Dieter Kochheim, Eine kurze Geschichte der Cybercrime

Es gibt die juristische Legende, dass in den Sechziger oder Siebziger Jahren des letzten Jahrhunderts ein Entwickler in ein Programm für die Abrechnung von Bankzinsen bewusst einen Rundungsfehler eingebaut habe. An der dritten (oder einer anderen) Nachkommastelle soll er den Guthabenwert abgeschnitten und einem eigenen Konto gutgeschrieben haben. Das soll ihm richtig Knete eingebracht haben. Belege dafür findet man hingegen nicht.

Diese Legende könnte die erste wirkliche Cybercrime-Aktion gewesen sein.

Ich habe jedenfalls (2008) die arbeitsteilige Cybercrime definiert als die vom Gewinnstreben bestimmte planmäßige Begehung von IT-Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind. Ihre planenden Täter greifen dazu auf etablierte Strukturen und Gruppen mit Spezialisten zurück, deren Dienste und Handlungen sie zur Erreichung des kriminellen Zieles zusammenführen. IT-Straftaten in diesem Sinne sind vor allem auch solche, die zu ihrer Ausführung technische Kommunikationsnetze nutzen.

Durch die Hervorhebung der Arbeitsteilung erweist sich die Cybercrime als eine sehr moderne Form der Kriminalität, was tatsächlich von den Erfahrungs- und Eckwerten aus den letzten 20 Jahren bestätigt wird.

In diesem Aufsatz geht es mir um die Wurzeln, die für die Cybercrime bestimmend gewesen sind, und um die Ausformungen, die sie von anderen Kriminalitätsformen abhebt. Dazu habe ich historische Eckdaten bestimmt, die für die Themenfelder Telekommunikation - TK, Informationstechnik - IT, Wirtschaft und schließlich Cybercrime ausschlaggebend sein dürften. Sie habe ich in ihrer zeitliche Abfolge betrachtet und nebeneinander gestellt.

Ob ich dabei immer die richtigen Meilensteine setze, ein technologischer Eckpunkt ein paar Jahre früher oder später anzusetzen wäre oder ob ich andere Schwerpunkte hätte benennen müssen, bleibt letztlich gleichgültig. Die Eckpunkte zeigen, dass die Wurzeln der IT mehrere Jahrhunderte zurückreichen und die der TK auch fast 200 Jahre. Die philosophischen und mathematischen Vorarbeiten (zum Beispiel von Leibnitz) habe ich dabei gar nicht betrachtet. Ihre Förderung und ihre Konturen verdanken sie jedenfalls der Industrialisierung.

Ich konzentriere mich auf die Cybercrime im engeren Sinne. Das sind die Erscheinungsformen, die die Telekommunikation und die Informationstechnik gezielt dazu missbrauchen, neue Formen von Kriminalität oder neue Varianten zu entwickeln, die dadurch zu eigenständigen Kriminalitätsformen wurden. Das gilt besonders für das Hacking, die Verbreitung von Malware und das Carding.

Das harmlos klingende Carding bezeichnet den Umgang mit ausgespähten Daten von Zahlungskarten und hat ein organisierte Struktur durch die Gründung von Carders-Planet bekommen (2001). Auch schon vorher wurden Karten gestohlen, ihre Daten ausgespäht und missbraucht. Das waren aber überwiegend Formen des Trickbetruges und des hilfsweisen Einsatzes von IT.

Besondere Formen des Cardings entstanden mit dem Phishing (etwa seit 1996) und dem Skimming, das um 2000 entstanden ist und seit 2003 den BGH beschäftigt (Tatzeit dort: 2001), wobei für mich ausschlaggebend der Einsatz von Lesegeräten ist (Skimmer). Besser umschrieben wird das Cading mit dem Oberbegriff „Identitätsdiebstahl“, der schließlich den Missbrauch aller persönlichen Daten für Geld- und Warengeschäfte sowie andere Handlungen unter einer fremden Identität meint.

Bis 1982 gab es Vorläufer der Cybercrime, aber keine Cybercrime, die diesen Namen verdient. Einer dieser Vorläufer ist das Phreaking (ab 1957), also die Leistungserschleichung bei Telefondiensten. Dasselbe gilt für das Hacking gegen Großrechner, das irgendwann in den Sechziger Jahren begann und von Studenten betrieben wurde, die die Rechner ihrer Unis zunächst spielerisch penetrierten. Auch die erste Spam-Mail war eher dumm und unüberlegt [1] als böswillig.

Böswilliges Hacking und Viren gab es schon vorher, aber die organisierte Cybercrime begann 1990 mit den ersten "Hackerfabriken" in Bulgarien, was ich auch erst seit dem äußerst wichtigen Aufsatz von Paget weiß [2]. Von da an ging sie ab, die Dinknesh [3].

Bewusst fehlen hier die Themen Urheberrechte, gewerbliche Schutzrechte, Betrug in Handelsplattformen und Webshops, Kinderpornographie, Stalking und böswillige Meinungsstreite. Diese Themen haben mit dem Internet neue Umgebungen und Ausprägungen erfahren, sind jedoch nicht wirklich neu. Sie verdienen der Beachtung, besonders dann, wenn sie zur Profitgewinnung und in verdeckten Strukturen eingesetzt werden. Dennoch vernachlässige ich sie, um den Blick auf die Cybercrime im engeren Sinne zu konzentrieren.

[1] ▸ Spam feiert 30. Geburtstag, Heise online 03.05.2008

[2] ▸ Mafia, Cybercrime und verwachsene Strukturen, 20.10.2010

[3] ▸ Wikipedia, Lucy

Jahr	Telekommunikation	Informationstechnik	Wirtschaft
1728		Lochstreifen (Holzplättchen, Webstühle)	
1835		Relais	
1837	Morsetelegraph		
1847			Siemens
1850	erstes atlantisches See-kabel		
1861	Telefon von Reis		
1871			Western Union führt Be-zahldienst ein
1877	Telefon-Standverbindung		
1881	Telefon-Zentrale		
1885			AT&T
1887		Tabelliermaschine, Lochkarte	
1890		Schallplatte	
1892	automatische Vermitt-lungsstelle		
1894			Kreditkarte

IT-Urzeit

Webstühle sind vorindustrielle Maschinen, die schon früh für die Massenproduktion optimiert wurden. Bereits 1728 - vor der Geburt Emanuel Kants - wurden die Webmuster von primitiven Vorgängern der Lochstreifen gesteuert. Sie bestanden aus aufgefädelten Holzplättchen. Dennoch war es möglich, mit ihnen Informationen zu transportieren und Arbeitsprozesse zu steuern. Das ist IT.

Das Relais war der erste elektromagnetische Schalter. Es entstand im im Jahr 1835. Mary Wollstonecraft Shelley hatte schon 1818 "Frankenstein" erfunden.

Die Industriealisierung ist die Wiege der Telekommunikation. Als ihren Startpunkt setze ich den Morsetelegraphen von 1837. Er nutzte elektrischen Strom und Kabel. Nur zehn Jahre später wurde die Firma Siemens gegründet.

Noch vor einer funktionstüchtigen Telefonie (Reis, 1861) wurde 1850 das erste transatlantische Seekabel verlegt - für die Kommunikation per Morsezeichen! Sie war so effektiv, dass es sich lohnte, das erste elektrotechnische Großprojekt durchzuführen.

1851 wurde Western Union gegründet und baute Telegraphenverbindungen quer durch die USA. 1871 begann das Unternehmen mit seinem Bezahldienst per telegraphischer Anweisung.

Die erste Großtechnologie für das moderne Informationszeitalter war die Telefonie. 1877 gab es die erste Telefon-Standverbindung und 1881 die erste Telefonzentrale mit dem "Fräulein vom Amt". 1885 wurde die Firma AT&T gegründet.

Die automatisierte Informationsverarbeitung dürfte ihren Meilenstein bei den Tabelliermaschinen haben. 1887 wurde die erste im Zusammenhang mit einer Volkszählung in den USA eingesetzt. Sie sortierte und addierte Informationspakete in Form von Lochkarten.

Als Basis für die modernen Datenträger nehme ich die analoge Schallplatte von 1890. 1892 folgte die automatische, relaisgesteuerte Vermittlungsstelle und damit nicht nur ein Meilenstein für die Telekommunikation, sondern auch für die elektronische Datenverarbeitung. Die Schaltung funktionierte seinerzeit noch auf der Grundlage verschieden langer Stromstöße. Sie bildet die Grundlage für die Adressierung bei der Telefonie.

1894 führten die ersten amerikanischen Restaurants Kreditkarten für ihre besten Kunden ein. Auf ihnen stand der "gute Name" des Kunden, an den später die Rechnung übersandt wurde. Das ist auch nichts anderes als der Deckel in der Stammkneipe.

Jahr	Telekommunikation	Informationstechnik	Wirtschaft	Cybercrime
1912		Röhrenverstärker		
1923		Enigma		
1924			IBM	
1934		Transistor		
1935		Tonband von AEG		
1938	Fernschreiber-Netz			
1939			Geldausgabeautomat	
1940		Magnetband		
1941		Z3		
1942		ENIAC		
1943		Colossus		

Dinosaurier

In der ersten Hälfte des Zwanzigsten Jahrhunderts wurden die grundlegenden Bausteine für die IT geschaffen und schließlich seit 1941 die ersten Computer gebaut.

1912 wurde das Relais von der Schalterröhre abgelöst und der erste Röhrenverstärker vorgestellt. Wie bei der Spule (Potentiometer) ließ sich damit nicht nur "Ein-Aus" schalten, sondern ließen sich auch Flussprozesse steuern. Es folgten der erste Weltkrieg und technologisch viele Verfeinerungen mechanischer Prozesse, die Flugtechnik und die Fließbandtechnik (Ford, 1913).

Enigma ist für mich der erste Prozessor (ab 1923). Die Chiffrier-Maschine ist elektrisch angetrieben und wandelt Zeichen in einem kryptischen Prozess in andere um. Dazu werden metallische Scheiben in das Gerät eingesetzt, die wie Platinen elektrische Ströme von einer Kontaktstelle zu einer anderen leiten. Durch das Drehen der Scheiben und ihren spezifischen Schalterfunktionenwerden die Informationen kryptographisch chiffriert.

1924 wurde die Firma IBM gegründet.

Zehn Jahre später wurde die Röhre als elektrischer Schalter abgelöst und entstand der Transistor. 1935 wurde das erste Tonbandgerät von AEG hergestellt.

Ein Meilenstein für die TK ist das Entstehen des ersten Fernschreibernetzes im Jahr 1938. Im Jahr darauf wurde der Geldautomat präsentiert und fand wenig Resonanz.

Während des Zweiten Weltkrieges folgten ganz große Innovationen in der IT: Nach der Massenproduktion von Magnetbändern (1940) stellte Konrad Zuse mit Z3 den ersten frei programmierbaren Computer fertig (1941, Dampfmaschinen-Computer). Die Maschine bestand aus Relais. 1942 und 1943 folgten ihr Röhren-Computer: ENIAC in Großbritannien und Colossus in den USA).

Jahr	Telekommunikation	Informationstechnik	Wirtschaft	Cybercrime
1947			GEMA	
1955		Transistorencomputer – TRADIC		
1956		Festplatte		
1957				Phreaking
1958		integrierter Schaltkreis		
1960	Nachrichtensatellit (Echo 1)			
1963		Kassettenrekorder - Philips		Hacking - Telefon
1964		Disk-Operating-System - IBM		
1966		Akustikkoppler - Modem		
1968		programmierbarer Taschenrechner - HP	Euro-Cheque	
1969	ARPANET	Unix, Diskette	EC-Karte, CompuServe	

Elektrotechnisches Zeitalter

Nach dem Zweiten Weltkrieg setzte die Massenproduktion elektrotechnischer Geräte ein und wurden weitere Bausteine geschaffen und verfeinert, die für die heutige IT unverzichtbar sind.

Schon 1947 wurde die GEMA gegründet, die hierzulande bekannteste Verwertungsgesellschaft für Urheberrechte.

Mit TRADIC wurde 1955 der erste mit Transistoren bestückte Computer in Betrieb genommen. 1956 wurden die ersten Festplatten hergestellt und lösten Magnet- und Lochstreifenbänder als Massenspeicher ab. 1958 folgte der integrierte Schaltkreis - IC. Das ist der erste elektronische Baustein, der in sich eine Vielzahl von Schaltungselementen und vor allem Transistoren vereint und damit die Mikrotechnik einleitete. Er ist der Vorläufer der heutigen Prozessoren. IC und Festplatte bilden zwei der wesentlichen Komponenten für die heutigen PCs.

Bereits 1957 tauchte mit dem Phreaking eine frühe Form der Cybercrime auf. Damit werden Methoden zusammengefasst, um kostenlos zu telefonieren. Ihre wichtigsten Methoden sind das Manipulieren des Wahlvorganges und das Ausnutzen ausgespähter Servicenummern, die die Mitarbeiter von Telefongesellschaften für Testzwecke verwendeten.

In den Sechziger Jahren wurden beim Militär und in den Universitäten die ersten Großrechner eingesetzt. Parallel dazu entstanden seit 1963 auch die ersten Formen des Hackings, das sich seinerzeit noch auf die Telefontechnik und ihre Anlagen beschränkte. Schon 1960 wurde der erste Nachrichtensatellit erprobt (Echo 1) und 1963 stellte die Firma Philips den ersten Kassettenrekorder vor.

Zur Steuerung von Großrechnern führte IBM 1964 das erste Disk-Operating-System ein, das den Hauptspeicher (= Arbeitsspeicher) revolutionierte.

1966 folgte der Akustikkoppler, eine besondere Art des Modems. Dieses Gerät wandelt digitale Daten in (analoge) Töne um, die im analogen Telefonnetz übertragen werden

können und in der Gegenstelle wieder in digitale Daten umgewandelt werden. Der Koppler hatte die Besonderheit, dass er zwei Röhren oder gewulste Ringe hatte, in die man einen Telefonhörer stecken konnte.

1968 begann Hewlett Packard mit dem Verkauf des ersten programmierbaren Taschenrechners (mit einer völlig verqueren Eingabelogik). Im Jahr darauf wurde nicht nur die erste Diskette vorgestellt, sondern entstand auch Unix für Großrechner. Das ist das seither führende Betriebssystem, das Computer, ihre Peripheriegeräte und Funktionen steuert. Der Kern von Windows kann noch heute seine Herkunft von Unix nicht leugnen und Linux ist nichts anderes als ein nachprogrammiertes Unix.

Am 25. August 1967 wurde das Fernsehen in Deutschland farbig.

Von wirtschaftlicher Bedeutung sind die Einführungen des Euro-Cheques (1968) und gleich darauf der EC-Karte (1969) als neue (neben den Kreditkarten der Restaurantketten, Schecks und andere Wertpapiere) allgemeingültige Zahlungsmittel neben dem Bargeld.

Die Epoche schließt ab mit dem ARPANET. Das war der erste permanente Netzverbund für (militärische) Großrechner, aus dem später das Internet werden würde. Auch die Firma CompuServe entstand 1969, die zunächst nur Rechnerzeit an andere Unternehmen vermietete.

Jahr	Telekommunikation	Informationstechnik	Wirtschaft	Cybercrime
1971		Prozessor - Intel		
1972		Magnetstreifen		
1973		PC - Xerox Alto	SWIFT	
1975	TCP/IP im Praxiseinsatz	SQL	Microsoft	
1976				Hacking-Jargon
1977			Oracle	
1978				Spam
1979		CD-ROM		

Elektronische Gründerzeit

In den Siebziger Jahren des Zwanzigsten Jahrhunderts entstand der erste PC und das wichtigste Protokoll für das Internet wurde eingeführt (TCP/IP). Mit Microsoft und Oracle entstanden (zum Beispiel) zwei Firmen, die in den folgenden Jahrzehnten bestimmend sein werden.

1971 präsentierte Intel den ersten Prozessor, also einen hochgerüsteten integrierten Schaltkreis, der für Rechenoperationen optimiert war.

1972 folgte der Magnetstreifen für Zahlungskarten und 1973 stellte Xerox mit Alto den ersten PC vor. Dieses Gerät verfügte bereits über ein Zeigegerät (Maus). Damit war der Startschuss für die moderne IT gefallen. Alle Miniaturisierungen waren abgeschlossen und zusammengeführt - ein Prozess über 30 Jahre seit der Z3.

1973 begann SWIFT, das erste internationale und zunehmend automatisierte Verrechnungssystem der Banken für den grenzüberschreitenden Zahlungsverkehr, das noch heute existiert. Es hat nur dadurch an Bedeutung verloren, weil sich daneben leistungsstarke Verrechnungssysteme für den privaten Zahlungsverkehr etabliert haben (zB Visa, Master, Maestro ua).

1975 wurde das Internetprotokoll (TCP/IP) für die internationalen Rechnerverbünde eingeführt. Es gilt bis heute und bildet das Regelwerk für die Adressierung und den Datenversand im Internet.

1975 entstand auch die Datenbanksprache SQL. Zusammen mit Unix bilden die Syntax und Leistungsfähigkeit von SQL die Basis für alle Relationalen Datenbanken. Beide wurden im Laufe der Zeit erweitert und optimiert und bilden Grundlagen für die heutige IT.

Ebenfalls in 1975 nahmen die jungen Gründer der Firma Microsoft ihren Geschäftsbetrieb auf.

Das Hacking war lange Jahre eine sportive akademische Besonderheit. Ihre spielerischen Protagonisten - die Hacker - waren von der Funktionsweise und den Möglichkeiten der IT begeistert, versuchten zu tricksen, fanden Sicherheitslücken und entwickelten bei diesen Gelegenheiten eine besondere Kultur, die zwischen zwei Extremen pendelt: Einerseits geht es ihr um die Absicherung der IT durch das Ausprobieren und Entdecken von Lücken und andererseits wurden mehr und mehr auch profitable Missbräuche praktiziert. Zunächst ging es dabei um zweierlei: Entweder um den parasitären Zugang zu sehr teurer Rechenzeit oder - mehr und mehr - um den Zugang zu geheimen Informationen anderer. Trotz aller Beteuerungen

der "wir sind die Guten" bewegt sich das Hacking noch immer in diesem grauen Spannungsfeld. 1976 ist deshalb ein Meilenstein, weil erstmals die Hacking-Kultur einen Namen bekam und ihr spezifischer Sprachgebrauch dokumentiert wurde.

1977 wurde die Firma Oracle gegründet, die ohne SQL nicht denkbar wäre. Sie ist noch heute weltweit der führende Datenbank-Anbieter.

1978 wurde die erste Spam-Mail versandt. Rücksichtslos und noch unbedacht an alle gerichtet, die seinerzeit am erreichbar Netz waren. 1979 folgte die Markteinführung der CD-ROM als Tonträger.

Jahr	Telekommunikation	Informationstechnik	Wirtschaft	Cybercrime
1980	Videotext			
1981		MS-DOS		Chaos Computer Club
1982		Multiplan	Adobe	Virus für Apple II
1983	Domain Name System, Bildschirmtext - BTX	MS-Word	c't	
1984			Dell	ccc: OnlineBanking-Manipulation, Cult of the Dead Cow
1985		Windows, MS-Excel		KGB-Hack, Bayerische Hackerpost: Trojaner, Gotscha: Trojaner, löscht Festplatte
1986	.de			Bootvirus für DOS
1987	ISDN - Einführung		McAfee	speicherresidenter Virus – Lehigh
1988			AOL	
1989	HTML, Mobiltelefon			Virenepidemie in Russland

Expansion und Missbrauch

Die Achtziger Jahre brachten den Durchbruch für die Anwenderprogramme. Es entstand langsam ein Massenmarkt, der mehr und mehr heiß umkämpft wurde. Der Sieger ist Microsoft. Ab der Mitte der Achtziger Jahre entfaltete sich auch mit Macht die frühe Cybercrime.

Ab 1981 vermarktete die noch unbedeutende Firma Microsoft das Betriebssystem DOS auf dem Consumer-Markt. Mit der Entwicklung des Tabellenkalkulationsprogrammes Multiplan startete das Unternehmen 1982 eine äußerst aggressive Verdrängungspolitik gegen alle Konkurrenten, die es mit dem Textverarbeitungsprogramm Word (1983) fortsetzte.

Mit Windows schuf MS 1985 die erste Version einer grafischen Anwenderoberfläche - nach dem Vorbild von Apple. Dabei waren das Betriebssystem als Geräteverwaltung und die Benutzerführung als grafischer Aufsatz noch getrennt. Das änderte sich erst 1994 mit OS2 - MS ungeliebtes Partnerprojekt mit IBM - und 1995 mit Windows 95.

Mit den grafischen Benutzeroberflächen und Anwenderprogrammen kam das Ende der allgegenwärtigen Kommandozeile, die nur bedienen konnte, wer sich mit der Syntax und den Funktionen seiner Programme auskannte. Multiplan war noch ein Zwitter, der dem Anwender tiefere Kenntnisse über Kommandozeichen abverlangte. Das wurde dann anders: Grafische Symbole (Icons) und intuitive Bedienelemente erschienen auf dem Bildschirm und erschlossen auch dem unwissenden Anwender einen mehr spielerischen Zugang zur IT.

Mit Excel schuf MS 1985 ein Tabellenkalkulationsprogramm, vor dem die meisten Konkurrenten tatsächlich kapitulierten.

Mit dem Testbeginn von Videotext (1980) entstand die erste grafische Form der elektronischen Kommunikation. Videotext ist, wie der Name schon sagt, textbasierend und dient im Fernsehen zu ergänzenden Programminformationen und Meldungen, die von dem Veranstalter eingespeist werden.

Dagegen ist Bildschirmtext (1983) ein System zur Netzkommunikation, das auf dem

Telefonnetz gründet. Es bedurfte eines besonderen Terminals oder eines Modems, wobei als Bildschirm der Fernseher verwendet werden konnte. BTX ging 1993 in Datex-J auf, das seinerseits 1997 eingestellt wurde.

Mit American Online - AOL - entstand 1988 (bis Mitte der Neunziger Jahre) eines der weltweit führenden Zugangsprovider zum Internet.

1983 wurde das Domain Name System - DNS - eingeführt. Es bildet eine Ergänzung zu dem nummerischen Adressen des Internetprotokolls und erleichtert die Navigation vermittels beschreibender Namen. Darauf wurde 1986 die deutsche Länderdomain .de eingerichtet. Der Namensraum wurde zunächst von der Uni Dortmund und ab 1993 von der Uni Karlsruhe verwaltet.

1979 hat die seinerzeit noch staatliche Telekom damit begonnen, ihre Vermittlungsstellen zu digitalisieren. Die Signalübertragung blieb zunächst analog. Das war der erste Schritt weg von der elektromagnetischen Adressierung und eröffnete den Weg zu Mehrwertdiensten, Rufnummernmitnahmen, Weiterschaltungen und anderen Schnickschnack, den wir heute kennen.

Im Jahr 1987 führte die Telekom ISDN ein, also die vollständig digitale Telefonie. Das System beruht auf zwei Netzen, dem Signalisierungsnetz, in dem die Verbindung mit Hilfe der in Datenbanken gespeicherten Anwenderdaten (Bestandsdaten) gesteuert und abgerechnet wird, und dem Verbindungsnetz, das der eigentlichen Kommunikation dient. Dadurch entsteht ein "intelligentes Netz", weil die Rufnummer nicht mehr von der physikalischen Netzbeschaffenheit und dem Standort des Anschlussinhabers abhängt, sondern von den Vermittlungsdaten, die für ihn gespeichert sind.

1989 wurde schließlich das erste Mobiltelefon vorgestellt.

Die Hypertext Markup Language - HTML - ist eine verhältnismäßig einfache Skriptsprache, mit der die Anzeigen auf einem Bildschirm einschließlich Text, Formatierung und Multimediaelementen gesteuert werden. Ohne sie ist das bunte Internet nicht vorstellbar. Sie wurde 1989 im Kernforschungszentrum CERN entwickelt.

1983 erschien erstmals die Computerzeitschrift . Sie existiert bis heute und dürfte das wichtigste Printmedium auf diesem Markt sein.

Die Firma Dell wurde 1984 gegründet.

Bereits 1981 wurde der Chaos Computer Club - CCC - gegründet. Er versucht, die Vorstellungswelt der klassischen "akademischen" Hacker zu bewahren, wozu nicht nur der spielerische und nicht immer ganz legale Umgang mit der IT gehört. Ihm muss man lassen, dass ihm destruktives und auf Gewinn ausgerichtetes Handeln fremd sind. Dafür hat der CCC immer stärker die Themen Informationssicherheit und Datenschutz besetzt. Das BVerfG hat ihn mehrfach zu Stellungnahmen aufgefordert und im Zusammenhang mit der Onlinedurchsuchung und der Vorratsdatenspeicherung breit zitiert.

1984 machte der CCC erstmals in der breiten Öffentlichkeit von sich reden, als er im Fernsehen die Lücken des Onlinebankings per BTX nachwies, indem seine Mitglieder 135.000 DM von einer Sparkasse in Hamburg auf sein eigenes Bankkonto verschoben.

Ein anderes Kaliber ist der 1984 in den USA gegründete Club "Cult of the Dead Cow". Er steht für Aktivismus, kämpft aggressiv gegen reaktionäre Webseiten, die gehackt und verändert werden (Defacement), und für Mei-

nungsfreiheit - vor allem in China. Er gibt auch ständig Anti-Malware-Software heraus.

1982 begann die Geschichte der Malware mit dem ersten umlaufenden Virus für Apple II. Viren zeichnen sich dadurch aus, dass sie sich in Dateien einnisten, mit ihnen transportiert und schließlich ausgeführt werden.

1985 begannen mehrere Hacker aus Hannover damit, im Auftrag des KGB militärische und andere an das Netz angeschlossene Einrichtungen in den USA nach verwertbaren Informationen auszuforschen. Clifford Stoll hat daraus einen spannenden Roman gemacht (Das Kuckucksei).

Auch 1985 berichtete die Bayerische Hackerpost erstmals über Trojaner. Sie zeichnen sich dadurch aus, dass sie sich als vollständiges Programm präsentieren, das eine nützliche Funktion hat. Im Hintergrund wirken sie hingegen schädlich - wie "Gotscha", der Festplatten löschte (ebenfalls 1985).

Noch sind es aber die Viren, die sich weiter entwickelten. 1986 wurde der erste Boot-Virus bekannt. Er nistet sich in den Massenspeicher-Medien ein, die zum Starten des Computers genutzt werden. Dadurch steht er nach jedem Start bereit, ohne dass eine Trägerdatei aufgerufen werden muss.

Lehigh war der erste speicherresidente Virus (1987). Er verblieb im Hauptspeicher und verbreitete sich als Boot-Virus auf alle Massenspeichermedien, mit denen der infizierte Computer in Berührung kam. Das galt auch für ganz neue oder frisch formatierte Massenspeicher.

1987 wurde das Unternehmen McAfee gegründet. Damit dürfte die kommerzielle Malware-Abwehr ihren Anfang genommen haben.

1989 brach in Russland eine richtige Virenepidemie aus. Mit böser Zunge könnte man behaupten: ... weil dort die meisten Raubkopien im Umlauf waren.

Jahr	Telekommunikation	Informationstechnik	Wirtschaft	Cybercrime
1990				polymorpher Virus, Hackerfabriken in Bulgarien
1991	D-Netz			
1992	RIPE-NCC	Windows 3.1, Linux	Adobe	
1994	Mehrwertdienste		Amazon, Yahoo	
1995	ISDN flächende-ckend, DE-CIX	Multi-Tasking unter Windows, Internet-Explorer	T-Online, eBay	SoftRAM
1996	DENIC eG		Schlund+Partner, Metager	Porno online, Phishing
1997			Strato, AlltheWeb, IuKDG	Dialer
1998	ICANN, DSL		Google, Napster (Filesha-ring)	Virusfabriken in Russland, Grabbing
1999		SETI (verteiltes Rech-nen), OpenOffice.org unter SUN		HangUp-Team (Galaiko, Petrichenko, Popow), Compuserve-Urteil

Internet und organisierter Viren-markt

In den Neunziger Jahren eroberte die IT den Massenmarkt, wurde das Internet geprägt und begann sich die Internetkriminalität zu organisieren.

Ganz wichtige Meilensteine setzte die TK: 1991 begann der breite Einsatz der mobilen Telefonie mit dem D-Netz. 1994 wurden die ersten Mehrwertdienste eingeführt. Sie ermöglichten Dank der intelligenten Netze die Abrechnung von Diensten, die sich nicht auf technische Verbindungen beschränkten, sondern auch kostenpflichtige Zusatzleistungen ermöglichten. Danach folgte die nächtliche Aufforderung im Fernsehen: "Ruf mich an!"

1995 war ISDN flächendeckend in Deutschland eingeführt und ihm folgte 1998 DSL. Schnelle und breitbandige Datenverbindungen hatte man sich bis dahin nur unter Einsatz von Glasfaserkabeln - auch auf der letzten Meile - versprochen. Mit DSL ist es möglich, die bestehenden Kupferkabel für die Breitbandtechnik zu nutzen. Seither wurde das Internet schneller, bunter und vielfältiger.

1992 nahm RIPE-NCC als europäische Namensraumverwaltung den Betrieb auf. Sie verwaltet die nummerischen Adressräume des Internetprotokolls, die für Europa bestimmt sind, die AS-Nummern für die autonomen Systeme und leitet Namensanfragen wegen den Second Level Domains der europäischen Länderverwaltungen weiter. Die Aufgabe der Länderverwaltungen hatte RIPE-NCC zunächst selber übernommen und schnell an die nationalen Betreiber abgegeben.

1995 übernahm der Branchenverband eco den deutschen Internetknoten - DE-CIX - und baute ihn in Frankfurt a.M. bis heute zum weltweit bedeutendsten aus. Über ihn wird

ein maßgeblicher Teil des Datenverkehrs nach Osteuropa und zum Nahen Osten abgewickelt.

1996 wurde die DENIC-Genossenschaft gegründet und übernahm von der Uni Karlsruhe die Verwaltung des deutschen Namensraumes. Ihrer liberalen Eintragungspraxis und den günstigen Preisen der Hosting-Unternehmen (zum Beispiel Schlund+Partner sowie Strato, gegründet 1996 und 1997) verdankt die .de-Domain ihre weltweit führende Rolle als Länderdomain.

1998 wurde mit ICANN eine Art Dachgesellschaft mit 21 Verwaltungsvorständen aus aller Welt für die Verwaltung der Adressräume, den Domänen und den Autonomen Systemen im Internet geschaffen. Diese Aufgaben hatte zuvor die IANA ausgeführt, die seither eine Art Unterabteilung der ICANN ist.

Die Internet-Verwaltung und besonders die über die zentralen Root-Server unterstand bis dahin unmittelbar den Verwaltungsbehörden der USA. Mit der Kontrolle über die Root-Server lässt sich in gewissen Grenzen die Erreichbarkeit steuern und ausschließen. Inzwischen werden auch auf anderen Kontinenten Root-Server betrieben, so dass eine einseitige Einflussnahme erheblich erschwert ist.

Durch die Verwaltung der nummerischen Adressräume, der zugelassenen DNS-Räume und der AS-Nummern kommt der ICANN noch immer eine mächtige politische Rolle zu. Die Dominanz der USA ist immer noch deutlich zu spüren.

Die grundlegenden technischen Durchbrüche für die IT waren in den Achtziger Jahren abgeschlossen. In den Neunziger Jahren eroberte sie den Massenmarkt, wobei der Anwenderoberfläche Windows 3.1 und die Fähigkeit zum Multi-Tasking seit Windows 95 besondere Bedeutungen zukommen dürften. Letzteres ist die Fähigkeit eines Computers, mehrere Verarbeitungsvorgänge gleichzeitig ausführen zu können. Das können auch Unix (seit 1969) und Linux (seit 1992), die jedoch auf dem Consumer-Markt noch keine Rolle spielten.

Mit Windows 3.1 hatte MS den Einfluss des Internets verschlafen. 1995 stellte das Unternehmen den ersten und kostenfreien Internet-Explorer zur Verfügung und verdrängte damit nachhaltig den Browser von Netscape. MS wurde in diesem Zusammenhang immer wieder vorgeworfen, durch das Bundlen von Betriebssystem und Browser den Marktzugang von Konkurrenten zu erschweren und zu behindern. Vor allem in Europa führte das zu wettbewerbsrechtlichen Sanktionen gegen das Unternehmen.

Schon 1992 entstand die Firma Adobe. Sie wurde vor Allem mit ihren PDF-Editoren bekannt, die den plattformunabhängigen Dokumentenaustausch möglich macht.

Erst 2002 kam mit Firefox ein Open Source-Produkt auf den Markt, das dem MS-Browser maßgebliche Marktanteile abgenommen hat.

Eine ernsthafte Konkurrenz zu den MS-Produkten begann 1999 zu reifen, als die Firma SUN, ein etablierter Anbieter von Großrechnern, die offenen Rechte für OpenOffice.org erwarb und die freie internationale Entwicklergemeinde unterstützte. Die Leistungsfähigkeit dieses Büro-Pakets mag nicht an das kommerzielle MS-Office heranreichen. Es bildet jedoch eine ernste Konkurrenz.

Auf dem deutschen Markt waren es besonders AOL, Compuserve und die 1995 von der Telekom gegründete Tochter T-Online, die Zugangsdienste zum Internet anboten. Alle drei Unternehmen verbanden das mit eigenen inhaltlichen Angeboten und Hostspeicher, auf dem sich ihre Kunden selber im Netz präsentieren konnten.

1994 entstand die Suchmaschine Yahoo, 1997 AlltheWeb (Fast) und erst 1998 Google. Sie durchforsteten mit Crawlern das Internet und bauten mächtige Datenbanken auf, wobei AlltheWeb zunächst mit einer exzellenten Treffsicherheit überraschte. Google hingegen optimiert bis heute seine Suchroutinen und wurde nicht zu unrecht zum Marktführer und zum kritisierten Datenkraken.

Mit Metager entstand 1996 beim Rechenzentrum der Uni Hannover eine Metasuchmaschine, die versprach, etwa 99 Prozent des deutschen Internets verfügbar zu machen. Dazu greift sie nicht auf eigene Datensammlungen zurück, sondern stellt die Antworten anderer Suchmaschinen zusammen und präsentiert sie dem Anwender.

Die beginnende Kommerzialisierung des Internets zeigen die Gründungen von Amazon (1994) und eBay (1995).

Napster war 1998 der erste Anbieter von Fielsharing-Diensten. Die dabei angebotenen und verbreiteten Dateien lagern nicht auf zentralen Fileservern, sondern werden von den beteiligten "Peers" unmittelbar getauscht. Der Tauschbörsen-Dienst verwaltet nur die Erreichbarkeit seiner Nutzer und den Bestand der von ihnen angebotenen Daten. Mit der zunehmenden Verbreitung geschützter Musik- und Filmwerke sowie kommerzieller Programme stehen die Tauschbörsen unter Kritik und rechtlichen Angriffen.

Auf der Suche nach Nachrichten von außerirdischen Intelligenzlern betreibt das SETI-Projekt seit 1999 eine Variante des Filesharings: Zur Auswertung von Protokollen wird die Rechenleistung von vielen angeschlossenen PCs dazu verwendet, nach Merkmalen für Intelligenz zu suchen. Diese Art des verteilten Rechnens wird heute auch in Botnetzen zum Knacken von Zugangscodes und Verschlüsselungen genutzt.

Als Reaktion auf die Virenscanner schufen die Malware-Schreiber 1990 den ersten polymorphen Virus. Er wandelte ständig seine Form und Größe, so dass er mit den gängigen Methoden nicht erkannt werden konnte.

1990 in Bulgarien und 1998 in Russland entstanden infolge von Wirtschaftskrisen Hackerfabriken und später in Russland auch Hackerschulen. In ihnen wurde im gewerbsmäßigen Stil Hacking-Angriffe und Malware-Programmierung als Auftragsarbeiten gegen Geld ausgeführt.

1996 wurden die ersten Porno-Angebote im Internet bekannt und entstand im Zusammenhang mit Spam-Mails das Phishing, also das gezielte Ausspähen von Zugangsdaten zum Online-Banking. 1999 gründeten Galaiko, Petrichenko und Popow das HangUp-Team, das in den Folgejahren bemerkenswerte Malware in Bezug auf Trojaner, Würmer und Botnetze herstellen wird.

1995 kam SoftRAM auf den Markt. DoubleSpace gab es bereits und es führte zu einer (leichten) Vergrößerung des Speicherplatzes auf Massenspeichern (Festplatten und Disketten), indem es alle Dateien zu einer einzelnen großen komprimierte. SoftRam versprach das auch für den damals ebenfalls noch raren und teuren Arbeitsspeicher. Der Fake flog nach einer Veröffentlichung in der c't auf.

1997 entstanden die Dialer. Diese Einwahlhilfen versprachen die automatische Konfiguration des Internet-Zugangs und verbogen die Einstellungen mit Wonne so, dass die PCs nur noch Kontakt zu teuren Mehrwertdiensten aufnahmen. Bemerkenswert war die Formvielfalt der Dialer und die Tricks, mit denen sie ausgestattet waren. Sie wurden besonders als Trojaner verteilt und es wurde davon berichtet, dass einzelne Varianten beim ersten Start heimlich und böswillig die Systemeinstellungen änderten und dann ihre

Form wandelten. Von da an fragte das Programm brav, ob es die Einstellungen ändern dürfe und zeigte an, welche Folgen das habe. Daran scheiterte auch die Strafverfolgung.

Die Abzocke endete 2003 mit einer Registrierungspflicht für Dialer und Mehrwertdienste (01900, 0900). Die frei tarifierbaren und vielfach missbrauchten Mehrwertdienstenummern unter 01900 verschwanden dadurch nach einer Übergangszeit ganz vom Markt.

Mit dem aufblühenden Domain Name System entstand 1998 das Grabbing, also das Wegschnappen von Marken- und anderen wertvollen Namen mit der Hoffnung, durch Verhandlungen einen guten Preis für sie zu erzielen. In Bezug auf Markennamen hat das die Rechtsprechung alsbald als Straftaten angesehen (Markenmissbrauch, Erpressung).

Mit dem Informations- und Kommunikationsdienstegesetz - IuKDG - wurde 1997 ein Gesetzeswerk zur Regulierung der TK und des Internet geschaffen. Breite Teile davon widmen sich der Gewährung von Anonymität und des Datenschutzes.

Ein Kernstück dabei ist das Telekommunikationsgesetz, das das Fernmeldeanlagengesetz ablöste. Der unsinnigen Trennung zwischen den Telediensten und den Mediendiensten wurde erst 2007 durch das Telemediengesetz ein Ende bereitet.

1999 erging das viel kritisierte Compuserve-Urteil gegen den deutschen Geschäftsführer des Unternehmens. Ihm wurde die Verantwortung für rechtswidrige, aber fremde Inhalte angelastet, die vor allem in den USA gehostet waren. Das Urteil blieb in der Berufung ohne Bestand.

Die Diskussion um die Verantwortung von Zugangs- und Hostprovidern für fremde Inhalte ist auch danach nie ganz abgebrochen und zuletzt im Zusammenhang mit der Sperrung kinderpornographischer Webseiten wieder aufgekeimt.

Jahr	Wirtschaft	Cybercrime
2000	Dotcom-Blase, EMV-Chip	Skimming mit Lesegeräten
2001	Wikipedia	CardersPlanet (Odessa), Javaphile (China) gegen Weißes Haus
2002	Firefox	Online-Wetten (Gambino Lucchese)
2003	Second Life	
2004	Flatrate, Flatrate, YouTube, Pirate Bay, Wikileaks	Sasser, Homebanking-Trojaner Korgo (HangUp)
2005		Sportwetten (betwsc.com; Offshore: Belize), TJX-Hack: 94 Millionen Kundendatensätze, Finanzagenten
2006	FaceBook, ccc: NEDAP-Wahlcomputer	Russian Business Network, Skt Petersburg, Botnet: Gozi (HangUp), McAfee: Organisierte Cybercrime
2007	iTAN	Pharming, Angriff auf Estland, Malware-Baukästen
2008		kombinierter Hacking- und Skimming-Angriff gegen RBS World Pay, dDoS gegen Litauen und Georgien
2009		Twitter-Wurm: JS/Twettir, russische Geldautomaten mit Trojaner infiziert
2010		Stuxnet
		Hacktivismus infolge Auseinandersetzung um Wikileaks

Kommerzielles Internet und organisierte Cybercrime

Seit 2000 hat sich das Internet als Wirtschaftsraum etabliert und sich die Cybercrime organisiert. Stuxnet von 2010 läutet den offenen Cyberwar ein.

Mit dem Platzen der Dotcom-Blase in 2000 wurde massenhaft Kapital vernichtet. Vage Hoffnungen und übersteigerte Erwartungen an längst nicht marktfähigen Produkten hatten massenhaft "Internet"-Firmen entstehen lassen, denen urplötzlich der Geldzufluss abgeschnitten war und die unter lautem Wehklagen verschwanden.

Nur die soliden Firmen aus den Neunziger Jahren überlebten das Desaster und es gibt nur wenige kommerzielle Neugründungen wie Second Life (2003), YouTube (2004) und FaceBook (2006), die sich besser oder schlechter auf dem Markt einrichten konnten.

Richtig erfolgreich wurde die Open Source-Bewegung mit dem freien Online-Lexikon Wikipedia (2001) und den Software-Produkten OpenOffice.org (ab 1999), Firefox (2002), Thunderbird (2003) sowie einem zum produktiven Einsatz fähigen Linux (2003) einschließlich Webserver (LAMP).

In dieser Reihe ist auch Wikileaks zu nennen, das seit 2004 politische Dokumente veröffentlicht und damit für Meinungsfreiheit und Informationsoffenheit kämpft - zuletzt durch die Veröffentlichung militärischer Dokumente aus den Kriegen in Afghanistan und im Irak.

Eine besondere Rolle spielt dabei die 2004 gegründete "Piratenbucht", die inzwischen den wohl bedeutendsten Filesharing-Dienst betreibt und damit auch den Zugang zu ge-

werblich geschützten Werken erleichtert. Aus der Unterstützung des Pirate Bay entstanden Piratenparteien, die in Schweden in das Parlament einzogen und in Deutschland beachtliche Erfolge verzeichnen.

Zwei wirtschaftliche Neuerungen sind hervorzuheben. Schon 2000 wurden auf den ersten Zahlungskarten der EMV-Chip eingeführt, der neben dem Maschinenlesbaren Merkmal den Missbrauch gefälschter Zahlungskarten wenn nicht verhindert, so doch erheblich erschwert. Als Reaktion auf das Phishing mit Spam-Mails führte die Finanzwirtschaft in Deutschland seit 2007 die indizierten TANs ein und erschwerte damit nachhaltig die Kartenkriminalität.

2006 demonstrierte der CCC die Anfälligkeit des NEDAP-Wahlcomputers, dessen Einführung in Deutschland schließlich vom BVerfG untersagt wurde.

In den letzten 10 Jahren hat sich das Internet zu einem festen Bestandteil von Gesellschaft, Wirtschaft und Verwaltung gemausert. Es lässt sich ohne Schmerzen nicht mehr "abschalten", wie hin und wieder gefordert wird. Das gilt besonders für die Wirtschaft, die maßgebliche Aufgaben im Bankenbereich und im Einzelhandel in das Internet verlagert hat und ohne Riesenaufwände nicht mehr zurückrudern könnte. Das gilt auch wegen der jetzt etablierten Informationsdienste. Auf heise.de, de.wikipedia.org, gesetze-im-internet.de und die Datenbanken von BGH und BVerfG mit allen neuen Entscheidungen möchte ich jedenfalls nicht mehr verzichten.

Zulauf haben jedenfalls auch die sozialen Netzwerke. Ihre Nutzer und Betreiber müssen sich erst noch daran gewöhnen, kritisch und vor allem selbstkritisch zu hinterfragen, was sie über sich offenbaren und womit sie sich angreifbar machen können.

Die Datenskandale aus den letzten Jahren zeigen, dass große Datensammlungen auch zum Missbrauch reizen. Die Situation erinnert an den Frühkapitalismus im ausgehenden Neunzehnten Jahrhundert, als Aktiengesellschaften und industrielle Großprojekte entstanden und platzten oder sich als Großbetrug enttarnten.

Das gilt jedenfalls auch für die Cybercrime, die im ersten Jahrzehnt des neuen Jahrtausends kräftig erblüht ist.

1991 wurde von 150 russischen Programmierern in Odessa CardersPlanet gegründet. Dieses Board diente zum Carding-Handel, also dem Handel mit ausgespähten Bank- und Zahlungskartendaten. Das reicht inzwischen von einfachen Kontodaten aus Magnetstreifen über Dumps mit Kontodaten einschließlich PIN und/oder Prüfnummer bis hin zu vollständigen Profilen mit Sozialversicherungsnummer, Konten bei PayPal und eBay usw.

Hinter CardersPlanet.com entstand eine mafiöse und hierarchische Organisation, die ihren "gerechten" Anteil an allen klein- und großkriminellen Geschäften abgriff. Andere Carder-Boards stiegen vermehrt auch in den Handel mit gefälschten Personalpapieren und Universitätsdiplomen ein. Berichte aus 2009 und 2010 sprechen von nachfolgenden Boards, die kostenpflichtige Monopole für kriminelle Dienste - etwa für Skimming-Geräte - vergeben, und Diensteanbieter, die für einen gehörigen Anteil Webshops und das Bezahlwesen für den illegalen Daten-, Programm- und Gerätehandel betreiben.

Seit 2002 veranstaltete der der amerikanisch-italienischen Mafia zugerechnete Gambino Lucchese Online-Wetten. 2005 folgten illegale Sportwetten bei betwsc.com, wobei die Server zunächst "Offshore" in Belize betrieben wurden.

Dagegen nimmt sich der heranwachsende Bengel aus der norddeutschen Tiefebene, der seit 2004 mit seinen Sasser-Würmern Privatanwender ohne Firewalls zur Verzweiflung brachte, fast schon putzig aus.

Würmer bestehen im Gegensatz zu Viren aus selbständigen Programmen, die sich in automatische Verarbeitungsprozesse des PCs einklinken. Sasser hat dabei so viel Eigenaktivität entfaltet, dass die PCs, kaum dass sie gestartet wurden, unter der Last wieder zusammen brachen. Das machen die heute üblichen Botprogramme ganz anders. Ihnen geht es darum, den Zombie zunächst auszuspähen und dann ganz lange und möglichst unbemerkt zu missbrauchen.

Sasser traf auch Fluggesellschaften und andere Unternehmen existenziell, die ganz still blieben. Aus gutem Grund. Nach US-amerikanischen Aktienrecht sind die Vorstände persönlich für die IT-Sicherheit verantwortlich und keiner war bereit, etwas anderes als einen unerwarteten technischen Ausfall einzuräumen.

Schon 2004 entwickelte das HangUp-Team den Homebanking-Trojaner Korgo. Unter seinem Einsatz kam es beim Phishing nicht mehr darauf an, den Bankkunden zur Angabe von Kontonummer, PIN und TAN zu überreden. Die Malware spähte das Onlinebanking unmittelbar aus. Die späteren und verfeinerten Varianten automatisierten den Prozess, gaukelten dem Anwender eine erfolgreiche Transaktion vor und missbrauchten die ausgespähte iTAN zeitgleich für eigene Überweisungen, nicht ohne auch den Internetzugang des Anwenders abzuschießen, um die Spuren der Malware und ihrer Hinterleute zu verwischen.

Der größte bislang bekannt gewordene Hack betraf den Finanzdienstleister TJX, wo ab 2005 etwa 94 Millionen Kundendatensätze gestohlen und noch bis vor kurzem in Dark Markets angeboten wurden. 2008 erfolgte der Hack bei RBS World Pay. Dort wurden zwar nur rund 100 Kundendaten abgegriffen, aber gleichzeitig die Limits ihrer Konten hoch gesetzt. Der Showdown erfolgte am 08.11.2008, als weltweit in 49 Städten und an 130 Geldautomaten das vom Skimming bekannte Cashing betrieben und rund 9 Millionen Dollar erbeutet wurden.

2009 wurde bekannt, dass russische Geldautomaten mit einem Trojaner infiziert waren und Skimming an der Quelle betrieben.

2005 wurden die Finanzagenten als Massenerscheinung bekannt. Sie richten heute vermehrt auf eigenen Namen neue Konten ein, über die beim Phishing oder anderen kriminellen Geschäften anfallenden Beuten weiter geleitet und gewaschen werden. Schon sehr früh schoss sich die Rechtsprechung auf sie ein und es hagelte Verurteilungen wegen leichtfertiger Geldwäsche. Die zivilrechtlichen Schäden tragen sie auch. Ein ganz schlechtes Geschäft.

2006 schlug das HangUp-Team wieder zu und verbreitete mit Gozi die erste funktionstüchtige Botnetz-Malware. Es arbeitete dabei wahrscheinlich mit dem Schurkenprovider Russian Business Network zusammen.

Botnetz-Programmen sind Malware, die sich auf die Fernsteuerung fremder Computer (Zombies) konzentriert. Wie andere Malware müssen sie sich zunächst verbreiten und einnisten.

Dazu dienen ganz bevorzugt die seit 2007 verbreiteten Pharmen. Von ihnen werden viele nachgemachte und manipulierte Webseiten bereit gestellt, die Injektionsverfahren verwenden, um im Browser des Anwenders schädlichen Code zu installieren. Dabei handelt es sich meistens nur um einen "Starter", also einen Kommandostring, mit dem die Malware erst geladen wird. Die nistet sich

anschließend ein, analysiert ihre Umgebung und fordert dann die Programmteile an, die sie hier braucht. Nach dem Update nistet sie sich im Zombie ein, tarnt sich und späht häufig erst einmal die persönlichen Daten des Anwenders aus, denen sie habhaft werden kann. Je nach ihrer Ausrichtung installiert sie Keylogger für die Tastatureingaben, andere Spionageroutinen, Mailserver für den E-Mail-Versand oder Webserver, um ihrerseits als Datenspeicher zu dienen.

Der Sturmwurm hat gezeigt, dass mit den Zombies sehr behutsam umgegangen wird. Die Malware hält sich sehr zurück, versucht, unauffällig zu bleiben und den laufenden Betrieb kaum zu beeinträchtigen. Sie aktualisiert sich und wartet auf Aufträge. Das kann der Versand von Spam, ein DoS-Angriff, die Übernahme von Verwaltungsfunktionen für das Botnetz oder einfach nur sein, ein Terminal für illegale Aktionen des Botnetz-Betreibers zu sein. Stets zu Diensten!

Die Programmierer von Botware müssen firm sein im Filesharing, der Fernwartung, im Missbrauch von Exploits (Schwachstellen in Programmen), im Einsatz von Rootkits (Tarnung) und den schädlichen Funktionen, die ausgeführt werden sollen. Dazu gehören auch Kenntnisse über wirtschaftliche Prozesse (Homebanking, Kursmanipulationen, Finanztransaktionen), das Social Engineering, um den Anwender zu übertölpeln und unachtsam zu belassen, und soziale Kompetenz, um sich vor der Strafverfolgung oder anderen peinlichen Nachstellungen zu schützen.

Eine solche Anforderungspalette können Einzelpersonen kaum leisten. Paget hat 2010 geschätzt, dass für den Betrieb eines Botnetzes etwa drei gute Programmierer nötig sind. Balduan hat schon 2008 über Operating Groups berichtet, die aus mehreren Handwerkern und einem "Kopf" bestehen, der über Aufträge verhandelt, die Arbeit den Handwerkern zuteilt und überwacht und schließlich den Lohn verteilt. Das gilt besonders auch für die Entwicklung von Malware, wobei Balduan Exploit-Händler und Rootkit-Entwickler als unabhängige Zulieferer ansieht.

Dieses Modell funktioniert nur auf Vorkasse. Seine extreme Ausprägung beschreibt Balduan mit den Koordinatoren. Sie sind kriminelle Projektmanager und kalkulieren nach Maßgabe von drei Messgrößen: Aufwand, Gewinn und Entdeckungsrisiko. Danach rekrutiert der Koordinator Leute für bestimmte Aufgaben oder kauft halbfertige Leistungen ein, zum Beispiel bereits ausgespähte Carding-Daten, um das Cashing zu betreiben.

Man munkelt, das nötige Kapital würde die russische Mafia vorstrecken.

Gehen wir einen Schritt zurück: 2007 traten verstärkt Malware-Bausätze in Erscheinung. Mit Klicken und einfachen Mausbewegungen ließen sich damit schädliche Programme basteln, die alsbald von den Virenscannern deaktiviert und entfernt wurden. Mit professioneller Malware hatten sie wenig zu tun.

Schon 2001 unternahm die chinesische Gruppe Javaphile einen Defacement-Angriff gegen das Weiße Haus und verschandelten dessen Webseite. Obwohl sich die Täter outeten, wurden sie in China nicht verfolgt. Ihr Kopf wurde statt dessen Sicherheitsberater.

Das leitet eine Bewegung ein, die Paget Hacktivism nennt. Weitere Höhepunkte dieser eher gesellschaftlichen Aktivitäten sind der cyberwar-ähnlichen Angriff auf Estland (2007) und die dDoS-Angriffe gegen die ungetreuen Länder Litauen und Georgien (2008) sowie gegen Radio Free Europe und im Zusammenhang mit Freiheitsbewegungen in den israelisch-palästinensischen Konflikten.

Die von Paget näher ausgeführten Beispiele zeigen, dass die Auseinandersetzungen auch auf der gesellschaftlichen Ebene immer nachhaltiger und zerstörerischer werden.

Damit ist der Übergang zum Cyberwar eingeleitet. Seine Protagonisten sind nicht nur die Militärs, sondern auch die machtvollen kriminellen Organisationen, starke nationalistische und aktivistische Gruppen, Terroristen und schließlich auch Wirtschaftsunternehmen, die mit Wirtschaftsspionage, destruktiven Nadelstichen und finalen Schlägen ihre Positionen behaupten oder verbessern wollen.

Die jüngst bekannt gewordene Malware Stuxnet markiert den Übergang zum heißer werdenden Cyberwar. Ihre Entwicklung scheint richtig teuer gewesen zu sein, sie greift mehrere bislang unbekannte Exploits unter MS an und hat sich auf die Steuerung von Industrieanlagen spezialisiert. Damit verlässt sie die virtuelle Welt und zeigt, dass sie Kritische Infrastrukturen angreifen kann.

Das letzte Wort gilt den Schurkenprovidern. Beispiel gebend ist das seit 2006 bekannte und später untergetauchte Russian Business Network - RBN, das WhoIs-Protection und Bulletproof-Server sowie die darum angesiedelten sozialen Dienste anbietet: Schweigen und von dem Verschwiegenen kassieren. Je mehr Nachfragen kommen, desto teurer wird der Service.

Nachtrag (Januar 2011):

WikiLeaks hat sich nicht nur einen Namen damit gemacht, als Whistleblower-Plattform Schlag auf Schlag geheime Dokumente aus dem Afghanistan- und dem Irak-Krieg sowie zuletzt diplomatische Depeschen der USA veröffentlicht hat. Bedeutender sind die Reaktionen darauf, Kontensperren und wechselseitige Angriffe von Unterstützern. Darin zeigt sich das, was vor allem McAfee vorausgesagt hat: *Die Grenze zwischen Internetkriminalität und Internetkrieg verschwimmt ... immer mehr*, der Hacktivismus nimmt zu und eskaliert immer stärker zum Cyberwar, in dem die Grenzen zwischen den Akteuren und ihren Zielen immer weiter verschwimmen.

Fazit. Keine Alternative

Die Menschheit hat mehrere Jahrhunderte gebraucht, um aus der Informationstechnik und der Telekommunikation eine virtuelle Umgebung mit Eigenleben und fester Einbindung in die Realität zu schaffen. Es hat keine zwei Jahrzehnte gedauert, um dieses Technotop mit wirtschaftlichen Mechanismen so auszufüllen, dass es nicht mehr wegzudenken ist. Das dritte Jahrtausend startet mit einer sklavischen Netzabhängigkeit, die nicht nur ungeahnte Informationschancen bietet, sondern auch Optionen zur physischen Vernichtung.

Huxley sprach angesichts der fordschen Industriealisierung und dem Totalitarismus von einer (faschistoiden) braven, besser gesagt: mutigen neuen Welt. Richtig mutig ist hingegen die Welt, in die wir uns gerade hinein bewegen.

Die Chancen und Gefahren der Cyberwelt sind längst nicht vollständig bewertet und gegeneinander abgewogen. Die Handelswirtschaft hat sich ihr aber bereits ergeben und ist kaum noch in der Lage, die Reißleine zu ziehen. Die Option, eine virtuelle Nebenwelt abzuschalten, gibt es nicht mehr. Sie ist zum integralen Bestandteil der realen Welt geworden.

Das zeigt sich nicht zuletzt daran, dass Informationsdienste und Handelsplattformen am einfachsten per Internet erreichbar und bedienbar sind. Auch in der Kommunikation gilt: Schnell, schneller, sofort.

Für politische und strategische Entscheidungen ist das gefährlich und tödlich. Im computerbasierten Börsenhandel haben dumme Zufälle zu Crashs und bei der Berliner Feuerwehr die 2000-Jahr-Umstellung zum Ausfall aller wichtigen Informations- und Kommunikationsstränge geführt. Ihre Lösch- und Rettungsfahrzeuge fuhren Streife durch Rauchschwaden und alkoholisierte Mitmenschen.

Einen Weg zurück gibt es aber nicht. Eine Finanzwirtschaft ohne Onlinebanking und international vernetzten Geldautomaten ist nicht wieder herstellbar. Dasselbe gilt für den großen Einzelhandel, der seine kleinen Filialen aufgegeben hat und sich jetzt im Internet präsentiert.

Auf die Marktübersichten und die Informationsangebote, die mir jetzt zur Verfügung stehen, möchte ich auch ohne Not nicht mehr verzichten.

Neue Gefahren

Stuxnet zeigt, dass wir an der Schwelle zum Cyberwar stehen. Seine Krieger werden sich nicht durch das Völkerrecht aufhalten lassen, sondern nur dann, wenn sie schmerzhafte Strafen zu erwarten haben.

Wir müssen einfach davon ausgehen, dass sich die Realität mit ihrem virtuellen Abbild verbunden hat. Es ist real und nicht mehr surreal, spiegelt die gewohnten Marktmechanismen wider und hat genügend Schnittstellen, wo die eine Umgebung in die andere übergehen kann. webmoney, paysafecard und das angestaubte e-Gold sind Beispiele für finanzwirtschaftliche Systeme, die sich gleichermaßen in der realen und der virtuellen Welt bewegen, die Homebankingtrojaner, die sich in der Transfer einschalten, und mehr noch der Stuxnet-Trojaner, der Industrieanlagen zu steuern und zu sabotieren vermag, sind Beispiele dafür, wie sich aus der virtuellen Welt heraus destruktiv auf die reale einwirken lässt.

Hinzu kommt das gezielte Hacking. Sein Etappenziel ist die Erlangung von Administratorenrechten. Wer über sie verfügt, kann alles manipulieren, was die angegriffene IT

zu verwalten und zu steuern vermag. Je tiefer die IT die Realität durchdringt, desto breiter sind auch die Manipulationsoptionen, die der Hacker erlangt. Er kann Klimaanlagen steuern, wodurch Lebensmittel, Medikamente oder anderes vernichtet wird, Transportsysteme stören oder wirtschaftliche Infrastrukturen verhemmungslosen. Ich denke dabei vor allem an finanzwirtschaftliche Clearingeinrichtungen und den nicht mehr nur computergestützten, sondern computerbasierenden Börsen- und Wertpapierhandel. Ich vermute, dass ihre Sicherungen unvollständig sind, weil es bislang nur um ihre operative Optimierung ging. Punktuelle und gezielte Angriffe könnten deshalb Chaos ohne Gleichem verursachen.

Dasselbe gilt für die Steuerung von Infrastrukturprozessen, zum Beispiel bei der Stromversorgung oder der Telekommunikation. Eine Überlastung an der einen Stelle, eine Fehlfunktion an der anderen und ein Ausfall an der dritten können Kaskadenprozesse auslösen, die das ganze System zerbrechen lassen. Wenn das Ganze erweitert wird mit gewaltigen Angriffen (Militär, Terrorismus, kriminelle Überfälle), dann haben wir den Cyberwar.

Neue Perspektiven

Wie kann man dem begegnen?

Zunächst mit Nachdenken und Analyse.

Unter dem Regime der schlanken Geschäftsprozesse und der Arbeitsverdichtung stehen für solche Aufgaben aber keine Leute und keine Ressourcen zur Verfügung. Politik, Verwaltung und die produktive Wirtschaft müssen deshalb wieder erkennen, dass sie nur dann überleben, wenn sie das Risiko-, Sicherheits- und Visionsmanagement installieren und fördern. In der öffentlichen Verwaltung beschränkt sich das häufig genug auf die Schaffung von Dienstanweisungen. Sie liefern im "Shit happens"-Fall einen Verantwortlichen und lassen die Organisation unangetastet und gut dastehen.

"Visionsmanagement" ist eine Wortschöpfung von mir. Damit meine ich eine besondere Form des Risikomanagements, das sich nicht nur an BSI- und anderen Regelwerken orientiert, sondern eigene Betriebsstrukturen, kriminelle Angriffsformen und wirtschaftliche Neuerungen betrachtet, um sie bewerten und Gefahren vorzubeugen. Dazu baucht man gute Leute, die aus dem Apparat selber kommen und, wie es auch für Führungsaufgaben gilt, frei von Arbeit sind.

Es bedarf nicht nur der organisationsbezogenen Betrachtung, sondern auch einer strategischen Bewertung von technischen und kriminellen Entwicklungen, um Gefahrenpunkte und -szenarien zu entdecken, die außerhalb der eigenen Organisation liegen. In der Pflicht sehe ich nicht nur die Polizei, sondern auch Hochschulen, Wirtschaftsverbände und Kooperationen zwischen ihnen.

Nicht zuletzt bedarf es auch einer neuen Ausrichtung der Strafverfolgung mit geschultem Personal und strategischer Ausrichtung. Es macht in diesem Bereich keinen Sinn, nur noch aufklärend Straftaten hinterher zu fahnden und nicht auch die Strukturen zu zerbrechen. Dazu ist vom Cyberfahnder schon genug geschrieben worden.

Hannover, November 2010