few examples.

Once upon a time, there was a library. They spent some € 10 000 for highly sophisticated firewall system in order to make their network safe from outside attacks.

Administrator login: Administrator
Password: Administrator

Welcome to the land of wasted money. Feel free to do whatever you want to…

Another example: You have very well established firewall system effectively protecting you from Internet attacks. There are some OPAC computers at your library for readers to allow them to search your catalogues. There is also an Internet Explorer installed there for users to browse outside sources. All potentially dangerous programs were de-installed from the computers to prevent users to misuse them. Is that safe? Of course it is not! It is relatively easy to use IE to download and run already prepared remote Java Script which allows a hacker to access not only OPAC computer but the whole network which is no longer protected by firewall, because the hacker is already behind it and OPAC account needs an access to main database. The chain is just as strong as its weakest link…

Another example from our own experience: We were making some cataloguing in one of remote branch libraries. The branch was not connected to any data line, so we tried to backup data some way. Therefore we put two discs in the computer, one mirroring the other one. That's quite efficient way to make data safer. However – the chain is just as strong as its weakest link. What was the weakest link? A window. Not Microsoft Windows, just a real plain window. Some burglar broke the glass in a night and stole the computer. The computer was worth just few hundreds of Euros but data were worth few months of work. The chain is just as strong as its weakest link…

What is the lesson? Identify the weakest link and invest your money and resources only there. Strengthening anything else but the weakest link brings little if no effect at all.

What jeopardizes our data?

1) System failures
   - Hardware failures (computer discs, networks,…)
   - Software failures (program crashes)
2) User mistakes
   - Authorized users (insiders) doing non-intentionally something wrong
3) Attacks
   - People (usually outsiders) deliberately attacking our data, both directly (hackers,…) or non-directly (viruses, Trojan horses, spyware,…)

How to protect our data against system failures?

First of all: **Do backup your data!** And do it regularly and frequently and store more then just one last copy. Any effort to prevent system failures is not 100 % effective and so there still is some danger left. And we may realize some day that our database is corrupt, erased or just lost because of disc failure. In such a case it is really a great difference if we must go back one day, one week, one year or we have no backup at all.

But even when we do our backups regularly and frequently, any system failure usually means trouble. We may lose some data or at least the main database is not accessible for some time. Therefore it is wise to reduce the probability of system failures as much as we can. Basically that is done by redundancy of critical system components. That means, that some critical components (like discs) are doubled or multiplied and in case of failure there is a substitute. How effective is redundancy approach?

Let's say that a probability of disc breaking down and destroying all the data just today is 1:1000. That's sounds quite fine, doesn't it? Well, if you use the disc for three years, i.e. for more than 1000 days, there is fairly high probability it will eventually break down during the period. What can we do? The simplest thing to do is to mirror[1] the disc to another identical one. If the probability of disc failure during the day is 1:1000, then probability of simultaneous failure of both discs during the day is 1:1000x1000 = 1:1 000 000. That means that by just doubling the costs we have raised the data security 1000 times. That is really not bad! Actually the whole idea of RAID disc arrays is based on this principle.

You may buy very good RAID 5 or RAID 50 disc arrays nowadays. They are not only safe, but pretty fast at the same time and they can accommodate several TB of data. It is wise to use high tech RAID disc array to accommodate at least most valuable and most accessed data. Of course, they are quite expensive too – top prices approaching half a million Euros.

But we usually do not have enough money to accommodate all our data that way. Fortunately, there is an option we can use, which is a kind of compromise between expensive RAID arrays and plain computer discs. Today's IDE discs are cheap (they cost just few hundreds Euros) and have capacity of hundreds GB (500 GB are the latest ones at the market). Contemporary PCs usually have a possibility to accommodate 2 or 4 identical IDE discs organized as RAID 1 or RAID 10 respectively. RAID 1 means just two identical discs containing the very same data (i.e. mirroring), RAID 10 uses 4 identical discs where data are divided to two discs and other two ones are mirroring them. For some 2000 Euros you can have a quite safe and fast data server with capacity about 1 TB.

How to protect our data against user mistakes?

First of all: **Do backup your data!** And do it regularly and frequently and store more then just one last copy. Any effort to prevent user mistakes is not 100 % effective and so there still is some danger left. Why? Because **people do mistakes!**
Everybody can make a mistake from time to time. You can not eliminate that; you can only reduce the number of mistakes people do and reduce their impact. There are basically two different strategies to reduce the number and impact of mistakes.
First strategy is system-based. You maintain a complex of access rights which determines who is allowed what. System must decide for every kind of operation if this particular user may do it. Drawback is that system administrators spend enormous amount of time changing system rights. That's because people are leaving jobs and new people are coming, organizational structures are changing, people are having holidays or they are ill and someone has to do their job etc. At the end everybody is using supervisor account whose password is empty or known to everybody, because that is the only way to do everyday work. Trust me; I experienced such a system some 12 years ago when I started to work at MLP.

[1] To mirror disc = to keep identical data on another disc all the time. It can be done by connecting two discs into one controller or by some other way.

The second strategy which I prefer much more is people-based. Every user has the same computer access rights. So they can do everything. But that does not mean they may do everything. To determine who is allowed to do the particular operation – that is not the system's task but the managers' task. People must know what they are and what they are not allowed to do. System's task is to record (log) all operations and also who made them. So if someone breaks the rules, there is evidence and there is responsibility. In a large complex organizational structure with hundreds of people you might implement some kind of mixed strategy where there are few (two, three) levels of access rights. We use this strategy at MLP with quite fine results.

Both strategies have one important precondition: every user must be identified. Therefore everybody must have his/her own account and really secret password which is known to nobody else. Actually, that is not so easy. First you must persuade people that they really must not tell anybody their passwords. In some organizations it is rather normal that people know passwords of their close colleagues. Especially when you use the strategy of system-based access rights it might be the simplest way how to deputize for colleagues. However it spoils the whole system and makes it useless. So again - people must not tell anybody their passwords. But even when people accept that, there still is the problem: what kind of password?
Generally passwords should be:

1) Easy to remember, otherwise people tend to write them down to papers next to the computer etc…
2) Long enough, usually password consisting of at least 8 characters is acceptable
3) Hard to guess, so no first or second names of relatives etc.,
4) Meaningless, otherwise they are easy to crack with special programs using huge dictionaries in few languages
5) Containing some non-alphabet characters and combining uppercase and lowercase letters, which makes password cracking even more difficult
6) Changed frequently, otherwise they eventually might become non-secret because of some mistake.

Obviously it is rather difficult to invent such a password so kind of compromise must take the place. However you should tell people what kind of passwords they may use and what they may not use.
There are systems combining password (or PIN) with some other authorization (chip cards, thumbprints etc.) which might improve the security a lot, but generally they are rather expensive.

Usually the most dangerous mistakes are the ones made by system administrators. They have high security clearance and access rights. It's good practice not to use administrator/root account for "normal" tasks. So every system administrator should have normal account with normal, non administrative privileges and use it for everyday tasks. It might prevent some mistakes, but not all of them. He must use his admin rights in order to maintain the system. And one horrible day, when everything is going wrong, telephones are ringing, users are complaining, he presses the OK button. And instantly he knows it was a terrible mistake. But it is too late.
There are some good practices which could reduce the loss. First of all – do make backups. Second – do not do too many changes in one step. Always verify that you have a valid backup, do just one change, test the system, backup the data and then do another step. It might be rather slow but it is much easier to identify mistakes and to rollback them.

How to protect our data against attacks?

First of all: **Do backup your data!** And do it regularly and frequently and store more then just one last copy. Any effort to secure data against attacks is not 100 % effective and so there still is some danger left. Why? Because **attackers are always one step further!** Even the best protected systems are infiltrated sometimes and we can read about successful attacks against banks, military institutions etc. We can spend not nearly comparable amount of money in order to protect ourselves. But that does not mean we cannot do anything. There are some things we can do:

Try not to be an attractive target. Attacking a system is difficult and dangerous. In most cases it is considered a crime with quite serious punishment. Therefore hackers need some motivation to attack just your system. They may do it for money or some similar benefit. They may want to add some money into their account or accounts of their friends or remove borrowed items from account records. Or they may want to steal personal data of our users and sell them to some direct mailing company. Therefore it is not really wise to produce public statements like: "We have everything in computers we do not use any paper records any more. And all our data are accessible via Internet – of course only to the authorized users. And our administrators can do all the maintenance remotely..." That will probably attract undesirable attention pretty soon.

But there might be other kind of motivation for hackers. Some of them do their dubious activities just for fun of facing a challenge. So again try to avoid public statements like: "Our system is 100 % hacker-proof. There is no way to break in. We are absolutely sure about it!" It's like wearing red t-shirt in bull corral...

Do use a firewall. It is relatively cheap to set up some firewall system to protect your network from attacks coming via Internet. And even cheap and simple firewalls can stop vast majority of attacks. Most attacks are just preliminary attempts, mostly provided by robots trying to reveal weak points. If the robot probes into your system and attempt is successfully bounced off, it usually stops and moves the aim to some other system. And to ensure that you need just some primitive router with capability of IP packet filtering. Which may be an old PC with installed LINUX operating system and few freeware programs – overall costs are some 300 Euros. Of course you may easily spend 30.000 Euros for highly sophisticated firewall system and you will get higher protection. But do not expect 100 times higher protection! Actually, the more the firewall is common and widely spread the more it is vulnerable. Using some exotic rare means of protection preferably developed by your own IT staff and used only by you might be the very best solution. It's much more difficult to attack unknown system then something very common with well known structure and weak points.

Lock your computer! Firewall cannot protect you from attacks using your internal computers, i.e. computers behind the firewall. Is such a thing possible? Of course it is! In libraries it is quite common that reference librarians leave their computers in order to help readers find items at shelves etc. If the abandoned computer is left unattended and unlocked for few minutes it might be enough for causing quite a serious problem. Most of operating systems have a capability to lock the workstation so it cannot be used without password. Easy enough; however most users are reluctant to do that. May be they are lazy, they may forget to do that. So it is managerial task to motivate the staff.

Also, among the other important means of data protection there are physical protection means which prevent unauthorized people to use staff computers. I am speaking about doors, windows, locks, alarms, guards etc…

Use some anti-virus protection. Basic anti-virus solution might be relatively cheap and there is a great difference between cheap protection and no protection at all. Most viruses are spread through e-mails so it is wise to equip your mail server with some kind of anti-virus plug-in. That might be quite cheap, for example at www.ararat.cz you may find a free solution called VirWall which might be used together with Mercury mail server. Similar protection might be established at your proxy server to prevent users to download infected programs from WWW or FTP servers. Anti virus protection at mail servers and proxy servers may eliminate vast majority of incoming infection and careful and updated virus protection at your main data servers may reduce impact of remaining infection. But there is still some danger left. You may consider installing virus protection at every single computer at your network. That is quite wise, but somewhat expensive at the same time. What is at least comparably effective is people-based protection. Again, establish a set of rules which are known to everybody and motivate people to follow them. Users should know they must not download and install new software without permission of system administrators and they will be responsible for any damage caused by breaking the rule. And everybody should know that "innocent" screen savers, IE plug-ins, simple games etc, are most common sources of infection.

Do not sell sensitive data! Especially do not sell user personal data, accounts and passwords. You do not do that of course. Unless … do you sell your old computers? Are their discs clean? I do not mean just formatted – it is relatively easy to restore data from formatted disc. They should be really wiped out with some special software. Otherwise it is like selling out keys from your expensive armour-plated doors.

Last three recommendations

First of all: **Do backup your data!** And do it regularly and frequently and store more then just one last copy. Do you know what the most usual day for backing up data is? Tomorrow! There is always so little pressure for making backups. System is going fine, we haven't needed any backup for years, so why just today? Tomorrow will do enough…

And do not only backup your data, distribute the backups too. Your data should be safe not only in case of hardware failure or hacker attack. There might also be cases of robbery, fire, flood or other disasters. Therefore it is good idea to keep backup data at another location. You might store backup tapes at some branch or even in bank safe. Problem is that transport backup media every day to some other location is quite annoying and expensive as well. When there is the permanent data line between different buildings of your institution, it probably is quite unused at night. Therefore you can copy data through data line to backup server located in another building. That backup strategy is not as expensive and it can protect your data even in case of serious disasters.

Value your data! We are used to say that our data are among our most valuable assets. But do we know how valuable they are? Do we appraise them? Can we tell how many Euros are they worth? Have we ever tried to insure them?
To calculate value of the data and the cost of their loss helps to make a decision about data protecting and related investments.

We may estimate cost of loosing today's data and rolling back to yesterday's copy to 50.000 Euros. It is cost of having library closed for two days trying to reconstruct all what has happened since the last backup and preparing system to operate again. It does not include cost of lost goodwill, related PR costs etc, but anyway, let's accept € 50.000 as estimated value. And let's say that probability of this to happen once during a year is 1:10. We can calculate "insurance value" as cost of lost (€ 50.000) multiplied by probability of happening it (0.1) In our case the "insurance value" is some 5.000 Euros. Therefore if we can nearly eliminate the probability of data lost, it is worth 5.000 Euros. And if we can do that on expense of € 3.000 (maybe by installing RAID disc array), it is pretty good investment!
That may sound too complicated, but it is not. Just spend few hours trying to imagine what we must do in different cases and what will be the cost of doing that. That will help a lot in establishing different strategies of data security and it will improve your negotiating position with money keepers too…

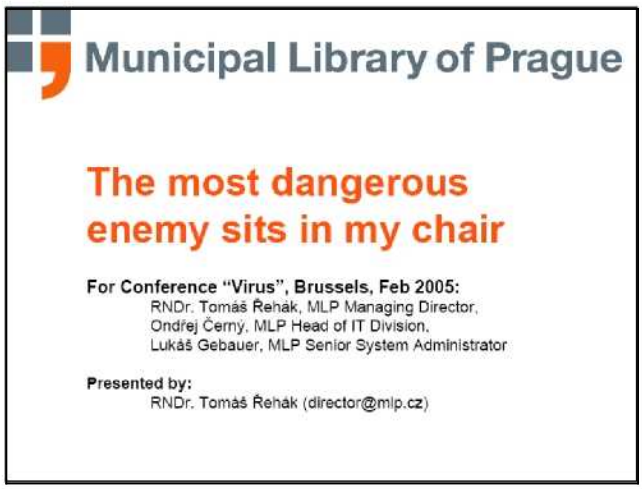
Be paranoiac! It is always wise to have at least one member of staff who is capable to think paranoiac way. You know those people: "And what would we do, if someone burglarizes into our server room during the night and establishes a new administrator account in order to have future access into our network?" Don't think it is impossible; just think it over few times to appraise such a possibility.

P.S.: Do backup your data!

Curriculum Vitae

Born 1964 at Prague. Graduated on Charles University in Prague, Faculty of Mathematics, Department of Probability and Mathematical Statistics.
Professional career: System analyst, IT teacher, Head of IT department, Deputy library director, Managing director.

Präsentation



Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Asymmetric Security and Network Intelligence: The Future

Fabio Ghioni, Telecom Italia

Abstract

Technology and the Internet have transformed criminals into pervasive entities that are able to launch attacks at any time and from virtually anywhere in the world. Information security specialists, both in National Security and private companies, are thus challenged with protecting the cyber-space against unpredictable and ever changing attacks. Information security in a business must be rethought on a multi-layered basis with the objective of defending all the levels and processes of an information system from both internal (employees or brute force) and external (such as distributed denial of service and above all industrial and competitive intelligence) malicious attacks.

Introduction

Since the break-up of the Soviet Union in 1991, the United States has been the world's sole superpower in terms of conventional weaponry. The US supremacy in conventional forces caused weaker opponents to use alternative and innovative weapons and tactics. The attacks of 11 September 2001 were the most devastating instance of "asymmetric attack" against the Western sense of invulnerability. In today's world of technological specialization, perpetrators and techniques have attained a high level of sophistication. In the last decade, the Information Age has dramatically changed the way in which the functioning of our societies is intertwined with technology.

Internet Age: New Environment and New Threats

Today most organizations are faced with a growing number of threats mainly arising from the heavy dependence of services upon Information Technology and the potential misuse of IT infrastructures due to their high flexibility. The electronic interconnection among many Critical Infrastructures poses obvious security problems. A great number of vital and private information is exchanged through the network..

The open architecture of the Internet has created a new medium for perpetrating crimes. The anonymity provided by the Net, as well as its global and unregulated nature, has produced an exponential explosion in the number and types of technology-based crimes. The growing number of Internet users has provided ill-intentioned people with a fertile environment for carrying out computer crimes. Small groups of individuals can access information resources located in diverse IT infrastructures with a minimum amount of effort and risk.

The spread of the Internet both for personal and business use has increased the number and variety of threats which all public and private institutions are faced with:

- Denial of Service
- Insider trading
- External and internal intrusion

- Distribution of pedo-pornographic material
- Theft of intellectual property
- Industrial espionage
- Data destruction or misappropriation
- Unauthorized access to confidential information
- Fraud
- Theft

The Asymmetric Threat

The concept of Asymmetric Threat is borrowed from the military definition of Asymmetric Warfare and it can be defined as: *"the broad and unpredictable spectrum of military, paramilitary and information operations conducted by nations, organizations or individuals or by indigenous or surrogate forces under their control, specifically targeting weaknesses and vulnerabilities within an enemy government or armed force."*
The increased complexity of technology and software combined with the greater ubiquity of the Internet has played a fundamental role in the upsurge of cyber crimes. The heavy dependence of systems upon the information infrastructure creates the ideal scenario for Asymmetric Conflict, where small groups of individuals can produce massive damage with a minimum effort and risk from virtually anywhere in the world.

Business Implications

The growing interdependence of infrastructures poses problems in terms of protection from accidental and malicious attacks and demands joint action in the building up of a comprehensive security concept against asymmetric threats. Providers delivering essential services are required to guarantee the integrity of the underlying infrastructure since they have become the backbone of social and economic life worldwide.

The Evolution of Critical Infrastructures

The underlying concepts of traditional infrastructures have been challenged by convergence within the computer and telecom industries. Public telecom infrastructures have moved from narrowband network for voice communication to interoperating and converging packet-switched networks. The convergence of voice and data applications is leading to the evolution of hybrid networks combining infrastructures of different jurisdictions and disciplines with those of public wireline and wireless carriers. Most sectors which are vital to our everyday activities, such as electricity and transport, heavily rely on public telecom infrastructures.

The Asymmetric Approach to Security

"Information is an asset which, like other important business assets, has value for an organization and consequently needs to be suitably protected. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected." (ISO 17799:2000) The exponential growth of incidents related to the loss of critical data urges all private and public entities to guarantee the security of information. The multifaced nature of the electronic datum requires a diversified approach to security. Information leakage is one of the most sensitive instances of corporate incidents entailing a criminal intention. Loss of critical

information may also depend upon inadequate protection, i.e. a lack of policy enforcement or a poor classification system
Internal data protection policies need to be enforced through *ad hoc* organizational and technical countermeasures. Information must be correctly classified in terms of confidentiality levels so that only authorized entities can access them. The definition of a comprehensive clearance procedure based on efficient permission parameters is essential for the implementation of an effective classification system.

Business Intelligence

"Business Intelligence is the activity of monitoring the environment external to the firm for information that is relevant for the decision making process in the company" (Benjamin Gilad, 1988)
The "situational awareness" concept, borrowed from military aviation, perfectly describes the essence of Business Intelligence, i.e. ensure one's surviving through a deep awareness of the environment so as to avoid threats and take up calculated risk. Business Intelligence activities allow to gather, analyze and circulate useful information to the top management.
Information is not in itself knowledge; the latter derives from an elaboration of the former unveiling the underlying structures. intelligence consists in using knowledge as a means of reaching a strategic objective. The most basic objective of counterintelligence is to protect information from those that are not authorized to receive it, to counter potential threats and to enhance security. Counterintelligence should not only protect against aggressive and illegal information collection but also against accidents such as unintentional information leakage that can harm a company and affect its ability to compete in its market.

Intelligent Network Security

An intelligent network (IN) is a service-independent telecommunications network, i.e. intelligence is taken out of the switch and placed in computer nodes that are distributed throughout the network. The advantages of an IN are the following:

- The network operator is able to develop and control services more efficiently;
- New capabilities can be rapidly introduced into the network;
- Services are easily customized to meet individual customer's needs.

When dealing with the security of strictly interconnected systems and networks it is necessary to view them both in their single components (ultraportable devices, Personal Area Networks, large databases or corporate WANs) and as a whole. Since it is not always possible to ensure accurate operations on the entire infrastructure, it is vital that organizations are able to monitor and manage incidents, cyber attacks and fraud against themselves and their clients through an integrated platform. An adequate platform for incident detection and management will rely on distributed "intelligent" probes and peripheral agents which will gather alarms from monitored systems and will screen traffic on a parametric basis. An integrated platform is vital to monitor and manage incidents and cyber attacks. Parametric interception is performed through probes which gather only investigation-related data flows. Parametric interception techniques were first used in the context of criminal investigation to outline "electronic identikits" of the alleged offenders, based on the "telematic fingerprints" which everyone scatters through the net while connected. Once a criminal activity has been identified, parameters are set which enable the probes to gather only investigation-related data flows. Today parametric interception is performed through specific appliances designed to

process data flows and behave in compliance with the set rules. It is possible to set a number of parameters which relate to specific criminal activities and monitor all electronic traffic falling within the given parameters. Peripheral agents detect events or trace atypical activities by performing a real-time analysis of a given subnet or connection.
A decision tree structure enables a real-time management of traffic. The application of such tools is not confined to basic network protection; indeed, it is possible to detect the content of specific data flows and thus trace the unauthorized transfer of sensitive information or the distribution of illegal material.

Conclusion

As technology develops and changes, we have to follow it at the same pace. National Agencies have to continually adapt their defence measures to the dynamic changes in the attacks they face. Corporations have to implement security measures that protect the users malicious attacks by cyber criminals, these attack techniques are almost as dynamic as the evolution of the technology they attack. To do so, both National Agencies and corporations have to invest time and money in security awareness and defence measures. The latter have to be resilient in so much that they have to withstand even the most brutal attack, but they must also be sufficiently flexible to be modified in time as the nature of the attacks morph and as the components of the network change and evolve.

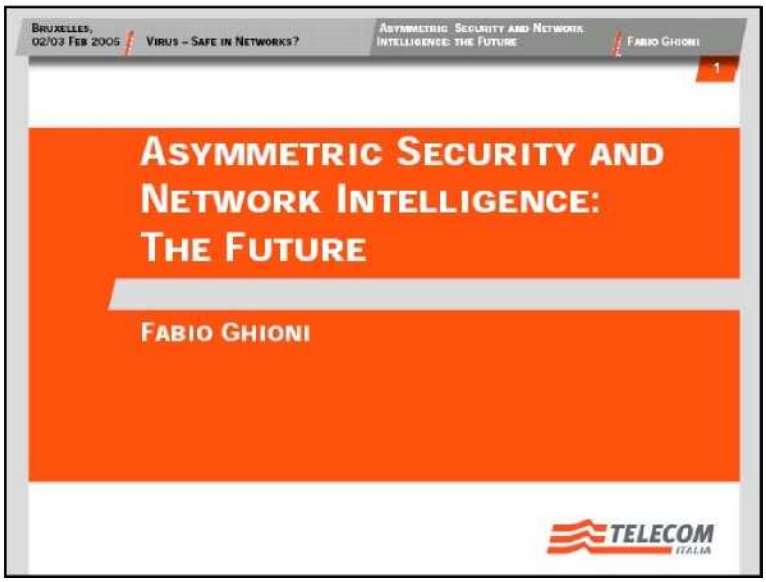
Bibliography

Schneier, B., Secrets & Lies: Digital Security in a Networked World, Wiley Computer Publishing, 2004
Nakra, P., Info-Terrorism in the Age of the Internet: Challenges and Initiatives, Journal of Competitive Intelligence and Management, v. 1 n. 2, pp. 1-10, Summer 2003

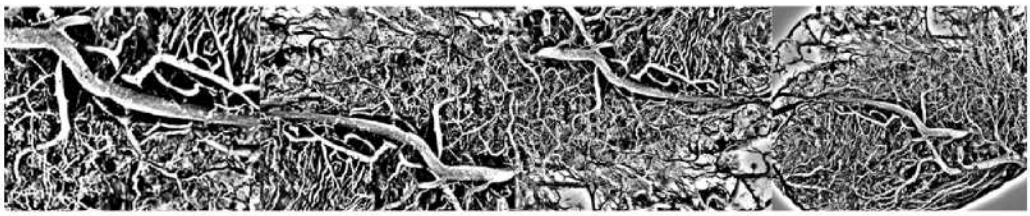
Curriculum Vitae

Fabio Ghioni is Security CTO in Telecom Italia Group, he is one of the major innovative and revolutionary professionals in the field of information security, competitive intelligence and the inventor of many of the new ways of managing national security in an asymmetric environment, interception and intrusion management. Consultant to several international institutions and governments, he has been crucial to the solution of many terrorism cases by supporting key institutions. Among others, he has serviced key leading international corporations in the military, telecommunications, banking and technology industries. He is personally leading research in major fields, ranging from mobile and wireless competitive security to the classification of information and forensics technologies applied to identity management and ambient intelligence as well as the application of ubiquitous network technologies in information security. He has a PhD in Clinical Psychology.

Präsentation

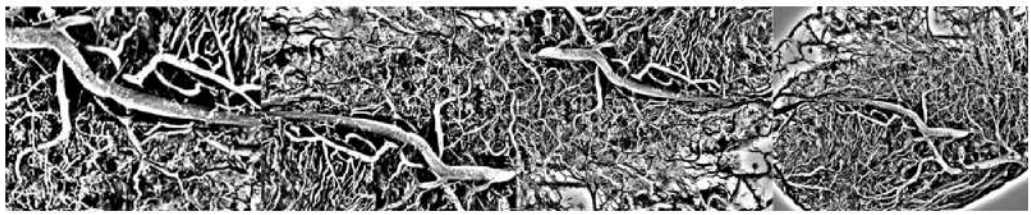


Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.



Sektion II

Reflektion über die Sicherheit im Netz aus philosophischer, ethischer und künstlerischer Sicht



System security and emergent processes in software systems

Prof. Peter Cornwell, Head of the Institute for Visual Media, Center for Art and Media, Karlsruhe

Curriculum Vitae

Peter Cornwell is director of the Institute for Visual Media, ZKM, Center for Art and Media Karlsruhe.
After education in art and computing science he worked in the computer industry in robotics, design automation and high performance graphics systems, heading European research for Texas Instruments and US virtual reality company Division.
Between 1995 and 2003 he managed research and taught computing at Imperial College, and media art at Central Saint Martins, London and more recently at the University of Applied Art, Vienna as well as at the Academy of Design Karlsruhe.

Does something like ethical hacking exist?

Jan Guldentops, Directeur BA Testlabs, Leuven

Abstract

White hat versus black hat - Is there such thing as ethical hacking?

To make errors is strictly human. No wonder there are security problems and other bugs in all software and network-infrastructure. So what do you do when you discover a potential, exploitable security-problem?

There are several approaches to the problem :

- First of all you can **be an ostrich** and put your head in the sand. You ignore the security-problem, keep quiet and hope nobody else will ever come across the same potential exploit.
- The second approach is to be a **whitehat hacker**: document the problem, see what you can do with it and how you can exploit it. After you have a clear overview of the problem, you contact the entity responsible for the infrastructure or the software and you warn them about your findings. Give the vendor/user enough time to fix it and then you make the problem public, so other people can learn from it and secure themselves against the problem.
- The last most dark approach is to become a **blackhat hacker:** you document the problem but keep the information to yourself. You exploit it for personal gain.

Which of these 3 approaches is the most ethical? Which approach helps society and the industry to best limit the damage caused by the human error? Which is the most academically sound ? Which is legal ?

Curriculum Vitae

Born in 1973, Master in Modern History, KU Leuven.

Jan Guldentops is a consultant and journalist fascinated by IT and network technology and the new academic and communicative opportunities it provides. His passion is combining technology and innovation with common sense into practical solutions that make a difference. His hobby is tinkering with the security of existing systems.

In 1993 he brought the first Belgian newspaper to the internet – the first of a long list of technology, internet and security-realisations. In 1996 he founded his own consultancy business named Better Access (now BA). He also documented his first big *security hack* exposing the lack of security of the Belgian internet banking service (Brabants Beroepskrediet). The following years he researched and documented several major security problems in technologies such as webservers, e-mailsystems and wireless networks.

He is a strong advocate of Linux and Open Source, because he believes it brings the openness of the academic world to a greedy business such as IT. A regular speaker on different technical security- and ITsubjects, he has published a book on the history of the internet and articles for magazines such as Datanews, SmartBusiness and Computing.

Präsentation

Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Bibliothek quo vadis? Sicher ins Netz

Christa Müller, Österreichische Nationalbibliothek, Wien

Der „Duden – Das große Wörterbuch der deutschen Sprache" gibt beim Wort „sicher" folgende zwei Hauptbedeutungen an:

1. ungefährdet, gefahrlos, von keiner Gefahr bedroht; geschützt;
2. ohne jeden Zweifel; gewiss [1]

In meinen Ausführungen möchte ich auf das Verhältnis dieser beiden Bedeutungen im Bezug auf Bibliotheken und die Digitalisierung ihrer Bestände bzw. die Verfügbarkeit im Netz eingehen.

1. Sicherheit vor dem Netz(zeitalter)

Als Ausgangspunkt der Überlegungen möchte ich die Österreichische Nationalbibliothek und ihr großes Digitalisierungsprojekt ANNO vorstellen. Es ist ja gemäß Bibliotheksordnung[2] die Aufgabe der Österreichischen Nationalbibliothek österreichische Publikationen

- zu sammeln
- zu bewahren und
- zugänglich zu machen.

Das schriftliche kulturelle Erbe – das in ihren Magazinen aufbewahrt wird – soll von möglichst vielen Menschen gelesen, und die darin enthaltenen Informationen rezipiert, interpretiert und produktiv für neue Texte verwendet werden können.

2. Sicherheit durch das Netz

Sicherheit ist schon in jeder traditionellen Bibliothek eine Herausforderung. Sie muss langfristig die Verfügbarkeit der Texte für die Leser sicherstellen. Die physische, die analoge Bibliothek strebt ein Gleichgewicht zwischen dem „Bewahren" und dem „Zugänglichmachen" an. Am besten gesichert sind die Bücher, wenn sie in den Magazinen verwahrt, klimakontrolliert gelagert und nicht ausgehoben werden. Bisher stand diesen idealen Archivierungsbedingungen der Wunsch nach Benützung der Bücher entgegen. Nun haben die Bibliotheken – mit Hilfe der Digitalisierung – die Möglichkeit ihr in der analogen Welt nur an einem Ort zugängliches Material weltweit 24 Stunden am Tag, sieben Tage die Woche – und dies ohne jegliche Gefährdung der Originale – dem Publikum zur Verfügung zu stellen. Selbst wenn der Forscher in der Bibliothek ist, sind viele Sammlungen für ihn nur eingeschränkt, unter bestimmten Bedingungen zugänglich. Oft kann pro Tag nur eine bestimmte Anzahl an Dokumenten vorgelegt werden. Nach der Digitalisierung können unikale und wertvolle Objekte außerhalb der Bibliothek auch von mehreren Forschern gleichzeitig studiert werden. Die Digitalisierung eröffnet außerdem neue Möglichkeiten für die inhaltliche Analyse von Material. Dank Texterkennung (OCR) können riesige Textmengen mit einer Suchanfrage zu einem Thema durchsucht werden.
Das online verfügbare Digitalisat erübrigt im besten Fall die Benützung des Originals, reduziert aber in jedem Fall die Anzahl der Dokumente, die manipuliert werden müssen. Fazit: Die Digitale Bibliothek hilft der analogen also, ihre Kernaufgaben zu optimieren. Bei

[1] Duden Das große Wörterbuch der deutschen Sprache in 10 Bänden. 3., völlig neu bearb. und erw. Aufl. Mannheim, Leipzig, Wien, Zürich: Dudenverlag 1999.
[2] Bibliotheksordnung vom 11. Januar 2002, BGBl. II, Nr. 12/2002

gleichzeitig verbesserter Zugänglichkeit kann auch die Langzeiterhaltung der physischen/ analogen/ gegenständlichen Originale verbessert werden.

3. Der virtuelle Lesesaal der Österreichischen Nationalbibliothek

Zentrum und Ziel der Digitalisierung ist der virtuelle Lesesaal. Nicht einige wenige, sehr wertvolle Objekte sollen unter großem Aufwand präsentiert werden, sondern eine Methode und ein Workflow werden gewählt, mit welchen es möglich ist, in überschaubarer Zeit eine kritische Masse online anzubieten. Dies geschieht in Hinblick auf den Benutzer, der nur dann – wenn ausreichend relevantes Material vorhanden ist – auch wirklich Nutzen hat und daher auch regelmäßig wieder kommt. Schritt für Schritt werden an der Österreichischen Nationalbibliothek verschiedene Textsorten digitalisiert: Zeitungen, Zeitschriften, Gesetzestexte, österreichische Erstausgaben,... Parallel dazu kommt es zu einer stufenweise Verbesserung des Nutzungskomforts: von der strukturierten Imageversion bis hin zur Durchsuchbarkeit von strukturiertem Text.
Auf der Prioritätenliste für das Digitalisieren stehen nur urheberrechtsfreie Texte. Den größten Bestand der Österreichischen Nationalbibliothek bilden historisch, kulturhistorisch, geistesgeschichtlich und politisch interessante Werke, also nicht aktuelle technische oder naturwissenschaftliche Texte mit einer „Halbwertszeit" von weniger als 5 Jahren. Der Inhalt dieser „historischen" Texte wird relevant und von Interesse bleiben.

4. ANNO – AustriaN Newspapers Online[3]

Seit Mai 2003 werden für das Projekt ANNO historische österreichische Zeitungen und Zeitschriften gescannt. Die Imagefiles werden in einer einfachen Struktur online gestellt. Derzeit werden pro Woche zwischen 20.000 und 100.000 Seiten gescannt und im Web verfügbar gemacht. Insgesamt sind schon mehr als 2,7 Millionen Seiten online. Der Zugang zu den gesamten Daten ist frei und kostenlos, die Benützer können einzelne Seiten in höchster Qualität als TIFF oder auch ganze Ausgaben als PDF herunterladen. Dieses Service – der erste Schritt zum umfassenden, virtuellen Lesesaal der Österreichischen Nationalbibliothek – wird mittlerweile täglich – d. h. Montag bis Sonntag – von mehr als 400 Lesern genutzt, wobei die Zahlen laufend steigen. Dieses muss sicher und verlässlich sein.

5. Das sichere Netz

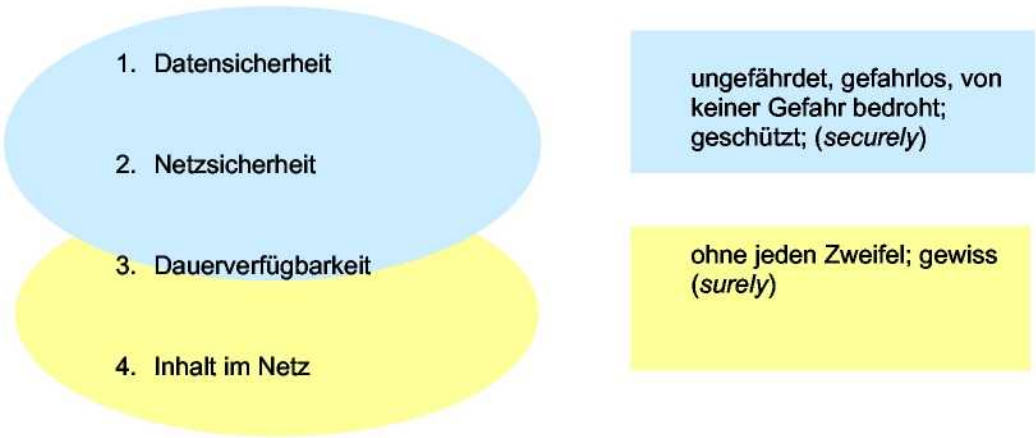
Welchen Zweck verfolgen nun die Sicherheitsvorkehrungen im Netz? Wer oder was soll vor wem oder was geschützt werden? Es werden die Server vor dem Zerstört werden z. B. durch Viren geschützt, sie werden vor den Zugriffen von Hackern abgesichert. Die Daten auf diesen Rechnern werden vor dem Gestohlen werden geschützt. Die Eigentümer wollen sich vor dem Verlust des alleinigen Rechts an diesen Daten schützen. Die illegale Nutzung ihrer Daten und daraus erzielte, unrechtmäßige Einnahmen sollen verhindert werden.Was ist die Konsequenz dieser Angst? Wie überall – es wird aufgerüstet! Proxy-Server werden vorgeschaltet, Firewalls werden aufgezogen, Virenscanner werden installiert,...
Der steigende Aufwand für Sicherheit, bewirkt – und dies muss zumindest diskutiert werden – auch steigende Einschränkungen durch diese „Sicherheit".

6. Sicher im Netz

Sicherheit bedeutet eben auch Verlässlichkeit, Zuverlässigkeit und Vertrauenswürdigkeit. Das Angebotene darf nicht manipuliert sein, nicht geleitet von unterschiedlichsten Interessen

[3] http://anno.onb.ac.at

selektiert werden. Es muss mit aller bibliothekarischen Sorgfalt und Verantwortlichkeit behandelt werden.



Die ersten drei Punkte, welche die erste Bedeutung des Worts sicher im Duden abdecken, dienen dazu, den vierten Punkt (die organisatorische und inhaltliche Sicherheit), oder die zweite Bedeutung des Wortes „sicher" zu ermöglichen.

a. Datensicherheit

1. Im Projekt ANNO werden die physischen Bände nach dem Scannen natürlich wieder ins Magazin gebracht. Aus den Fehleinschätzungen amerikanischer Mikroverfilmungsprojekte in den 50er und 60er Jahren, bei welchen nach dem Mikroverfilmen die Zeitungen systematisch aus den Magazinen entfernt wurden, haben wir gelernt. Dort wird jetzt – 50 Jahre später, obwohl der Mikrofilm eigentlich 400 Jahre hätte halten sollen, – neuerlich mit der Mikroverfilmung der Zeitungen begonnen, weil die Filme oft doch nicht mehr die heute benötigte Qualität haben. Nun aber mit dem großen Nachteil, dass bei manchen Zeitungstiteln nur mehr wenige physische Exemplare vorhanden sind.

2. Das Scanprojekt läuft hybrid ab, d. h. in einem Durchgang wird parallel mit dem Scan auch ein Mikrofilm erstellt.

3. Die Scans werden vom Scandienstleister auf CD-Rom (einem nicht wiederbeschreibbaren optischen Datenträger) ins Haus geliefert. Hier werden die Daten sofort – d. h. binnen zwei Arbeitstagen – auf einen Server gespielt. Dabei wird auch automatisch kontrolliert, ob die Dateien sich öffnen und kopieren lassen, ob die Dateien eine plausible Größe haben, ob die Struktur, in der sie geliefert wurden, passt, ...

4. Die gesamten Daten werden inklusive der Filestruktur und der Applikation wöchentlich auf Bänder gesichert. Diese werden im Tiefspeicher, fern dem Server aufbewahrt. Außerdem werden in periodischen Abständen Bänder in ein Hochsicherheitslager der Bundesregierung in einem Stollen in den Salzburger Bergen gebracht. Ob allerdings – wenn, wodurch auch immer (Erdbeben,...), alle Server in der Österreichischen Nationalbibliothek kaputt sind – das Wiederherstellen von ANNO wirklich möglich sein wird!? Etwa in Stollen gelagerte Bücher kann man in guten Zeiten wieder auf ihre Regale stellen, Magnetbänder sind zunächst einmal nicht unmittelbar lesbar.

b. Netzsicherheit

Zur Netzsicherheit tragen Firewalls, Zugriffsbeschränkungen und Securityupdates bei. Manchmal kann aber auch der Virenjäger, wenn z. B. des nächtens automatische Updates laufen, Systemausfälle heraufbeschwören „Sicher im Netz" bedeutet nicht nur Daten- und Netzwerksicherheit sondern auch die Strategie, mit der Dauerverfügbarkeit gewährleistet werden soll.

c. Dauerverfügbarkeit

Zu Beginn des Projektes ANNO hätte es schon ein fertiges Produkt für gescannte Zeitungen gegeben. In diesem wären allerdings die Daten in einem proprietären Format in einer uns nicht zugänglichen Struktur gespeichert worden. Neben Kostengründen waren es vor allem aber schwerwiegende Sicherheitsbedenken, warum wir uns gegen diese – für uns einfachere Möglichkeit – entschieden haben. Die Österreichische Nationalbibliothek wurde 1368 gegründet und hat den gesetzlichen Auftrag das schriftliche österreichische kulturelle Erbe zu sichern, zu bewahren und zugänglich zu machen. Entscheidungen werden daher mit einem Blick auf die langfristige Haltbarkeit und Verfügbarkeit getroffen. Sicherheit beginnt nicht erst in dem Moment, wenn die Daten im Netz sind und vor Viren-Attacken und Datenentwendung geschützt werden müssen. Für das Projekt ANNO begann Datensicherheit bei der Entscheidung für das Format der Daten, mit der Entwicklung einer eigenen Applikation, der Verwendung vorgefertigter Module und auch gekaufter Software, wobei aber jede Komponente ersetzt werden kann. Die Daten sind „frei" online. Der Benutzer muss sich nicht anmelden, die Nutzung ist kostenlos.
Wir sehen Dauerverfügbarkeit im Bereich des Digitalen vorrangig als eine Strategie, die den ganzen Projektaufbau und alle Projektkomponenten betrifft, und nicht ausschließlich als technische Lösung, die sehr spät im Projekt – erst beim Onlinestellen – ansetzt.

d. Inhalt im Netz

Text wird gesichert, indem er gelesen wird. Die Herausforderung für Bibliotheken ist nicht, dass Muster von Bits und Bytes nicht „gestohlen" werden, sondern dass das schriftliche Kulturgut im Netz ist, gelesen werden kann und dadurch lebendig bleibt. Texte werden von Schülern bearbeitet, von Studenten interpretiert, von Forschern analysiert und von der interessierten Öffentlichkeit gelesen. Anspruch des virtuellen Lesesaals der Österreichischen Nationalbibliothek ist es nicht, eine Reproduktion des Originals zu schaffen, sondern das textliche kulturelle Erbe mit der ganzen Sorgfalt und Erfahrung, dem ganzen Wissen und Können der Bibliothek, ins Netz zu bringen und es damit zu erleichtern, dass diese Texte auch im Bewusstsein der Menschen bleiben.

e. Der Weg ins Netz

Zusammenfassend lässt sich sagen, dass derzeit ein doppeltes Mühen der „Digitalen Bibliothek" auf dem Weg „Sicher ins Netz" – „Sicher im Netz" notwendig ist:

- für freien und reichlichen Zustrom des Contents ins Netz und
- für freien und ungehinderten Zugang zum Content im Netz

Eines ist aber gewiss! Die Zukunft der Bibliotheken wird „sicher im Netz" sein!

Curriculum Vitae

Christa Müller, geb. 1970 in Wien, studierte Geschichte, Deutschen Philologie und Kunstgeschichte an der Universität Wien. Während und nach dem Studium Teilnahme an Universitätsprojekten, die den Einsatz von EDV für die Geschichtsforschung erprobten. Seit 1996 an der Österreichischen Nationalbibliothek. 1998 Bibliothekspraktika in den USA. 1999 Absolvierung der Grundausbildung für den Bibliotheks-, Informations- und Dokumentationsdienst. Seit Ende 2002 für die Stabstelle Digitalisierung an der Österreichischen Nationalbibliothek verantwortlich. ANNO - AustriaN Newspapers Online ist das erste Massen(objekt)digitalisierungsprojekt, das umgesetzt wurde.

Präsentation

Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Sektion III

Technische Aspekte der Netzwerksicherheit

In a Magic triangle: IT-Security in a Research Centre

Dr. Thomas Eickermann, Head of the department communication systems, Central Institute for Applied Mathematics, Research Centre Jülich

Abstract

Not least because of the increasing thread by viruses and other malware, IT-security related issues are gaining public attention. At the same time the required technical and organisational effort of all users of information and communication technology to protect their computers and networks is increasing. The necessary measures and the related limitations imposed on communication conflict with the need for open high-performance networks. This is especially an issue for universities and public research institutions for which open communication is part of their culture and for which technologies like grid-computing open up completely new ways of worldwide cooperation, as subsumed under the term e-Science. This contribution discusses IT-security in this area of tension.

Introduction

Protecting its valuable IT-resources has always been an important task for any organisation that uses and relies on information technology. However, the threads and therefore also the focus of the measures against those threads have dramatically changed within the last decade(s). While the classic risks of physical damage (fire, water, etc.), theft, or loss of availability due to malfunction are still present, new threads emerging from viruses, worms, crackers, and script kids, or even more seriously by (industrial) espionage or sabotage to name but a few have gained ground, mainly enabled and supported by the ubiquitous internet. On the other hand, the increasing capacity and capabilities of the internet open up opportunities for communication and cooperation that go far beyond today's WWW. This is especially the case for research and educational institutions that just begin to explore the possibilities of the rapidly evolving Grid technologies to 'enhance science', subsumed under the term e-Science.

This generally leads to a set of conflicting goals, here called a magic triangle: the measures to enforce IT-security puts constraints on communication and the usage of IT-systems which conflict with the need for openness and ease of use. A third important goal is to limit costs of IT-security, which are generated not only by hardware and personal required to maintain a secure as well as open environment but also by impacting the productivity of all users. The rest of this contribution discusses this magic triangle and its edges security, openness and costs under the special viewpoint of a research institution. Although IT-security has many facets including organisational, juristic and ethical ones, the paper focuses on technical aspects. As a specific example, security issues related to Grids are discussed in more detail.

Security – things that need protection

As in every company, the administration of a research centre heavily relies on IT. The involved systems and services must fulfil availability constraints and confidentiality and

integrity of critical data like personnel data, financial and strategic information must be protected. Besides that, IT is at the core of the research centre's or university's business:

- Experiments are typically controlled by computers. A flaw in such a system may disrupt experiments, damage experimental devices or even harm humans (e.g. in medical research) or the environment.
- Experimental data are processed and stored on computer systems. Loss or corruption of that data can destroy the results of extensive scientific work. Data stolen or compromised prior to publication can have negative effects on the scientific reputation or cause financial loss in case of patents pending.
- The same holds for computer simulations, especially when performed on high-performance-computers: such supercomputers are scarce large-scale scientific devices and disruption of their operation or loss of data produced or stored on them wastes valuable resources.
- Universities and research centres often have powerful internet access and operate a large number of high-performance computers – often in combination with a relatively open security policy. This makes them attractive targets for crackers, who abuse those resources for further attacks against others or to host illegal content.

A common statement from users and system administrators in public research institutions is 'there is nothing secret on my computers, so there is no need to protect them'. While the first part of that statement may be true for some systems, the conclusion certainly is not, since every breached system is obviously a vantage point for attacks to the more critical systems in the same or a related organisation.

Freedom and functionality – things that need to be open

It is within the very nature of research that the internal and external communication has rapidly varying communication patterns and partners:

- Scientific institutes or individual scientists undergo partnerships and cooperations with other organisations or individuals all over the world. In the course of such cooperations, which may be limited to a single joint project or last over many years, they exchange not only ideas but also documents, programs and mutually grant access to each others resources. For example, multi-national cooperation on large-scale experiments is quite common. In that context, a foreign institute may own and control parts of the experiment and require privileged or even administrative access to the computer that controls that experiment or require fairly open communication channels between the cooperating institutes. While the communication itself can be protected by encryption, this inevitably creates networks of trust. A security breach in one institution may seriously impact the other, too.
- Visiting scientists usually bring their own laptops with them. Often, they need full access to the resources of the visited institute and thus cannot easily be isolated in quasi-external untrusted networks. Nevertheless, they also need to access their home institution e.g. for reading email. The other way round, employees attach laptops to the internal network that have operated in a possibly hostile environment (conferences, partner sites, at home) or connect to the network from such remote locations.
- The communication is not limited to the use of common protocols and applications like email, WWW, or secure shell. Self-developed applications often use different protocols that are not understood by common firewalls and are thus hard to integrate into a strict security policy.

In general, these examples show that, in contrast to typical commercial environments, the communication patterns and partners are not well defined in most research centres and universities. This is complemented by the fact that the individual institutes need certain

autonomy in planning their IT-projects. This limits the options to enforce a strict security policy by technical means like firewalls or other devices to restrict, separate, and monitor data communication.

Costs – what can be done and at what expense?

The most simple, reliable, and cost-effective security policy obviously is a complete separation of the internal IT-infrastructure from the outside world and from a part of the network that is allowed to communicate with the outside world (for Email, Web, etc.). For most organisations this will not be possible, and is obviously not an option for a research centre or university. Every other policy (except for providing no protection at all, which is obviously also not an option) will increase costs, technical and administrative complexity and put more responsibility and workload on the users and system administrators. Large parts of the IT-infrastructure can be managed centrally and thus cost-efficiently. A typical policy will include the following building blocks:

- The local network and its main entrances (internet, dial-in) are protected via firewalls, email-virus scanners and other central technical measures. The traffic is monitored to detect and possibly cut off attacks from outside.
- Standardised PCs in the administration as well as scientific workstations are equipped with personal firewalls and virus-scanners. Installation, management and necessary software updates are tested and deployed centrally. Systems-logs of critical systems are collected centrally and automatically correlated and scanned for suspicious events.
- With a state-of-the-art network design, critical parts of the infrastructure (like personnel data management) can be logically isolated from the rest of the network in virtual networks where they are safe, as long as the network components themselves are not compromised. Nuclear reactors or other expensive and potentially hazardous experiments will therefore operate in a physically separate network.

However, compared to commercial environments, there will be many systems that have to be configured and operated individually because they run special applications or contain unusual hardware components to control experiments, leaving the responsibility for their security with the 'local' system administrator. This makes training of the staff exceedingly important. Network based vulnerability tests of all IT-systems on a regular basis are a necessary and also tedious task, since thousands of individually managed systems have to be tested instead of a handful of representative computers.

Grids and e-Science – a partial solution?

A new quality of scientific cooperation is envisioned to be enabled by the upcoming Grid-technology (Foster & Kesselman, 1998). By definition, grids shall provide pervasive, secure, and seamless access to distributed computing resources across multiple administrative domains. This means that they provide the protocols and tools to form so-called 'virtual organisations' which share resources like computers, networks, data, experimental facilities and software in a seamless yet secure manner. The development of Grids is currently mainly driven by a few important scientific communities like high energy physics (which also invented the Web), climate research and scientific computing in general. The vision is to change the way IT-resources are shared as fundamentally as the Web changed the way to share data and thus lead to a new 'enhanced science' or e-Science. Security has been considered in the design of grid-software like Unicore (Erwin 2002) or Globus (www.globus.org) from the very beginning, and many problems are solved in their

architecture: Users and providers of a service mutually authenticate (verify their identity) by reliable technical procedures based on digital certificates. All communication is encrypted by default using 'strong' reliable methods.

- It will become easier to implement a fine-grained regulation of rights of remote partners in accessing the local resources e.g. by defining roles and by allowing access only via well-defined protocols and interfaces (services). However, it is unlikely that this will be a complete substitute for the 'privileged access' in very close collaborations as mentioned above.

However, there is quite a way to go before those solutions become a reality. There are practical problems that lie within deficiencies of current implementations. E.g. Grids based on Globus, the most widely deployed Grid-software today, do not work well with firewalls. Other functionalities like the fine-grained role-based access control are simply not implemented yet or cannot be used in real applications due to performance problems of the software. While these practical problems should be solved within a relatively short time-frame, there are some intrinsic security problems with Grids also:

- Virtualisation is a key-word for Grids. Here it means that a user does not have to know where a service that he uses is provided. In order to fully exploit this, there is a need for automated services to act on behalf of users, e.g. as agents or brokers that search for a wanted resource (database, library, computer ...) and negotiate contracts between providers and users. This means that a user has to trust such third parties and delegate some of his rights to it.
- Grid technology will make it a lot easier to offer services to a large, potentially anonymous group of users, based e.g. on the membership in a special community (virtual organisation) or on fees. Such services often require mutual trust of provider and consumer: a computer centre offering access to its computer cannot fully protect this computer against abuse by the user. On the other hand the user of such a service cannot fully protect his data that is processed on the remote computer from abuse by the owner of that computer.

In general, Grids will improve the security of access to and usage of remote services but on the other hand will open new fields of security problems that are not fully foreseen today. Therefore, one focus of D-Grid (www.d-grid.de), the German e-Science initiative launched in October 2004, is on security issues. Among the topics to be investigated here are the application-driven re-configuration of firewalls to allow high-performance communication between partners in a Grid on an as-needed basis, the definition of formal languages and procedures for contract negotiation, the creation of a public key infrastructure (for digital certificates) and many more.

Summary

While research centres and universities certainly share many IT-security related issues with companies or civil services, other issues are quite specific: a usually very heterogeneous hard- and software environment and a tendency to communicate a lot with varying external partners. In combination with the level of autonomy of the institutes within the centre and limited budgets this makes it difficult to maintain a level of IT-security that is equal to those achievable in other environments. There is some hope that emerging technologies like Grid computing will improve the situation.

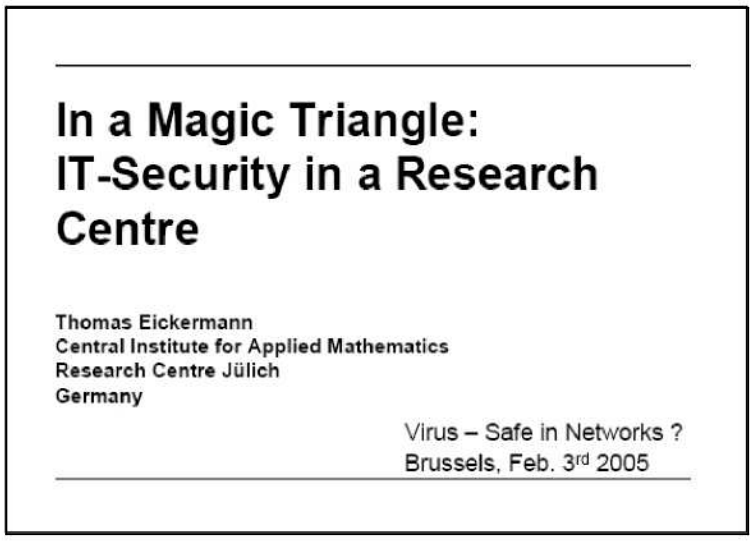
References

Erwin, D. (2002): UNICORE – a Grid computing environment. Concurrency Computation: Practice and Experience. 14 1395-1410.
Foster, I., Kesselman, C. (1998): The Grid – blueprint for a new computing infrastructure. Morgan Kaufmann Publishers.

Curriculum Vitae

Born 29.8.1964 in Düsseldorf.
1983-89 study of Physics at the Heinrich- Heine-University Düsseldorf, 1994 PhD with a thesis in theoretical Plasma Physics.
Since 1994 scientist at the Central Institute for Applied Mathematics at the Research Centre Jülich.
Areas of work: system administration, distributed supercomputing, networking.
Since 2002 head of the department communication systems, currently also IT-security officer of the Research Centre.

Präsentation



Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Secure Solutions for Public Networks and Workstations

Urpo Nylander, IT-Designer of Helsinki City Library Kirjakaapeli

Abstract

Customer Workstations

Commercial Solutions

A glance at today's commercial solutions how to secure customer workstations. Many companies offer today tailored data security solutions to very different needs. Especially different "terminal server" solutions have lately arisen. As an idea "Terminal server" is already old and well-found. Today's "terminal server" solutions have journeyd a long way from character- based world to today's graphical interfaces. As an example of a commercial solution is Helsinki City Library's Citrix based administrative concept for customer workstations.

Open Source Solutions

The possible Open Source application of customer workstations. Secure solutions do not need to be closed in order to be secure. In open source solutions data security is transparent, anyone who can read the code can check what certain application really does. The Open Source model suits public services especially well. It brings communal feeling to information technology and enables citizens' participation in services meant for them in an entirely new way. As an example of Open Source solution is Linux LTSP customer workstation concept at the Cable Book Library.

Do-it-yourself solutions

Practical tips on securing patron workstations at small libraries. How a small library in the remotest corner of Lapland can take care of their customers's data security as there is no ADP Unit in the municipality and the municipality is not yet ready for Open Source solution? Interface producers can provide you with the entire toolbox for interface securing and even free of charge. There is a lot of literature on the subject and more tips can be found on the Internet. You can tune a Windows computer to match almost C2 safety classification, even so that it will also function. As an example of a do-it-yourself solution are publishing workstations at the Cable Book Library.

Customer Networks and Laptops

The library as a provider of network connection: Experiences and noteworthy items regarding wired and wireless networks. The Lasipalatsi Media Centre has provided wired and wireless network connection to its customers already since 1998. Allowing customers with their own computers to the library's network may sound inviting troubles. Practice, however, has proved otherwise. However, there are certain things that should be taken into consideration when planning an open customer network. As examples of open customer networks are the Lasipalatsi customer network and the wlan concept developed by Helsinki City Library and City of Helsinki's Education Department.

Curriculum Vitae

Born 08/11/1973 Pulkkila, Finland
Secondary school graduate 1994
Started working in Helsinki City Library 1996

- Librarian, Pukinmäki Library & Mediatheque, 1996-1998
- Special Librarian, Cable Book Library, 1998-2001
- ICT Officer, Cable Book Library & iGS – information Gas Station, 2001-2004
- ICT Consultant, Cable Book Library, iGS & Library 10, 2004

Präsentation

Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Les PME et la sécurité ICT - «Vers une approche intégrale?»

Jan-Frans Lemmens, Publisher of „Best of Publishing", Brussels

Abstract

A lot of time – and money – is spent to fix security problems in software applications, network infrastructures, organisations... While holes are being fixed new security problems occur. Still the root causes of those problems are often conceptual mistakes or simply lack of awareness from IT administrators and end users. Does it need to be that way? Does it have to be broken before it gets fixed?

Introduction

Les technologies de l'information et de la communication (ICT) occupent une place sans cesse plus importante dans la stratégie des sociétés belges, quelle que soit la taille des entreprises ou la nature de leurs activités. Le rôle central de l'information numérique et des réseaux de communication dans les résultats des entreprises place le monde économique face à un défi énorme: la sécurité des systèmes et des données. Il va de soi que lorsque l'ICT intervient directement dans l'activité de l'entreprise, une indisponibilité temporaire ou une perte de données peut occasionner un sérieux préjudice à l'entreprise. Par ailleurs, cela s'applique également aux entreprises qui ne recourent que dans une moindre mesure à l'ICT. Un exemple simple: imaginez ce qui se passerait si vous deviez vous passer du téléphone ou de l'e-mail pendant toute une journée de travail...La sécurité ne se limite plus depuis longtemps à d'innocents virus écrits par des étudiants en informatique trop zélés, à d'ennuyeux courriers indésirables, à des spyware envahissants et autres nuisances: c'est avant tout une question de fiabilité de fonctionnement et de risques financiers, exprimés en monnaie sonnante et trébuchante... «Vers une approche intégrale?»

1. Les PME et la sécurité ICT

Bon nombre d'entreprises ont compris l'importance cruciale d'une protection efficace de l'environnement ICT. Ce n'est pas un hasard si différentes études nationales et internationales (dont une, en Belgique, réalisée fin 2004 par le bureau d'études InSites) démontrent que la sécurité informatique et des communications figure clairement tout en haut de la liste des dépenses ICT des entreprises pour 2005. Une conclusion qui ressort aussi de notre propre enquête, organisée auprès des lecteurs de PC World Belgium, en collaboration avec Computer Associates. Plus de 54% des personnes interrogées désignent la sécurité comme leur toute première priorité ICT (voir plus loin). Pourtant, il reste encore beaucoup de pain sur la planche.
Une autre étude récente (fin 2004) du CLUSIB, le Club de la Sécurité Informatique Belge, indique que la sécurité laisse encore à désirer dans de nombreuses entreprises. Plusieurs chiffres frappants ressortent de ce rapport:

- Seules 25% des entreprises belges disposent d'un budget spécifique pour la sécurité informatique.
- Une société belge sur trois n'a pas de responsable précis pour la sécurité IT.
- 40% des entreprises belges n'ont aucune règle concernant l'utilisation de l'Internet.

Dans ce White Paper, les auteurs abordent l'impact économique d'atteintes à la sécurité sur l'infrastructure IT et les données numériques au sens large. Dans ce cadre, ils ne se focalisent pas sur la technologie même, mais sur les aspects économiques pour les entreprises, en donnant un aperçu des différentes menaces et de la manière dont elles peuvent être neutralisées.

2. Le coût des atteintes à la sécurité

Combien une atteinte à la sécurité ICT coûte-t-elle à une entreprise? Poser la question est plus facile qu'y répondre. D'abord parce que le coût d'une atteinte à la sécurité est plutôt économique qu'un coût financier directement tangible. Prenons par exemple le problème du spam (emails commerciaux non souhaités). Avez-vous déjà calculé combien de temps vos collaborateurs perdent en moyenne par jour à "nettoyer" leur boîte de réception d'e-mails? Pour une entreprise qui n'est pas suffisamment protégée contre le courrier indésirable et qui compte plusieurs dizaines de collaborateurs, le coût peut rapidement grimper à de nombreux milliers d'euros en perte de productivité. Les chiffres qui suivent démontrent d'ailleurs que le spam est un réel problème. Le bureau d'études Osterman a calculé que la taille moyenne d'un e-mail a augmenté de 40% en un an, principalement en raison de l'utilisation accrue des pièces jointes (68%) et du spam (43%). Dans notre pays, comme l'écrivait le Tijd fin 2004, pas moins de 53% de tous les e-mails entrants relèvent du spam et, parmi ces messages indésirables, 1 sur 11 comporte un virus. Les virus sont toujours l'un des risques les plus connus contre la sécurité. Il existe une littérature très abondante sur le coût d'une attaque virale. Une étude du britannique "The Corporate IT Forum" a chiffré le coût moyen d'une attaque par des virus et des vers pour les entreprises anglaises à 122.000 livres (environ 170.000 euros...). Le forum a découvert que, par attaque virale, en moyenne 365 heures de travail de collaborateurs IT étaient nécessaires pour réparer les dégâts... Naturellement, ces différents éléments dépendent de la taille de l'entreprise, du nombre de systèmes infectés et de la gravité de l'attaque. En outre, l'étude a également été menée auprès de très grandes entreprises.

Le coût précis d'une attaque peut être calculé en reprenant plusieurs paramètres: - Impact immédiat suite à la perte éventuelle de données

- Le temps pendant lequel les collaborateurs dont les ordinateurs sont infectés ne sont pas productifs (nombre d'heures x salaire horaire moyen x nombre de collaborateurs)
- Le temps que votre département IT (ou votre partenaire externe) passe à réparer les dégâts subis (nombre d'heures x coût horaire moyen)
- Les dégâts périphériques éventuels, comme le préjudice pour votre image de marque (surtout quand vous recourez de manière intensive à l'ICT dans vos relations avec la clientèle...), le manque à gagner (par exemple, parce que vous êtes inaccessible pour vos clients), etc.

Une enquête réalisée par PC World Belgium (voir plus loin) révèle que rien que sur le plan de la perte des données, 13,5% des répondants indiquent que cette perte de données leur a coûté entre 5.000 et 25.000 euros. 63,5% rapportent pour un cas de perte de données un coût de moins de 5.000 euros, et 2% parlent de plus de 25.000 euros. Singulièrement, un cinquième des participants n'indiquent pas ce coût. Pour les attaques de virus, cette proportion atteint près d'un quart. Nous pouvons en conclure que bon nombre d'entreprises ne connaissent pas

le coût d'atteintes à la sécurité et on peut en outre se demander dans quelle mesure le coût estimé correspond effectivement au coût réel… Vous trouverez plus loin d'autres résultats de cette enquête et l'impact d'autres atteintes à la sécurité.

3. Les principaux risques pour la sécurité

3.1 Inventaire: sachez ce dont vous disposez

Tout environnement informatique est en évolution permanente. Vous achetez de nouveaux ordinateurs de bureau ou portables, vous mettez en service un nouveau serveur, installez de nouveaux logiciels ou décidez de mettre à jour des versions existantes. L'ancien matériel et les versions précédentes sont mises hors service, ou non. Les collaborateurs sont satisfaits de la station de travail que vous leur proposez, ou ils installent simplement eux-mêmes toutes sortes de logiciels supplémentaires. Vous achetez et enregistrez systématiquement des versions officielles de logiciels, c'est en tout cas ce que vous pensiez. Tous vos systèmes disposent toujours des mises à jour les plus récentes – ou le devraient, tout au moins. Même si vous gérez vous-même votre infrastructure IT au quotidien, il n'est pas simple de tenir à jour de quels ordinateurs avec quels logiciels (et quelles versions) vous disposez exactement, quand une copie de secours a été réalisée, sur quoi elle porte, où elle est conservée.
L'évaluation des risques pour la sécurité commence dès lors toujours par un inventaire approfondi. Un tour d'horizon annuel ou semestriel constitue un bon début, mais en fait, vous devriez connaître à tout moment la situation précise. La meilleure approche consiste dans une gestion permanente à l'aide d'utilitaires de type "Asset Management". Un inventaire permanent doit empêcher que des utilisateurs finaux n'installent eux-mêmes toutes sortes de logiciels entraînant une perte de productivité et des risques pour la sécurité – par exemple un programme de chat MSN, un programme d'échange Kazaa, des jeux de tous genres... Exemple de bonne pratique: seul l'administrateur peut installer des logiciels sur les stations de travail de l'entreprise. La perte de temps ne peut être une entrave, grâce à toutes sortes d'outils pour la distribution automatique de logiciels et la gestion de correctifs. Ainsi, vous évitez simultanément que des utilisateurs finaux zélés n'installent eux-mêmes des mises à jour – ce qui est souvent souhaitable mais entraîne parfois des conflits avec une application déjà installée. Enfin, de plus en plus de sociétés de logiciels incitent via des groupes de défense d'intérêts comme la Business Software Alliance (BSA) à un respect strict de leurs licences logicielles. Une bonne politique de licences commence évidemment par un inventaire correct.

3.2. Menaces techniques

La principale menace pour vos données critiques d'entreprise ne provient généralement pas d'étrangers malveillants, mais de vos systèmes IT eux-mêmes. Même quand vous optez pour du matériel de marque et des logiciels réputés, vous devez partir du principe qu'un système informatique peut tomber en panne à tout moment. Une simple panne de courant peut provisoirement rendre indisponible l'ensemble de l'activité de l'entreprise. En recourant à des méthodes et des procédures adaptées, vous devez veiller à ce que l'impact d'une telle panne reste limité. Vous pouvez prévoir un système de secours, de manière à être rapidement de nouveau opérationnel en cas de panne. Plus important encore, vous devez prévoir une copie de secours de toutes les données importantes, y compris une procédure pour les conserver et les restaurer. En fonction de la valeur objective des données, vous avez aussi intérêt à prévoir des procédures pour pallier les coups du sort les plus durs. Si vous conservez par exemple la copie de réserve de vos données tout près des systèmes informatiques, un grave incendie peut

s'avérer fatal. Les grandes entreprises financières sont même obligées de tenir compte de catastrophes graves, comme un attentat à la bombe, un crash aérien, etc. – et elles conservent par conséquent leurs données à plusieurs endroits, à une distance mutuelle minimale d'environ 30 km. Tenez également compte du fait que la popularité du PC – et tout particulièrement de l'ordinateur portable au cours de ces deux dernières années – fait en sorte que des données critiques d'entreprise sont souvent stockées uniquement sur un ordinateur individuel. Même si les utilisateurs peuvent graver à intervalles réguliers les principales données sur un CD ou DVD, une telle approche ne fait généralement pas l'objet de procédures strictes. Suite à une panne matérielle (disque dur défectueux), ou par exemple un vol, ces données peuvent être corrompues, détruites, voire tomber dans de mauvaises mains au moment le plus inattendu.
Une attention toute particulière doit être accordée à l'utilisation croissante d'ordinateurs de poche (PDA, ou Personal Digital Assistant) ou à la dernière génération des téléphones mobiles. Outre la communication, ils servent de plus en plus souvent à introduire, consulter ou traiter des données. Souvent, aucune copie de sécurité de ces données n'est faite. Il arrive évidemment très souvent que ce genre d'appareil tombe dans de mauvaises mains.

3.3. Menaces externes: qui et pourquoi? Experts informatiques, chasseurs de primes et autres en mal de reconnaissance

Le terme "hacker" renvoie initialement à la dextérité et la passion – quelqu'un d'étonnamment habile pour mettre à profit des failles de sécurité. Ce terme n'a pas nécessairement une connotation négative. Certains pirates considèrent leur activité comme un art noble, qui leur permet de montrer leurs connaissances techniques et de les transmettre à d'autres. Néanmoins, tout le monde sait qu'une partie de la communauté des pirates informatiques est animée d'intentions moins innocentes. Dans certains cas, on peut parler de cybercrime organisé, de sabotage et d'intrusion sur commande, commise bien souvent par des experts informatiques hautement qualifiés de l'étranger. A l'aide d'"exploits" – de petits programmes permettant au piratage de se dérouler de manière entièrement automatisée –, des "artistes" moins doués peuvent eux aussi attaquer vos systèmes. On parle alors de "Script kiddies", en renvoyant à des jeunes gens qui s'en prennent de préférence à des sites Web trop nets à leur goût. Les exploits sont également utilisés par des pirates chevronnés afin d'avoir un impact énorme en peu de temps. Les auteurs de virus forment une catégorie à part. Ils cherchent tout particulièrement des endroits vulnérables dans des programmes et des systèmes d'exploitation courants. Parfois, les auteurs de virus se contentent d'intégrer des "exploits" existants dans un virus ver. Ils conçoivent un logiciel qui est activé imperceptiblement quand vous l'ouvrez dans une application déterminée (virus), ou simplement lors de sa lecture (ver), et celui-ci tente de contaminer le plus grand nombre possible d'autres ordinateurs. Eventuellement, un ver ou un virus peut aussi avoir un effet nuisible sur le système même: cela peut aller d'un affichage innocent à l'écran (comme le jeu Tetris, par exemple) jusqu'à la destruction de toutes les données du disque dur. Fort heureusement, de nombreux auteurs de virus se contentent essentiellement d'explorer de nouvelles techniques et des concepts inédits de contamination. Particularité des virus et autres nuisances apparentées: le logiciel malveillant vise à se propager le plus possible. Cela signifie qu'il va mener sa propre vie, l'auteur n'ayant par la suite plus aucun contrôle sur son virus, comme en témoignent la propagation énorme du virus Anna Kournikova qui se voulait "une blague" initialement, l'Allemand "qui n'était pas mal intentionné" derrière le virus Sasser ou, plus récemment encore, le Britannique de 16 ans arrêté pour le ver Randex. La dernière génération de virus semble toutefois viser de plus en plus la diffusion d'autres logiciels malveillants, souvent axés sur la fraude et l'arnaque.La dernière génération de virus semble toutefois viser de plus en plus la diffusion d'autres **logiciels malveillants** Logiciels malveillants (Nuisibles).

3.4. Menaces internes: pas de confiance aveugle dans ses collaborateurs

Personne n'est infaillible. Et vos collaborateurs non plus. Vous avez tout intérêt à les protéger contre leurs propres faux pas. Qui plus est, quand on parle effectivement de vol de données d'entreprise, il n'est pas rare que l'un de ses propres collaborateurs en soit responsable.
Des collaborateurs mécontents, en particulier des collaborateurs IT, sont souvent les auteurs de destruction délibérée de données d'entreprise. Par conséquent, il est inutile d'investir lourdement dans la protection de vos systèmes IT depuis l'extérieur, s'il n'existe aucun contrôle sur le réseau interne. Une première méthode importante consiste dans l'utilisation généralisée de noms d'utilisateur et de mots de passe pour toutes les applications. Cette mesure offre une protection de base acceptable, mais surtout un moyen pour détecter après coup le responsable. Cela requiert toutefois également un "**logging**" suffisant, à savoir la consignation de toutes les actions dans un journal numérique. Evidemment, il est crucial que vos collaborateurs utilisent leurs informations de mot de passe de manière adaptée. Trop souvent, on constate que les mots de passe sont trop courts ou trop simples, qu'ils sont communiqués à des collègues, voire notés sur un bout de papier à côté de l'ordinateur. «La **motivation** des auteurs de malwares: fraude, cybercrime organisé, exploitation de réseaux zombies, vol, sabotage et cyberarnaque» (viruslist.com)

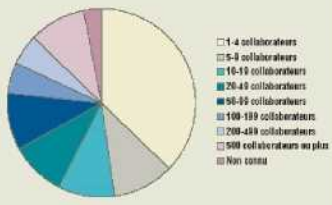
4. Enquête PC World Belgium: quelles menaces craignent le plus les PME belges?

4.1. Méthodologie

Sur base d'une enquête en ligne, proposée via la newsletter PC World, plusieurs centaines d'informaticiens et de chefs d'entreprises du monde des PME ont été interrogés. La rédaction a enregistré par la suite environ 120 réactions. Après élimination des réactions anonymes, des doublons et des réactions manifestement fallacieuses, nous avons conservé une centaine de réponses valables. Notons encore que la plupart des lecteurs de PC World Belgium recourent de manière intensive à l'ICT et que cette enquête propose un instantané des expériences des lecteurs plutôt qu'une analyse scientifique de "la PME". Néanmoins, l'enquête nous apprend énormément sur l'impact des atteintes à la sécurité dans les entreprises belges. Vous trouverez ci-dessous les résultats de l'enquête en ligne. Avec le nombre de répondants validés actuels, le minimum requis pour un échantillon représentatif n'est pas atteint. Néanmoins, il s'agit à notre connaissance de l'une des enquêtes les plus complètes de ce groupe-cible à ce jour. La répartition sur le plan de la taille est ainsi étonnamment représentative de l'économie belge.

Répartition des répondants en fonction de la taille de l'entreprise

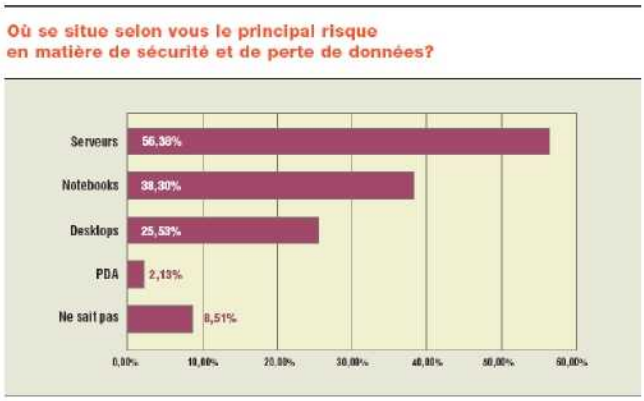
1-4 collaborateurs	37,23%
5-9 collaborateurs	10,64%
10-19 collaborateurs	9,57%
20-49 collaborateurs	9,57%
50-99 collaborateurs	9,57%
100-199 collaborateurs	5,32%
200-499 collaborateurs	5,32%
500 collaborateurs ou plus	9,57%
Non connu	3,19%



Le véritable groupe-cible de l'enquête consistait dans les PME belges (jusqu'à 49 collaborateurs), et elle représentent les deux tiers des répondants effectifs (67,01%). Ceux qui appliquent la description américaine du concept de PME (moins de 500 collaborateurs), retrouvent près de 90 pour cent du groupe-cible dans cette enquête. On peut dès lors parler d'une enquête suffisamment représentative.

4.2. Back-up et protection toujours axés sur les serveurs

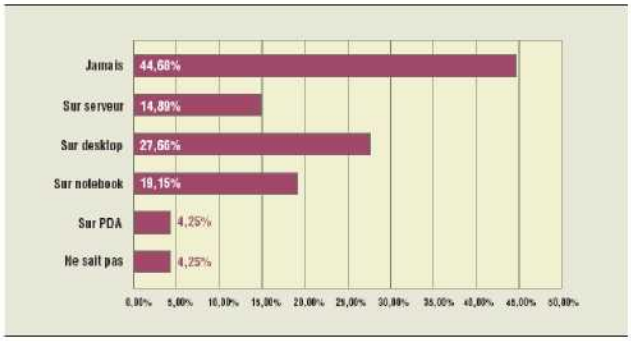
Plus de la moitié des répondants (56%) estiment que les serveurs courent le plus grand risque en matière de perte de données ou de risques de sécurité. C'est un raisonnement logique, vu que le serveur accueille généralement les données les plus précieuses, comme la base de données clients centrale, le système e-mail, etc. Les notebooks ou ordinateurs portables n'arrivent pas par hasard
à la deuxième place (les répondants ont été invités à composer un Top 3). En effet, ils sont – avec les PDA – probablement les plus sensibles aux dommages physiques, à la perte, au vol ou à l'infection vu qu'ils travaillent sur des réseaux non fiables hors des murs de l'entreprise. La grande différence entre les deux plates-formes est probablement imputable à une utilisation plus limitée du PDA à des fins d'entreprise.



4.3. Perte de données, surtout via des desktops et notebooks dans la pratique

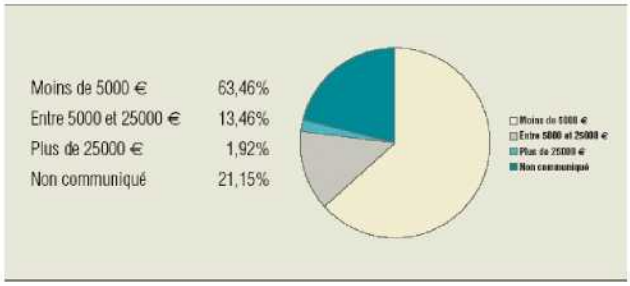
La problématique en matière de perte de données est un fait réel, auquel plus de la moitié des PME belges ont déjà été confrontées dans la pratique. Seulement un petit 45% des répondants affirment résolument qu'ils n'ont jamais subi de perte de données. Les données sur le serveur semblent généralement assez bien protégées: seul un petit 15% avoue avoir déjà perdu des données à ce niveau. Singulièrement, on observe que la perte de données sur PC de bureau (27,66%) est nettement plus élevée que sur des ordinateurs portables (19,15%). On ne peut que l'expliquer par la présence plus massive d'ordinateurs de bureau au sein des PME belges. Sur base de la tendance actuelle du marché, où les chiffres de ventes de notebooks approchent celles des desktops, on peut s'attendre à un revirement à terme – tout particulièrement parce que les ordinateurs portables, en raison du risque supérieur de vol et d'endommagement physique, représentent un facteur de risque plus élevé. Alors que seules 2 personnes avaient indiqué le PDA à la question précédente comme principal facteur de risque, le double de répondants avouent avoir déjà perdu des données de cette manière.

Avez-vous déjà été victime d'une perte de données? De quelle manière?



L'impact financier au sein des entreprises qui subissent une perte de données reste limité dans la majorité des cas à moins de 5000 euros (63,46%). Plus de 15 pour cent reconnaissent que cet incident leur a coûté plus de 5000 euros. Singulièrement, exactement la moitié de ces cas n'a jamais enregistré de perte de données sur le serveur. Plus d'un cinquième des répondants ne communiquent pas l'ampleur du préjudice, ou n'ont pas une idée précise des conséquences financières de la perte.

Impact financier de la perte de données



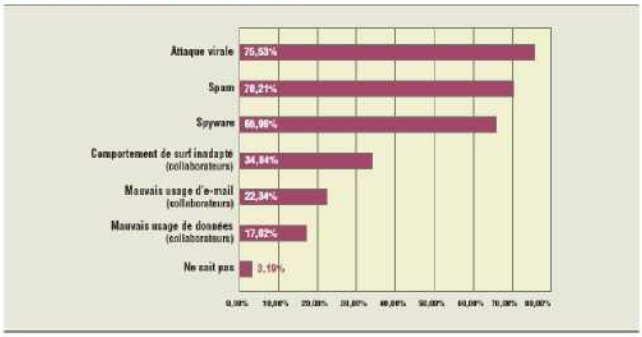
4.4. Virus, spam et spyware

Les attaques virales et le courrier indésirable sont les phénomènes les plus fastidieux aux yeux des PME belges. Rien d'étonnant. Les sociétés ont été confrontées aux virus depuis ces dix dernières années, sans interruption. Concernant le courrier indésirable, on doit constater avec prudence que "seulement" un bon 70% des répondants jugent le phénomène gênant. Il semble plutôt utopique d'en conclure que près de 30% ne reçoivent aucun spam. Par ailleurs, le nombre de plaintes quant aux le spywares est très étonnant. Près de deux répondants sur trois ont déjà rencontré des problèmes d'infection par des logiciels espions. Seulement un sur trois a eu des problèmes liés à un comportement de surf inadéquat. Le mauvais usage de l'e-mail et des données de l'entreprise sont eux aussi de réels problèmes, bien qu'ils touchent un groupe plus limité.

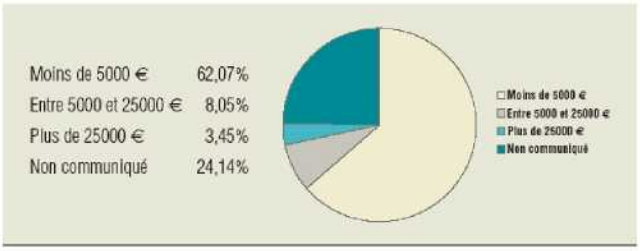
L'impact financier de ces problèmes de sécurité est tout aussi peu à sous-estimer. Tout d'abord, un nombre de répondants nettement plus élevé indique avoir déjà été confronté à l'un de ces phénomènes (92,55%), comparé à la perte de données (55,32%). Ensuite, le préjudice financier direct est au moins aussi grand que l'impact de la perte de données directe. Pas

moins de 3,45 pour cent avouent avoir subi un dommage supérieur à 25000 euros à la suite de virus et/ou d'autres phénomènes. Le groupe d'entre 5000 et 25000 euros est moins représenté que pour la perte de données. Près d'un quart des répondants – plus encore que pour la perte de données – n'a pas la moindre idée de ce que lui a coûté l'incident.

Avez-vous déjà été victime de...?



Impact financier de virus, spyware, spam, mauvais usage de données ou d'e-mail par des collaborateurs, ou comportement de surf inadapté



4.5. Prise de conscience, mais pas toujours une priorité ICT

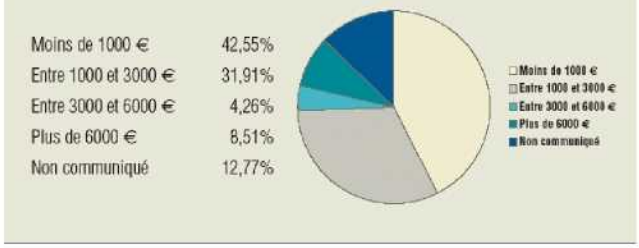
La majorité des PME belges se compose de bons citoyens Internet, qui disposent quasiment tous de la protection la plus indispensable. Plus de 88 pour cent ont un pare-feu et plus de 92 pour cent indiquent utiliser un logiciel antivirus sur tous leurs ordinateurs. Etonnamment, la protection contre le spam et les spyware est nettement moins répandue sur le marché, alors qu'il ressort de la question précédente qu'il s'agit d'un réel problème. Seulement quelque 56% utilisent un filtre antispam, alors que plus de 70% ont déjà eu à souffrir du spam. Exactement un répondant sur deux utilise une solution anti-spyware, tandis que deux sur trois ont déjà été importunés par des logiciels espions. "Je dispose d'un logiciel antivirus sur tous mes ordinateurs" - 92,55% "Je dispose d'un pare-feu" - 88,30% "Mon système e-mail est protégé par un filtre antispam" - 56,38% "Je dispose de logiciels anti-spyware sur tous mes ordinateurs" - 50% Les PME belges se montrent très zélées en matière de sécurité ICT. Plus de la moitié (54,25%) d'entre elles désignent même la protection ICT comme leur toute première priorité ICT. Plus de 80% des répondants comprennent que cette problématique est cruciale pour la continuité de leur entreprise. Autant indiquent qu'ils installent soigneusement et à temps des mises à jour de sécurité. Plus des trois quarts des répondants réalisent selon leurs propres dires des sauvegardes complètes chaque semaine. Plus de 60 pour cent ont intégré leurs mesures de sécurité dans une politique globale. Ce score peut être qualifié de très

encourageant. "Je trouve que l'ICT est cruciale pour la continuité de mon entreprise" - 80,85% "J'installe toujours les dernières mises à jour de mon logiciel de sécurité" - 80,85% "Je fais un back-up de toutes mes données au moins une fois par semaine" - 76,58% "Je dispose d'une politique pour protéger mes systèmes ICT" - 60,64% "La sécurité figure tout en haut de ma liste de priorités ICT" - 54,25% "L'importance de la sécurité ICT est exagérée" - 7,45%.
Un modeste 7,45% des répondants trouvent que toute la problématique en matière de sécurité ICT est exagérée. On soulignera que plus de la moitié d'entre eux sont à la tête d'entreprises de moins de 10 collaborateurs. Sont-ils moins prudents que d'autres? Seulement un d'entre eux ne dispose pas d'un logiciel antivirus, tandis qu'un seul autre n'a pas de pare-feu. Par conséquent, on peut plutôt parler de clients satisfaits.

4.6. Budgets trop limités

La prise de conscience n'est pas vraiment un point névralgique au sein des PME belges, bien que certains continueront toujours d'ignorer le problème. Il ne faut pas oublier que tous ceux qui ont complété cette enquête en ligne affichent a priori un sain intérêt pour la sécurité ICT. Le score en matière de conscience de la sécurité est par conséquent plus qu'honnête. Reste évidemment à savoir si cette prise de conscience se traduit effectivement dans les investissements ICT de ces entreprises. Et c'est précisément là que le bât blesse, surtout pour les entreprises de taille plus réduite.

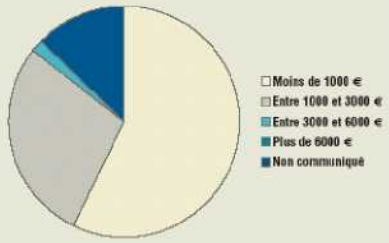
Dépenses annuelles en logiciels de sécurité au sein des entreprises belges



Alors que dans les entreprises de plus de 50 collaborateurs, les budgets nécessaires sont disponibles (28,57% d'entre elles mettent chaque année plus de 6000 euros sur la table), plus de 85 pour cent des PME au sens strict (jusqu'à 49 collaborateurs) doivent se contenter d'un budget de moins de 3000 euros pour les logiciels de sécurité. Plus de la moitié disposent même de moins de 1000 euros par an à ce niveau. La différence entre la prise de conscience et les investissements effectifs peut-elle être attribuée à des budgets trop limités accordés par la direction? Ce ne peut certainement pas être la seule explication, vu que plus de 52% des répondants indiquent être eux-mêmes le preneur de décision. En outre, un petit 5% des CEO laissent explicitement la responsabilité à leur personnel IT. Par conséquent, seule une minorité peut invoquer des restrictions budgétaires. On peut constater sans risque d'imprudence que ce qui manque surtout aux PME belges, c'est la conscience de la valeur réelle de leurs données numériques, de sorte qu'elles dégagent souvent des budgets trop limités pour celles-ci. Pour une partie des petites PME belges, il est naturellement possible que la véritable valeur des données d'entreprise soit effectivement très faible, parce qu'elles travaillent encore en grande partie de manière artisanale. Néanmoins, cela nous étonnerait que cette catégorie ait répondu massivement à notre enquête en ligne.

Dépenses annuelles en logiciels de sécurité au sein des PME belges comptant jusqu'à 49 collaborateurs

Moins de 1000 €	57,14%
Entre 1000 et 3000 €	28,57%
Entre 3000 et 6000 €	1,59%
Plus de 6000 €	0%
Non communiqué	12,77%



5. Conclusion

Il ressort de cette étude exclusive de PC World, menée en collaboration avec Computer Associates, que la protection et la sécurité sont un sujet brûlant pour les entreprises belges. Plus de la moitié des entreprises interrogées ont déjà perdu des données, dont les coûts varient selon elles de moins de 5000 euros jusqu'à plus de 25000 euros. Il en va de même pour les attaques de virus, les spyware, le courrier indésirable ainsi que le mauvais usage d'e-mail et de données. Bien que plus de 54 pour cent des entreprises déclarent que la sécurité se trouve tout en haut de la liste de leurs priorités ICT, le budget pour les logiciels de sécurité est généralement limité. Dans les PME de moins de 50 collaborateurs, pratiquement aucune ne dispose de plus de 3000 euros par an à ce niveau. Bien que de bonnes solutions soient certainement disponibles dans ce segment de prix, ces budgets ne semblent pas toujours en adéquation avec les risques réels. Enfin, les PME disposant de ces budgets sont pratiquement obligées d'opter pour une approche de sécurité intégrale, parce qu'elles n'ont ni les moyens ni l'expertise nécessaires pour parvenir à une protection totale avec des solutions Best-of-Breed.
«Les entreprises qui recourent aux meilleures pratiques consacrent en moyenne 14 pour cent de leur **budget** IT à la sécurité. La moyenne générale des dépenses de sécurité s'élève à 11 pour cent.» (Etude de CIO Magazine, CSO Magazine et PricewaterhouseCoopers, 3/1/2004)

Curriculum Vitae

Jan-Frans Lemmens started his journalist's career working for the leading Belgian newspapers De Standaard and Het Nieuwsblad in 1996-1997.
In 1998 he developed a strong interest in ICT and networking, working as a lab co-ordinator for BA Testlabs.
In early 2000 Jan-Frans decided to join the editorial team of CM Corporate, a high-quality Benelux title on professional ICT and software development. In the downturn CM Corporate got restyled to the monthly 'corporate.net' for which Jan-Frans was the prime - and only – one responsible, while also working for the weekly sister title Data News.

After 'corporate.net' was ultimately closed down in 2002, Jan-Frans joined the editorial team at the Belgian IDG affiliate as a chief editorial. He was responsible for managing the monthly titles Network & Telecom, Inside Internet, PC World Belgium, Channel World and Publish & Print.
Since august 2003 Jan-Frans rejoined BA Testlabs, offering expertise and solid tech journalism to most magazines on the market.
Since early 2005 Jan-Frans is working as a Publisher at Best of Publishing, responsible for IT titles like Network & Telecom, Inside (formerly Inside Internet), PC World and Channel World.

Präsentation

Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Hacking and Protecting a Cultural Website: The Case of CVC

Raquel Pérez-Colmenero, Instituto Cervantes, Madrid

Abstract

The Centro Virtual Cervantes is the face in the Internet of the Instituto Cervantes, a public organization devoted to spread the culture of those countries having Spanish as their mother language and to provide means for students and teachers of Spanish. The CVC houses, among many other contents, materials belonging to numerous artists and writers.
The CVC's basic goal is to provide any person interested in Spanish with means to looking at, learning, discussing, that is, to participate and share her or his experience about the Spanish language and the Spanish culture.
Besides, the CVC hosts a big Spanish course being used by means of agreements by universities and schools throughout the world. The use of this course is creating a relationship between students and also between tutors and students through the internet. This is, because of the interactivity of its materials and the learning environment, an unprecedented space in the field of virtual language teaching.
It is obvious that a site receiving one million visits per month, receives also attacks being faced at the CVC through the application of strict security policies, and putting to work all the necessary means -programs, machines and dedication.
The security policies accomplish three basic objectives:

- To keep up and to run the CVC's services, facing crashes, denying service attacks, etc.
- To keep in confidence the data of the tens of thousands registered users and the students of the Spanish course.
- To keep the integrity of the content hosted at the CVC servers.

Introduction

On the one hand, the CVC is the Cervantes Virtual Centre which is the headquarters of Cervantes Institute in the internet. It is a cultural website to spread our Spanish language and our culture all over the world. It was born in 1997, because of the quick increase of the Spanish demand. It is a centre dealing in the net, and extending to the whole word, opened night and day, working days and holidays.
On the other hand, AVE is our Spanish Virtual Course in internet. It is a virtual classroom for all the people who want to learn our language. It is offered a great number or interactive activities from beginners to advanced students interesting in learning our language.

Security, a critical aspect

Security is a critical aspect of the web applications. Web applications, by definition, allow the access of users to the central resources, this is the web server, through which, users can also enter others servers, such as, the web server.
But in my opinion, with the knowledge and the correct provision of security measures, resources can be protected and a safe environment where the users could work can also be provided.
It is an important task to avoid that a hacker or a cracker reaches his objective. Because of this, this task has to be done from a global point of view.
One of our main objectives is to protect and make safe the contents against possible hackers who could violate the security of our websites. One of the main reasons for this are the more than eighty thousand published pages, together with the more than seventeen thousand registered users in the website of Cervantes Virtual Centre.
On the other hand, when talking about our Spanish course, we are referring to over eight thousand five hundred students enrolled. Therefore, protecting the information we have makes the security of the Spanish course website to be the other of our main objectives.
Thus, it is an essential task of the technical team, which is a part of the CVC, to apply the necessary security policies in order to avoid possible attacks against our websites.

How can security be achieved?

Security can be understood as the system characteristics which tell us that this system is free of dangers for its components. This security can be achieved guaranteeing three things:

Confidence
Integrity
Availability

Speaking about confidence, I'll say that confidence consists of protecting the transmitted or stored data of non-authorized diffusions.
Everybody knows that the use of cryptographic methods, to a great extent, prevents the success of the attacker of cutting off the traffic between the web server and the user.
Talking about integrity, I'll just set off that it consists of detecting when the stored or transmitted data fields have been modified, deleted or reproduced.
Moving to availability, I'll point out that it is the capacity of a system or of a system resource of maintaining itself accessible and usable in view of the requests of authorized entities by the system.
It is important to establish the necessary security mechanisms in order to avoid the service refusal attacks.
We try to offer high availability systems that operate the same information in different servers, in order to guarantee the publication without interruption of every content during the 365 days and 24 hours/day in the year.

Where is the security apply from?

Preserving security in software applications development is as important as doing so on the website administration. There must be a coordination between the development team

and the systems team since the administration and maintains of the website depend on the way the software development is done.
The technical team in the CVC has the following objectives:

- ✓ To attain that the applications work through the security servers.
- ✓ To transfer the security accrediting patterns through the different levels of the application.
- ✓ To carry out the authorization.
- ✓ To guarantee the data integrity and privacy as they are spread along the public networks.
- ✓ To guarantee the security of the application state with a database.
- ✓ To make an application that could be enlarged to admit a larger number of users.

What is wanted to be protected?

According with our security policy: every element in our website should be protected, from any attempt of unauthorized access from the outside, including hardware, software and data.
What kind of data is used in the CVC?
For example, if a user wants to register in our web, these are the date that the user has to introduce.
Personal details, such us: name, surname, e-mail address, age and country.
Then, **Technical details**, such as, connection rate, operative system, if he has or has not sound card.
Why we need these technical details?
Well, for us would be useful to know the user's technical details to tackle the development of new web applications.
Also, **Professional details**. In the case the user were a Spanish teacher as a second language, he would introduce the name of his working place or the total number of students that he has. These details are useful for us in order to adapt our contents to the user's interests, and to know better the situation of the Spanish culture in the world.
Another example would be the case of a user who wanted to take part in the in the translation virtual workshop. Apart from introducing the details referred to the activity he does, he would also have to include in the personal details his mother tongue.
On the other hand, it is also important to know what kind of data is used in the Spanish course. So, if we access the virtual classroom for Spanish application, we will see that the details handled are again the personal details where we would have to include, apart from name, surname, address, country, or e-mail address, our city, postcode, nationality, date of birth or sex.
Also, academic, professional and access details should be introduced, together with details of the institution, class course an group.

The dilemma, functionality versus security

When developing an application some questions have to be raised.
On the one hand the necessary functionalities for the user to be able to develop his activities in an environment which fulfils his necessities has to be offered.

On the other hand, the security which guarantees the user's data confidence and the availability and integrity of the website can not be forgotten.
But the main aim of the Virtual Centre is to achieve that our web applications offer the user an updated working environment, together with the widest number of possible resources that would make the user an expert about our language and culture.
All this, of course, without forgetting the user's security guarantee together with the security of our websites.
I'll show you some examples of functionality applications offered by both the CVC and the AVE.
On the first place, I'll show you some of the web applications our CVC has,
For example, talking about virtual workshops, if we enter in the "translator's stand", we can see a virtual classroom for students of translation of English, French or German. The participants translate texts which have been prepared by a teaching team, who will later check them and suggest improvements and personalized recommendations.
We also offer the forum; we have four different spaces which make easy the exchange of information and opinion about aspects related to the teaching of Spanish.
They are discussion and debate canters, moderated by specialists of each field or topic.
We also offer interactive materials for children as well as videos.

Security policies

In order to establish the security policies necessary to protect both the CVC and the AVE, it is necessary to know which the characteristics of our settings are,

- The users have different types of explorers
- The anonymous users can explore the unrestricted pages of the application.
- Users have to register or begin a session through and html form in order to be able to see the restricted applications.
- The user's credentials are validated with a data base manager.
- All the information supplied by the user is validated in order to reduce the threat of SQL injection attacks.
- The database trusts the application to execute the authentication correctly. The application makes some calls to the database in name of the users.

In the setting we have just described, the web application presents a session entering page to accept the anonymous user's credentials.
The users obtaining the validation will be allowed to continue. However, the rest will have the access denied.
The database carries out the authentication trough an account of minimum privileges.
What is an authentication system?
Well, it is a security module which allows to identify who is the user who visits the pages.
Everybody knows that there are different authentication mechanisms, such as, digital certificates, authentication by forms and so on.
In the screen we can see an outline of an authentication system by forms. This outline implies the necessity of doing a development which prevents an intruder from going beyond the authentication mechanisms.
There is an entrance page in which both user and password are introduced in order to enter the restricted access application.

Once the user has introduced his user and password, these have to be checked in order to be validated against the database and to be able to obtain the credentials that allow him to enter.
Once the data has been checked to be time, it is necessary to do some security verifications to know if the access has been made successfully or if the page is being entered using forbidden way. The security layer in ASP is in charge of checking that a security context exists in order to show or not the restricted application which wants to be entered.
This security module will do all the suitable verifications and will operate allowing or denying the access, depending on the resulted verifications.
Apart from the code controls made in the web applications, the web server has to be shaped applying the necessary security policies to strengthen it in view of any attack.
A first safety barrier would be to establish in the web server the appropriate entry and execution permits to minimize the possibilities of any cracker writing his own code in a file inside a wrongly shaped folder, talking into account security. He would then be able to run it with the default granted permissions.

The case of CVC and AVE

When talking about the CVC, we are not only talking about a static web. There are numerous web applications where the user has to authenticate himself in order to be able to enter the restricted access application.
For example, lets enter the following application:
The world through words
We can see that we have established a first security level, which is an invisible url.
As second security level, the user and password page appears. Without the proper data, the user will have the restricted access application entrance denied.
Once we have entered the application, and if we copy the url and open another session in the navigator sticking the url, we will see that the page appearing is the user and password page instead of the page we wanted to enter. So, by means of the security layer established in every page, we are making sure that no intruder will be able to enter the application without logging in.
Another example would be the following web application:

The translator's stand
In this case, the security levels established are three:
The first level consists of an entering invisible url.
The second level is where the windows integrated authentication is carried out
And finally, in the third level, the authentication is made through user and password.

AVE
If we enter the Spanish course, we will come across a screen in which an entrance form appears. It is here where the student has to validate himself in order to obtain his credentials.
On the other hand, to maintain our students' integrity a hash function is used in order to validate the session in the web server.

Authorization from the development point of view
Once the system has authenticated the entrance of a user, depending on the user's profile, one setting or another will be accessed. Moreover, depending on the access level some operations will be carried out and others won't.
Talking about the different profiles a student could have in our Spanish course, I'll say that we have got two different setting.

Administration setting.
User's setting.

Each user who enters in each setting has gos a specific profile which allows him to enter a specific private module.
When talking about the administration setting the profiles a user can have are the following ones:

Administrator
Deputy Head of the Cervantes Institute
Deputy Head of linguistic technology
Administrative officer

Depending on their profile, each user will do more or less restricted operations.

Measures to take when developing a web page:

Html comments
The navigator ignores all the html comments when showing the page, but the comments can be seen when having a lot at the page code. So in this case we must be careful with the comments we write.

Links
The links can help us to understand the logic of the application. Moreover, used technologies can be identified.

E-mail addresses
Many pages have got references to e-mail addresses. They could be used by Spammers to obtain addresses to which they could send virus.

Hidden fields
You must be careful because the hidden fields can show parameters of the application.

Measures to take against invalid entrance attacks

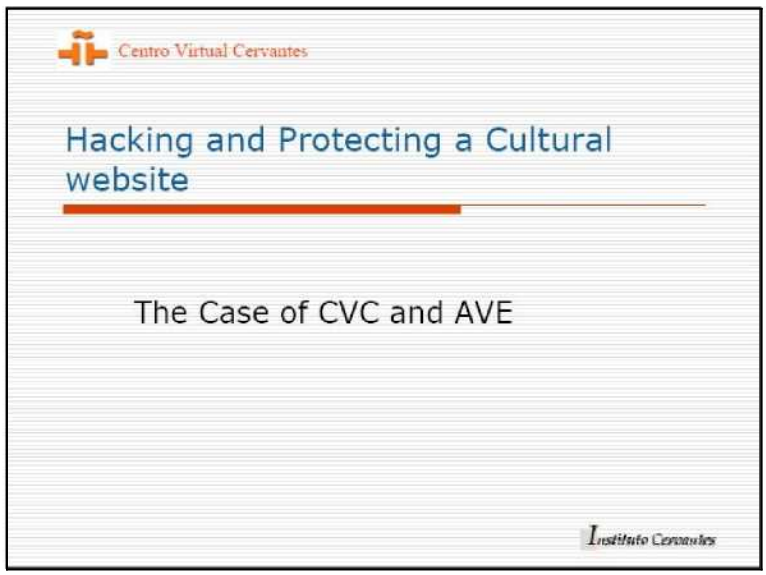
Canonization
Files inclusions containing the route "../" due to security primary route accesses are not allowed.

Buffer overflow
When developing certain functions care must be taken because they can provoke overflow which would change the return address.

Curriculum Vitae

Raquel Pérez-Colmenero (Guadalajara, Spain, 1969), formed academically on telecommunications, started her professional career working on computing application development, and has participated as a consultor and analyst in several linguistic technology projects.
She works since April 2003 at the Technical Department of the Virtual Centre of the Instituto Cervantes, collaborating in various research projects concerning web platforms, specifically a search machine which creates an specialised catalogue of URLs on Spanish language and culture as well as a Spanish Language Virtual Classroom.

Präsentation



Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Free internet access in public libraries: from security to filtering

Claire Chaumet, Head of the Information Service, Bibliothèque publique d'information, Paris

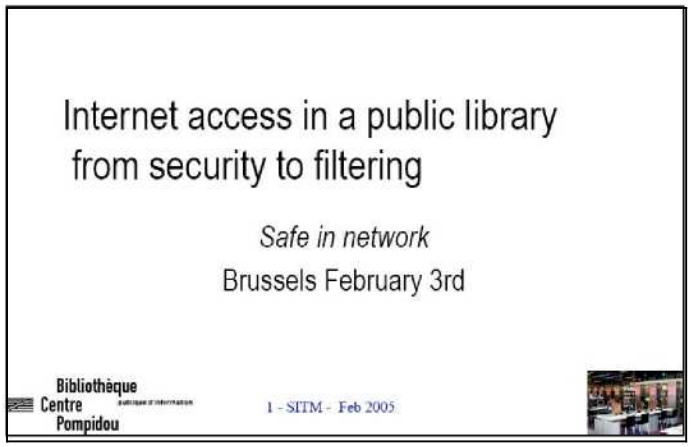
Abstract

The Information Public Library (Bpi Paris) manages 50 workstations with free access to internet since 1999.
At this date, a secure navigator was implemented to avoid user damages. This navigator was improved in 2002 to anticipate new threat.
In 2004 the library precised an "Internet User Chart" and implemented a new tool to filter inappropriate access (pornography, hacking, violence,..).
This paper presents the typology of current internet use and the technical architecture.

Curriculum Vitae

Claire Chaumet is the Information Service Manager of the Bpi (post degree in IT large data bases).
Her team (18 persons) is in charge of new projects, the technical survey and the maintenance of IS.
Before joining Bpi, she was project manager in the banking sector during 10 years and afterwards she was the Manager of an IS consultant team in a large

Präsentation



Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Network security - managing internal and external threats

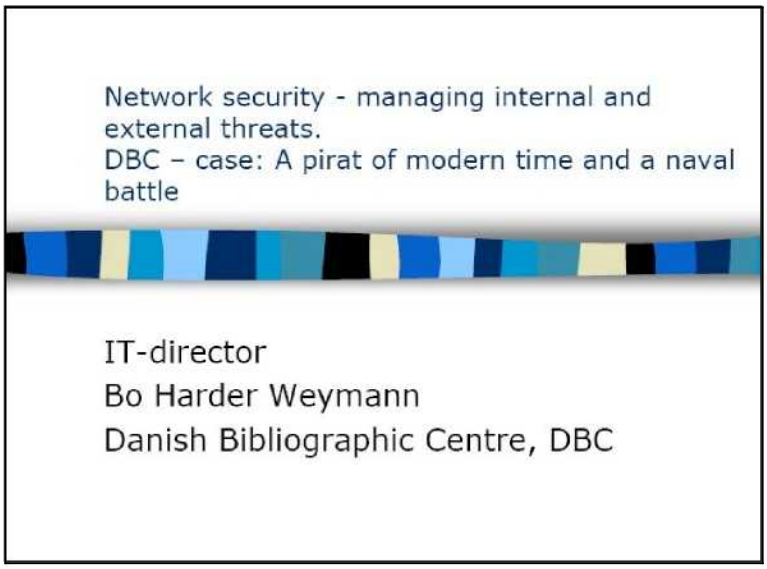
Bo Weymann, Head of IT-Service Center, Dansk BiblioteksCenter, Ballerup

Abstract

The focus is on management aspects of network security.
- Formulating a security policy
- Risk analysis and establishment of an appropiate level of security
- important security matters for libraries and other cultural institutions working with copyright in cultural products
- a case on DBC (piracy and consequenses for security policy and behaviour)

The focus contains leadership and the very important managerial issue of taking care of it-security on that level: Policies, organisation, etc.

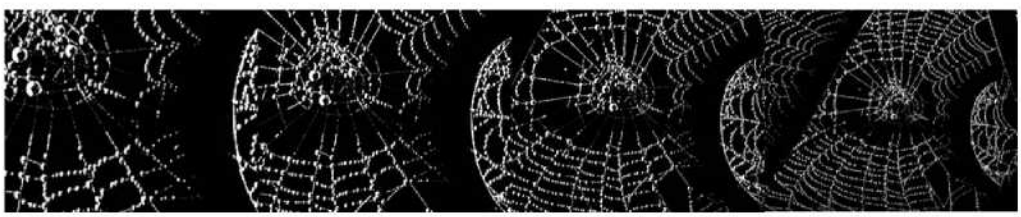
Präsentation



Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Sektion IV

Gesetzgebung und Netzwerksicherheit: ein nationaler und europäischer Überblick



Richtlinien der EG zum Urheberrecht und Netzwerksicherheit

Dr. Harald Müller, Leiter der Bibliothek des Max-Planck-Instituts für ausländisches öffentliches Recht und Völkerrecht, Heidelberg

Abstract

During the last couple of years the EC issued two directives on copyright in the information society, with effect on net security.
The directive 2001/29/EG on the harmonisation of certain aspects of copyright and related rights in the information society of 22 May 2001 contains several regulations on net security.
The directive 2004/48/EC of the European Parliament and of the Council on Measures and Procedures to ensure the enforcement of intellectual property rights of 29 April 2004 intends to give a copyright owner proper instruments for the realisation of his rights. The lecture presents all these legal instruments.

A. Sicher im Netz ?

Wenn man sich mit dem Thema Netzwerksicherheit beschäftigt, so verweisen Experten sofort auf die vielfältigen technischen Aspekte, Gefahren und Schutzmöglichkeiten. Viren und Trojaner, Firewall und Hacker werden in unzähligen Büchern, Aufsätzen und Konferenzen behandelt. Das Thema Sicherheit im Internet kann aber noch aus einem vollkommen anderen Blickwinkel betrachtet werden. Es weist Aspekte auf, an die der durchschnittliche Internetnutzer zunächst einmal überhaupt nicht denkt, wenn er von einer Webseite zur nächsten surft. Dabei erschließt sich die Perspektive sofort, wenn man die ganz naive Frage stellt, was sich eigentlich auf den Millionen von Webseiten im Internet befindet. Da gibt es Texte, Bilder, Musikdateien, Videosequenzen, Datenbanken und vieles andere mehr. Bei all diesen Objekten handelt es sich um Werke, die von einer kreativ tätigen Person geschaffen worden sind. Durch die rechtliche Brille betrachtet weisen alle Werke die juristische Eigenschaft auf, dass sie Eigentum darstellen. Irgendjemand, nämlich ein Autor, ein kommerzieller Verwerter, eine Organisation oder vielleicht die menschliche Gesellschaft allgemein ist Eigentümer all der Werke im Internet. Eigentum kann verkauft, genutzt, übertragen, aber auch gestohlen, missbraucht oder beschädigt werden. Und in diesem Zusammenhang stellt sich wie von selbst die Frage, wie eigentlich dieses Eigentum geschützt wird. Folglich enthält das Thema Netzwerksicherheit auch die Frage nach dem Schutz von Eigentum im Netz.

B. Schutz des geistigen Eigentums

Als Ergebnisse persönlicher Kreativität werden die beschriebenen Objekte (Werke im Internet) in der Sprache der Juristen mit dem Begriff geistiges Eigentum bezeichnet. Damit wird einerseits ein Bezug zum Oberbegriff des Eigentums hergestellt, andererseits aber auch eine Abgrenzung zu anderen Eigentumsarten (Sacheigentum, Eigentum an Rechten) vorgenommen. Der rechtliche Schutz des geistigen Eigentums geschieht durch das Urheberrecht.
Für die Europäischen Gemeinschaften bzw. die Europäische Union stellt geistiges Eigentum ein Wirtschaftsgut dar, das es umfassend zu schützen gilt. Deshalb haben EG/EU seit fast 20 Jahren den Schutz des geistigen Eigentums in das Zentrum ihrer Bemühungen gestellt. Ein Blick auf die nationalen Regelungen in den Mitgliedstaaten der Gemeinschaft lässt schnell deutlich werden, dass es beim Schutz des geistigen Eigentums in erster Linie auf eine Harmonisierung des Urheberrechts ankommt. Höchst unterschiedliche Bestimmungen in den Urheberrechtsgesetzen der EG-Mitgliedstaaten über Schutzumfang, Schutzdauer, Berechtigte, Ausnahmen usw. erfordern vorrangig eine Angleichung einzelstaatlicher Gesetze mit dem Ziel eines einheitlichen Schutzumfangs.
Nur ein harmonisiertes Urheberrecht gewährleistet das Erreichen der wirtschaftlichen und kulturellen Ziele von EG/EU, wie ein einheitlicher Binnenmarkt, der Schutz des Wettbewerbs und die Verwirklichung der wirtschaftlichen Grundfreiheiten. Der Schutz des geistigen Eigentums muss aber genauso die persönlichen Grundrechte, wie z.B. die Freiheit der Meinungsäußerung verbürgen.

C. Rechtsinstrumente der EU/EG

Zur Verwirklichung ihrer politischen Ziele bedient sich die EU verschiedener juristischer Instrumente, wie der Verordnung, der Richtlinie oder des Beschlusses. Im Hinblick auf die Harmonisierung des Urheberrechts kommt hauptsächlich die Richtlinie in Frage. Eine EU-Richtlinie gibt den Rahmen für ein nationales Gesetz, sie stellt Vorgaben an den einzelstaatlichen Gesetzgeber. Im Bereich Urheberrecht hat die EU/EG bereits in den 90er Jahren eine beachtliche Anzahl von Richtlinien erlassen. Es sind dies u.a.:

- 1991 Richtlinie zum Rechtsschutz von Computerprogrammen
- 1992 Vermiet- und Verleihrechtsrichtlinie
- 1993 Schutzdauer des Urheberrechts
- 1996 Schutz von Datenbanken

Keine dieser früheren Richtlinien erwähnt Datennetze wie das Internet. Nach der Jahrtausendwende hat die EU jedoch zwei Richtlinien zum Schutz des geistigen Eigentums erlassen, die sich ausdrücklich auch mit dem Schutz von Werken im Internet beschäftigen. Die wichtigsten Regelungen zur Netzwerksicherheit in diesen beiden Richtlinien sollen im Folgenden kurz vorgestellt werden.

D. Richtlinie zur Informationsgesellschaft

Die „Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft“ [1] nimmt an mehreren Stellen Bezug auf die moderne Informationstechnologie und die weltweiten Datennetze. Bereits in der Einleitung, im so genannten Erwägungsgrund 5 schreibt der europäische Gesetzgeber: “Die technische Entwicklung hat die Möglichkeiten für das geistige Schaffen, die Produktion und die Verwertung vervielfacht und diversifiziert.” Mit dem Hinweis auf die Errungenschaften der Informationstechnologie und der Datennetze weist der EG-Gesetzgeber darauf hin, dass zur Sicherheit im Netz auch die Harmonisierung und Weiterentwicklung des Urheberrechts gehört. Zur Verwirklichung dieses Ziel werden den Mitgliedstaaten mehrere urheberrechtliche Regelungen vorgeschrieben, die es bisher nur teilweise oder gar nicht in den nationalen Urheberrechtsgesetzen gibt.

1. Vervielfältigungsrecht

Artikel 2 der Richtlinie 2001/29/EG beschreibt das Vervielfältigungsrecht. Es handelt sich dabei um das ausschließliche Recht des Urhebers, die Vervielfältigung seines Werks zu erlauben oder zu verbieten. Dieses Recht steht genuin dem Urheber zu; es gehört damit zu den grundsätzlichen Rechten zum Schutz des geistigen Eigentums. Über jede Vervielfältigung hat zunächst einmal nur der Urheber zu entscheiden. Dieser Grundsatz gilt universell, d.h. er erstreckt sich auf jede Art und Weise, jede Form von Vervielfältigung, egal ob mittelbar der unmittelbar. Er gilt für analoge wie für digitale Kopien, für bedrucktes Papier genauso wie für Webseiten.

Die Richtlinie zur Informationsgesellschaft räumt aber gleichzeitig auch ein, dass im Bereich des Vervielfältigungsrechts eine überaus große Anzahl von Ausnahmen und Beschränkungen des Vervielfältigungsrechts möglich sind. Der Urheber muss es sich gefallen lassen, dass sein Recht zugunsten der Interessen der Allgemeinheit durch so genannte Schrankenregelungen eingeengt wird. In Artikel 5 der Richtlinie stellt der EG-Gesetzgeber einen umfangreichen Katalog von Schrankenregelungen auf, die die Mitgliedstaaten in ihren nationalen Urheberrechtsgesetzen aufnehmen können. Eine Vervielfältigung eines Werks ohne ausdrückliche Erlaubnis des Urhebers ist z.B. möglich für:

- vorübergehende Kopien als integralen Bestandteil einer technischen Übertragung im Computer oder Internet;
- analoge oder digitale Kopien für private Zwecke;
- Kopien im Rahmen der Tätigkeit von Bibliotheken;
- Kopien für Zwecke des Unterrichts und der wissenschaftlichen Forschung;
- Kopien für behinderte Menschen.

[1] Amtsblatt der EG L 167 vom 22. 6. 2001, S. 10-19.

Demzufolge ist es also vollkommen legal, wenn sich ein Internetnutzer einen Text ausdruckt oder ein Musikstück abspeichert, solange diese Werke rechtmäßig im Internet zugänglich gemacht werden. Allerdings wird in der Bevölkerung oft übersehen, dass es sich hierbei eigentlich um ein Ausnahmerecht handelt und das genuine Vervielfältigungsrecht ausschließlich dem Urheber zusteht. Die bekannte Diskussion um das „Recht auf die Privatkopie" bewegt sich deshalb häufig außerhalb der gesetzlichen Vorgaben.

2. Öffentliche Zugänglichmachung

Artikel 3 Abs. 1 der Richtlinie enthält eine Formulierung, die selbst viele Juristen auf den ersten Blick nicht verstehen: *Die Mitgliedstaaten sehen vor, dass den Urhebern das ausschließliche Recht zusteht, die drahtgebundene oder drahtlose öffentliche Wiedergabe ihrer Werke einschließlich der öffentlichen Zugänglichmachung der Werke in der Weise, dass sie Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich sind, zu erlauben oder zu verbieten.* Was ist damit gemeint?
Das sogenannte Recht der öffentlichen Zugänglichmachung beschreibt eine vollkommen neuartige Regelung im Urheberrecht. Mit dieser etwas seltsam klingenden Formulierung (englisch: right of communication to the public) findet nämlich das Internet gewissermaßen Eingang in das Urheberrechtsgesetz.
Die neue Bestimmung gibt einem Urheber das ausschließliche Recht zu entscheiden, ob sein Werk im Internet zugänglich gemacht wird (oder nicht). Es tritt damit gleichberechtigt neben die anderen elementaren Rechte des Urhebers, wie etwa die Rechte zur Veröffentlichung, zur Vervielfältigung, zur Verbreitung usw. Es dürfte nicht übertrieben sein, wenn man deshalb die Einführung des Rechts der öffentlichen Zugänglichmachung als wichtigste Neuerung in der Richtlinie 2001/29/EG bezeichnet.
Das Recht gemäß Artikel 3 Abs. 1 der Richtlinie ist vor allem von Betreibern von Webseiten zu beachten. Wer fremde Werke auf seinem Server ins Internet stellen will, benötigt hierzu die Übertragung des Rechts der öffentlichen Zugänglichmachung vom Urheber. Genauso wie bei anderen Urheberrechten geschieht das durch Einräumung von Nutzungsrechten. Bibliotheken und alle anderen Betreiber eines Servers müssen also Nutzungsrechte erwerben, wenn sie auf ihren Webseiten z.B. Photos oder Texte von dritten Personen öffentlich im Internet anbieten wollen. Besonders problematisch wird die Situation, wenn Bibliotheken retrodigitalisierte Werke ins Internet stellen, z.B. ältere Zeitschriften. Häufig sind die darin enthaltenen Beiträge noch urheberrechtlich geschützt, da die Autoren vor weniger als 70 Jahren verstorben sind. Eine öffentliche Zugänglichmachung ohne Genehmigung der Rechtsinhaber würde das Urheberrecht verletzen.

3. Verbreitungsrecht

Als weiteres zentrales Recht steht jedem Urheber die Entscheidung zu, ob sein Werk verbreitet wird oder nicht. Die häufigste Art der Verbreitung geschieht durch Veräußerung. Der Kaufvertrag kann sich auf das Original eines Werkes beziehen (z.B. ein Gemälde) oder ein Vervielfältigungsstück (z.B. ein Buch, eine CD). Artikel 4 der

Richtlinie schreibt den EU-Mitgliedstaaten den Rechtsrahmen vor, innerhalb dessen sie das Recht des Urhebers, über die Verbreitung seines Werks zu entscheiden, in ihren nationalen Urheberrechtsgesetzen ausformen können.
Das Verbreitungsrecht des Urhebers wird allerdings durch den in Artikel 4 Abs. 2 festgelegten Erschöpfungsgrundsatz eingeschränkt. Sobald ein Werk mit Zustimmung des Urhebers durch Erstverkauf in einem EU-Mitgliedstaat verbreitet worden ist, erschöpft sich sein Verbreitungsrecht, wird es sozusagen verbraucht. Der Urheber kann anschließende Verbreitungshandlungen wie den Weiterverkauf, die Ausleihe, die Vermietung nicht mehr untersagen. Der Erschöpfungsgrundsatz gilt allerdings nur für körperlich faßbare Werke. Es hat keine Auswirkung auf die öffentliche Zugänglichmachung von Werken im Internet. Deshalb dürfen Texte, Bilder, Musik, Dateien auf einem Webserver auch nicht einfach kopiert und über einen anderen Server weiter zugänglich gemacht werden. Für die öffentliche Zugänglichmachung in Datennetzen existiert kein Erschöpfungsgrundsatz.

4. Technische Schutzmaßnahmen

Mit der Regelung über technische Schutzmaßnahmen gewährt der Gesetzgeber einer weiteren Neuerung gesetzlichen Schutz, nämlich den sogenannten Digital Rights Management Systemen (DMRS). Bei digitalen Medien steht dem Rechtsinhaber die technische Möglichkeit zur Verfügung, durch z.B. paßwortgeschützte Zugangskontrolle, durch Kopiersperre, durch Verschlüsselung und viele andere Methoden die Nutzung eines Mediums beliebig zu kontrollieren. Artikel 6 der Richtlinie verbietet jede Umgehung derartiger technischer Schutzmaßnahmen. Genauso untersagt das Gesetz die Herstellung, Einfuhr, Verbreitung, Werbung und Dienstleistung von Umgehungstechniken, z.B. von Software zum „Knacken" der Schutzmaßnahmen.
Das Recht der technischen Schutzmaßnahmen gilt jedoch ebenfalls nicht schrankenlos. Der Gesetzgeber sieht auch die Möglichkeit eines Interessenkonflikts zwischen dem Rechtsinhaber und dem Nutzer eines Werkes. In Artikel 6 Abs. 4 wird dieser Konflikt zugunsten einer großen Gruppe von Benutzern unter Verweis auf die Schranken beim Vervielfältigungsrecht dahingehend aufgelöst, daß bei rechtmäßiger Nutzung eines durch technische Schutzmaßnahmen geschützten Werkes ein Rechtsanspruch auf Lieferung von Umgehungstechnik eingeräumt wird. Der europäische Gesetzgeber verpflichtet die Mitgliedstaaten, für etwa öffentlich zugängliche Bibliotheken, für Unterricht und wissenschaftliche Forschung, für Behinderte DMRS-Umgehungstechnik zur Verfügung zu stellen. Ein solcher Anspruch steht aber dem privaten Nutzer nicht zu. So ergibt sich die unerfreuliche Konsequenz, daß beim Zugriff auf z.B. kopiergeschützte Werke lediglich einem Wissenschaftler die Möglichkeit zur Umgehung geboten wird, aber auch nur als Rechtsanspruch gegen den Urheber. Selbsthilfe ist strikt verboten. Obwohl es also weiterhin rechtlich zulässig ist, von einer Musik-CD eine Kopie zum privaten Gebrauch herzustellen, kann die Musikindustrie dies in der Praxis durch eine Kopiersperre verhindern, ohne daß einer Privatperson noch eine legale Möglichkeit bleibt, ihr Recht irgendwie durchzusetzen. Faktisch ist damit das Ende der Privatkopie bereits eingeläutet.

5. Umsetzung in nationales Recht

Die Richtlinie 2001/29/EG zur Informationsgesellschaft ist mittlerweile in allen EU-Mitgliedstaaten in nationales Urheberrecht umgesetzt worden. Für Deutschland geschah dies durch das *„Gesetz zur Änderung des Urheberrechts in der Informationsgesellschaft vom 12. September 2003“* [2]. Im deutschen Urheberrechtsgesetz wurden folgende Bestimmungen geändert, ergänzt oder neu aufgenommen:

- Kopierrecht
- Elektronische Archive
- Vorübergehende Vervielfältigungen
- Öffentliche Wiedergabe
- Öffentliche Zugänglichmachung allgemein
- Öffentliche Zugänglichmachung für Unterricht und Forschung
- Technische Schutzmaßnahmen
- Bildkataloge
- Amtliche Werke
- Behinderte

In den anderen EU-Mitgliedstaaten traten ähnliche gesetzliche Änderungen in Kraft, obwohl sich manche Länder bei der faktischen Umsetzung teilweise schwer tun. So musste die EG-Kommission erst im Jahr 2004 Strafmaßnahmen gegen sechs Mitgliedstaaten androhen, die eine frühere urheberrechtliche Regelung aus der Vermiet- und Verleihrechtsrichtlinie von 1992 über die Ausleihvergütung im Zusammenhang mit Bibliotheken (Bibliothekstantieme) immer noch nicht praktisch umgesetzt hatten.

E. Durchsetzung des Rechts

Bei der zweiten Richtlinie, die es hier vorzustellen gilt, handelt es sich um die *„Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums“* [3]. Ihre Notwendigkeit beruht auf der Erkenntnis, dass es nicht genügt, Gesetze mit materiellen Rechten und Pflichten in Kraft zu setzen. Jedes Recht erfordert nämlich auch wirksame Instrumente, um es durchzusetzen, sonst bleibt es wirkungslos. Dies gilt selbstverständlich auch für den Schutz des geistigen Eigentums. Besonders das Internet wurde über viele Jahre als rechtsfreier Raum angesehen, in dem jedermann nach Belieben schalten und walten kann. Der Schutz des geistigen Eigentums erfordert deshalb wirksame rechtliche Instrumente zu seiner Durchsetzung. Die insoweit immer noch festzustellenden derzeitigen Unterschiede zwischen den Regelungen der Mitgliedstaaten verhindern, dass die bestehenden Rechte des geistigen Eigentums europaweit gleichmäßig geschützt werden.

[2] BGBl I 2003,1774
[3] Amtsblatt der EG L 195 vom 2.6. 2004, S. 16-25.

In Erwägungsgrund 9 der Richtlinie wird besonders auf die verstärkte Nutzung des Internets und den Vertrieb von Raubkopien hingewiesen.

Die Richtlinie 2004/48/EG nennt in Artikel 1 als geeignete Rechtsinstrumente Maßnahmen, Verfahren und Rechtsbehelfe. Diese müssen fair, gerecht, nicht unnötig kompliziert, wirksam, verhältnismäßig und abschreckend sein müssen. Da Beweise für die Feststellung einer Urheberrechtsverletzung von zentraler Bedeutung sind, muss sichergestellt werden, dass wirksame Mittel zur Vorlage, zur Erlangung und zur Sicherung von Beweismitteln in jedem EU-Mitgliedstaat zur Verfügung stehen. Deshalb schreibt Artikel 6 Abs. 1 eine Vorlagepflicht für Beweise vor. Zur Beweissicherung kann z.B. eine Beschlagnahme gerichtlich angeordnet werden. Gegen gewerblich Tätige soll ein umfassendes Recht auf Auskunft eingeführt werden.

Ferner sind einstweilige Maßnahmen unabdingbar, die unter Wahrung des Anspruchs auf rechtliches Gehör und der Verhältnismäßigkeit die unverzügliche Beendigung einer Urheberrechtsverletzung ermöglichen. Solche Eilmaßnahmen können die Untersagung einer Tätigkeit oder die Beschlagnahme von Waren sein. Schließlich müssen die Mitgliedstaaten einen Schadensersatzanspruch bei Verletzung des geistigen Eigentums vorsehen. Die Richtlinie enthält schließlich noch Regelungen über z.B. Prozesskosten, Veröffentlichung von Gerichtsentscheidungen und sonstige Sanktionen.

F. Fazit

Der Überblick hat gezeigt, dass die Sicherheit in Datennetzen den Schutz des darin befindlichen geistigen Eigentums erfordert. In allen Ländern der Erde behütet das Urheberrecht das geistige Eigentum. Besonders im Hinblick auf das weltumspannende Internet ist ein einheitlicher Urheberrechtsschutz in allen Staaten extrem wichtig. Die Europäische Union harmonisiert seit vielen Jahren das Urheberrecht in Europa. Besonders mit den letzten beiden Richtlinien 2001/29/EG und 2004/48/EG integriert der europäische Gesetzgeber den Schutz des geistigen Eigentums in Datennetzen in seine gesetzgeberischen Aktivitäten und schafft damit einen wirksamen Beitrag zur Sicherheit im Netz.

Curriculum Vitae

Dr. Harald Müller (55) is director of the library of the Max Planck Institute for Comparative Public Law and International Law in Heidelberg.
For decades active in numerous national and international boards, especially in der law commission of the German library association (formerly of the German library institute), he researches, teaches and publishes to all aspects of library law.

Präsentation

Die vollständige Präsentation befindet sich auf der beiliegenden CD-Rom.

Who is protecting what?

- The challenges of providing Internet access in public libraries -

Brendan Teeling, Assistant Director, An Chomhairle Leabharlanna - The Library Council, Dublin, Ireland

Abstract

Public Internet access has been provided in public libraries in Ireland since 2000. This paper surveys the challenges posed to library services by the security aspects of providing the service.

Public Libraries in Ireland

Public libraries in the Republic of Ireland are provided by local authorities, and there are thirty-two separate such authorities. Between them they operate a branch network of 345, a mobile library fleet of 29, and spend a total of €90 million per year, or €22.94 per capital per year.[1] Although some policies are set at national level, for example the *Branching Out* report, which sets out an eight-year programme of development, the delivery of the service is entirely a matter for individual local, or library, authorities. Thus, there can be wide variations in how particular services, such as the Internet access service, are delivered locally.

The development of Internet access in public libraries

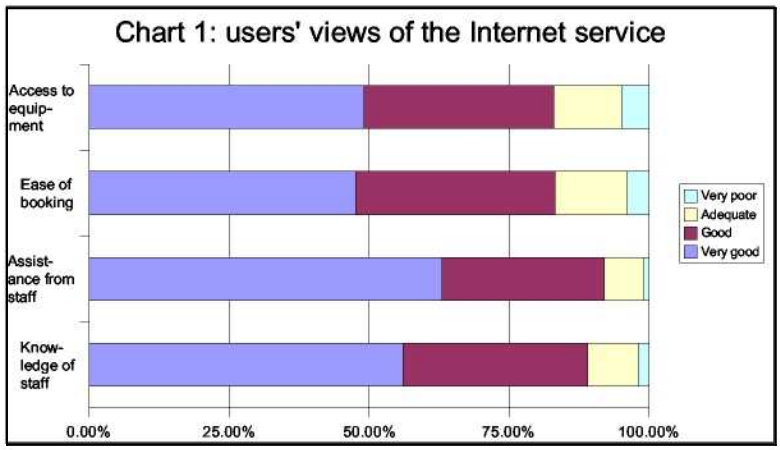
A brief survey of library literature suggests that Internet access in public libraries was considered as early as 1993, by the New York Public Library (Mastern). By 1995 17% of public library authorities in the UK were providing the service. By 2000 94.5% of public libraries in the USA offered public Internet access (Bertot and McClure, p.3), while in the following year 59% of all UK public library service points had public Internet access PCs (Howarth). Although one or two Irish public libraries started providing public Internet access in 1997, with funding from Microsoft, it was only in 2000 that provision on a national scale began. This was facilitated by a grant from central government to library authorities for the purchase of PCs, for public access use. The full purchase price of the PCs was grant-aided, and over the following two years PCs were installed in branches in all thirty-two library authorities in Ireland. Training was provided for staff in the use of the Internet, but the management of the service (including technical support) was, and remains, the responsibility of the library service locally. Different library services adopted different models for the management of the

1 See www.librarycouncil.ie for further information.

service. Some authorities contracted technical support from commercial companies, while others received support from within their own library or local authority service.
Although a minimum specification was laid down for grant-aided PCs, no requirements as regards operating system, software, or security were specified. Library authorities were free to select whatever systems they wished, and to implement their own choice of operating and security policies. By 2001 Internet access was available in public libraries throughout Ireland, with thirty-one of thirty-two library authorities providing the service. Public Internet access is now a normal part of public library services in Ireland, as in most countries in Europe.

Security threats and Internet access in public libraries

The security threats posed by the use of the Internet continue to grow and change. Symantec reported in September 2004 that phishing, spam, client-side attacks, spyware, and remotely controlled [ro]bot networks will continue to be growing security threats in 2005. Referring to spam alone, Symantec says: 'What was once merely an annoyance is now a serious security concern as Trojans, viruses, and phishing attempts continue to spread through spam' (Symantec, pp.42-6). Research in Ireland suggests that 46% of PCs in the workplace have been affected by viruses in the past, while 'understanding of key Internet security terms such as Operating System patches, phishing and modem hijacking is poor among work Internet users ...' (Department of Communications). In response to this research the Irish Government launched a national 'Make IT Secure' initiative in December 2004 (www.makeitsecure.ie).
Turning to the provision of Internet access in public libraries, the media (both general and professional) has tended to concentrate on the (more sensationalist) issue of use of library PCs to view pornography, and whether filtering should or should not be used, rather than on security issues. A search of Library and Information Science Abstracts (LISA) returned only ten articles on the subject of security and public Internet access, while 26 articles concerning pornography are listed.



If security issues are a major concern for the provision of Internet access, we might expect this to have an impact on the service as viewed by the people who use it. A Public Library User Survey (PLUS) carried out in 2002 showed that 17% of the 8.7 million adult visitors to Irish public libraries used the Internet (PLUS, p.9). Users' views

of the Internet service (Chart 1) were very positive: access to equipment was rated good or very good by 83% of users; 92% rated the assistance they received from staff as good or very good, and 89% rated staff knowledge as good or very good (ibid. p.14). The high levels of satisfaction with the Internet service suggest that any security problems which may exist in the service are not having a noticeable impact on the users of the service.
Anecdotal evidence suggests that from the staff point of view, the major issues that give rise to discussion about the service relate to the administration of the service (i.e. taking and managing bookings for the service). What then is the impact of security threats on public library Internet access?

Security threats and the views of library staff

In preparation for this paper, a survey was distributed to the librarians responsible for IT in public libraries. The survey (see appendix 1) was distributed by e-mail to 21 library authorities, and 14 responses were received. The responses are representative of the service as a whole, as they include large and small, urban and rural services.

Internet sessions

The 14 services provide a total of 689 Internet PCs in 176 branches.[2] The number of branches ranges from 3 to 32, while the number of PCs ranges from 26 to 90. 10 services provided figures for the number of Internet sessions offered, and these totalled 789,497. Of these, 643,126, or 81.46%, were taken up by the public. The rate of take-up across services ranged from 58% to 100%.

Sessions Offered	Sessions taken	% taken	Average take-up %
789,497	643,126	81.46	79.85

Table 1: Internet sessions provided (n=14)

PC management systems

12 of the 14 services use a PC management system (or a combination of systems) which typically reset the PC after each user's session (see table 2). The other 2 services plan to introduce management services in 2005.

2 A survey carried out by An Chomhairle Leabharlanna in October 2003 showed that there were 1,309 public access Internet PCs located in 312 branches in 32 library authorities.

Management system	No. installations
Deep Freeze	1
Interleaf (bespoke system)	1
Juzt-Reboot	1
NT4 profiles	1
PAC	1
PCReservation	1
Sitekiosk	1
Thin Client system	2
Winlock	2
WinU	3
None	2
Total	16

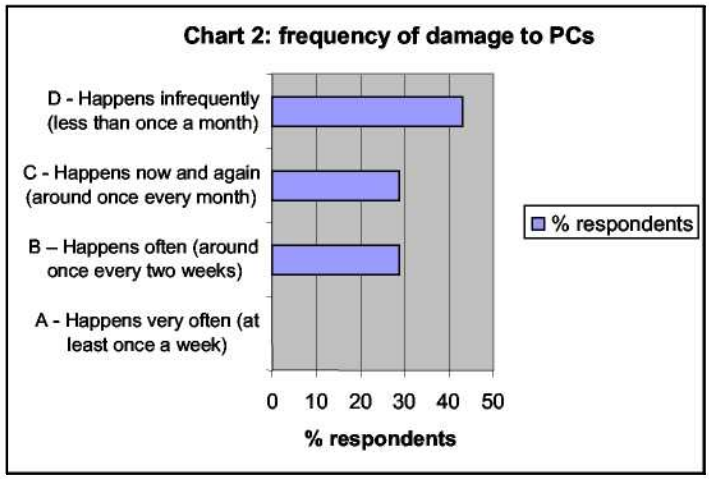
Table 2: PC management systems

That there are 10 different systems in use in 12 services shows that there is no national standard in this area: each authority selects its own system.
13 of the library services reported that they had anti-virus software installed on PCs, while the other plans to install it in 2005.

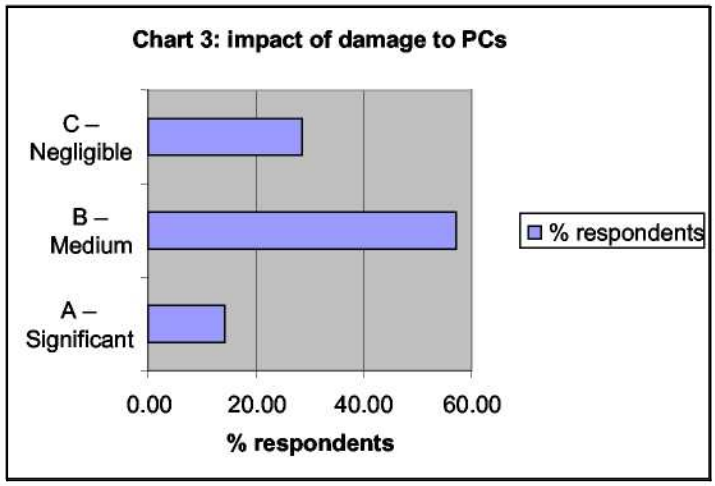
Anti-virus	No. installations
McAfee	4
None	1
Norton	4
Sophos	1
Symantec 9.0	4
Total	14

Table 3: anti-virus software installed

The diversity of programs in use is not as great as with the management systems but this is most likely a reflection of the market, dominated as it is by four products, all of which are in use in Irish libraries.
One area in which there is no diversity is in the browser used: all respondents use Internet Explorer on their public access PCs.
Library services are certainly aware of the risks of damage to PCs: such damage includes the deleting of system files and corruption of the registry. What is their experience of such damage? Respondents were asked to rate the frequency of incidents of damage to Internet PCs. As can be seen in chart 2, the majority of library services reported that damage occurred 'infrequently' (less than once a month); with remainder divided equally between 'now and again' (once a month) and 'often' (around once every two weeks). No respondent reported incidents as occurring 'very often'. In their comments respondents cite the use of the PC management system as the main factor in preventing damage.



Respondents were also asked to rate the impact of such incidents.

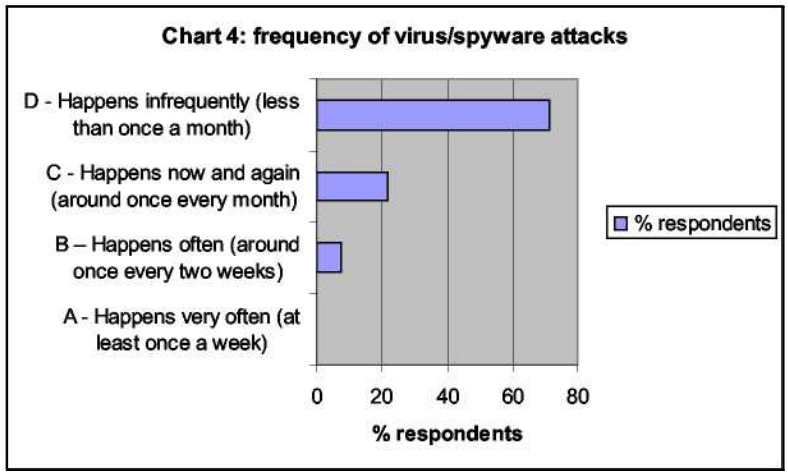


This chart shows that while the frequency of incidents of damage to PCs is not high, their impact cannot be ignored. 10 of the 14 respondents rated the impact (in terms of staff time and computer down-time) as 'medium; or greater. The source of damage to PCs is the user, who may cause such damage inadvertently or deliberately: only 2 of the library service believed that damage was caused deliberately in most instances.

Viruses and spyware enter the system from outside, and as mentioned above they constitute a major threat to computer networks. Library services were asked to rate the frequency of such incidents on their Internet PCs. Chart 4 suggests that although in general viruses and spyware are seen as a growing threat, they are not seen as a major problem in library Internet services as yet.

The implementation of anti-virus software by almost all respondents no doubt accounts in some part for the low impact of such attacks: 8 regard it as negligible, with 5 seeing the impact as 'medium' and only 1 as 'significant'. Only 4 respondents believe that

incidents of spyware and browser hijacking are increasing, although this is a trend reported by Symantec (and other research).



The reasons for the disparity between the experience of libraries and that of Internet users generally, backed up by the research, needs explanation. One possible reason may arise from the fact that public library Internet services are provided on a branch basis. It may be that staff at branch level are unaware of the level of incidents or that they are aware of them but do not (for whatever reason) report them. If this is the case then the data collected in this survey are incomplete, and the true levels of incidents and of impact are much higher. This requires further investigation.
Notwithstanding the above, 12 of the 14 library service do have measures in place to guard against spyware and hijacking, as set out in table 4. The diversity of measures employed is evident once again.

Software used	No. installations
Ad-Aware	*2*
Cybersitter	*1*
Juzt-Reboot	*2*
None	*2*
PAC Security Tool	*1*
Spybot	*6*
Total	*14*

Table 4: measures against spyware, etc.

Almost all library services in Ireland, including all those who responded to the survey, have online catalogues and library websites. Only one respondent reported hacking attempts against their catalogue or website. In most cases the online system, and indeed the website, are maintained by the local authority's central computer section and library staff would not necessarily be made aware of such attacks. Likewise, some library staff might not be aware of the specific measures employed to guard against attacks, with only 6 reporting having firewalls installed.

Conclusion

This small survey demonstrates that the general view of security threats held by Internet and network specialists, and seen by many Internet users daily, is not reflected in the experience of library services' public Internet provision. The frequency of damage to PCs, and of virus and spyware infestations is not high, though the impact of such incidents cannot be ignored. Almost all library services have installed management systems, and anti-virus and spyware software, evidence that they are aware of the threat. However, the relatively low level of reported incidents, and the consequent impact on service, requires further investigation. That awareness exists is also revealed in librarians' comments in response to the survey. Several respondents mentioned the importance of security, citing the need to maintain and update management systems and anti-virus software. Although the incidents of spyware have not been significant to date, many respondents expect the rate to increase (event if they have not seen such an increase so far). The level of impact of such threats may not be significant for those staffing the public Internet access service, but the potential impact on those using the service is much higher. More than one librarian cited the danger of a library patron falling prey to phishing, and submitting sensitive information in response to a fraudulent request. In addition to the harm caused to the user, the potential for that user seeking redress from the library service that provided the Internet PC and connection is very real.

Library services must employ a multi-faceted approach to dealing with Internet security threats. One facet is the use of up-to-date technology and the continuous monitoring of the effectiveness of the technology. A second is keeping abreast of new threats and the methods available to deal with them. A third, not addressed by the survey, is user education. This is important as it not only enhances the security of the libraries' own PCs, but also educates users about Internet security, and in doing so meets one of the objectives of the Internet service, namely the development of a participative information society. The fourth facet is perhaps the most important: library staff responsible for delivering the service at central and at branch level must be provided with the necessary training to enable them take the appropriate steps to protect their systems and their library users.

Curriculum Vitae

Brendan Teeling qualified as a librarian from University College, Dublin, in 1987. He worked on a number of local studies projects before joing Dublin City Public Libraries in 1994, as periodicals librarian. He was subsequently in charge of the International IMPAC Dublin Literary Award, before joining the Library Council as Assistant Director in 2000.

Brendan was Secretary of the Library Association of Ireland from 1992 to 1998, and remains a member of the Executive Board of the Association. He was awarded a Masters degree in local history from the National University of Ireland, Maynooth, in 2003.

Buchverlage und Internet - Risiken und Möglichkeiten – Rechtliche Hintergründe –

Anne Nina Schmid, Justitiarin, Verlagsgruppe Random House GmbH

Abstract

Die Verlagsgruppe Random House, Bertelsmann, betrachtet das Internet als zukunftsträchtige Plattform, um Verlagsinhalte in Form von Text- und Tondateien zu vertreiben oder umfassend in Suchmaschinenprogramme einzuspeisen.
Um dabei Urheberrechtsverletzungen zu vermeiden, ist u.a. streng darauf zu achten, dass sich die Autoren mit der Internetnutzung ihrer Werke einverstanden erklären und der Gefahr der Internetpiraterie entsprechend begegnet wird. Letzteres geschieht durch ständige Überwachung von Tauschbörsen und Auktionsforen, Kopierschutz und Anpassungen des deutschen Urhebervertragsrechtes, vorrangig aber durch vermehrtes Anbieten legaler und finanziell attraktiver Downloadmöglichkeiten.

1. Zum Unternehmen

Bertelsmann ist ein Unternehmen mit nahezu 80.000 Beschäftigten und knapp 20 Mrd. € Umsatz. Ein Bereich neben den Zeitungs- und Zeitschriftenverlagen von Gruner und Jahr, den Fernsehaktivitäten um RTL/Vox/ntv, den Buchclubs und dem Servicebereich von arvato sind die mit dem Buchclub nicht zu verwechselnden Buchverlage, die weltweit unter der Bezeichnung Random House zusammengefasst sind, jedoch länderspezifisch eigenständig arbeiten und rechtlich selbständig sind. Random House hat Niederlassungen u.a. in USA, Kanada, England, Australien, Neuseeland, Spanien, Japan und Deutschland.
Ich bin Justitiarin der deutschsprachigen Buchverlage, die als Verlagsgruppe Random House GmbH firmieren. Wir beschäftigen in mehr als 20 in München ansässigen Verlagen wie Siedler, Luchterhand, Blessing, Heyne und Goldmann ungefähr 500 Mitarbeiter und erzielen mit mehr als 1.000 Neuerscheinungen jährlich über 200 Millionen € Umsatz.
Bekannte Autoren unseres Hauses sind Christa Wolf, Helmut Schmidt, Frank Schirrmacher, Michael Crichton, John Grisham, Stephen King. Wie eigentlich alle Verlage vertreiben wir unsere Produkte nicht direkt an Leser. Daran änderte auch das Internet nichts: Wir vertreiben unsere Bücher lediglich an Wiederverkäufer, also an Buchhandlungen und an sog. Zwischenbuchhändler, die den Buchhandlungen mittels großer Präsenzlager schnelle Bestellmöglichkeiten seltener nachgefragter Bücher ermöglichen.

2. Interneteuphorie

Um das Jahr 2000 kam nicht nur die gesamte Wirtschaft sondern auch Bertelsmann zur Erkenntnis, dass die Zukunft dem Internet gehöre. Damals wollte sich keiner den Vorwurf gefallen lassen, er erkenne nicht die Möglichkeiten, die jenes neue Medium bieten könne. Sämtliche Geschäftsfelder wurden darauf untersucht, ob und wie sie übers Internet betrieben werden können. Bertelsmann schuf daraufhin bol.de, einen Konkurrenten zu amazon, der mittlerweile verkauft wurde. Random House US beteiligte sich an barnesandnobles.com. Die Verlagsgruppe Random House, über deren Erfahrungen ich heute sprechen möchte, war wie andere Verlage auch aufgeschreckt von Vorstößen wie desjenigen von Stephen King, der sich von den Buchverlagen lösen wollte und als ersten Versuch einen Roman ausschließlich online anbot und darauf setzte, dass seine Leser freiwillig dafür bezahlen würden. Dieser Versuch, so zeigte sich recht schnell, war erfolglos, da online-Nutzer sich erst daran gewöhnen mussten, für Inhalte Geld zu bezahlen und da Autoren recht schnell erkannten, was für Dienstleistungen Verlage ihren Autoren über die bloße Veröffentlichung hinaus noch liefern. Die Verlagsgruppe, anders als manch anderer Verlag, wollte nicht nur abwarten, wie sich der Markt entwickeln würde sondern wollte diesen aktiv mitbestimmen. Sie digitalisierte alle Texte ihrer Neuerscheinungen, um diese für Internet-User bildschirmlesbar zu gestalten. Unsere sog. backlist, also die noch lieferbaren Neuerscheinungen früherer Jahre, sollte ebenfalls vollständig digitalisiert werden. Dazu sollte es jedoch nie kommen. Man merkte nämlich schnell, dass die Vermarktung von Büchern übers Internet schwieriger werden würde als geplant.

3. Internet-Realität

3.1 Beteiligung an E-Book- Aktivitäten Dritter auf dem Gebiet des Internets

Unternehmen wie Rocket-E-Book, Getabstract oder Ciando wurden gegründet und konzentrierten sich auf den Vertrieb so genannter E-Books. E-Books sind Bücher in digitaler Form, die direkt per Download bezogen werden können.
Leser müssen nicht auf eine Auslieferung per Post warten oder einen Buchladen aufsuchen. Sie erhalten Ihr E-Book sofort, direkt auf den Computer - auch nachts oder an Feiertagen. Sie brauchen nur die Kapitel eines Buchs zu erwerben, die sie wirklich benötigen. In den meisten Fällen zahlen Kunden für ein E-Book weniger als für das „normale“ Buch, da E-Books nicht preisgebunden sind. Mit einem elektronischen Buch kann man Dinge machen, die bei einem normalen Buch nicht möglich sind: man kann im Buch suchen, mehrere Notizen einfügen, Lesezeichen setzen. Und u.U. kann der Text auch ausgedruckt werden. Wir belieferten diese Unternehmen mit digitalisierten Inhalten unseres eigens zu diesem Zweck gegründeten Verlagslabels Prisma Electronic Publishing.

RocketE-Book bot dem Leser die vollständigen Fassungen ansonsten in Papierform erschienener Bücher zum download an, Get abstract bietet komprimierte, auf fünf bis acht Seiten zusammengefasste Lektüre auf dem Gebiet der Wirtschaftsliteratur, Klassikerausgaben, also rechtefreie Belletristik, und Zeitschriften an. Ciando hat seinen Schwerpunkt auf der Möglichkeit, Bücher lediglich kapitelweise herunterzuladen.

Die jeweiligen Interessenten können sich die E-Books auf eigens konstruierte E-Book-Lesegeräte oder auf PC, MAC, Laptop oder auf einen Palm Handheld laden. Die Dateien sind zum Schutz der Urheberrechte verschlüsselt und können nicht weitergegeben werden.
Der Bildschirm eines Palm erwies sich aber als zu klein und damit unattraktiv für Leser, E-Book-Lesegeräte kosteten um die 300 € und wiesen eine im Vergleich zum guten alten gedruckten Buch eingeschränkte Lesequalität auf, konnten sich jedenfalls nie durchsetzen. Gegenwärtig wird an einem Nachfolgemodell mit sog. e-ink gearbeitet, das aber vorerst nur in Japan angeboten werden soll. RocketE-Book ist mittlerweile insolvent.

3.2 Beteiligung an sonstigen Aktivitäten Dritter auf dem Gebiet des Internets

Search inside the book

Die 2003 in den USA eingeführte Suchmaschinenprogramm "Search Inside the Book" ermöglicht es, im gesamten Text von rund 120.000 Büchern der 190 teilnehmenden Verlage mit gesamt 33 Mio. Seiten nach Suchbegriffen zu durchsuchen. Die Verlage können die Daten entweder als PDF-Datei zur Verfügung stellen oder Amazon zum Einscannen zur Verfügung stellen. Nicht registrierte Kunden können anhand einer Trefferliste zwei bis drei Sätze pro Buch vor bzw. nach einem Suchbegriff einsehen. Registrierte Kunden können sogar bis zu 20 Prozent eines Buchs pro Monat pauschal oder zwei Seiten vor und nach Suchbegriffen bis zur Grenze von 20 % durchlesen, ohne etwas dafür bezahlen zu müssen. Aus Sorge um Mißbrauchsmöglichkeiten können die ausgewählten Buchpassagen weder ausgedruckt noch heruntergeladen werden.
Das neue Angebot von Amazon, ganze Bücher nach Stichwörtern zu durchsuchen, wird in deutschen Verlagshäusern bislang eher zurückhaltend beurteilt. So wünschenswert die Promotion von Büchern auch sei, eine Volltextsuche werfe juristische Probleme auf, so Lutz Kettmann, Marketing- und Vertriebsgeschäftsführer bei Rowohlt. Schließlich tangierten solche Services immer das Urheberrecht. Auch Sabine Kohl, Mitarbeiterin in der Lizenzabteilung der Deutschen Verlags-Anstalt, sieht das Projekt »Search Inside the Book« problematisch. Schon jetzt werde in ihrem Haus immer wieder über die Bereitstellung von Textproben für elektronische Dienste diskutiert. »Ich gehe zunächst einmal davon aus, dass ein Internet-Buchhändler dasselbe Interesse hat wie sein Kollege im stationären Buchhandel: nämlich Bücher zu verkaufen«, kommentiert Eichborn-Lizenzchefin Jutta Willand. Um einen Eindruck von einem Text zu bekommen, reiche eine Leseprobe völlig aus.
Mit Ausnahme von Random House hat sich noch kein deutscher Verlag zur Teilnahme am Suchprogramm bereit erklärt, wohl auch, weil Amazon Presseberichte zufolge neben dem Multimediarecht (dem Recht, Lizenzmaterial zu erfassen, zu bearbeiten und auf elektronischem Weg zu speichern und zu verbreiten) auch weitergehende Rechte wie Merchandisingrechte, Werberechte, Senderechte und Sublizenzrechte verlangt.
Google plant gegenwärtig ebenfalls Buchinhaltssuchen wie Google Print (Belletristik und Sachbücher) und Google Scholar (Bibliotheksbestände). Der Internetsuchdienst hatte angekündigt, in den nächsten zehn Jahren 15 Mio. Bücher mit Hilfe von automatisch blätternden und fotografierenden Scan-Automaten für das Internet zu digitalisieren und über seine reguläre Suchmaschine anzubieten. Von Kooperationen mit Verlagen ist bislang nicht die Rede, allerdings haben Universitätsbibliotheken wie

Stanford, Oxford und Harvard ihre Beteiligung zugesagt, jedoch bislang nur hinsichtlich von Werken, die urheberrechtlich nicht mehr geschützt sind. Bei jüngeren Werken sollen nur Auszüge veröffentlicht werden.

Audible

Audible.de ist eine deutsche Tochter des US-Internet-Portals, das Downloads von Hörbüchern aktueller Bestseller, Klassiker, Sachbücher und bekannten Zeitungen und Zeitschriften z.B. Handelsblatt und ZEIT, ermöglicht. Interessenten können Audiotitel bequem auswählen, sofort herunterladen und auf mobile Player (iPod oder andere MP3-Player, PocketPC, Palm oder Smartphone,) oder direkt am PC/Mac oder einem anderen Endgerät anhören. In USA wird für 2004 30 Millionen Dollar Umsatz erwartet.

3.3 Eigene Aktivitäten der Verlagsgruppe Random House im Internet

Verlagshomepage www.randomhouse.de

Wie eigentlich jedes Unternehmen erkannten wir schnell, wie wichtig für den Kundenkotakt die Errichtung und regelmäßige Pflege einer Homepage ist. Die Seite www.randomhouse.de ist mittlerweile sowohl nach der Zahl der Zugriffe als auch laut unabhängigen Bewertungen hinsichtlich der Benutzerfreundlichkeit eine der führenden deutsche Verlagsseite. Wir bieten dort Informationen zu allen unseren Büchern, Autoren und Verlagen und vermelden täglich mehr als 11.000 Zugriffe bei einer 40 prozentigen jährlichen Steigerungsraten.

Homepage www.pressdepartment.de

Wir bieten Journalisten einen Zugang zu einer eigens für ihre Bedürfnisse gestalteten Homepage. Dort finden sich Informationen zum aktuellen Verlagsprogramm, Autorenfotos, abspielbare Autoren-O-Töne, Pressemitteilungen, ein Pressespiegel und Lesungstermine.

4. Perspektiven

Das Internet bietet nicht nur Chancen, sondern auch Risiken, wenn man das Internet nicht ernst nimmt. Hierfür dient die Musikindustrie als Beispiel. Der Ex-Deutschlandchef der Plattenfirma Universal, Tim Renner, wies bei einer Veranstaltung vor Verlegern darauf hin, dass Musik- wie Buchverlage klassisch vier Funktionen für ihre Urheber erfüllten: Sie agierten als Bank für die Urheber während des teuren und langwierigen Produktionsvorgangs, als Produzent während des aufwendigen Herstellungsvorgangs, als Vertriebseinheit und als Kommunikationsunternehmen. Durch das Internet würden alle vier Funktionen überflüssig: Die Produktion habe sich beschleunigt und verbilligt, der Vertrieb erfolge über das Internet und Kommunikation via Internet-Foren.
Dies habe dazu geführt, dass mittlerweile 50 % der Musiktitel heruntergeladen werden, zum Großteil illegal, was den Musikverlagen einen 40 %igen Umsatzrückgang in den letzten Jahren beschert und sie in ihrer bisherigen Funktion zumindest ernsthaft in Frage

gestellt hat. Auf den Einwand der Verleger, dieses Szenario betreffe doch vorrangig die Musikindustrie und nicht die viel stärker von der Haptik geprägte Buchbranche, erwiderte Renner, dass er ähnlich beschwichtigende Argumente vor wenigen Jahren auch von der Musikindustrie gehört habe, die sich mittlerweile ihre größten Krise seit Bestehen durchläuft. Angesichts der Möglichkeit von einrollbarem E-Paper, das in Kürze erhältlich ist, solle man sich auch als Buchverlag intensiv mit dem Internet beschäftigen. Man solle sich aber weniger mit den Gefahren, sprich mit verschärftem Kopierschutz, sondern mit den Möglichkeiten beschäftigen. Man solle Angebote legal schaffen, bevor sie illegal zugänglich seine. Man solle sich auf die Erwartungshaltung der Konsumenten einstellen, die sofortige und pausenlose Erreichbarkeit verlangten und dabei eine enge Betreuung wünschten, da die für das Internet typische große Vielfalt Bedarf nach Orientierung schaffe. Den Schwerpunkt der Online-Nutzung von Buchinhalten sah Renner eher auf dem Gebiet des Sach- und Fachbuchs, weniger auf dem Gebiet der Belletristik, dort allenfalls auf dem Gebiet der weniger anspruchsvollen Unterhaltung, z.B. bei Urlaubslektüre.

5. Rechtliche Situation bei Internetnutzung

Jede der aufgezeigten Nutzungsmöglichkeiten setzt voraus, dass den Verlagen, die Dritten Inhalte zur entgeltlichen Weitergabe an Kunden zur Verfügung stellen, diese Rechte auch gegenüber ihren Autoren zustehen.
Gesetzlich ist die Thematik in § 19 a UrhG zumindest erwähnt. Hier ist das Recht der öffentlichen Zugänglichmachung genannt und definiert als das dem Urheber zustehende Recht, sein Werk drahtgebunden oder drahtlos der Öffentlichkeit in einer Weise zugänglich zu machen, dass es Mitgliedern der Öffentlichkeit von Orten und zu Zeiten ihrer Wahl zugänglich ist.
Die grundsätzliche Belassung jener Rechte beim Urheber entspricht der Grundkonzeption des deutschen Urheberrechts, das vorsieht, dass alle Rechte, die nicht ausdrücklich bei Abschluss eines Nutzungsvertrages den Verwertern übertragen sind bzw. nach dem Vertragszweck als übertragen zu behandeln sind, beim Urheber verbleiben, sog. Zweckübertragungstheorie.
Nutzungsrechte für zum Zeitpunkt unbekannte Nutzungsarten konnten nach bisherigem Recht ohnehin den Verwertern nicht eingeräumt werden. Deshalb liegen üblicherweise sämtliche für eine Internetnutzung erforderlichen Rechte älterer Titel nicht bei den Verlagen sondern bei den Rechteinhabern, also Autoren und Agenten, und müssen nachträglich mühsam und meist kostenpflichtig eingeholt werden. Bei neuen Titeln werden diese Rechte möglichst vollumfänglich eingeholt. Die zu erzielenden Erlöse werden meist hälftig zwischen Verlag und Autoren geteilt, weil kostspielige Aufwendungen auf Verlagseite, anders als bei der klassischen Buchproduktion, nicht anfallen. An den Erlösen der klassischen Nutzung sind Autoren meist nur in Höhe von 10 % am Ladenpreis, sprich wegen der Rabattstruktur in Höhe von 20 % am Erlös beteiligt. Manche Autoren misstrauen jedoch einer Internet-Nutzung generell und verweigern jegliche Rechtseinräumung für dieses Gebiet.
Hier ein Beispiel für eine vertraglich zu vereinbarende Rechteklausel für Print-, E-Book und Audio- incl. Download-Nutzung von Buchrechten:

Der Autor überträgt dem Verlag

- das exklusive Buchrecht, d.h. das Recht, das Werk in beliebiger Form, Auflage und Menge zu vervielfältigen in jeder Buchausgabe und körperlichen elektronischen Ausgabe auf Datenträgern, beispielsweise Diskette oder CD-ROM DVD, oder sonstige digitale, analoge oder sonstigen Datenträger auf jede Art und Weise zu verbreiten. Diese Rechte umfassen beispielsweise die Veranstaltung von Hardcover-, Taschenbuch-, Paperback-, Sonder-, Reprint-, Schul-, Großdruck- oder (gekürzten) Digestausgaben, von Anthologien oder Gesamtausgaben. Zu den Vertriebswegen rechnen beispielsweise der Sortimentshandel, Mail Order, das Internet oder Sondermärkte.
- das Recht zum ganzen oder teilweisen Abdruck (z.B. als Vorabdruck oder als Nachabdruck) des Werkes oder von Teilen davon oder der nach ihm hergestellten Fassungen in eigenen oder fremden periodischen oder nicht-periodischen Druckschriften, auch als Fortsetzungsabdruck, sowie zur entsprechenden Einstellung in elektronische Medien, für Werbezwecke auch dann, wenn dafür Abdrucksvergütungen nicht erzielt werden.
- das exklusive Abrufrecht in jeder unkörperlichen elektronischen Ausgabe, d.h. das Recht der öffentlichen Zugänglichmachung des Werkes für nutzungsberechtigte Leser, in unkörperlicher Form, unabhängig von Art, Ort oder Medium des Abrufes und unabhängig von der Anzahl der Abrufenden oder der Anzahl der Abrufe. durch Online-Abruf und Wiedergabe des Werkes.
- das Recht der maschinenlesbaren Erfassung und elektronischen Speicherung des Werkes in einer Online-Datenbank, die der Verlag oder ein Dritter betreibt; weiterhin das öffentliche Angebot und die Bereithaltung des so gespeicherten Werkes oder von Werkteilen zum Online-Abruf; schließlich die Übermittlung (auch via Internet) des Werkes und dessen Wiedergabe am eigenen Bildschirm oder Lesegerät eines nutzungsberechtigten Lesers, etwa im Wege des e-books, einschließlich der Wiedergabe auf einem Multifunktionslesegerät wie etwa Handy, Palm, e-ink o.ä.
- das exklusive Hörbuchrecht in jeder Hörbuchfassung, d.h. das Recht zu Herstellung und Vertrieb des Werkes oder von Teilen des Werkes auf Vorrichtungen zur wiederholbaren Wiedergabe mittels analogen oder digitalen Bild- und/oder Tonträgern, z.B. Hörbücher, Audio-CDs, sowie das Recht zu deren Vervielfältigung, Verbreitung und öffentlichen Wiedergabe („Audio-Rechte").
- das Recht, die Vertragsaufnahmen in Datenbanken zu speichern und diese Nutzern mittels digitaler oder anderweitiger Speicher- bzw. Datenübertragungstechnik, mit oder ohne Zwischenspeicherung, derart zugänglich zu machen, daß diese von einem von ihnen individuell gewählten Ort und zu einer von ihnen individuell gewählten Zeit Zugang zu den Vertragsaufnahmen haben und dieses mittels TV, PC, Handy oder sonstigen Geräten mit oder ohne Draht bspw. via Internet, UMTS, Kabel, Satellit oder anderer Übertragungswege streamen und/oder downloaden und/oder wiedergeben können (Online-Recht);

6. Internetpiraterie

Wie die Musikindustrie leidet auch die Buchverlagsbranche an der Möglichkeit, Inhalte illegal aus dem Internet zu erhalten. Unser Verlag hat deshalb eine auf Pirateriefälle im Musikbereich spezialisierte Anwaltskanzlei mit der regelmäßigen Überwachung unseres Verlagsprogrammes auf Rechtsverletzungen im Internet beauftragt. Zu diesem Zweck arbeitet die Kanzlei mit einer Vielzahl von freien Mitarbeitern zusammen, die mittels spezialisierter Computerprogramme das WorldWideWeb nach unseren Büchern und Autoren durchsuchen, vor allem Online-Auktionshäuser und private Tauschbörsen. Entdeckte Angebote werden daraufhin überprüft, ob Rechtsverstöße vorliegen. Solche liegen etwa vor bei:
Druckereierzeugnisse: Hier gibt es Fälle von Herstellung und Verkauf von Raubkopien in elektronischer Form nach vorherigem Einscannen des Originals und des Vertriebs von illegalen E-Books auf CD-ROM oder mittels Versands als Datei per E-Mail oder in Papierform als Loseblattsammlungen von Kopien. Daneben gibt es selten gewordene Formen der klassischen Raubdrucke in Buchform, die übers Internet angeboten werden.
Hörbücher: Hier werden Raubkopien vornehmlich im mp3-Format hergestellt, die auf Computer-Festplatten, auf mp3-Playern (IPod) oder auf CD-ROM gespeichert werden und die Datenträger verkauft werden. Häufig werden die angebotenen Datenträger als angebliche Sicherungskopien zum Tauch oder Verkauf gestellt.
Statistische Angaben: Die von uns beauftragte Kanzlei ist für acht Buchverlagsgruppen sowie für alle großen Musikverlage tätig. 38 % der im Buchbereich verfolgten Rechtsverletzungen betreffen unsere Verlagsgruppe, obwohl wir nur über 12 % Marktanteil verfügen. Allerdings finden sich bei uns überdurchschnittlich viele anglo-amerikanische Bestsellerautoren, die bei Internetpiraten offensichtlich beliebt sind. 66 % der von der Kanzlei entdeckten Rechtsverletzungen spielen sich im Musikbereich ab, immerhin 34 % betreffen mittlerweile den Buchbereich. 64 % der Rechtsverstöße im Buchbereich betreffen E-Books, 19 % beziehen sich auf Hörbücher und 17 % auf Preisbindungsverstöße.
Während Online-Auktionshäuser üblicherweise bereitwillig Auskunft über Auktionsteilnehmer geben, ist dies bei privaten Tauschbörsen sehr viel schwieriger. Hier half kurzzeitig ein Auskunftsanspruch gegenüber Internet-Service Provider nach allgemeinen urheberrechtlichen Vorschriften, durchsetzbar sogar durch Einstweilige Verfügung, weil Tauschbörsen sehr kurzlebige Veranstaltungen sind. Ein solcher Anspruch auf Herausgabe von Daten potenzieller Anbieter von nicht-lizenzierten Inhalten wurde der Plattenfirma BMG vom LG München gegen einen Provider zugesprochen, vom OLG München aber vor kurzem abgelehnt. Auch das OLG Frankfurt verweigert Auskunftsansprüche die Durchsetzbarkeit.
Das Gericht lehnte die Pflicht eines Providers ab, einem Musikunternehmen den Namen eines seiner Kunden zugänglich zu machen, der über den Internet-Provider einen Musik-Server betrieb, von dem MP3-Musikdateien heruntergeladen werden konnten. Nach diesem Urteil (Az.: 11U 51/04) ist die Nennung des Kunden dem Internet-Dienstleister nicht zuzumuten. Die Plattenfirma hatte die illegale Downloadstation im Internet ausgemacht. Um herauszufinden, wer dahintersteckt, benötigte sie aber Angaben zur Identität des Betreibers. Als der Downloadbetreiber und der Service-Provider dem Wunsch der Plattenfirma nicht nachkamen, klagte das Unternehmen gegen den Provider, da er als Mitverantwortlicher an einer Rechtsverletzung zur Auskunft über Namen und Anschrift des Kunden verpflichtet sei. Der Grund für die

Zurückhaltung der Provider, ihre Kundendaten offen zulegen liegt nach Vermutung von Insidern darin, dass gerade die illegalen Download-Betreiber die besten weil häufigsten und dauerhaftesten Kunden der Provider sind.
Da der im Referentenentwurf vorliegende sog. Zweite Korb des Urheberrechts bislang keinen Auskunftsanspruch für derartige Fälle vorsieht, werden zahlreiche Interessenverbände versuchen, im laufenden Gesetzgebungsverfahren auf diese für Rechteinhaber untragbare Situation hinzuweisen.

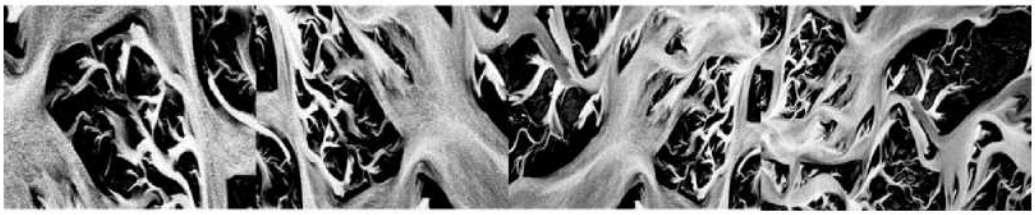
7. Urheberrechtsreformgesetz

Anfang dieses Jahres legte die Bundesjustizministerin ein Papier zu dem bevorstehenden Regierungsentwurf eines Gesetzes unter der Überschrift „Urheberrecht in der Wissensgesellschaft", auch Zweiter Korb genannt, vor. Der bereits im Jahre 2003 ins deutsche Urheberrecht aufgenommene sog. Erste Korb hatte eine EU-Richtlinie zum Urheberrecht in der Informationsgesellschaft umgesetzt und dabei vor allem Fragen des Kopierschutzes geregelt. Nach dem Subsidiaritätsgrundsatz ist der Erlass den Ersten Korb begleitender Regelungen der europarechtlichen Zuständigkeit enthoben.
Beim deshalb rein national zu entscheidenden Zweiten Korb geht es vor allem um Fragen der Privatkopie und deren heftig umstrittener, pauschalen Vergütung durch Geräteabgaben. Privatkopien sollen demnach auch weiterhin erlaubt sein, künftig macht sich aber strafbar, wer aus dem Internet offensichtlich rechtswidrig genutzte Vorlagen herunter lädt. Eine rechtswidrige Nutzung soll schon dann vorliegen, wenn jemand eine Original-CD oder eine für den Hausgebrauch erlaubte CD-Kopie („Sicherungskopie") zum Herunterladen ins Netz stellt. Daneben soll die Möglichkeit geschaffen werden, dass Urheber Verlagen Rechte an zum Zeitpunkt des Vertragsschlusses noch unbekannten Nutzungsarten einräumen. Zu Lebzeiten des Autors, der Rechte an noch unbekannten Nutzungsarten einräumt, hat dieser bis zum Beginn der Verwertung durch den Verlag die Möglichkeit zum Widerruf der eingeräumten Nutzung unbekannter Verwertungsarten. Die Erben des Autors allerdings verlieren das Widerrufsrecht allerdings.
Bislang gab es diese Möglichkeit nicht, so herrschte früher z. B. Streit darüber, ob ein Urheber, der einem Filmverlag Video-Rechte eingeräumt hatte, damit auch die Rechte an einer Nutzung für eine zum Zeitpunkt des Vertragsschlusses noch unbekannte DVD-Verwertung übertragen hatte.
In einem kürzlich in Deutschland Aufsehen erregenden Zeitungsbeitrag kritisierte der Nobelpreisträger Günter Grass die Möglichkeit, künftig Nutzungsrechte auch für zum Zeitpunkt des Vertragsschluss unbekannte Verwertungsarten zu übertragen. Ohne darauf hinzuweisen, dass auch weiterhin kein Urheber gezwungen ist, seine diesbezüglichen Rechte tatsächlich aus der Hand zu geben, stellt er fest, dass es wieder einmal die Künstler seien, deren Rechte als Urheber beschnitten oder nach ihrem Tod eliminiert werden sollen. Kann man hierbei Grass noch zugestehen, dass jener Punkt zumindest diskussionswürdig ist, geht seine Kritik an der künftig vorgesehen Regelung der Privatkopie wohl zu weit. Am historischen Beispiel „Der abenteuerliche Simplicius Simplicissimus" stellt er fest, dass manche Prosa nicht den Autor, sondern „Parasiten" reich mache. „Mit Hilfe neuer Medien" so fürchtet er, „feiert die Raubdruckpraxis des siebzehnten Jahrhunderts ungeahndet Wiederbelebung".
Für den belletristischen Buchbereich ist diese Befürchtung weit übertrieben, da der „Zweite Korb" nichts an der langjährigen Vorschrift ändert, wonach eine im

wesentlichen vollständige Privatkopie eines Buchs ohne Zustimmung des Berechtigten nur im Wege der schon seit dem Mittelalter gängigen Abschrift möglich ist. Daran, dass vermutlich auch nach Inkrafttreten des „Zweiten Korbs" wie bisher schon illegale Print- und Digitalkopien von Büchern hergestellt und vertrieben werden, vermag wohl kein Urheberrecht dieser Welt etwas zu ändern. Es liegt in der Natur der Dinge, dass von manchen Verletzern als Bagatelldelikte empfundene Rechtsverstöße vorkommen. Daran könnte selbst das von niemandem geforderte vollständige Verbot von Privatkopien nichts ändern.

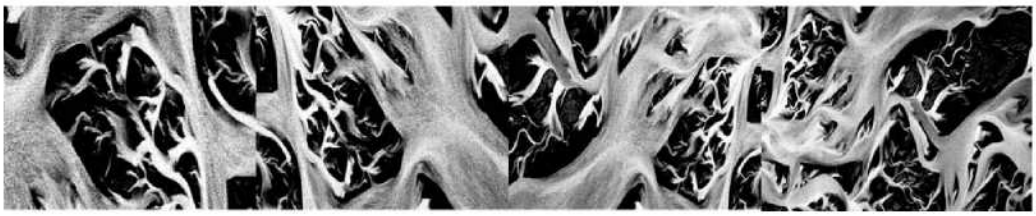
Curriculum Vitae

Anne Nina Schmid studierte Rechtswissenschaften in Regensburg, Perugia, München und Sydney. Tätigkeiten bei den Verlagen Süddeutsche Zeitung und Heinrich Bauer. In den Jahren 2001-2002 Mitarbeit in der Rechtsabteilung eines internationalen Film- und Merchandisingunternehmens. Seit 2003 Justiziarin der Verlagsgruppe Random House.



Sektion V

Netz – Zukunft – Sicherheit



Bad memories, bad dreams in library ICT security?

Dr. Julien Van Borm and Dr. Richard Philips, Chief librarian of the University of Antwerp and system manager of the library automation network organised by the University of Antwerp

Abstract

This paper describes the security procedures in Anet, the library automation network of the University of Antwerp in Belgium. It also explores the occasionally overhyped myths of ICT security in general using examples from the personal experience of the authors and a statement by the Gartner company.

Concern about data security is not new

Concern about data security in libraries is not new. Right from the beginning of the library automation era (the seventies of the past century), stories were told about lost punched cards and magnetic tapes. But even before that era a library was at risk of losing irreplaceable data. One of the authors of this article (J. Van Borm) had just started his library career at the University of Leuven–Louvain (at that time still a bilingual university). In the years previous to the splitting of this Belgian University into a Flemish and a French-speaking university the unrest among students of the two cultural groups was great. This unrest was combined with the general student unrest of 1968 throughout Europe and the world at large.

On the afternoon of October 17th 1969, the keeper of the catalogues came to see me and told me that two catalogue drawers full of written and typed catalogue cards were missing. These were in part irreplaceable since no duplicates existed for the titles kept in the over 300 faculty and departmental libraries. I soon discovered the relation between this fact and the general unrest at the university. On the morning of the same day, a student meeting had been held at the Faculty of Philosophy and Letters whereby the students had demanded the nomination of a Flemish librarian for the Central Library. At the same meeting action was announced against the library under the code name: "shoebox". For several days I tried to contact the authors of this action by strolling through the city of Leuven and visiting during and after work the pubs in which the student leaders of the Faculty of Philosophy and Letters were usually to be found. In vain! The drawers were only returned to the library in anonymously several weeks afterwards. Many years later I had a talk with one of the "perpetrators" of this act telling him that it almost had ended my library career. As a matter of fact, I got the information on the students meeting via a befriended student. She told me what had happened at that meeting, including the statement that a prominent Flemish professor had backed up the actions against the Central Library. Since I refused to reveal the name of the student who had passed on to me in confidence the information about the "shoebox" operation, I was accused by that same professor of spreading a defamatory statement. The university authorities were asked to put an end to my contract as an assistant librarian. The university authorities were wise enough not to accept the allegation and in doing so saved my library career. The lesson learnt: data loss can be lethal!

Another event took place several years later in 1986 at the University Library of Antwerp. The UIA library had started the automation of its catalogue pretty early in 1972 with the help of a small Oxford-based IT company called Oriel. In 1983, a contract was signed for an online integrated library automation system that was by that time already overdue. However, Oriel could not deliver the online system and the contract had to be aborted in 1985. The University of Antwerp then decided to go for an autonomous VUBIS installation. VUBIS[1], now distributed by GEAC, was at that time a still little known online library automation system. An ICT-trained member of staff was recruited, actually Dr. Richard Philips, the co-author of this paper, and a set of three PDP-11 minicomputers was installed to locally run the VUBIS system at the University of Antwerp. One afternoon the system started fading away. One after another the vital elements dropped dead and the risk of losing all the date became greater and greater at nightfall. Richard Philips, helped by one of the designers of the VUBIS system and an expert in the MUMPS database technology of those days, struggled almost throughout the night to stabilise the system and to prevent possible data loss. Both Richard and myself realised very well that a second "failure" so soon after the cancellation of the Oriel contract would lead to serious damage to the image of the library and most probably to a full stop of the ambitions of the library to operate its own library automation facility. The only thing I could do that afternoon and night was stand by and watch the lights of the PDP-11 fading and fetch some food and drink for the two IT specialists fighting the disaster. In the end, they managed to stop the degeneration to the system and saved almost all the irreplaceable data.

Bad memories, certainly! Bad dreams no! If all the prophets of doom were to be believed one had better not engage in (library) automation.

Gartner attacks overhyped security myths

In a recent statement Gartner, a US-based multinational ICT group, attacked five overhyped security myths[2].

- Internet Protocol (IP) telephony is unsafe;
- Mobile malware will cause widespread damage;
- "Warhol Worms" will make the Internet unreliable for business traffic and virtual private networks (VPNs);
- Regulatory compliance equals security;
- Wireless hot spots are unsafe.

"Many businesses are delaying rolling out high productivity technologies, such as wireless local area networks (WLANs) and IP telephony systems because they have seen so much hype about potential threats," said Lawrence Orans, principal analyst at Gartner. *"We've also seen the perceived need to spend on compliance reporting for Sarbanes-Oxley hyped beyond any connection with the reality of the legislation,"* added John Pescatore, vice president and Gartner Fellow. Gartner analysts examined the status of each of these over-hyped security risks. The full statement is to be found on the Gartner website[3]. An abridged version is given below.

[1] http://www.library.geac.com/page/home_LIB
[2] http://www.gartner.com/Init
[3] http://issj.sys-con.com/read/99106_p.htm

IP telephony is unsafe
"The reality is that security attacks are rare for IP telephony. Preventive measures for securing an IP telephony environment are very similar to securing a data-only environment".

Mobile malware will cause widespread damage
"The most effective approach to blocking mobile malware will be to block it in the network. Companies should ask their wireless service providers to document existing and planned capabilities. By the end of 2006, all wireless service providers should be required to offer over-the-air mobile malware protection".

Warhol Worms will make the Internet unreliable for business traffic and VPNs
One of the speakers at the conference Security in the Net organised by the Goethe Institut in Brussels referred to the dangers of a Warhol Worm infecting all unprotected systems on the Internet within minutes. The Gartner's answer is sharp and clear.

"The SQL Slammer Worm had a strong impact on the Internet in 2003.This is the only observed example of a Warhol Worm. Gartner analysts project that through 2007, the Internet will meet performance and security requirements for all business-to-consumer traffic, 70 percent of business-to-business traffic and more than half of corporate wide area network (WAN) traffic. Every organization should consider using Internet VPNs, and most should adopt them in some way".

Regulatory compliance equals security
"Regulations often provide a means to obtain funding for important security initiatives before incidents occur, but most regulations lead to increased reporting rather than increased levels of security. Regulations generally take more static looks at issues and generally don't lead to higher levels of security in proportion to the spending required to meet the letter of the law. The best way to increase enterprise IT security is to buy and build software that has fewer vulnerabilities".

Wireless hot spots are unsafe
Some of our libraries and information centres are already equipped with wireless hot spots and it certainly is one of the means to increase user-friendly systems and at the same time reduce the investment needed for installing and renewing the PC equipment in universities and libraries by relying on the laptops widely used by university students. The University of Antwerp is presently installing hot spots in all the reading rooms and in several other places on the university grounds.
Some fears exist about the dangers thought to be inherent in this new communication system. Here also, the recent report by Gartner is reassuring provided we take some good decisions.

"Uneducated consumers can fall prey to wireless hackers, but enterprises can equip and educate their mobile workers with the tools and knowledge to mitigate these threats and increase business productivity via hot spot usage".

The Gartner message alongside others is loud and clear: do not panic, take the necessary precautions and go on.

Data protection at the library of the University of Antwerp, Belgium

Over the past 20 years, the library of the University of Antwerp has created a large network of libraries depending upon the resources of Anet, the network of libraries around the university making use of the common hard- and/or software. This network presently encompasses over 50 libraries: university libraries, other research libraries and even the network of public libraries in the City of Antwerp.

The Anet network

Universities	• University of Antwerp • University of Hasselt
City of Antwerp	• AMVC – Flemish Cultural Archives • Antwerp Port Authority • Museum Plantin Moretus • Library of the OCMW-Antwerp • City Archives Antwerp • SBA – City Library
Hogescholen **Non-university higher education**	• Lessius Hogeschool • Hogeschool Antwerpen • Hogeschool Limburg • Karel de Grote Hogeschool • Plantijnhogeschool
Other libraries	• Barristers Association Antwerp • Theological and Pastoral Centre Antwerp • National Centre for Juvenile Literature Antwerp • KAVA - Royal Pharmaceutical Association Antwerp • Royal museum of Fine Arts Antwerp • POTVA – Police Training Centre Antwerp
Public libraries	• All public libraries in the city of Antwerp

What kind of precautions has Anet installed after the nearly disastrous start in 1986?

Environment
At the moment Anet uses six production servers with a variety of operating systems: Solaris, Windows 2000 Server and Linux. The production data on these servers (unique, irreplaceable data) totals 300 Gb.

Anet principles
The principles (P) for data security applied in Anet are the following:
P1. Accidents on the production servers hardly ever occur.
P2. The uptime of these servers is important but is not as stringent as e.g. in a hospital environment.
P3. Investment in backup facilities must be in relation to, and thus far lower than, investments in the production environment itself.

Four defence lines
Data protection is spread over several lines of defence. Defence line 1 is to be found in the very configuration of the servers.

- All the file systems with production information are mirrored, meaning that all data are always to be found on two disc arrays. This does not conflict with principle 3 (P3) as the acquisition cost of an extra array is minimal.
- The production data and software, independently of the operating system, is configured on all servers in absolutely the same way. An installation script is used for the software. It prescribes the autonomous installation and controls this operation using the technique of unit tests. This is in spite of the fact that the software for the Library Information (LIS): BROCADE uses some 200 Mb of code divided into 411 subprojects.
- As a result of this setup, the base line for the backup sits very high in the system. The backup does not have to deal with the underlying operating system. Only the production data require special attention. An extra advantage is that the backup data are "operating system agnostic". This is an extra asset for any possible recovery of the data and also for transferring data to a new server environment.

The second line of defence is a backup per machine on the hard disc itself. In accordance with P2 and P3, the production data are replicated to one of the discs of every machine. This is a truly quick backup (P3), but implies that for some time the machine is inaccessible for users, both end users and librarians. This is done on purpose to maintain the integrity of the backup data. This type of operation takes place at night and is part of a daily routine of automatic maintenance of the system initiated by the BROCADE LIS. In standard daytime, transactions in the LIS are carried out and written almost immediately in the local backup system.

A remarkable and not always well understood advantage of this backup phase is the automatic boot and reboot operation. Indeed, this activity, in full accordance with P2, halts the machine and reboots it immediately afterwards. Apart from some technical advantages, this approach also guarantees a faultless operation of the automatic procedures that are part of the foundation stones of the BROCADE LIS. This phase creates a maximum of 15 minutes of inconvenience for the user and runs overnight. However, our users overseas do not appreciate this rather limited time-out.

The third defence line starts immediately after the startup of the servers: the local backup is copied to a dedicated backup server (BS). In order to do so the local backup is partitioned into zones. Meta-information produced by the various servers and duplicated on BS describes these zones. A very important part of the meta-information provides information about the

backup zone under version control or without version control. Under version control, 12 versions are kept simultaneously for every zone on the BS: every one of the last 7 days, the last month and the last 4 quarters of the current year. The various versions not only guarantee the backup for hardware failures but also for human failures, which are unfortunately mostly only detected after some time. Zones under version control are without any exception primary data that cannot be found and retrieved elsewhere. Zones with temporary data, e.g. scans for document delivery which by definition and copyright law are not meant to be permanent, are not kept under version control. The data on the backup server have the following properties:

- Extended but purpose-oriented reporting about the various backups.
- The structure of the backup data is in line with, though not entirely identical to, the original data.
- Simple instruments of the operating system are to be used for setting back the backup data.
- Access to the BS by using SSH (Secure Shell) is quick and safe.
- The backup takes place under a fully operational system.
- All the data on all the servers are treated in the same way. This tremendously simplifies the documenting of the entire process. This BS is a Linux machine with a 3Tb capacity. This machine is heavily firewall-protected. The number of open communication ports is reduced to an access via SSH and is even then only accessible after RSA authentication.

The fourth defence line starts from the BS. The data on this machine is transferred to an NAS server at a remote site (another university campus) but within the same university Intranet. The aim is clear: avoid accidents that can destroy in one single blow all the servers of the LIS. However, at present not all data have yet been transferred. This is the temporary result of lack of bandwidth in the network and capacity on the NAS server.

Controls

The backups are under full control. The backup to the BS is integrated in the Probe system, a GSM-based warning system. If the backup of a zone is not finished within a predetermined period of time an SMS is automatically sent to the maintenance team carrying an ad hoc message. Manual checkup of the backup data is done as well. For the (near) future it is envisaged that an external organisation would check the integrity and the completeness of the procedures and backups.

Restore

Restoring the backup is another issue. The entire setup of the backup procedure has been designed so as to facilitate restore operation (in part, as well as full restoration of the data). Nevertheless, a full restore operation of all the data under the present hardware is a time-consuming operation. At the present moment, it would take roughly 24 hours. During that period the production servers would be largely unavailable forcing, for example, reading rooms to jump to the stand-alone circulation systems. This is the result of P1 and P2.

***

The Anet network of the University of Antwerp undoubtedly has tremendously enhanced data security, especially at an early stage in the design of the BROCADE LIS, but also in the way it has been implemented under the various operating systems in use. Anet refuses to believe that data can no longer be properly protected and agrees with the statements recently made by Gartner about overhyped security myths. Only the future will tell whether we were right not to have bad dreams for the future, based on bad memories from a far distant past.

Curriculum Vitae

Julien Van Borm (°1942) is presently chief librarian of the University of Antwerp in Belgium. He started his library career at the University of Leuven and the Université de Louvain (KUL-UCL) in 1967 and moved to Antwerp in 1972 where he has been the deputy director and later on the director of the library at UIA, a university institution that in 2003 became part of the newly integrated University of Antwerp. He is a member of several library organisations in Flanders, Belgium and the Netherlands and has been active in a series of international library projects in Europe and Africa.

Curriculum Vitae

Richard Philips (°1957) studied mathematics and informatics at the University of Ghent (Belgium). In 1986 he graduated in Ghent as doctor in sciences. In that same year he moved to Antwerp to become the system manager of what is called today Anet, the library automation network organised by the University of Antwerp. He also teaches telecommunication at the Library and Information Department of the University of Antwerp. He and his team developed the Brocade library automation system, currently in use by the University of Antwerp and a growing series of libraries in Belgium.

Final remarks: Net - Future - Security

Bernhard Smith, Head of Unit Interfaces, Directorate Information market, European Commission

We have now come to the very end of this conference and the organisers have asked me to summarise and close the meeting. So summarise I will - or a least try to! But first, I'm old enough to have some personnel reminiscences.
My background is in physics and I can remember when I met my first big mainframe computer in early-mid 70's. Even then you could feel the tension between those religious figures in white coats that tended the computer in its air-conditioned cathedral, and "user" or programmers. I remember when you went in with your set of punch cards prepared with loving attention – only to get them back sometime later (in my case a day later) with a printout and a cryptic error message saying that your program had failed.
Firstly, the priests of the computer did not care about the work you were doing nor the problems you had. Secondly, you had to take your error message and look up its meaning in the kind of IBM Bible hidden in one small room in the computer building (yes, computers needed whole building in those days). Thirdly, the error message pointed you to one of those equally incomprehensible expressions like "integer failed".
Is it not here that we find the origins of the battle between the programmer and the system operator, with the program/computer (and now network) resources as the battle ground? The originators of the first "viruses" were possibly just cpu "hogs", i.e. programmers writing and running large codes? In any case IBM may have a lot to answer for with its impossibly cryptic error messages that were more a provocation than a help.

I can still remember that it was fun to trick the computer to do things it did not want to do (or more correctly the system operation did not want you to do). Were not the very early computer games like Life or Spacewar the 1st viruses? They certainly were not work in the classical sense of the word, they consumed resources, and the programming ideas propagated at an impossible speed. Some people at the time said that Life consumed up to 20 % of the worlds cpu (around 1971). In any case the fact that these games were so successful was clearly seen as a victory of programmers over the system operator/owner.
Let me now fast forward, through the early days of viruses propagated on floppy disks, to today where, despite our security systems, fire walls, virus checkers, etc., we still get 100's of spam e-mails a week (or even every day). And where words like spyware and malware have become common terms in our everyday vocabularies. One key message from this meeting is that viruses are not going to go away, but, if anything, they will increasingly become more intelligent and more destructive.

So what did we all learn during these last 2 days?
From the first speaker Ernest Pöppel in his opening address we learned that the human brain is well defended against virus attack – but that our bodies' nervous system (i.e. input/output network) is not. It is interesting to see how modern day IT systems mimic biological systems and how we increasingly look to biology as a source of inspiration in trying to fight some problems such as viruses. If we do that we see that today's IT viruses are still rather

rudimentary. They are not "naturally" mobile in that they rely on their external environment (and often our own stupidity) for their mobility. They are not able to recognise energy/information as a resource to be stored for later use. They do not exploit addition sensory information that's now appearing in IT systems that would normally allow them to optimise their impact as a function of their external environment. Remember the "sit and wait" virus mentioned in one of the presentations – a virus that goes undetected and then wakes up months later and damages systems. Even that is dumb in that it is not really autonomous, self-aware and self-adapting. We don't yet have viruses that can run and hide! But we heard that the majority of really damaging viruses come out of university departments. And that tells us that new viruses will inevitably become more intelligent, be able to adapt and evolve, will learn to husband resources, migrate "natural", and understand their surroundings, and above all – will learn to optimise their destructive effects.

We also learnt that viruses are part of the emerging "e-war" – the information war. Both Fabio Ghioni from Telecom Italia and our white-hat hacker Jan Guldentops noted that so far viruses and hacking in general has not been really evil – but we all know that can't last!

Already today we learned that IT security is a big business cost, with physical protection and isolation as well as the increasingly centralised management and continuous monitoring and testing programmes. What we saw is that the effects of viruses are expensive in terms of IT budget/staff, in terms of company revenues, and in terms of organisations branding and marketing. We also saw that people don't want to talk about attacks (successful or unsuccessful). They deliberately choose not to publicise the damage caused. In addition companies "image" or "brand" is often high-jacked, e.g. we have all seen the dubious applications sending requests or product listing under a high-jacked company logo. And still companies react badly by ignoring this and claiming to be neither morally more financially responsible for the damage inflicted.

How would a library or museum react if their brand was high-jacked? Our Danish friend Bo Weymann gave us a first hand insight into the question. And it was not pretty to hear. Our friendly hacker Jan Guldentops also stressed this point – but from another perspective. He and I think rightly clamed that there was a place for the ethical tracker. That is not only to probe weaknesses but also to highlight and publicise those weaknesses, probably through a recognised pre-declaration procedure.

Throughout the 2-day meeting we had the opportunity to see – in a very practical away – how some libraries and other institutions are facing up to the security challenge.

What I retained from that was firstly the very broad-scale of the efforts made, secondly the considerable cost that must be associated with that effort, and thirdly the great body of expertise and skills that have been acquired. Again this effort is understandable – since libraries, research centres, etc are high-profile targets, and in some cases are by definition open locations. We heard that such sites often hold personal data, valuable experimental results, etc, and sensitive administrative information. We also heard that, perhaps, not enough is yet done to protect these "back-shop" operations. Again Jan Guldentops highlighted how easy it still was to find the weakest link and get past 400,000 € of security on the "front door" by spending 400 € to go through the back door. And another speaker stressed that we are in the near future going to be faced with a multitude of new challenges – the nomadic user with his desire for anytime/anywhere access groups collaborating over different locations, and the strong move towards a philosophy of openness. The same speaker mentioned that we could learn from the world of GRID's in their attempt to foster good security by making it easy. Sounds simple – but its true today that security measures are still far too complex, costly and, let's face it, 'high tech". What the GRID's approach offers for the future is easy cryptography along with a fine-again control of access rights.

What is clear is that our institutions, libraries, etc will be faced with a number of new security challenges in the coming years. Today more should be done to document and disseminate the valuable knowledge and experience already acquire in the larger organisations – and target those who are going to need it most - the smaller institutions – and, why not, even the individual citizen. We see today that librarians are looking to becoming both knowledge managers and at the same time more responsive to customer requirements. So all this leads me to ask if the future librarian should not become also a white hat hacker. Or, if nothing else, the source of knowledge and education for the citizen security, encryption, patches, etc. And, why not, the holder of the ethical high-ground in promoting information on security issues to the citizen.

For some of you this maybe a little over the top, but in a recent article in Edge, the Galen Law of the Small was discussed. It says that "small adjustments result in big changes". Another law is called Pöppel's Universal law – it asserts that "we take life 3 seconds at a time". So let's hope that this conference can be a catalyst for each and every one of us to make small changes to our daily practices – practices that can take just 3 seconds – and maybe that could produce big changes.

Let me close by saying that if I have not done justice to my task to summarise, at least let me do justice to the organisers of this conference. I would like to thank the Conferences sponsors – not only the wonderful organisation and welcome provided by the Goethe Institute here in Brussels - but also their collaborators the Bibliothèque Royale de Belgique, and the library in Jülich, Germany.

Kunstinstallation

Während der Tagung wurde eine Kunstinstallation zum Thema "Netzwerke" ausgestellt. Sie entstand durch Prof. Dr. Horst Halling in Zusammenarbeit mit Wilfried Stevens und Dr. Richard Patzak (Forschungszentrum Jülich). Die Kunstwerke sind in dem vorliegenden Proceedingsband vor den einzelnen Sektionen abgedruckt.

Kunstinstallation: Netzwerke

Die Installation bemüht sich um die Darstellung von Vernetzung, wie sie in Technik und Natur vielfältig auftritt. Die Bilder wurden aus Fotographien zusammengesetzt, wobei eine Kombination von Vergrößerungen eingesetzt wurde. Jeder Bildteil wird um etwa 40 % vergrößert und eventuell verkehrt an den kleineren Bildteil angefügt. Dadurch entsteht eine Kette von Vergrößerungen, die selbstähnlich sind und dadurch die Struktur des Netzes enthüllen. Als Netzwerke wurden folgende Themen gewählt: ein Spinnennetz, ein Netz von Herzkranzgefäßen, ein Netz von Kabeln, eine computererstellte Netzdarstellung und eine Landschaft von Sandbänken eines unregulierten Flusses.
Die zahlreichen Verästelungen, das Suchen und Finden von vergrößerten Strukturen, das Erkennen von Gemeinsamkeiten, von allem geht eine Faszination aus und vertieft den Begriff "Netz".

Mai 2005, H. Hallig

Schriften des Forschungszentrums Jülich
Reihe Bibliothek / Library

1. **Naturwissenschaft und Technik – nur für Männer? Frauen mischen mit!**
   Auswahl-Bibliographie Wissenschaftlerinnen (1999), 28 Seiten
   ISBN: 3-89336-246-0

4. **Schweißen & Schneiden**
   Wissenschaftliche Veröffentlichungen des Forschungszentrums Jülich (1997), 16 Seiten
   ISBN: 3-89336-208-8

5. **Verzeichnis der wissenschaftlich-technischen Publikationen** des Forschungszentrums Jülich
   Januar 1993 - Juli 1997 (1997), ca. 100 Seiten
   ISBN: 3-89336-209-6

6. **Biotechnologie**
   Wissenschaftliche Veröffentlichungen der Institute für Biotechnologie des Forschungszentrums Jülich
   Januar 1992 - Juni 1997 (1997), 48 Seiten
   ISBN: 3-89336-210-X

7. **Verzeichnis der wissenschaftlich-technischen Publikationen** des Forschungszentrums Jülich
   1997 bis 1999 (2000), 52 Seiten
   ISBN: 3-89336-260-6

8. **Kompendium Information**
   Teil I: Archive, Bibliotheken, Informations- und Dokumentationseinrichtungen
   Teil II: Ausbildungsstätten, Fort- und Weiterbildungsaktivitäten, Informationsdienste, Presse- und Nachrichtenagenturen, Verlagswesen und Buchhandel, Einrichtungen des Patent- und Normungswesen, Publikationen
   G. Steuer (2001), 1130 Seiten
   ISBN: 3-89336-286-X

9. **Die Zukunft des wissenschaftlichen Publizierens**
   Der Wissenschaftler im Dialog mit Verlag und Bibliothek
   Jülich, 28. bis 30. November 2001. 40 Jahre Zentralbibliothek. Konferenz und Firmenausstellung
   Tagungsprogramm und Kurzfassungen (2001), 50 Seiten
   ISBN: 3-89336-292-4

10. **Die Zukunft des wissenschaftlichen Publizierens**
    Der Wissenschaftler im Dialog mit Verlag und Bibliothek
    Jülich, 28. - 30.11.2001. Tagungsprogramm und Vorträge (2002), 184 Seiten
    ISBN: 3-89336-294-0 (broschiert)
    ISBN: 3-89336-295-9 (CD)

Schriften des Forschungszentrums Jülich
Reihe Bibliothek / Library

11. **Bibliometric Analysis in Science and Research**
Applications, Benefits and Limitations
2nd Conference of the Central Library, 5 – 7 November 2003, Jülich, Germany
Conference Proceedings (2003), 242 pages
ISBN: 3-89336-334-3

12. **Bibliometrische Analysen – Daten, Fakten und Methoden**
Grundwissen Bibliometrie für Wissenschaftler, Wissenschaftsmanager, Forschungseinrichtungen und Hochschulen
von Rafael Ball, Dirk Tunger (2005), 81 Seiten
ISBN: 3-89336-383-1

13. **VIRUS – Sicher im Netz?**
2. Internationale Konferenz zur Virtuellen Bibliothek des Goethe-Instituts Brüssel
Rafael Ball, Cornelia Röpke, Willy Vanderpijpen (Hrsg.)(2005), 137 Seiten mit beiliegender CD-ROM
ISBN: 3-89336-377-7

Organisatoren:

Goethe-Institut Brüssel, Belgien
Zentralbibliothek des Forschungszentrums Jülich, Deutschland
Bibliothèque Royale de Belgique/Koninklijke Bibliotheek van Belgie, Brüssel

In Zusammenarbeit mit:

Ambassade de France en Belgique, Botschaft der Bundesrepublik Deutschland, CICEB (Ceské Centrum, Det Danske Kulturinstitut, Instituto Cervantes, Istituto Italiano di Cultura, The Finnish Cultural Institute for Benelux, The Louvain Institute for Ireland in Belgium, Österreichisches Kulturforum), Information Society Technologies, ZKM (Zentrum für Kunst und Medientechnologie Karlsruhe)

Forschungszentrum Jülich
in der Helmholtz-Gemeinschaft

Band / Volume 13
ISBN 3-89336-377-7

Bibliothek
Library