

Alfred Krüger

Angriffe aus dem Netz

Die neue Szene des
digitalen Verbrechens



Alfred Krüger
E-Mail: akrue@t-online.de

Reihenherausgeber: Florian Rötzer, München, fr@heise.de

Copy-Editing und Lektorat: Susanne Rudi, Heidelberg
Satz & Herstellung: Birgit Bäuerlein
Umschlaggestaltung: Hannes Fuß, www.exclam.de
Druck und Bindung: Koninklijke Wöhrmann B.V., Zutphen, Niederlande

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

ISBN 3-936931-27-5
1. Auflage 2006
Copyright © 2006 Heise Zeitschriften Verlag GmbH & Co KG, Hannover

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten.
Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche
Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für
die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Alle Informationen in diesem Buch wurden mit größter Sorgfalt kontrolliert.

Weder Herausgeber, Autor noch Verlag können jedoch für Schäden haftbar gemacht
werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

Botnetze statt Baseballschläger

Ein Vorwort

Willkommen im digitalen Horrorladen World Wide Web! Hier wird gelogen und betrogen. Kriminelle, Abzocker und Cyberterroristen haben das Ruder übernommen. Spammer blockieren den Emailverkehr. Identitätsdiebe phishen die persönlichen Daten ihrer Online-Opfer ab. Online-Banking wird zum russischen Roulette, das nur einen einzigen Gewinner kennt: den Cyberkriminellen. Immer neue Viren, Würmer und Trojaner verschmutzen immer schneller das digitale Netz. Licht am Ende dieses kriminellen Cybertunnels ist nirgendwo in Sicht.

So weit das gängige Klischee, an dem vor allem jene Branche, die ihren Kunden Sicherheit im Internet verkaufen will, genüsslich strickt.

Russen-Mafia und Cosa Nostra stehen längst Gewehr bei Fuß, berichtet etwa die US-Sicherheitsfirma McAfee in ihrem Report über »Virtuelle Kriminalität in Europa«. Das organisierte Verbrechen hat Blut geleckt und bedient sich jener neuen Waffen, die das Internet zu bieten hat. Traditionelle Delikte wie Schutzgelderpressung erleben einen Aufschwung. Die Täter haben die althergebrachten Waffen zur Einschüchterung ihrer Opfer durch die digitalen Waffen des Internets ersetzt. Baseballschläger sind out – Botnetze sind in. Diese Netze bestehen aus Tausenden gleichgeschalteter Privatrechner, die durch Schadprogramme zu fernsteuerbaren Zombie-PCs umfunktioniert werden. Sie belagern auf Kommando jeden Server dieser Welt und bombardieren ihn so lange mit sinnlosen Anfragen, bis er überlastet abstürzt. Der Spuk ist erst vorbei, wenn die erpresste Online-Firma zahlt. So weit eines der Szenarien, die McAfee im Report zur aktuellen Lage an der europäischen Verbrechensfront entwirft.

Es kann jeden treffen, auch den deutschen Durchschnittsnutzer, meint McAfee und belegt diese Behauptung mit der bundesdeutschen Kriminalstatistik. »In Deutschland hat sich die Zahl der gemeldeten Computerverbrechen von ca. 15.000 im Jahr 1993 auf 60.000 im Jahr 2003 vervierfacht«, hat die US-Firma mit Sitz im kalifornischen Santa Clara nach offenbar intensiver Recherche herausgefunden.¹ Diese Zahlen haben einen kleinen, aber feinen

Schönheitsfehler: Mit den grandios entworfenen Bedrohungsszenarien, mit Cyberkrieg und Online-Verbrechen, mit virtueller Erpressung und organisierter Internetkriminalität haben sie kaum etwas zu tun.

Die Mehrzahl aller Straftaten, die im Jahr 2004 von der polizeilichen Kriminalstatistik unter Computerkriminalität einsortiert wurden, stammt aus der Welt der »Offline«-Kriminalität. In rund 36.000 Fällen ging es um Geldautomatenbetrug mit PIN-geschützten Geldkarten, in ca. 14.000 Fällen um Computerbetrug im Sinne des § 263a Strafgesetzbuch: Abrechnungsmanipulationen bei der betrieblichen Gehalts- und Rechnungszahlung sowie Bilanz- und Kontostandsmanipulationen – Straftaten, die eher selten von betriebsfremden kriminellen Hackern, umso häufiger jedoch von Mitarbeitern der betroffenen Firmen begangen werden. Alles in allem zeichnet die bundesdeutsche Kriminalstatistik ein vergleichsweise unspektakuläres Bild, das kaum geeignet ist, cyberkriminelle Bedrohungsszenarien stichhaltig mit Zahlen zu untermauern.

Entwarnung also auf der ganzen Linie? Keineswegs! Erstens sind die Kategorien der polizeilichen Kriminalstatistik veraltet. Das »Tatmittel« Internet wird nicht gesondert erfasst. Zweitens liefert jede Kriminalstatistik nur einen Ausschnitt des tatsächlichen Geschehens. Sie enthält nur die »erfassten Straftaten« und sagt nichts über jene Fälle aus, die im Dunkeln bleiben. Drittens schließlich zeigt bereits der Blick ins eigene Emailpostfach, dass Entwarnung völlig fehl am Platze ist. Phishing-Mails werden in immer neuen Varianten auf den Markt geworfen, die Spamlawine rollt, und aggressive Emailwürmer schlängeln sich durchs Internet.

Wer schreibt solche Schadprogramme und warum? Mit welchen Mitteln werden sie verbreitet? Wer pustet Phishing-Mails und Spam ins Internet? Wie arbeiten digitale Nepper, Schlepper, Bauernfänger? Wer spioniert den Nutzer mit welchen Mitteln aus? Dieses Buch wagt einen Blick hinter die Kulissen der cyberkriminellen Szene. Es seziert spektakuläre Einzelfälle, analysiert den kriminellen Netzalltag und beschreibt an ausgewählten Beispielen cyberkriminelle Machenschaften, Methoden und Motive.

Kriminelle Handlungen werden nicht begangen, weil sie technisch machbar, sondern weil sie profitabel sind. Kriminalität im Internet wird in diesem Buch nicht als technisches, sondern vorrangig als soziales Phänomen behandelt. eCommerce und Online-Banking boomen. Internetkriminalität wird deshalb als Begleiterscheinung dieses Booms verstanden. Internetkriminelle und halbseidene Datenschnüffler sind die Trittbrettfahrer einer breiten Kommerzialisierung des digitalen Einkaufsladens World Wide Web. Sie bedienen sich der Mittel, die das Internet zu bieten hat, und nutzen sie konsequent für ihre Zwecke.

1) http://www.mcafee.com/de/local_content/brochures/studie_virtuelle_kriminalitaet.pdf, S. 7.

Dieses Buch zeigt auf, wie gängige Formen von Internetkriminalität funktionieren. Es beschreibt, wie das Medium Internet nicht nur den Raum schafft, in dem Straftaten stattfinden, sondern wie es auch die Art und Weise bestimmt, in der kriminelle Handlungen geplant und durchgeführt werden. Ins Visier geraten dabei zwangsläufig auch jene halbseidenen Unternehmen mit bemüht legalem Anstrich, die ihren Heißhunger auf die Daten ihrer Kunden mit so genannter Spy- und Adware stillen wollen – ein Datenhunger, der auch die etablierte Softwarebranche plagt. Die Unternehmen dieser Branche wollen nur das Beste – die Daten ihrer Kunden –, und die Lizenz zum Schnüffeln erteilen sie sich selbst mit ihren »kleingedruckten« Geschäfts- oder Lizenzbedingungen. In der Theorie setzen sie dabei auf den mündigen Nutzer, der sich der Konsequenzen eines jeden Mausklicks stets bewusst ist. Wie sie ihn in der Praxis entmündigen, zeigt dieses Buch.

Dieses Vorwort wäre unvollständig ohne ein paar Dankesworte: Mein Dank gilt zunächst meiner Frau Edeltraud, die meine wechselnden Stimmungen erdulden musste und mir sämtliche Sinn-, Relevanz- und Zeitkrisen ausgeduldet hat. Danke auch an meine Töchter Anne und Amelie, denen ich mit meinen endlosen Monologen über Botnetze, DDoS-Angriffe und Datenspionage manchmal den letzten Nerv geraubt habe. Ein besonderes Dankeschön geht an Volker Heil von der EDV-Schule Heil in Fulda. Volker hat meine »tausend« Emails mit technischen Fragen geduldig gelesen und immer sachkompetent beantwortet. Danke auch an Denny Koch für seine kreativen Ideen zur Umschlaggestaltung. Last but not least geht mein Dank an Florian Rötzer von Telepolis für das in mich gesetzte Vertrauen.

Alfred Krüger

Göttingen, im Februar 2006