
Eddy Willems
Cybergefahr
Wie wir uns gegen Cyber-Crime und Online-Terror wehren können
SACHBUCH
Springer Spektrum

Cybergefahr

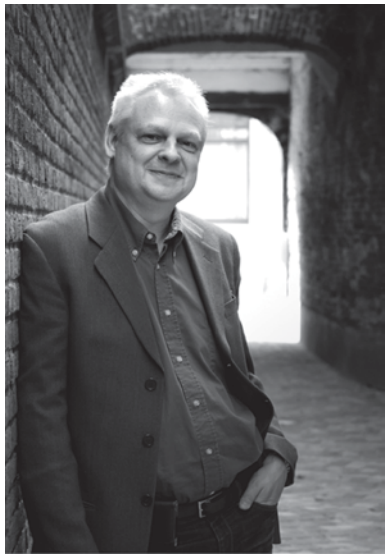

Foto: Peter Van de Kerckhove

Eddy Willems

Der belgische Malware-Experte **Eddy Willems** (1962) engagiert sich seit über 30 Jahren in den wichtigsten Organisationen zur IT-Sicherheit.

In seiner Position als Global Security Officer und Security Evangelist bei den G DATA SecurityLabs bildet er die Schnittstelle zwischen technischer Komplexität und dem Anwender. Er berät Unternehmen, hält Präsentationen und Seminare überall auf der Welt und ist gefragter Redner auf internationalen Konferenzen.

Nach seinem Informatik-Studium begann Willems seine Karriere 1984 als Systemanalyst. 1989 interessierte er sich erstmals für Computerviren und wurde 1991 Mitbegründer der EICAR, einer der ersten europäischen IT-Sicherheits-Organisationen. In den vergangenen 20 Jahren war Willems für verschiedene CERT-Organisationen, die internationale Polizei sowie für WildList und kommerzielle Unternehmen wie NOXS und Kaspersky Lab tätig. Er ist Vorstandsmitglied der AMTSO (Anti-Malware Testing Standards Organization), EICAR (European Institute for Computer Antivirus Research) und LSEC (Leaders in Security).

Eddy Willems

Cybergefahr

Wie wir uns gegen Cyber-Crime und Online-Terror wehren können

Springer Vieweg

Eddy Willems
Elewijt
Belgium

Herausgeber
Thorsten Urbanski
Bochum
Deutschland

Dieses Werk kam mit der freundlichen Unterstützung der Firma G DATA Software AG, Bochum, zustande.

Original title: Cybergevaar. Translated from the Dutch language www.lannoo.com

ISBN 978-3-658-04760-3 ISBN 978-3-658-04761-0 (eBook)
DOI 10.1007/978-3-658-04761-0

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

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Fachmedien Wiesbaden ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Danksagung

Ein Buch schreibt man nie allein. Deshalb möchte ich mich bei einigen Menschen bedanken.

An erster Stelle bei Nadine, meiner Frau. Ihr gebührt ganz besonderer Dank, denn nachdem ich bereits einige Jahre mit ihr über dieses Projekt debattiert hatte, war sie es, die den Ausschlag gab, letztendlich mit dem Buch zu beginnen. Sie war mein nicht-technischer, aber sehr aktiver Lektor, denn sie wollte jedes Detail ganz genau verstehen, weshalb ich mehrere Kapitel vollkommen neu schreiben musste. Sie traf immer genau den Punkt und wusste, womit sie mir weiterhelfen konnte.

Ich bedanke mich bei Stef Gyssels, einem guten Freund und Journalisten, der mir mit unzähligen gestalterischen Tipps unglaublich geholfen hat. Er lehrte mich, dass das Schreiben eines Buches eine ganz andere Herausforderung darstellt als das Schreiben eines Blogbeitrages oder ein Interview mit der einen oder anderen Zeitung. Ohne seine wertvollen Beiträge hätte es wahrscheinlich erheblich länger gedauert, dieses Buch zu schreiben.

Meine Geheimwaffe waren meine Kollegen der G Data: Jan Van Haver und Danielle van Leeuwen. Von ihren vielen kritischen Anmerkungen und Kommentaren habe ich enorm profitieren können. Jan, ich danke dir für die guten Tipps eines Bücherliebhabers und Danielle, dir danke ich für deine Recherchen und die detaillierten stilistischen Ergänzungen.

Besonders bedanken möchte ich mich bei meinem Kollegen und Herausgeber dieses Buches, Thorsten Urbanski, für seine wertvollen Hinweise zum deutschen Manuskript. Birgit Schöbitz und ihrem Team danke ich für die hervorragende Übersetzung.

Es fiel mir sehr schwer, mich zu entscheiden, welche Personen ich um einen Beitrag oder ihre Meinung bitten sollte. Ich habe mich auf neun Personen beschränken müssen. Daher geht mein Dank in alphabetischer Reihenfolge an: Ralf Benzmüller, Klaus Brunnstein, Bob Burls, Rainer Fahs, Richard Ford, Nikolaus Forgó, Natalya Kaspersky, Guy Kindermans und Peter Kruse.

Es wäre schön, wenn wir mit diesem Team die Welt ein wenig sicherer machen können!

Eddy Willems

Einleitung

In den vergangenen Monaten und Jahren ist uns eines immer wieder zweifelsfrei vor Augen geführt worden: Die Zeiten des unbesorgten Mailens und Surfens gehören endgültig der Vergangenheit an. Zuerst kam die PRISM-Affäre, gefolgt von der Entdeckung, dass die Vereinigten Staaten das Tun und Handeln der Vertreter der Europäischen Union im Netz in New York und Washington überwachen. Immer wieder werden wir mit der Nase darauf gestoßen: Das Netz steckt voller Gefahren und Bedrohungen. Ich möchte jeden von Ihnen – Jung und Alt, IT-ler oder Laien, Security-Fachmann oder Endverbraucher – über die möglichen Gefahren aufklären, die Ihnen online begegnen können, und Sie vor unerwünschten Folgen warnen.

Außerdem möchte ich Ihnen mit den Erkenntnissen aus meinem Buch ein Instrument bieten, mit dem Sie Gefahren vermeiden und so Schäden an PC, Smartphone oder anderen Geräten verhindern können.

Ich habe *Cybergefahr – Wie wir uns gegen Cyber-Crime und Online-Terror wehren können* in drei Teile aufgeteilt.

Im ersten Teil (Kap. 1 und 2) tauchen wir in die Geschichte ein, vom allerersten Virus bis zum Vormarsch all der Gefahren, die uns heute Tag für Tag bedrohen. In Kap. 2 widme ich meine besondere Aufmerksamkeit den Schreibern von Viren: Mit welcher Sorte Mensch haben wir es zu tun, was treibt diesen Menschenschlag an und wie gehen Antimalware-Programme mit diesen ganz besonderen Gegnern um? Dem Leser mag dies nicht besonders wichtig erscheinen, da er vor allem wissen möchte, was ihn heutzutage bedroht und wie er sich davor schützen kann. Ich bin allerdings davon überzeugt, dass es Ihnen helfen wird, die folgenden Kapitel besser zu verstehen: Sie werden viele Begriffe kennen lernen, die Ihnen später im Buch wieder begegnen werden. Sie erhalten einen tieferen Einblick in die Komplexität der heutigen Cyberwelt, die leider voller Gefahren steckt, und Sie werden verstehen, warum so viele Menschen gefesselt sind von all dem, was mit Malware zu tun hat. Mit ein wenig Glück werden Sie von diesem Virus (nein, nicht *dem* Virus) auch angesteckt.

Im zweiten Teil (Kap. 3 bis 6) steigen wir tiefer in das Thema der Cybergefahren ein: Wer sind die Akteure, was sind die Bedrohungen und wie kann man sie selbst bekämpfen? In Kap. 3 erhalten Sie einen tiefen Einblick in die Funktionsweise der „Untergrundwirtschaft" – dem Arbeits- und Betätigungsfeld der Cyberkriminellen. Das Ausmaß dieses

„Wirtschaftszweigs“, aber auch die professionelle Vorgehensweise, mit der die Kriminellen arbeiten, und das umfangreiche Angebot an geeigneten Produkten und Dienstleistungen dürften auch Sie sprachlos machen. Der Inhalt dieses Kapitels ist größtenteils das Ergebnis unterschiedlicher Studien meiner Kollegen der G DATA SecurityLabs, die sich dem Thema gewidmet haben. Ihnen gilt an dieser Stelle mein aufrichtiger Dank.

Wenn wir über Gefahren aus dem Cyberraum sprechen, darf ein Bereich nicht unter den Tisch fallen: politisch motivierte Cyberattacken. In Kap. 4 geht es somit um Cyberspionage, Cybersabotage, Terrorismus und Cyberkrieg.

Kapitel 5 ist der Antivirus-Industrie gewidmet: den Herstellern und Unternehmen, die alles daran setzen, das Internet für Nutzer sicherer zu machen. In Kap. 6 erwartet Sie eine Bestandsaufnahme: Welche Bedrohungen betrachten wir aktuell als die größte Gefahr für all diejenigen, die sich online begeben, also quasi für die halbe Welt?

Der dritte Teil dieses Buches enthält praktische Empfehlungen und Ratschläge zu allem, was Sie besser tun oder auch lassen sollten. In Kap. 7 wird zuerst mit Mythen und Missverständnissen aufgeräumt, sodass jedem klar wird, wo die echten Gefahren liegen und welche „Heilmethoden“ überhaupt nicht wirken. In Kap. 8 finden Sie dann eine ganze Reihe praktischer Tipps für jedermann, von den einfachsten Dingen („Halte deine Software auf dem aktuellen Stand“) bis zu einigen regelrechten Überraschungen („Klebe deine Webcam ab“ oder – zu einem meiner Favoriten – „Medientraining für Jedermann!“). Kapitel 9 geht mit einigen spezifischeren und manchmal auch technischen Tipps auf wirtschaftliche Aspekte ein.

Kapitel 10 und 11 beschäftigen sich damit, welche Rolle der Staat und die Medien bei der Bekämpfung dieser Gefahren spielen können und ob ihnen diese Aufgabe gelingen kann. In Kap. 12 werde ich Ihnen meine ganz eigene Vision zur „Zukunft der Malware“ erläutern, und auch, wie wir kommenden Gefahren die Stirn werden bieten können.

Als Autor habe ich meine Vision einer fernen Zukunft zu einer fiktiven Kurzgeschichte verarbeitet, in die ich verschiedene Prognosen über die Cybergefahren im Jahr 2033 eingeflochten habe.

Wer dieses Buch zu Ende liest, kann den Gefahren im Netz gut gewappnet gegenübertreten, davon bin ich überzeugt. Mein Traum ist es, durch mein Buch den Cyberkriminellen und anderen „zwielichtigen Gestalten“ im Internet das Leben ein Stück schwerer zu machen – denn: Je besser Internetnutzer über ihre Maschen informiert sind, umso schwerer werden sie zukünftig zu arglosen Cyberopfern. Es ist mir wichtig zu erfahren, ob mir dies gelungen ist und ich wünsche Ihnen viel Spaß beim Lesen. Ein guter Thriller sollte nie langatmig sein und ich hoffe doch schwer, dass mir dies gelungen ist. Ach ja, da fällt mir ein: Darf ich mich Ihnen zunächst einmal vorstellen?

Würden Sie mich bitte begleiten?

Wer schon einmal an einer organisierten Reise teilgenommen hat, weiß, wovon ich rede: Wir möchten unseren Reiseführer kennenlernen. Wer ist er, wo kommt er her und wieso entscheidet ausgerechnet er in den kommenden vierzehn Tagen, wohin die Reise geht, was wir über unser Urlaubsziel und die wunderbaren Dinge, denen wir unterwegs begegnen

werden, erfahren? Erst, wenn ich das Gefühl habe, meinen Reiseführer ein wenig kennengelernt zu haben, bin ich auch bereit, seinen Erzählungen ganz und gar zu folgen.

Aus diesem Grund halte ich es für eine gute Idee, mich Ihnen kurz vorzustellen. Denn schließlich wollen wir gemeinsam auf eine lange Reise durch die Welt der Cybergefahr gehen. Nach der Einleitung vertrauen Sie hoffentlich darauf, von dieser Reise wohlbehalten zurückzukehren. Dieses Abenteuer soll Sie fesseln und überraschen, ab und zu vielleicht sogar ein wenig schockieren, Sie aber letzten Endes klüger und vorsichtiger machen.

Meine Jugend und die Technik

Aufgewachsen bin ich in Mechelen (Belgien) als Sohn einer Unternehmerfamilie. Die Mittelschule dort war wahrscheinlich eine der ersten Schulen in Belgien, die ihre Schüler und Schülerinnen in Informatik unterrichtete. Die ersten Unterrichtseinheiten widmeten sich vorrangig einfachen Programmiersprachen wie Basic. Das war zwar nicht spektakulär, reichte aber aus, um mein Interesse zu wecken.

Nicht lange und ich verbrachte neben dem Experimentieren mit Elektronikbaukästen, Chemieprojekten und Amateurfunk (damals noch als CB oder 27 MC Funk bekannt) viel Zeit mit dem Programmieren, wobei mich sowohl der technische als auch der kommunikative Aspekt faszinierte.

1980 war Informatik ein vollkommen neues Studienfach. Die Universitäten waren noch voll und ganz damit beschäftigt, die erforderliche akademische Ausbildung umzusetzen und wussten anscheinend noch nicht so recht, wie sie damit umgehen sollten. Zuerst entschied ich mich, Computerwissenschaften an der Freien Universität Brüssel zu studieren, wechselte dann aber später zur heutigen Erasmus Hochschule. Schwerpunkt des Studiums war das Erlernen von Programmiersprachen wie Pascal, Assembler und Fortran, was für mich eigentlich mehr ein Vergnügen als Arbeit war.

Während meines Studiums arbeitete ich für das sogenannte „Freie Radio“ als technischer Mitarbeiter hinter den Kulissen – eine ausgesprochen interessante Zeit, in der ich eine Menge darüber lernte, wie wichtig eine klare und transparente Kommunikation mit einem breiten Publikum ist.

Erste Erfahrungen, erster PC

Nach meinem Abschluss fand ich sofort eine Anstellung als Programmierer bei einem Lebensmittelgroßhandel. Meine Aufgabe war es, mit Cobol auf einer großen Maschine von Bull Programme zu schreiben. Eine nette Erfahrung, aber schon bald ärgerte ich mich über die Benutzerunfreundlichkeit des Geräts: Wie bei den meisten Zentral- und Großrechnern und anderen Servern arbeitete man damals an schwarzen Bildschirmen mit grünen Zeichen. Außerdem waren diese großen Geräte vollkommen unhandlich: Man konnte sie nicht einmal mit nach Hause nehmen! Stellen Sie sich meine Begeisterung vor, als in unserer Firma der erste IBM-PC eingeführt wurde: Ein „tragbares“ Gerät, auf dem man Cobol programmieren konnte und das mit einer Festplatte mit einer Kapazität von sage und schreibe 5 MB ausgestattet war. Wie sollte die jemals voll werden, fragte ich mich damals. Ich erkannte sofort das Potenzial dieser Geräte. Es dauerte allerdings noch einige

Zeit, bis auch meine Kollegen davon überzeugt waren. Mir war schon damals klar, dass meine Zukunft quasi parallel zur Zukunft dieser Personalcomputer verlaufen würde.

1987 machte ich mich auf die Suche nach einer neuen Herausforderung und wurde bei der (damaligen) Vaderlandsche Verzekeringen (einer Tochter der Nationale Nederlanden, heute ING, ein niederländischer Bank- und Finanzdienstleister) fündig. Dort bot sich mir die Möglichkeit, meine beiden größten Leidenschaften zu vereinen: Als Mitarbeiter am Helpdesk hatte ich die tolle Aufgabe, Anwendern bei der Lösung ihrer Probleme zu helfen, durfte aber auch Software entwickeln, um die Funktion des Helpdesk zu verbessern. Zugleich bekamen wir die Möglichkeit, Selbststudien durchzuführen und neue Programme zu testen, was ich dankbar nutzte, um mein Software-Wissen zu erweitern.

1989 sollte ich die Nutzbarkeit eines Programms für unser Unternehmen prüfen, eine Aufgabe, die durchaus öfter vorkam. Ich bekam also eine Diskette, der ein Informatikbüchlein beigefügt war, in die Hand gedrückt. Mit dem darauf gespeicherten Programm sollte man angeblich feststellen können, ob man zur Risikogruppe der Personen gehörte, die an AIDS erkranken könnten. Die Software erwies sich als totaler Reinfall und ich fand es sehr ärgerlich, dass so etwas überhaupt getestet werden sollte.

Am nächsten Tag brach das Chaos in meinem Büro aus. Ich startete meinen PC und es passierte nichts, rein gar nichts. Auf dem Bildschirm wurde lediglich ein Fenster mit der Aufforderung angezeigt, dass ich Geld auf ein bestimmtes Konto überweisen solle. Ich startete den PC erneut, woraufhin sich gar nichts mehr tat. Ich ging von einem Bug aus. Ich startete den PC über die Systemdiskette und sah sofort, wo der „Fehler" lag: Der Pfad war verändert und verschlüsselt worden. Ohne dass es mir in diesem Moment bewusst wurde, hatte ich soeben Bekanntschaft mit der ersten „Ransomware" gemacht, also mit Schadprogrammen, die entwickelt wurden, um einen PC zu „kidnappen" und erst nach Zahlung des Lösegeldes wieder freizugeben. Doch mir gelang es, das Problem nach einigen Minuten zu beheben und dann ungehindert weiterzuarbeiten.

Wirklich überrascht war ich, als ich zwei Tage später während einer Sendung des nationalen Wirtschaftssenders VTM hörte, dass diese Ransomware sich unkontrolliert verbreiten würde und „kein einziges Unternehmen bislang eine Lösung hätte". Wie bitte? Kein einziges Unternehmen? Aber ich hatte das Problem gestern doch gelöst. Kurzerhand rief ich beim VTM-Journal an und erzählte von meinem Erfolg, der mir ohne größere Anstrengung gelungen war. Schon am nächsten Tag standen zwei Kamerateams vor meiner Tür und die Aufnahme wurde am selben Abend ausgestrahlt.

Der Malware-Zug war abgefahren

Um in der Terminologie der Malware zu bleiben: das Virus hatte mich infiziert. Mir wurde schlagartig klar, dass sich mir hier die Riesenchance auftat, das zu tun, was ich immer tun wollte: Computerviren aufzuspüren und zu analysieren und ein geeignetes Gegenmittel zu entwickeln. Ich fing an, über die entsprechenden Bulletinboards nach den Experten und Unternehmen zu forschen, die sich mit Viren beschäftigten. Auf diese Weise stieß ich unweigerlich auf Namen wie McAfee und Dr. Solomon, aber auch auf interessante Persönlichkeiten wie Dr. Sarah Gordon (siehe Kap. 2.7).

1991 wurde ich zu einer Konferenz rund um das Thema Virenbekämpfung nach Brüssel eingeladen. An diesem Ort versammelten sich alle bedeutenden Persönlichkeiten aus der ganzen Welt: Dr. Solomon höchstpersönlich, Vesselin Bontchev und viele andere. Ich war mir sicher: Dies würde mehr als nur ein Hobby werden, das war nicht mehr und nicht weniger als meine berufliche Zukunft. Während der Konferenz wurde auch EICAR[1] gegründet und so kam es, dass ich mich heute stolz als Gründungsmitglied dieser Organisation bezeichnen darf.

Glücklicherweise schätzte man bei De Vaderlandsche mein Interesse für Viren und meine Erfahrungen als Programmierer, sodass meine Leidenschaft für dieses Thema auch im Beruf von Nutzen war. Inzwischen wurden Bulletinboards von E-Mails und Webseiten abgelöst. Auch wenn dies zu Beginn alles andere als einfach war: Nachdem ich endlich die richtige Software zum Browsen gefunden hatte – und sie nach einem stundenlangen Kampf korrekt konfiguriert hatte – war ich endlich am Ziel und konnte surfen … um sogleich zu entdecken, dass online noch gähnende Leere herrschte!

Über Viren und andere Formen der Malware gab es damals im Netz absolut nichts zu finden. Selbst Firmen wie McAfee waren 1994 online noch nicht vertreten. Und so beschloss ich kurzerhand eine eigene Internetseite mit Informationen zu Viren & Co. ins Netz zu stellen: www.wavci.com. Auf dieser Webseite fanden Besucher zudem eine Vielzahl von weiterführenden Links zu IT-Security-Seiten. Mein Ziel war es, eine Art Antiviren-Enzyklopädie anzulegen. Dieses Projekt erregte umgehend die Aufmerksamkeit vieler Sicherheitsexperten. In kürzester Zeit erhielt ich eine Vielzahl von Einladungen zu IT-Veranstaltungen – unter anderem zur Virus Bulletin Conference in Brighton 1996. Dort lernte ich Harry De Smedt kennen. Harry war Manager bei der Data Alert, der Abteilung der Unit 4, die sich auf Sicherheitssoftware spezialisiert hatte: Data Alert vertrieb Dr. Solomon's Antivirus Toolkit, seinerzeit eines der renommiertesten Antivirenprogramme. Harry De Smedt kannte mich durch meine Aktivitäten im Netz bereits relativ gut und bevor ich mich versah, bekam ich auch schon ein Jobangebot.

So trat ich am 1. Januar 1997 bei dem damaligen Lieferanten für Sicherheitsdienstleistungen Data Alert meine neue Stelle an. Seitdem habe ich an fast allen Antiviren-Konferenzen teilgenommen. Allerdings steht bei mir eine Veranstaltung nach wie vor ganz oben auf der Liste: die Virus Bulletin! Hier trifft sich alles, was Rang und Namen hat, und für mich gibt es keinen besseren Ort, um sich zu informieren und sein Netzwerk zu erweitern. Auch die Konferenzen von EICAR und CARO[2] sind absolut empfehlenswert. Müsste ich mich auf wenige Konferenzen im Jahr beschränken, so wären es diese drei.

Aus der Data Alert ging nach einigen Jahren (und Übernahmen) die NOXS, der Sicherheitspfeiler innerhalb der Unit 4 Agresso hervor, die unter dem Namen UNIT4 noch immer zu einem der wichtigsten IT-Lieferanten auf dem Markt gehört. Zufall oder nicht, während dieser Jahre durfte ich die größten Persönlichkeiten der Antiviruswelt kennen lernen: Sarah Gordon, Righard Zwienenberg, Dr. Solomon, Mikko Hyppönen und andere.

[1] European Institute for Anti-Virus Research (s. Kap. 5.2.2).

[2] Computer Anti-Virus Research Organisation (s. Kap. 5.2.1).

Und ich wurde Mitglied des Vforum, einer exklusiven Community aus Virenexperten, in die man nur auf Einladung aufgenommen wird. Alle Größen meiner Branche sind dort vertreten.

Die Antivirus-Community ist eine sehr eng verbundene Gruppe, denn Antivirus-Lieferanten sind sehr solidarische Leute, die ihr Wissen über Malware gerne teilen. Auch ich setzte mich mit aller Kraft dafür ein, Viren zu analysieren, schon allein deshalb, weil ich dadurch bei etlichen Unternehmen Malware aufspüren konnte.

Meine Aufgabe innerhalb der NOXS lag vor allem in der Forschung, Beratung und Kundenschulung. NOXS, die später in die Westcon Security überging, entwickelte sich zu einem großen Unternehmen und genoss einen hervorragenden Ruf. Ich wurde bei mehr als tausend Unternehmen eingesetzt, von ganz kleinen Firmen bis zu den ganz großen Konzernen, auch Ministerien und Behörden gehörten zu meinen Kunden. Für Projekte im Ausland was ich ebenfalls zuständig (mehr dazu unter „Kein Problem in Saudi-Arabien" am Ende dieses Kapitels). Gab es doch mal ein Problem, bei dem ich nicht weiter wusste, zückte ich einfach mein „rotes Büchlein", das die Kontaktdaten zahlreicher Kollegen enthielt, die bei den größten Softwareherstellern tätig waren und mir mit Rat und Tat Tag und Nacht zur Verfügung standen. Das „menschliche" Netzwerk ist in der Welt der Cyber-Sicherheit mindestens ebenso wichtig wie alles Wissenswerte über Malware.

Im Jahr 2000, zu Zeiten des „Love letter"-Virus, beschloss der belgische Minister für Telekommunikation, Rik Daems, eine Art Antimalware-Netz zu gründen, und zwar „in enger Zusammenarbeit mit der Bevölkerung". Als ich diese Meldung abends im Fernsehen hörte, traute ich meinen Ohren nicht. Weshalb wurde von einer engen Beteiligung des belgischen Volkes gesprochen, obwohl meines Wissens kein einziger Belgier konsultiert worden war? Mit dieser Wut im Bauch wandte ich mich ein weiteres Mal an VTM, die sehr empfänglich für meine Kritik waren, was nicht nur zu meinem zweiten Auftritt in dem Sender führte, sondern auch zu einer konkreten Zusammenarbeit mit der belgischen Regierung. Ich arbeitete an dem Netz des Ministeriums, das für die Malwarebekämpfung zuständig war, einem Vorgänger des heutigen Computer Emergency Response Teams (CERT). Zu Beginn dieses Projekts gab es hin und wieder Warnungen vor gefährlichen Viren und anderen Computerbedrohungen über die öffentlichen Radiosender, gewissermaßen digitale Verkehrsnachrichten: „Wir bitten Sie um Vorsicht: Es gibt einen neuen Virus…". Niemand wollte Panik verbreiten, aber Vorsicht war durchaus geboten. Das gilt übrigens auch heute noch.

In dieser Zeit trat ich gelegentlich als offizieller Sprecher der Gruppe auf und gab zahlreiche Interviews. Außerdem fungierte ich als Berater für Computerschädlinge: War der Virus gefährlich oder ein Hoax (siehe Kap. 8.16), musste die Bevölkerung gewarnt werden? Ich muss sagen, wir waren sehr aktiv damals, und viel engagierter als das heutige CERT in Belgien.

Meine Jahre als Evangelist

NOXS bildete jahrelang ein starkes Team an Sicherheitsexperten, von denen die meisten auch heute noch hohe Positionen in der Sicherheitswelt innehaben. Es war mir ein beson-

deres Vergnügen, in diesem Team über Jahre hinweg gegen Cyberkriminalität zu kämpfen. Doch jede Geschichte, so schön sie auch sein mag, hat mal ein Ende.

Ende 2007 wechselte ich zu den Kaspersky Labs, einem bekannten Hersteller von Antimalware-Software. Ich hatte mich für den Jobwechsel entschieden, weil ich dort nicht nur in der Forschung eingesetzt wurde, sondern als „Antimalware-Botschafter" Menschen über Cybergefahren aufklären durfte. So wurde ich ein Kaspersky-Evangelist und Teil des Kaspersky-Expertenteams. Ich wusste genau, woran die Mitbewerber scheiterten und konnte zugleich die breite Öffentlichkeit auf die Bedeutung von IT-Sicherheit hinweisen. Diese Aufgabe war ganz nach meinem Geschmack.

Einige Jahre später bot sich mir die Chance, beim deutschen Antivirus-Unternehmen G DATA Software AG einzusteigen. Dieses Angebot konnte und wollte ich nicht ablehnen, denn es war eine hervorragende Gelegenheit, noch mehr dazuzulernen und den Finger am Puls der Zeit zu haben. So wagte ich Anfang 2010 den Wechsel – eine Entscheidung, die ich nicht einen Moment bereut habe. Hier herrscht trotz der harten Arbeit ein fantastisches Arbeitsklima und es wird viel miteinander gelacht.

Seit März 2001 sitze ich im Vorstand der Antivirus-Organisation EICAR und bekleide dort den Posten des Director Security Industry Relationships. Aufgrund meiner Tätigkeit für EICAR und AMTSO (einem weltweiten IT-Sicherheitsunternehmen, dem ich mich ebenso wie der EICAR in einem späteren Kapitel ausführlich widmen werde) einerseits und meinem Job bei G DATA andererseits habe ich für mich alles erreicht, was ich mir für meine Karriere immer als Ziel gesetzt hatte. Ich genieße einen großen Spielraum auf technischer Ebene, aber auch den Freiraum auf der menschlichen Seite und nicht zuletzt die ganz persönliche Erkenntnis, dass ich mit meiner Arbeit Menschen helfen kann. Mein größter Wunsch ist es daher, dass Ihnen dieses Buch helfen und viel Ärger ersparen wird.

Haftungsausschluss

Eines noch, bevor wir tiefer in die Materie eintauchen. Obwohl ich schon seit vielen Jahren international tätig bin, können doch einzelne Beispiele oder Anekdoten „belgisch" eingefärbt sein. Natürlich schildere ich Beispiele, die auch für Leser aus anderen Ländern relevant sind. Ausgangspunkt war immer mein Gedanke: Was interessiert den Leser eines Buches über Cybergefahren? Und zwar unabhängig von seiner Nationalität oder seinem Wohnort.

Gleiches gilt für Grafiken, Schemata und Zahlen, die in dieses Buch eingeflossen sind. Zu meinem Glück stehen mir durch G DATA eine Vielzahl relevanter Daten und Statistiken zur Verfügung. Dies ermöglicht mir, die aktuelle Gefahrenlage zu jedem Zeitpunkt richtig einzuschätzen und zu bewerten.

So, genug des Vorspanns – nun werden wir gemeinsam die fesselnde Welt der Cybergefahren betreten. Folgen Sie den Wegweisern, passen Sie gut auf, und verirren Sie sich bloß nicht… denn hinter jeder Ecke lauern Gefahren.

Aus dem Tagebuch
„Kein Problem in Saudi-Arabien“
Oktober 2001

Mitunter geraten wir von einer Minute zur anderen in Situationen, die unser Leben auf den Kopf stellen. Unmittelbar nach den Anschlägen vom 11. September war es für Amerikaner relativ kompliziert, in arabische Länder zu reisen, und Unternehmen wie McAfee fanden kaum Leute, die bereit waren, in diesen Regionen Aufträge zu übernehmen. So machten sich zahllose Firmen auf die Suche nach Europäern, die kompetent und abenteuerlustig – oder aus Sicht von so manchem verrückt – genug waren, diese Aufgaben zu übernehmen. Richtig, ich spreche von Männern wie mir. Ich flog also nach Saudi Arabien, um Saudi Aramco, die weltweit größte Mineralölgesellschaft, im Rahmen ihrer Sicherheitsprojekte zu betreuen.

Nach einem langen Flug landete ich abends gegen halb elf mit dem sicheren Gefühl, dass dies noch ein langer Abend werden würde. Schon das Warten an der Passkontrolle dauerte eine gefühlte Ewigkeit. Doch dann wurde ich aufgefordert, mich an einer kürzeren Schlange anzustellen. Was für ein Glück, dachte ich noch, bis ich an der Reihe war. Meine Notebook-Tasche wurde einer umfangreichen Untersuchung unterzogen und der Blick eines Zollbeamten fiel auf einen Stapel Disketten, die ich in meiner Tasche verstaut hatte. Auf diesen Disketten befanden sich einige erst kürzlich „gefangene“ Viren. Der Beamte vermutete allerdings Pornos oder andere illegale Daten und konfiszierte die Disketten wie auch meinen Pass. Obwohl ich eindringlich davor warnte, dass das Laden dieser Disketten zu einer Infizierung ihrer Systeme führen könnte, ließen sich die Zollbeamten nicht davon abbringen, die Disketten genauer zu untersuchen. Jede meiner Warnungen wurde mit einem knappen „*Kein Problem, Sir*“, kommentiert, sprich geflissentlich ignoriert. Ich konnte erkennen, wie die Warnhinweise auf den Bildschirmen einander in rasantem Tempo folgten, von einem Virenscanner fehlte jede Spur. Etwas später durfte ich den Flughafen samt Pass und Disketten verlassen. Ob diese Beamten danach immer noch „*kein Problem*“ hatten, wage ich ernsthaft zu bezweifeln.

Als ich damals einen Artikel über diesen Zwischenfall für die Fachzeitschrift *Virus Bulletin* verfasste, ließ ich die Frage, ob das Computersystem des Flughafens nun tatsächlich mit meinen Viren infiziert worden war, bewusst unbeantwortet. Eigentlich aber wusste ich das mit absoluter Sicherheit, und nur einige Tage später kam die offizielle Bestätigung, als ich in der Zeitung las, dass der arabische Flughafen Opfer eines schweren Virenangriffs geworden sei. Für mich eine eher ungewöhnliche Premiere, denn normalerweise bin ich Teil der Lösung, doch in diesem Fall war ich Teil des Problems. *Wie gesagt, „Kein Problem, Sir“ dürfte die Untertreibung des Jahres gewesen sein.*

Inhaltsverzeichnis

Dreißig Jahre Malware – ein kurzer Abriss

1

Vorab eine Warnung: Menschen mit lebhafter Fantasie könnten dieses Kapitel als ziemlich unangenehm empfinden. Denn es wimmelt von Viren, Würmern und anderen ungebetenen Gästen wie Trojanern. Und trotzdem sollten Sie sich mit den verschiedenen Formen der Malware, mit der unerwünschten Software in Ihrem System und auf Ihrer Festplatte, auseinandersetzen. Als kleine Entschädigung erfahren Sie Interessantes über Anna Kurnikova und kommen sogar in den Genuss einer Liebeserklärung.

Zunächst möchte ich Ihnen noch ein paar der wichtigsten Begriffe erklären, die zuhauf in diesem Buch vorkommen, auch auf die Gefahr hin, dass Sie sie alle kennen.

1.1 Was ist Malware?

Malware (die allgemeine Abkürzung für *Malicious Software*) ist ein Sammelbegriff für alle Arten an Software, die in böser Absicht geschrieben wurde. Viren, Würmer, Trojaner, Spyware und alle anderen Formen bösartiger und möglichst schädlicher Software fallen unter den Oberbegriff der „Malware“. Interessant ist übrigens, dass dieser Begriff erst viele Jahre nach dem Auftauchen der ersten Viren und Würmer erfunden wurde, als es innerhalb kürzester Zeit so unglaublich viele Typen an Schadsoftware gab, dass man einen Begriff finden musste, um alle unter einen Hut zu bekommen.

1.2 Was ist ein Virus?

In der Biologie ist ein Virus ein Organismus, der sich in einem Wirt einnistet, zum Beispiel im menschlichen Körper, sich in diesem ausbreitet und oftmals sogar den Tod des Wirts zur Folge hat. Ein *Computervirus* wird so genannt, weil er im Prinzip genau dasselbe

E. Willems, *Cybergefahr,* DOI 10.1007/978-3-658-04761-0_1

macht. Es handelt sich um ein Computerprogramm, das sich in eine Datei einnisten kann und somit auch in das Betriebssystem selbst. Im günstigsten Fall nimmt es nur Speicherplatz in Beschlag und drosselt die Rechnerleistung. Im ungünstigsten Fall aber richtet der Virus so großen Schaden an einem PC an, dass dieser komplett unbrauchbar wird. Bei einem solchen Angriff können viele Daten unwiederbringlich verloren gehen, im schlimmsten Fall sogar alle Daten der Festplatte.

Heutzutage gehen Viren auf einem Computer anders vor. Meistens werden Dateien installiert, über die Kriminelle den PC ferngesteuert für ihre üblen Machenschaften nutzen können. Darauf werden wir in den nächsten Kapiteln noch genauer eingehen.

Ein sogenannter *Wurm* ist eine andere Form von Malware. Auch hier wird eine Datei auf dem Computer installiert, die versucht, sich auf anderen Computern auszubreiten. Ein Virus zielt vor allem darauf ab, sich in einen PC einzunisten, während ein Wurm sich vielmehr so weit wie möglich verbreiten möchte.

Auch die *Spyware* ist eine üble Form von Malware, die mittlerweile immer öfter zum Einsatz kommt. Spyware versteckt sich in einem PC und verfolgt die gesamten Aktivitäten des Benutzers. Vor allem das Surfverhalten wird registriert und später an Dritte verkauft. Aber auch *Keylogger*, die registrieren, was über die Tastatur eingegeben wird, sind eine Form von Spyware.

Zum Schluss noch ein absoluter „Leckerbissen“: das Trojanische Pferd, kurz: der *Trojaner*. Sie kennen sicherlich das Trojanische Pferd aus der griechischen Mythologie. Nach langer Belagerung von Troja beschließen die griechischen Krieger, ihren Feind durch eine List zu besiegen und schenken den Trojanern ein riesiges Holzpferd als scheinbare Versöhnungsgabe. Die Trojaner nehmen das Geschenk freudig an, weil sie der Überzeugung sind, der Krieg sei damit vorbei. Aber in der Nacht klettern aus diesem Pferd einige Griechen, die sich darin versteckt hatten, und öffnen die Tore von Troja, sodass die Griechen letzten Endes ungehindert hinter die Schutzmauern gelangen und nach Troja einmarschieren können. Ein *Trojaner* im PC geht genauso vor. Sie können sich also denken, was er anrichten kann. Sobald er sich in einem System eingenistet hat, öffnet er die Tore für Kriminelle, die dann ungehindert den befallenen PC für ihre Zwecke nutzen können. Der Unterschied ist, dass es sich hier nicht um ein Tor im eigentlichen Sinne handelt, sondern vielmehr um eine Art Hintertür, denn oftmals merkt der Nutzer gar nichts davon. Es kann lange dauern, bis der Schaden bemerkt wird. Heutzutage entstehen immer mehr *Trojaner* in den unterschiedlichsten Formen. Sie sorgen dafür, dass ein PC in ein Botnetz integriert werden kann. Auch darauf komme ich im weiteren Verlauf des Buches noch einmal zurück (siehe Kap. 1.4). Es gibt einen großen Unterschied zwischen Viren, Würmern und Trojanern: Letztere verbreiten sich nicht automatisch auf andere Rechner.

► **Achtung** Einen Computervirus in Umlauf zu bringen, stellt fast weltweit eine Straftat dar. Sollten Sie trotzdem einmal mit einem Computervirus experimentieren wollen: Ich habe Sie gewarnt!

1.3 Die erste Generation

Experten sind sich nicht einig, was denn nun der erste Virus war. Für die einen ist es der *Elk Cloner* aus dem Jahr 1982, andere meinen, es sei der Wurm *Creeper* gewesen, ein experimentelles Computerprogramm von 1971. Die meisten Fachleute halten den *Brain*-Virus von 1986 für den ersten Übeltäter. Sowohl der Elk Cloner als auch der Creeper entsprechen mehr oder weniger der Definition eines Virus, die von dem Wissenschaftler Frederick Cohen 1983 festgelegt und später für allgemein gültig erklärt wurde. Allerdings hat er diese Definition erst im Jahre 1983 zu Papier gebracht, ebenso wie übrigens auch den Begriff des „Virus". Das ist einer der Gründe dafür, warum der Elk Cloner lange Zeit nicht allgemein als Virus galt – bei so manchem ist das noch immer so. Ein anderer Grund dürfte sein, dass es einige Jahre relativ ruhig an der Virenfront war und das aktive Virenzeitalter erst mit dem Erscheinen des Brain eingeläutet wurde. Beide Standpunkte haben ihre Berechtigung, Fakt jedoch ist, dass Brain der erste (PC-) Virus war, der aufgetreten ist, nachdem Cohen diesen Begriff eingeführt hatte.

Hätten Sie's gewusst … ?

Jahrelang sah die Apple-Fangemeinde auf die Windows-Plattform herab, weil fast alle Viren auf Windows zu finden waren, weshalb aus ihrer Sicht Windows die Quelle allen Übels war. Doch Elk Cloner, der erste „virus avant la lettre" wurde speziell für MacOS geschrieben und war daher nur auf Apple Computern zu finden. Daher gilt: Kein System ist eine Insel – auch nicht MacOs!

Brain dürfte übrigens zwar der erste Virus gewesen sein, sicher aber nicht der schnellste. Kein Wunder, denn damals gab es kein superschnelles Internet, das der Virus hätte nutzen können. Seine Ausbreitung erfolgte über Floppy-Disks, das heißt, entscheidend war, wie schnell eine infizierte Diskette von einem PC zum anderen gelangte. Damals konnte man die Quelle eines Virus noch ermitteln, zumindest wenn man wusste, wo man zu suchen hatte. Über die Floppy-Disk gelangte der Virus in den Bootsektor (das Startprogramm) des Computers und von dort auf eine neue, in den PC geschobene Diskette. „Floppy-Disk" war übrigens noch wortwörtlich zu verstehen: eine „wabbelige" Scheibe mit einem Durchmesser von rund dreizehn Zentimetern (51/4 Inch), auf der im günstigsten Fall ein gutes Megabyte gespeichert werden konnte.

► **Bootsektor** Wenn in der Antiviren-Industrie oder dem Rest der IT-Welt vom Bootsektor die Rede ist, geht es mit Sicherheit nicht um die Schifffahrt oder einen Yachthafen. *„To boot"* heißt übersetzt „starten" und der Bootsektor ist somit der Teil einer Diskette oder (Partition) einer Festplatte, der angesprochen wird, um einen PC zu starten, und zwar mit allen Instruktionen für das Startverfahren.