Wolfgang A. Halang
Robert Fitz

Nicht hackbare Rechner und nicht brechbare Kryptographie

2. Auflage

EBOOK INSIDE

Springer Vieweg

Nicht hackbare Rechner und nicht brechbare Kryptographie

Wolfgang A. Halang · Robert Fitz

Nicht hackbare Rechner und nicht brechbare Kryptographie

2., wesentlich neu bearbeitete und erweiterte Auflage

Springer Vieweg

Wolfgang A. Halang
Qingdao Uni. of Science
and Technology
Qingdao
China

Robert Fitz
Hochschule f. Angewandte
Wiss. Hamburg
Hamburg
Deutschland

ISBN 978-3-662-58026-4 ISBN 978-3-662-58027-1 (eBook)
https://doi.org/10.1007/978-3-662-58027-1

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Ursprünglich erschienen im Datakontext-Verlag, 2002

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Jedesmal, wenn in den Medien wieder über Fälle wie einen großen Datendiebstahl bei einem Internetkonzern, über das Eindringen von Hackern in das Netz des Deutschen Bundestages oder eine Abhöraffäre sowie die damit verbundenen Schäden berichtet und suggeriert wird, dass es letztendlich keinen wirklich effektiven Schutz dagegen gebe, halten sich die beiden Autoren dieses Buches die Bäuche vor Lachen. Genauso würde wahrscheinlich auch Konrad Zuse, der Erfinder programmgesteuerter Datenverarbeitungsmaschinen, über heutige IKT-Sicherheitsprobleme lachen. Wenn Sie das vorliegende Buch gelesen haben werden, werden auch Sie zu den Lachern gehören.

Der Tatsache, dass alle heute gegen Hacker- und Abhörangriffe eingesetzten Maßnahmen weder uneingeschränkt wirksam und schon gar nicht nachhaltig sind, stellt das vorliegende Buch seine Botschaft entgegen: Schadprogramme, also Viren, Würmer, Trojanische Pferde und ausführbare Internetinhalte, verursachen zwar große Verluste, stellen aber ein technisch sehr leicht lösbares Problem dar; denn – wie wir sehen werden – ist seit fast zwei Jahrhunderten das Konstruktionsprinzip bekannt, programmgesteuerte Digitalrechner mit physisch von ihren Datenspeichern getrennten sowie gerätetechnisch schreibgeschützten Programmspeichern auszustatten und derart unüberwindbar gegen alle heutigen und zukünftigen, auf Schadprogrammen basierenden Angriffsarten zu schützen. Weiterhin gibt es auch seit rund eineinhalb Jahrhunderten perfekt sichere Methoden zur Datenchiffrierung mit Einmalschlüsseln, die nicht nur systematisch nicht brechbar sind und es auch nie sein werden, sondern die auch einfach und leicht verständlich sind. Allein ihre Anwendung kann das Ausspähen abgehörter oder gespeicherter Daten nachhaltig verhindern.

Das vorliegende Buch richtet sich einerseits an alle technisch interessierten Anwender, die mehr über die wahren Gründe der Angreifbarkeit heutiger Systeme und Netze erfahren möchten, um kompetent mitreden und um sichere Systeme und Netze einfordern zu können. In der Komplexität heutiger Systeme wird der Leser ein Flickwerk aus wenig durchdachten und sich als ungeeignet erweisenden Lösungen erkennen, die jeglicher Innovation entgegenstehen. Andererseits werden in Form von Patenten bzw. Patentanmeldungen seit bereits etwa zwei Jahrzehnten den Stand der Technik definierende Architekturkonzepte zur Entwicklung sicherer Rechensysteme vorgestellt. Die entsprechenden

Maßnahmen sind auch zur Sicherung handlicher Kommunikations- und Datenverarbeitungsgeräte (Mobiltelefone, Smartphones, Tablet-PCs etc.) geeignet, die sich in den letzten Jahren rasant verbreitet haben, womit sie in den Fokus von Angreifern gerückt sind. Wegen ihrer Angreifbarkeit durch direkten physikalischen Zugriff bedarf diese Geräteklasse jedoch zusätzlichen Schutzes. Wie er sich technisch recht leicht realisieren lässt, wird hier gezeigt.

Zweifelsohne ist der Titel dieses Buches mit dem zweimal darin enthaltenen „nicht“ stilistisch nicht gelungen. Aber den Autoren ist nichts Besseres eingefallen, um absolut unmissverständlich auszudrücken, dass es einerseits um Digitalrechner geht, die schlicht und einfach nicht gehackt werden können, weil dies konstruktionsbedingt ausgeschlossen ist, und andererseits um kryptographische Verfahren, deren perfekte Sicherheit auf der mathematischen Unmöglichkeit beruht, eine Gleichung mit zwei Unbekannten zu lösen. Von gegen Schadprogramme gesicherten Rechnern und sicherer Kryptographie zu reden, wäre zu schwach gewesen, weil das auch andere tun, wenn sie über marktübliche Abwehrmaßnahmen gegen Hacking sowie gängige kryptographische Verfahren berichten, die aber nie absolut sicher sind. Außerdem ist der Begriff Sicherheit nach DIN/VDE 31 000 Teil 2 relativ: Er lässt immer noch ein Restrisiko jenseits eines gesellschaftlich als tragbar angesehenen Grenzrisikos zu. In den hier betrachteten Domänen besteht jedoch kein Restrisko: Digitalrechner lassen sich absolut hackingresistent bauen und Verschlüsselungen können perfekt sicher, d. h. unbrechbar sein.

Dieses Buch zeigt auf, was entweder in Vergessenheit geraten ist oder permanent aus welchen Gründen auch immer von Fachwelt und Öffentlichkeit ignoriert wird. Es legt dar, dass abschließende Lösungen für allgemein als gesellschaftliche Probleme betrachtete und durch den Einsatz ungeeigneter Methoden und minderwertiger technischer Artefakte verursachte Schwierigkeiten seit Jahrzehnten bzw. fast zwei Jahrhunderten bekannt sind – mithin schon zu Zeiten, als es weder Digitalrechner noch Rechnernetze gab und die Probleme noch gar nicht entstanden waren. Warum diese Lösungen nicht auf dem Markt erhältlich sind und warum sie in der Praxis nicht eingesetzt werden, möchten die Autoren hier nicht diskutieren. Sie überlassen es Ihnen, sich zu dieser höchst interessanten Fragestellung eine eigene Meinung zu bilden.

Im Sommer 2018

Prof. Dr. Dr. Wolfgang A. Halang
Prof. Dr.-Ing. Robert Fitz

Inhaltsverzeichnis

Abkürzungen und Akronyme

AES	Advanced Encryption Standard
API	Application Programming Interface
App	Applikation
ASCII	American Standard Code for Information Interchange
BASIC	Beginner's All-Purpose Symbolic Instruction Code
BAT	Batch
BGB	Bürgerliches Gesetzbuch
BIOS	Basic Input Output System
BK	Bundeskriminalamt (in Österreich)
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMWi	Bundesministerium für Wirtschaft und Technologie
Bot	Roboter
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAD	Computer Added Design
CD	Compact Disk
CD-ROM	Compact Disk-Read Only Memory
CD-RW	Compact Disk-Read Write
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team / Coordination Center
CMOS	Complementary Metal Oxid Semiconductor
COM	Command
CPU	Central Processing Unit
CSI	Computer Security Institute

DCC	Direct Client Connection
DD	Double Density
DES	Data Encryption Standard
DFN	Deutsches Forschungsnetz
DIN	Deutsches Institut für Normung e.V.
DLL	Dynamic Link Library
DMV	Demonstrationsmakrovirus
DNS	Domain Name Service
DOC	Document
DOS	Disk Operating System
DOS/VS	Disk Operating System/Virtual Storage
DOT	Document Template
DVD	Digital Versatile Disk
EDV	Elektronische Datenverarbeitung
EEPROM	Electrical Erasable Programmable Read Only Memory
EIDE	Enanced Integrated Drive Electronics
EPROM	Erasable Programmable Read Only Memory
Europol	Europäisches Polizeiamt
EXE	Executable
E-Business	Electronic Business
E-Commerce	Electronic Commerce
E-Mail	Electronic Mail
FAT	File Allocation Table
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GPS	Global Positioning System
GPT	GUID Partition Table
GSM	Global System for Mobile Communication
GUID	Globally Unique Identifier
HD	High Density
HTML	Hyper Text Markup Language
IBAN	International Bank Account Number
ICSA	International Computer Security Association
IDE	Integrated Drive Electronics
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems

IKT	Informations- und Kommunikationstechnik
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IRC	Internet Relay Chat
IrDA	Infrared Data Association
IRS	Intrusion Reaction Systems
ISDN	Integrated Services Digital Network
IT	Informationstechnologie
iTAN	indizierte Transaktionsnummer
ITW	In The Wild
JCL	Job Control Language
LAN	Local Area Network
LBA	Linear Block Address
MAPI	Messaging Application Programming Interface
MBR	Master Boot Record
Me	Millennium edition
MS	Microsoft
NATO	North Atlantic Treaty Organization
NCSA	National Computer Security Association
NT	New Technology
NTFS	New Technology File System
OSI	Open System Interconnection
OS/2	Operating System/2
OVL	Overlay
PC	Personal Computer
PDA	Personal Digital Assistent
PGP	Pretty Good Privacy
PIN	Personal Identification Number
POST	Power On Self Test
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
ROM	Read Only Memory
SCR	Script
SD	Secure Digital
SoC	System on Chip
SPS	Speicherprogrammierbare Steuerung
SSD	Solid State Disk

StGB	Strafgesetzbuch
SYS	System
S/MIME	Secure / Multipurpose Internet Mail Extensions
TCP	Transmission Control Protocol
TSR	Terminate Stay Resident
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus
VBA	Visual Basic for Applications
VBS	Visual Basic Script
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
WAB	Windows Address Book
WAN	Wide Area Network
WAP	Wireless Application Protocol
WinCC	Windows Control Center
WLAN	Wireless Local Area Network
WSH	Windows Scripting Host
WWW	World Wide Web

Sicherheitszustand von Rechnern und Netzen

1

Kaum ein anderes technisches Gebiet besitzt für die Menschen unseres Kulturkreises eine solche Bedeutung wie die Informationstechnik mit ihren vielfältigen Auswirkungen in privaten und beruflichen Bereichen. Der weltweite Zusammenschluss vieler Rechner bzw. digitaler Systeme zu einem Netz ließ wiederum das Internet mit seinen enormen Informations- und Kommunikationsmöglichkeiten entstehen. Durch die erweiterten Möglichkeiten ist allerdings auch die Anzahl potentieller Eindringlinge gestiegen. Die Erfahrung hat gezeigt, dass vorhandene Sicherheitslücken mit nachträglichen Erweiterungen bestehender Systeme im Allgemeinen nicht geschlossen werden können. Allerdings entspricht diese Vorgehensweise der gängigen Praxis. Eine solche Methode muss zwangsläufig fehlschlagen, was durch die jüngsten Entwicklungen auf dem Sektor der Schadprogramme überdeutlich unterstrichen wird.

1.1 Motivation

Um dem untragbaren Zustand, dass weltweit nahezu jeder, der rudimentäre Kenntnisse der Datenverarbeitung und genügend kriminelle Energie besitzt, die Rechner von Regierungen, international tätigen Gesellschaften und Unternehmen lahmlegen oder Daten manipulieren oder löschen und dadurch horrende Schäden verursachen kann, endlich ein Ende zu bereiten, werden in diesem Buch gerätetechnisch unterstützte programmunbeeinflussbare Maßnahmen vorgestellt, die in der Lage sind, Eindringlinge – insbesondere in Form von Malware, also *Viren*, *Würmer*, *Trojanische Pferde* und *ausführbare Internetinhalte* – dauerhaft und sicher unwirksam zu machen, wobei die genaue Schädlingsspezifikation für die Wirksamkeit dieser Maßnahmen unerheblich ist.

Zum derzeitigen Zustand der Unsicherheit ist es primär durch die schnellen, gut ausgebauten globalen Kommunikationssysteme gekommen, die rasche Verbreitung soft-

W. A. Halang, R. Fitz, *Nicht hackbare Rechner und nicht brechbare Kryptographie*,
https://doi.org/10.1007/978-3-662-58027-1_1

warebasierter Schädlinge ermöglichen. Wurde in früheren Jahren ein programmbasierter Schädling entdeckt, so hatten die mit der Bekämpfung softwaretechnischer Schädlinge befassten Unternehmen in der Regel genügend Zeit, ihre Produkte zu aktualisieren. Während die heutzutage gebräuchlichen Softwareprodukte lediglich vor bereits bekannter Malware einen gewissen Schutz bieten, sind die meisten Systeme neuer, noch nicht bekannter Malware schutzlos ausgeliefert. Da allerdings, je nach Zählweise und betrachtetem Einfallstor, täglich einige hundert bis mehrere tausend neue Schädlinge hinzukommen, raten manche Experten, die installierte Antivirensoftware mindestens stündlich zu aktualisieren.

Wie dringend notwendig eine Lösung dieses Problems ist, kann man sich leicht vor Augen führen, wenn man an den immensen volks- und betriebswirtschaftlichen Schaden denkt, den diese Schädlinge verursachen. Wie Studien namhafter Organisationen (siehe z. B. [16]) belegen, sind die durch Malware verursachten Gefahren und Schäden in den letzten Jahren drastisch gestiegen. Nach Untersuchungen des Bundeskriminalamtes (BKA) [6, 7] hat der allein durch Internetkriminalität verursachte Schaden schon 2011 in Deutschland 71,2 Millionen Euro betragen. Dies bedeutet eine Steigerung gegenüber dem Vorjahr um 16 %. Ferner konnte eine gesteigerte Professionalität der eingesetzten Schadsoftware verzeichnet werden. Eine zunehmend verbreitete Variante der Internetkriminalität ist ferner digitale Erpressung, bei der entweder ein digitales Schutzgeld in Form von bspw. Paysafecard-Guthaben verlangt wird, um wieder Zugang zu den durch einen softwarebasierten Schädling verschlüsselten eigenen Daten auf dem Massenspeicher des eigenen Systems zu bekommen, oder um sich von einem bevorstehenden Überflutungsangriff oder davon freizukaufen, dass kompromittierende Daten, die ein Schädling auf dem eigenen Rechner ausgespäht hat, nicht in Umlauf gebracht werden, oder einfach nur dafür, dass sich der Angreifer bereiterklärt, nicht publik zu machen, dass das System des Opfers erfolgreich angegriffen worden ist, denn dies könnte neben einem Imageverlust je nach Organisation auch Umsatzeinbußen oder Schlimmeres nach sich ziehen. Daher ist es verständlich, dass viele Betroffene von Anzeigen absehen und die Dunkelziffer extrem groß sein dürfte. Laut Angaben des BKAs sind allerdings nicht nur befürchtete Rufschädigungen für das zögerliche Anzeigeverhalten ausschlaggebend, sondern auch fehlendes Vertrauen in die Kompetenz der Sicherheitsbehörden. Besonders gefährdet seien daher viele deutsche mittelständische Unternehmen, da diese zu den weltweit innovativsten zählen und dies Begehrlichkeiten weckt. Ferner habe sich gezeigt, dass mobile Endgeräte wie bspw. Smartphones ein zunehmend lukratives Ziel seien, um entweder das im Online-Banking häufig verwendete SMS-basierte Authentifikationsverfahren zu kompromittieren oder um diese Geräte als Bestandteile in Botnetze zu integrieren, da sie in der Regel dauerhafte Netzverbindungen unterhielten. Bereits im Mai 2000 richtete ein einziger programmbasierter Schädling laut [2] weltweit einen Schaden von rund zehn Milliarden Dollar an, sodass sich einer Studie [22] zufolge die durch Malware verursachten Kosten, inklusive nicht realisierter Verkäufe und Produktionsausfälle, schon für das Jahr 2000 auf weltweit 1,6 Billionen Dollar beliefen. Laut einer Veröffentlichung des österreichischen Bundeskriminalamtes (BK) [5] geht Europol davon aus, dass sich der allein durch Cyberkriminalität verursachte Schaden weltweit auf jährlich 750 Milliarden Euro beläuft.

Statistiken und Befragungen hin oder her, es bleibt festzuhalten, dass circa eine Billion Euro jährlich für eine höchst unnötige und vor allem vermeidbare Sache ausgegeben werden. Wie obige Ausführungen ferner zeigen, ist dies kein vorübergehendes Problem, sondern besteht in ähnlicher Größenordnung schon seit mehreren Jahrzehnten, und es ist nicht abzusehen, dass sich an dieser Situation zukünftig etwas im positiven Sinne ändern wird. Im Gegenteil ist eher davon auszugehen, dass sich dieser Zustand noch weiter durch extrem leistungsfähige, aber unzureichend geschützte mobile Geräte wie Smartphones weiter verschärfen wird. Diese Entwicklung aufzuzeigen, wird einen gewissen Teil des vorliegenden Buches einnehmen. Aber selbst wenn die Gefährdungssituation nur auf dem derzeitigen Stand stagnieren würde, bedeutete dies, dass nicht nur in den letzten 18 Jahren circa 18 Billionen Euro unnützerweise verschwendet wurden, sondern dass auch zukünftig jedes Jahr weitere Unsummen versanden würden, denn wir werden sowohl aufzeigen, dass nicht nur die Gefährdungsproblematik seit mindestens dieser Zeit bekannt ist, als auch darlegen, dass wirkungsvolle konstruktive Lösungen, die uns vor diesen Gefahren sicher schützen könnten, seit langer Zeit existieren.

Wenn sich aufmerksame Leser an dieser Stelle berechtigterweise fragen, warum dann aber bisher nichts unternommen wurde, um der Problematik Herr zu werden und das Übel an den Wurzeln zu packen, sondern lediglich die einen oder anderen Symptome behandelt werden, muss man sich nur die Frage stellen, wer Nutzen aus dieser Situation zieht. Wir werden dieser Fragestellung im Folgenden nachgehen, um die Zusammenhänge aufzuzeigen und die eigentliche Problematik besser verstehen zu können, denn es handelt sich hierbei – wie fälschlicherweise oft angenommen wird – *nicht* um ein rein technisches Problem.

Aber was bringt Menschen dazu, z. B. Viren zu programmieren, wobei das Wort Viren hier in der – wie so oft in der einschlägigen Literatur zu diesem Thema – verallgemeinerten Bedeutung als Oberbegriff für alle Arten von Malware verstanden werden soll? Lediglich 5 % der gefassten Virenprogrammierer gaben als Beweggrund Verärgerung, z. B. über bestimmte Unternehmen, an. Der weitaus größte Teil tut es entweder aus Geltungssucht oder aus Geldgier, wobei kein persönlicher Groll gegen ein potentielles Opfer vorhanden ist. Spätestes hier wird deutlich, dass es sich im Grunde genommen um ein gesellschaftliches Problem handelt. Dabei sollte man sich für einen Moment vor Augen halten, welche enormen Ressourcen zur Verfügung stehen könnten, wenn es gelänge, Wissen und Arbeitseifer der Virenprogrammierer in konstruktive Bahnen zu lenken. Da dies aber äußerst schwierig sein dürfte, soll das vorliegende Buch zumindest dazu beitragen, potentielle Opfer sicher vor Eindringlingen zu schützen und das einseitige, höchst lukrative „Spiel“ endgültig zu beenden, auf das sich Antivirensoftwarehäuser sowie Virenprogrammierer und -verbreiter auf Kosten der Endanwender eingelassen haben.

Die Regeln dieses „Spiels“ sind leicht erklärt. Es gibt im Prinzip drei Parteien:

- **Virenprogrammierer oder -verbreiter** stellen die Täter dar, die sich zur Aufgabe gemacht haben, möglichst effektive Schädlinge zu entwickeln und unter Pseudonymen zu verbreiten oder sich einfach nur die angebotenen Werkzeuge zu Nutzen zu machen, um

mittels krimineller IT-basierter Handlungen illegal Geld zu erhalten. Bei Erfolg ist Ersteren Achtung und Anerkennung ihrer Fangemeinde gewiss und Letzteren winken relativ große Geldbeträge als Belohnung bei, im Vergleich zu anderen kriminellen Handlungen, vergleichsweise geringem Risiko. Insbesondere bei Letzteren handelt es sich laut [12] um international agierende Gruppen von Straftätern.

- **Antivirensoftwarehäuser** haben eine Art „Schutzmachtfunktion“ übernommen, deren Aufgabe darin besteht, die Angst vor Angriffen durch Malware in den Medien präsent zu halten, den Eindruck zu erwecken, ihre Produkte könnten einen realen Schutz bieten, und sich diese Bemühungen entsprechend honorieren zu lassen.

- **Anwender** von Datenverarbeitungsanlagen oder mobilen Geräten werden angehalten, immer die neuesten Antivirenprodukte zu kaufen und auf ihren Anlagen bzw. Geräten zu installieren, d. h. für die Kosten aufzukommen, Arbeit zu leisten und den Schaden zu haben, wenn die Softwareunternehmen nicht schnell genug waren, d. h. sie haben die Opferrolle inne.

Wie die Bank beim Roulette, so gewinnt eine Gruppe immer – die Softwarehersteller.

Da es sich hierbei, wie gesagt, um ein gesellschaftliches Phänomen handelt, schließen sich auch Virenprogrammierer oft zu Gruppen zusammen, in denen sie ihre Erfahrungen austauschen und durch besonders spektakuläre „Erfolge“ ihr Ansehen in der Gruppe verbessern sowie die Stellung der eigenen Gruppe gegenüber rivalisierenden Gruppen erhöhen.

Doch wie alle Gruppierungen benötigt auch die virenprogrammierende Zunft ein Forum. Früher waren dies meist die sogenannten Mailboxen, die dem „Untergrund“ als Informationsweg dienten. Um Zugang zu diesem Zirkel zu bekommen, mussten Neulinge oft ganze Kataloge von Fragen beantworten, bevor ihnen erlaubt wurde, auf entsprechende Datenbereiche zuzugreifen und sich dort Informationen, Tricks und Programmierwerkzeuge zu besorgen. Durch diese Fragenkataloge wurde erreicht, dass man quasi unter sich blieb und nur jemand aufgenommen wurde, der schon einschlägige Erfahrungen nachweisen konnte.

Später wurde von einigen Mailboxbetreibern eine andere Methode eingeführt, um den Zugriff auf ihre Informationspools zu beschränken: Nur wer ein neues, noch unbekanntes Virus vorweisen konnte, wurde aufgenommen und bekam entsprechende Zugriffsrechte eingeräumt. Da es aber nicht jedem möglich war, ein wirklich neues, selbstprogrammiertes Virus vorzuweisen, verfiel man darauf, ein bekanntes Virus nur soweit abzuändern, dass es von keinem Antivirenprogramm mehr erkannt werden konnte. Dies ist einer der Gründe, weshalb es von einigen Viren eine Unzahl verschiedener Varianten gibt, die sich nur unwesentlich unterscheiden.

Mailboxen spielen heutzutage nur noch eine untergeordnete Rolle als Kommunikationsmittel für Virenprogrammierer und solche, die es werden wollen. Das Internet bietet der Virenprogrammiererszene wesentlich umfassendere, schnellere und kostengünstigere Möglichkeiten. Besonders durch die grafische Aufbereitung des Internets mittels des

World Wide Web (WWW) wurde dieses Medium auch Anwendern zugänglich, die sich nicht mit Programmierung in irgendeiner Form beschäftigen. Dadurch hat sich auch die Informationssituation für potentielle Virenprogrammierer „entspannt“: Es ist heutzutage kein Problem mehr, sich ganze Virensammlungen aus dem Internet zu besorgen oder Programmiertipps zum Erstellen von Viren zu lesen. Ferner gibt es mittlerweile Virenkonstruktionswerkzeuge, die auch Nichtfachleute in die Lage versetzen, sich ihre eigenen Viren zu bauen.

Verschärft wurde die Situation noch durch das Aufkommen der sogenannten Makroviren, mit deren Hilfe nicht nur ausführbare Programme, sondern auch Dokumente Träger von Malware sein können. Des Weiteren kommt hinzu, dass Makrosprachen sehr leicht zu erlernen sind. Wem das alles noch zu kompliziert ist, der hat heutzutage sogar die Möglichkeit, sich sein Virenarsenal für wenig Geld über das Internet oder auf Datenträgern nach Hause schicken zu lassen, d. h. in Folge der heutigen schnellen Kommunikationswege sind nur noch die allerneuesten Viren und Informationen den eigentlichen Virenprogrammierern vorenthalten. Dies führt zu der jetzigen Situation, dass Personen, die sich über Ausmaß und Folgen einer Infektion mit Malware nicht bewusst, geschweige denn in der Lage sind, diese selbstständig zu kreieren, doch mit Malware „herumspielen“ (siehe [14, 15]).

So wird bspw. in [35] beschrieben, wie man Malware programmieren, kostenlos telefonieren oder fremde Mobilfunkmailboxen abhören oder manipulieren kann. An diesem Buch haben „legendäre Hacker“ aus verschiedenen ehemaligen Szenegruppen mitgewirkt. Als Zugabe bekommt jeder Leser ein Passwort für spezielle Internetseiten, über die er eine Zeit lang laufend mit den neuesten Schädlingen versorgt wird.

Einer Zeitschrift, in der zwei die Vorgehensweise von Angreifern beleuchtende Artikel [23, 29] enthalten sind, ist eine CD-ROM beigelegt, die einige Schadprogramme enthält, mit denen die Leser ihre „Sicherheit testen“ können. Sie können damit ausprobieren, welche Möglichkeiten derartige Programme bieten und wie einfach sie sich bedienen lassen. Allerdings wird in [29] darauf hingewiesen, dass aus rechtlichen Gründen keine detaillierten Anleitungen zur Benutzung der Programme enthalten sind, was auf Grund der erwähnten einfachen Bedienbarkeit auch nicht nötig ist. Aus Sicht der Autoren bzw. der Zeitschrift besteht ebenfalls kein Grund mehr, in den Artikeln mit detaillierten Anleitungen zu werben, da der Leser, wenn er diese liest, die Zeitschrift inklusive CD-ROM für einen einstelligen Euro-Betrag bereits gekauft hat und für diesen Preis kaum mehr erwartet.

Hinzu kommt, dass Rechner mit den dazugehörigen Kommunikationseinrichtungen heute eine wesentlich bedeutendere Rolle als früher einnehmen. Man denke nur an die neuesten Entwicklungen im Bereich des elektronischen Handels, wo Bankgeschäfte, Bestellungen, Aktienhandel und Reisebuchungen längst schon Realität sind. Gerade die Unternehmen, die sich mit *E-Business* beschäftigen und denen enorme Aktienkurssteigerungen prophezeit werden, erleiden häufig empfindliche Kurseinbrüche, wenn wieder einmal bekannt wird, dass sie das Sicherheitsproblem nicht gelöst haben.

In [25] ist bspw. zu lesen, dass das Internet oft als Modell für die Kommunikationstechnik der entstehenden Informationsgesellschaft gelte oder gar mit dieser gleichgesetzt werde, wobei die Frage der Sicherheit jedoch noch nicht zufriedenstellend geklärt sei.

Es wird darauf hingewiesen, dass sich viele Menschen zunehmend verunsichert und einer Großtechnologie ausgesetzt fühlten, bei der die vertrauten Formen des sozialen Verhaltens, Vertrauens und des Schutzes in den Hintergrund träten. Die Lösung liege in der Dezentralisierung der Sicherheit und der Möglichkeit zur Selbstbestimmung der Kommunikationsteilnehmer. Die geforderte Dezentralisierung bedeutet aber, dass die angestrebte Sicherheit in jedem und damit durch jedes einzelne System realisiert wird. Es ist die dem vorliegenden Buch gestellte Aufgabe, gerade dafür die nötigen Grundlagen zu vermitteln.

Wer hofft, das Problem könne sich durch Evaluation und Zertifizierung auf der Basis bekannter IT-Sicherheitsevaluationskriterien lösen lassen, sei auf [27] verwiesen: „Im Übrigen bleibt den Anwendern oft nur das diffuse – und oft irreführende – Gefühl, ein zertifiziertes Produkt oder System könne schon nicht ganz schlecht sein." Weiter wird darin ausgeführt, dass diese Maßnahmen auf Grund ihrer Vorgaben den Herstellern und Verkäufern sowie den Evaluations- und Zertifizierungsstellen und manchmal den Betreibern von Datenverarbeitungsanlagen nutzen, aber selten den Anwendern. An dieser Stelle wollen wir nun die eingangs gestellte Frage aufgreifen, wem der derzeitige Zustand der Angreifbarkeit von IT-Systemen primär nutzt, denn es gab hier in der Tat eine gewisse Verschiebung gegenüber den letzten Jahren. Ganz am Anfang war die Programmierung von Malware nur wenigen Personen möglich, die den dafür notwendigen technischen Sachverstand besaßen. Dieser Personengruppe genügte es auch oftmals, durch ein Schadprogramm auf eine Schwachstelle ohne die Intention aufmerksam zu machen, größeren Schaden anrichten zu wollen. Mit der Verfügbarkeit einfacher, auch ohne tieferen informationstechnischen Sachverstand zu bedienender Virenkonstruktionswerkzeuge trat eine zahlenmäßig wesentlich größere Gruppe auf den Plan, die die Folgen ihres Tuns oft gar nicht abschätzen konnte. Diese Gruppe sorgte in der Vergangenheit auf Grund der enormen Schäden immer wieder für spektakuläre Schlagzeilen in den Medien. Mit der Zurverfügungstellung extrem einfach zu bedienender Werkzeuge zur Modifikation und Verbreitung von Malware und dem Bekanntwerden, dass sich damit auch Geld „verdienen" lässt, traten dann auch international agierende kriminelle Banden in Erscheinung, die damit ihr Glück versuchen. Über diese Gruppen wird, aus bereits zuvor ausgeführten Gründen, meist nicht gesprochen, genauso wenig wie über industrielle Konkurrenten, Geheimdienste oder andere staatliche Überwachungsbehörden, die ebenfalls ihren Nutzen daraus ziehen. Nicht vergessen werden soll an dieser Stelle die Antivirensoftwareindustrie, die natürlich auch enorme finanzielle Gewinne aus der derzeitigen Situation erwirtschaftet und deshalb kein wirkliches Interesse an einer endgültigen Lösung des Problems haben kann.

Laut [1] erklärten einer globalen Studie zufolge 73 % aller befragten Unternehmen, dass sie bereits im Jahr 2009 Opfer von Internetangriffen wurden, wobei ein Drittel dieser Angriffe erfolgreich waren. Ferner wird darin ausgeführt, dass täglich weltweit fünfzehn Lücken in Softwareprodukten entdeckt würden, auf deren Basis jede zweite Sekunde ein neues Schadprogramm entwickelt würde und derzeit täglich 40.000 Webseiten im Internet mit Malware infiziert würden. Ferner würden bereits seit 2005 zielgerichtete Cyberspionageangriffe auf Bundesbehörden und Industrie beobachtet, von denen allerdings nur einer