Zeitschrift: Schweizerische Zeitschrift für Kriminologie = Revue suisse de criminologie = Rivista svizzera di criminologia = Swiss Journal of Criminology

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 2 (2003)

Heft: 2

Artikel: Die inhärente Gefahrenproblematik der E-Mails

Autor: Bruderer, Jean-Pierre

DOI: https://doi.org/10.5169/seals-1050869

Jean-Pierre Bruderer

Die inhärente Gefahrenproblematik der E-Mails

Zusammenfassung
Die kriminologischen Aspekte der diversen Angriffe und Delikte über E-Mail, insbesondere betrügerischer Art, werden definiert, erläutert und quantifiziert. Der heutige und zukünftige Stand der potenziellen Gefahren wird beschrieben und in verständlicher Weise dargestellt. Welche Schritte können unternommen werden, um in technischer, gesetzlicher Hinsicht oder durch Vereinbarungen zwischen den Beteiligten das Risiko auf ein vernünftiges Mass zu reduzieren, ohne dass die Privatsphäre beeinträchtigt oder benachteiligt wird?

Résumé
Les aspects criminologiques des diverses attaques et délits par e-mail, en particulier ceux de type frauduleux, sont définis, expliqués et quantifiés. La situation actuelle et future des dangers potentiels est analysée et representée sous une forme graphique intégrée. Quelles sont les mesures à entreprendre afin d'être à même, sur le plan technique, législatif ou par des accords entre les interéssés, de réduire le risque à un niveau acceptable, sans pour autant mettre en cause ou réduire la sphère privée?

Summary
The criminological aspects of the various attacks and offences by e-mail, in particular those of fraudulent type, are defined, explained and quantified. The current and foreseeable situation of the potential dangers is analyzed and represented in an integrated graphical form. Which steps can be undertaken, in technical and legal regards or by agreements between the involved persons, in order to reduce the risk to a reasonable level, without impairing or reducing privacy?

1. Vorwort

Heutzutage ist E-Mail das meistgebrauchte Kommunikationswerkzeug von Internetbenutzern. Tagtäglich bekommen wir Dutzende von Mitteilungen verschiedenster Herkunft. Jeden Tag ärgern wir uns über nicht willkommene E-Mails und verwenden Zeit, Energie und öfters Unverständnis mit der Lektüre der Inhalte und der mühsamen Triage von Informationen, die wir behalten resp. lesen wollen und die wir eliminieren müssen. Nun ist es meistens so, speziell für Private und Kleinunternehmer, dass man alles lesen oder sich den Inhalt mindestens anschauen muss, um überhaupt in der Lage zu sein, eine Triage durchzuführen. Alles das ist verbunden mit dem subjektiven Gefahrenbewusstsein, dass man täglich vor Viren, Trojanern, Pädophilie, Hackern u. v. a. Begriffen gewarnt wird. Es sind Begriffe und Gefahren, die den meisten Benutzern gar nicht materiell bekannt sind. Wenn man davon ausgeht, dass Mittel- und Grossunternehmen sowie Ausbildungsinstitutionen, Verwaltungen und Behörden meistens mit vernünftigen IT-Werkzeugen und Personal dotiert sind, womit sie sich grundsätzlich gegen solche Unsicherheiten und Gefahren schützen können, sieht die Lage für die grosse Mehrheit der Internetbenutzer ganz anders aus! Dieses letztere Segment der Internetwelt ist zum grössten Teil völlig der Technologie und den damit verbundenen Angriffen und Gefahren ausgeliefert. Heute lebt man damit, betrachtet es als ein obligates Übel und jeder ist auf sich selbst angewiesen, sich zu wehren oder zu schützen! Diese Arbeit soll Vorgänge in Schwung bringen sowohl beim Gesetzgeber wie bei allen Internetintermediären, um dieser Situation mit aktiven Massnahmen, mit Schwerpunkt Kleinunternehmer und Private, entgegenzuwirken.

2. Kriminologische Aspekte der diversen Angriffe durch Internet über E-Mails

2.1. Definition: Was ist eine E-Mail und wie funktioniert sie?

Eine E-Mail ist ein Briefversand und -empfang mit Internet und wird immer an einen E-Mail

Server gesendet, der sie so lange zwischenspeichert, bis die elektronische Post vom eigentlichem Adressaten per Software – einem E-Mail Client – abgeholt wird. E-Mail-Programme wie Outlook von Microsoft Corp. erlauben das Versenden und Empfangen moderner «HTML-E-Mails». Dabei handelt es sich um Nachrichten, die wie WWW-Seiten formatiert werden. Sie erlauben fettgeschriebenen, kursiven und unterstrichenen Text sowie die Einbindung von Grafiken und Hintergrundbildern. Damit lässt sich zwar die Optik verbessern, solche E-Mails können aber auch schädliche Programmroutinen enthalten, die theoretisch wie praktisch Festplatteninhalte verändern und ausspionieren können. HTML-E-Mails, die zudem grösser sind als vergleichbare im Standard-ASCII-Format erstellte E-Mails, sollten deshalb vermieden werden[1].

Solange ein ASCII-Zeichensatz gebraucht wird ist die E-Mail gefahrlos. Die Kernproblematik für Angriffe und Gefahren liegt also innerhalb der E-Mail, beim Einsatz erweiterter Zeichensätze (MIME) z.B. für die Benutzung von HTML und angewandten Techniken (Webseiten Format), sowie der Benutzung von (Attachment)-Anlagen, die mögliche gefährdende Programmteile beinhalten können.

Meistens benutzen kleine Unternehmen (KU) und Private die E-Mail-Server der Internet Service Provider (ISP). Auf ihrer Anlage haben sie lediglich einen E-Mail-Client (Outlook, Eudora). Der Endbenutzer oder unser Zielpublikum kann natürlich seinen eigenen E-Mail-Server installieren und betreiben. Solche Tools sind günstig zu kaufen und eher einfach zu benutzen. Eine vernünftige Sicherheit setzt jedoch voraus, dass diese Benutzer entsprechend ausgebildet und mit den notwendigen Sicherheitstools ausgerüstet sind.

2.2. *Die Herkunftsarten der E-Mails und statistische Zahlen*

Vier verschiedene Herkunftsmöglichkeiten (Inflow) von E-Mails sind zu unterscheiden:

- Nachrichten stammen von Bekannten oder aus Freundeskreisen,
- weitere Nachrichten kommen vom USENET oder aus Foren,
- eine weitere Kategorie ist die der Internet-Provider und des E-Business, die E-Mails für Reklamezwecke zuschicken nachdem man sich dafür eingetragen hat (Opt-in) und
- letztlich kommen die «unerwünschten» E-Mails oder sogenannte SPAM. Der Begriff «unerwünscht» ist allerdings kein abgrenzender Begriff da er oft subjektiv erfasst wird. Grundsätzlich kann ein Betrugsversuch (SCAM) von irgendeiner Kategorie stammen, konzentriert sich jedoch auf die Kategorie SPAM.

International Data Corp. (IDC) gibt für das Jahr 2001 täglich 31 Milliarden E-Mails weltweit bekannt[2], was etwa für 500 000 000 angegebene weltweite Internetbenutzer einen Durchschnitt von heute 50–60 E-Mails über alle persönlichen Mailboxen pro Tag bedeuten würde. Zur Kenntnis nehmen kann man auch die durchschnittliche Anzahl von 1.8 E-Mailboxen pro E-Mailbenutzer. Für die Schweiz entspräche das für alle Benutzer von über 3 000 000[3] einer Anzahl von zirka 150 000 000[4] «Inflow»-E-Mails pro Tag oder ungefähr 20–30 Mitteilungen pro Mailbox pro Tag! Die Gratis-E-Mailbox ist praktisch, jedoch meistens ungenügend geschützt sowie mit Opt-In-Werbemails gekoppelt, dazu ist sie ein begünstigender Faktor für die Inflation des E-Mailflusses, der oft gar nicht notwendig wäre.

2.3. *Was für Betrugsarten[5] (SCAMs) werden als solche anerkannt und verfolgt?*

- Advance Fee Loans: Kredit mit Anzahlung.
- Bogus Credit Card Offers: Unbrauchbare Kreditkarten mit Anzahlung.
- Business Opportunities: Versprechen hoher Renditen für das eigene Unternehmen.
- Buyers Clubs: Einkaufsgruppierungen mit Anzahlung sowie Charity Scams: Betrügerische karitative Organisationen.
- Computer Equipment and Software: Extrem billige Waren mit unklarer Herkunft und Qualität.
- Credit Card Loss Protection: Betrügerische Garantien und Anzahlungen für verlorene Kreditkarten.
- Credit Repair: Täuschung Dritter mit falschen Urkunden.
- General Merchandise Sales: Falsche oder keine Lieferung sowie verbotene Produkte.
- Information/Adult Services: Access durch kostspielige Internet Anschlüsse von Erwachsenen-Seiten.

1 http://www.glossar.de/glossar/1frame.htm?http%3A//www.glossar.de/glossar/z_email.htm.
2 http://www.idcresearch.com/getdoc.jhtml?containerId=27975.
3 www.wemf.ch/d/studien/manet.shtml.
4 www.statistik.admin.ch unter: société de communication.
5 National Consumers League, Washington, D.C. 20006 http://www.fraud.org/tips/internet/internet/inttip/inttip.htm.

- Internet Access Services: Betrügerisches Angebot an Dienstleistungen, die nie erbracht werden.
- Investment Scams: z.B. Optionen und Future-Handel sowie Penny-Stocks, Churning.
- Job Scams: Angebote von Jobs oder Dienstleistungen gegen Anzahlung.
- Magazine Sales: Angebot und Verkauf literarischer Natur, die nicht geliefert werden.
- Nigerian Money Offers: Transfer von Geldern aus Nigeria.
- Online Auctions: Nicht liefern, mangelnde Qualität oder kopierte Werke.
- Prizes and Sweepstakes: Lotterien gegen Entgelt.
- Pyramids and Multilevel Marketing: Schneeballsysteme allgemein.
- Scholarship Scams: Lernangebote mit Diplomen.
- Travel Fraud: Meistens Time-Share.
- Work-at-Home Scams: Nebenjobs für Heimarbeiter, die meistens in schneeballsystemartigen Aktivitäten enden.

Für die meisten dieser Betrugsarten bestehen Trendanalysen und Daten aus den USA, die wir später veranschaulichen werden. Auf nationaler Stufe gibt es keine Statistiken und Daten. Hier wäre auch eine Stichprobenerhebung von grösstem Nutzen[6]!

2.4. Angriffe zum Missbrauch oder zur Kontrolle des PCs[7] oder LAN kommen meistens über die Anlage (Attachment) der E-Mail

Es ist nicht der Sinn dieser Arbeit, die verschiedenen Angriffsarten inhaltlich und technisch zu analysieren[8]. Wir werden jedoch verschiedenste Angriffsformen in den weiteren Kapiteln explizit erklären (Trojaner, Keylogger, Virus, Worm).

Eine Kuriosität, die meistens völlig unbeachtet, unbekannt und eher mysteriös im Vorgehen scheint, sind die Web-Bugs oder Web-Beacons. Diese unsichtbaren Pixel/Bilder sind in HTML-E-Mails eingebettet und werden manchmal für forensische, jedoch massenweise für Marketing- und Kundenprofilierungs-Zwecke ohne das Wissen des Benutzers eingesetzt. Ich erwähne hier diese Möglichkeit, obschon es sich a posteriori nicht um einen direkten Angriff handelt, jedoch die objektive Möglichkeit besteht, Persönlichkeitsprofile und Personendaten durch Queranalysen zu erzeugen, daran zu gelangen und sie später wieder bei SPAM oder Marketinganalysen einzusetzen[9].

Zum jetzigen Zeitpunkt genügt es, zu verstehen, dass diese Angriffsarten täglich vorkommen und alle Internetbenutzer darunter leiden müssen. Es bestehen einige Angaben über den wirtschaftlichen Schaden, die m. E. jedoch rein spekulativer Natur sind. Es ist jedoch unbestritten, dass jeder Angriff viel Zeit und auch Geld und Verluste herbeiführt. Meiner Kenntnis nach wurden keine Stichprobenerhebungen und Umfragen bei Kleinunternehmern und Privatbenutzern durchgeführt, die relevant sind. Schutz gegen solche Angriffe wird anhand von Virenschutz-Software geleistet. Diese Applikationen müssen jedoch von den Benutzern selbst gekauft, (herunter-)geladen, installiert und à jour gehalten werden. Neben dem Vorbehalt, dass nicht jedermann in der Lage ist, diese Handhabungen professionell durchzuführen, kommt die Problematik der Geschwindigkeit und Frequenz dazu, mit der solche Angriffe ausgeführt werden. Wie später noch gezeigt wird, ist die Tendenz solcher Gefahren exponentiell steigend!

2.5. Attacken um private PCs oder Netzwerke zu zerstören oder zu lähmen (DOS, E-Mail Bombing)

Praktisch jeder PC kann angegriffen werden. In der Praxis haben die ISPs, die ja meistens auch die Mail-Server einsetzen, auch die notwendigen Abwehrmassnamen bereit, um solchen Attacken entgegenzuwirken. Diese Art von Attacken kann für unsere Arbeit vernachlässigt werden, da nur sehr selten Private und KUs Opfer solchen Angriffe sind.

2.6. Kriminologische Angaben für Betrugsversuche per E-Mail

Ausgangslage und Erkenntnisse von frühren Arbeiten: Je höher die Frequenz eines Vorkommnisses im Betrugsbereich, desto kleiner der verursachte Schaden. Die Frequenz der Delikte steht im direkten Verhältnis zur Kommunikationstechnik. Das Internet spielt dabei eine wesentliche Rolle in der Zunahme und Frequenz

6 NDS-BWK 1: Workshops I+II: Anlagebetrug: Teil Kriminologie: 2002.
7 PC ist von der Usanz her ein Begriff (Personal Computer) der auf IBM und Microsoft-Normen und -Kompatibilität hinweist. Darum werden heute diverse Begriffe wie Laptop, Desktop, PAD, Handhelds usw. gebraucht um auf die Unabhängigkeit der anwendbaren Betriebsysteme hinzudeuten. Für unsere Arbeit brauchen wir «PC» im generischen Sinne.
8 www.symantec.com oder www.mcaffee.com.
9 http://www.bugnosis.org und http://www.privacyfoundation.org/resources/webbug.asp.

von wertmässig eher bescheidenen Delikten. E contrario, je persönlicher der Kontakt mit dem Opfer und je komplexer das Geschäft ist, desto grösser ist der Schadenswert pro Fall[10].

Zum Zwecke der Vergleichbarkeit und der Analyse haben wir mehrere Kausalvariablen definiert und segmentiert. Diese Typologie findet sich im Anhang: Kriterien und Katalogisierung von Variablen im Bereiche des Internetbetruges durch E-Mail. Die verschiedenen Kausalvariablen sind: kriminelle Organisationsstruktur, Komplexität des Vorganges, Frequenz, Kontaktart zum potentiellen Opfer (da wir aber die Betrugsarten auf Internet per E-Mail analysieren ist diese Segmentierung nicht relevant) der Schadenswert sowie, abgeleitet als abhängige Variable, der prozentuale Gesamtanteil einer Betrugsart.

Als Grundlage für diese Analyse haben wir drei amerikanische Studien genommen und erweitert[11]. Die erste stammt von Internet Fraud Watch[12]. Die US-Organisation National Consumer League's arbeitet mit The national Association of Attorneys General and the Federal Trade Commission (FTC) zusammen. Quasi als Konkurrentin arbeitet eine andere US-Organisation namens IFCC: The Internet Fraud Complaint Centre mit National White Collar Crime Centre and the Federal Bureau of Investigation zusammen. Die IFCC hat auch eine Trendstudie in Bearbeitung[13]. Erstaunlicherweise überschneiden sich die beiden Studien eher schlecht, sind trotzdem z. T. aufschlussreich, weil sie dem Publikum mindestens Angaben und Trends zu Verfügung stellen. Da die Angaben nur auf voluntärer Basis von Betroffenen beruhen, kann von statistisch relevanten Daten nicht die Rede sein. Die FTC erstellt jährlich seine eigene Zusammenstellung[14].

Wir notieren dabei den Einbezug des Diebstahls von Credit/Debit-Cards und den Missbrauch von Identitäten als zusätzliche Betrugsart. Unseres Erachtens ist der CC/DC-Betrug nicht ein typischer Internet- oder E-Mail Betrug, obschon die Übermittlung der Inhaberdaten mit unverschlüsselten Kommunikationsträgern grundsätzlich als fahrlässig zu beurteilen ist. Frequenzen und Sachschäden werden vom FTC nicht über Internet publiziert.

Die FTC meldet für das Jahr 2001 Schäden von über USD 160 000 000 und über 118 000 Klagen. Diese Information ist interessant, weil man damit einige Hochrechnungen wagen darf. Experten der IFCC gehen davon aus dass nur 10% der Betrugsfälle gemeldet werden. Eine einfache Rechnung für die USA ergäbe Folgendes: Schaden USD 1 600 000 000 mit 1 118 000 Fällen und einen ausbezahlten Betrag von 1838 USD für 74% der Betroffenen (Medianwert circa. 270 USD).

Anzahl Internet Verbindungen in den USA[15] in 2001, 102 000 000. Das Ratio bewegt sich bis 1% oder ein Interbetrugsfall pro hundert Internetbenutzern pro Jahr.

Auf schweizerische Verhältnisse angepasst würden diese Kennzahlen Folgendes ergeben:

Anzahl Internet Verbindungen (private und KUs) in der Schweiz 2001: 2 800 000[16]. Mögliche Geschädigte bis 1%= bis 28 000. Ergebnis: Schaden bis CHF 60 000 000 pro Jahr für die analysierten E-Mail Betrugsmöglichkeiten und das Zielpublikum.

10 NDS-BWK 1 Luzern: Workshops I+II: Anlagebetrug: Teil Kriminologie: 2002.

11 Für die Vollständigkeit der Quellen erwähnen wir noch: http://www.imsn-ricc.org/ und www.econsumer.gov . Das Seco ist Mitglied beider OECD Organisationen: http://www.seco-admin.ch/d_index.html. Die verfügbaren Informationen die in den Beschwerdetrends (http://www.econsumer.gov/deutsch/contentfiles/pdfs/German.pdf) sind für unsere Arbeit nicht verwendbar.

12 www.fraud.org/tips/internet/internet/inttip/inttip.htm.

13 Home Page : http://www1.ifccfbi.gov/index.asp.

14 www.consumer.gov/sentinel/images/charts/top2001.pdf.

15 Von Jupitermedia Corporation: http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html.

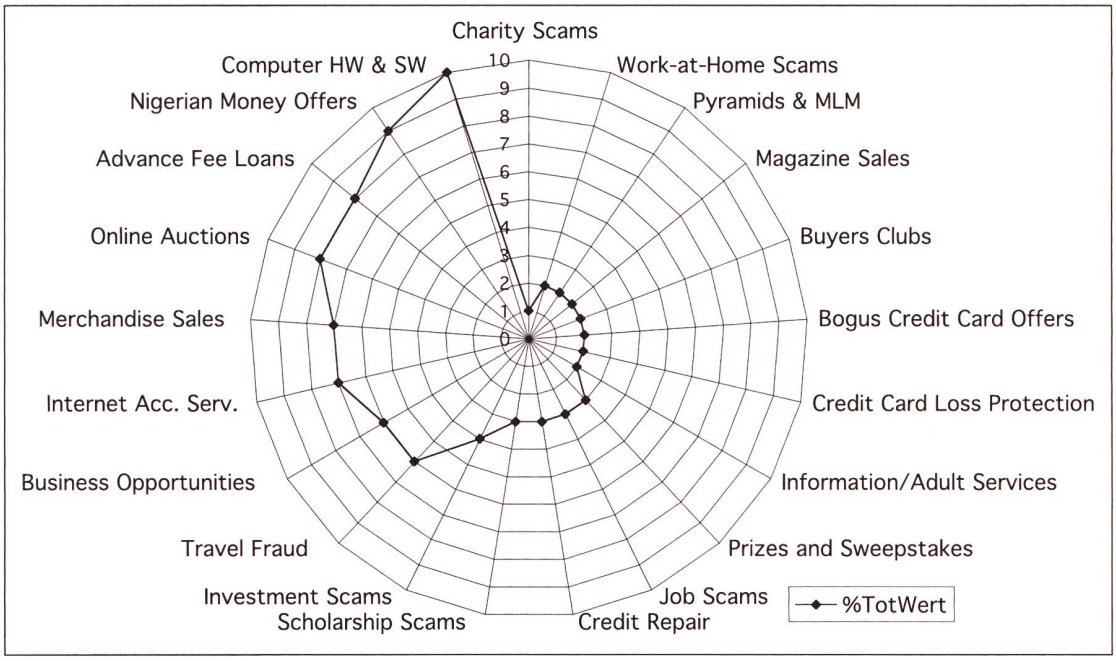
16 http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106f_302_synth.htm.

Die bearbeitete Tabelle mit den verschiedenen Variablen ergibt folgende Resultate[17]:

Betrugsarten	Organisation	Komplexität	Wert/Klasse	Frequenz	%TotWert
Charity Scams	5	5	1	1	1
Work-at-Home Scams	4	4	1	2	2
Pyramids & MLM	2	2	2	1	2
Magazine Sales	5	3	2	1	2
Buyers Clubs	5	5	3	1	2
Bogus Credit Card Offers	6	7	3	1	2
Credit Card Loss Protection	6	6	3	1	2
Information/Adult Services	7	6	3	1	2
Prizes and Sweepstakes	7	6	2	4	3
Job Scams	4	3	4	1	3
Credit Repair	5	3	4	1	3
Scholarship Scams	5	4	8	1	3
Investment Scams	7	7	10	1	4
Travel Fraud	6	6	10	2	6
Business Opportunities	7	6	10	2	6
Internet Access Services	7	4	4	4	7
General Merchandise Sales	5	4	6	5	7

Es ist sehr erstaunlich, dass speziell im Bereich Investment und Börse wenige Daten erfasst worden sind! Das kann ein Hinweis sein, dass sich nur Ausgebildete und Wohlvermögende (Siehe: Technokrat[18]) ausserhalb des Internets damit beschäftigen und oder dass sich ein Kunde selten ohne Nachfolgeerklärungen auf dieses Business einlässt! Frappant sind natürlich die eher tieferen Sachschäden der Internetbetrüge, die aber erwartungsgemäss mit unserem globalen Betrugsmodell kohärent bleiben.

Die gesamtwirtschaftliche Relevanz der E-Mail Betrugsarten:

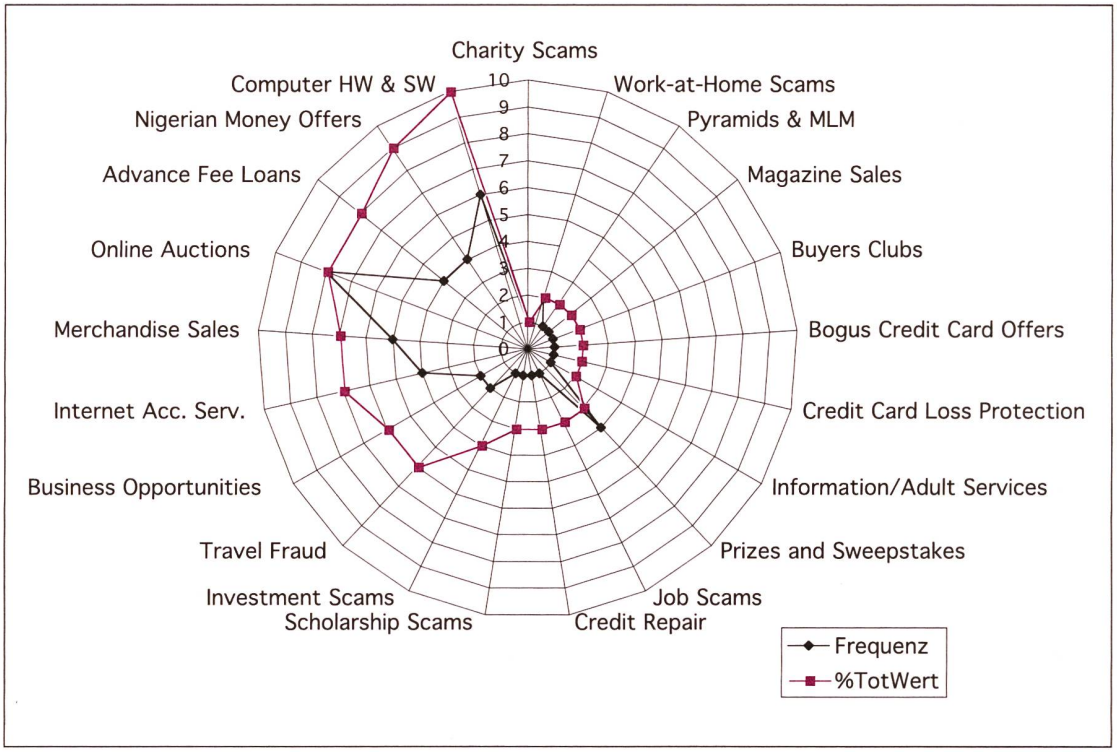


Einleuchtend sowohl für Präventivmassnahmen wie für den Schutz der Internetbenutzer ist die linke Seite des Bildes. Mit dieser Information kann man auch entsprechende Prioritäten festsetzen.

17 Bemerkung zur Tabelle: Diese Daten konnten nicht mit Hilfe statistischer Erhebungen durchgeführt werden, sondern wurden mit Hilfe zahlreicher Informationsquellen erzeugt. Sie sind also nicht als abschliessend und wissenschaftlich eindeutig klare Daten zu betrachten und dienen lediglich dem Verständnis der Tendenzen und der Prioritäten.

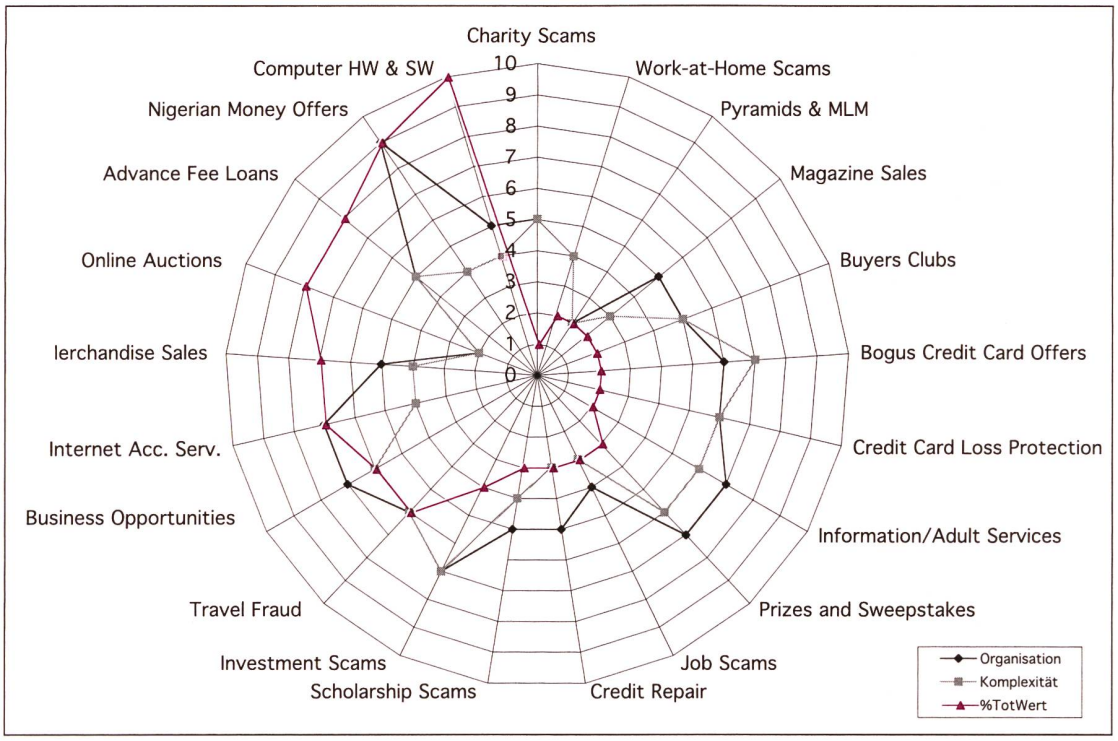
18 VI Materialien b) Kriterien und Katalogisierung von Variablen im Bereiche des Internetbetruges durch E-Mail.

Gesamtanteil der E-Mailbetrugsarten vs. Intensität der Angriffe:



Die Angaben deuten auf eine mögliche Hierarchie der E-Mail-Frequenz, die man in der Mailbox findet. Es deutet hin, dass sowohl Opt-in als auch SPAM dabei benutzt werden. Die Korrelation der Variablen beträgt 0.81. Mehr + wiederholte Angriffe = bessere Erfolge!

Gesamtanteil der E-Mailbetrugsarten vs. Komplexität und kriminellen Struktur:



Die Korrelation zwischen Organisationsform und Komplexität beträgt 0.65 und ist somit zu berücksichtigen. Zu bemerken ist, dass die Wichtigkeit der Betrugsarten weder mit der Organisationsform noch mit der Komplexität des Vorganges korreliert sind! Es braucht somit keine oder kleinere Strukturen um einen Erfolg zu erzeugen, wie auch grössere (kriminelle) Organisationen und Strukturen notwendig sein können um «bescheidene» Resultate zu erreichen. Hinter jedem Typ von Organisation kann aber ein überlagertes OK stehen! Eine permanente Trendanalyse der verschiedensten Betrugsarten ist umso wichtiger, als sich die Techniken, Vorgänge und Mentalitäten sich sehr schnell verändern können[19].

Cyberatlas[20] prognostiziert für die kommenden Jahre einen Benutzerzuwachs von 445.9 Millionen auf 709.1 Millionen im Jahr 2004, also eine Zuwachsrate von zirka 50%. Was die Anzahl E-Mails betrifft schätzt International Data Corp (IDC) für das Jahr 2006 täglich über 60 Milliarden E-Mails weltweit[21]. Somit ergäbe das eine Verdoppelung des Verkehrs und eine Progression des E-Mail Inflow von über 40% auf circa 80 pro Benutzer pro Tag oder circa 40 pro Mailbox! Die Problematik der Bearbeitung dieses Problems ist bei grösseren Unternehmen erkannt worden. Was die KUs und privaten Personen betrifft, ist dieses Problem weder aktuell noch sind Massnahmen getroffen worden, um der Arbeitslast und den Gefahren mit wirksamen Mitteln entgegenzuwirken. Somit liegt es klar auf der Hand, dass die beschriebenen Gefahren zurzeit eine schöne und viel versprechende Zukunft vor sich haben!

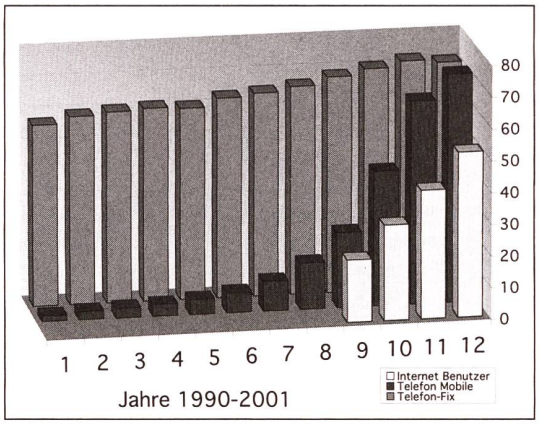
Ob die Missbrauchmöglichkeiten der heutigen HTML-E-Mail Technologie sowie neue Technologien in diesen Prognosen berücksichtigt wurden, ist eine offene Frage, die wir im nächsten Kapitel besprechen wollen.

3. Technische Aspekte und Entwicklungen im Zusammenhang mit der E-Mail Gefahrenproblematik

3.1. Der Handy Markt zum Vergleich der Internetbenutzern

Ende 2001 hatten 72.4% der Bevölkerung ein Mobiltelefonabonnement[22], das sind mehr als jene für Festnetzanschlüsse! Die Entwicklung, im Vergleich von Internetanschlüssen (Gelb) zu MobilT (Violett) für die letzten Jahre ist in der linken Graphik ersichtlich.

Absolute Werte ergeben für 2001 bis 2002 folgende Daten: 2 200 000 Internetanschlüsse 3 000 000 Internet- und 5 200 000 Handybenutzer. Die Benutzerwelten beider Gruppen decken sich von Natur aus vermutlich stark, somit kann man ohne grösseres Risiko sagen, dass der Internetbenutzer ideale Vorraussetzungen mit sich bringt um sich auch für die Handytechnologie zu interessieren und damit die Entwicklung



dieser Produkte zu verfolgen. Dieser Gruppe von Leuten erscheint die heutige Handy Technologie natürlich eher archaisch und limitiert!

Warum ist diese Gegenüberstellung interessant? Nachdem SMS und WAP nur einige Jahre mit grossem Erfolg am Markt angekommen sind, werden sie nach und nach ersetzt werden. Techniken wie MMS (Multimedia Messaging Service) einerseits und die Miniaturisierung diverser Komponenten andererseits, erlauben den Einbau von diversen Betriebssystemen in Telefongeräte. Heute schon mit GPRS und in 1 bis 3 Jahren mit der UMTS-Technologie wird genügend Bandbreite (Geschwindigkeit und Kapazität) angeboten werden, um Betriebssysteme auf Pocket-Computer (Palm, Microsoft CE, Symbian Linux oder MAC) mit HMTL und andere ähnliche Programmiersprachen wie die neue SMIL-Technologie von Handys auf «Telefon-Computer» zu übernehmen.

Am 24.10.2002 meldete GSMBOX[24]: «Orange SA, l'un des premiers opérateurs mondiaux de téléphonie mobile, filiale de France Télécom, et Microsoft Corp., premier fournisseur mondial de

19 http://www1.ifccfbi.gov Siehe Trendanalyse und Jahresvergleiche 1999–2001.
20 http://cyberatlas.internet.com/big_picture/geographics/print/0,,5911_151151,00.html.
21 http://www.idcresearch.com/getdoc.jhtml?containerId=27975&sectionId=tableofcontent&pageType=SECTION.
22 http://www.statistik.admin.ch/stat_ch/ber20/indic-soc-info/ind30106f_302_synth.htm.
24 http://fr.gsmbox.com.

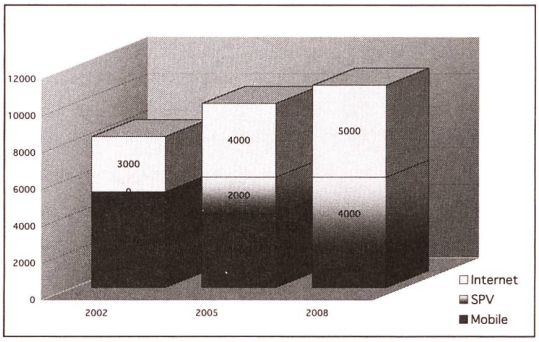
services logiciels et de technologies Internet pour les entreprises et les particuliers, annoncent le lancement du SPV[25] (Son Photo Vidéo), le premier Smartphone sous Windows. Le SPV est un téléphone mobile qui, pour la première fois, offre un accès ouvert au monde des services Internet et permet une synchronisation avec un PC grâce à sa station d'accueil et au logiciel Microsoft Outlook fourni dans le coffret. Il se distingue également par sa compacité et la qualité haute résolution de son écran 65 000 couleurs, ainsi que par une parfaite acoustique.»

Diese Mitteilung ist insofern von zentraler Wichtigkeit, weil sie den strategischen Entscheid von Microsoft bestätigt, in den sehr profitablen Markt der Mobiltelefone einzusteigen und sich somit einen neuen und enormen Markt anzueignen, wie das für den PC Markt (leider[26]) der Fall ist. Seit dem Jahr 2000 hat der Handy-Hersteller Nokia mit seiner Nokia 9XXX-Communicator Serie[27] und dem Symbian-OS-Betriebssystem den Markt zu erobern versucht. Es reichte ihm jedoch aus mehreren Gründen – nicht zuletzt infolge der limitierten Geschwindigkeit von GSM – bis jetzt nicht, sich erfolgreich durchzusetzen. Da der Markt mehr und mehr Brandbreite anbietet, werden die Vorteile und die Kompatibilität der Betriebsysteme (Palm, Symbian oder Linux) mit den PCs und Pocket-PCs und deren Microsoft-Betriebsystemen sowie das neue Angebot mit SPV umso beliebter sein und auf fruchtbaren Boden fallen.

Es kommt mittelfristig zu einem technischen Zusammenschluss von Telefonie und Pocket-Computern, der unumgänglich ist!

3.2. Der Handy Markt im Vergleich zu Internetbenutzern

Wenn wir uns auf die schweizerische Ebene beschränken, kann das Potenzial für die nächsten 2–6 Jahre folgendermassen umrissen werden: Auf einer ersten Ebene können die jetzigen Desktop/PC-Benutzer auf den Markt des SPV aufspringen. Das sind zirka 3 000 000 Benutzer, die den aktuellen Benutzerstand verdoppeln könnten. Mit der Senkung der Preise für SPV, die man erwartet, werden zusätzliche Handykunden in den SPV- Kreis einbezogen. Das könnte nochmals eine Verdoppelung der Benutzer bedeuten. Somit kann man, ohne zu weit ins Detail gehen zu wollen, vom Potenzial her annehmen, dass sich die heutige Gefahrenwelt u.U. verdreifachen kann. Dieser Zuwachs ist bedingt durch das Angebot an Breitband im



Telekommunikationssektor sowie den Zusammenschluss von Telefonie und Pocket-Computer-Technologie.

Diese Entwicklung wird natürlich zum Zuwachs der Möglichkeiten von diversen Angriffen auch massgebend beitragen. Was den Bereich der Viren, Trojaner, Würmer u.a. betrifft, wird die Zielgruppe viel grösser sein und besonders riskant wird die Schnelligkeit der Infizierungen sein, die sich u.U. im Minuten- oder Stundenbereich nicht nur auf schweizerischer Ebene, sondern europaweit oder sogar weltweit verbreiten können. Diese Situation kann materiell Dutzende von Providern während Stunden wenn nicht Tagen stilllegen. Die Konsequenzen sind absehbar. Was die Betrugsproblematik betrifft, inkl. SPAM und alle «Reize», die durch das Internet angeboten werden, wird sich die Flut von E-Mails und Angeboten im gleichen Masse wie für die oben genannten Attacken verdoppeln oder verdreifachen. Damit werden Betrugsmöglichkeiten und Erfolge proportional steigen. Mehr + wiederholte Angriffe = Grössere Erfolge!

Bei einer Wahrnehmung dieser möglichen Zukunftsrisiken scheint es wichtig, den heutigen Stand des Rechts und der getroffen Gegenmassnahmen zu prüfen! Darum werden wir in Kapitel 4 verschiedene Problemkreise, welche die Sicherheit der Benutzer beeinflussen, eingehender analysieren.

25 Wir werden aus praktischen Gründen als Begriff für die neue kombinierte Technologie in dieser Arbeit das Akronym SPV verwenden.

26 Meines Erachtens ist die monopolistische Position eines Softwareherstellers nach rein wirtschaftlicher und sicherheitspolitischer Betrachtung weder vertretbar noch akzeptabel. Linux als ernster «Kleinkonkurrent» wird sich vielleicht in diesem neuen Markt auch erfolgreich durchsetzen können!

27 http://www.nokia.ch/german/phones/9210i/specs.html.

4. Recht, Interessenkonflikt, Politik und Internationalisierung als Einflussfaktoren

Wir beschränken uns auf Gefahren, die durch E-Mails heraufbeschworen werden können, siehe dazu Abschnitt 2.1. Da SPAM einen markanten Anteil der Verantwortung für alle Arten von Angriffsmöglichkeiten trägt, werden wir diese Problematik mit einbeziehen. Wir betonen nochmals, dass Betrugsversuche durchaus mittels Mail-Listen (Opt-in), USENET oder sogar durch Freunde (Schneeballsysteme) erfolgen können. Dabei ist es wichtig, die Gesamtheit der E-Mail-Herkunft im Auge zu behalten.

Die Risiken teilen sich in zwei Gruppen: a) Attacken mit Viren, Würmern oder Trojanern inkl. Spionage-Software und b) Betrugsversuche, um den Kunden in Versuchung zu führen, bei Anbietern (E-Commerce oder Privaten) für eine Dienstleistung einen Auftrag und damit Geld zu erhalten. In allen Fällen kann man davon ausgehen, dass die Täterschaft mit Vorsatz handelt.

4.1. Praktische Aspekte nach Schweizer Recht aus der Sicht der Benutzer-Opfer

Viren, Würmer oder Trojaner inkl. Spionage-Software sind Angriffe, die in der Literatur nicht oft juristisch besprochen wurden[28]. Die strafrechtlichen Aspekte kann man folgendermassen umschreiben:

Viren

Grundsätzlich kann Art. 144bis StGB, Datenbeschädigung, zur Anwendung kommen:

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.
   Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.
2. Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.
   Handelt der Täter gewerbsmässig, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

   Allerdings ist zu beachten, dass nicht alle Viren den Bedingungen des Art. 144bis genügen, da sich einige nur auf der Harddisk festsetzen, ohne weitere Schäden anzurichten.

Würmer

Im Gegensatz zu Viren expandieren Würmer, z.B. eingenistet in Dokumente, von selbst, indem sie aus der Adressendatei Adressen aussuchen, meistens in Microsoft Outlook, und sich dann an verschiedenste Adressaten weiterverschicken und somit andere Systeme verseuchen. Die Schäden können für das infizierte System fataler Natur sein. Die Anwendung von Art. 144bis StGB, Datenbeschädigung, hat auch für Würmer ihre Berechtigung und es gelten daher dieselben Überlegungen bezüglich der Risiken für die Opfer.

Trojaner

Ein Trojaner repliziert sich nicht von selbst und führt verschiedene ungewollte Programme auf einem System durch. Ein Trojaner wird meistens mit Vorsatz einem Opfer verdeckt zugeschickt oder vom Opfer unbewusst von einer anderen Anlage heruntergeladen. Ein Trojaner ist demzufolge ein reines Vehikel, das auch keinen Erfolg bewirken könnte, wenn es leer wäre. Somit kann ein Trojaner eine lange Liste von möglichen Programmen verstecken, die sowohl destruktiver wie informativer Natur sein können.

Ein Virus- oder Wurm-Opfer trägt a posteriori keine Verantwortung gegenüber Dritten, die es weiter infiziert, wenn es nicht mit Vorsatz handelt. Allerdings, da sich ein Virus selbst repliziert (sich jedoch nicht von selbst auf externe Systeme ausbreitet, wie das Würmer tun), kann es durchaus vorkommen, dass das erste Opfer ungewollt eine solche infizierte Datei weitergibt und damit andere Systeme infiziert, im Speziellen mit der Virusvariante der Macro-Viren, die sich z.B. in Windows-Outlook-Dateien einnisten können. Da stellt sich natürlich die Frage der Mitverantwortlichkeit des ersten Opfers für einen eventuellen Mangel an Sorgfalt bei der Handhabung seines Systems, wenn das zweite Opfer finanzielle Ansprüche erhebt. Damit könnte das erste Opfer beweisen müssen, dass es zum Zeitpunkt des Versandes der

28 http://www.weblaw.ch/jusletter/Artikel.jsp?ArticleNr=1957&Language=1 Computer crimes in Cyberspace A comparative analysis of criminal law in Germany, Switzerland and Northern Europe von Prof. Dr. Christian Schwarzenegger.

infizierten Folge-E-Mail nicht wusste oder wissen konnte, dass sein Computer bereits infiziert war. Dazu kommt, dass Gerichte immer noch mit der genauen Definition der IT-Begriffe konfrontiert bleiben. Somit sind die Gerichte oft auf den genauen Sachverhalt angewiesen, der meistens von IT-Experten beschrieben werden kann. Durch die Schnelllebigkeit der IT und insbesondere die unzähligen eingesetzten Attackenvarianten, die u.U. Hunderte pro Jahr betragen und somit Definitionen und den Sachverhalt wieder in Frage stellen, sind alle beteiligten Opfer, Kläger, Ermittlungsbehörden und Gerichte in ihren Aktionen gelähmt und auf die Mitarbeit von externen Experten angewiesen. Da solche Expertisen mehrere Monate in Anspruch nehmen und die Prozesse mehrere Jahre dauern, kann diese Situation bei bestem Willen alle entmutigen. Dies erklärt auch, obwohl Tausende von Benutzern jährlich von Angriffen betroffen sind, warum heute unserem Wissen nach keine Verfahren laufen[29].

Spionage-Software[30]

Neben Viren und Würmern kann ein Trojaner sehr oft Spionage-Software transportieren. Keylogger sind herkömmliche Applikationen, die mit der Absicht des Ausspionierens von Passwörtern und besuchten Web-Seiten oder zur Kontrolle von Korrespondenz eingesetzt werden. Die Abgrenzung zwischen erlaubt und nicht erlaubt hängt von der Absicht und dem Vorsatz ab. Strafrechtlich kommt hier Folgendes zur Anwendung, abhängig von der Bereicherungsabsicht entweder:

Art. 143 StGB, Unbefugte Datenbeschaffung

1. Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.
2. Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Oder: Art. 143bis StGB, Unbefugtes Eindringen in ein Datenverarbeitungssystem

Wer ohne Bereicherungsabsicht auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

Ferner sind für solche Delikte auch Aspekte des DSG, UWG zusätzlich zum ZGB/OR zu prüfen.

Eine Spionage-Software kann ohne weiteres einem Täter die technische Möglichkeit bieten, um verdeckt und im Unwissen des Besitzers der missbrauchten Anlage über dieses Drittsystem auf dem Internet ein Delikt, das dem Art. 147 StGB entspricht, durchzuführen.

Art. 147 StGB Betrügerischer Missbrauch einer Datenverarbeitungsanlage

1. Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.
2. Handelt der Täter gewerbsmässig, so wird er mit Zuchthaus bis zu zehn Jahren oder mit Gefängnis nicht unter drei Monaten bestraft.
3. Der betrügerische Missbrauch einer Datenverarbeitungsanlage zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Aus der Sicht der Benutzer-Opfer sind diese repressiven Massnahmen ein kleiner Trost, da sie u.U. selbst zur Verantwortung gezogen werden könnten und mit der Komplexität, Zeit, Schwierigkeit und nicht zuletzt mit den damit verbundenen Anwalts- und Expertenkosten, wenn ein Prozess sich z.B. auf die internationale Ebene ausdehnt, konfrontiert werden. Auf ziviler Ebene ist die Situation genauso schwierig, da die klagende Partei noch den Beweis des erlittenen Schadens erbringen muss. Wer will heute schon in KUs oder als Privater solche

29 Wenn solche Verfahren im Gange wären, wäre es auch für unsere Problematik höchst interessant diese verfolgen zu können.

30 http://dir.searchcentralstation.com/spyware.html at The Web's Most Convenient Source for Searching.

Verfahren in die Wege leiten, wenn die Kosten meistens die Schäden übersteigen und sich solche Angriffe mehrmals pro Jahr wiederholen? Präventive und adäquate Schutzmassnahmen muss jeder mögliche Betroffene selbst treffen, zum Beispiel die Installation von Anti-Viren, -Trojanern, -Würmern sowie anderer «Firewalls» vornehmen, und, was die wenigsten tun, eine angebrachte Software gegen Spionage und Keylogger installieren. Das alles bedingt relativ hohe Summen, viel Zeit und Erfahrung, um einigermassen zur Abwehr bereit zu sein. Von den Grenzkosten her ist dies aber immer noch billiger, als straf- und zivilrechtliche Verfahren einzuleiten. Dieser Umstand ist jedoch nicht tolerierbar, solange die Gesellschaft nicht die notwendigen und möglichen Massnahmen getroffen hat, solche Risiken auf ein akzeptables Niveau zu reduzieren. Meines Erachtens akzeptiert jeder vernünftige Bürger, ein Restrisiko auf sich zu nehmen, wenn diese Voraussetzungen erfüllt sind. Solange es nicht so ist, werden Hemmschwellen, Unsicherheiten und Frust die Entwicklung speziell von E-Commerce weiter bremsen.
Die rechtliche Lage sowie die jetzigen Strukturen für den Bereich Internet und im Speziellen durch E-Mail erwirkte Betrügereien sind aus diversen Optiken zu betrachten.

Bagatellenproblematik[31]: Wie früher schon begründet, handelt es sich um Betrugsarten, deren Frequenz sehr hoch und deren Einzelwerte niedrig sind, jedoch höhere Gesamtwertanteile ausweisen und vom Sachverhalt her öfters einfachere Betrugsarten über das Internet sind! In Anbetracht der durch die Täterschaft gesamthaft bewirkten hohen Schäden und eher kleinen Schäden pro Betrugsopfer fragt man sich, wie die Haltung der Ermittlungsbehörden in diesem Spannungsfeld ist? Art. 172ter StGB und der Aspekt des «geringen Vermögenswertes» gemäss BGE 121 IV 191 können ein Grund sein, solche Delikte zu vernachlässigen. Weiter stehen heute weder ein Kompetenzzentrum noch eine effektive Clearingstelle zur Verfügung, die in der Lage wären, die Klagen für dieselben Betrügereien zu sammeln, zu koordinieren und/oder zu bearbeiten. Der Fall «Genesis» ist für diese Thematik ein Schulbeispiel. Seitens der Betrogenen stellt sich da wieder die Frage des Kosten-Nutzen-Verhältnisses. Die Hemmungen und die finanziellen Aspekte sind dieselben wie oben beschrieben. In einem derartigen Umfeld fehlt es an Motivation, sowohl bei den Opfern wie bei den rechtlichen Instanzen.

SPAM[32] ist ein Übel, das täglich in der Literatur kommentiert wird. Im Gegensatz zur EU besteht in der Schweiz keine ausdrückliche Regelung für das Spamming. Vorgesehen ist im neuen Fernmeldegesetz (FMG) der Art. 45a, Unerwünschte Mitteilungen: Anbieterinnen von Fernmeldediensten verhindern mit geeigneten und zumutbaren Massnahmen die Übermittlung von Werbemitteilungen an Kundinnen und Kunden, die dazu nicht ihre ausdrückliche Zustimmung gegeben haben oder nicht schon in einer Geschäftsbeziehung mit der Absenderin oder dem Absender der Mitteilung stehen.

Demzufolge wird in absehbarer Zeit (1–2 Jahre) in der Schweiz das Spamming strafbar und das dürfte einen Beitrag zum aktiven Schutz der Benutzer leisten. Zumindest was die Verbreitung unerlaubter Werbung schweizerischer und europäischer Herkunft betrifft, dürfte dies positive Auswirkungen haben. Meine Besorgnis bleibt trotzdem gross, da Spamming weiterhin massiv eingesetzt werden kann und auch wird. Der Grund dafür liegt darin, dass es für jedermann einfach ist, einen eigenen E-Mail-Server einzusetzen, Werbemails übers Ausland oder von nicht regulierten Gebieten aus zu versenden. Insbesondere durch den Einsatz von Proxy Servern[33] wird die Täterschaft weiterhin verdeckt bleiben. Das Aufdecken der Täterschaft ist durch den Gebrauch solcher Mittel nur sehr schwer möglich – wenn überhaupt!

Die Überprüfungs- und Vorsichtspflichten der Geschädigten. Bei einer Klage auf Betrug gemäss Art. 146 StGB, Warenfälschung, ist es von vorneherein unklar, ob die Klägerin in der Lage sein wird, beweisen zu können, dass sie alle Vorsichtsmassnahmen gemäss Lehre und Rechtsprechung eingehalten hat. Die meisten Betrugsarten kommen a priori aus dem angelsächsischen Raum, sind in englischer Sprache[34] (heute mehr und mehr in verschiedene

31 II Literaturverzeichnis: NDS-BWK 1: Workshops I+II: Anlagebetrug: Teil Kriminologie: 2002

32 http://www.weblaw.ch/kompetenzzentrum/content/mathias_kummer_spamming.pdf

33 Mit dem Gebrauch von 2-4 hintereinander gereihten Proxy-Servern die sich zwischen den Computern des Senders und des Adressaten befinden, bildet der Spammer eine anonymisierende Kette, die weltweit zerstreut sein kann. Damit verhindert er kurzfristige und rasche Ermittlungen. Da er aber die Kette willkürlich nach jeder versandten E-Mail wechseln kann, steht der Ermittler vor einem Problem ohne verhältnismässige Lösung.

34 Ein markanter Anstieg von betrügerischen Vorkehren über E-Mail, seit kürzerem auch in deutscher Sprache aus dem nordeuropäischem Raum kommend.

Sprachen übersetzt), können aber materiell von irgendeinem Punkt unseres Planeten Erde kommen. Eine Klägerin kann mit dem Einwand konfrontiert sein, sie hätte wissen müssen und können, dass Betrugsrisiken von E-Commerce sowie durch Private grösser sind als mit den üblichen lokalen Einkaufsschemen. Ferner zu beachten, und das kann eine entscheidende Hemmschwelle für ein Opfer sein, ist die Problematik der meist durch den Import von ausländischen Dienstleistungen und Gegenständen induzierten eventualvorsätzlichen MwSt.-Hinterziehungen[35]. Allerdings muss sich die Klägerin von Anfang an bewusst sein, dass sie gegebenenfalls für dieses Verhalten zur Rechenschaft gezogen werden kann!

4.2. Dogmatische Aspekte, Interessenkonflikte, Föderalismus und Informationspolitik

4.2.1 Dogmatische Gedanken zur E-Mail

Das Fernmeldegesetz (FMG) definiert weder Elektronische Post noch E-Mail oder angewandte Mailvarianten[36]. Im VüPF wird das Wort E-Mail in der ganzen Verordnung angewendet. Wir müssen annehmen, dass es im Sinne von Elektronischer Post zu verstehen ist und damit alle Mailvarianten[36] miteinbezogen sind. Der Inhalt der E-Mail wird folgendermassen definiert: «Art. 2 Definitionen f. Nutzinformationen: der Anteil des zu überwachenden Fernmeldeverkehrs, welcher die zwischen Benutzenden bzw. zwischen deren Endeinrichtungen ausgetauschten Informationen (z. B. Laute, Telefax, E-Mails) enthält;»

Im Datenschutzgesetz (DSG) werden die «Nicht»-Personendaten definiert[37]. Dazu kommt noch in BGE 1A.104/1999/odi vom 05.04.2000: «[...]Dieser Umstand würde nichts daran ändern, dass im Rahmen des technisch Möglichen die Geheimsphäre der E-Mail-Benützer dennoch verfassungsmässig zu wahren ist». Damit erkennen wir, dass E-Mail formell nirgends definiert ist und die Begriffe Personendaten, persönliche Daten, Geheimsphäre und Nutzinformationen ohne Abgrenzung gebraucht werden. Somit ist die Verständlichkeit der Gesetze für den Leser nicht besonders erleichtert! Mindestens ist BV Art. 13 «Schutz der Privatsphäre 1. Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs. 2. Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.» eine Erleichterung. Wir brauchen somit den Wortlaut «persönliche Daten» als Gesamtbegriff, den wir aber hier nicht abschliessend definieren. Die Formulierung bleibt damit offen!

Wenn wir von einer E-Mail in unserem Kontext sprechen, stossen wir auf die Fragestellung: Was ist der genaue Inhalt des Kommunikationsträgers? (E-Mail und Attachment). Ganz bestimmt sind es persönliche Daten die geschützt sein müssen. Wir haben aber auch gesehen, dass dieselben Kommunikationsträger in sich nicht ersichtliche Angriffsmittel verbergen können (es spielt an sich keine Rolle, ob diese Angriffsmittel im Träger oder am Träger «angezapft» sind). Diese Situation ist an sich nicht neu und kommt beim Brief- und Postverkehr manchmal auch vor (Anthrax oder Briefbomben), bei der E-Mail allerdings mit bemerkenswerten Unterschieden zu andern Kommunikationsträgern. Infizierte E-Mails können in einem gleichen Zeitraum in Unmengen versandt werden. Es sind auch Merkmale, die intern zu Unterschieden zur Natur der elektronischen Post sowie extern zu anderen Kommunikationsträgern führen:

a) E-Mail als Kommunikationsträger ist nicht ummittelbar lesbar, aber automatisch oder elektronisch replizierbar. Ein Fax (elektronisch oder manuell) kann keine Viren verbergen. b) Eine E-Mail geht in die Kategorie der elektronischen Post, ist aber innerhalb dieser Kategorie von SMS, WAP und MMS zu differenzieren. c) Die Einzigartigkeit der E-Mail ist somit die Möglichkeit, zusätzliche nicht ersichtliche Angriffsmittel zu vehikulieren und zu verbergen[38]. Eine E-Mail gleicht deshalb weder einem Brief oder Fax noch einem Fernmeldegespräch. Darum besteht m.E. eine Konfusion beim Gesetzgeber, wenn man annimmt, dass eine E-Mail anderen Kommunikationsträgern gleichzustellen und gleich zu behandeln sei. Wenn die «E-Mail» als rechtlich definiertes Kommunikationsvehikel in der Kategorie

35 Vallender K. A., Schweizerisches Steuer-Lexikon, Bundessteuern 2, Seite 44 und folgende.

36 FMG Art. 3 Begriffe In diesem Gesetz bedeuten:
a. Informationen: für Menschen, andere Lebewesen oder Maschinen bestimmte Zeichen, Signale, Schriftzeichen, Bilder, Laute und Darstellungen jeder anderen Art.

37 Im Sinne von: Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt, Art. 2 Geltungsbereich Abs. 2a DSG.

38 Wir besprechen hier nicht die Problematik, Handhabung und Verhaltensweise bei Sondermassnahmen, was die Erfassung, Überwachung und Bearbeitung von verseuchten E-Mails anbetrifft!

Merkmale	Computer oder Schrift Urkunde	Unmittelbare Lesbar- oder Hörbarkeit	Automatische Replizierbarkeit	Verseuchung durch Viren[45]
Elektronische Post				
a) E-Mail mit HTML inkl. Anhang	CU	nein	ja	ja
b) E-Mail ASCII oder SMS	CU	nein	ja	nein
c) WAP	CU	nein	ja	möglich
d) MMS	CU	nein	ja	möglich
Brief	SU	ja	nein	nein
Fax elektronisch	CU!	nein	ja	nein
Fax manuell	-	ja	nein	nein

«elektronische Post» anerkannt wäre, wären damit auch die Anwendungsbereiche von Gesetzen und Verordnungen eindeutiger zu definieren und zielgerichteter durchsetzbar. Die Lehre könnte dabei zur Problematik Sicherheit contra Schutz der persönlichen Daten und der präzisen Definitionen von E-Mail und anderer elektronischer Post abschliessend Stellung nehmen.

4.2.2. ISPs und Interessenkonflikte mit BüPf, FMG und DSG

Der Stellenwert des Schutzes der persönlichen Daten ist von Natur aus hoch. Viele Gruppierungen und Organisationen sind unter dem Stichwort «Privacy» sehr aktiv. Die Gründe dazu kann jedermann im heutigen weltpolitischen Umfeld der US-Machtdominanz und der täglichen Nachrichten von «Big Brother»-ähnlichen Vorkommnissen verstehen und begrüssen. In diesem schwierigen Spannungsfeld müssen die Vorlagen, Vernehmlassungen und Gesetze für Sicherheits-, Schutz und Repressivmassnahmen letztlich auch im Interesse der Bevölkerung durchgezogen werden. Oftmals ist dies verbunden mit viel Kritik und Unbehagen. Das DSG hat bei diesen Vernehmlassungen und Vorlagen eine gewisse Garantenposition, um den Schutz der persönlichen Daten und der Geheimhaltung der Kommunikationsinhalte zu verteidigen. Es ist eine Art heilige Kuh, die quasi unantastbar ist! Die Schlüsselstelle der ISPs ist für KUs und Private aber so wichtig, dass ohne ihre aktive Miteinbeziehung in die Konstruktion von Schutzmassnahmen keine Lösung vorstellbar ist.

Es ist klar, dass die ISPs von Natur aus und auch als Unternehmen äusserst ungern Auflagen und Mehrkosten auf sich nehmen wollen und eine eher negative Einstellung zu diesem Vorgehen haben, das die allgemeinen Interessen vertritt. Aus der Sicht der Benutzer aber bieten viele ISPs ungenügende Dienstleistungen, insbesondere bezüglich Sicherheit und Schutz der meist zahlenden Kunden. Verschlüsselung, Virencheck[39] der Attachments, Virencheck im HTML-Format, Junk-E-Mail oder SPAM sind entweder «unbekannte» Begriffe oder es werden nur dürftige Anwendungen angeboten, bei denen der Benutzer meistens die ganze Arbeit selber machen muss.

Wir haben mehrere ISPs seit Jahren bezüglich der oben genannten Kriterien getestet und benutzt[40]. Ein beispielhaftes Angebot ist das private deutsche Unternehmen WEB.DE, das alle Kriterien, mit Ausnahme von SPAM, erfüllt. Das Dienstleistungsunternehmen ist mit dem heutigen Stand der Technik und mit seinem Angebot (frei und zahlend) an vorderster Front[41]. Das Erstaunlichste ist, dass äusserst gute Produkte zur Anwendung kommen könnten, wenn dies die ISPs tun wollten. Wir denken da im Speziellen an Anti-Spam- und Anti-Viren-Konzepte und -Produkte. Zum Beispiel existieren weltweit Black-Listen von bekannten Spammern, die von verschiedenen Organisationen à jour gehalten werden. Einige Anwendungen haben diese Black-Listen in ihre Anti-Spam-Software integriert. Damit wird ohne menschliche Intervention eine grosse und zeitraubende Selektionsarbeit automatisch durchgeführt! Erwägungen, weshalb solche Anwendungen nicht von ISPs eingesetzt werden, sind finanzieller und opportun-minimalistischer Natur und lassen sich nur durch Konkurrenz- und Ertragsmotive erklären. Demzufolge bieten mindestens in der Schweiz die ISPs keinen akzeptablen Schutz vor den definierten Gefahren und Angriffen. Die Be-

39 Virencheck wird als Sammelbegriff für sämtlich beschriebene Angriffsformen, die durch E-Mails importiert werden, gebraucht.

40 Siehe auch: http://www.pctip.ch/archiv/2002/10.asp suche unter 11/02 Wie sicher sind Ihre E-Mails?

41 Siehe www.web.de.

nutzer haben auch hier das Recht auf eine qualitativ hochstehende Dienstleistung hinsichtlich Schutzmassnahmen und Komfort, besonders in der Schweiz, die weltweit eine der grössten Internet-Benutzerraten ausweist.

Bei Verdacht eines gefährlichen Inhalts in einem Brief kann die Post diesen scannen und, wenn der Verdacht begründet ist, angemessene Massnahmen anordnen oder anordnen lassen, um den Brief zu öffnen und die Gefahr zu entfernen. Dieses manuelle Vorgehen wäre für E-Mails unverhältnismässig. Dafür gibt es Virenscanner. Beim Scannen kann nicht ausgeschlossen werden, dass der Inhalt der Nachricht gelesen werden kann. Wenn eine E-Mail infiziert ist, wird es gemeldet und sie wird neutralisiert. A posteriori kann ein Sachkundiger immer noch Teile des Inhalts lesen, wenn er auf die neutralisierte Datei Zugriff hat. Solange eine private Person einen Virenscanner einsetzt, stellt das kein Problem dar. Wenn eine Drittperson im Auftrag handelt und diese Drittperson den Inhalt beim Scannen nicht ändert oder weiterverwendet und die entsprechenden überprüfbaren Massnahmen trifft, dann sollte einer solchen Vorgehensweise nichts im Wege stehen.

Auf deutschem Gebiet führt die WEB.DE auf Antrag zwei Operationen durch: a) HTML-E-Mail auf eine ungefährliche, lesbare Art umsetzen und auf Viren checken b) Virencheck für Attachments mit vorherigem Bestätigungsantrag. An sich ist das perfekt. Es liegt auf der Hand, dass dieser Vorgang auch von Schweizer ISPs angewendet werden sollte, allerdings unter Berücksichtigung der Anwendung von gesetzlichen Vorschriften und Massnahmen gemäss FMG und DSG.

4.2.3. Massnahmen auf Bundesebene

Das Bundesamt für Polizei[42] hat die Problematik der Cyberkriminalität erst spät wirklich erkannt und hinkt heute noch ein wenig hinter ausländischen Konkurrenzstaaten her. Die Befugnisse und Aufgaben der zukünftigen Cybercops stehen auf wackligen Beinen. Es ist unklar, wie weit und wie konsequent Informationen im Bereich der Wirtschaftskriminalität gesucht werden, was überhaupt mit diesen geschehen wird und wie sie zu den betroffenen Benutzerkreisen gelangen sollen. Meines Erachtens liegt diese Situation weniger an der Wachsamkeit einzelner Organe oder Personen, als viel mehr an der Festlegung von Prioritäten durch die Politik, die föderalistischen Strukturen und Gremien, wie z. B. den kantonalen Polizeidirektoren-Konferenzen, Vernehmlassungen und parlamentarischen Prozessen, bei denen langsamer entschieden wird als notwendig wäre. Die Kompetenzverteilung zwischen Bund und Kantonen aber, ist und bleibt aus rein technischer Sicht KEIN gewichtiges Hindernis für Lösungsansätze. Zum ersten braucht es eine Grundlage mit wissenschaftlich überprüften Daten im Bereich der Wirtschaftskriminalität und insbesondere auch der Cyberkriminalität, um sicherheits- und schutz-strategische Ziele definieren zu können. Zum zweiten wird eine Lageanalyse durchgeführt, um mit Kosten-Nutzen-Gegenüberstellungen sachlich über die Realisierung von möglichen Aufgabenteilungs-Varianten im Bereich Prävention, Repression und Schutz zu befinden. Durch die Errichtung von interkantonalen Kompetenz- und/oder Clearingzentren werden die Sicherheits- und schutzpolitischen Ziele durchgesetzt.

4.2.4 Die Beteiligung des SECO an der Bekämpfung der Internetkriminalität

Die Schweiz ist zusammen mit anderen OECD-Mitgliedern, zirka 30, an folgende Organisationen angegliedert: http://www.imsnricc.org/ und www.econsumer.gov. Bei econsumer.org kann ein Geschädigter oder Opfer ein Beschwerde per Internet einreichen. Der Erfolg scheint bis jetzt bescheiden zu sein und das Angebot ist in der Benutzerwelt unbekannt.

4.2.5. Die Konsumentenschutzorganisationen

Die Stiftung für Konsumentenschutz bietet mehrere Links auf der Seite Computer+Internet[43]. Die Unterstützung wird von Swiss Internet User Group gewährleistet. Eine umfassende Beschreibung der Betrugsproblematik ist darin nicht zu finden.

4.2.6. Die jetzige Schutzmassnahmenpolitik aus der Sicht der Benutzer

Heute ist aus der Sicht der Benutzer weder von einem nationalen strategischen Schutzkonzept gegen Betrug noch gegen Betrug über das Internet zu hören, wie das für die Finanzmarkt-Aufsicht und -Regulierung für den Schutz des Finanzplatzes Schweiz der Fall ist. Eine öffent-

42 http://www.bap.admin.ch/d/aktuell/berichte/Cybercrime_SAB_200110_d.pdf.

43 http://www.konsumentenschutz.ch/content/links_computer_internet.html.

liche Informationsstelle, Meldestelle für Wirtschaftskriminalität oder ein pro-aktives Schutzkonzept für die Bevölkerung bestehen nicht. Noch sind die Voraussetzungen dafür nicht geschaffen, solange die Wahrnehmung der Probleme und Zukunftsrisiken nicht auf die politische Ebene gelangt sind.

4.3. Internationale Massnahmen und Wahrnehmungen

Auf der Ebene des Europarates besteht die Convention on cybercrime[44]. «The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.» Die Ratifizierung der Konvention konnte aus gesetzlichen Gründen von der Schweiz noch nicht vorgenommen werden. Das Werk ist jedoch ein wesentlicher Beitrag zur politischen Förderung der Wahrnehmung der Probleme, der Klärung verschiedener Aspekte des Internets und deren Lösung, die uns alle betreffen.

Auf EU-Ebene ist die Kommission auch im Kampf gegen die Cyber-Kriminalität im breitesten Sinne aktiv. Es sollen hier informativ nur die Links angegeben werden[45].

Die US Behörden haben eine offizielle Melde- und Informationsstelle für Cyberkriminalität. Dieses Organ wird von der Criminal Division of the US Department of Justice geführt[46].Wir haben am Anfang unserer Arbeit eingehend die verschiedenen US-Organisationen besprochen, die sich mit Internetbetrug befassen. Bemerkenswert ist die aktuelle eingeleitete Aktion der Administration Bush unter dem Titel: The national Strategy to secure Cyberspace[47]. Dieses US-Dokument, als nationale Plattform gestaltet, dient somit als Grundlage einer regen Diskussion und ist meines Erachtens auch ein Konzept, das durchaus, wenn auch nicht bedingungslos, in angebrachter Form für die Vorbereitung einer schweizerischen, nationalen Strategie gedacht sein kann. Durch Sensibilisierung und Motivation aller Partner, die von der Problematik in der Schweiz betroffen sind, kann damit auch das Bewusstsein für die Mitverantwortung aller Betroffenen gefördert werden.

4.4. E-Mail, ein Vehikel ohne Schutz!

Abschliessend für dieses Kapitel kann für den heutigen Zustand in der Schweiz bezüglich aktivem Schutz für KUs und Private, sei es für Betrügereien und Angriffe über E-Mail oder für die übergeordnete Cyberkriminalität, Folgendes festgestellt werden:

a) E-Mail wird als Kommunikationsträger rechtlich ungenügend definiert. Es bestehen keine für E-Mail bestimmte gesetzliche Grundlagen die den Eigenschaften dieses Trägers Rechnung tragen um spezifische Handlungen zu verbieten oder anzuordnen.
b) ISPs vertreten in Bezug auf Dienstleistung und Schutz gegenüber den Kunden eine minimalistische Haltung, obschon diese eine eminent wichtige und zentrale Rolle spielen sollten.
c) Die grosse Mehrheit (95% der 3 000 000 Benutzer) sind nicht in der Lage, die technischen Sicherheitsprobleme ohne grosse Ausgaben für Spezialisten und Anschaffung von Spezialsoftware sicherzustellen. Hilflosigkeit und Unbehagen herrschen.
d) Die gleichen Benutzer sind bei den oben geschilderten Betrugsarten und Angriffen meistens hilflos, weil die Unkenntnis und die Angst vor Rechtsschritten hemmend wirken. Das gilt auch dann, wenn eine kritische Haltung gegenüber Lieferanten und Dienstleistenden einzunehmen wäre.
e) Kontextbezogen steht keine öffentliche Struktur zu Verfügung um die Benutzer aktiv zu informieren. Bekannte Meldestellen und Ausbildungsprogramme gibt es auch nicht.
f) Strukturell bestehen weder strategische Zielsetzungen noch Grundlagen, die es erlauben würden, solche mit wissenschaftlich erzeugten Daten zu gestalten. Die föderalistischen Strukturen wirkend bremsend. Die Wahrnehmung der Zukunftsrisiken ist auf politischer Ebene nicht spürbar.

44 http://www.coe.int/de/default.asp#Suche und der Text der Convention: http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Combating_economic_crime/Cybercrime/Convention/default.asp#TopOfPage.
45 Siehe die Web-Seite http://europa.eu.int/information_society/topics/telecoms/internet/crime/index_en.htm und das Programm http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf.
46 http://www.cybercrime.gov.
47 http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html#Intro.

5. Massnahmen kontext-, struktur- und individuell- bezogener Natur

Konsens genügt bei Sicherheitsfragen nicht. Empfehlungen sind auch keine Lösungen, solange sie nicht rechtskräftig umgesetzt werden. Mit diesem Vorsatz wollen wir diverse Aspekte der Schutzproblematik im Internet, insbesondere für die inhärenten E-Mail Gefahren angehen:

5.1. Utopie und Zielsetzungen

Das Schöne bei einer Utopie ist die Überzeugung des Betroffenen, dass etwas zu erreichen sei, obschon die Mittel und der Wille der anderen dazu fehlen. Meistens ist eine Utopie aber materiell durchführbar, andere Einflussfaktoren erlauben das sofortige Erreichen des Zieles jedoch nicht. Was für Ziele hätten wir?

Global gesehen stellen wir fest, dass sämtliche Hardware-Komponenten eine Nummer tragen (z. B. MAC), die weltweit eindeutig (französisch: univoque) gekennzeichnet ist. Alle Computer, die im Internet verbunden sind, sind mit einer eindeutigen Nummer versehen (IP). Alle Telefone haben auch eine eindeutige Nummer! Somit kann man sich vorstellen, dass jeder Internetbenutzer, der auf dem Netz Mitteilungen senden oder empfangen will, also eine Mailbox braucht, dazu eine eindeutige Identifikation erhält[48]. Darunter versteht man eine I-Identity. Diese Nummer kann durch bestehende Organisationen vergeben werden, die z.B. heute schon die IP-Adressen verwalten. Jede I-Identity gibt das Recht, nebst der wirklichen Identität des Inhabers, zur Wahrung der Anonymität, mit Pseudonymen im Internet zu verkehren. Eine Person kann mehrere I-Identities besitzen. ISPs haben die Auflage, bei Neukunden persönlich geschützte E-Mailboxen mit I-Identity anzubieten und unter ihrer Obhut zu verwalten. Für Unternehmen kommen die gleichen Regeln sinngemäss zur Anwendung. Ein Internetbenutzer kann auf dem Netz surfen, Dateien herunterladen und chatten, auch wenn er keine I-Identity besitzt.

Mit der Anwendung einer solcher Regel wird die Kernursache von Angriffen und infizierten E-Mails grösstenteils gelöst, da wie bei IPs, Autonummernschildern usw. der Absender identifizierbar ist. Bei ankommenden E-Mails, SMS, WAP oder MMS prüft der Mail-Server, ob die I-Identity gültig ist. Wenn dies nicht der Fall ist, wird die Nachricht nicht erfasst. Die Durchführbarkeit ist technisch ohne weiteres möglich.

Der Identifizierungsaufwand des Benutzers muss im Verhältnis zum Risiko bleiben. Zum Beispiel: Bei der Eröffnung einer E-Mailbox bei WEB.DE verlangt die Firma die Zustelladresse des Benutzers. WEB.DE schickt per Post einen Code, den der Benutzer eingeben wird, um in die Zone zu gelangen, wo alle Schutzmassnahmen (kostenlos) angewendet werden. Für kostenpflichtige Dienstleistungen wird die Identität per CC/DC erfasst. Weitere komplementäre Möglichkeiten für die Vertrauensförderung und Identifizierung werden z. B. von Verisign[49] angeboten.

Wir sind seit mehreren Jahren mit der Macht- und Monopolposition von Microsoft Corp. konfrontiert. Diese Situation hat einen direkten Einfluss auf die geforderten Preise dieser Firma. Betriebssysteme sind nach 2 bis 3 Jahren obsolet und neuere Versionen von Anwendungspaketen wie Office werden auch alle 2 Jahre erneuert und zu stolzen (mehrere hundert CHF) Preisen angeboten. Hier geht es nicht mehr um den freien Markt, es geht darum, dass der Benutzer es kaufen muss, weil er sonst schlicht und einfach administrative und technische Probleme bekommt, die sein Überleben am Markt gefährden können. Dazu kommt noch, dass der Umstieg auf andere Ersatz-Plattformen von Microsoft nicht erleichtert wird. Der wichtigste Teil des Problems für unser Vorhaben liegt jedoch in der Qualität des Produktes resp. den Fehlern in Programmen, die direkte Auswirkungen haben, wie z. B. ein Crash und indirekte Mängel, die genau durch externe Angreifer bewusst ausgenutzt werden. Dies ist der Fall bei den meisten Würmern, die Schlagzeilen gemacht haben! Wo liegt hier die Haftpflicht von Microsoft? Wolfgang Straub kommentiert in «Software als Produkt»[50] die heutige Orientierung der Rechtssprechung. Es besteht kein Zweifel daran, dass die Programmfehler in Microsofts Programmen mitverantwortlich sind für die in Millionenhöhe USD angegebenen Schäden. Bis heute habe ich aber noch kein zivilrechtliches Urteil gelesen, das in Richtung Haftung oder Schadenersatz geht. Es ist auch frappant festzustellen, dass mehrere Anti-Viren-Programme von verschiedenen Herstellern auf dem Markt gedeihen.

48 Siehe www.icq.com Diese Organisation verwendet auch eine eindeutige Identitätsnummer. Die Identität des Inhabers wird aber nicht geprüft.

49 http://www.verisign.com/

50 http://www.weblaw.ch/jusletter/Artikel.jsp?ArticleNr=1580&Language=1.

Was diese Unternehmen anbieten, ist kostspielig, öfters dürftig und verlangt dazu noch viel Know-how vom Endbenutzer. Dabei könnte Microsoft Corp. durch die Behebung ihrer Fehler diese Zusatzprodukte zum Teil nutzlos machen oder ein Teil dieser Tools könnte direkt in den Anwendungen von Microsoft eingebaut werden. Diese Situation mag nur die Softwarehersteller befriedigen, ist aber wirtschaftlich gesehen Unsinn. Diese Tatsachen sind natürlich der grossen Mehrheit unbekannt und bleiben verschwiegen, da sowieso nicht viel dagegen zu machen wäre!

5.2. Strukturelle Anpassungen

Immer noch ein wenig im Bereich der Utopie, aber trotzdem in greifbarer Nähe, scheint mir die Verwirklichung einer strategischen Plattform zur Definition der Risiken in Bezug auf Wirtschaftskriminalität und insbesondere der Cyberkriminalität in Anbetracht der heutigen Lage, der zukünftigen möglichen Entwicklung, des aktiven Schutzes der Betroffenen, der Verantwortung der verschiedenen Intermediäre auf dem Markt, der Zuständigkeiten des Staates, der notwendigen Ausbildung der verschiedenen Verantwortungsebenen sowie der Durchsetzung von regulatorischen und Aufsichtsmassnahmen und des dazu angepassten Instrumentariums. Dafür braucht es zunächst die Erfassung der Sachverhalte, Tatbestände, Sozial-Sachschäden und die Evaluation der Risiken durch eine entsprechende Task-Force. Die Verwirklichung einer solchen strategischen Plattform ist politischer Natur. Dunkelziffern ergeben für den Anlagebetrug im breitesten Sinne Werte von CHF 10 000 000 000 pro Jahr. Nur schon Gross- und Mittelfirmen erleiden mit WK (Fraud) einen Verlust von zirka CHF 150 000 000 pro Jahr. Unsere Arbeit deutet auf Betrugszahlen über Internet von bis zu CHF 60 000 000 pro Jahr hin. Indikatoren geben Alarmwarnungen für die Zukunft, insbesondere bei Internet, ab. Die Kosten für ein entsprechendes Instrumentarium sind zu vergleichen mit den erworbenen Resultaten, der Rationalisierung in der Koordination im Kampf gegen die WK sowie der Verantwortlichkeit des Staates, die notwendige Infrastruktur zum Gedeihen der Bürger, der Wirtschaft und der Gesellschaft zu sichern. Ich will nochmals betonen, dass zirka 90% aller Unternehmen Kleinfirmen sind. Die Wertschöpfung ist in diesen Betrieben von zentraler Bedeutung für unsere Entwicklung und Stabilität. Die KUs haben die gleichen Auflagen wie Mittel- und Grossunternehmen, sind aber ungleich gerüstet. Damit ist das Risiko bei KUs und Privaten auch am grössten.

5.3. Kontextbezogene Massnahmen

Weg von der Utopie; unmittelbar realisierbare Vorhaben werden dazu beitragen, die Zuversicht der Benutzer in die New Economy, das Sicherheitsbewusstsein und das Vertrauen zum Staat zu steigern!

5.3.1. Die Verantwortung der ISPs

Die Rolle und die Verantwortlichkeiten dieser Intermediäre muss klargestellt werden. Wir kennen heute in der Schweiz keine Dienstleistungsgesellschaft, die im Bereich des öffentlichen Verkehrs oder der Kommunikationsbranche nicht entweder eine Bewilligung oder öfters eine Konzession hat. Bei beiden Varianten werden klare technische Zielsetzungen, Auflagen und Aufgaben bestimmt. Bei der Konzession werden meistens noch finanzielle Sicherheiten dazu verlangt. Es ist klar, dass die Internetbranche jung ist und sich in einem enorm schnell entwickelnden Umfeld bewegt. Dabei sind mehrere ISPs finanziell ungenügend gerüstet, und nachweisbar ist bei den meisten, wie dies in der New Economy und im E-Commerce noch der Fall ist, die Ertragslage entweder schwach und Verluste meistens hoch. Wenn jedoch eine Firma mit so sensiblen Informationen wie persönlichen Daten umgeht, dann kann der Benutzer auch erwarten, dass alle Massnahmen getroffen werden, wie dies bei anderen konzessionierten Unternehmen in der Kommunikationsbranche der Fall ist.

5.3.2. Schutzmassnahmen und ISP

Von Benutzerseite her kann man erstaunt sein, dass die ersten Massnahmen, die mit ISPs ausgehandelt und durchgesetzt worden sind, ausgerechnet nur repressiver Natur waren! Diese Auflagen haben den ISPs Investitionen in beträchtlicher Höhe abverlangt und sind weder wertschöpfend noch tragen sie zur Kredibilität oder zum Ansehen dieser Firmen auf dem Markt bei. Zurzeit laufen neue Gespräche zwischen dem BAKOM, BAJ und den ISPs über das Thema der Strafbarkeit von Providern[51]. Wenn man heute von Schutzmassnahmen spricht, sind es demzufolge solche, die in erster Linie

51 http://www.bakom.ch/de/telekommunikation/internet/provider/index.html.

dem staatlichen Repressionsapparat helfen (ohne Probleme ist BüPF aber bekanntlich auch nicht), seine Aufgaben zu erfüllen. Dabei ist aktiver Schutz der Benutzer aber noch nicht garantiert.

Der aktive Schutz für Benutzer ist unbefriedigend, vor allem weil die ISPs wenig dazu beitragen. Die Gründe wurden erwähnt. Wir können davon ausgehen, dass die ISPs an Vertrauen und an Gedeihen gewinnen würden (Zuwachs E-Commerce usw.), wenn diese den Benutzern entgegenkämen und ihr Angebot, wie das bei WEB.DE der Fall ist, erweitern würden. Im Klartext heisst das: a) Einsatz von Tools, die E-Mails und Anlagen auf Viren scannen und diese auch melden. b) Automatisch für E-Mails unbekannter Herkunft das HTML-Format in risikoloses Leseformat umsetzen. c) Anti-Spam-Werkzeuge einsetzen, die mit internationalen Black-Lists den Absender eingehender E-Mails überprüfen und diese entweder vernichten oder anderswo nach den Wünschen der Benutzer ablegen. d) Jede ankommende E-Mail auf die Herkunft prüfen, indem die Adresse des Absenders gecheckt wird (so genannter Finger[52] oder E-Mail Verifier), bei Fehlermeldung wird diese E-Mail zerstört. e) Anhand der Adressenverwaltung auf dem Mail-Server des ISPs bei Eingang einer E-Mail überprüfen, ob die Adresse schon erfasst wurde. Wenn dies nicht der Fall ist, dem Benutzer die Möglichkeit anbieten, diese Adresse sofort zu erfassen oder automatisch per Nachfrage-E-Mail beim Absender verlangen, die genauen Rand-Daten mitzuteilen. Solche E-Mails gehen damit in eine Warteliste, bis die Angaben vollständig und akzeptiert sind. f) Auf einfache Art die Adresse des E-Mailbox-Inhabers überprüfen, indem er über Postversand einen ihm zugewiesenen Code aktiviert, um zusätzliche Sicherheitsprogramme benutzen zu können.

Diese Beispiele sind nicht ohne Aufwendungen durch den ISP zu realisieren. Dafür gibt es zwei Möglichkeiten: a) Wenn es im Interesse der Öffentlichkeit ist, kann das BAKOM im Rahmen der Konzession oder Bewilligung solche Standards gegen Bezahlung zur Verfügung stellen. b) Die ISPs bieten dem Benutzer verschiedene Dienstleistungsvarianten an, die gegen Bezahlung erhältlich sind. Der Benutzer ist gerne bereit, wenn er sich teure Anti-Spam- und Antiviren-Software ersparen kann, dafür bei einem Provider einen angemessenen Betrag zu bezahlen.

52 A UNIX program that takes an e-mail address as input and returns information about the user who owns that e-mail address.

5.3.3. *Schutzmassnahmen in Zusammenarbeit mit dem EJPD-BAP*

Wir haben uns früher über die Vorhaben der Gruppe Cyberkriminalität des BAPs geäussert. An dieser Stelle kann man eine sinnvolle und pro-aktive Benutzung des Wissens von mehreren Stellen des BAPs anstreben, indem das EJPD alle Informationen, welche die Cyberkriminalität im weitesten Sinne betreffen, auf angebrachte Art und Weise dem Benutzer zur Verfügung stellen kann.

Vom Prinzip her ist das Vorgehen einfach: Beim Anklicken einer Webseite werden Warnungen in geeigneter Form angezeigt - über E-Mail, direkt durch das BAP oder vom ISP vorgespeichert am Bildschirm des Benutzers. Eine Warnung verhindert in keinem Falle den Zugriff auf diese Seiten, es obliegt nachher dem Benutzer, sein Verhalten den Warnungen anzupassen. Sollte ein Benutzer bei einem Vorfall diese Warnung missachten, könnte die Gefahr bestehen, dass dies als Argument gegen ihn verwendet wird. In Anbetracht der Vorsichtsmassnahmen, die jeder Einzelne anwenden muss, dürfte dies jedoch keine Behinderung des Konzeptes bedeuten. Es ist uns bewusst, dass für die Benutzer, die anonym auf dem Netz surfen wollen, eine direkte Warnung nichts bringen kann. Es scheint uns daher angebracht, zusätzlich eine vom BAP geführte Webseite vorzusehen, in der alle Warnungen in geeigneter Form präsentiert werden.

Zur Durchführbarkeit dieser Massnahme gibt es mehrere materielle Bedingungen: a) Unterstützung auf der politischen Ebene. b) Abklärung der rechtlichen Lage. c) Aktive Mitarbeit der ISPs. d) PR-Plan für die Information der Benutzer.

5.4. *Individuellbezogene Massnahmen*

Als Massnahme vorzuschlagen, die Leute sollen besser ausgebildet werden, ist eine Aussage, die inhaltslos ist, solange man das Zielpublikum nicht kennt und auch nicht weiss, wie man an die Leute herankommt und was die Informations- und Ausbildungsbedürfnisse sind. Unser Zielpublikum ist heterogen und zerstreut, kommt aus diversen Alters-, Einkommens-, Kultur-, Sprach- und Ausbildungsgruppen. Eine mögliche Benutzersegmentierung ist

ersichtlich im Anhang: Kriterien und Katalogisierung von Variablen im Bereiche des Internetbetruges durch E-Mail. Leider konnte eine Analyse nach Angriffs- und Betrugsarten nicht durchgeführt werden, da materiell keine Angaben zur Verfügung standen. Wir haben auch schon in einem anderen Beitrag eingehend bewiesen, dass auf schweizerischer Ebene bedauerlicherweise überhaupt keine Daten und Statistiken erhältlich sind. Wir vertreten auch die Ansicht, dass eine solche Studie auf schweizerischer Ebene in Anbetracht der Summen, die auf dem Spiel stehen, durchgeführt werden müsste!

Trotzdem ist es mit den heutigen Techniken und der angebrachten Benutzersegmentierung möglich, ein Informationsprogramm zu gestalten und dementsprechend auch Akzente zu setzen. Damit kann über mehrere Kanäle die Sensibilisierung, die Information sowie die Ausbildung der einzelnen Zielgruppen tatkräftig gefördert und zum grössten Teil sichergestellt werden.

Anhang:

Kriterien und Katalogisierung von Variablen im Bereiche des Internetbetruges durch E-Mail

Wert: (in US$ oder €)

2 unter 200
3 200–400
4 400–600
6 600–1000
8 1000–5000
9 5000–10 000
10 über 100 000

Frequenz des Sachverhaltes

Von 1 bis 10. Die Segmentierung erfolgte auf diversen angepassten und kombinierten Prozentsätzen und Daten der FTC, IFCC und IFC. Massgebend sind diese der FTC, da die Angaben mengenmässig repräsentativ sind. Für unbekannte Angaben wurde der Wert 1 eingesetzt. Identity Theft wurde nicht berücksichtigt.

Organisation oder Kriminalisierungsgrad

1 Kiddy-Hacker Gelegenheit
2 einzelne Person situativ
3 einzelne Person beruflich
4 Berufsfachperson Spezialist
5 Berufsfachleute (Tätergruppe)
6 technologische Struktur (HW, SW, Logistik)
7 technologische Struktur mit Spezialisten
8 komplexe Struktur mit Spezialisten
9 OK (Organisierte Kriminalität)
10 Mafia-Strukturen (Organisiertes Verbrechen)

Komplexität des Vorganges

1 kopierbar, leicht erlernbar
2 fachmännisches Wissen einzeln
3 Spezialist einzeln
4 fachmännisches Wissen mit Gehilfen lokal
5 Beziehungsnetz und Komplizen lokal
6 fachmännisches Wissen mit Gehilfen international
7 Beziehungsnetz und Komplizen international
8 Komplexe internationale Verbindungen
9 Komplexe internationale Verbindungen, langfristige Aktion
10 hochqualifizierte Personen mit aussergewöhnlichen technischen Mitteln weltweit

Kontaktart zum Opfer

1 nur persönlich und vertraulich
2 nur persönlich (Affinitäten)
3 persönlich
4 über Referenz
5 Kundenbearbeitung
6 Nachrichten/Informationen
7 Reklame allgemein
8 http und Banners
9 Mailing kontrolliert
10 Spamming

Segmentierung Anleger-Opfer-Teilnehmer

Beruf:	normal:	rational und wirtschaftlich, formal richtig und überlegt
Beruf:	gedrängt:	rational in wirtschaftlichem Zwang (situativ)
Beruf:	anorm:	kriminell veranlagt, vorbestraft
Privat:	jung:	Alter unter 23, selbstständig, studierend, ungebunden und eher lebensfreudig und rezeptiv. Niedriges Einkommen
Privat:	Haushalt I:	Alter 24–35, Familien-Typ, mit Kindern, verpflichtet, berufstätig mit Laufbahn, Einkommen CHF 50 000–80 000.

Privat:	Haushalt II:	Alter 36–55, Familien-Typ, stabil, spart und investiert sicher. Einkommen CHF 80 000–150 000
Privat:	Technokrat:	Alter 36–55, erfolgreich und selbstbewusst, investitionsfreudig, Einkommen über CHF 150 000
Privat:	Rentner:	Alter über 55–60, kulturell und sicherheitsbewusst, Einkommen CHF 50 000–80 000

Jean-Pierre BRUDERER, PhD
CORIA International llc
Corporate Integrity Advisors
PO Box 317, World Trade Center
CH-6892 Lugano-Agno
E-Mail: coria@wtclugano.ch
URL: www.coria-llc.com