ABSOLVENTEN NACHRICHTEN

Du!

Német-diplomások
Egyesülete
információs kiadványa

13. évfolyam/Jahrgang
Nr. 2. szám Juli 2006 július

Der Bundestags-präsident auf unserer 12. JAHRESKONFERENZ

Ehrengast unserer 12. Konferenz war der Präsident des Deutschen Bundestags, Herr Dr. Lammert. In seiner Eröffnungsrede gab er eine kurzweilige Übersicht der ungarisch-deutschen Beziehungen im Bereich Kultur aus den letzten Jahrhunderten. Anschließend waren Vorträge über vier spannende Gebiete der Informatik im Alltag zu hören. Die Fragen, die zahlreich aus dem Publikum gestellt wurden und die lebhaften Gespräche im Anschluss an die Veranstaltung bewiesen, dass das Thema unabhängig von Beruf, Alter, Geschlecht oder Interesse von den Mitgliedern unseres Vereins sehr positiv aufgenommen wurde.

KULTURFRÜHLING
Német kulturális és művelődési hetek
Deutsche Kultur- und Bildungswochen

FESTREDE

des Bundestagspräsidenten DR. NORBERT LAMMERT in Budapest am 22. April 2006 vor der Jahreskonferenz des Vereins Deutscher Akademiker aus Ungarn, welche in Zusammenarbeit mit dem Altstipendiatenclub der Hanns-Seidel-Stiftung stattfand.

Meine Teilnahme an Ihrer Veranstaltung fügt sich ein in eine Reihe von Terminen, die ich an diesem Wochenende in Budapest wahrnehme und die, keineswegs zufällig, ausnahmslos alle mit den kulturpolitischen Beziehungen zwischen unseren Ländern zu tun haben. Insofern hat es schon eine innere Logik, dass in der in Ihrem Programm angekündigten Festrede ausschließlich von den kulturellen und akademischen Beziehungen zwischen Deutschland und Ungarn die Rede ist, als ob es politische und wirtschaftliche Beziehungen gar nicht gäbe. Die gibt es selbstverständlich auch, und sie sind ähnlich bemerkenswert wie die kulturellen und akademischen Beziehungen. Aber dass letztere inzwischen einen eigenen Stellenwert, einen eigenen Rang gewonnen haben, das gehört auch nach meiner Empfindung durchaus zu den Errungenschaften der jüngeren Entwicklung. Ich bin Ihrem Verein ausgesprochen dankbar, dass er sich in einer besonderen Weise und besonders erfolgreich darum bemüht, Ihre eigenen biographischen Erfahrungen zur Grundlage eines gemeinsamen Engagements zu machen, das sich gerade diesen kulturellen, bildungspolitischen, akademischen Beziehungen zwischen unseren Ländern widmet.

Im Freundschaftsvertrag zwischen Deutschland und Ungarn – oder, wie er genau heißt, dem „Deutsch-Ungarischen Vertrag über freundschaftliche Zusammenarbeit und Partnerschaft in Europa“ aus dem Jahr 1992 ist von „in Jahrhunderten gewachsener traditioneller Freundschaft zwischen beiden Ländern und Völkern“ die Rede. Und es gehört vielleicht schon zu den gelegentlich vorschnell für selbstverständlich gehaltenen Besonderheiten der deutsch-ungarischen Beziehungen, dass eine solche Bemerkung kaum noch jemand wahrnimmt, weil der Hinweis auf diese traditionell freundschaftlichen Beziehungen zwischen unseren Ländern für kaum noch aufregend gehalten wird. Mindestens im Kontext der deutschen Geschichte ist das aber eine aufregende Bemerkung, denn mir fallen nicht viele Länder in Europa ein, von denen wir das in gleicher Weise behaupten können, schon gar nicht über einen Zeitraum von über 1000 Jahren. In diesen 1000 Jahren hat es vielfältige Beziehungen und Kontakte gegeben, die im übrigen in beiden Fällen, Deutschland wie Ungarn, sich zum größeren Teil auf einen Zeitraum beziehen, in dem unsere jeweiligen Länder die Souveränität von Nationalstaaten gar nicht erreicht hatten, wie es ja überhaupt zu unserem gemeinsamen Schicksal gehört, dass Ungarn wie große Teile Deutschlands jahrhundertelang von Österreich dominiert wurden. Das hat uns offenkundig auch zusammengeschweißt und schafft eine nachhaltige Motivation für die Bewältigung der gemeinsamen Zukunft.

Auch wenn man der Versuchung widersteht, einen großzügigen Blick zurück in eine eindrucksvolle gemeinsame Vergangenheit zu werfen und in der unmittelbaren, auch noch die eigene Lebenserfahrung prägenden Vergangenheit bleibt, dann stößt man wieder auf eine Besonderheit in den deutsch-ungarischen Beziehungen, für die es eine unmittelbare Parallele zwischen zwei anderen europäischen Ländern wiederum nicht gibt, und zwar am Ende eines außerordentlich komplizierten, grausamen, blutigen Jahrhunderts, an dessen Verlauf Deutschland, wie jeder weiß, maßgeblichen Anteil hatte, mit der Folge, dass die zweite Hälfte des 20. Jahrhunderts von einer Teilung Europas gekennzeichnet war. Dass am Ende ausgerechnet dieses 20. Jahrhundert

dieser Kontinent wieder zusammengefunden hat und nun wieder zusammenwächst – politisch, wirtschaftlich, kulturell – das hat wieder in einer besonderen Weise etwas mit Deutschland und Ungarn zu tun. Denn es ist ja keine Übertreibung, sondern die schlichte Wahrheit, was Helmut Kohl formuliert hat, nämlich dass der erste Stein aus der Berliner Mauer in Ungarn herausgebrochen worden ist. Und dass mit der Durchschneidung der Stacheldrahtzäune zwischen der ungarischen und der österreichischen Grenze die Mauer, die Trennung in Europa irreversibel aufgehoben wurde, von der viele schon geglaubt hatten, dass sie nie mehr zu überwinden sei. Ich persönlich gehöre übrigens zu denjenigen, die das nicht nur für ein herausragendes Ereignis oder gar für selbstverständlich halten, sondern für eine grandiose Errungenschaft unserer gemeinsamen Geschichte. Und ich hoffe, dass es so bleibt. Jedenfalls weiß ich, dass diese Erfahrung des Jahres 1989 und der Beitrag, den Ungarn für die Überwindung der Spaltung Deutschlands geleistet hat, nicht nur im Gedächtnis der Deutschen fest verankert ist, sondern auch in der Seele unseres Landes. Aber weil es leider so ist, dass wir uns sehr schnell auch an außergewöhnliche Veränderungen gewöhnen, muss man solche Erfahrungen aktiv bewahren, im Bewusstsein halten, um daraus auch für die Zukunft Funken schlagen zu können. Ich habe persönlich keinen Zweifel daran, dass unsere Enkel wahrscheinlich noch mehr als unsere Kinder uns einmal nach den Erfahrungen der späten 80er und 90er Jahre des 20. Jahrhunderts fragen werden, weil diese doch ganz offenkundig zu den aufregendsten Phasen der europäischen Geschichte und damit der deutschen Nationalgeschichte wie der ungarischen Nationalgeschichte gehören. Auch dann wird es darauf ankommen, deutlich zu machen, dass das, was sich in den extrem kurzen Zeiträumen an – im wörtlichen Sinne – revolutionären Veränderungen abgespielt hat, nicht über Nacht über uns gekommen ist, sondern dass es Voraussetzungen hatte; und dass zu den Voraussetzungen dieses großen Veränderungsprozesses, der schließlich im Fall der Berliner Mauer kulminierte, natürlich der Volksaufstand in Ungarn 1956 gehört, dessen 50. Jahrestag Sie und wir in diesem Jahr begehen, ebenso wie der Prager Frühling 1968. Wenn es so etwas wie Pyrrhussiege gibt, dann gehören für mich der Prager Frühling wie der Ungarische Volksaufstand gewissermaßen zu den Pyrrhusniederlagen. Aus dem Scheitern dieser damaligen Aufstände ist die Substanz gewachsen, die schließlich die Veränderungen so unvermeidlich gemacht haben, die dann Ende der 80er Jahre, Anfang der 90er Jahre stattgefunden haben. Dazu gehört als drittes großes Ereignis die Solidarnosc und das, was sich in Danzig und Warschau daraus entwickelt hat. Mit anderen Worten: die Berliner Mauer ist nicht voraussetzungslos gefallen, sondern sie ist gefallen als Folge einer Vielzahl von einzelnen Anläufen und Bewegungen, die jede einzelne für sich allein nicht ausgereicht hätten, die aber in der Entschlossenheit, auch Scheitern nicht als endgültig hinzunehmen, sondern immer wieder neu

anzurennen, das Ergebnis möglich gemacht haben, das wir heute für eine ganz grundlegende Veränderung der europäischen Geschichte, aber eben nicht für selbstverständlich halten dürfen.

Vielleicht wissen es von Ihnen nicht alle, deswegen trage ich es gerne vor, dass wir am Reichstagsgebäude in Berlin aus Anlass des 3. Jahrestages der Öffnung der Grenze zwischen Ungarn und Österreich eine Plakette angebracht haben, um auf diesen Zusammenhang aufmerksam zu machen. Und wenn man selber schon nicht aktiv gestaltend an den großen Veränderungen beteiligt war, freut man sich, wenn man wenigstens an deren Erinnerung einen kleinen Anteil haben kann. Ich bin häufig ganz berührt, wenn mich Staatspräsidenten oder Parlamentspräsidenten aus anderen Ländern auf diese Plakette ansprechen und auf den exklusiven Status, den wir ganz offenkundig in unserer eigenen jüngeren Nationalgeschichte den deutsch-ungarischen Beziehungen beimessen. Und dann erläutere ich gerne, welcher Zusammenhang hier tatsächlich nach unserer Wahrnehmung und nach unserer Erfahrung besteht. Diese Plakette sagt ausdrücklich, sie sei ein Zeichen der Freundschaft zwischen dem deutschen und ungarischen Volk für ein vereintes Deutschland, für ein unabhängiges Ungarn, für ein demokratisches Europa. Und nun kommt es darauf an, was wir aus dieser Geschichte machen. Ich behaupte nicht, es hätte in der jahrhundertelangen europäischen Geschichte nicht auch andere Phasen für Anläufe zu großen Veränderungen gegeben. Aber es hat nie zuvor eine Situation gegeben, in der so viele europäische Staaten in einer auch nur annähernd vergleichbaren Weise gleiche Chancen der Partizipation an der Gestaltung der gemeinsamen Zukunft gehabt hätten und in der die Voraussetzungen für eine gleichberechtigte, gemeinsame Entwicklung in die Zukunft hinein ähnlich gut waren wie jetzt am Beginn des 21. Jahrhunderts. Alle anderen Anläufe für transnationale Zusammenschlüsse fanden unter den Bedingungen der Überlegenheit einer Nation gegenüber anderen statt. Das neue Europa entsteht unter völlig anderen Vorzeichen. Es gibt keinen Führungsanspruch eines Landes, es gibt keine dominierende Metropole. Dieses Europa entsteht multilateral, dezentral, föderal, mit all den Komplizierungen, die sich daraus ergeben. Jeder, der jemals auch nur in der Nähe irgendeines europäischen Gremiums gesessen hat, weiß, dass das nicht nur gemütliche Veranstaltungen sind. Und welche handfesten Komplikationen sich daraus ergeben, dass da eben nicht der eine das Sagen hat und die anderen das mit einer Mischung aus Einsicht und Verzweiflung abnicken. Was diese Art von erzwungener Mitwirkung angeht, haben übrigens die Ungarn wie die Menschen in der DDR jahrzehntelange bittere Erfahrungen hinter sich. Dies macht auch hinreichend klar, warum der Ehrgeiz gerade der neuen Mitgliedstaaten der Europäischen Gemeinschaft, die gewonnene Souveränität nun auch wahrzunehmen, mindestens so ausgeprägt ist wie der Ehrgeiz von Franzosen, Briten, Spaniern oder Iren, was wiederum das Zustandekommen europäischer Vereinbarungen nicht immer erleichtert, aber den qualitativen Veränderungsprozess verdeutlicht, den wir hier miteinander geschafft haben. Dass wir uns heute an dieser Weggabelung der gemeinsamen Geschichte befinden, hat nach meiner festen Überzeugung mindestens so viel mit Kultur wie mit Politik zu tun. Denn dass dieser Kontinent nicht längst ein für alle Mal auseinandergefallen ist, ist im Kern die Folge der gemeinsamen kulturellen Substanz. Es ist eben trotz gigantischer politischer Verirrungen, trotz heftiger ökonomischer Wettbewerbssituation nach wie vor mehr an Gemeinsamkeit vorhanden als an Trennendem. Deswegen müssen alle diejenigen – mit welcher Aufgabe und in welchem Teil unseres gesellschaftlichen Gefüges auch immer –, die an der Zukunftsperspektive ein Interesse haben, dieses Gemeinsame pflegen. Also bin ich heute morgen auch besonders gerne hier, weil ich weiß, dass dies ein Verein ist, der sich das buchstäblich auf die Fahne geschrieben hat und wo der Ertrag dieser Erfahrungen ein so fester

Bestandteil der eigenen Biographie ist, dass man nicht nur die Mitglieder dieses Vereins nicht davon überzeugen muss, wie wichtig solche Verbindungen sind, sondern dass sich daraus für viele auch eine Motivation ergibt, andere von der Nützlichkeit, von der Wichtigkeit solcher Kontakte und Beziehungen zu Überzeugen.

Ich freue mich, dass die Beziehungen zwischen unseren beiden Ländern gerade mit Blick auf Kultur und Bildung in den vergangenen Jahren immer dichter geworden sind. Ich habe gerade gehört, dass es leider immer seltener vorkommt, dass Ungarn Vollstudien in Deutschland absolvieren. Das muss mir schon deswegen einleuchten, weil das für deutsche Studenten im Ausland in gleicher Weise zu beobachten ist. Ich halte es aber auch nicht für die entscheidende Frage der Zukunft, ob jemand ein komplettes Studium statt im Heimatland in irgendeinem Nachbarstaat absolviert. Aber dass möglichst viele neben den Erfahrungen in der eigenen Umgebung auch Erfahrungen im Ausland sammeln und auf diese Weise nicht nur akademische, sondern auch Lebenserfahrung, zusätzliche Einsichten und Erfahrungen gewinnen, das halte ich schon für eine wichtige gemeinsame Aufgabe. Und wenn man die Größenordnung betrachtet, liegt Ungarn nach wie vor in der Spitzengruppe aller bilateralen Programme. Wir haben nach wie vor Hunderte – wenn nicht Tausende – von Stipendiaten und Studenten und Austauschschülern aus Ungarn in Deutschland. Es gibt ein starkes Engagement der deutschen Kulturinstitutionen hier im Land. Es gibt eine Auslandsschule hier in Budapest, die zu den besten – jedenfalls vom äußeren Erscheinungsbild – gehört, die ich überhaupt in der Welt gesehen habe. Ich habe sie kurz nach der Eröffnung einmal besucht und spontan gedacht: Da hätte ich meine Schulzeit auch gerne verbracht, nicht nur mit Blick auf die Lage und das architektonische Konzept, sondern, wie mir von allen Seiten bestätigt wird, auch was den Ruf dieser Schule mit Blick auf Kompetenzen und Qualifikation betrifft. Wir haben vorhin kurz darüber gesprochen, dass wir aus vielen Gründen uns in einer Phase befinden, in der die Bildungssysteme weltweit expandieren und in der es auch ein überragendes Interesse daran gibt, dass der Anteil der jungen Menschen, die höhere Qualifikation erwerben, von Jahrgang zu Jahrgang möglichst immer größer wird, was viele, wiederum ökonomische Hintergründe hat. Aber wir müssen gerade, weil das so ist, um so sorgfältiger darauf achten, dass die Ausweitung mit Blick auf die Quantitäten nicht auf Kosten der Qualitäten geht. Hier besteht ein akutes Risiko, was ich leider auch mit Blick auf deutsche Bildungseinrichtungen bestätigen muss. Es ist viel einfacher, die Anzahl der Abiturienten pro

Jahrgang nach oben zu treiben, schon gar in einem staatlich dominierten Bildungssystem, wo der Staat selber die Standards setzt, mit denen er insofern beliebige, politisch gesetzte Quoten erreichen kann. Und wenn sich ein staatliches Bildungssystem zum Ziel setzte, dass 80% oder 90% jedes Jahrgangs die allgemeine Hochschulreife erwerben müssten, ist die Erreichung dieses Ziels technisch mühelos zu erreichen, indem die Standards entsprechend abgesenkt werden. Genau das kann aber nicht die Lösung der Herausforderungen sein, vor denen wir stehen. Die Justierung zwischen den quantitativen und den qualitativen Anforderungen unserer Bildungssysteme, übrigens von Kindergärten angefangen bis zu den Hochschulen und den Forschungseinrichtungen, wird eine der zentralen Herausforderungen der Zukunft sein müssen. Auch dafür brauchen wir verstärkt internationale Kooperation. Das Risiko, dass die Ausweitung von Quantitäten auf Kosten der Qualität geht, ist um so höher, je mehr sich solche Entwicklungen allein in nationalen Kontexten abspielen. Sobald sie durch internationale Kooperationen begleitet und damit herausgefordert werden, sinkt das Risiko, weil man sich internationalen Vergleichen stellen muss. Deswegen haben wir ein vitales Interesse an der Intensivierung solcher Kooperationen des Austausches, sowohl während des Studiums wie auch in den professionellen Phasen danach. Jedem von uns fallen jetzt Felder ein, in denen man sich eine Ausweitung vorhandener Kooperationen gut vorstellen könnte, mir auch. Die Phantasie ist da in der Regel ausgeprägter als die verfügbaren Ressourcen. Wir werden auch auf neue Kooperationsformen achten müssen, um die notwendigerweise immer begrenzten Ressourcen durch Bündelung zu optimieren. Ich freue mich, dass es in immer stärkerem Maße gelingt, neben den klassischen Finanzierungsquelllen, also in der Regel öffentlichen Haushalten des Bundes und der Länder, zunehmend Unternehmen und Verbände für solche Kooperationen zu gewinnen, die mit eigenen, zum Teil beachtlichen Mitteln, in solche Kooperationen mit einsteigen. Sie täten es übrigens nicht, wenn sie das nicht für ein vitales eigenes Interesse hielten. Es ist also nicht nur eine karitative Bewusstseinsveränderung, sondern eine Wahrnehmung wohlverstandener eigener Interessen, was ich ohne jeden Unterton des Vorwurfs sage. Je mehr Unternehmen begreifen, dass sie an solchen Entwicklungen ein nicht weniger ausgeprägtes Interesse haben müssen als amtierende Regierungen in Nationalstaaten oder Parlamente, desto größer sind die Aussichten, dass sich solche Kooperationen auch in Zukunft weiterentwickeln und immer mehr Betriebe und Unternehmen daran teilhaben. Ich freue mich, dass das nicht nur für Kooperationen im akademischen Bereich und im Bildungsbereich zunehmend gilt, bei denen dieses vitale Interesse relativ deutlich auf der Hand liegt, sondern dass es zunehmend auch für kulturelle Aktivitäten zu beobachten ist, bei denen es ein eigenes wirtschaftliches Interesse auch bei mittelfristiger Betrachtung nicht gibt. Deswegen gilt dieser Art von Zusammenarbeit mein besonderer Respekt.

Mein Besuch findet ja auch deswegen an diesem Wochenende statt, weil im Rahmen des Deutschen Kulturfrühlings heute abend ein besonderes, herausragendes Ereignis stattfindet mit dem Konzert der Zwölf Cellisten der Berliner Philharmoniker. Auch dieses Ereignis wäre allein aus den finanziellen Zuschüssen des Auswärtigen Amtes nicht zustande gekommen, und dass es zustande kommt, ist hier wie bei anderen Kulturereignissen dieser Stadt wie in Berlin auch eine sympathische Folge des immer selbstverständlicher werdenden Zusammenwirkens von öffentlichen und privaten Händen, die Ereignisse möglich machen, die weder der eine noch der andere alleine realisieren könnte.

Ich will eine Schlussbemerkung machen, von der ich mir wünsche, dass vielleicht auch Sie mit Ihrem Verein sich an der Umsetzung dieser Überlegung nach Ihren Möglichkeiten ein bisschen beteiligen. Ich habe zu Beginn von den Besonderheiten der deutsch-ungarischen

Beziehungen gesprochen, von denen ich meine, dass sie nicht nur für die Vergangenheit nachweisbar sind, sondern dass sie auch für die Zukunft fruchtbar gemacht werden sollten. Und da gibt es in unmittelbarer Zukunft eine Zielmarke, die, wie ich finde, eine besonders naheliegende gemeinsame Orientierung sein könnte. Das ist das Jahr 2010, wenn Ungarn und Deutschland die europäische Kulturhauptstadt stellen, Pécs für Ungarn und das Ruhrgebiet in Deutschland. Nach meinem Verständnis ist diese Idee einer jährlichen Kulturhauptstadt Europas – die sich ja jetzt erst in der allerjüngsten Vergangenheit durch Doppelbenennungen vervielfältigt hat, was nun wiederum mit dem Zusammenwachsen Europas und der Überwindung der Trennung zwischen einem östlichen und westlichen Teil ursächlich zusammenhängt – überhaupt nur dann sinnvoll, wenn es nicht als einmaliges jährliches Ereignis missverstanden wird. Die Konzentration von spektakulären Opern- und Theateraufführungen, Konzerten usw. in einem einzigen Jahr rechtfertigt den Aufwand nicht, der dafür häufig getrieben wird. Der Aufwand rechtfertigt sich aber dann, wenn die Strecke bis zum Jahr 2010 für eine Festigung des Stellenwertes von Kunst und Kultur für unsere Lebenswirklichkeit genutzt wird und wenn sich aus den Aktivitäten, die für dieses Jahr vorbereitet werden, dann nachhaltige Veränderungen für die Zukunft ergeben. Und da fiele mir manches ein, jedenfalls mit Blick auf die deutsche Kulturhauptstadt, und möglicherweise gilt ähnliches auch für die ungarische Kulturhauptstadt, was man im Blick auf das Jahr 2010 jetzt anpacken kann. Ich fände es außerordentlich reizvoll, wenn wir das in einer deutsch-ungarischen Kooperation täten. Wenn sich daraus ab sofort in den Jahren 2006, 2007, 2008, 2009 deutsch-ungarische Kooperationen in diesem Bereich von Kultur und Bildung und akademischer Zusammenarbeit ergäben, die dann im Jahre 2010 gewissermaßen „europaweit ausstellungsreif“ würden als Leuchtfeuer, als Orientierungsfeuer für die Zukunft. Das kann, wie gesagt, niemand alleine realisieren, auch nicht die deutsche oder die ungarische Regierung, und schon gar nicht die Stadtverwaltung von Pécs oder von Essen, sondern das muss, wenn überhaupt, ein großes gemeinsames ehrgeiziges Engagement von vielen Beteiligten werden.

Ich hoffe, Sie empfinden es nicht als groben Missbrauch einer Festrede, die eigentlich ein paar unverbindliche Bemerkungen zum Stand der akademischen und kulturellen Beziehungen zwischen unseren Ländern machen sollte, wenn ich zum Schluss ausdrücklich um dieses Engagement werbe und sage: Wenn uns die Beziehung zwischen unseren Ländern im allgemeinen, die Kulturbeziehung zwischen unseren Ländern im besonderen so wichtig sind, wie wir gerne behaupten, dann müssen wir bei gegebenen Anlässen den Nachweis führen, dass wir daraus etwas machen wollen. Ich bin jedenfalls zu jeder Zusammenarbeit in diesem Kontext gerne bereit, bedanke mich bei Ihnen sehr für die Einladung zu Ihrem diesjährigen Jahrestreffen und wünsche dem weiteren Verlauf dieser Veranstaltung guten Erfolg und hoffe, dass auf dieser zuletzt angedeuteten Strecke sich noch vielfältige Gelegenheiten zur Begegnung und Vertiefung und Konkretisierung dieser Überlegung ergeben.

Herzlichen Dank.

NANOTECHNOLOGIE – hilft sie, die DIGITALE KULTUR zu bewahren?

DR. MOJZES IMRE
– Technische und Wirtschaftswissenschaftliche Universität Budapest

Auch unsere tagtäglichen Erfahrungen zeigen, dass wir uns sowohl bei unserer Arbeit, als auch im Privatleben immer mehr auf die Möglichkeiten der Informatik und der Telekommunikation stützen. Diese Geräte dienen uns mit einer ständig steigenden Intelligenz, von Fall zu Fall bieten sie sogar Leistungen, die wir überhaupt nicht in der Lage sind anzuwenden. Hinsichtlich ihrer Funktionsweise nutzen diese Geräte in ihrem Inneren die sog. digitale Technologie. Es ist interessant, dass wir uns in unserer Denkweise sehr oft der Gegenüberstellung zweier Sachen bedienen – wie z.B. ja-nein, schwarz-weiß, ying-yang –aber die Elektrik anfangs als analoge Technik, d.h. als kontinuierliches Signal angewendet wurde. Die Digitalisierung, die eine Erfindung aus der Mitte des 20. Jahrhunderts ist, trat danach immer mehr in den Vordergrund. Unsere Empfindung, unsere Sinnesorgane empfangen zwar ständig die Signale der Außenwelt und unser Gehirn verarbeitet diese, doch die vom Menschen geschaffenen, wirklich erfolgreichen elektronischen Sensoren produzieren digitale Signale. Wir wandeln dementsprechend die analogen Signale der Welt in einen Signalstrom um, der schon mit Signalen wie hoch-niedrig, groß-klein usw. beschrieben werden kann.

Die Entwicklung der Mikroelektronik zeigte auch, dass die Speicherung der Signale unter optimalen Bedingungen in der digitalen Form stattfindet. Dies kann auch so veranschaulicht werden, dass sich eine mit einer Kugel markierte Information entweder auf dem obersten Regal oder auf dem untersten befindet. Die elektronische Version dieser Analogie ist dann der Zustand, in dem wir für die Realisierung einen Transistor einsetzen. Der Transistor, der 1948 zur gleichen Zeit wie die Kreditkarte erfunden wurde, ist als ein Schalter mit zwei Zuständen zu sehen, wie ein Stromschalter, der sich entweder im eingeschalteten oder ausgeschalteten Zustand befindet. Es ist einfach nachvollziehbar: je mehr solche Schaltelemente, eigentlich elementare Speicherfächer, wir besitzen, desto mehr digitale Signale können wir speichern. Dieses Beispiel kann folgendermaßen veranschaulicht werden: je mehr Signale wir in digitale Signale umwandeln, desto mehr solche elementaren Speicherzellen brauchen wir für die Speicherung.

Es gibt noch viele weitere Prinzipien, nach denen noch Speicherelemente geschaffen werden können. Eine weit verbreitete Form ist z. B. die Magnetspeicherung, die z. B. bei den Tonbändern und den Disketten realisiert wird.

Die Entwicklung der Mikroelektronik in den letzten Jahrzehnten führte dazu, dass wir Speicher aus Silizium herstellen können, die eine sehr große Dichte an solchen Elementen vorweisen. Das Silizium stellt etwa ein Viertel der Masse des Globus dar, d.h. bei der Informationsspeicherung dieser Art zeichnen sich

keine Rohstoffgrenzen ab. Dank der Mikroelektronik ist dieses Material – das Einkristallsilizium – das vollkommenste und reinste durch den Menschen hergestellte Material. Wir können uns das so vorstellen, dass in einem zwei Meter hohen Einkristall mit dem Durchmesser einer Pizza kein einziger Kristallfehler vorkommt. Und diese Eigenschaft konnte bereits erreicht werden, obwohl die Herstellungstechnologie erst sechzig Jahre alt ist – die Qualität übertrifft jedoch bei weitem die des Kupfers (Kupferzeit 4 bis. 2. Jahrtausend v. Chr.) und des Eisens (Eisenzeit: Mitte des 2. Jahrtausends v. Chr.), trotz der langjährigen Produktionserfahrungen mit diesen. Dies ist also das Material, dessen Reinheit auch die der Medikamente bei weitem übertrifft. Wenn wir auf den entsprechend verarbeiteten dünnen Scheiben dieses Materials die oben genannten Transistoren unterbringen, können wir eine Einheit zur Informationsspeicherung schaffen, die in einer unglaublichen Dichte die Informationen speichert. Die Menge der auf diese Art und Weise hergestellten Transistoren können wir uns so vorstellen, dass 2004 weltweit auf jedes einzelne produzierte Reiskorn 100 Stück hergestellte Transistoren kamen. Wir brauchen jedoch keine Angst davor zu haben, von einem riesigen Berg von Transistoren überschüttet zu werden, da das Volumen dieser Transistoren nur ein Zehnmillionstel des Volumens der Reiskörner erreicht. Für die Größenordnung der so hergestellten Transistoren ist der millionste Teil des Meters, der Mikrometer, schon eine zu große Einheit. Die Größe des Mikrometers kann folgendermaßen veranschaulicht werden: der Durchmesser eines Haares je nach Person macht 20-40 Mikron aus. Es liegt also auf der Hand, dass wir diese Transistoren mit bloßem Auge gar nicht unterscheiden können; ihre Herstellung braucht einen Ansatz, der von den herkömmlichen Technologien abweicht. Für die Beschreibung ihrer Formate ist der Milliardste Teil des Meters zu benutzen. Diese Zahl kann folgendermaßen veranschaulicht werden: Wir würden imaginär die etwa eine Milliarde Einwohner Indiens in einer Reihe aufstellen. Einvernehmlich gehören diejenigen Objekte zum Begriff der Nanotechnologie, bei denen irgendein charakteristischer Wert die 100 Nanometer nicht übersteigt. Das bedeutet, dass die ersten zehn Inder ein T-Shirt mit der Schrift NANO tragen dürften. Zur weiteren Veranschaulichung können wir damit fortfahren, dass die charakteristische Größe eines Atoms in diesem Vergleich einem halben

Inder entspricht. Zurzeit erreichen die Spitzenmodelle der Speicherelemente 50-70 Nanometer, sie entsprechen also der Größe von 50 bis 70 Menschen mit dem T-Shirt. In letzter Zeit fiel die Informationsspeicherung noch in den Bereich der Mikroelektronik, diese Elemente werden auch in unseren PC-s auf unserem Tisch eingesetzt. Diese Geräte haben bereits früher eine unglaubliche Menge an Informationen gespeichert. Neben diesen Schaltkreisen, die auf der Basis der Halbleitertechnik funktionieren, spielen heute noch diejenigen Geräte eine Rolle, die für das Einschreiben und/oder Ablesen der Informationen auch mechanische Bewegungen in Anspruch nehmen. Zu diesen gehören z.B. die CD- und DVD-Player, die Disketten und Magnetbänder. Die Tendenz zeigt, dass diese Geräte mit der Zeit aus der alltäglichen Praxis verdrängt werden.

Alle Geräte in der Kette der Herstellung, Weiterleitung und Speicherung von Informationen müssen konsistent sein. Es reicht also nicht, große Mengen an Informationen speichern zu können, wir müssen auch für die Weitergabe und die Verarbeitung sorgen. Die am meisten verbreitete Form dafür ist heutzutage die Breitband-Übertragungstechnik, für die mehrere Methoden bekannt sind, die wir aber jetzt nicht im Einzelnen untersuchen wollen.

Die Schlüsselfrage ist die Dauerhaftigkeit der Aufbewahrung der Kultur, die immer mehr auch in digitaler Form erscheint – wobei das Wort digital besonders betont wird. Bedauerlicherweise ist das zurzeit bekannte dauerhafteste Informationsspeichermedium das Papier, danach kommt das Zelluloid und weit abgeschlagen die Materialien der Magnet-, der elektronischen und optischen Speicher bzw. die Speichermedien selbst. Dazu kommt noch, dass das nicht auf Papier basierende Speichern in den meisten Fällen eine kontinuierliche Energieversorgung und Auffrischung notwendig macht. Von Zeit zu Zeit müssen also die nicht auf dem Papier gespeicherten Informationen auf neue Datenträger kopiert werden. Dies bedarf natürlich erheblicher Ressourcen. Ein solches imaginäres elektronisches Archiv ist also nicht eine Art verlassener Umschlagplatz, sondern eine Werkstatt, die kontinuierlich Wartungsarbeiten wahrnimmt. Nach unserem heutigen Kenntnisstand und auf Grund unserer jetzigen Materialien muss alle ein bis zwei Jahre transkribiert werden. Die Bestimmung des Zeitintervalls wird dadurch erschwert, dass man als Benutzer mit diesen Produkten nicht die langjährigen Erfahrungen machen konnte wie z. B. mit dem Zelluloid.

Weiter erschwert wird die Situation dadurch, dass parallel zur Speicherung auch die Aufbewahrung, die Wartung und die Ersatzteilversorgung der Abspielgeräte gewährleistet sein muss [1]. Dies könnte man vielleicht am besten so veranschaulichen, wenn wir gedanklich den Versuch unternehmen, irgendein Ersatzteil für den Projektor eines Films zu kaufen, der mit einer Super-8-Kamrea aufgenommen wurde. Wir begegnen erstaunten Verkäufern, die sich fragen, warum wir wohl keinen CD-Player kaufen. Sie begreifen oft nur schwer, dass die alte Schallplatte mit dem Darsteller oder Orchester eine kulturelle Information trägt, die heute auf CD-s noch nicht zugänglich ist. Es liegt also auf der Hand, dass die auf diesen Datenträgern gespeicherten Informationen auf Datenträger transkribiert werden müssen, die mit den heutigen Abspielgeräten die Informationen reproduzieren können.

Die Frage hat auch bedeutende urheberrechtliche Aspekte. Diese würde ich gern mit einem meiner Lieblingslieder, dem „Yellow Submarine“ der Beatles, veranschaulichen. Zuerst hörte ich es auf einer LP-Platte, die aus Jugoslawien eingeschmuggelt wurde, wobei ich jetzt schon zugeben kann, dass ich dafür weder Zoll noch Tantiemen bezahlte. Später kaufte ich es in Wien auf einer SP-Platte, dabei zahlte ich im Preis auch die Tantiemen mit, aber mit dem Zoll war da auch nichts. Später hatte ich die oben genannte Musik auf meinen Tonbandgeräten, sowohl Spulentonbandgerät als auch Kassettenrecorder, zurzeit höre ich es von der CD. Laut geltendem Recht hätte ich jedes Mal,

wenn ich die genannte Musik kaufte, Tantiemen zahlen müssen. Der Widerspruch besteht also darin, dass ich nicht für das Hören der „Yellow Submarine“ die Tantiemen zahlte, sondern für jede Version des mit unterschiedlichen Technologien aufgezeichneten Werks eine diesbezügliche Zahlungspflicht entstand. Es stellt sich also die Frage, ob von uns mit Recht Tantiemen eingeholt werden, wenn wir im Zuge der Aufbewahrung der digitalen Kultur die Kunstwerke oder auch andere, urheberrechtlich geschützte Werke mit einer anderen Technologie aufbewahren und eventuell auch noch verbreiten? Dabei möchte ich das sehr geehrte Publikum darauf aufmerksam machen, dass in der Rundfunkgesetzgebung das Prinzip der technologischen Unabhängigkeit bereits realisiert wurde, d.h. der Nutzer der Dienstleistung hat damit nichts zu tun und auch keinen Einfluss darauf, mit welcher Technologie die Signale übertragen werden. Reklamation gibt es nur in Bezug auf die Qualität.

Die digitale Aufbewahrung der Daten ist also nicht nur eine Frage der Technologie. Die im Urheberrecht definierte „Einheit des Werks“ ist nämlich im Falle der auch in digitaler Form vorhandenen Werke mittels moderner digitaler Technik manipulierbar, und das ist nur bei bestem Willen als Verbesserung zu verstehen. Wir können aus der auf einer alten Platte aufbewahrten Produktion eines längst verstorbenen Sängers die Fehler und die Geräusche herausfiltern. Hier möchte ich das verehrte Publikum daran erinnern, dass ein bedeutender Teil der seinerzeit erfolgreichen Beatles-Platten noch mit der Mono-Technologie vertrieben wurde, wie auch die über sie gemachten Kinofilme und sonstige Aufzeichnungen noch Schwarz-Weiß-Aufnahmen waren. Mit Hilfe der digitalen Technologie wurde erreicht, dass heutzutage die Filmausschnitte aus der Zeit des 2. Weltkrieges coloriert werden und wir so auch die Farben der damaligen Uniformen erkennen können. Es ist sehr schwer die Grenze zu ziehen, inwiefern wir uns in dieser Hinsicht in die Formenwelt und das Erscheinungsbild der Filme einmischen dürfen, die ja schon an und für sich durch das Urheberrecht geschützt sind. Natürlich betrachten wir auch die inhaltliche und formale Einheit des Werks als maßgebend.

In Bezug auf die digitale Technik sollten wir auch noch die Rolle und das Schicksal der Privatarchive ansprechen. Mit der Verbreitung der Infokommunikationsgeräte stieg nämlich die Menge der von Privatpersonen angefertigten audiovisuellen Werke außerordentlich an.

Die erste Frage heißt: kann dieser quantitative Anstieg zu einem qualitativen Übergang führen? In dieser Frage möchten wir uns hier nicht festlegen, nur darauf hinweisen, dass man sich bereits im 2. Weltkrieg bei der Vorbereitung auf den D-Day in großem Maße auf die von englischen Touristen von der anderen Küstenseite gemachten Aufnahmen gestützt hat.

Die zweite Frage ist, inwiefern diese Informationsmenge überhaupt genutzt werden kann, abgesehen z. B. von der Darstellung der Menschen auf den Bildern. Denken wir nur daran, wie wichtig die Informationen waren, zu denen wir durch die Gemälde gelangt sind, die die Heiligen nicht mehr ikonenartig darstellen, sondern im Hintergrund hie und da eine Burg oder auf dem Tisch ein Werkzeug oder ein Besteck auftaucht.

In der digitalen Informationsspeicherung müssen wir also sowohl über die zeitnahe, als auch über die erneuerte Speicherung Entscheidungen treffen. Die Strategie kann nämlich nicht aufgehen, dass wir alles aufbewahren, selbst dann nicht, wenn die mengenmäßigen Indikatoren der digitalen Speicherung die Menge der auf dem Papier aufbewahrten Informationen bei weitem übersteigt. Die Papierinformationen entstehen nämlich in einer Menge von vielen, vielen laufenden Metern von Dokumenten und auch ihre Aufbewahrung bedarf kontinuierlicher Aufwendungen. Bei der Speicherung stellt sich immer wieder die Frage, was wir mit den ursprünglichen Informationsträgern tun. Bei Kunstwerken kommt man überhaupt nicht auf den Gedanken, die Originalwerke zu vernichten, während wir unsere Alltagsdokumente gern aussortieren. Sollte die Nanotechnologie in der Tat in den Alltag der

Informationsspeicherung einziehen, erhalten auch Individuen weitere bedeutende Speicherkapazitäten. Es liegt auf der Hand, unsere Materialien von den früheren Rechnern ohne auszusortieren auf unsere neuen zu kopieren. Dies kann auch für unsere Kulturwerte gelten, sowohl im privaten als auch im öffentlichen Leben.

Die digitale Technologie – einschließlich Nanotechnologie – schafft auch für die Präsentation kultureller Werte neue Möglichkeiten. In den Museen ermöglicht sie die mehrstufige Information und Suche, sie verwirklicht Interaktivität. Dadurch kann das präsentierte Werk in seinen breiteren Zusammenhängen situiert werden. Bei der Präsentation ist die Speicherung und Darbietung des sich bewegenden Bildes in ständig hoher Qualität als eine elementare Erwartung zu sehen, was die Menge der zu speichernden Informationen und somit der – nicht nur elektronischen Speicherung – auf der Basis der Nanotechnologie bedeutend erhöhen dürfte.

Die digital gespeicherte Information macht auch möglich, dass viele gleichzeitig zu dieser Zugang haben, und zwar ohne geographische Einschränkung. Hier sind die Chancen für den Zugang – unserer Ansicht nach – natürlich nur im inhaltlichen und nicht im ästhetischen Sinne gleich, weil ich meine, dass das Lesen eines echten Buches, die Teilnahme an einem echten Konzert durch nichts ersetzt werden kann, mindestens für diejenigen nicht, die dafür die Möglichkeiten haben. Die durch die Digitalisierung und Nanotechnologie entstehenden großen Kapazitäten ermöglichen jedoch, dass man das Erlebnis ohne Qualitätsminderung übertragen kann – in Hochauflösung, farbig, stereo, quadrophon...

Die Nanotechnologie erweitert auch die Möglichkeit der Netzwerke, das wir in Bezug auf die Breitbandübertragung schon früher angesprochen haben. Die Speicherung von großen Mengen Informationen müssen wir uns nämlich nicht unbedingt so vorstellen, dass diese vor uns auf dem Tisch zugänglich sein müssen. Es reicht, die Möglichkeit zu schaffen, dass wir zu jeder Zeit die gewünschte Information erreichen können. „Jederzeit“ meint hier, dass die Leistung am Arbeitsplatz, unterwegs, zu Hause immer das gleiche Niveau hat und für uns die gleichen Informationen erreichbar sind. Dabei kann die Nanotechnologie viel helfen: durch ihre Anwendung kann man ein schärferes Bild mit höherer Auflösung auch auf den Displays unserer Mobilgeräte erhalten.

Zusammenfassend lässt sich also feststellen, dass die Nanotechnologie in der digitalen Speicherung nicht nur eine Kapazitätssteigerung bedeutet. Sie bietet, in einem System organisiert, auch neue Möglichkeiten zur Darstellung kultureller Werte.

Wir müssen uns jedoch auch als Mensch viel ändern, weil ich das Gefühl habe, dass die Technik ein wenig nach vorn gelaufen ist, und die Grenzen unserer Möglichkeiten eher die eigenen Grenzen als die der Technologie [1, 2] sind. Der durchschnittliche Mensch braucht nämlich Zeit, um sich daran zu gewöhnen, dass die Dinge um ihn herum immer mehr elektronisch sind, das heißt, dass aus den meisten Sachen ein e-etwas wird. Und diese Sachen werden auch in den mobilen Anwendungen immer mehr zugänglich, d.h. die e-etwas werden mobil und es entstehen die m-etwas.

Ich meine, diese Geräte werden wir dann richtig mögen, wenn die Buchstaben vor dem Wort „etwas“ eine ganz neue Bedeutung erhalten. Dazu ist es aber notwendig, dass der Buchstabe „m“ vor den Wörtern nicht die Bedeutung „mobil“, sondern „menschlich“ trägt.

Literaturhinweis

[1] Infocommunication Technologies and Man. (in English) Ed. I. Mojzes
Műegyetemi Kiadó, ISBN 963 420 821 5, Budapest, 2004
[2] e-valami. (in Hungarian) Mojzes I. Mikrotechnika, 2006.

INFORMATIK im Alltag

Köstlichkeiten aus der Küche der Informatik

DIE KALTE VORSPEISE – SPAM

FAZEKAS LÁSZLÓ
– SysPac Hungária Kft.

SPAM ist in vielen Teilen der Welt, aber vor allem aber in den USA, als Marke für Dosenfleisch bekannt. Das Produkt wird von der Firma Hormel Foods Inc. seit 1937 produziert und vertrieben. Im deutschsprachigen Raum ist Dosenfleisch (spiced ham) unter dem Namen „Frühstücksfleisch“ bekannt.

Bei seiner Einführung wurde das o. g. Dosenfleisch noch HORMEL Spiced Ham (HORMEL Würzschinken) genannt. Danach wurde ein Wettbewerb ausgeschrieben, bei dem die Konsumenten aufgefordert wurden, einen Namen zu kreieren, der den Geschmack des Produktes wiederspiegelt. So wurden „sp“ von spiced und „am“ von ham zu SPAM zusammengefügt.

BEGRIFFS-HERKUNFT

Der Begriff entstammt einem Sketch der englischen Comedyserie „Monty Python's Flying Circus“. In einem Café besteht die Speisekarte ausschließlich aus Gerichten mit SPAM, welche in ihrem Namen „SPAM“ teilweise mehrfach hintereinander enthalten.

Ein Gast verlangt nach einem Gericht ohne SPAM, die Kellnerin empfiehlt ein Gericht mit „wenig“ SPAM; als sich der Gast darüber aufregt, fällt ein Chor aus Wikingern, die die beiden anderen Tische besetzen, mit einem Loblied auf SPAM ein, bis der Sketch im Chaos versinkt. Im anschließenden Abspann wurden die Namen der Mitwirkenden ebenfalls um „SPAM“

ergänzt. Im Sketch wird das Wort SPAM insgesamt knapp 100 Mal erwähnt.

Durch diesen Sketch wurde der Begriff SPAM auch in die Informatik eingeführt. Er bedeutet heute den ungebetenen, massenhaften, meist strafbaren Versand von Nachrichten. Diesen Missbrauch bezeichnet man als Spamming oder Spammen, die „Täter" als Spammer.

ARTEN VON SPAM

E-Mail-Spam

E-Mail-Spam wird auch als UBE (unsolicited bulk e-mail) bezeichnet. Je nach Motiv und Ursache unterscheidet man:

• Unsolicited Commercial E-Mail, UCE, also Werbung. Meist handelt es sich dabei um dubiose oder besonders günstige Angebote bzgl. Sex (Penisverlängerung) und Lebensqualität, Software, Markenprodukte, Medikamente etc.

• Scam. „Beworben" wird hierbei oft eine Gelegenheit, bei der der Empfänger leicht an Geld kommen kann. Besonders häufig fällt dabei die Nigeria-Connection auf, leicht zu erkennen an einem sehr langen, larmoyanten, anbiedernden Text, oft in Großbuchstaben und mit geradezu aberwitzig hohen Geldbeträgen.

• Phishing Mails. Hier wird versucht, an vertrauliche Daten des Empfängers zu kommen. Üblicherweise behauptet die Mail von einem dem Empfänger bekannten Unternehmen oder Anbieter zu kommen und enthält Links zu den vermeintlichen Einstiegsseiten. Wird diese Art Betrugsmail massenhaft versendet, wird meist auf Anbieter mit entsprechend vielen Kunden gezielt oder auf Bereiche, wo der Betrüger einen Zusammenhang zwischen Adressen und Anbieter herstellen kann, z.B. beim Mail-Provider.

• Würmer und Viren. Der Verbreiter trägt die Schuld daran, dass sich diese von seinem Rechner aus weiterverbreiten. Er ergriff nicht die allgemein bekannten Schutzmaßnahmen, damit Datei-Anhänge in den E-Mails, die er empfängt, nicht vollautomatisch ausgeführt werden, oder er hat absichtlich auf so ein Attachment geklickt, ohne mit dem vermeintlichen Absender etwas Derartiges vereinbart zu haben.

• Belästigungs-Mails ohne nähere Information an diejenigen, deren E-Mail-Adresse als Absender von Wurm- oder Virus-E-Mails gefälscht war. Der Täter hat eine defekte Virenschutz-Software in Betrieb gesetzt, die vollautomatisch diesen Vandalismus begeht, ohne sich darüber Gedanken zu machen, dass Würmer und Viren immer gefälschte Absender tragen und dass die Opfer mit solchen Mitteilungen nichts anfangen können, wenn eine Kopie der zurückgewiesenen E-Mail mit allen Headern fehlt, welche eine Recherche nach der Herkunft erlauben würde.

• Newsletter und Mailinglisten, bei denen man von unbekannten Dritten als Abonnent eingetragen wurde und denen der nötige Schutzmechanismus fehlt, um solche gefälschten Bestellungen zu erkennen.

• Joe-Jobs: UBEs, die so aussehen, als kämen sie von einer anderen Person als dem Täter. Zum Beispiel hat der Täter den Namen und/oder die E-Mail-Adresse einer bestimmten Drittperson in der E-Mail angegeben. Verfolgungsmaßnahmen gegen den vermeintlichen Täter treffen und schaden der Drittperson, was das eigentliche Ziel des Joe Jobs ist.

• HOAXes. Sensationelle, aber meist falsche Gerüchte, die unbedarft an möglichst viele Freunde und Bekannte weitergeleitet werden, weil sie so aufregend sind. Siehe auch Kettenbriefe. Im Gegensatz zu Würmern wird hier der Empfänger selbst dazu gebracht, die Mail zu verbreiten.

Mobile Spam

Auch die Kommunikation per Handy ist von Spam betroffen, durch den verstärkten Einsatz von Mobile Marketing zur Marktforschung, sowie durch unerwünschte SMS, die in Japan schon bis zu 90 % aller elektronischen Nachrichten ausmachen. Eine weitere Variante sind hier sogenannte Spam- oder Ping-Anrufe, die nur Sekundenbruchteile dauern und den Angerufenen zum Rückruf und damit zur unwissentlichen Wahl eines teuren Mehrwertdienstes verleiten sollen.

DIE WARME VORSPEISE – VIREN

Ein Computervirus ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und sich dadurch reproduziert. Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware, am Betriebssystem oder an der Software vornehmen. Der Begriff Computervirus wird auch fälschlich für Computerwürmer und Trojanische Pferde genutzt, da der Übergang inzwischen fließend und für Anwender oft nicht erkennbar ist.

UNTERSCHIED ZWISCHEN VIRUS, WURM UND TROJANISCHEM PFERD

Computerviren und Würmer verbreiten sich beide auf Rechnersystemen, doch sie basieren zum Teil auf vollkommen verschiedenen Konzepten und Techniken.

Ein Virus verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese ggf. so anpasst, dass das Virus mit ausgeführt wird, wenn das Wirtsprogramm gestartet wird. Zu den infizierbaren Dateien zählen normale Programmdateien, Programmbibliotheken, Skripte, Dokumente mit Makros oder anderen ausführbaren Inhalten sowie Bootsektoren.

Die Verbreitung auf neue Systeme erfolgt durch versehentliches (gelegentlich auch absichtliches) Kopieren einer infizierten Wirtsdatei auf das neue System durch einen Anwender. Dabei ist es unerheblich, auf welchem Weg diese Wirtsdatei kopiert wird: Früher waren die Hauptverbreitungswege Wechselmedien wie Disketten, heute sind es Rechnernetze z.B. via E-Mail zugesandt, von FTP-Servern, Web-Servern oder aus Tauschbörsen heruntergeladen. Es existieren auch Viren, die Dateien in freigegebenen Ordnern in LAN-Netzwerken infizieren, wenn sie entsprechende Rechte besitzen.

Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versuchen aktiv in neue Systeme einzudringen. Sie nutzen dazu Sicherheitsprobleme auf dem Zielsystem aus, wie z.B.:

- Netzwerk-Dienste, die Standardpasswörter oder gar kein Passwort benutzen
- Design- und Programmierfehler in Netzwerk-Diensten
- Design- und Programmierfehler in Anwenderprogrammen, die Netzwerkdienste benutzen z.B. E-Mail-Clients

Ein Wurm kann sich dann wie ein Virus in eine andere Programmdatei einfügen. Meistens versucht er sich jedoch nur an einer unauffälligen Stelle im System mit einem unauffälligen Namen zu verbergen und verändert das Zielsystem so, dass beim Systemstart der Wurm aufgerufen wird (wie etwa die Autostart-Funktion in Microsoft-Windows-Systemen).

Trojanische Pferde sind Programme, die auf fremde Computer eingeschleust werden (oder zufällig dorthin gelangen) und schließlich – vom Anwender unbemerkt - diesem nicht genannte Aktionen ausführen. Sie sind als nützliche Programme getarnt, indem sie beispielsweise den Dateinamen einer nützlichen Datei benutzen, oder neben ihrer versteckten Funktion tatsächlich eine nützliche Funktionalität aufweisen. Die heimliche Funktion eines

Trojaners kann auch darin bestehen, ein Schadprogramm auf dem PC zu installieren, welches infolgedessen unabhängig vom Trojaner meist versteckt auf dem PC arbeitet. Der tatsächliche Nutzen einer Datei, die ein Trojanisches Pferd enthält, kann beliebiger Art sein. So können u.a. eigenständige Spionageprogramme auf den Rechner gelangen (z. B. Sniffer oder Komponenten, die Tastatureingaben aufzeichnen, sogenannte Keylogger). Auch ermöglicht ein solcher Trojaner die heimliche Installation eines Backdoorprogramms, welches es gestattet, den Computer über ein Netzwerk (z.B. dem Internet) fernzusteuern, ohne dass der Anwender dies kontrollieren kann. Durch das Löschen des Trojanerprogramms werden die heimlich installierten Schadprogramme nicht automatisch mit entfernt.

Wichtig zu erwähnen ist noch das sog. Botnet. Der Begriff ist eine Abkürzung von Robotnetzwerk. Unter einem Botnet versteht man ein fernsteuerbares Netzwerk von PCs, welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für Spam-Verbreitung, Denial-of-Service-Attacken usw. verwendet werden, zum Teil ohne dass die betroffenen PC-Nutzer etwas davon mitbekommen.

Die Gefahr, die von Botnets ausgeht, ist extrem hoch, da die von ihnen ausgeführten DDoS-Attacken und Spam-Nachrichten eine enorme Bedrohung für Anbieter von Internetdiensten jeglicher Art darstellen. Das Hauptpotenzial von Botnets besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt. Somit ist es einem Botnet von ausreichender Größe durch Senden von immensen Datenmengen möglich, die Anbindungen der attackierten Serviceanbieter zu verstopfen. Da die Netze meistens aus übernommenen Heim-PCs aus verschiedensten Regionen (und somit breitem IP-Adressenspektrum) bestehen, können die betroffenen Anbieter nur bedingt mit Schutzmaßnahmen wie Paketfiltern vorgehen.

DAS HAUPTGERICHT – HACKER

Nach allgemeinem Verständnis ist ein Hacker ein überaus talentierter Computerspezialist, der Sicherheitsbarrieren überwinden und in fremde Systeme eindringen kann.

„Hacker“ findet in den Medien meist im Kontext eines destruktiven Computerexperten Anwendung, der seine Fertigkeiten vornehmlich für kriminelle Zwecke nutzt. Davon abgeleitet, wird er umgangssprachlich häufig mit kriminellen Subjekten in Verbindung gebracht, die Böses im Schilde führen und der Gesellschaft Schaden zufügen.

Der Begriff Hacker wurde in den 70er bis Anfang der 80er Jahre als Bezeichnung für einen außergewöhnlich guten Programmierer geprägt. Davon abgeleitet gleicht das Wort innerhalb der Programmierer- und Hackerszene auch heute noch einem Rang: Es zeugt von Respekt und stellt eine Auszeichnung für außergewöhnlich gute Fähigkeiten dar, welche von Mitgliedern der Szene als nicht vorschnell verliehen gilt.

Mitte der 80er Jahre standen Hacker vornehmlich für wissbegierige Menschen, welche die Welt der Computer erforschten, dabei in die Tiefen der Materie eindrangen und sich dadurch auch in fremde Systeme hacken konnten. Aufgrund der Faszination von der letzteren Fähigkeit, wurden sie vor allem gegen Ende der 80er Jahre durch Film und Presse stark übertrieben dargestellt. Eine recht begrenzte Definition des Begriffs erreichte so die Köpfe der Bevölkerung und ließ den Mythos Hacker, wie er heute sprachgebräuchlich verwendet wird, entstehen.

Seit 1990 gibt es eine strikte Trennung zwischen Hackern und Crackern. Destruktive Hacker werden abwertend Crasher oder Cracker genannt.

DIE UNTERTEILUNG ZWISCHEN HACKER UND CRASHER BZW. CRACKER

Stark vereinfacht ausgedrückt, lösen Hacker Probleme und bauen etwas auf, wohingegen Crasher Probleme erzeugen bzw. etwas zerstören. Im Detail bauen Hacker beispielsweise Informationsnetze auf, machen auf Sicherheitslücken aufmerksam (und erreichen so, dass diese geschlossen werden), schreiben zum Teil Freeware oder Open-Source-Software oder betätigen sich konstruktiv in einem anderen Umfeld, welches zu den zahlreichen Insiderdefinitionen des Begriffs Hacker passt. Crasher legen hingegen Computer- und Telefonnetze lahm, löschen oder verändern wichtige Daten, bereichern sich auf kriminelle Art oder terrorisieren ihre Mitmenschen durch absichtlich herbeigeführte Abstürze der Rechner. Doch spätestens wenn es um politisch motivierte Aktionen geht, wird ersichtlich, dass es an einer wirklich klaren Trennlinie zwischen „gut“ und „böse“ mangelt, was eine solche Unterteilung unpraktikabel macht.

„BLACK-“, „WHITE-“ UND „GREY-HATS“

In der IT-Security-Szene wird manchmal eine Unterteilung der Hacker in „Black-“, „White-“ und „Grey-Hats“ benutzt, die auf der Einteilung aus alten Western-Filmen basiert, welche „Cowboys“ auf Grund der Farbe ihres Huts als „böse“ (schwarz), „gut“ (weiß) oder „neutral“ (grau) charakterisiert:

- Black-Hats („Schwarz-Hüte“) handeln mit krimineller Energie, und beabsichtigen beispielsweise, das Zielsystem zu beschädigen oder Daten zu stehlen. Zu dieser Untergruppe zählt man auch die Cyberpunker, die als wahre Meister ihres Fachs gelten, aber nur nach ihren eigenen Regeln leben.
- Ein White-Hat („Weiß-Hut“) nutzt sein Wissen sowohl innerhalb der Gesetze als auch der Hackerethik, beispielsweise indem er professionell Penetrationstests ausführt.
- Grey-Hats („Grau-Hüte“) verstoßen möglicherweise gegen Gesetze oder restriktive Auslegungen der Hackerethik, allerdings zum

Erreichen eines höheren Ziels. Beispielsweise durch die Veröffentlichung von Sicherheitslücken, um ein Leugnen unmöglich zu machen und die Verantwortlichen dazu zu zwingen, diese zu beheben. Grey-Hats zeichnen sich dadurch aus, dass sie nicht eindeutig als „gut“ oder „böse“ einzustufen sind.

Menschen passen allerdings selten eindeutig unter nur einen der Hüte. In der Praxis nimmt diese Unterteilung daher nur wenig Bezug auf real existierende Personen und steht vielmehr als Begrifflichkeit für eine bestimmte Art des Hackens.

Die meisten Menschen verwenden „Hacker“ weiterhin als Oberbegriff, der sowohl die („guten“) Hacker als auch die („bösen“) Cracker bzw. Crasher einschließt, und dominieren so die umgangssprachliche Bedeutung. Bezogen auf die IT-Sicherheit ist der Begriff „Hacker“ in dieser Form längst zu einem Elementarbegriff geworden.

BERÜHMTE HACKER

Technikfachleute

- Ken Thompson und Dennis Ritchie erfanden in den frühen 1970er Jahren die heute weit verbreitete Programmiersprache C und entwickelten 1969 UNIX.
- Eric S. Raymond ist Autor und Programmierer von Open-Source-Software.
- Linus Torvalds begann 1991 die Entwicklung des Linux-Kernels.

• Tron wies die Fälschbarkeit von GSM-Karten nach und entwickelte ein verschlüsselungsfähiges und preiswertes ISDN-Telefon.

• John T. Draper alias Cap'n Crunch war der erste Phreaker bzw. Telefonhacker. Er schaffte es, kostenlos zu telefonieren, und entdeckte weitere Methoden zur Manipulation von Telefonleitungen.

Ethische Hacker

• Wau Holland, Mitbegründer des Chaos Computer Clubs (1981)

• Loyd Blankenship, Autor des Artikels The Conscience of a Hacker

• Richard Stallman ist unter anderem Gründer der Free Software Foundation (FSF)

Kriminelle Cracker

• Robert Tappan Morris schrieb 1988 den Morris-Wurm.

• Kevin Mitnick ist ein für Social Engineering bekannter Hacker, der erst nach mehreren Jahren Flucht vom FBI gefasst werden konnte.

• Lex Luthor, der 1984 die legendäre Hackergruppe Legion of Doom gründete und Anfang der 90er Jahre einen Hackerkrieg anfing, der in der Operation Sundevil durch den US Geheimdienst Secret Service zerschlagen wurde.

• Karl Koch brach zusammen mit Markus Hess Ende der 80er Jahre in militärische US-Netzwerke ein, um Daten an den KGB zu verkaufen; anfangs aus ideellen Gründen und Neugier; später um seine Drogensucht dadurch zu finanzieren.

• Kevin Poulsen manipulierte Telefonanlagen von Radiosendern, um bei Gewinnspielen Autos, Reisen und Geld zu gewinnen; er wurde später vom FBI verhaftet.

DAS DESSERT – PHISHING

Phishing ist eine Form des Trickbetruges im Internet. Die Bezeichnung leitet sich vom Fischen (engl. fishing) nach persönlichen Daten ab. Für den Wortanfang „P“ gibt es zwei Erklärungen: zum einen könnte es eine Zusammenfassung von „Password Fishing“ sein. Eine andere Erklärung der Ersetzung des „F“ durch „Ph“ stellt eine Imitation des Begriffes Phreaking dar, der sich in den 70er Jahren durch eine Zusammenziehung von „Phone“ und „Freak“ ergab.

Phishing-Angriffsziele sind Zugangsdaten, z. B. für Banken (Onlinebanking), Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Kontaktportale. Der Phisher schickt seinem Opfer offiziell wirkende Schreiben, meist E-Mails, die es dazu verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben.

Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Durch den Missbrauch der persönlichen Daten entstehen beträchtliche Schäden in Form von Vermögensschäden (z. B. Überweisung von Geldbeträgen fremder Konten), Rufschädigung (z. B. Versteigerung gestohlener Waren unter fremdem Namen bei Online-Auktionen) oder Schäden durch Aufwendungen für Aufklärung und Wiedergutmachung. Über die Höhe der Schäden gibt es nur Schätzungen, die zwischen mehreren hundert Millionen Dollar und Milliarden-Beträgen schwanken (Stand: Februar 2005).

METHODEN DER DATENBESCHAFFUNG

Im Allgemeinen beginnt eine Phishing-Attacke mit einer persönlich gehaltenen, offiziell anmutenden E-Mail oder einem Massenversand von E-Mails. Der Empfänger soll eine betrügerische Website besuchen, die täuschend echt aussieht und unter einem Vorwand zur Eingabe seiner Zugangsdaten auffordert. Folgt er dieser Aufforderung, gelangen seine Zugangsdaten in die Hände der Urheber der Phishing-Attacke. Was dann folgt, soll nur noch das nachträgliche Misstrauen des Opfers zerstreuen: Eine kurze Bestätigung oder eine falsche Fehlermeldung.

Eine andere Variante bindet ein Formular direkt innerhalb einer HTML-E-Mail ein, das zur Eingabe der vertraulichen Daten auffordert und diese an die Urheber sendet. Auf eine Phishing-Website wird hierbei verzichtet.

METHODEN DER VERSCHLEIERUNG

E-Mail

Die E-Mail wird als HTML-E-Mail, eine E-Mail mit den grafischen Möglichkeiten von Webseiten, verfasst. Der Linktext zeigt die Originaladresse an, während das unsichtbare Linkziel auf die Adresse der gefälschten Website verweist.

Mit der Einbindung von HTML kann der im Mail-Programm sichtbare Link tatsächlich auf eine ganz andere Webseite verweisen. Zwar lässt sich ersehen, dass das Linkziel auf eine andere Webseite verweist. Allerdings können auch diese Angaben über Skripttechniken verfälscht werden. In anderen Fällen wird der Link als Grafik dargestellt. Auf dem Bildschirm des Anwenders erscheint zwar Text, dieser ist allerdings eine Grafik. Hierfür wird meistens auch die E-Mail-Adresse des Absenders gefälscht.

Webpräsenz

Die gefälschten Zielseiten haben meistens gefälschte Namen oder Bezeichnungen, die ähnlich klingen wie die offiziellen Seiten der Firmen. Die Zielseiten mit dem Webformular haben das gleiche Aussehen wie die Originalseiten. Sie sind also nur sehr schwer als Fälschungen identifizierbar. Im Allgemeinen sollte der Anwender die originalen Internet-Seitenadressen z. B. seiner Bank kennen. Die Adresszeile des Webbrowsers verrät, falls er sich nicht auf der Originalwebsite befindet.

Eine Adresszeile der Form z. B.: http://217.257.123.67/security/ * verrät eindeutig, dass man sich nicht auf den Seiten einer Bank

befindet. Deshalb werden Domainnamen (Internet-Adressnamen) benutzt, die den Bankadressen täuschend ähnlich sehen, z. B. http://www.security-beispielbank.de/ *

Erkennung

Erfahrene Mail-Nutzer erkennen Phishing-E-Mails auf den ersten Blick, insbesondere anhand typischer Merkmale:

1. Dringlichkeit: Es wird aufgefordert, schnellstmöglich etwas durchzuführen, oft eine angebliche Sicherheitsüberprüfung, Verifikation, Freischaltung oder andere wichtig klingende Aktionen.

2. Drohung: Es wird angedroht, dass bei Nichtbeachtung ein Zugang gesperrt oder gelöscht, bzw. etwas anderes Schlimmes oder Lästiges geschehen werde.

3. Abfrage sicherheitsrelevanter Informationen: Entweder in einem Formular innerhalb der E-Mail oder auf einer verlinkten Website. Am häufigsten Onlinebanking-Passworte und TANs, aber auch Passworte anderer Dienste (z.B. Versandhäuser, Online-Auktionshäuser). Besondere Vorsicht ist geboten, wenn zur Eingabe mehrerer TANs aufgefordert wird.

4. Webseite: Die E-Mail enthält einen Link zum Anklicken.

5. Unpersönlich: Nur eine allgemeine Anrede wie „Sehr geehrter Kunde“ oder „Sehr geehrtes Mitglied“.

6. Fehler: Rechtschreib- und Grammatikfehler im Text, beispielsweise „ae“ anstatt „ä“ oder ungebräuchliche Worte (beispielsweise „eintasten“ anstatt „eingeben“).

7. Meist fehlende oder fehlerhafte Zertifikate der Webseite.

E-Mails, in denen man nach persönlichen Daten wie Passwörter oder TANs gefragt wird, sind grundsätzlich gefälscht und können gelöscht werden, selbst wenn sie keine der oben genannten Merkmale aufweisen.

SCHUTZ

Vorsicht im Umgang mit vertraulichen Daten:

• Rufen Sie niemals die Websites sicherheitsrelevanter Dienste über einen Link aus einer unaufgefordert zugesandten E-Mail auf. URLs und E-Mail-Absenderadressen können gefälscht werden und sind nicht vertrauenswürdig.

• Geben Sie die URL zum Onlinebanking immer von Hand in die Adresszeile des Browsers ein oder benutzen Sie im Browser gespeicherte Lesezeichen, die Sie zuvor sorgfältig angelegt haben. Vor Nutzung sicherheitsrelevanter Dienste sollten keine weiteren Browserfenster oder Tabs geöffnet sein.

• Nutzen Sie alternative Browser wie den aktuellen Firefox von Mozilla mit der Zusatzerweiterung Spoofstick. Diese Erweiterung zeigt den Namen der Internetadresse an, auf der man sich momentan wirklich befindet.

• Prüfen Sie nach Möglichkeit die Verschlüsselung der Webseite, insbesondere den elektronischen Fingerabdruck (Fingerprint) des Zertifikats. Nur so können Sie zweifelsfrei sicherstellen, dass Sie tatsächlich mit dem Server des Anbieters (z. B. Bankrechner) verbunden sind. Der Dienstleister stellt Ihnen auf Anfrage die nötigen Informationen zum Abgleich zur Verfügung.

• Seien Sie misstrauisch, wenn Sie unaufgefordert auf sicherheitsrelevante Bereiche angesprochen werden. Fragen Sie bei den Dienstanbietern nach, wenn Sie unsicher sind. Derartige Rückfragen liefern den Betreibern der betroffenen Dienste meist erst den Hinweis, dass eine Phishing-Attacke gegen ihre Kunden läuft.

Allgemein gilt: Banken und Versicherungen bitten nie um die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per E-Mail, per SMS oder telefonisch. Finanzdienstleister senden bei sicherheitsrelevanten Fragen Briefe und Einschreiben via Briefpost bzw. man bittet um einen persönlichen Besuch des Kunden in der Filiale.

Quelle:

1. Peter Warren & Michael Streeter: Az Internet sötét oldala, HVG Kiadó Rt., Budapest 2005

2. http://de.wikipedia.org

„IT im ALLTAG von MAGYAR POSTA“ – „Heute & Morgen“

MICHAEL PAUSINGER
– SIEMENS
Industrial Solutions & Services

Sie werden sich fragen wie ich auf dieses Thema gekommen bin! Die letzten Monate habe ich für Magyar Posta gearbeitet und war fasziniert davon, wie IT „Heute“ dort eingesetzt wird, ständig wächst und für das „Morgen“ weiterentwickelt wird!

Wie diese Informations-Technologie funktioniert, will ich Ihnen heute an Hand von Beispielen bei Postdiensten – die im wesentlichen auch bei Magyar Posta zutreffen - näher bringen.

- Wozu braucht Magyar Posta Informations-Technologie?
- Wo setzt Magyar Posta überhaupt IT ein?
- Wo sehen Sie IT im Alltag von Magyar Posta?

IT ist das wichtigste Mittel, um alle Post-Prozesse transparent zu machen, sie zu steuern, zu überwachen, zu sichern und sie wirtschaftlich und wettbewerbsfähig zu machen.

Informations-Technologie für Post- und Logistik-Dienste ist heute schon weit mehr als nur ein einfaches Werkzeug um Büros und Maschinen zu betreiben! Mit ihr wird die Sicherheit und Korrektheit auf dem postalischen Weg enorm verbessert, ja sichergestellt.

Der „Alltag“ des Postdienstes basiert „Heute“ schon auf Informations-Technologie und er wird „Morgen“ noch mehr auf IT setzen, da IT einer der wichtigsten „Business Driver“ ist.

Wo werden Sie persönlich konfrontiert mit der IT im Alltag von Magyar Posta? Sie bemerken den Postdienst wahrscheinlich kaum, er arbeitet ganz dezent und unbemerkt!

Dennoch ist Ihnen die ganze postalische Prozesskette der Magyar Posta sehr vertraut – vom Briefkasten über das Postamt, die Transportlogistik, die Verteilzentren – das OLK – Országos Logisztikai Központ – Budapest, die Briefträger bei der Zustellung und die vielen Briefe und Postkarten in Ihrem Briefkasten – leider natürlich auch die Rechnungen!

Täglich begegnen Ihnen all diese Menschen, Fahrzeuge, Produkte des Postdienstes - sie sind schon ganz selbstverständlich für Sie.

Wo ist bei all dem die Informations-Technologie – werden Sie fragen? Sie ist vorhanden, aber sie ist wahrscheinlich nicht so offensichtlich für Sie! Lassen Sie uns einfach ein wenig genauer hinschauen. Lassen Sie uns zuerst einmal die gesamte Kette der Postversorgung ansehen – siehe Abbildung 1.

Es gibt folgende Teilprozesse:

- Die Einsammlung der Post mit Briefkasten, Massenauflieferer, Postamt,...
- Die Transportlogistik zur Kollektion der Post – Fahrer, Van‘s,...
- Die Postämter als Sammel- und Vorverarbeitungs-Einheiten
- Die Transportlogistik von den Postämtern zu den Sortierzentren (z. B. OLK)
- Das OLK- Sortierzentrum zur landesweiten Sortierung der Post – Briefe & Pakete

Abbildung 1: Das Post- und Logistik-Netzwerk der Magyar Posta

- Die Transportlogistik zur Distribution der Post - zu den Postämtern & Großempfängern
- Die Postämter als Distributions-Einheiten für die Post
- Die Zustellung – Briefträger, Massenpost-Empfänger (HVR)

Alle beteiligten Personen, Fahrzeuge, Einheiten, Ressourcen, etc. müssen dem IT-System a priori bekannt sein. Eine künftige IT-Lösung mit „Online-Dokumentation" des Gefahrenübergangs durch Handheld-Terminals wäre eine zusätzliche Absicherung der Postprozesse. So könnte man beispielsweise bei der Zustellung den Empfang einer Sendung oder den „Cash on Delivery" Vorgang über das Handheld-Terminal quittieren lassen.

Ferner muss die zeitliche Abfolge der einzelnen Teilprozesse, ihre korrekte und richtige Nutzung durch die berechtigten Personen und zur korrekten Zeit dem IT System bekannt, ja genau vorgegeben sein.

WIE BEKOMMT MAN DIESE DATEN IN DAS IT-SYSTEM HINEIN?

Das IT-System der Postdienste lässt sich am besten in einer IT-Pyramide darstellen – siehe Abbildung 2. In den verschiedenen Ebenen der Pyramide werden ganz unterschiedliche Funktionen/Anwendungen umgesetzt und können dort bearbeitet werden.

Jede Schicht hat seine spezielle Aufgabe. In der ersten Schicht – die Schicht, die direkt mit den physikalischen Prozessen verbunden ist, werden alle Steuer-, Kontroll-, Identifizier-, Prüf- und Daten-Akquisitions-Aufgaben für diese physikalischen Prozesse gesteuert, kontrolliert und abgewickelt.

Das heißt, die Steuerung und Kontrolle der Ressourcen des operationellen Betriebs wie Angestellte/Postarbeiter, Brief-Sortier-Maschinen, Roll-Container, Behälter, Transport-LKWs, Sub-Unternehmer etc., erfolgt in dieser Schicht.

Abbildung 2: Informations-Technologie und das physikalische Post-Netzwerk

Die erste „IT-Pyramiden-Ebene“ ist also direkt der physikalischen Ebene zugeordnet und muss völlig vordefiniert sein, um die physikalische Ebene überhaupt korrekt steuern und kontrollieren zu können.

Diese erste „IT-Ebene“ prüft auch die „Fingerabdrücke“ auf Zulässigkeit und sie prüft die korrekte Nutzung der Prozesse und Teilprozesse.

In den darüber liegenden Schichten werden in der Regel alle Verwaltungs- und Managementaufgaben abgehandelt, die in irgendeiner Form mit den physikalischen Post- und Logistik-Prozessen zu tun haben.

Typische Aufgaben sind z. B. die Unterstützung von Post- Management, Vertrieb und Marketing, Kunden-Betreuung, Produktions-Kontrolle, Sortier-Zentrums- (OLK-) Kontrolle, regionale und nationale Kontrolle – Postämter, Transport-Logistik, etc.

Alle Schichten müssen schon vor der realen und operationellen Nutzung programmiert sein und präzise funktionieren, da sie nur dann die realen Prozesse und alle darüber liegenden Schichten steuern und kontrollieren können.

WAS SIND DIE „FINGERABDRÜCKE“ IM POSTALISCHEN NETZWERK?

Nichts anderes als eineindeutige Identifizierkriterien, die die einzelnen Elemente und Einheiten der Post-Prozess-Kette identifizieren sollen, damit das IT-System prüfen kann, ob der Vorgang korrekt ist, in der richtigen Reihenfolge stattfindet und ob die beteiligten Ressourcen berechtigt sind in diesen Prozessen mitzuwirken.

Wenn man z. B. den Verlust einer „Wertsendung“ nachvollziehen will, ist diese eindeutige Identifizierung unerlässlich! Die nachfolgenden postalische Einheiten/Elemente können beispielsweise folgende „Fingerabdrücke“ haben: siehe auch Abbildung 3.

Briefkasten:
Eindeutige Nummer – z. B. BK123 468 – oder ein Barcode zum abgreifen mit Lesegerät fest am Briefkasten angebracht

Briefkasten-Leerer:
Ausweis mit Barcode

Van zum Leeren:
Van-Kennzeichen – HGB 234-12 - oder/und Transponder/RFID – Radio Frequenz Identifikation – am Fahrzeug angebracht

Kollektions-Postamt:
Eindeutige Nummer – PA 62 – oder/und Barcode zum abstreifen an der Pforte/am Eingang zum Postamt

Transport- LKW:
Postamt zum OLK: Kennzeichen – IJHS 789-12 – oder/und Transponder/RFID – Radio Frequenz Identifikation - am Fahrzeug

Fahrer LKW:
Postamt zum OLK: Ausweis mit Barcode

Sortierzentrum OLK:
Spezielle Eindeutige Nummer – OLK 123 – oder/und Barcode zum abstreifen an der Pforte/am Eingang zum OLK

Transport-LKW:
OLK zum Postamt : Kennzeichen – GEB 332-12 – oder/und Transponder/RFID – Radio Frequenz Identifikation – am Fahrzeug

Fahrer LKW:
OLK zum Postamt : Ausweis mit Barcode
Zustell-Postamt: Eindeutige Nummer – PA 114 – oder/und Barcode zum abstreifen an der Pforte/am Eingang zum Postamt

Transport-LKW:
OLK zum Großkunden: Kennzeichen – GEB 332-12 – oder/und Transponder/RFID – Radio Frequenz Identifikation – am Fahrzeug

Fahrer LKW:
OLK zum Großkunden: Ausweis mit Barcode

Zusteller(in):
Postamt zum Kunden: Ausweis mit Barcode oder/und Hand-Terminal mit eindeutigem Identifikator

WIE WERDEN DIESE „FINGERABDRÜCKE“ GENUTZT?

Hier einige Beispiele davon, die in direktem Bezug zur gesamten postalischen Prozesskette stehen – siehe auch Abbildung 3. Der Briefkasten hat beispielsweise eine eindeutige Nummer – BK 123 468 – oder einen Barcode.

Der Briefkasten-Leerer würde dann diesen „Briefkasten-Fingerabdruck“ aufnehmen und das IT-System kann prüfen, ob der Briefkasten in der korrekten Einsammelroute zur rechten Zeit entleert wurde.

Der Briefkasten-Leerer würde sich beim Einsteigen in seinen Van mit seinem Ausweis (mit Barcode) beim IT-System melden und den „Fingerabdruck“ des Van‘s – Kennzeichen „HGB 234-12“ – dem IT-System zusätzlich melden.

Das IT-System kann dann prüfen, ob Fahrer und Van „zusammenpassen“. Entleert der Fahrer den Briefkasten, würde er sich mit seinem Ausweis beim IT-System melden und das System könnte prüfen, ob „Fingerabdruck“ von Fahrer und Briefkasten „zusammenpassen“ und ob er überhaupt und zu welcher Zeit entleert wurde. Diese Prozedur und diese Prüfungen durch das IT-System geht im Prinzip auf der gesamten Post- Prozess-Kette so weiter.

Bis jetzt haben wir hauptsächlich über die beteiligten Personen, Fahrzeuge, Einheiten, Ressourcen, Teil-Prozessreihenfolge, Zeitabfolgen, etc. gesprochen, die dem IT-System bekannt sein müssen, und wie man sie identifizieren kann – wir haben über deren „Fingerabdrücke“ gesprochen.

Was ist mit den wichtigsten Elementen der Postdienste - Brief, Paket, etc.? Was ist z. B. der Fingerabdruck eines Briefes? Wie wird der Fingerabdruck eines Briefes „genommen“? Das Bild eines jeden Briefs wird in den Sortiermaschinen in Sekundenbruchteilen aufgenommen und zu einem Graubild gewandelt. – siehe Abbildung 4.

Die einzelnen kleinen grauen Flächen des Graubildes werden mit ihren Grauwerten – Zahlen – gespeichert. So bekommt man einen

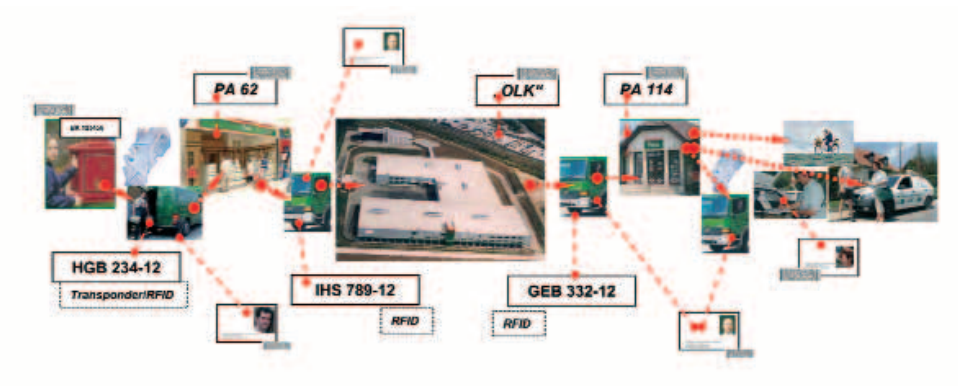


Abbildung 3: IT mit Objekt-Identifikation – „Fingerabdrücke“ – und das Post-Netzwerk

„Fingerabdruck“ von der gesamten Brief-Fläche!

Das reicht aber noch nicht. Man nimmt sich den Adressblock der Empfänger-Adresse und erzeugt ein noch feineres Graubild-Muster mit noch genaueren Grauwerten. Das ist der zweite Teil des Brief-Fingerabdrucks – der „Finger-abdruck der Adresse“ – aus dem man auch die Adresse ermittelt - siehe Abbildung 4.

Erst wenn das IT-System den „Finger-abdruck“ eines jeden Poststücks hat, kann es über die Identifizierung prüfen, ob es zur rechten Zeit, am rechten Ort, von dem richtigen Teilprozess bzw. Bearbeiter, also von all den beteiligten Elementen auf der gesamten Prozess-Kette korrekt und zuverlässig gehandhabt wurde.

Diese Identifizierung geschieht aber nicht nur allein über die Brief- und Paket-Finger-abdrücke, sondern über all die schon häufig erwähnten „Fingerabdrücke“ auf der ganzen Strecke/Prozess-Kette.

Wie geschieht das? Das Post-IT-System muss genaue Information darüber haben, was jedes

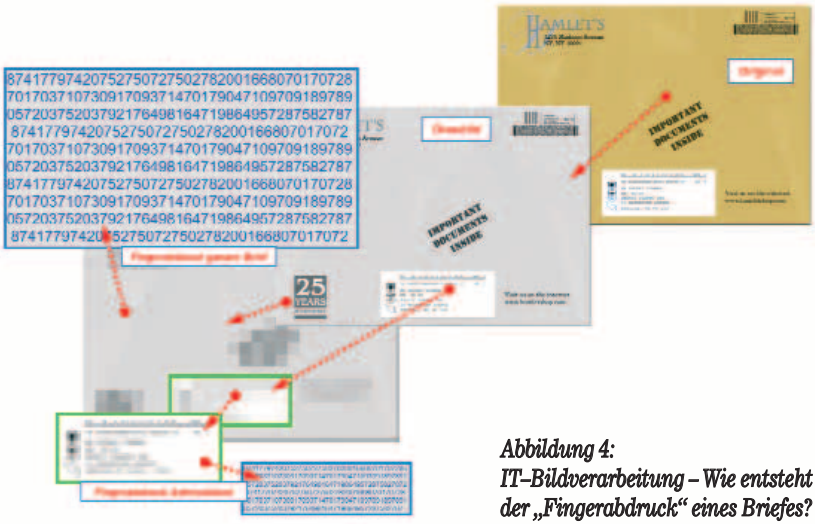


Abbildung 4:
IT–Bildverarbeitung – Wie entsteht der „Fingerabdruck" eines Briefes?

Element, jede operationelle Einheit in dem gesamten Prozess-Netzwerk – repräsentiert durch einen Identifikator / „Fingerabdruck" – tun darf, bzw. tun muss/sollte.

Erst dann kann das IT- System über die Identifizierung der beteiligten Elemente auf der gesamten Strecke/Prozess-Kette die Korrektheit und Zulässigkeit ermitteln.

Diese Identifizierung geschieht über die schon häufig erwähnten „Fingerabdrücke" auf der ganzen Strecke/Prozess-Kette.

Wie geschieht das? Was dürfen „Fingerabdrücke" im postalischen Netzwerk tun? Was tut das Post-Informations-System mit „Fingerabdrücken"? Auf Abbildung 3 sind die Fingerabdrücke der Elemente im Post-Prozess-Netzwerk dargestellt und auf Abbildung 5 sind typische „Fingerabdrücke" einiger Elemente mit ihren Rechten und Pflichten dargestellt.

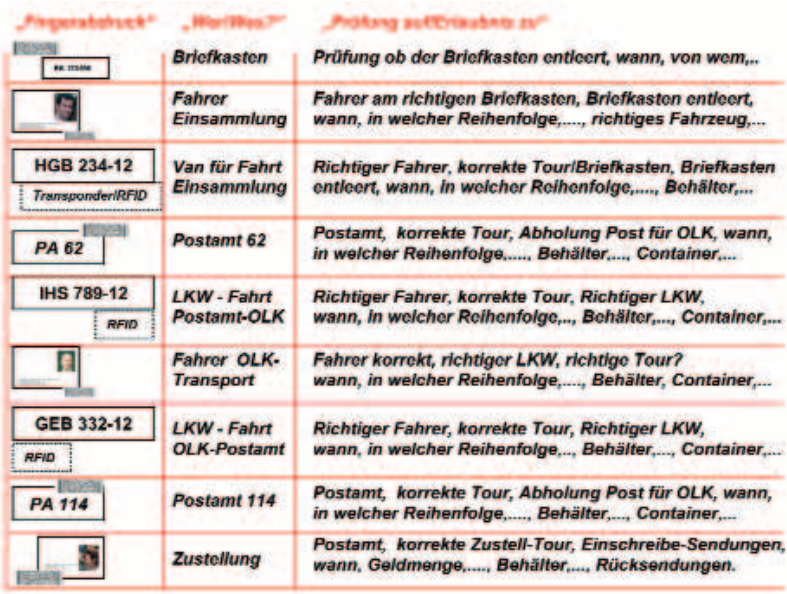
Basierend auf dieser „Erlaubnis-/Prüf- Matrix kann das IT-System all die erforderlichen Kontrollen, Steuerungen und Prüfungen durchführen.

Aber nicht nur die Fingerabdrücke und deren entsprechende Elemente müssen dem IT-System bekannt sein, sondern die gesamte postalische Prozess-Abfolge mit allen Elementen, Ressourcen, Maschinen, sowie deren Alternativen und Sonderbehandlungen.

Bevor also der erste physikalische Post-Prozess-Schritt per IT geprüft und gesteuert werden kann, muss „Alles" schon vorab in der IT-Pyramide programmiert sein – siehe Abbildung 6.

Man muss also erst alle erforderlichen Prozessdaten des physischen Post-Prozesses in die „Logische Daten-Pyramide" – in das „Logische Prozess-Abbild" gebracht haben, bevor man den operationellen physischen Prozess steuern und prüfen kann. Das gilt für all die wichtigen Teilprozesse - die wir schon kennen:

- Die Einsammlung der Post mit Briefkasten, Massenauflieferer, Postamt,...
- Die Transportlogistik zur Kollektion der Post – Fahrer, Van's,...
- Die Postämter als Sammel- und Vorverarbeitungs- Einheiten
- Die Transportlogistik von den Postämtern zu den Sortierzentren (z. B. OLK)
- Das OLK-Sortierzentrum zur landesweiten Sortierung der Post – Briefe & Pakete
- Die Transportlogistik zur Distribution der Post - zu den Postämtern & Großempfängern



„Fingerabdruck"	„Wer/Was?"	„Prüfung auf/Erlaubnis zu"
	Briefkasten	Prüfung ob der Briefkasten entleert, wann, von wem,..
	Fahrer Einsammlung	Fahrer am richtigen Briefkasten, Briefkasten entleert, wann, in welcher Reihenfolge,...., richtiges Fahrzeug,...
HGB 234-12 Transponder/RFID	Van für Fahrt Einsammlung	Richtiger Fahrer, korrekte Tour/Briefkasten, Briefkasten entleert, wann, in welcher Reihenfolge,...., Behälter,...
PA 62	Postamt 62	Postamt, korrekte Tour, Abholung Post für OLK, wann, in welcher Reihenfolge,...., Behälter,...., Container,...
IHS 789-12 RFID	LKW - Fahrt Postamt-OLK	Richtiger Fahrer, korrekte Tour, Richtiger LKW, wann, in welcher Reihenfolge,..., Behälter,...., Container,...
	Fahrer OLK-Transport	Fahrer korrekt, richtiger LKW, richtige Tour? wann, in welcher Reihenfolge,...., Behälter, Container,...
GEB 332-12 RFID	LKW - Fahrt OLK-Postamt	Richtiger Fahrer, korrekte Tour, Richtiger LKW, wann, in welcher Reihenfolge,..., Behälter,...., Container,...
PA 114	Postamt 114	Postamt, korrekte Tour, Abholung Post für OLK, wann, in welcher Reihenfolge,...., Behälter,...., Container,...
	Zustellung	Postamt, korrekte Zustell-Tour, Einschreibe-Sendungen, wann, Geldmenge,...., Behälter,...., Rücksendungen.

Abbildung 5: Die „Erlaubnis-/Prüf- Matrix für Fingerabdrücke" - z. B. in der Post-Logistik

- Die Postämter als Distributions-Einheiten für die Post
- Die Zustellung – Briefträger, Massenpost-Empfänger (HVR)

Alle in diesen Teilprozessen beteiligten Personen, Fahrzeuge, Einheiten, Ressourcen, etc. müssen schon vor dem ersten physikalischen Prozess-Schritt im postalischen Netzwerk dem IT-System bekannt sein.

Ferner muss die zeitliche Abfolge der einzelnen Teilprozesse, ihre korrekte und richtige Nutzung durch die berechtigten Personen zur richtigen Zeit dem IT System bekannt sein.

Dazu werden beispielsweise folgende Daten benötigt:

- „Fingerabdrücke" – Daten der Ausweise, Transponder - RFID- Tags, Nummernschilder,...
- Prozesse und Teilprozesse und deren korrekte Abfolgen,
- Bediener, Nutzer, Operatoren,... die diese Prozesse steuern und nutzen dürfen
- Rechte & Pflichten der Bediener, Nutzer, Operatoren - wer darf welche Prozesse nutzen?
- Wer darf die Rechte vergeben und wer legt die Pflichten der Nutzer fest

Wie bekommt man nun diese Daten in die IT-Pyramide hinein? Wie werden sie dem IT-System bekannt gemacht? Das geschieht durch sehr detailliertes und genaues vorheriges Festlegen und Programmieren der gesamten Prozesskette im logischen IT-Abbild des physikalischen Post-Prozess-Netzwerks.

In der IT-Pyramide – Abbildung 6 – ist dies prinzipiell dargestellt. Die Funktionen der verschiedenen Schichten und Ebenen der IT-Pyramide sind bereits weiter oben spezifiziert worden. Ebenso ist das Handhaben der Fingerabdrücke schon weiter oben dargestellt worden.

Auf Abbildung 6 ist gezeigt, dass sich alle Elemente/Einheiten/Ressourcen in jedem Teilprozesse mit ihrem speziellen „Fingerabdruck" identifizieren müssen.

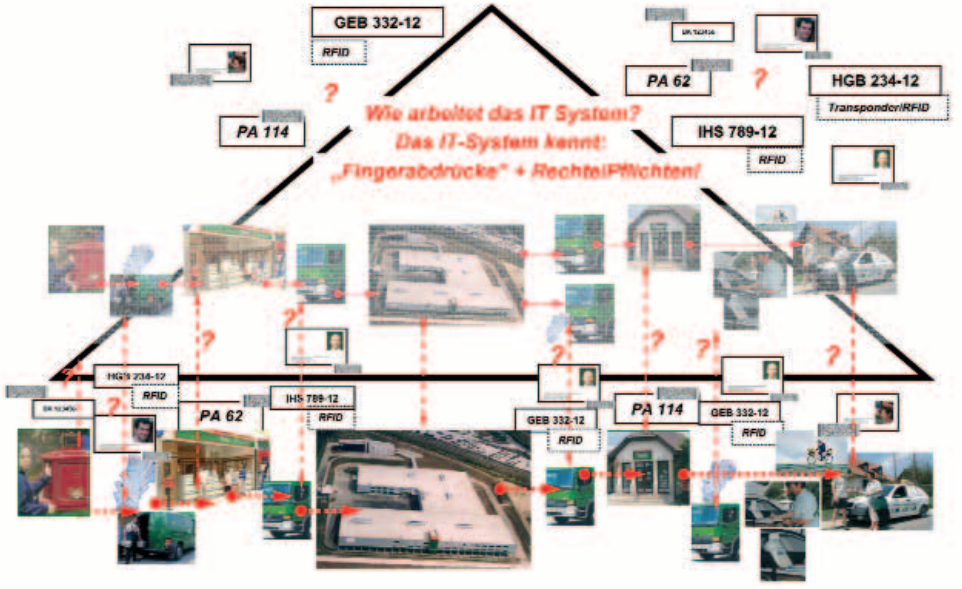


Abbildung 6: Wie arbeitet das Post IT-System im realen Betrieb mit „Fingerabdrücken"?

Das IT-System prüft dann über die „Fingerabdrücke", ob die Elemente/Einheiten/Ressourcen berechtigt sind, in dem speziellen Teilprozess zu arbeiten und ob sie in der korrekten Abfolge arbeiten.

Die lückenlose Identifizierung und Steuerung der Prozesse/Teilprozesse durch IT gilt natürlich auch für die internen Prozesse und Teilprozesse in den Verarbeitungszentren, wie für das OLK – Orszagos Logisztikai Központ in Budapest - siehe Abbildung 7.

Diese lückenlose Identifizierung schafft enorme Verarbeitungsvorteile. Wenn man z. B. die „Fingerabdrücke" der einzelnen Briefe aus den Briefsortier-Maschinen hat, und die Maschine diese Briefe in die Behälter sortiert – die eine eindeutige Identifizierung/Barcode/... „Fingerabdruck" haben, weiß das IT- System

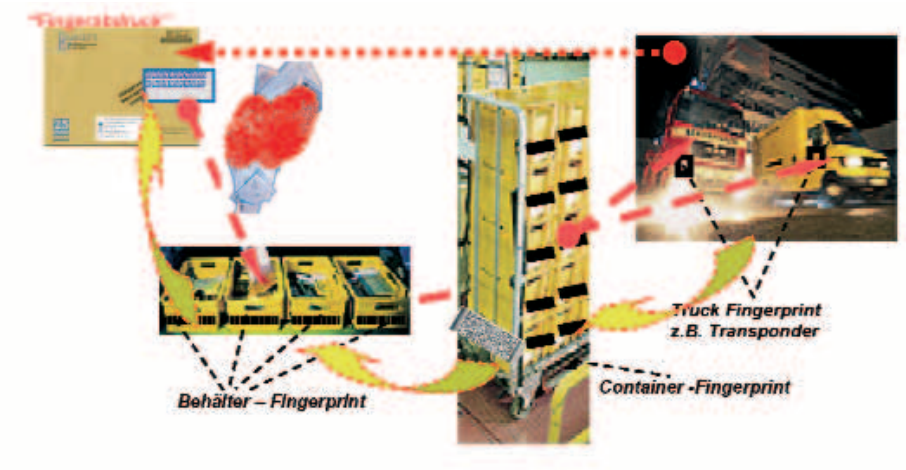


Abbildung 7: Identifizier-Technologie/ -Konzept – im Sortierzentrum „Fingerabdruck“

sofort, wenn es den Behälter-„Fingerabdruck“ liest, welche Briefe in diesem Behälter sind.

Steckt man diese Behälter in einen Container mit eindeutiger Identifizierung/Barcode/... „Fingerabdruck“ und liest die „Fingerabdrücke“ der Behälter beim Einstapeln, so weiß man sofort, wenn man den Container-„Fingerabdruck“ liest, welche Behälter im Container sind und somit automatisch welche Briefe in diesem Container sind.

Lädt man diese Container mit eindeutiger Identifizierung/Barcode/... „Fingerabdruck“ in einen LKW und liest die „Fingerabdrücke“ der Container beim Einladen, so weiß man sofort, wenn man den LKW-„Fingerabdruck“ – Transponder/RFID- Tag liest, welche Container in ihm sind und somit automatisch, welche Behälter im LKW sind und somit auch, welche Briefe in diesem LKW sind.

Überall, wo nun der LKW kontrolliert wird – „LKW-Fingerabdruck“ – weiß man sofort, welche Briefe in ihm sind. Auch bei diesen Vorgängen macht eine lückenlose Vordefinition und Vorprogrammierung der Prozesse und Teilprozesse in der IT-Pyramide erst eine lückenlose Betriebsdaten-Erfassung und korrekte Prozess-Verfolgung und Steuerung möglich. Auch dazu braucht man in der IT-Pyramide natürlich jeden erlaubten und zulässigen Brief-, Behälter-, Container- und LKW- „Fingerabdruck“. So viel zu dem IT-System in Verarbeitungszentren.

WAS KÖNNTE MAN BEI DEM IT-SYSTEM NOCH MEHR FÜR EIN „MORGEN“ TUN?

Sehr wichtig ist es dort etwas zu tun, wo es den Post-Kunden, also – „Sie“ – persönlich am meisten trifft!

Das könnte beispielsweise sein:

- Einsatz von Handheld-Terminals bei der Zustellung, oder
- eine Zustell- Ankündigung per E-Mail oder einer SMS an das mobile Telefon, oder
- Verfolgung von Sendungen über das Internet – „Track & Trace“, oder

So viel zu einem „Morgen“ des IT-Systems. Ich hoffe, Ihnen durch die vorangehenden Ausführungen die IT im Alltag der Magyar Posta näher gebracht zu haben. Wenn sie irgendwo das Logo von Magyar Posta sehen, denken Sie an die „IT- Pyramide“ und was sie für Sie im „Magyar-Posta-Alltag“ alles leistet.

Gegenwart und Zukunft der SICHERHEIT in der INFORMATIK

Risiko- und prioritätsbasierter präventiver Schutz gegen komplexe Bedrohungen

BARNA TAMÁS
– McAfee, Inc.

Vielleicht wäre dieser Titel angebracht, wenn wir Gegenwart und Zukunft der Informatiksicherheit evaluieren und zusammenfassen möchten, d. h. wenn wir die aktuellen Herausforderungen und Bedrohungen, die möglichen Antworten, die Zukunftsperspektiven und die möglicherweise voraussagbaren Risiken analysieren, mit denen Organisationen und User konfrontiert sind bzw. werden.

Es ist wichtig zu erwähnen, dass die geschäftlichen Interessen der Unternehmen in zunehmendem Masse verlangen, dass die geschäftliche Kommunikation durch das Internet erfolgt (Kontakte zu den Kunden, Partnern und Standorten usw.). Das bedeutet, dass der Sicherheit eine erhöhte Bedeutung zukommt, da auf der anderen Seite sichtbar wird, dass die Angriffe, die früher als guter Gag galten (script kidding), heute eine zerstörerische Wirkung entfalten können. Denn die verlorengegangene Zeit, in der ein Unternehmen wegen eines DOS-Angriffes (Denial Of Service) keine Dienstleistungen anbieten kann, kann äusserst hohe Kosten verursachen.

Im Bereich der Viren lässt sich beobachten, (so auch im vergangenen Jahr), dass immer neue Mutanten und Varianten der grossen „klassischen" Schädlinge in Umlauf geraten und ernsthafte Probleme verursachen. Wenn wir die Frage nach der Sicherheit stellen, stellt sich immer wieder heraus, dass viele Unternehmen gegen die Viren einfach nicht gerüstet sich.

In den Informatiksystemen ist auch in Ungarn nachzuweisen, dass die Viren der jüngsten Vergangenheit stattlich repräsentiert sind. Bei ungarischen Unternehmen wurden in diesem Jahren hauptsächlich folgende Viren ertappt:

- Zafi-D, B
- Netsky-P
- Sobig
- Mytob BE, AS, GH, EP
- Bagle (die Varianten aa, ai, bb und bd)
- Sober (besonders die Varianten Z, N)

Es ist wichtig zu vermerken, dass in diesem Jahr noch kein nach AVER als „high risk" eingestufter Virus identifiziert wurde, aber die oben genannte Liste zeigt, dass es ziemlich viele medium (mittelmässige) Viren gab. Es ist hervorzuheben, dass diese Viren zahlreiche Mutanten, Varianten haben.

Im Jahre 2005 war die wichtigste Zielsetzung der Virenschreiber nicht mehr, die globalen Angriffe zu initiieren, sondern vielmehr, für kleinere Bereiche schädliche Programme zu verfassen. Der Grund dafür ist, dass der Schutz gegen in kleiner Zahl wirksamen Viren schwieriger ist, da die weiterentwickelten Versionen der Virenschutzprogramme lang-

samer angefertigt werden. Ausserdem sind die Virenschreiber bemüht, Programme zu schreiben, die ihnen auch materiellen Nutzen bringt.

Eine negative Sensation ist, dass nach mehreren sicherheitsrelevanten Studien die Datenfischerei immer mehr Probleme verursacht: Heute ist von solchen Zwischenfällen jeder vierte User betroffen.

Die oben angeführten Untersuchungen wurden vom AVERT (Anti-Virus Emergency Response Team des McAfees, dem grössten Forschungsteam seiner Art, durchgeführt.

Um die Risiken und die darauf zu gebenden Antworten glaubhaft beurteilen zu können, müssen wir den Sinn des Sicherheits-Lebenszyklusmodells verstehen, welches einen dynamischen, ständige Eingriffe beanspruchenden Prozess darstellt.

Die oben genannten Bedrohungen haben ein für allemal nachgewiesen, dass die guten alten Schutzmaßnahmen (Virenschutz; Feuerwand, Beobachtungssysteme) nicht mehr ausreichen. Wegen ihrer Reaktivität sind sie auf der Palette der Informatiksicherheit notwendig, aber da ungefähr 70% der Bedrohungen unbekannt sind, ist der präventive Schutz nötig. Gleichzeitig ist es immer schwieriger zu entscheiden, wann im Falle eines Unternehmens die LAN-Kontakte aufhören und die WAN-Kontakte beginnen.

Die reaktiven Lösungen geben nur auf die bekannten Angriffe eine Antwort: Der bekannte exploit, worm usw. erscheint im System, und die Softwares reagieren. Im Falle eines Virus wird sofort ein pattern (Virenmuster) erstellt, das auch in die Virendefinitionsdatei aufgenommen wird. Für den Angriff wird eine Signatur erstellt.

Die Angriffe lassen sich in zwei Gruppen aufteilen:

- Angriffe gegen das System
- Angriffe gegen das Netz

Vor diesem Hintergrund hat sich McAfee zu 100% auf die präventiven Schutzlösungen umgestellt, unsere Produkte werden nach der Ebene des Systems oder des Netzes klassifiziert. Die Existenzberechtigung der zentralen Sicherheitsrahmensysteme muss auch unbedingt erwähnt werden, mit denen wir das zentrale Management unserer Produkte verwirklichen.

Von einem Unternehmen, das sich mit Sicherheit beschäftigt, kann man mit Fug und Recht erwarten, dass es Lösungspakete anbietet, die alle Plattformen unterstützen, handele es sich um Produktionsfirmen oder Systemintegratoren.

Immer mehr Unternehmen enscheiden sich für den risikobasierten Ansatz beim Schutz gegen Angriffe und suchen komplette Risikomanagementssoftwares. Die Erklärung dafür ist, dass es leider keine fehlerfreien Softwares gibt; je verletzbarer ein System ist, desto häufiger kommt es zu regelmässigen Reparaturen. Das patch management wird im Kreise der Organisationen eine immer wichtigere Rolle spielen.

Andererseits wurden bei grossen multinationalen Unternehmen gewisse Regelungen obligatorisch eingeführt (Basler Richtlinie, BS7799, SOX), die auch Multis in Ungarn betreffen. In der Zukunft kommt den riskmanagement-Lösungen eine immer grössere Bedeutung zu. Das Verständnis und die Einhaltung des Lebenszyklusmodells der Verletzbarkeit ist die Grundlage für den erfolgreichen präventiven Schutz!

Wir haben bereits Massnahmen eingeleitet, damit unsere Partner diese neuen Technologien umfassend kennenlernen, und bei den grösseren Unternehmen haben wir die bestehenden Sicherheitsregelungen studiert, vor allem die Schwachstellen.

Die Anzahl der unerwünschten Mails zeigt eine steigende Tendenz, insbesondere bei grossen Unternehmen, wo die unerwünschte Post 40%-50% der Korrespondenz ausmachen kann. Der Schutz dagegen ist das elementare Interesse eines jeden Unternehmens. Im Sinne der Effektivität sollte bereits auf der Übergangsebene filtriert werden.

Es gibt immer mehr mobile Geräte und User, was widerum neuen Viren den Boden ebnen kann. Die Anzahl dieser Viren wird in den kommenden Jahren eine steigende Tendenz zeigen. Heutzutage kann jedes seriöse Unternehmen mit umfassenden Lösungen und Technologien aufwarten.

Das schwächste Kettenglied bei der Sicherheit stellt der Mensch dar. Aus diesem Grunde kann die Bedeutung der Bildung nicht genug betont werden.

Zusammenfassend kann gesagt werden, dass sich die Voraussagen der vergangenen Jahre erfüllt haben; nämlich dass die geschäftlichen Interessen kontinuierlich steigen und die Bereitschaft wächst. Gleichzeitig werden die Angriffe immer kompexer, verfeinerter, und gegen diese können wir nur mit präventiven Maßnahmen kämpfen.

Wir müssen uns den Herausforderungen im Bereich der Sicherheit stellen, denn Sicherheit ist kein Zustand, nur ein Prozess. Ein Sicherheitsunternehmen, dass dies nicht begreift, wird untergehen.

TOVÁBBI 2006-OS RENDEZVÉNYEINK

VOLLVERSAMMLUNG – KÖZGYŰLÉS

2006. november

pontos dátum és helyszín a következő számunkban!!!!!

OKTOBERFEST

2006. október 14. – 18 óra

LeTEREMTÉStörténet

Kezdetben teremté az Úr a Bitet és a Byte-ot. És teremté ezekből a Szó-t. És a Szó-ban két bit volt, és nem létezett semmi más. És az Úr elválasztotta az Egyet a Nullától. És látá az Úr, hogy ez jó. És mondá az Úr: Legyen Adat. És így történt. És mondá az Úr: Foglalja el az Adat a megfelelő helyet. És megteremté az Úr a floppy diszkeket, a hard diszkeket és a kompakt diszkeket. És látá az Úr, hogy ez jó.

És mondá az Úr: Legyen Számítógép, ahova a floppy diszkeket, hard diszkeket és kompakt diszkeket be lehet helyezni, és elnevezte Hardvernek. És látá az Úr, hogy ez jó. És Szoftver még nem létezett akkor. De az Úr megteremtette a Programokat, nagyokat és kicsiket az ő fajtájuk szerint. És mondá az Úr: szaporodjatok és sokasodjatok, és töltsétek meg a Memóriát.

És mondá az Úr: Teremtsünk Programozót, és alkosson a Programozó új Programokat, és irányítsa a Számítógépeket, a Programokat és az Adatokat. És megteremté az Úr a Programozót, és elhelyezte a Számítóközpontban. És megmutatta neki az Úr a Könyvtárszerkezetet, és mondá neki az Úr: Használhatsz minden Könyvtárat és Alkönyvtárat, de NE HASZNÁLD a Windows-t.

És mondá az Úr: Nem jó a Programozónak egyedül. Álmot bocsátott rá, és kivette egyik oldalbordáját, és másik lényt teremtett belőle, aki felnéz a Programozóra, aki szereti azt, amit a Programozó csinál, és elnevezte az Úr ezt a lényt Felhasználónak.

És ott volt a Programozó és a Felhasználó a csupasz DOS alatt, és látá az Úr, hogy jó. De Bill okosabb volt az Úr minden más teremtményénél. És Bill megkérdezte a Felhasználót: Mondta-e az Úr, hogy ne futtass egyetlen programot sem?

És a Felhasználó válaszolt: Azt mondta az Úr, hogy használhatunk minden Programot, minden Adatot, de mondta, hogy soha se használjuk a Windowst. És monda Bill a Felhasználónak: Hogyan beszélhetsz olyasmiről, amit még ki sem próbáltál? Abban a pillanatban, hogy a Windows-t futtatod, olyan leszel, mint az Úr. Képes leszel bármit létrehozni egy egyszerű egérkattintással!

És a Felhasználó látá, hogy a Windows gyümölcsei szebbek és könnyebb őket használni. És látá a Felhasználó, hogy minden tudás haszontalan, mert a Windows képes azokat helyettesíteni. És a Felhasználó installálta számítógépén a Windowst, és mondta a Programozónak, hogy ez jó. És a Programozó azonnal elkezdte keresni az új drivereket. És megkérdezte őt az Úr: Mit keresel? És a Programozó válaszolt: Új drivereket keresek, mert nem találom őket a DOS-ban.

És monda az Úr: Ki mondta neked, hogy új driverekre van szükséged? Futtattad a Windowst? És a programozó válaszolt: Bill mondta nekünk! És monda az Úr Billnek: Azért, amit tettél, gyűlölt leszel minden teremtmény előtt. És a Felhasználó boldogtalan lesz miattad. És örökké a Windowst kell árulnod. És monda az Úr a Felhasználónak: Azért, amit tettél, csalódni fogsz a Windowsban, és az megeszi minden Erőforrásodat. Lassú programokat kell majd használnod, és örökkön örökké a Programozó segítségére fogsz szorulni. És monda az Úr a Programozónak: Azért, mert hallgattál a Felhasználóra, sohasem leszel boldog. Programjaidban hemzsegni fognak a hibák, és ki kell javítanod őket, és újra ki kell javítanod őket az idők végezetéig.

És az Úr kiűzte őket a Számítóközpontból, az ajtót bezárta, és jelszóval levédte. ÁLTALÁNOS VÉDELMI HIBA (GENERAL PROTECTION FAULT).

Rumszauer Péter

A „nagy NDK-s buli“

Az évszázadvég találkozója“ – akár ez is lehetett volna a cím, hiszen a Wende körüli és azt követő időszak végzősei találkozóját szervezte meg Bruchmann Zsuzsa és Gerő Ági március 4-én Zuglóban. Köszönet Nekik fáradhatatlan előkészítésükért, amit legjobban azzal honoráltak társaink, hogy közel százan elmentek. Reméljük újabb hagyomány teremtődött!“

Tizenéves koromban mindig csak a jövő számított; huszonévesen sem gyakran gondoltam a múltra. Most, lassan harmincöt évesen bizony-bizony előfordul, hogy gondolatban a múltban járok. Nem vágyom vissza, mert ezzel a mindennapi örömöket hazudtolnám meg; csak „elábrándozgatok“, most már nemcsak a jövőről, hanem a múltról is.

Bizony nem voltam én ezzel egyedül, amikor tavaly szeptemberben megszületett a „nagy NDK-s buli“ gondolata. Mert hiába a mindennapi örömök, ha az egyetemi emlékeket csak az NDK-sokkal (szerencsére tényleg sokkal) lehet újra átélni.

Gerő Ágival már októberben szétküldtük az első kör meghívókat, mivel nem akartuk a véletlenre bízni, hogy ki jön el. Március 4-ig hétről hétre hatványozódott a jelentkezők száma, mindenki tudott újabb és újabb címeket és neveket. A szeptemberi 30-ról márciusra közel 150 egykori NDK-st (az 1986 és 1996 között végzettek köréből) találtunk meg. Közülük 98-an jelentkeztek vissza a találkozóra, s 95-nek sikerült is eljönnie.

Mikor Ágival elkezdtük szervezni a találkozót, úgy gondoltam nem lesz könnyű összehozni ennyi embert. Arról nem is beszélve, hogy többük eltűnt a hétköznapokból, s ki gondolta volna, hogy megtalálunk 10-15 éve nem látott drezdait, berlinit, halleit, weimarit, illmenauit, cottbusit stb., pláne olyat, akit utoljára a budaörsi úti előkészítőn láttunk. Hála az internet adta lehetőségeknek, a kint töltött 4-6 év összetartó erejének, csupán két-három

email kérdése, s mindenki elérhető. S mit ad a véletlen? A szomszédom a berlini évfolyamtársam főnöke, volt munkahelyemen egy drezdai NDK-ssal ismerkedtem meg, s interjún voltam egy berlini HfÖ-snél. Mások gyerekeiken keresztül futnak össze szülői értekezleten, vagy véletlenül ugyanabba az utcába költöznek.

Kicsi a világ! Mindig hallunk egymásról, de nagyon megérett az idő a nagy találkozásra. Amikor nem csak úgy futtában, hanem nyugodtan, órákon keresztül, vacsora és borozgatás közben elmesélhetjük és meghallgathatjuk az ismert és új történeteket, a budaörsi úttól a 15-20 évvel későbbi hétköznapokig. Megnéztünk több száz gyerek fényképet, a legszebbeket, több száz régit az NDK-s napokból. Köszönet Kis Erának és akik még segítettek Neki, hogy éjszakákat töltve igazi NDK-s fényképeket gyűjtöttek, válogattak és projektorra vittek! Milyen jó volt látni azt a nagymintás tapétát a kollégium faláról, a hepehupás PVC-padlót, a jobb időket látott királykék-drapp matracokat az elengedhetetlen emeletes ágyakon, a fiúkat hosszú hajjal és bajusszal, a lányokat dauerolt lobonccal, répanadrágban és vastag övvel a derekukon. Azt a zenét hallgattuk, amit minden buliban végigüvöltöttünk; most már csak olyan szolidan, családanyásan és családapásan táncoltunk rá. S még mindig bírtuk reggel hatig!

Ez pont így volt jó! Pár órára visszacsöppeni a múltba, elfelejteni a mindennapok szürkeségét, de elmesélni az örömét, azoknak, akikkel megosztottuk éveken keresztül a mindennapok szürkeségét és örömét.

Hát ilyen volt a „nagy NDK-s buli"! Majd megismételjük! Hogy mikor? Arra majd megint megérik az idő, majd belülről megint jön az érzés, hogy milyen jó lenne találkozni a berliniekkel, drezdaiakkal, lipcseiekkel, weimariakkal stb. Azaz minden március első szombatján!!!! Veletek! Megtaláljuk egymást!

Köszönjük a lelkesedést, a segítséget a szervezésben, s hogy eljöttetek!

Bruchmann (Fazekas) Zsuzsa

NEUERSCHEINUNG:
„Mit dem Motorrad durch den Zeuner-Bau“

Studenten der ersten Nachkriegs-Generation erinnern sich

Ob Rübenernte in Mecklenburg, eine Reminiszenz an das Wohnheim „Aquarium“ oder phantasievolle Ulks zum Diplomabschluss – das druckfrisch vorliegende Buch erzählt auf mehr als 200 Seiten Geschichten an und aus der TH/TU Dresden der 50er bis 70er Jahre.

17 Autoren lassen den Leser teilhaben an den Befindlichkeiten der Studentengenerationen der ersten Jahrzehnte der DDR. Sie waren geprägt von Neuanfängen, von Hoffnungen, aber auch von politischen Repressalien, die ihren Ausdruck beispielsweise in Studentenprotesten 1956 fanden. Immer wieder aber werden in den Episoden die Lebenslust und auch der Erfinderreichtum spürbar.

Die sehr persönlichen Erzählungen spiegeln facettenreich Zeitgeschichte wieder. Es werden nachdenkliche, schwärmerische und lustige Erlebnisse geschildert und allen ist ein überaus positiver Grundtenor gemeinsam – die Freude am Leben, die Lust am Lernen sowie Hochachtung vor und Verbundenheit mit den Professoren.

Das Büchlein ist gegen eine Schutzgebühr von fünf Euro ab sofort erhältlich in: Informationsstelle der TU Dresden, Mommsenstr. 9, Glaspavillon, 01069 Dresden Öffnungszeiten: Mo bis Fr, 8:00 bis 18:00 Uhr

In der Rubrik „Lesererzählungen“ des Absolventenmagazins „Kontakt-online“ sind bereits einige dieser Geschichten veröffentlicht.

Zum Probelesen: http://www.tu-dresden.de/absolventenmagazin

Susann Mayer
Absolventenreferentin der TU Dresden
Tel.: 0351 463-36278
E-Mail: Susann.Mayer@ tu-dresden.de

Felelős kiadó / *Verantwortlicher Herausgeber*: Bornemissza Tamás, az Egyesület elnöke • Szerkesztőség / *Redaktion*: Alapfi László, Bornemissza Péter, Bruchmann Zsuzsa, Fixl Renáta, Jánosi József, Jánosi Kerstin, Korencsy Ottó, Nagy Edit, Tubik Zoltán, Rumszauer Péter, Scheida Péter • Szerkesztés, tördelés / *Layout*: Rácz Julianna • Lektor / *Lektor*: Hambuch Erika • A szerkesztőség címe / *Adresse*: 1631 Budapest Pf. 28. Fax: 36-1-403-6412 • Nyomás / *Druck*: Raabe-Kiadó Budapest – Regia Rex Nyomda Székesfehérvár • Megjelenik 1250 példányban, évente háromszor *Erscheint jährlich dreimal, Auflagenhöhe: 1250*