
DIETER KOCHHEIM
CYBERCRIME
MALWARE
SOCIAL ENGINEERING
UNDERGROUND ECONOMY

Die Zitate in den Fußnoten, das Inhaltsverzeichnis und einzelne Textpassagen sind im PDF-Dokument mit Links unterlegt, die einen einfachen Zugriff auf die Quellen oder eine Bewegung im Dokument zulassen. Sie erscheinen in blauer Farbe. In ausgedruckter Form sind die Quellen leider nicht sichtbar.

Thema: **Cybercrime**
Autor: Dieter Kochheim
Version: 1.02
Stand: 24.05.2010
Cover: Kochheim

Impressum: **CF**, cyberfahnder.de

Einführung: Cybercrime

Das IT-Strafrecht im engeren Sinne umfasst die Straftaten, die die Informations- und Kommunikationstechnik direkt betreffen. Als ihre Hauptgruppen sehe ich, leicht abweichend von der üblichen Klassifikation an:

⇨ die Computersabotage,
⇨ der persönliche Lebens- und Geheimbereich,
⇨ die strafbaren Vorbereitungshandlungen und
⇨ den Schutz des Rechtsverkehrs.

Hinzu kommt das IT-Strafrecht im weiteren Sinne. Es umfasst die klassische Kriminalität, die sich zu ihrer Begehung der IKT bedient. Dazu gehören ganz besonders der Betrug und die Äußerungsdelikte (Beleidigung, Verleumdung, Bloßstellung). Als ihre Hauptgruppen sehe ich an:

⇨ das Nebenstrafrecht,
⇨ die Inhaltsdelikte und
⇨ den Anlagenschutz.

In diesem Arbeitspapier geht es jedoch nicht um die Einzelheiten der rechtlichen Beurteilung der Cybercrime, sondern um ihre Erscheinungs- und Organisationsformen. Es ist eine Bestandsaufnahme, die den Blick auf die moderne Kriminalität schärfen soll, und soll eine Grundlage dafür schaffen, die Probleme im Einzelfall einzugrenzen und Lösungswege zu finden.

Die Cybercrime ist ein zentrales Thema des ▸ Cyberfahnders. Schon 2007 befasste er sich mit dem Phishing in der damals praktizierten Form, die zunächst nur die Kontaktaufnahme zu den Finanzagenten und schließlich zu den Bankkunden, deren Kontozugangsdaten ausgespäht werden sollten, per Spam-Mail kannte [1]. Die Methoden des Identitätsdiebstahls und seiner besonderen Erscheinungsform des Phishings (password stealer) haben sich binnen kurzer Zeit geändert und vor Allem verfeinert und professionalisiert [2].

Zunächst widmete sich der Cyberfahnder den Grundlagen und beschrieb dazu die möglichen Angriffspunkte bei vernetzten Computern [3] und den wichtigsten Teilaspekten der Cybercrime. Das gilt vor Allem für den hier erstmals veröffentlichten Beitrag über den ▸ Identitätsdiebstahl und das Phishing, die ▸ Botnetze und den Entwicklungen bei der ▸ Malware. Die damit verbunden Fragen werden im ▸ **Teil A.** angesprochen.

Abgelöst davon beschäftigt sich ▸ **Teil B.** mit den nicht-technischen Angriffsmethoden, die als ▸ **Social Engineering** bekannt sind. Sie schließen die geschickten Formulierungen in Spam-Mails, das Ausspionieren von Organisationen und den direkten Kontakt zu deren Mitarbeitern mit ein. Damit verlassen sie die technischen Gefahren, die der Informations- und Kommunikationstechnnik drohen.

Der ▸ **Teil C.** beschäftigt sich mit der ▸ **Underground Economy** des Internets und ihren organisatorischen Strukturen, soweit sie bereits erkennbar sind [4].

Die einzelnen Aufsätze sind unabhängig voneinander seit 2007 zu verschiedenen Zeiten entstanden. Wiederholungen wegen einzelner Aspekte lassen sich schon deshalb nicht vermeiden. Hinzu kommt, dass jeder Aufsatz die Cybercrime aus einem eigenen Blickwinkel betrachtet, so dass auch deshalb Überschneidungen zwangsläufig sind.

Dieter Kochheim, Mai 2010

18.05.2010: 53 Korrekturen

24.05.2010: Aktualisierung und Überarbeitung [5]

---

1 Arbeitspapier **CF**, Phishing, 2007 (PDF)

2 **CF**, Phishing mit Homebanking-Malware, 22.10.2008; **CF**, gewandelte Angriffe aus dem Netz, 29.11.2008; **CF**, neue Methode gegen Homebanking-Malware, 06.11.2008.

3 Angestaubt und noch immer aktuell: **CF**, IT-Sicherheit, Schwachstellen, Angriffe,2007

4 **CF**, Basar für tatgeneigte Täter, 11.04.2010; **CF**, modulare Kriminalität, 05.10.2008.

5 Jüngst erschienen ist: Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

A. Angriffe auf IKT-Systeme

Den Einstieg in den ersten Teil bilden die bekannten und hypothetischen ▸ **Angriffe auf vernetzte IKT-Systeme** [6] ungeachtet dessen, ob es sich um einzelne PCs, häusliche Netzwerke, mobile Endgeräte oder professionelle Firmennetzwerke handelt. Ihre potentielle Gefährdung besteht darin, dass sie Schnittstellen für Außenverbindungen haben, die den Einstieg für äußere Angreifer prinzipiell ermöglichen. Einige der weniger bekannten Schnittstellen, so etwa der Nahfunk, die Telefonanlage oder die TV-Karte, wirkten 2007 noch exotisch und utopisch, wenig realistisch und versponnen. Durch Zeitablauf hat sich die Berechtigung des Ansatzes bestätigt, auch weit hergeholte Gefahrenquellen zu betrachten.

Dem folgt ein Rückblick auf die ersten Formen der Cybercrime, die von ▸ **Nummerntricks** [7] geprägt waren. Sie gilt es deshalb im Blick zu behalten, weil es sich gezeigt hat, dass sie in gewandelter Form immer wieder auftauchen können und das auch dann, wenn sie längst als überholt gelten.

Daran schließen sich die Aufsätze über die ▸ **Malware** [8], den ▸ **Identitätsdiebstahl** und die ▸ **Botnetze** [9] an.

Neu geschrieben wurde der Aufsatz über den ▸ Identitätsdiebstahl und das Phishing. In ihn flossen mehrere Meldungen aus dem Cyberfahnder ein und einzelne Passagen aus dem ▸ Arbeitspapier Phishing aus 2007 haben immer noch eine aktuelle Bedeutung.

A.1 IT-Sicherheit, Schwachstellen, Angriffe [10]

Wir müssen davon ausgehen, dass die Angreifer auf IT-Systeme äußerst kreativ sind und jede technische Neuentwicklung darauf prüfen, wie sie penetriert und für ihre Zwecke ausgenutzt werden kann. Ich will die Situation weder dramatisieren noch bagatellisieren. Die Gefahr, angegriffen und ausgenutzt zu werden, ist akut. Das kann sehr schlimm sein, wenn ein Angriff zu unmittelbaren Vermögensschäden führt (Phishing, Kontomanipulationen, Identitätsklau), aber auch dann, wenn unsere technischen Kapazitäten in Beschlag genommen werden (Übernahme in ein Botnetz).

Wir müssen ferner davon ausgehen, dass sich die Vernetzung der IKT nicht mehr umkehren lässt. Dies zu fordern wäre auch das falsche Signal. Das Internet hat einen Qualitätssprung ausgelöst, soweit es um die Beschaffung von alltäglichen und besonderen Informationen geht, und die Computertechnik gibt uns Verwaltungs- und Gestaltungsmöglichkeiten, die ohne sie undenkbar wäre. Das gilt für die schlichte Textverarbeitung, die hier zum Einsatz kommt, ebenso wie für die Onlineautorisierung der internationalen Finanzwirtschaft [11].

Dem weiteren Aufsatz liegen einige Annahmen zugrunde, die das Verständnis erleichtern sollen:

⇨ Grundsätzlich jede Schnittstelle zur Außenverbindung birgt die Gefahr, angegriffen, übernommen und überwunden zu werden. Erst bei einer kritischen Risikobewertung kann sich herausstellen, dass nur ein zu vernachlässigendes Risiko besteht. Zu der Bewertung gehört auch die Frage, ob die Schnittstelle überhaupt benötigt wird. Ist das nicht der Fall, sollte sie im Zweifel deaktiviert werden.

⇨ Je intelligenter eine IKT-Komponente ist, desto anfälliger ist sie für einen Angriff. Intelligenz in diesem Sinne umfasst mehrere Aspekte.

⇨ Der erste ist die Steuerungsfähigkeit. Geräte, die über ein eigenes Betriebssystem verfügen, er-

---

6 Informations- und Kommunikationstechnik - **IKT**

7 **CF**, Nummerntricks. Adressenschwindel bei Telefondiensten und im Internet, 21.11.2008

8 **CF**, Malware, 12.05.2008

9 **CF**, Botnetze, Sommer 2007

10 Überarbeitete Fassung des Aufsatzes von 2007: **CF**, IT-Sicherheit, Schwachstellen, Angriffe, 2007

11 Kochheim, Arbeitspapier Skimming #2, März 2010

öffnen damit grundsätzlich auch, dass das Betriebssystem falsch funktioniert oder über eine Schwachstelle angegriffen werden kann. Das gilt zum Beispiel für Netzwerkkomponenten (Switches, Router) oder selbständige Funktionskarten (Grafikkarte, TV-Karte, Schnittstelle zur Telekommunikation).

⇨ Der zweite Aspekt ist die Speicherfähigkeit. Dort, wo variable Daten gespeichert werden können, können grundsätzlich auch feindliche Daten abgelegt und der Kontrolle durch Firewalls und Virenscanner entzogen werden. Das gilt etwa für Netzwerkspeicher (Festplatten im LAN [12] [13]), Cache-Speicher [14] oder das für den Systemstart nötige BIOS [15].

⇨ Der dritte ist schließlich die Updatefähigkeit. Sie setzt sowohl die Steuerungs- als auch die Speicherfähigkeit voraus und eröffnet einem Angreifer die Gelegenheit, manipulierten Code einzuschleusen, wenn er auf den Updatevorgang Einfluss nehmen kann.

⇨ Abschottung bietet Schutz. Sie lässt sich erreichen durch Verzicht auf technische Intelligenz [16] und auf unnötige Schnittstellen oder ihre Beschränkung [17] und Überwachung [18].

[12] Wegen der technischen Einzelheiten wird auf die Wikipedia verwiesen. Die Links werden mit „WP“ gekennzeichnet: **WP**, Hauptseite.

[13] **WP**, LAN: Local Area Network. Betriebliche oder häusliche Netzwerke, die in aller Regel über einen gemeinsamen Zugang zum Internet verfügen.

[14] **WP**, Cache-Speicher: Zwischenspeicher.

[15] BIOS: Basic Input Output System zur Erkennung der Systemkomponenten und zum Start des Betriebssystems auf der Anwenderebene.

[16] Ich verweise dazu immer wieder auf die „fest verdrahteten“ **WP**, RISC-Prozessoren und bekomme dafür Prügel. Sie enthalten unveränderliche Rechenoperatoren und sind besonders schnell. Ihr Nachteil ist, dass sie veränderten Anforderungen nicht angepasst und vor Allem nicht Update-fähig sind.

[17] Gemeint sind besonders Firewalls, die die Ports und Protokolle einschränken, auf denen die Internet-Kommunikation beruht, die Systemeinstellungen, also die Beschränkung der Anwenderrechte im Normalbetrieb, und der Ausschluss von Schreibrechten, während besonders sensible Arbeiten ausgeführt werden (Homebanking, Bankix).

[18] Zusammenspiel von Firewall, Virenscanner und Systembeschränkungen, womit hier der Ausschluss von Programminstallationen ohne Administratorenrechte gemeint ist.

A.1 1. Heimnetz-Architektur

Betrachten wir zunächst ein besser ausgestattetes häusliches oder gewerbliches DSL-Netzwerk (Grafik auf der nächsten Seite).

Die Grafik zeigt drei farbig unterlegte "Räume". Wir beginnen mit dem grauen Bereich, der sich auf die Netzwerktechnik beschränkt.

Die eingehenden Signale durchlaufen zunächst einen Splitter, der die Telefonie- und die Datenübermittlungen voneinander trennt. Wegen der Telefonie kann eine ISDN-fähige Telefonanlage unmittelbar angeschlossen sein [19]. Wird eine analoge Telefonanlage (weiter-) verwendet, muss zwischen ihr und dem Splitter ein NTBA [20] geschaltet werden, der wechselseitig die analogen in digitale Signale wandelt.

Für die Kommunikation zwischen dem PC als Endgerät auf der einen Seite und dem DSL-Zugangsprovider andererseits wird ein DSL-Modem verwendet [21]. An ihm kann ein einzelner PC direkt angeschlossen sein oder aber, wie im Schaubild, eine aktive Netzwerkkomponente, die die Datenkommunikation aufnimmt, vermittelt und weiter leitet.

Die DSL-typischen Geräte, Splitter, NTBA und DSL-Modem, bereiten Signalströme für ihren jeweiligen Verwendungszweck auf und enthalten entsprechend wenig "Intelligenz".

Die einfachste Form einer aktiven Netzwerkkomponente ist ein Hub [22]. Er nimmt ihm zugeleitete Daten auf und schickt sie gleichzeitig an alle an ihm angeschlossenen Geräte weiter, ohne dabei ein besonderes Ziel auszuwählen. Dagegen löst ein Switch [23] die eingehenden Datenströme auf und sendet sie nur an die Zieladresse weiter, für die sie bestimmt sind. Ein Router verbindet in der

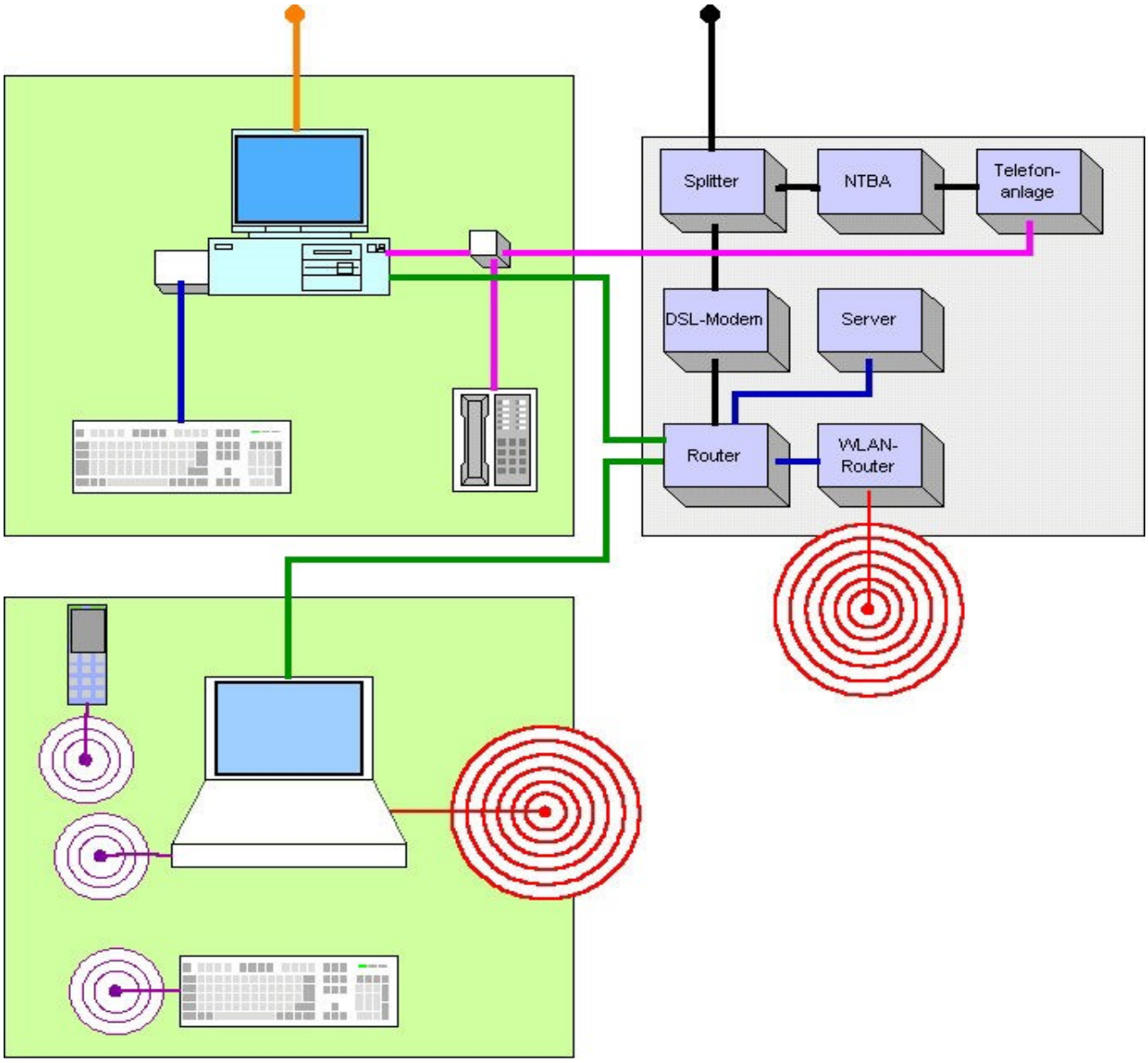
[19] **WP**, Integrated Services Digital Network – ISDN

[20] **WP**, Network Termination for ISDN Basic rate Access - NTBA

[21] **WP**, Digital Subscriber Line - DSL

[22] **WP**, Hub (Netzwerkkomponente)

[23] **WP**, Switch (Netzwerkomponente)



Regel zwei Netze miteinander (Gateway [24]) und verhält sich gegenüber dem Netz, das er "kennt", wie ein Switch. Gegenüber den anderen Netzen verhält er sich hingegen wie ein Hub und sendet alle unbekannt adressierten Datenpakete ungerichtet in das zweite Netz, hier also in Richtung des Zugangsproviders.

Zwei nicht übliche Komponenten sind an den Router im Schaubild angeschlossen: Ein "Server" [25] und ein WLAN-Router [26].

In Privathaushalten wird man in aller Regel keinen gesonderten Router finden, sondern nur einen WLAN-Router, der ein Funknetz aufbaut, die Verbindung zum Provider herstellt und an den noch ein oder mehrere PCs angeschlossen werden können. Solche Geräte verbinden die Funktionalitäten Funknetz und Routing miteinander. Die besondere Funktion des WLAN-Routers ist es aber, ein Funknetz einzurichten, über das mehrere Endgeräte drahtlos vernetzt werden können.

Der "Server" kann mehrere Aufgaben haben. In kleinen und mittleren Unternehmen kann er besonders als Fax- und E-Mail-Server eingerichtet sein, der sowohl den ein- und ausgehenden Verkehr verarbeitet und die Eingänge speichert.

Im privaten Bereich ist eher zu erwarten, dass ein gemeinsamer Server für die Speicherung und Bereitstellung von Dokumenten (Urlaubsfotos u.ä.)

[24] **WP**, Gateway (Netzwerkkomponente), Verbindungsstelle zwischen verschiedenen Netzen.

[25] **WP**, Server

[26] **WP**, WLAN-Router (Wireless Access Point)

verwendet wird, die allen Beteiligten zur Verfügung stehen sollen, ohne dass man sich gegenseitig Zugriff auf die privaten PCs geben will. Das ist eine unter Sicherheitsgesichtspunkten durchaus sinnvolle Strategie, bei der die privaten PCs konsequent gegen Außenzugriffe abgeschirmt werden.

Die grün unterlegten Bereiche sind schnell erklärt. Oben ist ein PC dargestellt, der sowohl per Datenleitung wie auch per Telefonleitung mit den zentralen Einrichtungen verbunden ist. Unten wird ein Laptop gezeigt, das per Kabel und per WLAN vernetzt ist. Auf die Einzelheiten kommen wir noch zurück.

A.1 2. "harte" physikalische Angriffspunkte

Wegen der Gefahrenpunkte betrachten wir zunächst die einzelnen technischen Komponenten in einem Netzwerk, ihre Eignung, missbraucht zu werden, und die von ihnen ausgehenden Gefahren.

Wenn eine Komponente penetriert werden kann, so heißt das nicht, dass ein Angreifer durch sie einen vollständigen Zugriff auf alle Daten im Netzwerk erringen kann. Üblich für das Vorgehen von Hackern ist es aber, dass sie Schritt für Schritt in ein System eindringen und dazu auch Zwischenstationen verwenden, die sie nur als Sprungbrett zur nächsten oder zum Belauschen des Datenverkehrs verwenden können. Ihr Ziel ist es jedoch, an die sensiblen Daten in einer IT-Anlage heranzukommen, und dazu brauchen sie administratorische Rechte, also den Vollzugriff auf das System.

A.1 2.1 technische Geräte als Gefahrenquelle

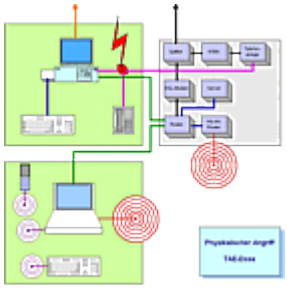
Zur Datenspionage und zur fremden Beherrschung von EDV-Systemen eignen sich grundsätzlich alle Zugänge, Verbindungen und Schnittstellen, die ein Computer zulässt. Es gilt der Grundsatz: Je komfortabler er eingerichtet ist und je einfacher (unbedachter) sich mit ihm arbeiten lässt, desto gefährdeter ist er. Die beste Sicherung des Systems nutzt nichts, wenn es irgendwo eine Hintertür oder eine Öffnung offen lässt.

Wenn der Angreifer als Einbrecher oder bei einer sich bietenden Gelegenheit selber Netzwerktechnik installieren oder konfigurieren kann, kann er sich an den meisten Sicherheitsmaßnahmen vorbei bewegen und Hintertüren installieren (Rootkit). IT-Sicherheit beginnt bei der einfachen Technik und abgeschlossenen Räumen.

Technisch-physikalische Angriffe sind eher im Zusammenhang mit der (Industrie-) Spionage zu erwarten und weniger im privaten Bereich. Wie sich der Angreifer einen direkten körperlichen Zugang verschaffen kann, lehrt das ▸ Social Engineering, was nichts anderes ist als eine Sammlung modernisierter Detektivmethoden [27].

Sie können jedoch zu einem unmittelbaren, unverzögerten und direkten Zugriff führen, wobei alle Sicherungsmaßnahmen umgangen und ein als sicher geglaubtes System unmittelbar, aus sich selbst heraus angegriffen werden kann. Das macht sie besonders gefährlich.

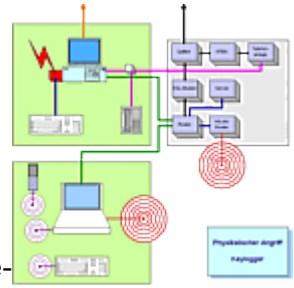
A.1 2.2 Telefonanschluss



Das gilt besonders für Abhöreinrichtungen in der Telefontechnik wie links gezeigt innerhalb einer Telefonsteckdose. Hier können sehr komfortabel der Telefonverkehr und die Verbindungsdaten mitgeschnitten werden. Dieser Angriff eignet sich hingegen weniger für die Penetration anderer Geräte, weil dazu - wie auch mit der Malware - weitere Sicherheitslücken überwunden werden müssen oder eine Außenverbindung geschaffen werden muss. Unmöglich ist das nicht.

[27] Interessante Einblicke in die Spionagemethoden - ganz ohne EDV - bietet Andreas Eschbach, Der Nobelpreis [ausgewählte Zitate, Bergisch Gladbach (Lübbe) 2005].

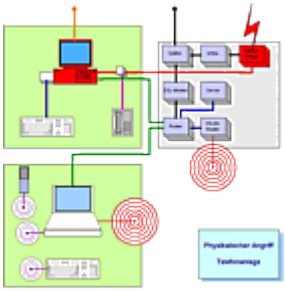
A.1 2.3 Keylogger



Keylogger dienen dazu, die Tastatureingaben zu protokollieren. Sie werden meist unscheinbar zwischen den Tastaturstecker und der Eingangsbuchse des PCs gesteckt [28]. Sie müssen nach einer gewissen Zeit ausgewechselt oder so konstruiert werden, dass sie ihre Protokolldaten drahtgebunden oder per Funk weiter vermitteln.

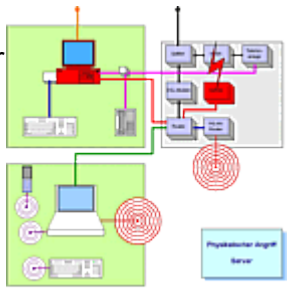
Der Einsatz von Keyloggern ist besonders im Zusammenhang mit der Überwachung von Arbeitnehmern bekannt geworden. In modernen Anwendungsfällen kommen jedoch keine Hardware-Keylogger zum Einsatz, sondern ihre Software-Varianten [29].

A.1 2.4 Telefonanlage, Server



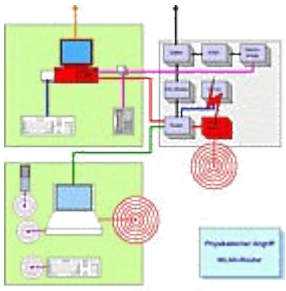
Wegen der Gefahr, die von technischen Angriffspunkten ausgeht, gilt, dass sie umso höher ist, je "intelligenter" die Schnittstelle ist. Das hängt von ihrer operativen Leistung (Rechenleistung) und ihrem Speichervolumen ab.

Gegenüber den bislang vorgestellten Komponenten ist die Telefonanlage ein "Geistesriese", ein Computer im Kleinen. Wenn sie eine direkte Verbindung zum PC hat und auf ISDN-Technik beruht, kann sie die interne Steuerung des PCs übernehmen, wenn sie entsprechend angeleitet wird.



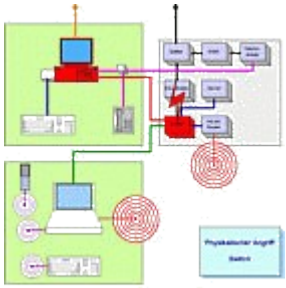
Noch verheerender kann ein penetrierter Server wirken. Er ist nicht nur ein vollwertiger Computer, sondern häufig auch noch ein besonders gut ausgestatteter und leistungsfähiger, der von den anderen Geräten im Netzwerk als besonders vertrauenswürdig angesehen wird, weil er zentrale Dienste wie z.B. die Verwaltung gemeinsamer Dokumente, von Backups, die E-Mail-Konten, den Fax-Versand und ihren -Empfang zur Verfügung stellt.

A.1 2.5 WLAN-Router, Switch



Besonders populär, allerdings für Angriffe aus dem Fremdnetz, sind die Ausnutzung und Übernahme von WLAN-Routern, die mehrere mobile Geräte miteinander verbinden.

WLAN-Router sind aber nicht nur Access Points für die Funknetzverbindung, sondern - quasi zur anderen Seite hin - auch vollwertige, mit dem Netz verkabelte Komponenten. Wer ihn steuert, kann alle Signale, Zugangscodes und Inhalte protokollieren, alle Beteiligten vom WLAN ausschließen und schließlich auch auf die anderen Netzkomponenten zugreifen. Er hat damit ebenfalls den direkten Zugang zum Internet per Festnetz.



Router oder Switche eignen sich besonders dazu, Daten zu protokollieren und das Netzwerk zu stören. Mit ihnen kann sich der Angreifer den Zugang zu allen angeschlossenen Geräten verschaffen und jedes einzelne von der Netznutzung ausschließen.

Handelt es sich dabei um einen modernen Switch, so enthält er sogar ein abgespecktes, aber vollwertiges Betriebssystem, das prinzipiell fremde Programme speichern, verwalten und ausführen kann. Auch an Speicherplatz fehlt es ihnen nicht, weil sie auch im Normalbetrieb die durchgeleiteten Daten puffern, also zwischenspeichern [30].

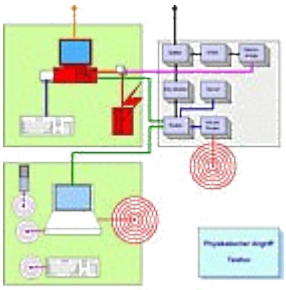
---

[28] Siehe **CF**, Phishing. Keylogger, 2007.

[29] Siehe Anmerkungen in der Urfassung.

[30] Darin unterscheiden sich die aktiven Netzwerkkomponenten von den Medienwandlern, mit denen z.B. Kupfer- und Glasfaserkabel miteinander gekoppelt werden können. Diese puffern in aller Regel die verarbeiteten Daten nicht, so dass Medienwandler gelegentlich zu Nadelöhren in weit verzweigten Netzen werden können.

A.1 2.6 Telefon



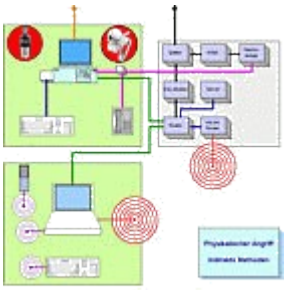
Die Infiltration eines Telefonapparates (Endeinrichtung) mag wenig spektakulär sein. Dennoch kann darüber ein direkter Kontakt zur EDV-Anlage möglich sein und deren Penetration.

Telefonapparate sind allerdings in aller Regel nicht sonderlich "intelligent", so dass die Gestaltungsfreiräume für den Angreifer sehr eingeschränkt sind.

Sie bieten aber auch den direkten Zugang zur Telefonanlage. Kann sie manipuliert werden und hat sie direkte Anschlüsse zu den Arbeitsplatzrechnern, kann über sie der direkte Zugang zu deren Daten, Funktionen und Rechten hergestellt werden.

Das gilt noch mehr, wenn Voice over IP [31] zum Einsatz kommt. VoIP nutzt für die Sprach- und Datenkommunikation dieselben Kabel und Schnittstellen ("Konvergenz") und schafft dann, wenn kostengünstige Lösungen per PC verwendet werden, einen direkten Zugang zur Datenverarbeitung [32].

A.1 2.7 Klassiker und Kuckuck



Die Darstellung wäre unvollständig, wenn nicht auch zwei geradezu "klassische" Abhör- und Angriffsmethoden genannt würden.

Mit Mikrofonen und Kameras können menschliche Handlungen, ihre Sprache und nicht zuletzt ihre Aktivitäten am Computer überwacht und "mitgehört" werden.

Nicht selten sind diese Geräte bereits mit dem PC verbaut (Multimedia-PC) und werden für die Internet-Telefonie genutzt. Der Angreifer, der die Daten von der Soundkarte mitlesen kann, verfügt damit auch über die ein- und ausgehenden Sprachdaten.

Mit ihnen kann er womöglich mehr und gefährlichere oder geheime Informationen sammeln, als wenn er Schritt für Schritt in ein gut gesichertes EDV-System eindringen muss. Die einfachsten Methoden sind manchmal die erfolgreichsten.

Für Paranoia sorgt auch eine klassische und einfache Vorstellung: Ein Besucher, Geschäftspartner oder Konkurrent kommt in das Unternehmen und hat seinen Laptop dabei. Sobald er unbeaufsichtigt ist, sucht er ein leeres Büro auf und stöpselt seinen Laptop in die ungesicherte Netzwerkdose. Sogleich ist er mit dem Firmennetzwerk verbunden und kann schalten und walten.

Moderne Netzwerkkomponenten für den professionellen Einsatz lassen den Zugang solcher fremden Geräte nicht zu, weil sie die MAC-Adresse auslesen [33] und vergleichen. Sie sind dadurch aber so "intelligent", dass sie ihrerseits zum Angriff reizen.

Noch einfacher macht man es dem Angreifer, wenn die Mitarbeiter ihre PCs während ihrer Pausen und Abwesenheiten eingeschaltet lassen und weder Bildschirmschoner noch andere Maßnahmen eine Authentifizierung verlangen.

A.1 3. Angriffe aus dem Netz

Verabschieden wir uns von der Vorstellung, dass Netze nur aus Kabeln bestehen. Die Funk- und Nahfunktechnik werden auf den folgenden Seiten dargestellt.

Verabschieden wir uns auch davon, dass die Datensicherheit immer auch mit Datennetzen in Verbindung steht. Außerhalb unserer Wohnungen, Firmen und Behörden gibt es längst keine Trennung mehr zwischen der Daten- und Sprachkommunikation. Sie verwenden dieselben Netze und Infrastrukturen.

---

31 **WP**, Voice over IP - VoIP (IP-Telefonie)

32 Siehe auch **CF**, Online-Zugriff an der Quelle, 08.11.2008.

33 **WP**, Media Access Control - MAC

A.1 3.1 Hacking

Gegenüber technisch-physikalischen Angriffen haben Angriffe aus dem Netz den Vorteil, dass sie ohne teure Geräte und ohne körperlichen Zugang und Installationen auskommen. Sie nutzen Schwachstellen und Lücken aus, die die Hersteller von Hard- und Software unbedacht ließen oder die der Anwender nicht kennt und schließt [34].

Die Angriffe aus dem Netz kennzeichnen das klassische Hacking. Bei ihm kommt es darauf an, Hintertüren oder Schwachstellen im Computer oder EDV-System auszukundschaften und schließlich zu missbrauchen, um in sie einzudringen. Manche Komponenten, insbesondere Netzwerkkomponenten eignen sich nur zum Protokollieren und Umleiten der durchgehenden Datenströme oder dienen dem Angreifer als Zwischenschritt zum Erreichen der datenverarbeitenden EDV.

A.1 3.2 Telefonanlage

Seit der Umstellung der Telekommunikationstechnik von der analogen zur digitalen Technik verfügen wir über ein Signalisierungsnetz, das wegen seiner Eigenschaften vom öffentlichen Interesse kaum wahrgenommen wird [35]. Per ISDN nutzt es den B-Kanal, um Wahlverbindungen herzustellen, Wähltöne zu übermitteln und Sonderdienste zu vermitteln (Mehrwertdienste, Auskunftsdienste, Netzvorwahlen [Call-by-Call]).

Die Telefonanlage ist häufig genug ein "PC im Kleinem", also "intelligent" in dem Sinne, dass sie elektronische Datenverarbeitungen selbständig erledigen kann.

Je intelligenter unsere Haus-Telefonanlage ist, desto prinzipiell gefährlicher ist sie auch für unsere Datenkommunikation.

Vielfach ist sie direkt mit den Arbeitsplatzrechnern verbunden. Sie ist eine erhebliche Gefahrenquelle, insbesondere dann, wenn sie günstige Fernverbindungstarife selber ermittelt oder die Fernwartung für die Hersteller- oder Vertriebsfirma zulässt.

Auf das EDV-System kann sie entweder über das gesonderte Telefonnetz oder, wenn VoIP eingesetzt wird, direkt über die Datenverbindungen zugreifen.

A.1 3.3 aktive Komponenten

Die aktiven Komponenten wurden bereits im Zusammenhang mit den physikalischen Angriffspunkten angesprochen. Soweit sie der Verbindungsvermittlung dienen, stellen sie keine nennenswerte Hindernisse für einen Angreifer dar. Sind sie hingegen mit "Intelligenz" ausgestattet und haben eigene Sicherheitsfunktionen, können sie einem Angreifer einerseits den Durchgriff erschweren. Andererseits liefern sie ihm, wenn sie vom Hacker übernommen werden können, einen komfortablen Vorposten, von dem aus der Datenverkehr überwacht und der nächste Angriffsschritt durchgeführt werden kann. Router und Switche lassen sich nicht nur mit dem Hacking, sondern auch mit massiven Angriffen überwinden, indem sie mit Datenlast bombardiert und überlastet werden [36].

Server sind vollwertige und häufig auch hochwertige Computer. Kann sich ein Angreifer in ihnen mit Systemverwalterrechten (Administrator, Datenveränderung) einnisten, steht ihm das lokale Netzwerk offen. Wenn die übrigen Computer im Netzwerk unzureichend abgesichert sind, kann er auf diese zugreifen.

Das ist prinzipiell auch vermittels eines Netzwerkdruckers möglich, der über das Internetprotokoll in das LAN eingebunden ist [37].

---

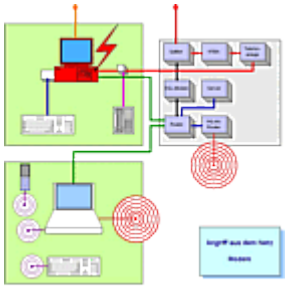
[34] Siehe unten **A.3 Malware**.

[35] Siehe **CF**, TK-Netze, 2007

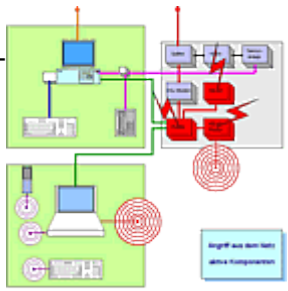
[36] **WP**, Pufferüberlauf (Buffer overflow)

[37] Malte Jeschke, Sicherheitslücke Drucker, tecchannel 03.11.2006

A.1 3.4 internes Modem. Fremdnetzzugang



Externe und interne Modems , die zum Beispiel zum Faxempfang verwendet werden, sowie direkte ISDN-Anschlüsse am PC bieten über die Telefonleitung einen Fremdnetzzugang, der an den übrigen Sicherheitsvorkehrungen vorbei zu einem unmittelbaren Angriff genutzt werden kann. Eine solche Direktverbindung mit dem Telefonnetz und an dem Datennetz vorbei dürfte die bekannteste Sicherheitslücke sein, die für Hacking-Aktionen genutzt werden kann.



Nur ausnahmsweise kommen zwei weitere Fremdnetzverbindungen zur Datenkommunikation in Betracht. Das sind z.B. TV-Karten mit ihren Anschlüssen für den Fernseh- und Rundfunkempfang. Die TV-Karte hat eine direkte Verbindung zu den anderen Komponenten des Computers, aber nur eine beschränkte "Intelligenz" (hier Kommandosatz), der für einen Angriff missbraucht werden könnte.

Prinzipiell kommt auch das Stromnetz als Fremdnetzzugang in Betracht, wenn es auch zur Anlieferung von Telekommunikationsdiensten dient. Im Normalfall geht von ihm keine Gefahr aus, weil es an einer Schnitt- und Übersetzungsstelle zwischen der Stromversorgung und den "intelligenten" Komponenten des Computers fehlt.

A.1 4. Angriffe auf Funk-Schnittstellen

Erst vor wenigen Jahren sind lokale Funknetze bekannt und populär geworden (WLAN [39]). Sie sparen die häusliche Verkabelung, lassen sich schnell einrichten und arbeiten verlässlich.

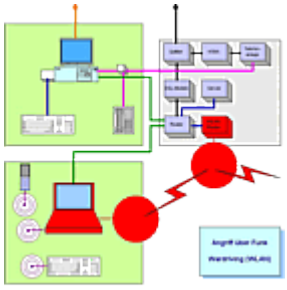
Alsbald häuften sich die Berichte über teure Telefonrechnungen durch Internetnutzung und besondere Dienste, so dass auch bekannt wurde, dass sich Dritte in das Funknetz einschleichen und Kosten verursachen können. Es entwickelte sich eine eigenständige Trittbrettfahrer-Kultur, das Wardriving [40]. Die Wardriver durchstöbern systematisch die Wohn- und Geschäftsgebiete auf der Suche nach offen, ungeschützten oder leicht korrumpierbaren Funknetzen.

Die Opfer, die ihr Funknetz ungesichert lassen (genaue Bestimmung der zugangsberechtigten Geräte, Verschlüsselung, Beschränkung der zugelassenen Onlinezugriffe), blieben hilflos, weil sie die Trittbrettfahrer nicht namhaft machen konnten, auf ihren Kosten sitzen blieben und eine strafrechtliche Verfolgung ebenfalls nicht stattfand, weil die missbräuchliche Nutzung ungeschützter Techniken keine Straftat ist.

Es setzte sich die Erkenntnis durch, dass man zumindest die übermittelten Daten verschlüsseln müsse. Der dazu zunächst verwendete Standard, WEP [41], erwies sich sehr schnell als unsicher. Mit den richtigen Programmen ließ er sich binnen weniger Minuten brechen. Erst der neue Standard WPA [42] erwies sich als hinreichend sicher.

In der Hackergemeinde hat sich zwischenzeitlich eine eigenständige Zeichensprache zur Kennzeichnung identifizierter Funknetze etabliert (Warchalking [43]), die an die klassischen Gaunerzinken erinnert [44].

A.1 4.1 Wardriving: Eindringen in lokale Funknetze



Die marktüblichen Programme richten die WLAN-fähigen Geräte so ein, dass sie nach Funknetzen automatisch suchen. Sie tragen damit dem Umstand Rechnung, dass es viele offene WLANs gibt, die dazu bestimmt sind, z.B. den Kunden eines Hotels oder

38 **WP**, Modem

39 **WP**, Wireless Local Area Network - WLAN

40 **WP**, Wardriving

41 **WP**, Wired Equivalent Privacy - WEP

42 **WP**, Wi-Fi Protected Access - WPA

43 **WP**, Warchalking

44 Gaunerzinken, Rotwelsch

Restaurants einen komfortablen Zugang zum Internet und zu ihren E-Mails zu geben (Hotspots). Diese Anbieter sichern aber in aller Regel ihre eigene EDV dadurch ab, dass sie sie in gesonderten Netzen betreiben, und beschränken den Internetzugriff auf den einfachen Zugang, wobei kostenpflichtige Dienste ausgeschlossen sind.

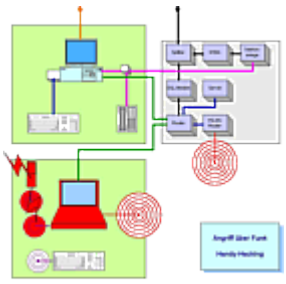
In der Anfangszeit wurden WLAN-Router an Privatkunden so ausgeliefert, dass die Verschlüsselung extra eingestellt werden musste. Das hat sich schnell geändert.

Über einen ungesicherten WLAN-Router erhält der Angreifer auch den Zugriff auf die Endgeräte, die per Kabel vernetzt sind. Der Zugang zum Internet und dessen missbräuchliche Nutzung ist dann fast schon unvermeidlich.

A.1 4.2 Nahfunk

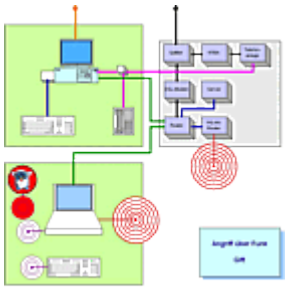
Die Reichweite von WLANs ist begrenzt. Sie richtet sich auch nach der Bauweise der Gebäude (Betondecken sind meist undurchdringlich) und dem Standort des Funk-Routers.

Daneben gibt es aber auch verschiedene Methoden des Nahfunks. Ein üblicher Standard ist Bluetooth [45]. Mit ihm werden Kopfhörer, Tastaturen und nicht zuletzt Mobiltelefone mit dem PC oder Laptop drahtlos verbunden.



Ungeachtet dessen, dass die biologischen Wirkungen der verschiedenen Funkfrequenzen und -stärken streitig sind, kann über das Mobiltelefon ein fast unbemerkter Kontakt hergestellt und missbraucht werden. Wer achtet schon immer auf die verschiedenen Statusanzeigen am unteren Rand seines Laptops?

Als Kontaktquelle für den Kontakt per Bluetooth kommt alles in Betracht, auch das Geschenk eines nicht wohlmeinenden Geschäftspartners, in dessen Inneren unerkannt Technik versteckt ist, die ihre frisch gewonnenen Erkenntnisse über das Innenleben Ihres Laptops wie ein Mobilfunkgerät weiter sendet.



Für die Signalübermittlung auf kurzer Entfernung kann neben der Funk- auch die Infrarottechnik genutzt werden. Anstelle der Bluetooth-Technik kommen auch andere Mobilfunktechniken in Betracht wie zum Beispiel UMTS [46].

A.1 5. Angriffe mit Crimeware

Unter Crimeware [47] werden alle Programme zusammen gefasst, die ausdrücklich dazu bestimmt sind, kriminellen Zwecken zu dienen.

Die Crimeware wird flankiert von üblichen Netzwerkwerkzeugen, die zumeist nützlich eingesetzt, aber auch missbraucht werden können. Dies gilt besonders für das Kommando Ping [48], das von jedem üblichen Betriebssystem geliefert wird und zu der Prüfung dient, ob eine Netzverbindung besteht [49]. Es kann auch dazu missbraucht werden, aktive IP-Adressen und offene Ports zu erkunden, um diese sodann gezielt anzugreifen. Genauso verhält es sich mit Traceroute [50], das den Weg eines Datenpakets im Netz protokolliert und damit einem Angreifer auch zeigt, welche Stationen sich für einen Angriff lohnen, um schließlich das Ziel zu korrumpieren.

Den Kern der Crimeware stellen Viren, Würmer, Trojaner und Keylogger dar (▸ Malware), die verschiedene Strategien und Wege der Infiltration nutzen [51]. Während Viren und die Würmer der ersten Generation immer Träger benötigten, also Dateien, in die sie sich eingefügt (Viren) oder an die sie sich angehängt haben (Würmer), können IP-Würmer der neuen Generation selbständig An-

---

45 **WP**, Bluetooth

46 **WP**, Universal Mobile Telecommunications System - UMTS

47 **WP**, Crimeware

48 **WP**, Ping

49 Siehe auch **CF**, Auskunftsdienste im Internet, 06.12.2009.

50 **WP**, Traceroute

51 Erklärungen für **WP**, Malware, **WP**, Adware, **WP**, Keylogger, **WP**, Spyware, **WP**, Trojaner, **WP**, Viren und **WP**, Würmer.

griffsziele erkunden und attackieren. Trojaner verstecken sich in anderen Programmen, die dem Anwender einen besonderen Nutzwert versprechen und handeln sozusagen im Geheimen.

Keylogger und Spyware bezeichnen hingegen die Funktionsweise der Malware, aber nicht die Art des Vorgehens bei der Infiltration.

A.1 5.1 Malware

Zur Abwehr der Malware werden verschiedene Programme wie Virenscanner und Firewalls sowie ihre ständigen Aktualisierungen angeboten. Sie bieten einen Grundschutz. Während die Virenscanner noch vor ein paar Jahren mehr als 90 % der Malware auf Anhieb erkannten ist die Erkennungsrate inzwischen auf unter 40 % gesunken. Sie sind nach wie vor nötig, müssen aber um weitere Schutzmaßnahmen ergänzt werden.

Eine wichtige Aufgabe kommt insoweit den Programmherstellern zu, die die in ihren Anwendungen enthaltenen Sicherheitslücken (Exploits) immer schneller erkennen und mit Updates schließen müssen.

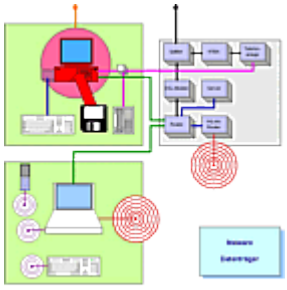
Ebenso wichtig sind die Maßnahmen, die der Anwender und die IT-Organisation durchführen müssen, in die er eingebunden ist. Dazu gehören vor Allem die Rechteverwaltung (keine Programminstallation, beschränkte Schreibrechte) und die kritische Beobachtung des laufenden Betriebs sowie der eigenen Handlungen.

Aber auch die Techniken, die die Malware-Programmierer verwenden, sind nicht banal. Sie nutzen alle Möglichkeiten der Tarnung und Täuschung. Dazu wird die Malware nicht nur in die Lage versetzt, ihren Namen, ihren Standort und ihre Form zu verändern, sondern vor allem, sich über eine Netzverbindung zu erweitern, zu aktualisieren und weiter zu verbreiten (Tarnkappentechnik für Viren, Stealth-Viren [52]).

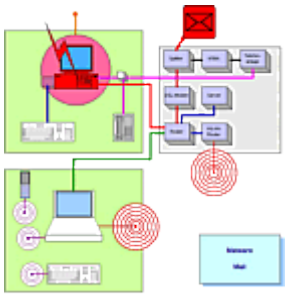
Die Infiltration erfolgt immer über bekannte oder noch allgemein unbekannte Sicherheitslücken, also offene Zugänge oder Verbindungen, die mit massenhaftem "Datendruck" sturmreif geschossen werden können (Pufferüberlauf).

Dem Nachwuchs der Angreifer wird es dadurch leicht gemacht, dass inzwischen regelrechte Baukästen (Toolkits [53]) im Umlauf sind, mit denen sich per Mausklick die Malware, ihre Zugangsstrategie und ihre Schadfunktion "zusammenklicken" lassen (ursprüngliche Bedeutung von Rootkit [54]; jetzt: Werkzeugsammlung, mit dem ein kompromittiertes System für den künftigen Missbrauch präpariert wird). Dazu ist kein besonderes Wissen mehr nötig.

A.1 5.2 Datenträger, E-Mail



Der klassische Datenspeicher zum Transport von Malware ist die Diskette, die keine Bedeutung mehr hat und von großvolumigen optischen (CD, DVD), elektronischen (USB-Stick) und magnetischen Datenträgern (Wechselfestplatten) abgelöst wurde. Wichtig dabei ist, dass diese Datenträger entweder zum Starten des Systems verwendet werden, wozu die Malware in den Bootbereich eingefügt wird, der vom Computer beim Start ausgelesen und ausgeführt wird, oder Programme enthält, die der Anwender unbedarft und ungeprüft startet.



Die zweite wichtige Infiltrationsmethode bedient sich Trägerdateien, die die Programmumgebung ausnutzen, in der ihr Wirt gestartet wird. Besonders anfällig dafür sind Office Anwendungen wegen Visual Basic for Applications - VBA, andere Formate wie PDF, die Java for Applications benötigen, Internetbrowser,

---

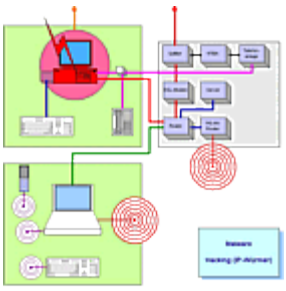
52 **WP**, Stealth-Viren

53 Toolkit: "Baukasten" (Werkzeugkasten) zum einfachen Zusammenbau von Programmen mit ausgewählten Funktionen, besonders auch zur Herstellung von Malware;
Phishing-Tool kreiert neue Betrüger-Sites in Sekunden, tecchannel 12.07.2007;
Trojaner-Basteln für Dummys, Heise online 20.07.2007

54 **WP**, Rootkit

die zur Präsentation directX benötigen und an erster Stelle E-Mail-Programme, die Dateianhänge automatisch anzeigen. Die Aufzählung ließe sich beliebig fortsetzen.

A.1 5.3 E-Hacking



IP-Würmer sind automatische Hacker, die über das Netz Angriffsziele wegen ihrer Erreichbarkeit und Anfälligkeit detektieren. Während die anderen Malware-Programme eine Mitwirkung des Opfers benötigen (Installation eines Datenträgers, Ausführen einer Datei), nutzen sie die fehlende Aufmerksamkeit des Opfers dadurch aus, dass es die nötigen Abwehrmaßnahmen unterlässt (Hintertüren, offene Systeme, unzureichende Firewalls und Virenscanner).

Gepaart mit den entsprechenden Schadfunktionen, die z.B. gezielt auf das Homebanking abgestimmt sein können, zeigen sie eine neue Qualität von Gefährlichkeit, die bislang unbekannt war. Auch im Zusammenhang mit ▸ Botnetzen spielen sie eine bedeutende Rolle.

A.1 6. Standard-Schutzmaßnahmen

Im privaten Bereich erfolgen zumeist breitflächige Angriffe mit Crimeware und zwar entweder mit infizierten Webseiten (verstärkt auch in sozialen Netzwerken), die über den Webbrowser in das System eindringen, mit E-Mail-Anhängen, die die Malware enthalten und vereinzelt gegen Netzwerkrouter. Für die Massenerscheinung ist ausschlaggebend, dass sie ungezielt erfolgt und bevorzugt Sicherheitsmängel in gängigen Betriebssystemen, Browsern und Anwenderprogrammen zur Infiltration nutzt.

Die Tendenz geht jedoch dahin, dass die Angriffe immer gezielter gegen Personengruppen mit gleichen Interessen und Neigungen, öffentlich bekannten oder wohlhabenden Personen sowie zur gezielten Spionage gegen Unternehmen und Organisationen geführt werden. Je gezielter ein Angriff erfolgt, desto ungewöhnlicher kann auch die Methode sein, mit der Angriff ausgeführt wird. Der individuelle Angriff erfolgt nicht wahllos mittels Crimeware, sondern erfolgt durch einen Hacker, der sich zur Unterstützung der Crimeware bedient.

Der Einsatz von breit gestreuter Malware ist eine eher junge Erscheinungsform. Die frühen Hacking-Angriffe richteten sich ganz gezielt gegen staatliche Einrichtungen, Universitäten und Unternehmen, wobei vor Allem ungeschützte Schnittstellen, verwaiste Netzkomponenten und Fernwartungszugänge kompromittiert wurden, um schrittweise immer tiefer in das fremde Netz einzudringen.

Einige grundlegende Schutzvorkehrungen für Privatanwender haben im Laufe der Jahre ihre Bedeutung erhalten [55].

A.1 6.1 Sensible Daten

Arbeiten Sie mit sensiblen Daten, deren unbefugte Kenntnis oder Verwendung Sie oder andere schaden können? Solche Daten gehören verschlüsselt oder auf mobile Datenträger gespeichert, die Sie sicher verwahren müssen.

Das gilt besonders auch für freie Netzspeicher bei Google, gmx oder anderen Anbietern, auf denen Sie Ihre Daten ablegen, um auf sie bei jeder Gelegenheit zugreifen zu können. Verwenden Sie Verschlüsselungen und verzichten Sie darauf, sensible Daten im öffentlichen Netz zu speichern.

A.1 6.2 Kontodaten, TAN

Kontozugangsdaten für Verkaufsplattformen, zum Homebanking und ganz besonders die Transaktionsnummern für das Homebanking gehören nicht im Computer gespeichert. Fragt Ihr Browser, ob die Zugangsdaten gespeichert werden sollen, was sehr bequem wäre, klicken Sie auf "nein". Solche Daten verwahren Sie entweder nur in gut verschlüsselten Dateien oder notieren Sie auf Papier, das Sie sicher verwahren.

[55] Der Text ist 2007 geschrieben worden und wirkt deshalb bereits etwas antiquiert. Nur dort, wo er überholt oder unvollständig war, habe ich ihn überarbeitet und ergänzt.

Verwenden Sie Kennworte, die Sie sich gut merken können, aber verwenden Sie dabei auch Sonderzeichen und Zahlen! Wählen Sie verschiedene Kennworte für ihre Konten und wechseln Sie die Kennworte in regelmäßigen Abständen.

Misstrauen Sie falschen Freunden und Fremden und geben Ihre Zugangsdaten nur dann preis, wenn Sie dem anderen auch wirklich vertrauen und die Preisgabe auch erforderlich ist.

A.1 6.3 Virenscanner, Firewall

Virenscanner und Firewall gehören zum Basisschutz. Jeder private PC, der an das Internet angebunden ist, muss über sie verfügen, wollen Sie sich nicht dem Vorwurf der Fahrlässigkeit aussetzen. Die Programme werden häufig von den Hersteller mitgeliefert (seit Windows XP) oder von Dritten kostenlos angeboten. Achten Sie auch darauf, dass die Signaturen für den Virenscanner und die Sicherheitseinstellungen regelmäßig aktualisiert werden.

Auch wenn wegen der Vielzahl der heutigen Malware die Erkennungsrate der Virenscanner stark zurückgegangen ist, so wehren sie mit ihnen wenigstens die älteren Varianten ab, die immer noch im Umlauf sein können.

Besonders wichtig sind deshalb die Firewalls in Verbindung mit Virenscannern geworden. Sie sperren Nebenzugänge aus dem Internet, überwachen online die Aktivitäten, die im Webbrowser und im E-Mail-Browser ausgeführt werden, und warnen bei ungewöhnlichen Funktionen. Damit lässt sich die überwiegende Masse der Angriffe abwehren.

A.1 6.4 Datensicherung

Eine regelmäßige Datensicherung ihrer am häufigsten verwendeten Dateien gehört zum Basisschutz. Kopieren Sie sie auf Wechseldatenträger oder verwenden Sie ein Backupprogramm. Backupdateien gehören auf einen gesonderten Datenträger (Wechselfestplatte, CD, DVD).

Wollen Sie Dateien langfristig aufbewahren (z.B. Fotos), müssen Sie die Daten spätestens nach 10 Jahren auf einen anderen Datenträger kopieren, weil alle heute angebotenen verschleißen können. Vermeiden Sie dabei Verschlüsselungen und Kompressionen (ZIP), weil sie möglicherweise nach längerem Zeitablauf nicht mehr funktionieren, und verwenden Sie marktübliche und gebräuchliche Dateiformate.

A.1 6.5 Administratorenrechte

Arbeiten Sie nur dann als Administrator, wenn Sie wirklich neue Programme installieren wollen oder Administratorenrechte zwingend erforderlich sind. Wenn möglich, trennen Sie dabei die Verbindung zum Internet (was meistens deshalb nicht geht, weil die Programme per Download angeboten werden).

A.1 6.6 Updates

Installieren Sie die vom Hersteller ihres Betriebssystems angeboten Updates (Service Packs von Microsoft), weil sie immer Sicherheitslücken schließen, die unmittelbar nach ihrem Erscheinen von Malware ausgenutzt werden. Fertigen Sie jedoch vor der Installation ein Komplett-Backup - man weiß ja nie.

Vermeiden Sie jedoch die unüberlegte Aktualisierung anderer Programme und neuer "Spielzeuge", die sich Ihnen zum Download anbieten. Neue Versionen können die Leistung Ihres PCs überfordern und zum Absturz bringen. Programme aus unbekannten Quellen könnten sich als Spyware oder Trojanische Pferde herausstellen.

A.1 6.7 Originale

Verwahren Sie die Datenträger mit Ihren gekauften und ständig eingesetzten Programmen an einem Ort auf, wo Sie sie auch wieder finden. Dazu gehören auch die Passwörter der Hersteller. So können Sie nach einem fatalen Ausfall alle Programme wieder herstellen und Ihre Daten weiter verarbeiten.

A.1 6.8 Schnittstellen

Moderne Laptops bringen eine Fülle von physikalischen Schnittstellen mit. Schalten Sie die WLAN- und Bluetooth-Funktionen ab, wenn Sie sie nicht benötigen.

A.1 6.9 Funknetz

Nutzen Sie alle Sicherheitseinstellungen, die Ihr WLAN-Router bietet. Verteilen Sie feste IP-Adressen für alle Geräte, die Sie zulassen wollen, und verwenden Sie eine starke Verschlüsselung (WPA).

A.1 6.10 Fremdnetze und Angriffspunkte

Betreiben Sie keine ungeschützten Computer in ihrem Netzwerk.

Für kleine private Netze gilt: Geben Sie Ihren PC und ihren Drucker nicht für andere Mitglieder im Netzwerk frei. Wenn Sie sicher gehen wollen, tauschen Sie innerhalb der Gruppe die Daten entweder per Datenträger oder per E-Mail aus (Verringerung des Zeitfensters für eine Penetration).

A.1 6.11 mobiles Computing

Neben Verschleiß und Malware ist Ihr Laptop, das Sie mobil einsetzen, zwei weiteren wesentlichen Gefahren ausgesetzt: Diebstahl und unbefugte Nutzung.

Unbefugte Nutzung: Arbeiten Sie in der Öffentlichkeit niemals als Administrator.

Fahren Sie das Gerät vollständig runter, wenn Sie es vorübergehend - auch in beaufsichtigten Räumen - unbeobachtet zurück lassen müssen.

Ein "Spielkalb" oder böswilliger Mitmensch könnte ansonsten die viele Jahre lang in der Öffentlichkeit nicht bekannte Festplattenverschlüsselung aktivieren und für die Preisgabe des Ihnen dann unbekannten Kennworts eine gewisse Aufwandsentschädigung verlangen.

Sichern Sie Ihre wichtigsten Daten auf mobile Speicher (USB-Stick oder -Festplatte), die Sie bequem am Körper tragen können.

A.1 6.12 Hotspots. Öffentliche Funknetze

Öffentliche Hotspots für den bequemen Zugang zu einem WLAN per Laptop sind besonders anfällig dafür, dass der Ihnen unbekannte Betreiber oder ein Spion Ihren Datenverkehr mitschneidet oder sogar als Man-in-the-Middle agiert. Verarbeiten Sie vertrauliche Daten per mobile Computing nur in gesicherten Verbindungen (Virtual Private Network - VPN - mit Verschlüsselung).

A.1 7. verschiedene Nutzungen

A.1 7.1 Renate Mustermann und Otto Normalverbraucher

Für "einfache" Privatanwender reichen in aller Regel die oben genannten Sicherheitsvorkehrungen aus. Wichtig dabei ist, dass Sie sich fragen und bewusst machen, ob Sie mit personenbezogenen oder sogar sensiblen Daten arbeiten und welche Folgen Sie sich ausmalen, wenn diese missbraucht werden.

Private Netze und Funknetze lassen sich mit einem angemessenen technischen Aufwand kaum vollständig gegen Angriffe von außen absichern. Sie müssen im Allgemeinen keine Spionage-Hardware und keine Hacker befürchten, die sich "einfach mal umschauen wollen", wohl aber Malware und Hacking im Zusammenhang mit Ihren Kontodaten (Homebanking, eBay, Man-in-the-Middle).

Ihre Bemühungen müssen sich deshalb auf Ihr Arbeitsgerät, also Ihren PC oder Ihr Laptop konzentrieren. Vermeiden Sie deshalb technische Spielereien in Ihrem Netzwerk, besonders ständig erreichbare Netz-Festplatten und Server für die gemeinsame Dateiablage oder Backups.

Besondere Sicherungspflichten für Privatleute gibt es bislang nicht. Es entwickelt sich allerdings eine Rechtsprechung, die jedenfalls wegen grober Fahrlässigkeit Schadenersatzansprüche wegen unerlaubter Handlungen (§ 823 BGB) erwarten lässt.

Ungeachtet dessen vermeiden Sie persönlichen Ärger und finanzielle Verluste, wenn Sie Ihrer pri-

vaten Informationstechnik einen Grundschutz verpassen.

Das gilt besonders für private Funknetze. Der geduldete oder unbefugte Missbrauch Ihres Zugangs zum Internet führt zunächst zu Ihnen, weil von außen nur die IP-Adresse Ihres Routers bekannt wird, mit dem die Verbindung zum Internet aufgebaut wurde. Wegen Schadenersatzansprüche und strafrechtliche Ermittlungen wird man sich also zuerst an Sie als den Betreiber wenden.

Dasselbe müssen Sie befürchten, dass Ihre persönlichen Daten von einem Unbekannten zum Beispiel für unlautere Geschäfte bei eBay oder zu volksverhetzenden Präsentationen missbraucht werden.

A.1 7.2 berufliche und geschäftliche Datenverarbeitung

Bei der beruflichen oder geschäftlichen Datenverarbeitung unterliegen Sie weiter gehenden Sorgfaltspflichten als bei der reinen Privatnutzung, weil Sie Vertraulichkeits-, vertraglichen Partnerschutz-, Datenschutz- und firmenrechtlichen Handlungsanforderungen unterliegen können.

Vermeiden Sie deshalb den sorglosen Umgang mit ungeschützten Daten und machen Sie gelegentlich eine Risikoanalyse: Wen könnte ich mit der Preisgabe der bei mir gespeicherten Daten Schaden zufügen und wer könnte ein besonderes Interesse an der Erlangung dieser Daten haben?

Wenn Sie in Workgroups, also mit mehreren vernetzten Arbeitsplätzen arbeiten müssen, so vermeiden Sie möglichst den Anschluss an das Internet und errichten ein Kabelnetzwerk, kein WLAN. Auch der Aufwand, zwei Netzwerke aufzubauen, könnte den Aufwand lohnen. In dem einen, isolierten Netz verarbeiten Sie die sensiblen Daten, in dem anderen agieren Sie in der Öffentlichkeit. Vermeiden Sie dabei aber unbedingt unbedachte Schnittstellen, vor allem für die Telekommunikation, und Arbeitsplätze, die gleichzeitig mit beiden Netzen verbunden sind. Wenn Sie Daten zwischen beiden Netzen austauschen, verwenden Sie physikalische Datenträger und achten gleichzeitig darauf, dass auch das isolierte Netz hinreichend durch aktualisierte Virenscanner gegen Malware geschützt ist.

A.1 7.3 gewerbliche und professionelle Datenverarbeitung

Die Geschäftsführer und Vorstände von Kapitalgesellschaften unterliegen nach US-amerikanischem und europäischem Gesellschaftsrecht einer unmittelbaren Verpflichtung zur IT-Sicherheit. Verstöße und Schluderigkeiten können zu empfindlichen persönlichen Schadenersatzpflichten führen.

Aber auch die Leitungen und Sicherheitsverantwortlichen anderer großer Organisationen (z.B. Hochschulen, die als öffentlich-rechtliche Körperschaften in der Öffentlichkeit agieren) unterliegen erhöhten Anforderungen aus dem Datenschutz und als Träger privater Geheimnisse.

Die gewerbliche und professionelle Datenverarbeitung verlangt deshalb nach einer klaren Strategie zur IT-Sicherheit, nach geregelten Prozessen zum IT-Betrieb und nach einer ständigen Risikoanalyse. Die Einzelheiten ergeben aus dem Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik - BSI - und aus der einschlägigen Fachliteratur.

Wegen der IT-Architektur zeigt die übernächste Seite ein Beispiel, wie mit einer Demilitarisierten Zone und dem Einsatz von Firewalls eine Abschottung erreicht werden kann.

Im Hinblick auf die aufgezeichneten Angriffspunkte und -methoden kommen alle Gefahrenquellen in Betracht. Malware- und Hacker-Schutz ist dabei ein Massengeschäft, der Schutz der eigenen Geheimnisse ein weiteres beachtliches Aufgabengebiet. Konkurrenten und böswillige Angreifer könnten alle Register zum Ausforschen und Penetrieren bis hin zur Erpressung ziehen und auch vor Spionage- und terroristischen Attacken nicht zurück schrecken.

Das größte Sicherheitsrisiko stellt dabei der Mensch dar. Das können uninformierte, unbedarfte und bequeme Mitarbeiter sein, die Sicherheitsregeln nicht beachten oder bewusst umgehen, halbwissende Kollegen, die ihren "Spieltrieb" aus-

leben, oder ehemalige Mitarbeiter, die Ihr Wissen zu schädlichen Aktionen ausnutzen.

IT-Sicherheit beschränkt sich dabei nicht auf den Betrieb von Technik. Die Beispiele für das Social Engineering zeigen deutlich, dass auch das soziale Kommunikationsverhalten – nicht zuletzt mit Kunden, Partnern und in sozialen Netzwerken, die physikalische Sicherheit (Serverräume, Schließanlagen, Zugangskontrollen) und das allgemeine Sicherheitsverständnis aller Mitarbeiter gefordert sind.

A.1 8. Bestandteile eines professionellen Netzwerkes

In dem abschließenden Teil werfen wir einen groben Blick auf die professionelle Organisation von IT-Sicherheit. Sie verlangt nach einer klaren physikalischen Ordnung, um Quereinstiege und Hintertüren zu vermeiden.

A.1 8.1 professionelles Firmennetz

Ohne eine Firewall am unmittelbaren Netzeingang kommt kein professionelles Netzwerk aus. Erforderlich ist eine Hardware-basierende Firewall mit nur einem Eingang und einem Ausgang, die auch nur eine einzige Aufgabe hat: den aus- und vor allem eingehenden Datenverkehr zu überwachen, zu analysieren, nötigenfalls zu blockieren und ganz besonders alle Anstrengungen von außen zu unterbinden, protokollierend oder steuernd auf das Innere des Unternehmens Einfluss zu nehmen (im Schaubild: links oben, roter Block, FW1).

Im Hinblick darauf, dass immer mehr Dienste mit einem unmittelbaren Außenkontakt für E-Mail oder die Unternehmenspräsentation gefordert werden (Internet-Shopping, eGovernment), müssen Firewalls in einem gewissen Maße Außenkontakte zulassen. Es hat sich deshalb in der Praxis mehr und mehr durchgesetzt, dass vor der eigentlichen (produktiven) Unternehmens-IT eine besonders geschützte Zone errichtet wird, die nur für die Außenkontakte bestimmt ist (demilitarisierte Zone - DMZ; hellblau unterlegter Bereich).

Sie muss von der Unternehmens-IT mit einer weiteren und besonders restriktiv arbeitenden Firewall getrennt werden (links oben, roter Block, FW2).

Rechts oben ist im Bild ein sogenannter Honeypot vorgesehen. Es handelt sich dabei um eine Art Hinterzimmer, in dem interessante und in aller Regel falsche Daten bereit gehalten werden. Der Honeypot ist entweder durch keine Firewall geschützt oder durch eine, die verhältnismäßig einfach überwunden werden kann. Zu ihm und seinen "Spieldaten" sollen Angreifer gelockt werden, um sie von dem internen LAN abzulenken und bei ihren Handlungen beobachten zu können.

Ich halte das Honeypot-Konzept für eine informationstheoretische Spielerei mit mehreren Nachteilen: Es akzeptiert, dass sich Angreifer in der DMZ austoben und die dort vorgehaltenen, keineswegs unwichtigen Daten kompromittieren können. Dazu vernachlässigt es womöglich den sicheren Betrieb der Firewall "FW1" und verursacht wirtschaftlich fragwürdige Kosten für die Technik und den Betrieb des Honeypots.

A.1 8.2 Demilitarisierte Zone - DMZ

In der DMZ werden die Geräte und Dienste installiert, die einen unmittelbaren Außenkontakt benötigen. Untereinander werden sie mit einer (intelligenten) aktiven Netzwerkkomponente verbunden, einem Switch (oranger Block, Sw). Im Gegensatz zu "dummen Datenpumpen" (z.B. einem Hub) kann der Switch Datenverbindungen zielgerichtet lenken und zum Beispiel einem Hacker, der die Eingangs-Firewall überwunden hat (FW1), schwer behindern.

In die DMZ gehört auf jeden Fall der Webserver (gelber Block, WS), auf den die Kunden und die Öffentlichkeit zugreifen können. Je nach Bedarf muss ihm auch ein Datenbankserver zur Seite gestellt werden, der jedenfalls einen Teil der Unternehmensdaten enthält, die der Öffentlichkeit zugänglich gemacht werden sollen.

Im Beispiel ist auch der Mailserver in der DMZ platziert worden (gelber Block, MS). Seine Aufgaben können jedoch auch getrennt werden.

Dann werden nur die Funktionalitäten zum E-Mail-Versand in der DMZ vorgehalten, die Verwaltung der Postfächer für die Unternehmensangehörigen wird dazu in den geschützten Bereich verlagert, also ins Unternehmensinnere.

Die Entscheidung über die Architektur hängt ab von einer Abwägung zwischen den Risiken und den Kosten.

Im Beispiel ist auch der Proxy-Server (hellblauer Block, PS) in der DMZ. er verwaltet den Zugang der Mitarbeiter zum Internet und zwischenspeichert die Inhalte aus dem Internet. Auch seine Aufgaben können gesplittet werden. Dann dient er in der DMZ nur als Zwischenspeicher (Cache) und wird die Benutzerverwaltung im geschützten Unternehmensinneren geleistet.

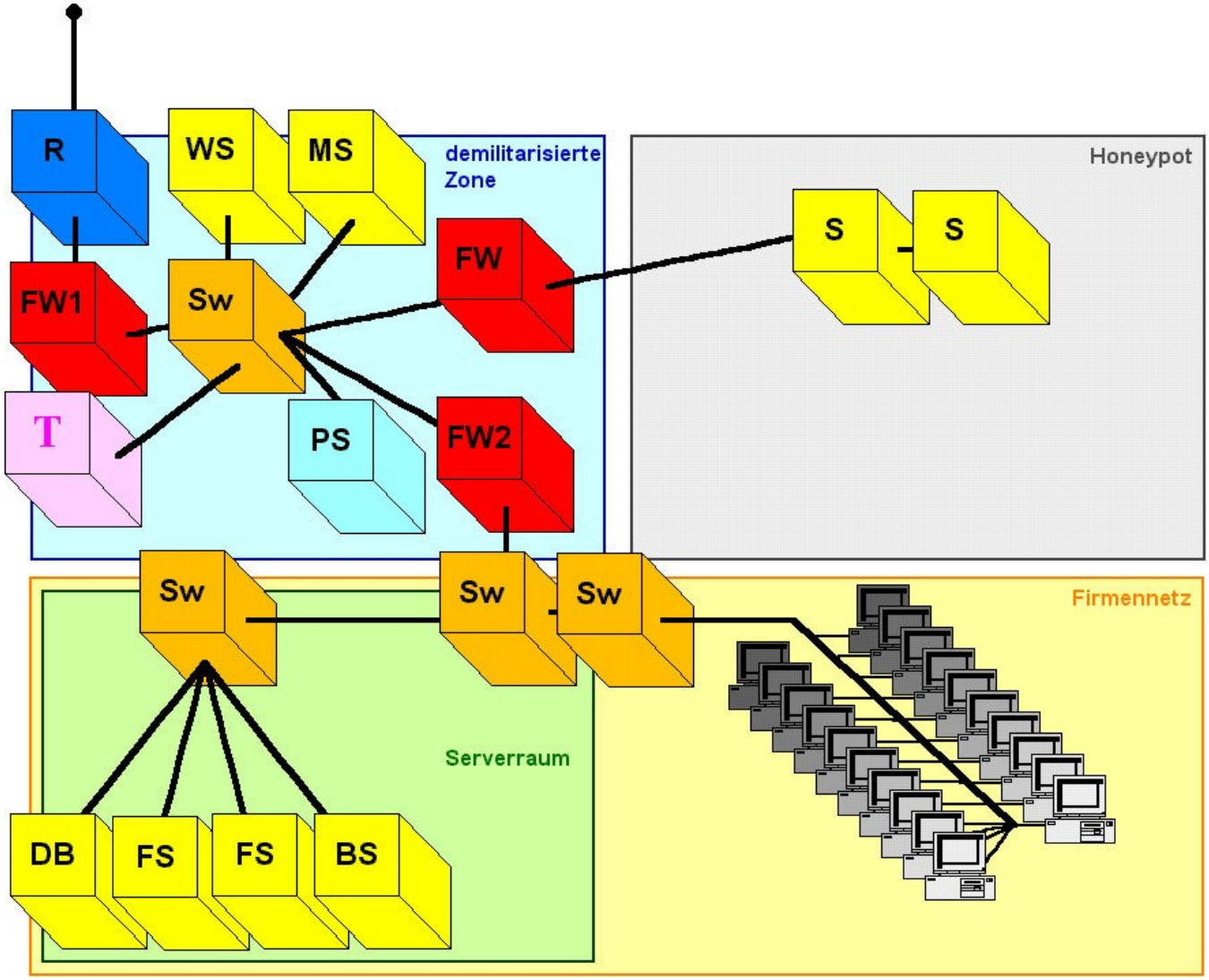
Aufgrund einer Risiko- und Wirtschaftlichkeitsuntersuchung muss auch entschieden werden, wo und wie der Server für die Telekommunikation eingerichtet wird (rosa Block, T). Auch insoweit kann es sich anbieten, nur die Vermittlungsfunktionen in die DMZ zu verlegen, die Verwaltung der eingehenden Faxe und Sprachnachrichten hingegen in den geschützten inneren Bereich des Unternehmens.

A.1 8.3 internes LAN

Die innere Firewall (FW2) muss so eingerichtet werden, dass sie wirklich nur die nötigsten Datenverbindungen zulässt.

Alle Daten, die schutzwürdig sind, gehören in den inneren, besonders geschützten Bereich. Das sind vor allem die Datenbanken und Dokumentensammlungen (gelbe Blöcke, DB und FS [Fileserver]) sowie die Ausfall- und Datensicherungskomponenten (gelber Block, BS [Backup]).

Diese technischen Einrichtungen gehören auch



nicht in irgendeine Abstellkammer, sondern in einen zugangsgesicherten Serverraum mit einer Klimaanlage, mit einer unabhängigen Stromversorgung - USV - und einer Zugangssicherung. Sie sind das Herzstück des Unternehmens (grün unterlegter Bereich).

Ausfallsysteme und das Archiv für die Datensicherungsspeicher gehören in einen räumlich weit getrennten Serverraum. Die beste Ausstattung für die Daten- und Ausfallsicherung nützt nichts, wenn ein Feuer oder ein brutaler Angriff beide auf einen Schlag vernichten kann.

A.1 8.4 Sicherheitsüberwachung

Neben der Sicherheits- und Firewalltechnik, allgemein zusammengefasst unter "Security", haben sich mehrere Modelle und Strategien etabliert, die sich der aktiven Sicherheitsüberwachung widmen.

Der Grundgedanke dafür ist, dass allein nur die Reaktion auf Sicherheitsgefahren nicht ausreicht, sondern dass Sicherheitsstrategien entwickelt werden müssen, die vorausschauend sind und die noch unbekannte Quellen für Beeinträchtigungen schließen oder zumindest überwachen, um gefährliche Ereignisse und Allgemeinumstände zu melden.

Die Palette dieser Maßnahmen reicht von der Serverraumüberwachung (Rauchmelder, Temperatur, Bewegungsmelder) über die Betriebsbereitschaft (Auslastung, Defekte) und die Netzverfügbarkeit bis hin zu Umweltmeldungen (Hochwasser- und Unwettermeldungen).

Für den IT-internen Bereich wurden verschiedene Techniken und Strategien entwickelt, um Angriffe und zufällige Belastungen zu erkennen und abzuwehren. An erster Stelle sind dazu die Methoden zur Intrusion Detection zu nennen, die sich der Erkennung, Beobachtung und Abwehr von Angriffen widmen. Sie benötigen eine ausgefeilte und teure Technik, haben aber zwei Zielrichtungen.

Die Erkennung von Angriffen gegen das IT-System ist wirtschaftlich notwendig (auch wegen der damit verbundenen Personalkosten). Ob es dazu auch eines Honeypots bedarf, um einen Angreifer in einer geschützten Umgebung mit banalen oder falschen Informationen zu beobachten, muss anhand der besonderen Bedürfnisse der Organisation entschieden werden. Im Allgemeinen dürfte der Honeypot nicht erforderlich und wirtschaftlich ineffektiv sein.

A.1 8.5 Sicherheitskultur und Akzeptanz

Das sicherste IT-System ist das, das den IT-Verantwortlichen den höchsten Grad an Kontrolle und den Mitarbeitern die geringste Möglichkeit zur Manipulation lässt. Das gilt nicht nur wegen mutwilliger Provokationen der Mitarbeiter, sondern vor allem deshalb, damit Malware und Hacker nicht die Systemrechte der Mitarbeiter für ihre Missbräuche ausnutzen können.

Sicherheitsbewusste IT-Organisationen neigen dazu, ihre eigenen Sicherheitsinteressen in den Vordergrund zu stellen und gleichzeitig die Sicherheitsinteressen anderer zu ignorieren.

eBay ist ein Beispiel dafür, das mir besonders aufgefallen ist und deshalb hervorgehoben wird. Dieses Unternehmen gibt umfassende Informationen an Strafverfolgungsbehörden, wenn sie sich eBay öffnen. Das widerspricht aber der Sicherheitsphilosophie der Polizei und der Staatsanwaltschaft, die gerne auch ihre eigenen IT-Systeme schützen wollen [56].

Eine Sicherheitskultur nach dem Grundsatz, "ich akzeptiere Deine Sicherheitsinteressen und Du meine", ist noch nicht hinreichend verbreitet.

Eine strikte IT-Organisation neigt zum Totalitarismus. Sie bevormundet die Anwender (zu Recht?), ist konservativ in dem Sinne, dass alle Neuerungen das funktionierende System beeinträchtigen könnten, und will die totale Kontrolle der Technik und ihrer Anwendung erreichen.

Solange Unternehmen und Behörden die IT-Organisation und ihre Ausrichtung nicht zu ihrem bestimmenden Unternehmensziel machen, werden sie die unternehmenspsychologischen und wirtschaftlichen Dimensionen nicht begreifen. Die Informationstechnik hat in den letzten beiden Jahrzehnten heftig dazu beigetragen, Arbeitsab-

[56] Siehe auch **CF**, Overlay-Netze der öffentlichen Verwaltung, 2008

läufe zu optimieren und die Produktivität zu erhöhen. Sie war willkommen, um wirtschaftliche Kennzahlen zu erreichen. Das hat sie getan.

Jetzt ist eine Umbruchsituation erreicht. Ohne IT können große (und ganz viele kleine) Organisationen nicht mehr handeln und wirtschaftlich tätig werden.

Dadurch werden die Folgekosten interessant.

Die Unternehmens-IT muss jetzt transparent und gestaltbar werden. Sie muss sich wandelnden Unternehmenszielen (Enterprise-Management) und den internen Unternehmensprozessen öffnen.

Die Unternehmensleitung und die Mitarbeitervertretung haben gemeinsame, aber auch elementar entgegengesetzte Interessen. Beide gilt es, auch im Hinblick auf die IT, zu bedienen und zu sichern.

Die Arbeitnehmerinteressen spielen für die Strategien zur IT-Sicherheit bislang keine Rolle. Das wird sich ändern müssen. Aber auch die Unternehmensleitungen werden im Hinblick auf ihre Unternehmensziele neue Perspektiven entwickeln müssen

Je weniger Einfluss die Mitarbeiter auf ihre Arbeitsumgebungen haben, desto größer sind die Möglichkeiten ihrer Unternehmensleitung, Arbeits- und Leistungskontrolle auszuüben (Big Brother).

Je mehr die Unternehmensleitung die Gestaltungs- und Zugriffsmöglichkeiten ihrer Mitarbeiter einschränkt, desto weniger Ideen, Innovationen und Genialitäten kommen ihr zu Gute. Gleichzeitig sinkt die Arbeitszufriedenheit.

Die Ära der Kostensenkung ist vorbei. Künftig ist es erforderlich, einen vernünftigen Ausgleich zwischen Unternehmensgewinnen, Arbeitnehmerinteressen und (neu) der IT-Sicherheit zu erlangen.

A.2 Nummerntricks

Adressenschwindel bei Telefondiensten und im Internet [57]

Die ersten Erscheinungsformen der Cybercrime im Zusammenhang mit der Digitalisierung der Telekommunikation [58] und der breiten privaten Nutzung des Internets konnten durch regulatorische, also durch gesetzliche Maßnahmen beschränkt werden. Das betrifft vor allem den schrankenlosen Missbrauch von Mehrwertdiensterufnummern aus dem 190-0-Rufnummernkreis, Dialer und die nur verhalten aufgetretenen Probleme im Zusammenhang mit kostenpflichtigen Rückrufen. Für alle drei Erscheinungsformen aus dem zurückliegenden und angehenden Jahrhunderten gilt, dass sie zurückgedrängt und erschwert wurden. Sie können in neuer Form wieder in Erscheinung treten, so dass sie in Erinnerung bleiben sollten.

Dieser Aufsatz widmet sich besonders den Adresssystemen der Telekommunikation und des Internets [59] unter dem Gesichtspunkt der Adressenmanipulation.

Die Einführung von Mehrwertdiensten ermöglichte es, unmittelbar über die Abrechnungen der Anschlussnetzbetreiber zu Geld zu kommen, ohne komplizierte Verwertungsmaßnahmen durchführen zu müssen, die wir vom klassischen Phishing [60] kennen: Ausspähen, Kontomissbrauch, Beutesicherung mit Finanzagenten.

Bei den neuen Formen der Cybercrime [61] ist zu beobachten, dass sie sich immer schneller wandeln und neu geschaffene Abwehrmethoden unterlaufen. Sie scheinen aus der Lernfähigkeit des Gesetzgebers ihrerseits gelernt zu haben, verdecken

Nummer	Beschreibung
110	Betreiberkennzahlen [62]
115	Einheitlicher Behördenruf
116	Harmonisierte Dienste von sozialem Wert (kostenlos)
118	Auskunftsdienste
12	Kurzwahl- und Neuartige Dienste (innovative Dienste)
137	Massenverkehr zu bestimmten Zielen: MABEZ (z.B. für das Televoting)
180	Geteilte Kosten (Shared Cost-Dienst - SC)
181	internat. Direktverbindungen; Internationale Virtuelle Private Netze
191 - 194	Online-Dienste
32	Nationale Teilnehmerrufnummern
700	Persönliche Rufnummern
800	Entgeltfreie Telefondienste
900	Mehrwertdienste; Premium-Dienste
9009	Anwählprogramme (Dialer), R-Gespräche, Premium-SMS

ihre kriminellen Aktivitäten und nutzen vermehrt die Methoden der heimlichen Geldwäsche als die des bargeldlosen Zahlungsverkehrs, der von Aufsichtseinrichtungen beobachtet wird und staatlichen Regulierungen unterworfen werden kann.

A.2 1. intelligente Nummernverwaltung

Die analoge Telefonie ist ein technisches Verbindungssystem, das sich auf die Schaltung von Einzelverbindungen in einem Netz beschränkt. Es kennt nur wenige Sondernummern wie die Notrufe 110 und 112, die in allen Ortsnetzen reserviert werden mussten. Abrechnungssysteme für Fremddienste, Rufnummernmitnahmen und besondere Dienste (siehe Tabelle oben) ließen sich damit nicht realisieren.

Die moderne Telekommunikation beruht auf intelligenten digitalen Netzen, die eine differenzierte Nummernverwaltung zulassen. Digitale Netze sind erst aufgrund des internationalen Standards

---

[57] Dieser Aufsatz vom 21.11.2008 führt einen Beitrag aus dem EDV-Workshop aus dem Jahr 2003 fort, aus dem einige der Beispiele stammen. Der Text wurde vollständig neu gefasst. Einzelne Passagen sind bereits an anderer Stelle im Cyberfahnder erschienen und werden hier zusammen gefasst.

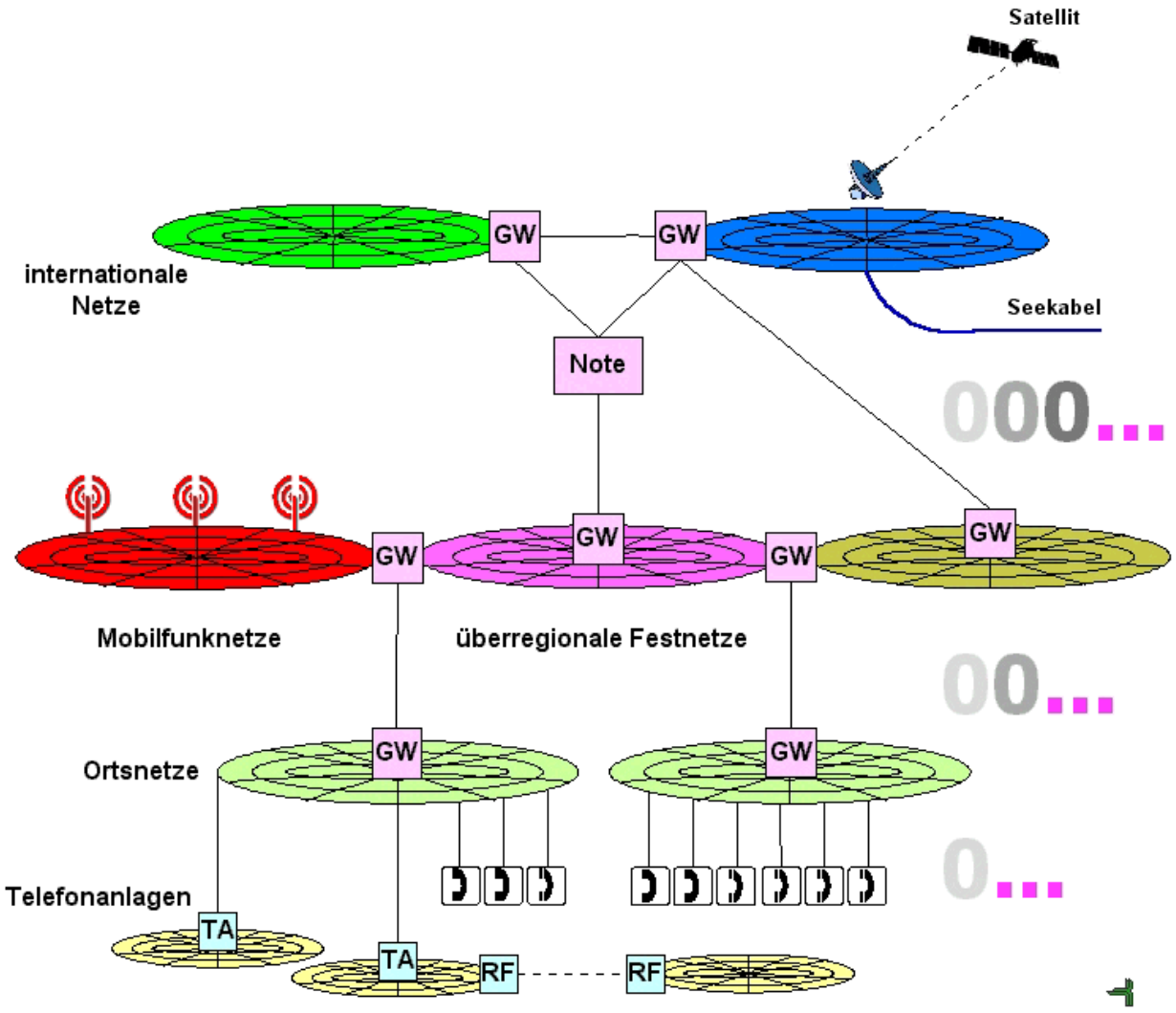
[58] Siehe auch: **CF**, Führung Cybercrime, 07.08.2008 und **CF**, Formen der IT-Kriminalität, 2007.

[59] Vertiefend zum Internet:
CF, internationale Kabel und Netze, 2007,
CF, autonome Systeme und Tiers, 2007,
CF, Namensauflösung im DNS, 2007.

[60] **CF**, Phishing mit Homebanking-Malware, 22.10.2008

[61] **CF**, Cybercrime und IT-Strafrecht, 08.08.2008

[62] Die Bundesnetzagentur hat ihren Webauftritt umgestellt, so dass die ursprünglich gesetzten Links nicht mehr zutreffen.



für ISDN [63] möglich, worauf die Deutsche Telekom seit 1989 ihr Telefonnetz umgerüstet hat. Vor allem zur breitbandigen Netzverbindung [64] wird ISDN seit den neunziger Jahren zusammen mit den DSL-Standards [65] betrieben, die besondere Anforderungen an die Leistungsfähigkeit der Verbindungsnetze stellen [66].

Intelligente Netze [67] benötigen zu ihrem Betrieb und ihrer Steuerung einer zentralen Daten- und Nummernverwaltung, die es ermöglicht, unabhängig von dem mechanischen Nummernsystem der klassischen, analogen Telefonie [68] Sondernummern und -dienste anzusteuern und abzurechnen. Dazu verlangt der ISDN-Standard, dass neben dem Sprachnetz, das für die Übertragung von Sprache und Daten verwendet wird, ein Signalisierungsnetz [69] besteht, das für den Verbindungsaufbau und ihren Bestand zuständig ist [70].

Die Tabelle (Vorseite) zeigt die wichtigsten Rufnummernblöcke, die für besondere und Premium-Dienste reserviert sind (Nummernverwaltung [71]).

Für die digitalen Anschluss- und Verbindungsnetze gilt, dass sie konvergent sind, also für die Sprach- und Datendienste gleichermaßen genutzt

63 **WP**, Integrated Services Digital Network - ISDN

64 Siehe **CF**, Netzneutralität und Breitbandtechnik, 08.12.2007, und **CF**, kollabiert das Internet? 13.09.2008.

65 **WP**, Digital Subscriber Line – DSL, siehe auch **CF**, DSL-Versorgung in Deutschland, 08.12.2007.

66 **CF**, Backbone der DTAG, 08.12.2007, **CF**, TK-Netze, 2007, **CF**, Roaming im Verbindungsnetz, 23.08.2008.

67 **WP**, Intelligentes Netz, **CF**, TK-Netze, 2007.

68 **WP**, Telefonnetz

69 **WP**, Signalisierungsnetz

70 **WP**, Festnetz-Struktur

71 **BNA**, Nummernverwaltung

werden können (Netzkonvergenz [72]). Für die Adressierung und Übertragung werden nur verschiedene Protokolle und Standards verwendet, die dieselbe physikalische Netzstruktur verwenden. Durch die Internettelefonie [73] (Voice over IP – VoIP [74]) ist selbst die protokollarische Trennung aufgehoben worden.

A.2 2. 1900-Nummern. Abrechnung. Missbrauch

Bis 2003 erregten die Mehrwertdienstenummer 190 und die Dialer eine besondere Aufmerksamkeit, weil sie häufig zu Missbräuchen genutzt wurden.

Das Besondere an der 190-0-Nummer war, dass diese Anschlüsse frei tarifierbar waren. Das heißt, dass der Anschlussinhaber mit seinem Netzbetreiber die Höhe der Verbindungskosten vereinbaren konnte. Meldungen über horrende Kosten für eine einmalige Einwahl oder für Zeitblöcke waren an der Tagesordnung.

Möglich machte das die Einführung von Premium Rate-Diensten, die zwei Gebührenanteile enthalten, einen für die Netzverbindung, der für die Netzbetreiber bestimmt ist, und einen mehr oder weniger großen, der an den Anschlussinhaber abgeführt wird.

Der Zweck der Mehrwertdienste besteht darin, die Telekommunikation zur Verbreitung und Abrechnung von Dienstleistungen zu nutzen und dem Dienstleistenden die Identifikation des Anrufers zu ersparen, indem die Abrechnung durch den Anschlussnetzbetreiber erfolgt. Gedacht war an Beratungsdienste (Rechtsanwälte, Lebenshilfe, Auskünfte, Testergebnisse) und zum Beispiel an die kostenpflichtigen Downloads zur Verbreitung von Dateien, Musik und Programmen. Bekannt wurden sie jedoch eher durch die instinktorientierten Angebote [75] werbender Damen.

Die Missbräuche von Premium Rate-Diensten erfolgten auf verschiedene Weisen: Täuschung über die Tatsache, dass ein solcher Dienst angerufen wird, kostenpflichtige Warteschleifen, Schlechtleistung und untergeschobene Dialer.

In der Anfangszeit der Mehrwertdienste kamen den Abzockern mehrere Mängel des Systems zu Gute: Jedenfalls der 190-0-Nummernkreis war wegen der Verbindungskosten nicht gedeckelt und es gab lediglich ein Verzeichnis - bei der damals noch: Regulierungsbehörde für Telekommunikation und Post - RegTP - über die Carrier, denen Teile aus dem Rufnummern-Block zugewiesen waren. Die Carrier hingegen bedienten sich bei dem Vertrieb der Anschlussnummern Reselern [76], die ihrerseits Unterhändler beauftragten und diese wiederum andere. Durch eine lange Kette solcher Unterhändler, die nicht selten ins Ausland reichte, konnte die Identität eines missbräuchlich handelnden Anschlussinhabers vollständig verschleiert werden.

Auch die Verteilung der Premium Rate-Gebühren ließ sich nicht immer leicht verfolgen. Ihre Abrechnung und ihr Einzug ist die Aufgabe des Zugangsnetzbetreibers (Carrier) gegenüber seinem Kunden (Anschlussinhaber). Dabei erfolgt die Abrechnung automatisch während der Verbindung aufgrund einer Rückmeldung des Inhabers des Rufnummernblocks, wobei es sich um einige wenige Carrier handelt, und der Zeittaktabrechnung des Anschlussnetzbetreibers, der die Gebühren gegenüber seinen Kunden abrechnet (die Anrufer).

Die Einnahmen mit Ausnahme des Anteils für die Verbindung führen die Anschlussnetzbetreiber an die anderen großen Carrier ab und diese, nach Abzug ihres Anteils, an die Inkassostellen der Reseller. Dadurch entstanden Verwertungsketten, die denen der Unterhändler-Ketten entsprachen und die sich ebenfalls nicht selten im fernen Ausland "verliefen".

---

[72] **CF**, Netzkonvergenz, 12.02.2008

[73] **CF**, Abgrenzungen, 2007

[74] **CF**, Formen der Quellenüberwachung, 08.11.2008

[75] **CF**, instinktorientierte Online-Angebote, 23.01.2008

[76] **WP**, Wiederverkäufer

A.2 3. Dialer

Dialer sind Einwahlprogramme, *mit deren Hilfe über das analoge Telefon- oder das ISDN-Netz eine Wählverbindung zum Internet oder anderen Computernetzwerken aufgebaut werden kann* [77]. Nach dieser allgemeinen Definition sind sie ein Hilfsmittel zur Unterstützung des Anwenders dabei, seinen PC in ein Netzwerk einzubinden oder internetfähig zu machen.

Die Kehrseite davon: Dialer sind auch in der Lage, neben bestehenden Netzwerkverbindungen solche zu anderen Zugangsprovidern einzurichten oder die Grundeinstellungen zu überschreiben.

Missbräuchlich (bis etwa 2003) eingesetzte Dialer funktionierten so, wie wir es heute von der Malware gewohnt sind, nur dass sie noch keinen modularen Aufbau kannten [78]. Zunächst mussten die Hemmungen des Anwenders überwunden oder das Dialerprogramm verdeckt installiert werden. Lautere Installationsprogramme geben dabei klar bekannt, welches die Auswirkungen ihres Einsatzes sind und vor allem, welche Kosten dadurch entstehen. Unlautere verschweigen das und versuchen, ihre Konfiguration an die Stelle der Standardeinstellungen zu setzen. Es gab Meldungen, wonach Dialer nach der Art der Trojaner mit anderen Programmen installiert wurden und dass sie sogar ihre Gestalt wechseln konnten: Ihre spätere Analyse zeigte, dass sie sich offen zu erkennen gaben, was sie bei der Erstinstallation tatsächlich nicht taten.

A.2 3.1 wider dem Missbrauch

Die Mängel im technischen System und seiner Organisation, die im Zusammenhang mit den Mehrwertdiensten angesprochen wurden, kamen auch den Dialern zu Gute, die in aller Regel mit einem Premium Rate-Dienst gekoppelt wurden [79].

Dank des Gesetzes gegen den Missbrauch von Mehrwertdiensten aus dem April 2003 [80] wurde den Missbräuchen weitgehend der Boden entzogen, indem die Bundesnetzagentur - BNA - mit der Regulierung beauftragt wurde. Sie richtete drei Datenbanken für die Registrierung von 900er- und 190er-Anschlüssen sowie für Dialer ein [81]. Ohne Registrierung können seither weder die Kosten für die Mehrwertdienstnummern noch für Dialer, jedenfalls im gerichtlichen Verfahren, geltend gemacht werden. Die Praxis zeigt, dass die BNA zwar so gut wie keine Kontrolle bei der Eintragung ausübt, aber sehr schnell dabei ist, auffällige Anbieter wieder zu löschen.

Gleichzeitig wurden die Belehrungspflichten verschärft und die Kosten gedeckelt. Seit 2006 können die 190-Nummern nicht mehr eingesetzt werden. In der Übergangszeit waren sie dadurch privilegiert, dass in der Datenbank bei der BNA nicht die Anschlussinhaber, sondern die Anschlussnetzbetreiber eingetragen waren.

Dialer sind seither fast ganz vom Markt verschwunden, aber ganz maßgeblich aus einem anderen Grund: Unter DSL funktionieren sie nur dann, wenn der PC neben einer DSL-Verbindung auch über einen Anschluss zum Telefonnetz verfügt. Das ist nur noch selten der Fall, etwa dann, wenn der PC auch für den Versand und den Empfang von Faxschreiben über das Telefonnetz genutzt wird.

A.2 3.2 rechtliche Handhabung

Die seinerzeit von mir im Gespräch mit anderen Kollegen entwickelte Handhabung und strafrechtliche Beurteilung der verschiedenen Dialer-Formen hat sich auch aus heutiger Sicht nicht geändert und kann auf Mehrwertdienste aus dem 900er-Nummernblock übertragen werden:

⇨ Erklärt die Menü- und Programmführung bei der Installation alle Funktionsweisen offen und deutlich - dass eine neue DFÜ-Netzwerkverbindung erzeugt oder eine bestehende überschrieben wird, dass alle künftigen Verbindungen über die 900er Nummer abgewickelt werden - und muss der Kunde die Installation bewusst mit

---

77 **WP**, Dialer

78 **CF**, Malware. Tarnung und Täuschung, 12.05.2008; **CF**, strafbare Vorbereitungshandlungen, 2007

79 **CF**, IT-Straftaten: Mehrwertdienste. Dialer, 2007

80 Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Mehrwertdiensterufnummern, 09.08.2003

81 **BNA**, Dialerdatenbank; **BNA**, 0900-Datenbank

einem Klick bestätigen, dann liegt gar keine Strafbarkeit vor.

⇨ Werden Teile der Funktionsweise weniger offen erläutert - also etwa der Umstand, dass künftig alle Internetverbindungen mit der teuren Nummer abgewickelt werden oder dass bereits die einmalige Verbindungsaufnahme zu unerwarteten Kosten in Höhe von mehreren 100 € führt, dann kommt in Anlehnung an die Rechtsprechung zum Offertenbetrug [82] § 263 StGB in Betracht (die Vermögensverfügung besteht in der unüberlegten, auf einer Täuschung beruhenden Installation des Programms; sie verwirklicht sich bei den künftigen, kostenauslösenden Einwahlen).

⇨ Werden Teile der Funktionsweise verschwiegen und erfolgt eine teilweise Installation ohne Kenntnis des Anwenders, so dürfte das eine Datenveränderung i.S.v. § 303a StGB sein (Veränderung der DFÜ-Verbindung oder - ganz gemein - der Registry-Eintragungen). Wird die DFÜ-Verbindung zum teuren Anschluss unbewusst vom Anwender hergestellt, so dürfte § 263a StGB zum Tragen kommen. Die heimliche Installation stellt dann den Beginn des Versuchsstadium dar.

⇨ Wird das Programm insgesamt heimlich oder sogar gegen den ausdrücklichen Willen des Anwenders gestartet (deaktivierter "Abbrechen"-Button), handelt es sich ebenfalls um eine Datenveränderung in Tateinheit mit versuchtem Computerbetrug. Die Abgrenzung zwischen Vorbereitungshandlung und Versuch muss im Einzelfall geklärt werden. Die Tat wird bei der nächsten Internetverbindung vollendet.

A.2 4. Regelungen im TKG

Die Abrechnungsmodalitäten sind jetzt in den §§ 45g, 45h TKG geregelt. Danach sind die Zugangsnetzbetreiber weiterhin verpflichtet, die Forderungen Dritter (aus Premium Rate-Diensten) in Rechnung zu stellen. Dabei müssen die Dritten einschließlich ihrer Kontaktdaten und kostenfreien Servicenummern genau bezeichnet und der Kunde darüber belehrt werden, dass er *begründete Einwendungen gegen einzelne in der Rechnung gestellte Forderungen erheben kann* (§ 45h Abs. 3 TKG).

13a.	§ 66a S. 1, 2, 6, 7 oder 8	unrichtige Preisangabe
13b.	§ 66a S. 3	zu kurze Preisangabe
13c.	§ 66a S. 4	unrichtige Hinweise
13d.	§ 66b Abs. 1 S. 1	unrichtige Preisansage
13e.	§ 66c Abs. 1 S. 1	unvollständige Preisanzeige
13f.	§ 66d Abs. 1 oder 2	Überschreitung der Preisgrenze
13g.	§ 66e Abs. 1 S. 1	verspätete Verbindungstrennung
13h.	§ 66f Abs. 1 S. 1	Einsatz unregistrierter Dialer
13i.	§ 66i Abs. 1 S. 2	Gespräch als Mehrwertdienst
13j.	§ 66j Abs. 1 S. 1 oder 3	unzulässiger Einsatz von Kurzwahlen

Der Nummerierung widmen sich jetzt die §§ 66 ff. TKG. Als Reaktion auf frühere Abzockereien sind eine Reihe von Verstößen bereits als Ordnungswidrigkeiten nach § 149 TKG verfolgbar (siehe Tabelle oben). Die BNA als Verwaltungsbehörde kann sie mit einer Geldbuße bis zu 100.000 € ahnden.

Auch in das neue Hackerstrafrecht [83] sind jedenfalls insoweit Schlussfolgerungen aus den früheren Missbräuchen eingeflossen, dass erhebliche Formen der Computersabotage - auch gegen Privatleute - nach § 303b StGB strafbar sind.

Zuletzt per 01.09.2007 sind weitere Änderungen im TKG vorgenommen worden [84], die besonders die Kostenklarheit und -begrenzung zum Gegenstand haben.

---

82 **CF**, Offertenbetrug, 02.08.2008

83 **CF**, Computersabotage, 2007

84 **CF**, mehr Preisangaben bei TK-Diensten, 28.08.2007

Die Telefongesellschaft Prompt hat den Rückruf als neue Einnahmequelle erschlossen. Für einen Anruf beim Kunden kassiert der Anbieter 0190-Gebühren. Der Ablauf ist einfach: Der Kunde ruft eine kostenfreie 0800-Rufnummer an und gibt dort die Nummer des Anschlusses an, auf dem er einen Rückruf wünscht. Anschließend erfolgt ein Anruf von Prompt - zu 0190-Konditionen. Den Posten findet der Angerufene anschließend auf der Telefonrechnung mit dem Stichwort TeleInternet Services ...

Eines der ersten entsprechenden Angebote, 'Recall Direct' der Firma EST24, ging im Juli in Betrieb. Nach Angaben der Firma handelte es sich nur um einen Testlauf, allerdings tauchten die entsprechenden Posten bereits auf Telefonrechnungen von Kunden auf. Bei EST24 konnte man während des Tests von jedem beliebigen deutschen Anschluss aus anrufen, sogar vom Handy. Der Anrufer erhielt eine Ansage mit dem Hinweis, dass der Rückruf kostenpflichtig sein werde und der Aufforderung, die gewünschte Telefonnummer im Festnetz einzutippen. An dieser Stelle nannte der Anbieter einen Minutenpreis von 1,99 Euro.

Urs Mansmann in c't 10/02, S. 94

A.2 5. kostenpflichtige Rückrufe

2002 tauchten einige wenige Meldungen über Missbräuche im Zusammenhang mit einem seinerzeit neuen technischen Dienst auf, bei dem die Verbindungs- und Dienstleistungsentgelte nicht dem Anrufer, sondern dem Angerufenen belastet wurden [85] (R-Gespräche; siehe Zitat oben).

Der mögliche Missbrauch dieser technischen Abrechnungsumleitung musste besonders jene vorsichtigen Mitmenschen schrecken, die bei ihrem Anschlussnetzbetreiber die Sperrung von Premium Rate-Nummern beantragt hatten. Das verhinderte aber nur die unbedachte ***Anwahl*** einer teuren Anschlussnummer, nicht aber den ***Anruf von*** einer solchen.

Der einzige mir in Erinnerung gebliebene Missbrauchsfall wurde ebenfalls von Mansmann in der c't berichtet [86], indem er ein Behindertenwohnheim vorstellte, in dem alle Telefone für abgehende Anrufe gesperrt waren. Einer der Bewohner forderte jedoch per Handy Rückrufe auf sein stationäres Telefon an, die schließlich mit Kosten von rund 440 Euro zu Buche schlugen.

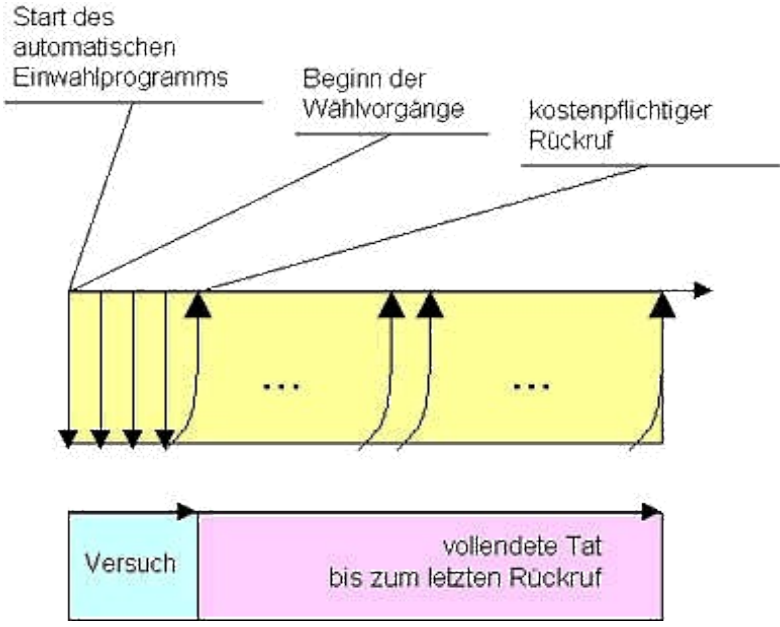
Derartige Fälle werden jetzt von § 66i TKG unterbunden.

A.2 6.1 Rückruftrick

Die erfolgreiche Regulierung hat die extremen Auswüchse verschwinden lassen. Missbräuche von Mehrwertdiensten werden dadurch aber nicht völlig verhindert.

Eine besonders dreiste Form des Rückruftricks wurde 2002 publik und kann sich jederzeit wiederholen [87]. Von den kostenpflichtigen Rückrufen unterscheidet sich diese Fallgruppe dadurch, dass der Anrufer zu einem eigenen Handeln aufgerufen wird.

Der Inhaber von mehreren Mehrwertdienstenummern startete auf seinem Computer ein Programm, das den D1-Nummernkreis systematisch anwählte und die Verbindung sofort wieder unterbrach. Das reicht aber für die Meldung "Anruf in Abwesenheit" auf dem Handy. Nur wenige der Empfänger wählten den Anrufer an und bekamen das Freizeichen zu hören, so als wenn keine Verbindung zustande gekommen wäre. Das Freizeichen stammte jedoch vom Tonband und der Gebührenzähler lief. Sehr lukrativ. Der Täter wurde



[85] Urs Mansmann in c't 10/2002, S. 94 und c't 22/2002, S. 46

[86] Urs Mansmann, Erste Rückruf-Opfer. Die neue 'Mehrwert'-Masche bringt schon Profit, c't 22/2002, S. 46

[87] 0190-Betrug: Jetzt mit "gefälschten" Freizeichen, Heise online 07.08.2002

später wegen Betruges (§ 263 StGB) zu Freiheitsstrafe verurteilt

Mit der zunehmenden Neigung, ständig erreichbar zu sein [88], steigt auch die Gefahr, dass die Leute auf solche Tricks hereinfallen.

A.2 6.2 einheitliche prozessuale Tat

Eine wichtige strafrechtliche Konsequenz weist der geschilderte Fall auf, die auch für den Massenversand von Spam- und Phishing-Mails gilt: Der Täter handelt nur einmal, indem er den Versand von Nachrichten startet. Die potentiellen Opfer sind aber breit in der Fläche verstreut. Wenn sie mit einer Verzögerung von mehreren Wochen mit ihrer Telefonrechnung zur Polizei gehen, um einen Betrug anzuzeigen, werden sie zu ihrer örtlichen Polizei gehen, die womöglich sogar den Inhaber der Mehrwertdienstenummer ermittelt und die Akten an die Staatsanwaltschaft abgibt.

Der überschaubare Schaden, den der einzelne Anzeigeerstatter erlitten hat, könnte den zuständigen Staatsanwalt dazu veranlassen, das Ermittlungsverfahren gegen eine geringe Geldauflage vorläufig gemäß § 153a StPO einzustellen. Zahlt der Täter die Buße, dann tritt wegen aller anderen Geschädigten Strafklageverbrauch [89] ein (Art. 103 Abs. 3 Grundgesetz - GG), weil alle Schadensereignisse auf das Einmal-Handeln des Täters beim Start des Computerprogramms zurück gehen. Sie beruhen auf einer einheitlichen prozessualen Tat (§ 264 Abs. 1 StPO).

Wegen solcher massenwirksamen Handlungen von Straftätern wird sich die Strafverfolgung zunehmend sensibilisieren müssen.

A.2 7. versteckte Netz- und Auslandsvorwahlen

Eine Masche aus optischen Werbemedien funktioniert noch immer: Das Verstecken verdächtiger Anschlussnummern in einem Rattenschwanz aus Ziffern.

Im ersten Beispiel wird die Mehrwertdienstnummer hinter der deutschen Auslandsvorwahl versteckt, wobei zusätzlich die Gruppierung der Ziffern von dem verräterischen String ablenken soll.

004 - 990 - 012 - 345 - 678 - 901	
Auflösung der Ziffernfolge:	
Auslandsvorwahl:	0049
Premium Rate-Dienst:	900
Anschlussnummer:	1234567..

Das zweite Beispiel ist eine Variante, bei der die Netzvorwahl der DTAG verwendet wird. Hierbei wird außerdem die verdächtige Nummer dadurch versteckt, dass eine ununterbrochene Ziffernfolge präsentiert wird.

Um die Verwirrung zu erhöhen müssen nur noch ein paar Ziffern an die Anschlussnummer angefügt werden. Häufig konnten jedenfalls die Anschlussnetzbetreiber keine Auskunft über den Inhaber des Anschlusses geben.

0103390012345678 90	
Auflösung der Ziffernfolge:	
Netzvorwahl:	01033
Premium Rate-Dienst:	900
Anschlussnummer:	1234567..

Auch für Auskunftsdienste und Kurzwahlnummern können neben den Verbindungskosten Dienstleistungskosten erhoben werden [90]. Über einen Missbrauchsfall berichtete die Neue Presse bereits 2002 [91]. Dasselbe gilt grundsätzlich für

[88] **CF**, Kommunikationsflut, 29.10.2007

[89] **WP**, Strafklageverbrauch

[90] Tabelle S. 24.

[91] Neue Presse, 11845 - Die neue Abzocke per Telefon, 04.10.2002 (Zitat auf der Folgeseite).

11845 - Die neue Abzocke per Telefon

Das Landeskriminalamt (LKA) warnt vor einer neuen Telefonbetrugs-Masche.

"Die Täter antworten auf Zeitungsanzeigen und bitten die Inserenten auf Mailbox und Anrufbeantworter um einen Rückruf", sagt LKA-Sprecher Frank Federau. Dazu geben sie die Kurzwahlnummer 11845 an.

Das Problem: "Wer diese Nummer wählt, tritt in die Kostenfalle", so Federau. Denn dort melde sich ein angeblicher Telekom-Auftragsdienst. Der Anrufer werde in eine aussichtslose Warteschleife geschickt - und die kostet 1,99 Euro pro Minute. Der gewünschte Teilnehmer werde nicht erreicht. Nach Auskunft der Telekorn hat das Unternehmen nichts mit der Servicenummer zu tun. ...

Neue Presse, 04.10.2002

MABEZ-Nummern [92], die jedoch nur vorübergehend und gezielt von der BNA vergeben werden.

Über die Verwendung einer sehr teuren Verbindung kann man auch täuschen, indem man als Rückruf-Nummer eine Auslandsvorwahl angibt, die teure Tarife möglich macht. Dies gilt z.B. fürdie Salomonen mit der Vorwahl +677 oder 00677 [93]. Auch Nauru mit der Vorwahl ... 674 ist als Netzadresse eines automatischen Dialers bekannt geworden, der seit der Nacht zum 23.11.2002 den Rufnummernbereich des Mobilfunkproviders O2 mit Kurzanrufen abarbeitete. Dies war die dritte Rückrufserie unter Verwendung von Naurus Netzvorwahl, die seinerzeit bekannt geworden war.

Welche Ländervorwahlen seit 2002 noch hinzu gekommen sind, habe ich nicht verfolgt.

Die bereits älteren Beispiele zeigen, wie ungeläufige technische Funktionen mit betrügerischen Tricks verbunden werden können, um die Opfer zu übertölpeln. Die oben angesprochene, optische Tarnung kann noch dadurch verstärkt werden, dass gemeinhin unbekannte Vorwahl- oder Dienstenummern verwendet werden. Das gilt jedenfalls für die Auskunftsdienste, die sich inzwischen ebenfalls stark auf instinktorientierte Auskünfte konzentriert haben, die Kurzwahl- und (eingeschränkt) die MABEZ-Nummern sowie die exotischen Auslandsvorwahlen.

[92] Massenverkehrsnummern für das Televoting.

[93] c't 10/02, S. 39

A.2 8. kriminelle Verbindungen

Die bisherigen Beispiele sind darauf ausgerichtet gewesen, den Anschlussinhaber zu täuschen und dazu zu veranlassen, teure Verbindungen aufzunehmen. Sie ähneln den Trickbetrügereien, die vom Täter handwerkliches Geschick verlangen [94]. Zwei Hacking-Beispiele sollen das Bild abrunden.

Fernwartungsfähige Telefonanlagen sind anfällig für Angriffe von außen. Lassen sie die Fernwartung zu und sind die Grundeinstellungen der Hersteller "offen", so fällt es Hackern leicht, über den ISDN-B-Kanal die Anlage zu manipulieren und z.B. so einzustellen, dass die Anlage selbsttätig anstelle von Mitteilungsdiensten, die die aktuellen günstigsten Fernverbindungen übermitteln, teure Mehrwertdienstenummern anruft. In einem schon 2002 bekannt gewordenen Fall sind dadurch Kosten in Höhe von 4.000,- Euro verursacht worden [95]. Daneben sind sie auch anfällig gegenüber gebräuchlichen Angriffsmethoden: Telefonanlagen sind immer "intelligenter" im informationstechnischem Sinne geworden und können wegen ihrer Steuerung unbekannte Sicherheitslücken aufweisen. Dadurch sind sie anfällig gegen Brute Force-Angriffe [96] und Buffer Overflows [97].

Über einen eher seltenen Fall hatte das Landgericht Hannover zu befinden. Es ordnete am 25.06.01 - 33 Qs 123/01 - als Beschwerdegericht die Untersuchungshaft gegen einen Beschuldigten an, dem 47 Straftaten des Computerbetruges (§ 263a StGB) mit folgenden Besonderheiten vorgeworfen wurden:

[94] Das gilt auch für andere Kriminalitätsformen, z.B. für das von mir, jedenfalls begrifflich, eingeführte **CF**, Proll-Skimming, 18.05.2008.

[95] Betrug per TK-Anlage, c't 24/2002, S. 71

[96] Bei **WP**, Brute-Force-Angriffen wird eine passwortgesteuerte Zugangssicherung so lange mit neuen Passwörtern penetriert, bis die zutreffende Kombination gefunden ist; siehe **CF**, Passwörter und Sicherungscode, 2007.

[97] Buffer Overflow: **WP**, Pufferüberlauf. Hierbei wird der Arbeitsspeicher eines Zielsystems mit einer Vielzahl von Verarbeitungsanfragen überlastet. Im Gegensatz zum verteilten Angriff (**CF**, Sommer 2007; DoS), mit dem der Absturz des Zielsystems bezweckt wird, ist beim Buffer Overflow den Anfragen Schadcode beigefügt, der vom überlasteten System ausgeführt werden soll.

Der dem Beschuldigten zur Last gelegte Sachverhalt ist als Computerbetrug in der Tatbestandsalternative des "unbefugten Verwendens von Daten" im Sinne des § 263a StGB strafbar. Das Herstellen der Telekommunikationsverbindung, entweder vom Festanschluss ... oder vom Mobiltelefon des Geschädigten O. ..., ist als Datenverarbeitungsvorgang zu werten.

Denn bei der Herstellung solcher Verbindungen handelt es sich um automatisierte Vorgänge, bei denen durch Aufnahme von Daten und deren Verknüpfung Arbeitsergebnisse - namentlich gebührenpflichtige Telekommunikationsverbindungen - erzielt werden. Über eine bloße Manipulation an der Hardware gehen die Tathandlungen des Beschuldigten demnach hinaus.

Der Beschuldigte hat diesen Datenverarbeitungsvorgang missbraucht, indem er als Unbefugter die Daten, die zur Herstellung der Verbindungen vom jeweils konkret genutzten Anschluss zu der von ihm betriebenen 0190ger Telefonnummer notwendig waren, eingesetzt hat, obwohl er zur Herstellung dieser Verbindungen nicht berechtigt war. Berechtigt waren die M.-Hotelgesellschaft in den Fällen in denen Verbindungen von hoteleigenen Anschlüssen hergestellt wurden; bzw. in den Fällen in denen die Telefonverbindungen vom Mobiltelefon aus erfolgten, der Geschädigte O. Eine vertragliche Befugnis, die jeweiligen Telefonanschlüsse in irgendeiner Form zu nutzen, hatte der Beschuldigte nicht.

... Im vorliegenden Fall ist Grundlage der Taten dagegen eine verbotene Eigenmacht des Beschuldigten. Dem Beschuldigten ist letztlich im Rahmen der Begrenzung des weit gefassten Tatbestandsmerkmals "unbefugt", welches jedes vertragswidrige Verhalten umfassen würde, ein betrugsspezifisches Verhalten zur Last zu legen. Geschäftsgrundlage eines jeden Telekommunikationsvertrages ist die in diesem Rahmen bestehende Berechtigung zur Nutzung der Anlage sowie der Inanspruchnahme der daraus resultierenden Leistung. Gehört aber die Befugnis des Täters zur Inanspruchnahme der Computerleistung zur Geschäftsgrundlage, ist das Schweigen über den Mangel der Befugnis als schlüssiges Vorspiegeln der Verwendungsberechtigung zu werten. Dies ist vorliegend der Fall. Der Umstand, dass der Beschuldigte keinen Zugangscode überwinden musste, weil sowohl die Telefonanlage im Hotel als auch das Mobiltelefon freigeschaltet waren, spielt dabei keine Rolle, weil die Eingabe eines bestimmten Zugangscodes nur eine besonders evidente Form der Täuschung über die Berechtigung darstellt.

Beschluss des LG Hannover vom 25.06.01 - 33 Qs 123/01 (Vermerk des Kammervorsitzenden, Auszug)

Der Beschuldigte war als Kontrolleur einer Putzkolonne in einem Hotel tätig. Er ließ sich zunächst eine 0190-Servicenummer einrichten. Im Mai 2001 benutzte er unberechtigt verschiedene Telefongeräte des Hotels und das Handy eines Hotelgastes, um seine kostenintensive Servicenummer anzurufen. Die dadurch entstandenen Gebühren in Höhe von mehreren tausend DM wurden seinem Konto gutgeschrieben (siehe links).

A.2 9. Adressierung im Internetprotokoll

Verschleierungen wie bei den versteckten Vorwahlnummern sind auch im Zusammenhang mit Internetadressen möglich. Die Requests for Comments – RFC [98]– dienen zur Standardisierung der Internet-Technik und damit zur Vereinheitlichung der üblichen Anwendungen und Dateiformate. Der RFC 2396 widmet sich dem Uniform Resource Locator – URL [99], also dem Kernstück der Adressierung im Internetprotokoll [100] und dem Domain Name System – DNS [101].

Die danach üblichen Adressen weisen eine einheitliche Struktur auf:

http://www.cyberfahnder.de	
Auflösung der DNS-Adresse:	
Hypertext Transfer Protocol [102]:	http
World Wide Web [103] (Netz):	www
Second Level Domain [104]:	cyberfahnder
Top Level Domain [105]:	de

Die Auflösung dieses Adressen-Strings erfolgt jedoch von rechts nach links, also vom Namensraum ausgehend, und die Punkte sowie "://" dienen als Feldtrenner. Rechts daneben können noch Unterverzeichnisse und Dokumente ange-

98 **WP**, Request for Comments - RFC
99 **WP**, Uniform Resource Locator - URL
100 **WP**, Internet Protocol
101 **CF**, Auflösung von DNS-Adressen, 2007
102 **WP**, Hypertext Transfer Protocol - HTTP
103 **WP**, World Wide Web - WWW
104 **WP**, Second Level Domain - SLD
105 **WP**, Top Level Domain - TLD

geben werden, links neben der SLD weitere Subdomains.

Als Feldtrenner für die Unterverzeichnisse dient der Schrägstrich. Dagegen werden die Subdomains [106] mit Hilfe von Punkten in den String eingeführt.

Unterverzeichnisse und Dokumente:
http://www.kochheim.de/cf/nav/impressum.htm
Subdomain:
http://www.dokumente.cyberfahnder.de

RFC 2396 eröffnet aber auch die Möglichkeit, Zusatzinformationen zur Steuerung von Prozessen und zur Identifikation (Zugangsberechtigung, Rechtesteuerung) anzufügen. Sie erscheinen dann links vom Domänennamen.

Der wichtige Feldtrenner ist dabei das Arroba-Zeichen: @ [107]. Es bewirkt, dass für die Adressierung nur der String rechts von ihm verwendet wird. Der linke Teil des Strings wird ignoriert, weil er nur für die Zielanwendung bedeutsam ist.

Kontozugang:
http://Konto%7c:Kennwort@www.cyberfahnder.de

Das europäisch geprägte Auge schaut jedoch weniger zum (rechten) Ende einer Zeichenkette, sondern eher zu ihrem (linken) Anfang. Deshalb lassen sich ihrem rechten Teil Adressangaben verstecken, wenn am Beginn des Strings unverdächtige Angaben gemacht werden.

Dieser URL führt nicht zu "meine-Bank.de" sondern zu "abzocker.ru".

Täuschung über Zieladresse:
http://meine-bank.de/zugang@www.abzocker.ru

Eine Abwandlung dieses Tricks wird auch im Zusammenhang mit E-Mail-Anhängen verwendet. Eine Programmdatei, die Malware installieren soll, verrät sich zum Beispiel durch ihre Endung ".exe" (für execute, deutsch: ausführen). Wenn man einem Dateinamen jedoch unverdächtige Endungen anfügt, dann kann der unbedarfte Anwender über die Gefährlichkeit der Datei getäuscht werden.

Im folgenden Beispiel handelt es sich nicht um eine (auch nicht ganz harmlose [108]) PDF-Datei, sondern um ein Programm, das alles Mögliche anstellen kann.

Täuschung über das Dateiformat:
Rechnung.pdf.exe

Dieser Trick funktioniert noch viel besser, wenn der Anwender eines der WindowsBetriebssysteme nutzt, bei der die echte Endung eines Dateinamens ausgeblendet wird. Er sieht dann nur: Rechnung.pdf.

Die Liberalisierung für die Gestaltung von Dateinamen, die vor 15 Jahren von Windows 95 eingeführt wurde, hat auch ihre Kehrseite. Anwenderfreundlichkeit wendet sich sehr schnell zur Gefahr.

Zur Tarnung von DNS-Adressen werden inzwischen auch die verschiedenen Zeichensätze verwendet, die im Internet zugelassen sind. Bei der Homograph Spoofing Attack wird zum Beispiel das kyrillische „а“ anstelle des lateinischen „a“ im Domainnamen verwendet. Die westeuropäisch eingestellten Browser zeigen beide identisch an. Tatsächlich bestehen die Namen aber aus verschiedenen Zeichenfolgen; zum Beispeil: PayPal [109].

[106] **WP**, Subdomain

[107] **CF**, Ät, 10.01.2008

[108] **CF**, Tarnung und Täuschung, 12.05.2008

[109] **CF**, Homograph Spoofing Attack, 17.05.2010; siehe Kasten auf der Folgeseite

Bemerkenswert ist, dass die APWG bislang nur sehr wenige sogenannte Homograph Spoofing Attacks im Zusammenhang mit der Unterstützung des International Domain Name (IDN) beobachtet hat. Dabei sehen Zeichen in einer URL zwar richtig aus, sind es aber nicht. Beispielsweise werden ein kyrillisches a und ein lateinisches a von den meisten Zeichensätzen grafisch gleich dargestellt, obwohl es sich um unterschiedliche Zeichen handelt (look alike character). Diesen Umstand könnten Phisher bei Adressen wie www.paypal.com prinzipiell zur Täuschung benutzen. Die APWG vermutet, dass Phisher nicht darauf zurückgreifen, weil der Domainname ohnehin keine Rolle spiele – offenbar prüfen Anwender URLs immer noch nicht sorgfältig genug. [110]

A.2 10. Umleitungen im Internet

Die bislang vorgestellten Täuschungen bei der Adressierung im Internet zielen darauf ab, dass der Anwender unbedarft handelt. Sie sind Methoden des Social Engineering, also der Suggestion und der Manipulation.

Die moderne Malware [111] manipuliert informationstechnische Verarbeitungsvorgänge hingegen im Geheimen, unbemerkt und fatal. Ihre bevorzugten Ziele sind korrumpierte Internetseiten, der Verarbeitungsvorgang im laufenden Betrieb eines PCs und schließlich sein Systemstart.

Manipulationen beim Systemstart setzen voraus, dass die Schadsoftware das Zielsystem bereits infiziert hat, ohne sich (bislang) einnisten, also installieren zu können. Die Malware (der Starter) wartet darauf, zusammen mit einem normalen Systemstart in das System eindringen zu können. Anfällig dafür sind innere Komponenten, die Speicherfunktionen haben [112], und Netzkomponenten, die regelmäßig angesprochen werden [113]. Bei die-sen Geräten handelt es sich selber um "intelligente" informationsverarbeitende Systeme, die ihrerseits infiziert sein und den Startvorgang zur Infiltration nutzen können [118].

Der Zugriff auf das Internet erfolgt nicht nur dadurch, dass der Anwender seine E-Mails oder im Browser Webseiten aufruft. Viele Programme machen das auch selbsttätig, um nach neuen Meldungen, Virensignaturen oder Programmversionennachzufragen. Solche vom PC zugelassenen Netzkontakte lassen sich prinzipiell auch von der

DNS-Poisoning

Diese Methode setzt voraus, dass der PC bereits mit Malware infiziert ist. Sie verändert die Eintragungen in der lokalen Hostdatei [114], die dazu dient, die DNS-Namen [115] häufig besuchter Webseiten in ihre nummerische Adresse für das Internetprotokoll umzuwandeln. Das gemeine daran ist, dass der PC zunächst die Hostdatei danach fragt, ob ihr die gesuchte IP-Adresse bekannt ist, ohne die DNS-Server im Internet abzufragen. Enthält sie veränderte Daten zum Beispiel für das Internet-Banking, werden sie automatisch zu einer nachgemachten Webseite geführt, die Ihre Bankdaten ausspioniert (zum Beispiel durch einen Man-in-the-Middle-Angriff [116]).

serverbasiertes DNS-Poisoning

Das serverbasierte DNS-Poisoning ähnelt der ersten Variante, nur dass hierbei die DNS-Tabellen eines häuslichen Netzes oder eines Zugangsproviders korrumpiert werden. Besonders unauffällig sind Manipulationen an den den Netzkomponenten kleiner häuslicher oder betrieblicher Netze, weil sie in aller Regel einmal eingerichtet, kaum überwacht und deshalb vom Anwender bald nicht mehr als Gefahrenquelle wahrgenommen werden [117].

Die Host-Tabellen großer Zugangsprovider sind zwar schon Opfer von Angriffen geworden. Bei ihnen ist jedoch die Kontrolldichte höher, so dass die Manipulationen schneller bemerkt und korrigiert werden.

---

[110] Daniel **Bachfeld**, Einzelne Bande war für zwei Drittel aller Phishing-Angriffe verantwortlich, Heise online 17.05.2010

[111] **CF**, Phishing mit Homebanking-Malware, 22.10.2008

[112] Neben den Komponenten für den Startprozess (**WP**, Basic Input Output System - BIOS, **WP**, Bootbereiche von Speichermedien) können dazu auch Peripheriegeräte wie die Grafik-, Sound- und TV-Karten missbraucht werden, die alle wegen ihrer Funktionstüchtigkeit angesprochen werden.

[113] **WP**, Router, **WP**, Switch, **WP**, Wireless LAN

[114] Unter Windows: C:\WINDOWS\system32\ drivers\etc\lmhosts; siehe auch Namensauflösung.

[115] **CF**, Auflösung von DNS-Adressen, 2007

[116] **CF**, The Man-in-the-Middle, Sommer 2007

[117] **CF**, Umleitungen zu manipulierten Webseiten, 09.12.2008

[118] Trojaner konfiguriert Router um, Heise online 13.06.2008; siehe auch **CF**, Malware. Betriebssystem, 12.05.2008

iframe-Umleitung

Hierbei werden die Suchfunktionen auf Webseiten missbraucht, wenn sie die von ihnen vermittelten Suchanfragen für Google zwischenspeichern. Danach ist es möglich, in die Adressen auf der Ergebnisseite von Google "iframe-Tags" einzuschmuggeln [119]. Iframes sind dazu eingeführt worden, um auf einer Webseite Bereiche festzulegen, in denen fremde Dateien (zum Beispiel Werbung) eingeblendet werden können. In Verbindung mit DNS-Adressen werden die Browser jedoch auf eine Seite geführt, die der Angreifer bestimmt (Drive-By-Download). *Dort werden dann Antivirenprogramme oder Video-Codecs zum Download angeboten, in denen allerdings der Trojaner Zlob stecken soll* (Heise online).

Eine neue Variante soll statt iframes JavaScript in die Ergebnislisten injizieren [120].

gehackte Webserver

Dynamische Webseiten werden auf eine Abfrage jeweils neu zusammen gestellt. Dadurch kann das Erscheinen von Artikeln, Werbeeinblendungen und Aktualisierungen zeitlich gesteuert und angepasst werden. Die Bestandteile der Webseite sind dabei in einer Datenbank gespeichert (Content Management System).

Wenn die Datenbank gehackt wird, kann in der neu generierten Seite auch Schadcode eingebettet werden [121].

Malware missbrauchen.

Eine kriminelle Variante davon ist das DNS-Poisoning, bei dem die lokale Hostdatei manipuliert wird (siehe Kasten), um unbemerkt auf präparierte Internetseiten umzuleiten. Diese Methode ist besonders im Zusammenhang mit der Weiterentwicklung des Phishings [122] zum Pharming [123] und bei der Infiltration mit Botsoftware bekannt geworden.

Die angesprochenen Manipulationsmethoden dienen dazu, entweder

⇨ den Anwender auf nachgemachte Webseiten zu locken, um seine privaten Daten abzugreifen [124],
⇨ einen Starter für die Installation mit Malware einzuschleusen oder
⇨ die Malware direkt in das Zielsystem einzubringen.

Ein Beispiel für das serverbasierte DNS-Poisoning wurde 2008 bekannt [125], wobei ein DSL-Router auf einen vorgegaukelten DHCP-Server [126] im lokalen Netz umgeleitet wird, der seinerseits mit einem externen DNS-Server verbindet [127].

A.2 11. Angriffe gegen Webserver und CMS

Beim Cross-Site-Scripting werden in den Code der Originalseite im Internet korrumpierte Teile eingesetzt, die den Kunden unbemerkt zu einer manipulierten Seite führen.

Das gilt besonders für die iframe-Umleitung. Hierbei werden vor allem die Suchfunktionen auf Webseiten missbraucht, wenn sie die von ihnen vermittelten Suchanfragen für Google zwischenspeichern. Danach ist es zum Beispiel möglich, in die Adressen auf der Ergebnisseite von Google "iframe-Tags" einzuschmuggeln [128]. iframes sind dazu eingeführt worden, um auf einer Webseite Bereiche festzulegen, in denen fremde Dateien (zum Beispiel Werbung) eingeblendet werden können. In Verbindung mit DNS-Adressen werden die Browser jedoch auf eine Seite geführt, die der Angreifer bestimmt (Drive-By-Download). Dort werden dann Antivirenprogramme oder Video--Codecs zum Download angeboten, in denen allerdings der Trojaner Zlob stecken soll.

---

[119] Betrüger missbrauchen Suchfunktionen bekannter Webseiten, Heise Security 08.03.2008

[120] Massenhacks von Webseiten werden zur Plage, Heise online 14.03.2008

[121] Wieder groß angelegte Angriffe auf Web-Anwender im Gange, Heise Security 09.01.2008; Massen-SQL-Einspeisung geht weiter, tecchannel 10.05.2008

[122] **CF**, Massenhacks von Webseiten werden zur Plage, 14.03.2008

[123] **CF**, Pharming, 2007

[124] **CF**, Umleitungen zu manipulierten Webseiten, 09.12.2008

[125] **CF**, DNS-Poisoning, 21.11.2008; **CF**, Pharming, 2007

[126] **WP**, Dynamic Host Configuration Protocol - DHCP

[127] **CF**, Umleitungen zu manipulierten Webseiten, 09.12.2008

[128] Betrüger missbrauchen Suchfunktionen bekannter Webseiten, Heise Security 08.03.2008

Dynamische Webseiten basieren nicht auf einzelnen, in Handarbeit erstellten Skriptdateien (wie der Cyberfahnder), sondern aus aktuell aus einer Datenbank erstellten Textfragmenten (Content Management System - CMS [129]). Hackt man die ihnen zugrunde liegende Datenbank, kann mit den manipulierten Ergebnisseiten beliebiger Schadcode verbreitet werden [130].

A.2 12. Fazit

Der Adressenschwindel dient der Desorientierung und soll die Nutzer der Telekommunikation und des Internets zu Endpunkten führen, deren Existenz und deren Funktionsweise sie nicht erwarten. Das gilt für teure Mehrwertdienste ebenso wie für Pharmen, in denen mit nachgemachten Bankseiten oder anderen Internetdiensten eine gewohnte, aber eben falsche und gefährliche Umgebung vorgegaukelt wird.

Manuel Schmitt behauptet, die Strafverfolgung anhand von identifizierten IP-Adressen berge Fehler und könne zur Verfolgung Unschuldiger führen [131]. Das ist Unfug [132].

Ungeachtet dessen: Die Methoden der unauffälligen Entführung haben sich immer mehr verfeinert und werden sich immer weiter perfektionieren. Das gilt auch für die Methoden zu ihrer Abwehr, die die früheren Abzockmethoden verdrängt haben. Das alte Igel-und-Hase-Spiel wird sich hingegen fortsetzen und die kriminellen Abzocker werden uns immer wieder Überraschungen bereiten.

Kann man ihnen begegnen?

Ich glaube, dass die Strafverfolgung Schritthalten kann mit den Gedankenwelten und der Phantasie der modernen Abzocker und Kriminellen, wenn sie die Cybercrime ernst nimmt und ihr die nötigen Ressourcen zur Verfügung gestellt werden [133].

Eine der wichtigsten Voraussetzungen dafür ist, motivierte und neugierigen Leute zu gewinnen, die einen wesentlichen Teil ihrer Arbeitszeit mit der eigenen Fortbildung und Recherche verbringen und genügend Zeit dazu haben, zu überlegen, abzuwägen und zu analysieren. Das Tagesgeschäft muss dazu entsprechend beschränkt sein. Die üblichen Effektivitätsanforderungen lassen sich auf eine strategische Cybercrimebekämpfung nicht anwenden. Sie ist ein Wert an sich.

---

[129] Content Management System - CMS

[130] Wieder groß angelegte Angriffe auf Web-Anwender im Gange, Heise Security 09.01.2008

[131] Manuel **Schmitt**, IP-Adressen nur mit sicherem Routing eindeutig, Heise online 13.05.2010

[132] **CF**, IP-Adressen ohne Beweiswert, 16.05.2010

[133] **CF**, Straftaten mit der Informations- und Kommunikationstechnik, 09.03.2010

A.3 Malware [134]

Die Methoden für das Ausspähen von Daten und die Infiltration mit schädlicher Software - zusammen gefasst: Malware [135]- betreffen alle Verarbeitungsprozesse, die von einem PC ausgeführt werden. Immer geht es darum, mit automatischen Prozessen in die Prozessverarbeitung des PCs zu gelangen, um den "Rechner" für fremde Zwecke zu missbrauchen. Darin unterscheidet sie sich von dem Hacking [136], bei dem der Angriff unmittelbar von einem Menschen gesteuert wird.

Die Infiltrationsmethoden für die Malware haben sich im Zeitverlauf gewandelt. Ihre älteste Form ist der Virus [137], also ein kleines Programm, das sich in eine Trägerdatei hineinkopiert und mit ihr zusammen ausgeführt wird (passive Aktivierung). Würmer [138] sind hingegen selbständige Programmdateien, die aktive Umgebungen ausnutzen, um ausgeführt zu werden. Das kann dadurch geschehen, dass sie als Anhänge zu E-Mails übermittelt werden oder in andere Dokumente eingebettet sind, die aktive Elemente enthalten, die vom System automatisch geladen werden (activeX [139], Java [140]; Office-Programme [141], Multimedia-Player [142], PDF [143] und andere Anwenderprogramme [144]).

Eine andere Strategie verfolgen IP-Würmer [145], die Netzadressen automatisch absuchen und in fremde Systeme eindringen, indem sie Sicherheitslücken beim Netzzugang ausnutzen.

Eine genaue Grenzziehung zwischen den drei Angriffsstrategien ist nicht immer möglich, weil es durchaus Mischformen und Varianten gibt. So vereint der Trojaner [146] eine nützliche Anwendung mit schädlichen Aktivitäten, die er im Geheimen ausführt.

A.3 1. Tarnung und Täuschung

Die Malware kennt nur zwei Übertragungstechniken: Datenträger oder Netzverbindung [147]. Bei der Netzverbindung sind drei grundlegend unterschiedliche Methoden möglich:

⇨ Die Malware bedient sich eines Trägers, indem sie sich als Anlage [148] an eine E-Mail hängt (Wurm) oder ein Bestandteil eines ansonsten ungefährlich oder gar nützlich wirkenden Programms ist (Trojaner).

⇨ Sie attackiert von außen die Sicherheitseinstellungen des angegriffenen Systems und nutzt anschließend andere Sicherheitslücken aus, um sich einzunisten (IP-Wurm).

⇨ Sie verbirgt sich in harmlos wirkenden Scriptcodes. Dabei kann es sich um nachgemachte Homebanking-Seiten, um Links in E-Mails, Foren oder Webseiten handeln oder um unbemerkt startende Routinen (Code Injection [149]; Peer-to-Peer [150], Download [151]).

Wegen der Infektionsstrategie verwendet die Malware alle Spielarten des Versteckens (Trojaner), des selbständigen Angriffs und des Übertölpelns. Beim selbständigen Angriff werden technische Funktionen genutzt, die den Missbrauch aufgrund von Sicherheitslücken oder unbedarften Systemeinstellungen ermöglichen.

Auch die Methoden der Täuschung sind vielfältig (▸ Social Engineering). Sie reichen vom Plagiat (nachgemachte Webseiten, Pharming [152]), über

---

134 Die Urfassung dieses Aufsatzes stammt vom 12.05.2008.

135 **WP**, Schadprogramm

136 **WP**, Hacker

137 **WP**, Computervirus

138 **WP**, Computerwurm

139 **WP**, ActiveX

140 **WP**, Java (Programmiersprache)

141 **WP**, Office-Paket

142 **WP**, Mediaplayer

143 **WP**, Portable Document Format

144 **WP**, Anwendungssoftware

145 **CF**, IP-Würmer, 2007

146 **WP**, Trojanisches Pferd (Computerprogramm)

147 Gemeint sind kabelgebundene und drahtlose Netze. Selten sind unmittelbare Manipulationen am Computer (Keylogger, Hardwareinstallation oder Ausführung eines Programmes am angegriffenen Rechner).

148 **WP**, Dateianhänge

149 Siehe unten.

150 **WP**, Peer-to-Peer - P2P

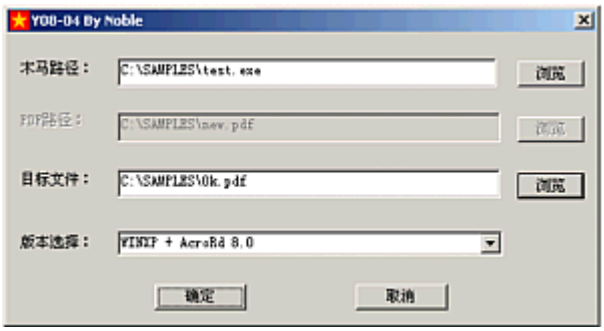
151 **WP**, Herunterladen

152 **CF**, Massenhacks von Webseiten werden zur

aufreizende Angebote ("Frau in Deiner Nähe sucht Gelegenheit zum Seitensprung") und andere Formen der Gier (Finanzagenten [153], Nigeria-Connection [154]) bis hin zur Maskerade (Bestellbestätigung [155], Rechnung [156], Kontobelastung [157], "Betti meldet sich").

Daneben kommen technische Tricks zur Tarnung zum Einsatz. Die installierte Malware verändert ihr Erscheinungsbild, wechselt ihren Standort (Stealth-Viren [158]) oder setzt den Virenscanner außer Betrieb (Retro-Viren [159]). Mit den Zombie-Programmen zur Botnetzsteuerung [160] wurden schließlich auf breiter Ebene Malwareversionen eingesetzt, die modular [161] aufgebaut sind. Für die Infiltration wird nur ein Grundmodul benötigt, das sich einnistet, tarnt, eine Verbindung zum Netz schafft (Backdoor [162], Rootkit [163]) und schließlich einen FTP-Server [164] installiert. Mit ihm können beliebige Bestandteile nachgeladen und installiert werden, so dass die Malware für jeden Zweck umgerüstet werden kann.

Für die Zukunft ist abzusehen, dass die Malware ihre Grundkomponenten in die Speicherchips [165] von Hardwareelementen [166] (Grafikkarte [167], TV-Karte [168], Switch [169], DSL-Router [170]) kopiert, wo sie von Virenscannern unbemerkt bleibt und sich auch dann neu installieren kann, wenn eine Festplatte formatiert und ein Betriebssystem neu installiert wird.



Eingabemaske für den Einbau von Malware in PDF-Dokumente [171]

A.3 2. Massenware und gezielte Spionage

Malware ist Massenware. Sie ist auf den breitflächigen Einsatz ausgerichtet und von ihm abhängig. Deshalb werden auch vorwiegend die am Markt erfolgreichen Betriebssysteme von Malware angegriffen. Wenn sie irgendeine Schwachstelle haben, dann können sie sehr schnell in großer Anzahl kompromittiert werden, allein weil sie eine große Verbreitung haben.

Die Betriebssysteme von Microsoft werden nicht deshalb immer wieder als Opfer von Malware-Kampagnen bekannt, weil sie besonders schlecht wären, sondern weil sie sich auf fast jedem privaten Rechner befinden. Neuerdings vermehren sich aber die Meldungen, die von Angriffen auf Linux- und MacIntosh-Systeme berichten.

Linux [172] basiert auf der Kommandosprache des klassischen UNIX [173] und ist besonders begehrt für den Betrieb von Datenbank- und Webservern sowie für die Steuerung von Firewalls, Switche und andere "intelligente" Netzwerkkomponenten.

MacIntosh (Apple) [174] war ganz lange Zeit führend bei der grafischen Benutzerführung, führte als

Plage, 14.03.2008

153 **CF**, Finanzagenten, 2007

154 **CF**, Evergreen: Vorschussbetrug nach Nigeria-Art, 17.03.2008

155 **CF**, gemeiner Versuch: Zahlungsbestätigung, 21.03.2008

156 **CF**, Abzocke mit KATI, 15.04.2008

157 **CF**, Testbelastung, 11.09.2007

158 **WP**, Stealth-Viren

159 **WP**, Retro-Viren

160 **CF**, zentrale Steuerung, Sommer 2007

161 **CF**, Anatomie des Sturm-Wurms, 06.03.2008

162 **WP**, Backdoor

163 **WP**, Rootkit

164 **WP**, File Transfer Protocol - FTP

165 **WP**, Integrierter Schaltkreis

166 **CF**, Angriffsobjekt PC, 2007 (Auseinandersetzung mit der Onlinedurchsuchung).

167 **WP**, Grafikkarte

168 **WP**, TV-Karte

169 **WP**, Switch (Computertechnik)

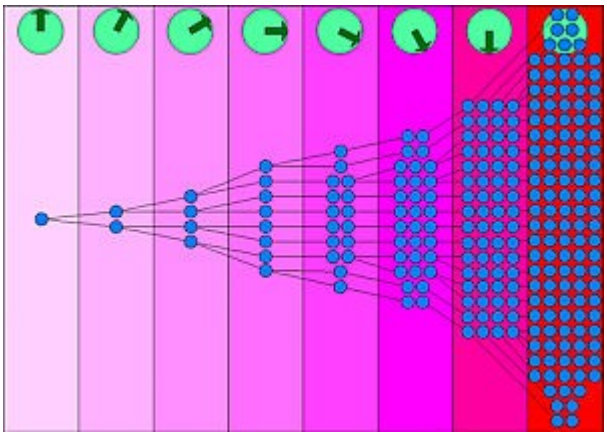
170 **CF**, Angriffe auf DSL-Router, 23.01.2008

171 F-Secure, Creating Malicous PDF Files, 02.06.2008; Angriffe über präparierte PDF-Dateien werden ausgefeilter, Heise online 03.06.2008

172 **WP**, Linux

173 **WP**, UNIX

174 **WP**, Apple Macintosh


die pandemische Ausbreitung von Malware

erstes Betriebssystem die Steuerung mit der Computermaus ein, war beliebt bei den Medienschaffenden, weil es besonders gut die Grafikbearbeitung und die Herstellung von Druck- und Layoutvorlagen (Desktop Publishing [175]) unterstützte, und blieb ein Nischenprodukt für die Anwender, die etwas mehr für eine nicht mehr ganz aktuelle Technik auszugeben bereit waren.

Mit dem iPhone und anderen Produkten drängt Apple jetzt auf den breiteren Konsumentenmarkt. Deshalb werden seine Geräte auch verstärkt zum Opfer von Malware.

Die Entwicklung und Verbreitung von Malware ist Hacking nach der Methode des Gießkannenprinzips. Wie beim Spamming gilt: Es ist egal, wen es trifft. Hauptsache ist, dass es trifft.

Den "Malworkern" ist die Identität des Opfers, seine Konfession, seine weltanschaulichen Vorstellungen im Übrigen und sein Einkommen völlig egal. Wenn sich sein Bankkonto für illegale Transaktionen ausnutzen, sein Kundenkonto für den Absatz von Hehlerware missbrauchen oder sein PC als Zombie für ein Botnetz korrumpieren lässt, dann schlagen sie ungeachtet der geschädigten Person und bedenkenlos zu.

Am Anfang waren die Spammer [176], die wenigstens noch legale Standbeine im Direktmarketing und im Adressenhandel hatten. Die ersten nur-kriminell ausgerichteten Softwareentwickler waren die Phisher [177]. Ihnen folgten die Botnetzer [178] und die mehr im Handwerk verwurzelten, aber sehr schadensträchtigen Skimmer [179].

Daneben ist eine professionelle Szene entstanden, die sich dem gezielten Angriff auf Unternehmen und Einzelpersonen widmet. Sie lässt sich teuer für Malware und Aufträge bezahlen, die zur Industriespionage [180], zur Ausforschung geheimer Informationen oder zum Abhören prominenter Personen eingesetzt werden. Das funktioniert meistens nur mit einer gehörigen Portion ▸ Social Engineering.

Beide Erscheinungsformen der massenhaften und der individuellen Penetration werden uns weiter begleiten und beschäftigen.

A.3 3. Crimeware

Der Begriff Crimeware [181] taucht seit 2006 verstärkt im Internet auf und umfasst alle Formen schädlicher Software, die für kriminelle Zwecke missbraucht werden.

Während bei Malware häufig das „nicht wirtschaftlich“ motivierte Verursachen von digitalen Schäden an Computern im Vordergrund steht, wird Crimeware ausschließlich entwickelt und verbreitet, um damit Geld durch kriminelle Aktivitäten zu verdienen [182].

Der Begriff ist gut gewählt, weil er alle schädlichen Programme, die bislang als Malware bezeichnet wurden (Viren, Würmer, Trojaner, Spyware [183]), erweitert auf alle Formen, die zum Angriff auf sensible Daten und die Privatsphäre verwendet werden.

---

175 **WP**, Desktop-Publishing - DTP

176 **CF**, Zusammenarbeit der Szenen, 2007

177 **CF**, Phishing, 2007

178 **CF**, Botnetze, Sommer 2007

179 **CF**, arbeitsteiliges Skimming, 18.05.2008

180 **CF**, erhebliche Schäden durch Industriespionage, 11.03.2008

181 **CF**, Angriffe mit Crimeware, 2007

182 **WP**, Crimeware

183 **WP**, Spyware

A.3 4. Angriffsmethoden

A.3 4.1 Bootvorgang

Der Start eines PCs ist ein meist vollständig automatisierter Vorgang [184], der von Malware dazu genutzt werden kann, dass ihre Komponenten, die im System nach der Infektion schlummern, tatsächlich auch installiert und aktiviert werden.

Die älteste Methode ist die, dass Datenträger verseucht werden, um beim Start des Systems die Malware zu installieren [185]. Hierzu kann jeder Datenträger missbraucht werden, ob Festplatte, Diskette, CD-ROM oder USB-Stick, wenn es gelingt, die Malware in den Bootsektor [186] des Datenträgers zu schreiben, der immer zuerst ausgeführt wird.

Die hier platzierte Malware muss nur ein einziges Kommando enthalten, das die an anderer Stelle gespeicherten oder aus dem Netz abgeforderten Programmteile lädt.

Auf den Bootsektor greifen das BIOS [187], das die Hardware betriebsbereit macht, und das Betriebssystem [188] zu, das die Arbeitsumgebung für die Programme herstellt. Das BIOS enthält in einem Speicherchip "fest verdrahtete" Bestandteile, die als solche nicht manipuliert werden können. Daneben verfügt es jedoch auch über programmierbare Teile, die missbraucht und mit Malware überschrieben werden können. Das heißt, dass die Malware auch das BIOS infizieren kann, was von modernen Systemen weitgehend unterbunden wird (aber prinzipiell nicht ausgeschlossen ist).

Überwachungs-Hardware, die nicht nur Datenströme kopiert (Keylogger [189]), muss vom BIOS aktiviert werden. Dazu bedarf es entweder einer spezifischen Anmeldung dieses Geräts oder die Nutzung einer Sowieso-Schnittstelle. Dafür bietet sich ganz besonders die USB-Schnittstelle [190] an, die inzwischen durchgängig von allen Peripheriegeräten und Spielereien genutzt wird. Der USB liefert Betriebsstrom und transportiert Daten in beide Richtungen. Über ihn lassen sich die PCs auch steuern und booten. Er ist die optimale Schnittstelle für Missbräuche und lässt sich auch nicht abschalten, weil er für andere nützliche Anwendungen gebraucht wird (Tastatur, Maus, Drucker, Scanner, externe Festplatte, Speicherstick, digitale Kamera ...).

A.3 4.2 Betriebssystem

Nachdem das BIOS die physikalische Umgebung des PCs aktiviert hat, gestaltet das Betriebssystem die Umgebung für die Programme, die zum Einsatz kommen sollen.

Um die Besonderheiten jedes einzelnen Systems berücksichtigen zu können, greift das Betriebssystem dabei auf Systemtabellen und ausführbare Skripte zurück, die ebenfalls infiltriert sein können. Wie gesagt: Ein einziges böswilliges Kommando reicht!

Klassisch für DOS (Microsoft) [191] sind das die Dateien config.sys [192] und autoexec.bat [193]. Unter UNIX [194] übernimmt diese Aufgaben u.a. die Crontab [195]. Seit der Einführung von Windows 98 werden die Konfigurationsdaten in eine dafür vorgesehene Datenbank geschrieben, die Registry [196]. Alle Manipulationen an diesen Konfigurationsdateien führen dazu, dass während des Starts des Betriebssystems Malware installiert werden kann.

Mit dem Betriebssystem werden auch andere Programme auf Vorrat geladen. Das verzögert zwar den Systemstart, beschleunigt jedoch die laufende Arbeit am PC.

Zu diesen Programmen gehören vor Allem die Firewall und der Virenscanner, das können aber auch Büroanwendungen und E-Mail-Browser sein (Outlook [197] wird häufig beim Startvorgang aufge-

[184] **WP**, Booten
[185] **WP**, Bootvirus
[186] **WP**, Master Boot Record
[187] **WP**, Basic Input Output System - BIOS
[188] **WP**, Betriebssystem (Operation System - OS)
[189] **WP**, Keylogger
[190] **WP**, Universal Serial Bus - USB
[191] **WP**, Microsoft Disk Operating System
[192] **WP**, Config.sys
[193] **WP**, Autoexec.bat
[194] **WP**, Unix
[195] **WP**, Cron
[196] **WP**, Windows-Registrierungsdatenbank
[197] **WP**, Outlook

rufen). Verantwortlich dafür sind in erster Linie die Pfadeintragungen in der Registry, die für Autostart-Programme vorgesehen sind, oder die Programme, die sich in dem Autostart-Verzeichnis befinden.

Beide werden von modernen Betriebssystemen im Verein mit Firewalls und Virenscannern argwöhnisch überwacht. Das bedeutet aber nicht, dass die Infektion dadurch ausgeschlossen ist. Gut getarnte Malware setzt auf andere, als gutwillig eingestufte Programme auf und schleicht sich damit ein. Dazu eignen sich besonders auch die "gutwilligen" Programmbibliotheken (DLL-Injection [198]), die die Objekte und andere Umgebungsvariablen verwalten, auf die die Anwenderprogramme dann zurück greifen.

Beim Systemstart wird meistens auch die Netzverbindung geprüft, indem der PC mit dem nächsten Netzknoten [199] Kontakt aufnimmt (Router [200], Switch [201], Wireless LAN [202]). Dadurch wird das System nach außen geöffnet. Bei den genannten Geräten handelt es sich selber um "intelligente" informationsverarbeitende Systeme [203], die ihrerseits infiziert sein und den Startvorgang zur Infiltration nutzen können [204].

Der Zugriff auf das Internet erfolgt nicht nur dadurch, dass der Anwender seine E-Mails oder im Browser Webseiten aufruft. Viele Programme machen das auch selbsttätig, um nach neuen Meldungen, Virensignaturen oder Programmversionen nachzufragen. Solche vom PC zugelassenen Netzkontakte lassen sich prinzipiell auch von der Malware missbrauchen.

Eine Variante davon ist das DNS-Poisoning [205], bei dem die lokale Hostdatei manipuliert wird, um unbemerkt auf präparierte Internetseiten umzuleiten. Diese Methode ist besonders im Zusammenhang mit dem Phishing und der Infiltration mit Botsoftware bekannt geworden.

A.3 4.3 Systemstart

Die zentralen technischen Komponenten des PCs sind der Prozessor [206], der eigentliche "Rechner", der Arbeitsspeicher [207] (auch Hauptspeicher) und der Massenspeicher [208] (Festplatte).

Der Prozessor wird für die datentechnischen Verarbeitungsvorgänge benötigt. Er führt den Programmcode aus, liest Daten, verarbeitet sie, leitet sie zu anderen Schnittstellen, z.B. zum Bildschirm, und speichert Dateien ab. Zur Beschleunigung seiner Arbeitsoperationen verfügt er immer häufiger über eigenen Cachespeicher (Zwischenspeicher), der sich auch für eine Infiltration eignet [209].

Anders ist das beim Arbeitsspeicher. Beim Pufferüberlauf [210] (buffer overflow) werden gezielt bestimmte Speicheradressen angesprochen, um deren Kapazität zu überlasten. Dabei kommt es zum "Überlauf", indem die angelieferten Daten zu anderen Adressbereichen verlagert werden. Das führt meistens zum Systemabsturz, kann aber auch dazu genutzt werden, Malwarecode einzuschleusen.

Anspruchsvolle technische Erweiterungen sind häufig wie ein selbständiger PC im PC konstruiert. Das gilt vor Allem für hochwertige Grafik- und Videokarten, die über eigene Prozessoren und Arbeitsspeicher verfügen und damit das System im Übrigen entlasten.

Je verbreiteter solche Karten sind, desto attraktiver werden sie für die Malware, um böswillige Verarbeitungsprozesse, die im Hauptsystem zu auffällig wären, hierhin zu verlagern.

Dasselbe Vorgehen ist auch bei vernetzten Syste-

198 **WP**, DLL-Injection

199 **CF**, Angriffe aus dem Netz, 2007

200 **WP**, Router

201 **WP**, Switch (Computertechnik)

202 **WP**, Wireless Local Area Network - WLAN

203 **CF**, Telefonanlage, Server, 2007

204 Trojaner konfiguriert Router um, Heise online 13.06.2008

205 **CF**, Massenhacks von Webseiten werden zur Plage, 14.03.2008

206 **WP**, Prozessor (Hardware)

207 **WP**, Arbeitsspeicher

208 **WP**, Massenspeicher

209 Hacker finden einen neuen Platz, um rootkits zu verbergen, tecchannel 10.05.2008

210 **WP**, Pufferüberlauf

men möglich. Beim verteilten Rechnen [211] werden die Verarbeitungsvorgänge zu ihrer Beschleunigung auf verschiedene Systeme und ihre Ergebnisse zentral zusammen geführt [212]. Ohne diese Technik wären Google und andere große Netzanwendungen nicht denkbar.

Sie kann von der Malware - vor Allem in Botnetzen, die über eine Vielzahl von Rechnern verfügen - dazu genutzt werden, den gezielt angegriffenen Rechner nur mit geringfügigen Lese- und Schreibprozessen zu belasten und die kapazitätsintensiven und auffälligen Prozesse auf andere Rechner zu verteilen (Brute-Force-Methode [213] zum Cracking [214]).

A.3 4.4 laufender Betrieb

Neben dem direkten Eingriff auf Systemkomponenten versucht vor Allem die klassische Malware sich in laufende Verarbeitungsprozesse einzuschleichen. Das geschieht beim Bootvorgang ebenso wie beim laufenden Betrieb.

Anfällig dafür sind solche Programme, die im Hintergrund laufen und die Arbeit mit dem PC erleichtern sollen. Besonders bekannt geworden sind insoweit die E-Mail-Browser, die die Anhänge von E-Mails [215] automatisch ausführen. Moderne Programme verhindern das und untersuchen die Anhänge zugleich auf schädliche Inhalte. Die Malworker sind deshalb dazu übergegangen, dem Anwender Versprechungen zu machen, um ihn zum unbedarften Programmstart zu bewegen.

Aber auch andere Anwenderprogramme sind anfällig. Das Office-Paket von Microsoft [216] stellt mit Visual Basic for Applications - VBA [217] - eine Umgebung für selbst ausführende Makros [218] zur Verfügung, die auch mit schädlichem Code bestückt sein können und mit Word-Dokumenten [219], Excel-Tabellen [220] oder Powerpoint-Präsentationen [221] verbreitet werden.

Inzwischen wird auch von infizierten PDF-Dokumenten [222] (Adobe [223]) berichtet [224], die als Laufzeitumgebung nach Java (for Applications [225]) verlangen. Dasselbe gilt für den FlashPlayer [226] von Adobe [227].

Hinter der Makrosprache VBA stecken Programmmodule, die unter ActiveX [228] zusammen gefasst werden und die Datenverarbeitung unterstützen. Das gilt besonders für grafiklastige Anwendungen, z.B. für Computerspiele.

Besonders Trojaner, aber auch andere selbstablaufende Programme (mit .exe und anderen Extensionen) nutzen hingegen die Kommandoumgebung, die das Betriebssystem zur Verfügung stellt.

Daneben dienen, wie schon gesagt, exotische Abspielprogramme für Musik und Videos sowie als besondere Software für geschlossene Anwenderkreise beworbene Programme zum Transport von Malware. Dies gilt besonders für instinktorientierte Online-Angebote [229] und Warez-Seiten [230].

---

211 **WP**, Verteiltes Rechnen

212 Siehe: **CF**, Passwort vergessen? Cloud hilft! 19.12.2009

213 **WP**, Brute-Force-Methode

214 **WP**, Cracker (Computersicherheit)

215 **WP**, Dateianhänge

216 **WP**, Microsoft Office

217 **WP**, Visual Basic for Applications - VBA

218 **WP**, Makro

219 **WP**, Microsoft Word

220 **WP**, Microsoft Excel

221 **WP**, Microsoft PowerPoint

222 **WP**, Portable Document Format - PDF

223 **WP**, Adobe Systems

224 Angriffe über präparierte PDF-Dateien werden ausgefeilter, Heise online 03.06.2008

225 **WP**, Java (Programmiersprache)

226 **WP**, Adobe Flash

227 Kritische Schwachstelle im Flash Player wird aktiv ausgenutzt, Heise online 28.05.2008

228 **WP**, ActiveX

229 **CF**, instinktorientierte Online-Angebote, 23.01.2008

230 **WP**, Warez

A.3 4.5 online

Der Anwender, der eine fremde Webseite aufruft, gibt dabei einige Basisdaten über sich preis. Das ist zunächst die nummerische Internetadresse, mit der er sich bewegt und die ihm in aller Regel von seinem Zugangsprovider vorübergehend (dynamisch) zugewiesen wird. Daneben offenbart er auch den Typ seines Webbrowsers und seinen "Referrer" [231], wenn er etwa eine Suchmaschine oder eine Linksammlung genutzt hat.

Auch die auf seinem System vorhandenen Cookies sind lesbar, wenn sie vom Zielserver angefordert werden, und können weitere personenbezogene Daten enthalten. Das gilt besonders für die HTTP-Cookies [232], die vom Webbrowser gespeichert und übermittelt werden.

Diese relativ allgemeinen Informationen sind nicht besonders gefährlich und bieten nur wenige Angriffspunkte. Sie offenbaren allerdings die persönlichen Neigungen und Eigenschaften des Anwenders, die zum ▸ Social Engineering missbraucht werden können.

Wegen der im Browser gespeicherten Zugangsdaten für das Homebanking oder Shopping im Internet sieht das schon anders aus. Sie können zwar nicht unmittelbar ausgelesen werden, wohl aber, wenn es dem Angreifer gelingt, den PC mit Malware zu infiltrieren.

Die dazu verwendeten Methoden wurden bereits angesprochen. Es handelt sich um das DNS-Poisoning [233], bei dem die interne Host-Datei so umgeschrieben wird, dass der Browser zu einer nachgemachten und präparierten Seite geführt wird, die iframe-Umleitung [234] und das Hacking von Datenbanken für die Bestückung dynamischer Webseiten (SQL-Injection [235]).

Die aufgerufene Webseite kann zudem so präpariert sein, dass sie unter Ausnutzung von Schwachstellen im Browser eigene Aktivitäten ausführt. Die dazu verwendeten Kommandos können sowohl im Quellcode der Seite (vor Allem Java-Script [236]) oder in einem plötzlich erscheinenden Werbefenster (Pop-up [237]) eingebunden sein. Dasselbe gilt für iFrames [238], die häufig für Werbeeinblendungen von fremden Seiten verwendet werden und deshalb auch zur Einschleusung von Schadcode missbraucht werden können.

Diese aktiven Funktionen können dann zu einem Drive-by-Download [239] führen, bei dem allein schon das Aufrufen der Seite dazu reicht, dass die Malware unbemerkt zum Anwender übermittelt wird.

Besondere Vorsicht ist geboten, wenn die Website ein Plug-in [240] zum Download anbietet, das angeblich für irgendwelche besondere Dienste notwendig sei. Damit soll in aller Regel der Browser manipuliert und die Malware direkt installiert werden.

Ganz ähnlich funktioniert die Verbreitung über Peer-to-Peer-Netzwerke [241] (Tauschbörsen [242]), wobei der Download nicht von einem Webserver, sondern von einem Partner erfolgt.

Ganz unbemerkt kann ein Angreifer dann die Malware einsetzen, wenn bereits eine "Hintertür" (Backdoor [243]) besteht, die entweder mit einem Rootkit [244] oder bereits herstellerseits eingerichtet wurde (Fernwartung [245]). Besonders gefürchtet sind insoweit Telefonanlagen [246], die häufig eine direkte Verbindung zum informationsverarbeitenden System haben und das besonders dann, wenn Voice-over-IP [247] - VoIP - genutzt wird (Internettelefonie).

---

231 **WP**, Referrer
232 **WP**, HTTP-Cookie
233 Siehe oben.
234 Siehe oben.
235 **WP**, SQL-Injection
236 **WP**, JavaScript
237 **WP**, Pop-up
238 **WP**, Inlineframe
239 **WP**, Drive-by-Download
240 **WP**, Plug-in
241 **WP**, Peer-to-Peer
242 **WP**, Tauschbörse
243 **WP**, Backdoor
244 **WP**, Rootkit
245 **WP**, Fernwartung
246 **CF**, Telefonanlagen
247 **WP**, IP-Telefonie

Zur Vertiefung ist auf Bachfeld zu verweisen [248]. Mit fachlicher Tiefe beschäftigt er sich in der Zeitschrift c't mit den aktuellen Gefahren aus dem Netz und beschreibt er die Techniken im Zusammenhang mit infizierten Webseiten. Dazu geht er zunächst auf das Cross-Site-Scripting [249] am Beispiel des XSS-Wurms ein, wobei mit Hilfe von eingeschleusten Kommandofolgen (JavaScript) versucht wird, diese zusammen mit ungeschützten Systemfunktionen auszuführen. Anschließend beschreibt er Angriffe auf DSL-Router und Webseiten mit dem Cross Site Request Forgery – CSRF [250], wobei die schädlichen Kommandoanweisungen zusammen mit einem Link übertragen werden [251]. Es folgen Ausführungen zum DNS-Poisoning [252], dessen Servervariante Bachfeld als DNS-Rebinding vorstellt, und zu IFrames [253].

Abschließend stellt Bachfeld die Same Origin Policy - SOP [254]- vor, die danach verlangt, dass das aufrufende Kommando aus derselben Quelle stammen muss wie das damit ausgeführte Programm. Die SOP verhindert damit viele Formen der vorgestellten Angriffe, nicht aber zum Beispiel das Nachladen von Grafiken in IFrames.

A.3 5. Abwehr

Gegen die technisch ausgerichteten Angriffe helfen vor Allem die ständige Aktualisierung der eingesetzten Programme, der Einsatz einer Firewall (zum Absichern benutzter und Schließen ungenutzter Zugangswege) und eines Virenscanners, der kontinuierlich den Onlineverkehr und die Prozessverarbeitung überwacht.

Daneben ist das Nutzungsverhalten besonders wichtig. Richten Sie unter Windows ein Benutzerkonto ohne Administratorenrechte ein. Die Installation von Programmen und Malware ohne Ihr Zutun wird dadurch ausgeschlossen.

Wenn Sie außerdem keine Zugangsdaten (und besonders keine TANs) im System speichern und bei verlockenden Diensten erst nachdenken und dann handeln, kann Ihnen fast nichts mehr passieren [255].

A.3 6. Fazit

Malworker versuchen, persönliche Daten auszuforschen und zu missbrauchen oder den PC für andere Böswilligkeiten [256] zu verwenden. Sowohl ihre technischen Methoden wie auch ihre Überredungskünste haben sie immer mehr verfeinert, um fremde Systeme infiltrieren und ihre Malware installieren zu können.

Dazu werden entweder präparierte Datenträger oder Netzverbindungen verwendet. Wegen der Netzverbindungen kommen alle Dienste in Betracht, die das Internet und das digitale Telefon bieten.

Malware soll den Missbrauch unterstützen und ist deshalb wegen ihrer zerstörerischen Eigenschaften zurückhaltend. Manchmal kommt es jedoch zu dummen Zufällen [257].

Es mag sie gegeben haben, die Spielkälber unter den Hackern und Malware-Entwicklern, die nur ihren Spaß haben wollten und wenig Schaden anrichteten. Die moderne Malware ist jedoch professionelles Werkzeug, um Straftaten zu begehen.

---

[248] Dirk **Bachfeld**, Dunkle Flecken. Neuartige Angriffe überrumpeln Webanwender, c't 11/2008, S. 82; siehe auch **CF**, gewandelte Angriffe aus dem Netz, 29.11.2008.

[249] **WP**, Cross-Site Scripting

[250] **WP**, Cross-Site Request Forgery

[251] Siehe auch **CF**, Nummerntricks. Adressierung im Internetprotokoll, 21.11.2008

[252] **CF**, DNS-Poisoning, 21.11.2008

[253] **CF**, Angriffe gegen Webserver, 21.11.2008

[254] **WP**, Same Origin Policy - SOP

[255] Wegen der weiteren Einzelheiten siehe ▸ **A.1**.

[256] **CF**, verteilter Angriff, 2007

[257] **CF**, alte Praktiken im neuen Gewand, 2007

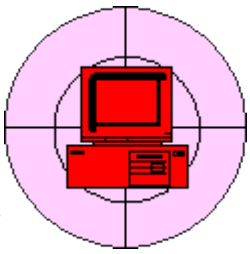
A.4 Identitätsdiebstahl und Phishing [258]

Die Einsätze von Malware [259] und des Social Engineerings [260] waren lange davon geprägt, dass sie zerstörerischen Zwecken dienten [261]. Das hat sich in den letzten Jahren geändert [262]. Digitale Angriffe werden fast nur noch mit dem Ziel durchgeführt, kriminellen Gewinn zu machen, und das heißt in aller Regel, Konto- und andere persönliche oder gewerbliche Daten auszuspähen, um sie zur Erpressung oder zum Missbrauch zu verkaufen oder selber zu verwenden.

A.4 1. Identitätsdiebstahl

Der Identitätsdiebstahl [263] ist das Ausspähen persönlicher (Echt-) Daten mit dem Ziel, mit ihnen Zugang zu fremden Online-Konten zu bekommen, um mit den fremden Daten Leistungen zu erlangen, Geschäfte abzuschließen, die zulasten des Kontoinhabers gebucht werden, oder um sich unter fremder Identität im Internet und anderswo zu bewegen [264].

Online-Konten in diesem Sinne sind nicht nur Bankkonten, sondern alle Accounts, die Zugang zu



exklusiven Diensten und Leistungen gewähren. Sie können bei Handelsplattformen wie Amazon oder eBay bestehen [265], bei Warenhäusern, Informationsdiensten (Fachinformationen, Zeitungen, Wetterdienst), virtuellen Veranstaltungen wie Second Life [266] oder geschlossene Spiele [267], zu Versanddiensten wie DHL [268] und UPS [269] und schließlich zum Onlinebanking [270] und anderen Bezahldiensten [271] wie PayPal [272], E-Gold [273] und WebMoney [274].

In der Zeitschrift c't hat Bachfeld die Situation zutreffend beschrieben [275]:

Leider ist im Internet nichts mehr isoliert zu betrachten, alles ist irgendwie miteinander verknüpft – und das wissen die Betrüger für sich zu nutzen. Das sollte allerdings kein Grund sein, den Kopf in den Sand zu stecken und gar nicht mehr ins Internet zu gehen. ...

---

[258] Die frühen Formen des Phishings werden in dem ersten hier veröffentlichten Arbeitspapier beschrieben: **CF**, Phishing. Wie funktionieren die Informationstechnik und das Internet? 22.01.2007.

Die Erscheinungsformen des Phishings haben sich stark gewandelt und werden in diesem neuen Aufsatz als besondere Ausprägung des Identitätsdiebstahls behandelt.

Die Prognosen, die ich 2007 angestellt habe, sind weitgehend eingetreten. Das „alte“ Arbeitspapier ist auch deshalb noch immer von Interesse, weil es zeigt, wie Internetadresse und Header-Daten in E-Mails interpretiert werden können.

Siehe auch:
CF, Suchmaschinen und -techniken, 29.12.2008;
CF, Auskunftsdienste im Internet, 06.12.2009;
CF, eurasische Verbindungen, 06.12.2009

[259] Siehe oben ▸ **A.3**.

[260] Siehe unten ▸ **B.**

[261] Siehe noch **CF**, neue Herausforderungen, 2007 (**WP**, Sasser).

[262] Siehe auch **CF**, Länderstudie USA, 27.07.2008 (digitaler Bürgerkrieg).

[263] **WP**, Identitätsdiebstahl

[264] François **Paget**, Identitätsdiebstahl, McAfee 04.01.2007 (ZIP-Datei)

[265] **CF**, Missbrauchsgefahren, 2007

[266] **CF**, Second Slum, 15.12.2007

[267] **CF**, Länderstudie China, 27.07.2008 (Real Money Trade - RMT)

[268] **WP**, DHL

[269] **WP**, United Parcel Service

[270] **CF**, Sicherheit von Homebanking-Portalen, 22.03.2008; **CF**, sicheres Homebanking, 19.12.2008

[271] **CF**, Internet-Finanzdienste, 2007; **CF**, neuartige Finanzdienste, 2007; **CF**, Bezahlen im Internet, 19.06.2008.

[272] **CF**, PayPal-Phishing, 13.05.2009

[273] **CF**, Verrechnungssysteme auf der Basis von Edelmetallen, 2007

[274] **CF**, Botnetz-Software und -Betreiber, 13.07.2008

[275] Dirk **Bachfeld**, Dunkle Flecken. Neuartige Angriffe überrumpeln Webanwender, c't 11/2008, S. 82; siehe auch **CF**, gewandelte Angriffe aus dem Netz, 29.11.2008.

A.4 2. Kontoübernahmen

Die wichtigste Form des Identitätsdiebstahls ist die Übernahme bestehender fremder Konten. Eine besondere Bedeutung kommt dabei den Handelsplattformen mit Bewertungssystemen zu [276]. Unauffällige Konten mit guten Bewertungen eignen sich besonders gut zum Stoßbetrug oder zum Absatz von Hehlerware [277].

Zunächst muss der Angreifer die Kontozugangsdaten ausspähen. Dazu wendet er entweder die üblichen Überredungsmethoden (soziale Kontakte, vorgetäuschte E-Mails, die angeblich vom Veranstalter stammen und zur Bestätigung der Zugangsdaten auffordern) oder technische Methoden an (Malware, präparierte Webseiten, Keylogger).

Mit diesen Daten dringt er in das fremde Konto ein und sperrt den Berechtigten dadurch aus, dass er das Zugangskennwort ändert. Alle weiteren Änderungen in den Kontoeinstellungen richten sich danach, welche Ziele der Angreifer verfolgt.

⇨ *Geschäfte zulasten des Inhabers*. In diesem Fall nutzt der Angreifer vor Allem das hinterlegte Bankkonto des Inhabers für die Bezahlung von Diensten und Leistungen. Er lässt also die Zahlungsdaten unberührt und ändert nur die Lieferadresse, an die zum Beispiel Warensendungen gerichtet werden sollen. Nach erfolgter Lieferung wird die Lieferadresse wieder gelöscht, um die Nachverfolgung zu erschweren.

⇨ *Betrug und Absatzgeschäfte*. Wenn der Angreifer auf Handelsplattformen betrügerische Geschäfte abwickeln oder Hehlerware absetzen will, dann ändert er die Kontodaten, an die die Bezahlung gerichtet werden soll. Zu gegebener Zeit wird das vom Angreifer eingetragene Konto wieder gelöscht, um die Nachverfolgung zu erschweren.

⇨ *verschleierte Zahlungsströme*. Gar keine Änderungen nimmt der Angreifer dann vor, wenn er ein Bank- oder Bezahlkonto nur zur Durchschleusung von Zahlungen verwenden will. Er parkt den Zahlungseingang auf dem gekaperten Konto und leitet ihn im Lastschriftverfahren weiter [278]. Das kann er auch ohne TAN oder iTAN [279] machen.

Alle Formen des Identitätsdiebstahls können zu brutalen Missbräuchen genutzt werden, bei denen der Angreifer davon ausgeht, dass das Konto alsbald verbrannt und für ihn unbrauchbar ist. Er kann aber auch behutsame Missbräuche unternehmen, die kaum auffallen, weil er seine Kontoeinstellungen immer wieder zurücksetzt, um sich das gekaperte Konto möglichst lange zu erhalten.

Im weiteren Sinne gehört auch die Identitätsverschleierung dazu. Sie zeigt sich einerseits in der Einrichtung von neuen Konten unter fremden Echtdaten, die besonders im Zusammenhang mit Warenbestellungen und Handelsgeschäften beobachtet wird. Andererseits können Konten auch unter erfundenen Daten eingerichtet werden, die vor Allem zur Kommunikation und zur Verbreitung von Dateien genutzt werden. Schließlich kann es auch darum gehen, eine vollständige Tarnidentität aufzubauen, die mit falschen Personalpapieren und einer Legende untermauert wird, zu der auch E-Mail- und andere Konten zum täglichen Bedarf und zur Kommunikation gehören. Somit erzielen auch die Daten ausgespähter E-Mail-Konten hohe Schwarzmarktpreise [280]. Der einfachste Fall der Identitätstäuschung ist die Umgehung von Altersbeschränkungen mit fremden oder vorgetäuschten Personalien [281].

---

[276] Siehe auch **CF**, Identitätsdiebstahl. Mischformen, 19.04.2009;
CF, Plattformhaftung bei Identitätsdiebstahl, 12.04.2008

[277] **CF**, Entwicklungen, 01.11.2008;
CF, falsche Produkte und Hehlerware, 23.02.2008.

[278] **CF**, Einzugsermächtigung und Lastschriftverfahren, 2007

[279] **CF**, Sicherheit von Homebanking-Portalen, 22.03.2008

[280] **CF**, Schwarzmarkt, 19.12.2008;
Thorsten **Holz**, Markus **Engelberth**, Felix **Freiling**, Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones, Uni Mannheim 18.12.2008 (englisch);
Keylogger unter die Lupe genommen, Heise Security 18.12.2008;
Kriminelle verdienen kräftig an Keyloggern, tecchannel 19.12.2008.

[281] Vornamen und die Seriennummern von Personalausweisen lassen eine Abschätzung des Alters des Verwenders zu. Inzwischen gibt es Programme, die das digitale Abbild eines Personalausweises so darstellen, dass ein Kind als angeblich Erwachsener durchkommt.

A.4 3. Ziele des Identitätsdiebstahls

Allen Zielen des Identitätsdiebstahls ist gemein, dass der Angreifer seine eigene Identität tarnt. Wegen seiner Beweggründe im Einzelfall sind sie vielfältig:

⇨ Belastung von fremden Verkehrskonten bei Banken und Leistungsanbietern.

⇨ Ausnutzung des Rufes, z.B. im Zusammenhang mit den Bewertungen bei eBay.

⇨ Abschluss betrügerischer Geschäfte mit Vorauszahlungen des getäuschten Käufers.

⇨ Nutzung und Verschleierung des Zahlungsverkehrs über Bankkonten und neue Bezahlsysteme.

⇨ Erlangung virtueller Werte in digitalen Welten und Online-Spielen.

Bei den ersten drei Ausprägungen dürfte die strafrechtliche Bewertung verhältnismäßig einfach sein, wenn auch im Einzelfall immer Probleme zu erwarten sind. Das Problem ist jedoch, dass das Internet ortsungebunden ist und das deutsche Strafrecht an den nationalen Grenzen seine Wirkung verliert.

⇨ Wenn „echte Menschen“ getäuscht werden und dadurch einen Vermögensnachteil erleiden, handelt es sich in aller Regel um einen Betrug gemäß § 263 StGB.

⇨ Wenn automatische Prozesse – allein schon durch die unbefugte Nutzung fremder Daten – beeinflusst werden und dadurch fremdes Vermögen verringert wird, dürfte zumeist ein Computerbetrug gemäß § 263a StGB vorliegen [282].

⇨ Die Veränderung der Kontodaten, um damit Geschäfte oder Zahlungen abzuwickeln, dürfte als Fälschung beweiserheblicher Daten im Sinne von § 269 StGB zu behandeln sein [283].

⇨ Allein schon die Aussperrung des berechtigten Inhabers durch Veränderung des Zugangspasswortes würde ich als Datenveränderung und Computersabotage gemäß §§ 303a und 303b StGB ansehen [284].

Wegen der Verschleierung des Zahlungsverkehrs ist ebenfalls § 269 StGB zu prüfen. Es handelt sich um ein Urkundsdelikt, so dass es dann bedeutsam ist, wenn die Identitätsmerkmale des Kontonutzers verschleiert werden. Außerdem kommt § 303a StGB (Datenveränderung) schon dann in Betracht, wenn die Daten des berechtigten Inhabers verändert werden.

§ 269 StGB kennt zwei Tathandlungen der Datenmanipulation, nämlich das Speichern und das Verändern, wodurch sowohl die Manipulation stationärer Daten, die bereits gespeichert sind, der Verarbeitungsvorgang, nach dem die Daten schließlich gespeichert werden, als auch an den Daten umfasst ist, die nach ihrer Veränderung an eine andere Stelle übermittelt werden. Hierbei ist zu prüfen, ob die verfälschten Daten

⇨ Einfluss auf eine Rechtsbeziehung haben, von der mindestens bei einem Beteiligten Rechte oder Pflichten berührt werden,

⇨ sich auf einen konkreten Aussteller beziehen, der mithilfe der Daten seine Rechtsbeziehungen gestaltet, und

⇨ in einer Rechtsbeziehung Beweis für eine Tatsache erbringen sollen.

Mindestens vier wichtige Anwendungsfälle sind von der Rechtspraxis als strafbare Fälschung beweiserheblicher Daten anerkannt worden:

⇨ Manipulation des Guthabens auf einer Guthabenkarte [285],

⇨ nachgemachte E-Mails, die zum Beispiel den Anschein erwecken, von einer Bank zu stammen (Phishing),

⇨ nachgemachte Websites, die ebenfalls den Anschein vermitteln sollen, sie würden von einer

---

[282] **CF**, Computerbetrug, 2007

[283] **CF**, Fälschung beweiserheblicher Daten, 2007

[284] **CF**, Computersabotage, 2007.
Zu berücksichtigen ist die gesetzliche Definition in § 202a Abs. 2 StGB. Die Daten müssen entweder physikalisch gespeichert sein, dann können sie ausgespäht werden (§ 202a Abs. 1 StGB), oder sie müssen übermittelt werden, dann greift das Abfangen von Daten (§ 202b StGB). Nicht erfasst sind jedenfalls die unmittelbaren Dateneingaben mit einer Tastatur oder anderen physikalischen Schnittstellen (Tablet, Scanner).

[285] **CF**, "Nachladen" von Guthabenkarten, 2007 (Telefonkarte);
BGH, Beschluss vom 13.05.2003 - 3 StR 128/03.

Bank oder einem anderen Anbieter stammen und

⇨ Auftreten unter fremdem Namen (Identitätsdiebstahl im engeren Sinne) [286].

Wenn es um den Absatz gestohlener, ertrogener oder anderweitig rechtswidrig erlangter Waren geht, ist wegen des Helfers (Finanz- und andere Agenten) Hehlerei zu prüfen (§ 259 StGB). Soweit es um die Sicherung rechtswidrig erlangter Forderungen geht (Bankguthaben oder andere Forderungen, die nicht körperlich sind), kommt auch Geldwäsche in Betracht (§ 261 StGB). Die Verschiebung von gestohlenen Daten, die man Datenhehlerei nennen würde, ist für sich allein nicht strafbar [287].

A.4 4. virtuelle Kriminalität

Für den „Diebstahl" virtueller Werte in digitalen Welten und Online-Spielen gibt es vereinzelte Beispiele. Sie betreffen den Ausschluss von Mitspielern, die gemeinsam ein Raumschiff für eine virtuelle Umgebung konstruiert haben [288], den Diebstahl von kostenpflichtigen Möbeln aus einer virtuellen Hotelsuite [289], Ausstattungsgegenstände für virtuelle Spiele [290] und von Spielgeld, das dort zum Einsatz kommt [291]. Den Höhepunkt markiert der rachsüchtige virtuelle Mord einer betrogenen Mitspielerin, die das Benutzerprofil ihres (virtuell!) Geschiedenen löschte [292].

Die rechtliche Einstufung dieser virtuellen Kriminalität ist nicht immer ganz einfach, orientiert sich am Einzelfall und bewegt sich wegen der Kontomanipulationen im Bereich des Ausspähens und Abfangens von Daten (§§ 202a, 202b StGB), der Datenveränderung (§ 303a StGB), und dort, wo Werte verschoben werden, die auch in der realen Welt einen wirtschaftlichen Wert haben (Möbel im virtuellen Hotel), beim Computerbetrug (§ 263a StGB) und der Fälschung beweiserheblicher Daten (§ 269 StGB).

In dem Fall, dass jugendliche Mitspieler mit realer Gewalt die Herausgabe virtueller Spielausstattungen verlangt haben, handelt es sich um eine schlichte räuberische Erpressung (§ 255 StGB).

Beachtlich ist die Bedeutung, die virtuelle Spiele haben. McAfees Länderstudie für China macht das besonders deutlich [293]. Hier sind Goldfarmen entstanden, in denen rund 100.000 bezahlte Spieler Punktestände erspielen, die dann an zahlungsbereite Interessenten verkauft werden. Dort, wo sich Wirtschaft mit klingender Münze zeigt, verwaschen und überschneiden sich die Grenzen zwischen virtueller und realer Welt. Das hat schon sehr schnell das Second Life gezeigt, wo Banken gecrasht sind [294], Kinderpornos ausgetauscht und mit Prostitution Geld [295] gemacht wurde.

---

[286] Siehe Alexander **Schultz**, § 269 StGB - Fälschung beweiserheblicher Daten, mediendelikte.de;
AG Euskirchen, Urteil vom 19.06.2006 - 5 Ds 279/05 (bei www.a-i3.org);
bestätigendes Berufungsurteil des **LG Bonn**, Urteil vom 13.10.2006 - 36 B 24/06 (ebenda).

[287] Eine Ausnahme gibt es nur im Zusammenhang mit Geschäfts- und Betriebsgeheimnissen: § 17 UWG.

[288] **CF**, künftige Herausforderungen, 2007

[289] **CF**, Diebstahl virtueller Sachen, 15.11.2007

[290] **CF**, virtueller Diebstahl, 25.10.2008

[291] **CF**, Diebstahl in Online-Spiel, 01.02.2009

[292] **CF**, virtueller Mord, 31.10.2008

[293] **CF**, globale Sicherheitsbedrohungen. China, 27.07.2008

[294] **CF**, Bankenkrach in der Zweiten Welt, 20.08.2007

[295] **CF**, Prostitution im Second Life, 21.10.2007

A.4 5. Zahlungs- und Geschäftsverkehr

Im Zusammenhang mit dem Zahlungs- und Geschäftsverkehr haben sich besondere Formen des Identitätsdiebstahls herausgebildet, die im einzelnen betrachtet werden müssen.

A.4 5.1 Carding

Beim Ausspähen von Kontodaten geraten nicht nur die Homebanking-Daten [296] der Opfer in das Interesse der Täter, sondern auch andere persönliche Daten, die sich verkaufen oder anderweitig missbrauchen lassen [297]. Das Bundeskriminalamt fasst diese Formen des Kreditkartenbetruges [298] unter dem Begriff Carding zusammen [299], womit die umfassende Verwertung von EC- und Kreditkartendaten gemeint ist – vom Ausspähen der Kartennummern und Sicherheitsschlüssel über deren Vermarktung im Web bis zur Produktion gefälschter Kartenkopien [300].

Der Handel mit Kreditkartendaten dürfte den größten Anteil an der Underground Economy ausmachen [301]. Dort sollen 2007 *gestohlene Waren und entsprechende Dienstleistungen im geschätzten Gesamtwert von 276 Millionen Dollar angeboten* worden sein [302]. Am meisten würden Kreditkarteninformationen gehandelt werden (31 %), was einem Missbrauchsvolumen von 5,3 Milliarden Dollar entspräche. Ihnen sollen mit 20 % Marktanteil die Kontozugangsinformationen folgen, die ein Missbrauchspotential von 1,7 Milliarden Dollar präsentieren würden.

Für diese Form des Betruges werden manipulierte Webseiten eingesetzt, die den Besuchern lukrative Angebote vorgaukeln und bei dieser Gelegenheit die Kreditkartendaten abfragen, oder Malware mit Keylogger-Eigenschaften, die den Online-Verkehr des Opfers protokollieren [303]. Solche Protokolle erstellt inzwischen jede gut gemachte Bot-Software. Schon seit 2005 soll der Homebanking-Trojaner Torpig im Einsatz sein, der unter Windows *neben Daten für Bankkonten auch Kreditkartendaten und FTP-Accounts ausspäht* [304].

Das Carding beschränkt sich hingegen nicht auf Kreditkarten, sondern tritt auch im Zusammenhang mit anderen Guthabenkarten auf, zum Beispiel mit „nachgefüllten“ Tankkarten. Sie täuschen die prüfende Automatik über den Wert der Gegenleistung, die in Anspruch genommen werden kann [305].

A.4 5.2 Phishing in neuen Formen

Beim Phishing [306] geht es den Tätern darum, die Kontozugangsdaten zum Onlinebanking auszuspähen und für Kontoverfügungen zu missbrauchen [307]. In seiner ersten Erscheinungsform zeigte es sich in der Weise [308], dass mit verschiedenen Spam-Mail-Kampagnen Bankkunden mit mehr oder weniger originellen Forderungen zur Preisgabe ihrer Kontozugangsdaten und besonders von Transaktionsnummern – TAN – bewegt werden sollten [309]. Hierzu kamen vor allem E-Mails mit Formulareigenschaften zum Einsatz, bei der die Kontodaten in die vorgegebenen Felder eingetragen werden sollten [310]. Mit anderen Spam-Kampagnen wurden und werden noch immer Finanzagenten geworben, die die erbeuteten Gel-

---

296 Siehe **5.2 Phishing**.

297 Siehe auch **CF**, Carder, 13.07.2008

298 **WP**, Kreditkartenbetrug

299 **CF**, Zahlungskartenkriminalität, 01.11.2008

300 Thomas **Kuhn**, Die raffiniert dreisten Tricks der Online-Betrüger, wiwo.de 06.11.2008

301 **CF**, Schattenwirtschaft im Internet, 24.11.2008

302 Cyberkriminelle lieben Kreditkarten, tecchannel 24.11.2008

303 **CF**, Gegenspionage wider 'ZeuS' und 'Nethell', 19.12.2008

304 Trojaner stiehlt Zugangsdaten von 300.000 Bankkonten, Heise online 03.11.2008

305 **CF**, "Nachladen" von Guthabenkarten, 2007

306 **WP**, Phishing

307 **CF**, Phishing: Zusammenfassung krimineller Methoden, 2007

308 Siehe auch **CF**, Phishing. Wie funktionieren die Informationstechnik und das Internet? 22.01.2007.

309 **CF**, Phishing-Aktion, 2007;
die alte Vorgehensweise taucht gelegentlich immer noch auf: **CF**, TAN-Nachweis, 02.03.2010.

310 **CF**, Formen des Phishings, 2007;
siehe auch **CF**, Urteil gegen Phisher-Gruppe, 04.09.2008

der an die Hinterleute weiter leiten sollen [311].

Ende 2007 wandelte sich die Gestalt des Phishings [312]. Die E-Mails forderten die Bankkunden nicht mehr dazu auf, per Mail zu antworten, sondern aus Sicherheitsgründen die (nachgemachte) Bankseite im Internet aufzusuchen, um dort weitere Anweisungen zu erhalten. Daraus wurde schnell ein Massenphänomen, das als Pharming bezeichnet wird [313]. Dazu werden auf einem gehackten Webserver eine Vielzahl nachgemachter Bankseiten verschiedener Finanzinstitute abgelegt, zu denen die Kunden verführt werden. Auch wenn die nachgemachten Webauftritte nur wenige Tage aktiv blieben, so reichte das den Tätern für ihre kriminellen Geschäfte aus.

Gleichzeitig wurden das Layout der Anschreiben und der Webseiten immer besser und auch die Sprache fehlerfrei und jargonangemessen [314]. Als thematischer Aufhänger wird jede Gelegenheit genutzt, um das Interesse der Bankkunden zu wecken, so auch die Finanzkrise [315].

Seit 2008 werden kaum noch Phishing-Mails versandt. Die Täter sind dazu übergegangen, harmlos wirkende und in den Suchmaschinen gut platzierte Webseiten zu manipulieren, um darüber Bankkunden auf nachgemachte Bankseiten zu führen [316]. Dazu entstand äußerst schnell in der Underground Economy ein Markt für ausgespähte Konto- (Phishing) und Kartendaten (Carding) [317] sowie Dienstangebote zur Erstellung von Phishing-Seiten [318].

Dadurch ist das Phishing und der Einsatz von Botnetzen zusammen gewachsen. Beide benötigen eine ständige Verfügbarkeit im Netz, die Botnetze für ihre CC- [319] und Fluxserver [320] und Phishing-Malware für ihre Updates sowie für die Formulare, die sie beim Angriff einsetzt [321].

Die wichtigste Gegenmaßnahme der Finanzwirtschaft ist die Einführung indizierten Transaktionsnummern, iTAN gewesen [322]. Bei ihrem Einsatz fragt das Rechenzentrum der Bank keine beliebige TAN aus der dem Kunden vorliegenden Liste ab, sondern eine bestimmte aus der jetzt durchnummerierten Liste. Verwandte Verfahren werden zum Beispiel unter den Bezeichnungen mTAN [323] und eTAN [324] betrieben. Bei einem anderen, aufwändigen Verfahren werden Grafiken und Schlüsselcodes sowohl per Internet wie auch per Mobilfunk ausgetauscht, wobei grafische Anzeigen manuell übertragen werden müssen [325].

Silentbanker war der erste im Herbst 2007 aufgetretene Trojaner, der sich unmittelbar in den Homebanking-Vorgang einschaltete und Kontoverfügungen manipulierte [326]. In Brasilien wird der dort sehr verbreitete Einsatz von Onlinebanking-Malware unter dem Begriff Password Stealer diskutiert [327].

Die neue Generation dieser Malware überträgt zunächst nur einen Loader. Dabei handelt es sich meistens um sehr kleine Kommandopakete, die sich zusammen mit attraktiven Anwendungen, Dokumenten oder Bildern einnisten und installie-

---

311 **CF**, Finanzagenten, 2007

312 **CF**, Lagebild IT-Sicherheit 2007, 12.03.2008

313 **CF**, Anstieg von Phishing-Seiten (Pharming), 21.06.2007

314 **CF**, Länderstudie Deutschland, 27.07.2008

315 **CF**, Die Krisenphisher, 22.12.2008

316 **CF**, Massenhacks von Webseiten werden zur Plage, 14.03.2008

317 **CF**, geklaute Daten zum Schnäppchenpreis, 09.04.2008

318 **CF**, qualitätskontrollierter Kontomissbrauch, 09.05.2008

319 Command-and-Control-Server; zentrale Steuerung eines Botnetzes.

320 Dezentrale Steuerung eines Botnetzes durch (gekaperte) Webserver. Dabei bleibt der CC-Server getarnt.

321 Daniel **Bachfeld**, Einzelne Bande war für zwei Drittel aller Phishing-Angriffe verantwortlich, Heise online 17.05.2010

322 Sie wird gelegentlich auch mit einer Bestätigungsnummer – BEN – kombiniert.

323 **CF**, Sicherheit von Homebanking-Portalen, 22.03.2008;
CF, Bezahlen mit dem Handy, 25.01.2008

324 **WP**, eTAN-Generator (BW-Bank)

325 Fotohandy-Verfahren trickst Trojaner aus, tecchannel 05.11.2008

326 **CF**, neue Methode gegen Homebanking-Malware, 06.11.2008

327 **CF**, Länderstudie Brasilien, 27.07.2008

ren [328]. Nach der Methode, die auch die Botnetz-Malware verwendet, nimmt der Loader sodann Kontakt zu seinem Update-Server auf und lädt die Programmteile und Einstellungen, die als Malware zum Einsatz kommen sollen. Auf diese Weise können auch neue Bestandteile installiert oder die Tarnung erneuert werden [329].

Die ersten bekannt gewordenen Formen überwachten und protokollierten den Homebanking-Vorgang, brachen eine Überweisung des Opfers nach Eingabe der Transaktionsnummer – TAN – ab und übermittelten die Kontozugangsdaten, also Kontonummer und Persönliche Identifikationsnummer – PIN – sowie die ausgespähte TAN an die Drop Zone, den sicheren Speicherort des Täters. Danach kappte die Malware die Internetverbindung des Opfers und verhinderte die Wiederaufnahme der Verbindung. Aus der Drop Zone nahm der Täter die ausgespähten Daten auf und missbrauchte das Konto des Opfers mit etwas zeitlichem Verzug.

Die Entwicklung ging weiter. Neuere Methoden führen den Missbrauch direkt während der Homebanking-Session des Opfers aus [330]. Dazu kann die Malware selbständig eine Überweisung generieren mit den Empfängerdaten, die ihr entweder fest einprogrammiert sind oder die sie vom Update-Server holt. Von dem Opfer erfordert sie entweder mit Tricks die Eingabe der vom Bankserver erforderten iTAN (z.B. mit einem Sicherheitshinweis oder anlässlich von Seitenaufrufen, die üblicherweise keine Angabe einer iTAN verlangen - wie bei der Kontoübersicht) oder sie wartet, bis das Opfer selber eine Transaktion ausführt. In diesen Fällen wird dem Opfer mit entsprechend manipulierten Bildschirmanzeigen vorgegaukelt, dass nur die von ihm gewollte Transaktion ausgeführt oder bestätigt wird. Bachfeld: *Solche Trojaner bauen eigene Verbindungen zum Online-Banking des Kunden auf und nehmen mit einer abgeluchsten TAN eigene Überweisungen vor. Dabei präsentieren sie dem Anwender im Browser nachgemachte Banking-Seiten. Der Trojaner Win32.Banker.ohq soll beispielsweise laut dem Antiviren-Spezialisten Kaspersky 56 Bankenseiten imitieren können.*

Eine Variante davon übermittelt den Beginn der Homebanking-Session dem Täter, der sich dann als Man-in-the-Middle einklinken kann und die beschriebenen Manipulationen von Hand durchführen kann.

Auf eine gemeine Phishing-Variante ist ein Mitarbeiter der US-Supermarktkette Supervalu hereingefallen. In einer E-Mail haben die Täter behauptet, dass sich die Kontoverbindungen von zwei Lieferanten geändert habe. Der Mitarbeiter änderte die Kontodaten. Dadurch flossen innerhalb weniger Tage etwa 10 Millionen $ auf Nimmerwiedersehen auf die Konten der Phisher [331].

A.4 5.3 Beutesicherung

Finanzagenten dienen dazu, die Geldbeträge von den Konten der Phishingopfer an die Hinterleute weiter zu senden. In den frühen Fällen versuchten die Täter, das Geld unmittelbar in die Länder des Baltikums oder nach Russland zu überweisen, was an den Sicherheitsprüfungen der Banken ganz überwiegend scheiterte.

Die Finanzagenten wurden meistens damit beauftragt, das auf ihren Konten eingehende Geld über Western Union ins Ausland zu transferieren [332]. Das Unternehmen geriet dadurch in den Ruf, leichtfertig Kriminelle zu unterstützen, und leitete bereits 2006 Gegenmaßnahmen ein. Seither sind keine anonymen Transaktionen in Deutschland möglich und müssen sich alle Kunden ausweisen. Im Ausland sieht das anders aus; die Empfänger bleiben unerkannt.

Nach einem oder zwei Einsätzen sind die Finanzagenten verbrannt. Sie machen sich wegen leichtfertiger Geldwäsche strafbar [333] (§ 261 StGB) und haften den Phishingopfern in voller Höhe des Geldbetrages, der ihren Konten belas-

[328] **CF**, Phishing mit Homebanking-Malware, 22.10.2008

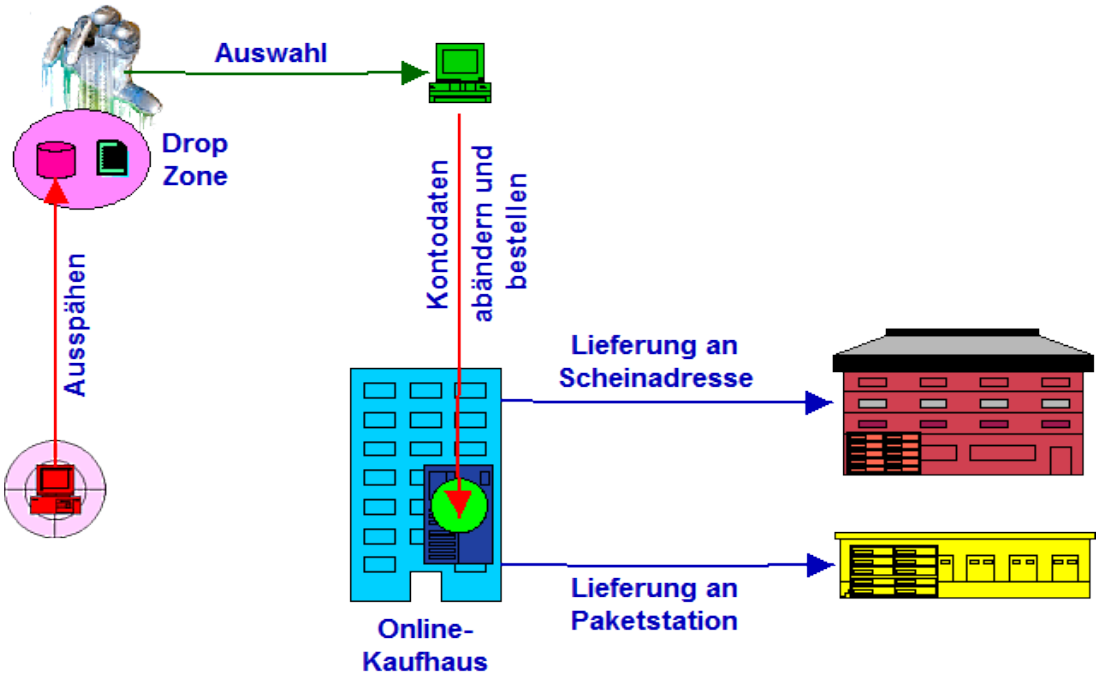
[329] **CF**, Formularfelder von Trojaner Limbo, 30.09.2008

[330] Daniel **Bachfeld**, Zahl oder Karte. Sicherer Zugriff aufs Online-Konto, c't 17/2008, S. 94

[331] **CF**, Kontoverbindungs-Phishing, 31.10.2007

[332] **CF**, Auslandsüberweisungen per Bargeldtransfer, 2007

[333] **CF**, Finanzagenten, 2007



tet wurde [334].

Die Beutesicherung stellt deshalb eines der größten Probleme für die Phishing-Täter dar. Sie experimentieren deshalb mit allen Formen der Geldwäsche, die schon bekannt sind [335] und mit Web-Money und Paysafecard weitere Spielarten bekommen haben [336].

Eine Variante davon sind die Paketagenten [337]. Sie stellen keine Lieferadresse für Geldüberweisungen zur Verfügung, sondern empfangen an ihrer Privatadresse Pakete, die mit werthaltigen Waren gefüllt sind (Elektronik, Arzneimittel und entsprechende Handelsgüter) und die sie an die ausländische Zieladresse weiter senden. Nicht selten wird bei ihrer Einwerbung an ihrem Robin-Hood-Nerv gerüttelt: Die Handelsbeschränkungen der EU würden Drittländer benachteiligen und deshalb könnten die Paketagenten mehr Gerechtigkeit in die Handelswelt durch ihr Tun bringen. Natürlich sei alles ganz legal – wenn da nicht das Strafrecht wäre (Absatzhilfe [338], § 259 Abs. 1 StGB).

Jedenfalls im Zusammenhang mit dem Phishing scheinen sich die Täter qualifiziert und getrennt zu haben. Die Anwerbung von Finanzagenten und die Durchführung des Phishings selber scheinen jetzt unterschiedliche Operation Groups zu praktizieren.

A.4 5.4 Online-Warenhäuser

Das Schaubild zeigt das vollständige Vorgehen der Täter beim Missbrauch von ausgespähten Zugangsdaten zu Warenhaus-Konten. Zunächst werden von einer Malware die persönlichen Daten des Opfers ausgespäht, protokolliert und in einer Drop Zone [339] wahllos abgelegt. "Interessenten" können dann mit einer einfachen Software den Datenbestand sichten, auswerten und die sie interessierenden Daten erwerben.

Mit diesen Daten sucht der Täter das vom Opfer genutzte Online-Warenhaus auf und ändert zunächst das Kennwort, womit er den rechtmäßigen Inhaber des Kontos von der weiteren Nutzung ausschließt. Sodann ändert der Täter die Lieferadresse. Die neue Lieferadresse wird meistens sein:

⇨ Anschrift eines Agenten, der den Weiterversand durchführt. Wie dem Finanzagenten droht diesem Annahmeagenten die Identifikation und Strafverfolgung.

---

[334] Zum Beispiel LG Köln, Urteil vom 05.12.2007 - 9 S 195/07

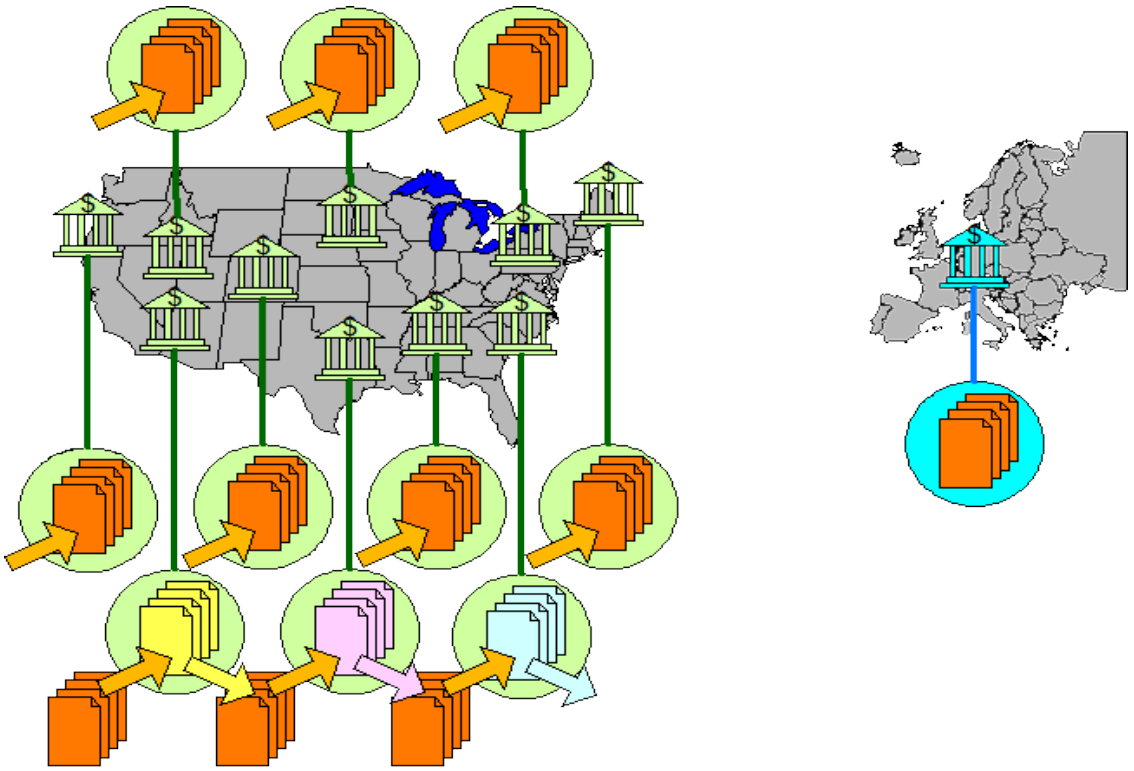
[335] **CF**, grenzüberschreitender Vermögenstransfer, 2007

[336] **CF**, Beutesicherung, 11.04.2010

[337] **CF**, Transfer von Sachwerten, 2007

[338] Dieter **Kochheim**, Der Hehler ist kein Stehler. Hehlerei und Absatzhilfe, 11.11.2009

[339] **CF**, Drop Zone, 13.07.2008



⇨ Scheinadresse, z.B. eine leer stehende Wohnung in einem Mehrfamilienhaus. Am Klingelschild und am Briefkasten müssen nur passende Namen angebracht werden. Für die Kontrolle des Briefkastens und die Entnahme von Zustellbenachrichtigungen empfiehlt sich ein freundlicher Hausbewohner.

⇨ Gemietetes Paketfach in einer Packstation. Die Abholung erfolgt dann anonym und außerhalb der Geschäftszeit.

⇨ Die Lieferung an eine Packstation lässt sich auch mit einem Nachsendeantrag koppeln. Das verhindert, dass das Warenhaus misstrauisch wird.

⇨ Lieferung ins Ausland. Die europa- und weltweit operierenden Paketdienste machen es möglich. Nur das Warenhaus wird das wahrscheinlich nicht mitmachen.

Sobald die Kontodaten abgeändert sind, kann der Täter bestellen. Das Nachsehen hat das Opfer, dessen Daten missbraucht werden. Seinem Konto werden die Kosten belastet und es hat den Ärger am Hals.

A.4 **5.5 Aktienkursmanipulation**

In der klassischen Variante der Aktienkursmanipulation erwirbt der Täter zunächst Penny-Stocks zu einem kleinen Preis und versucht dann mit Spam-Aktionen und anderer gezielter Öffentlichkeitsarbeit Käufer für diese Aktien zu gewinnen. Je mehr er zum Kauf überredet, desto höher steigt der Marktpreis der Aktien und damit der Depotwert des Täters. Zur passenden Zeit verkauft er seine Aktien zu dem gepushten Preis.

Eine neue Spielart verzichtet auf die Öffentlichkeitsarbeit und ersetzt sie durch Hacking und Kontomanipulationen.

Zunächst muss der Täter auch bei dieser Methode investieren, indem er ein Aktienpaket mit Penny-Stocks erwirbt und vom Ausland aus in ein Aktiendepot in Deutschland stellt (blau unterlegt). Danach startet er eine groß angelegte Aktion in den USA, bei der er die Aktiendepots von Bankkunden missbraucht. Die einlagernden Wertpapiere verkauft der Täter und erwirbt dafür genau die Penny-Stocks, die er vorher selber eingekauft hat (hellgrün unterlegt).

Je mehr Depots er auf diese Weise missbraucht, desto höher steigt der Kurs der Aktien und damit auch der Kurswert seines Depots. Sobald der

Einkauf der Aktien den Grad der Marktsättigung und der Kurs den höchstmöglichen Stand erreicht haben, verkauft der Täter seinen eigenen Wertpapierbestand - an eines der von ihm missbrauchten USA-Depots und mit höchsten Gewinn. Diesen streicht er ein, indem er das eigene Depot in Deutschland auflöst. In den USA verlieren die manipulierten Depots darauf ganz erheblich an Wert. Die meisten dürften dann auf fast Null gefahren sein (insbesondere dann, wenn der Täter im Aktienhandel auch aus den Depots mit großen Beständen, die er zu Beginn seiner Aktion angelegt hat, Verkäufe zulässt).

Dieses Beispiel zeigt die fatale Folge davon, dass im Bereich der Cybercrime die Täter zwar international agieren, die Rechtsordnungen jedoch an den nationalstaatlichen Grenzen enden.

Selbst wenn man auf das Beispiel vollständig das deutsche Strafrecht anwenden könnte, wären die Einrichtung, der Betrieb und die Auflösung des Aktiendepots in Deutschland - für sich allein betrachtet - nicht strafbar.

Die Manipulationen in den USA wären nach deutschem Recht als Computerbetrug (§ 263a StGB) und Fälschung beweiserheblicher Daten (§ 269 StGB) strafbar. Der Handlungsort und alle anderen eine örtliche Zuständigkeit begründenden Umstände sind im Ausland angesiedelt, so dass die Strafverfolgung in Deutschland nicht zulässig ist.

Die Wertsteigerung des Aktiendepots in Deutschland begründet keinen Erfolgsort im Sinne von § 7 Abs. 1 StPO. Das liegt daran, dass die Strafvorschrift über den Betrug (§ 263 StGB) und ihr folgend für den Computerbetrug (§ 263a StGB) nach einer Stoffgleichheit zwischen den Vermögensschäden, die durch die Manipulationen in den USA entstanden sind, und dem Vermögenszuwachs verlangen, den er erlangt hat.

Daran fehlt es aus zwei Gründen. Der Wertverlust in den USA tritt erst ein, nachdem der Täter seinen Aktienbestand verkauft hat und er weitere Kursmanipulationen in den USA unterlässt. Die Stoffgleichheit verlangt hingegen, dass ein Vermögensnachteil auf der einen Seite unmittelbar zu einem Vermögensvorteil auf der anderen Seite führt.

Außerdem erfolgt die Wertsteigerung im deutschen Depot nicht dadurch, dass Zahlungen eingehen, sondern dadurch, dass der Tauschwert an der Börse gestiegen ist. Der Wertzuwachs gründet also auf einem Tauschmechanismus, auf den der Täter zwar mittelbar (durch immer neue Kaufnachfragen) Einfluss genommen, den er aber nicht unmittelbar beeinflusst hat. Somit fehlt es an der Stoffgleichheit.

A.4 6. Fazit

Mit der wachsenden Internetnutzung entfaltet und verbreitet sich auch der Identitätsdiebstahl. Ihm geht es darum, andere zu schädigen, indem ihr Ansehen missbraucht oder ihr Vermögen gestohlen wird.

Seine Formen richten sich gegen alle sozialen und wirtschaftlichen Prozesse im Internet. Bevorzugt werden Geldgeschäfte. Aber auch private Äußerungen können zum Social Engineering und zur Tarnung der Täter missbraucht werden.

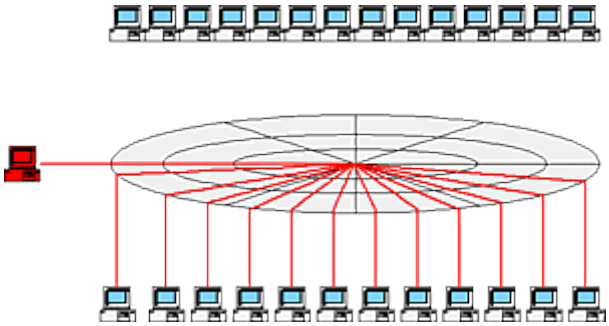
Das Internet ist keine Kuschelzone, sondern ein öffentlicher Raum, in dem Gefahren lauern. Es verlangt nach einem bewussten Umgang und einer gewissen Zurückhaltung, wenn es um die Offenbarung peinlicher oder wirtschaftlich wertvoller Informationen geht.

Jede offenbarte Information, die für sich alleine oder in Verbindung mit anderen Informationen einen Missbrauch ermöglicht, birgt die Gefahr, dass ein solcher Missbrauch auch erfolgt. Das lehren die hier beschriebenen Beispiele. Sie zeigen auch, dass das Internet kein abgeschlossenes Paralleluniversum ist, sondern ein integraler Bestandteil unserer heutigen Lebensumgebung. Es hat Besonderheiten, weil es keine Grenzen und wahrnehmbare Entfernungen kennt. Dadurch ist es schnelllebig und pausenlos.

A.5 Botnetze

1993 wurde die erste Botsoftware eingesetzt: Eggdrop [340]. Spätestens seit 2005 sind die Botnetze im Interesse der Fachöffentlichkeit [341], während die meisten Privatanwender wenig über sie wissen [342]. Es handelt sich dabei um infiltrierte Rechner in großer Zahl [343], die z.B. für Spam-Aktionen oder verteilte Angriffe [344] missbraucht werden können. Drei Gruppierungen scheinen dabei um den größten Marktanteil zu kämpfen: Warezov, Bagle und Zhelatin.

In der frühen Entwicklungsphase war das Schicksal eines infiltrierten PCs in erster Linie ärgerlich und kostenträchtig, weil die Bot-Malware "nur" Kosten für die Verbindungen zum Internet schmarozte, echte Schäden aber nur bei Dritten verursachte (Sankt Florian lässt grüßen). Mit den Entwicklungen im Zusammenhang mit dem Phishing und dem Identitätsdiebstahl sind alle befangenen PCs aber beängstigenden Gefahren unterworfen.



Botnetze: Angriff der unerkannten Computerzombies

... Der Ursprung der Botnetze liegt in der Internet Relay Chat (IRC)-Szene und klingt wie ein Märchen. Einst wurden dort Nutzer, die gegen die Regeln verstießen, hinausgeworfen - eine virtuelle Vertreibung aus dem Paradies. Einige von ihnen wollten sich rächen und entwickelten Wege, um die IRC-Server oder Kanäle zu schädigen. Dies war vor allem deswegen so einfach, weil IRC ein sehr offenes Protokoll ist, das ähnlich wie SMTP (Send Mail Transfer Protocol), leicht missbraucht werden kann. Im Laufe der Zeit entwickelten sich kleine Programme, die nun auch Server angreifen konnten, die nichts mit IRC zu tun hatten - die ersten Denial-of-Service-Attacken. Noch heute nutzen viele Hacker den IRC-Kanal als Kommunikationsstrang, über den sie ihre Botnetze kontrollieren.

Um ein Botnetz zu bauen, muss das entsprechende Programm erst einmal auf den Nutzerrechner gelangen. Meisten werden dafür Sicherheitslücken in Windows oder Server-Systemen ausgenutzt. Viren oder Würmer dringen durch diese Schlupflöcher auf den Rechnern ein und hinterlassen tief im System eine kleine .exe-Datei, die sich selbst fortpflanzt und durch eine Hintertür Kontakt mit ihrem "Herren" aufnimmt. Das tut sie, indem sie sich auf einen bestimmten IRC-Channel einwählt und dort still und leise auf Befehle wartet. Der Nutzer bekommt davon im Idealfall nichts mit. … [345]

A.5 1. Infektion und Infiltration

Zum "Zombie" wird der eigene Rechner zunächst durch Injektion. Sie nutzt alle Wege, die die Malware kennt: Fremde Datenträger, Anhänge an E-Mails, Infusionen (Injektions) beim Aufruf von Webseiten - als Beigabe zu aktiven Funktionen - und die direkte Manipulation eines Handwerkers. Im zweiten Schritt muss sie sich einnisten (Infektion)

Gegen die Methoden des Social Engineering, die uns zu übertöpeln versuchen (persönliche Kontakte, E-Mail-Anhänge, Website-Injection), hilft die Vorsicht in Kombination mit Firewalls und Virenscannern, die auch gegen die aktive Malware wirken (z.B. IP-Würmer).

---

[340] Rob **Thomas**, Was sind Bots und Botnetze? RUS-Cert 2003

[341] Sturm-Wurm-Botnetz mit über 1,7 Millionen Drohnen, Heise online 18.08.2007

Tom **Fischer**, Botnets, RUS-Cert - Uni Stuttgart 14.03.2005

BSI, Bot-Netze, BSI 2007

[342] Symantec-Umfrage: Bots und Botnetze kaum bekannt, Heise Security 15.06.2007

[343] Schädliche E-Mails bauen riesige Botnetze auf, Chip online 23.08.2007;

Krieg der Würmer, Heise online 14.05.2007;

Weihnachten ließ Botnetze schrumpfen, Heise online 28.12.2006

[344] **WP**, Distributed Denial of Service - DDoS

[345] Auszug aus Nicola D. **Schmidt**, Botnetze: Angriff der unerkannten Computerzombies, ZDNet.de 26.08.2005

Die Methoden, fremde Rechner steuern zu wollen, entstammen offenbar verschiedenen Quellen.

ZDNet.de sieht ihren technischen Ursprung zu Recht im Internet Relay Chat – IRC [346].

Hier ging es aber um sehr harte Methoden, um Zugangsbeschränkungen zu umgehen. Die aktuelle Botnetz-Software ist feinsinniger [347] und dürfte wegen ihrer Steuerungsfunktionen ihre Heimat eher in den gewerblichen Strategien zur Softwareverteilung und im zentralen IT-Management haben [348].

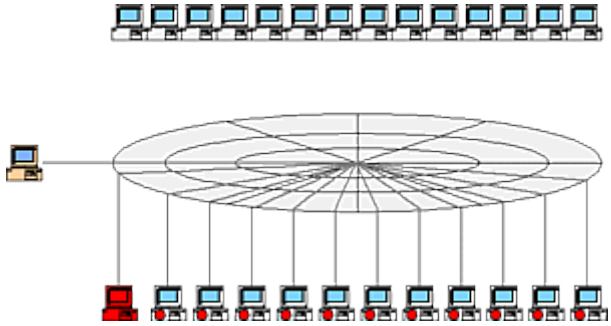
Mit der Botsteuerung "Zunker" lassen sich zum Beispiel alle infiltrierten Systeme wegen ihrer Erreichbarkeit und Leistungsmerkmale überwachen, steuern und für Aktionen koordinieren [349]. Diese Funktionsvielfalt ist sonst nur aus der Fernwartung [350] für zentral verwaltete Computernetzwerke bekannt.

A.5 2. Übernahme. Konsole

Die ersten Schritte für die Infiltration unternimmt die Bot-Software selbsttätig. Sie wirkt so, wie es auch von anderen Würmern und Trojanern bekannt ist, nistet sich ein, manipuliert die Sicherheitseinstellungen sowie die Firewall und tarnt sich vor der Entdeckung durch Viren- und anderen Malwarescannern [351].

Anschließend prüft sie, ob der infiltrierte Rechner eine Verbindung zum Internet hat und meldet sich dann bei der Botnetz-Steuerung als bereit.

Die zentrale Steuerung sollte keinen direkten Hinweis auf den Angreifer geben. Deshalb befindet sie



sich in aller Regel auf einem gehackten IRC-Server.

Der Angreifer kann das infiltrierte System missbrauchen wie ein erfolgreicher Hacker. Alle Systemfunktionen, Dokumente und ungesicherte Informationen stehen ihm offen [352].

Eine übliche Strategie besteht darin, das System als Konsole für die Botnetzverwaltung einzurichten und hiermit die übrigen Zombies zu verwalten und zu steuern. Bei einer Analyse des Botnetzes kann dann nur der infiltrierte Rechner festgestellt werden, nicht aber die Herkunft des Angreifers.

A.5 3. zentrale und dezentrale Steuerung

Für die Steuerung des Botnetzes muss zumindest ein zentraler Server eingerichtet werden. Seine wichtigste Eigenschaft ist die, dass er eine kontinuierliche Verbindung zum Internet haben muss, also kein Gelegenheitsnutzer ist. Hierzu eignen sich am besten Webserver, die als Hostserver Internetauftritte präsentieren. Beliebte Standorte für missbrauchte Systeme sind in den USA und in Asien. Mit der zunehmenden Verbreitung dedizierter Server [353] bei Privatanwendern und ihrer häufig unzureichenden Sicherung dürften besonders diese Systeme zum Missbrauch reizen.

Die zentrale Steuerung kann für verschiedene Zwecke eingesetzt werden. Die gebräuchlichsten sind:

⇨ Kontaktstelle für infiltrierte Botrechner

⇨ Ablagestelle für ausspionierte Daten

⇨ Depot für Programmupdates

---

346 **WP**, Internet Relay Chat - IRC

347 Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006;
Ihr PC als Komplize: Piraten-Software gezielt bekämpfen, Heise online 06.01.2007

348 **WP**, IT Infrastructure Library - ITIL

349 "Zunker", das Administrator-Tool für Bot-Netze, IT-Defender.com 15.05.2007
Zunker Bot, PandaLabs Blog 08.05.2007;
Screenshot, ebd.

350 **WP**, Fernwartung

351 **CF**, Datenveränderung, 2007; **CF**, Computersabotage, 2007; **CF**, Superwürmer, 2007; **CF**, Malware, 12.05.2008.

352 Vergleichbar mit der Quellen-TKÜ: **CF**, Online-Zugriff an der Quelle, 08.11.2008.

353 **WP**, Dedizierter Server

⇨ Hostplattform für "Pharmen"

Aktuelle Botnetze haben keine zentrale Steuerung, sondern verfügen über eine Zwischenschicht aus Proxyservern [354].

Bei ihnen wird zwischen dem zentralen IRC-Server, dem "Mutterschiff", und den infizierten Zombies ein "Fast-Flux-Netz" installiert, das aus Proxyservern besteht, von denen jeder ein Teil der Zombies steuert und verwaltet.

Hierzu bekommen die Zombies bereits mehrere Internetadressen (IP) einprogrammiert, an die sie ihre Bereitschaft melden. Wird der erste Kontakt herstellt, können sie mit neuen Instruktionen versehen werden. Fällt ein Proxy aus, so können seine Aufgaben von einem anderen wahrgenommen werden.

Das "Mutterschiff" versteckt sich hinter den Proxies und kann vom Zombie aus nicht lokalisiert werden. Erst wenn die "Abwehr" einen der Proxies überwachen kann, kann sie dessen Steuerung und somit das "Mutterschiff" erkennen.

A.5 4. Einrichtung des Botnetzes

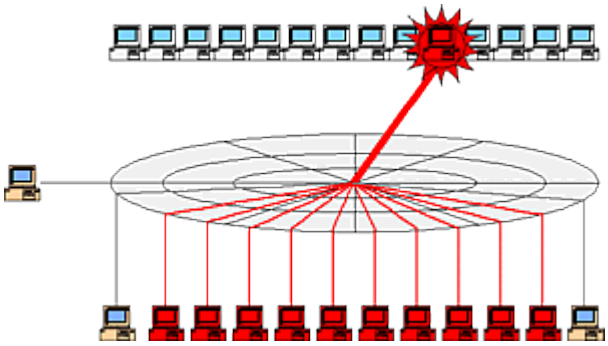
Die infiltrierten Rechner melden ihre "Bereitschaft" an die einprogrammierte IP-Adresse des "Mutterschiffes" oder den zwischengeschalteten Proxyservern.

Während die Dateien, die für die Infiltration erforderlich sind, so klein gehalten werden können, wie sie für den Angriff nötig sind, können jetzt neue Versionen (Updates), Erweiterungen und Einsatzziele übermittelt und installiert werden.

Über diese perfide Strategie verfügen erst neuere Würmer und Trojaner. Sie zeigt das erhebliche Wissen, die konsequente Planung und die gewissenlose Durchführung, die mit den modernen Angriffen mit den Methoden der Cybercrime verbunden sind. Die kriminelle Energie, mit der die Botnetz-Betreiber agieren, steht der der Phisher in nichts nach [355].

[354] Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007, S. 76; **CF**, Angriffe und Botnetze, 01.10.2007.

[355] **CF**, Phishing, organisierte Strukturen, 2007



A.5 5. kriminelle Einsätze

Im Anschluss an die Übernahme durchforstet die Bot-Malware zunächst den Zombie nach den persönlichen Daten des Anwenders, die sich zu einem Missbrauch eignen. Sie werden an eine Drop Zone gesendet, wo sie in aller Regel von Interessierten durchgesehen und erworben werden können.

Ein „guter“ Zombie ist ein technisch gut ausgestattetes System mit einem ständigen Anschluss an das Internet. Mit möglichst vielen Zombies, die in das Botnetz eingebunden sind, lassen sich jede Menge krimineller Aktionen durchführen – und damit Geld verdienen.

A.5 5.1 verteilter Angriff

Ein häufiger Einsatz ist die Durchführung von verteilten Angriffen [356]- DDoS. Hierbei richten viele koordinierte Rechner immer wieder dieselben Kontaktanfragen an einen ausgewählten Server, der diese Menge irgendwann nicht mehr bewältigen kann und seinen Betrieb einstellt. Viele namhafte Internetdienste sind bereits das Opfer solcher Angriffe geworden [357].

Allein mit der Drohung der Täter, sie könnten gegen einen gewerblichen Internetdienst einen DDoS-Angriff durchführen, lässt sich Geld verdienen. Solche Ansinnen sind seit Jahren bekannt

[356] **WP**, Denial of Service (Distributed Denial of Service – DdoS); siehe Grafik oben.

[357] **BSI**, Denial-of-Service-Attacken, BSI 2007; Matthias **Bernauer**, Leonard **Rau**, Netzwerkangriffe durch DDoS-Attacken, Uni Freiburg 27.01.2006; Mailserver ächzen unter Spam-Last, Heise online 25.05.2007; **CF**, täglich 250.000 neue Zombies, 26.09.2007

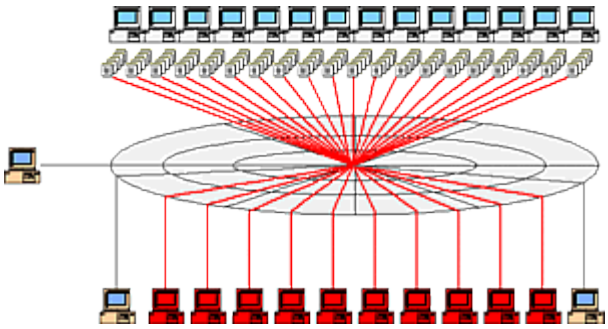
und man nennt sie auch Erpressung [358] (§ 253 StGB, [359]).

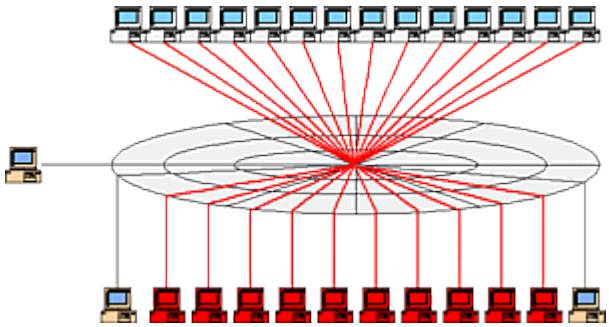
Die Folgen eines DDoS-Angriffs können aber auch ganz unbeabsichtigt aufgrund eines unvorhergesehenen Interesses der Internet-Öffentlichkeit eintreten, wie eBay schmerzlich erfahren hat [360].

A.5 5.2 Spamming und Phishing

Das werbende Spamming [361] und das Phishing [362] sind erst dadurch möglich geworden, dass E-Mails massenhaft an eine Vielzahl von Empfängern versandt werden und nur eine verschwindende Zahl erfolgreich bleibt [363].

Schon der "normale" Versand von Spam-Mails ist kostengünstig. Noch billiger wird er, wenn gehackte Server oder Botnetze zum Einsatz kommen [364].





[358] Beispiele: Belohnung für Hinweise zu DDoS-Attacken, Heise online 12.07.2007;
Patrick **Brauch**, Geld oder Netz! Kriminelle erpressen Online-Wettbüros mit DDoS-Attacken, c't 14/2004, S. 48;
Frank **Ziemann**, Erpressungen mit DDoS-Angriffen nehmen zu, PC-Welt 20.05.2005;
50 Jahre Haft für den PC-Kidnapper? spiegel.de 04.11.2005.

[359] **CF**, besonders schwere Computersabotage, 2007

[360] BR, "Papst-Golf" wird zum Streitwagen, br-online.de 06.05.2005 (nicht mehr verfügbar);
Papst-Golf bringt fast 190.000 Euro - und Streit, netzwelt 06.05.2005.
Als „Heise-DoS“ ist der Effekt bekannt, dass Quellen, zu denen das Online-Magazin verlinkt, durch den plötzlichen Besucheransturm nur noch verzögert reagieren oder gar nicht mehr erreichbar sind;
WP, Slashdot-Effekt.

[361] **CF**, Spamming mit missbrauchter Absenderadresse, 23.04.2007

[362] Siehe **CF**, Zusammenarbeit der Szenen, 2007;
Spammer und Phisher rüsten auf, Heise online 18.08.2007;
E-Mails: 90 Prozent sind Spam, Heise online 13.05.2007;
Viren- und Botnet-Aktivitäten haben zugenommen, itseccity.de 18.04.2007;
Das Dreckige Dutzend: Die zwölf aktivsten Länder beim Spam-Versand Stratio-Wurm sorgt für Anstieg bei weltweitem Spam-Aufkommen, Sophos 06.11.2006.

[363] Kalkuliert werden die Spams wohl üblicherweise mit einer Erfolgsquote von 0,1 %; siehe: Alfred Krüger, Angriffe aus dem Netz. Die neue Szene des digitalen Verbrechens, Heise Verlag 2006, S. 66 f.

[364] Siehe: 50 Jahre Haft für den PC-Kidnapper? spiegel.de 04.11.2005.

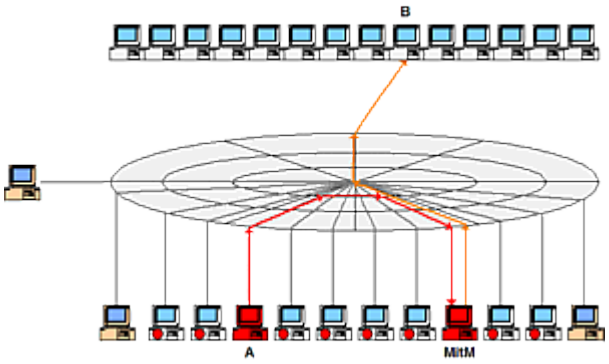
A.5 5.3 direkte Angriffe

Botnetze sind darauf angelegt, größer und größer zu werden. Die größten Masseneffekte lassen sich entweder durch die Versendung von Spam-Mails mit Malware-Anhängen erreichen oder indem man die Malware Adressbereiche im Internet auf Endgeräte mit Sicherheitslücken scannen lässt.

Gemeint ist die Technik der IP-Würmer, die im Internet kaum beschrieben oder diskutiert wird [365]. Sie arbeiten automatisch und suchen systematisch vorgegebene Adressen nach dem Internetprotokoll [366] nach Rechnern ab, die sie übernehmen können.

Im Fall ihres Erfolgs übertragen sie eine Basisversion von sich auf den Zielrechner, die sich wie die Software von Botnetzen einnistet, aktualisiert und erweitert.

Dazu müssen sie eine Sicherheitslücke ausnutzen, die der Programmierer exklusiv nutzt oder die erst kurzfristig bekannt ist, so dass erwartet werden kann, dass sie noch nicht von allen Anwendern geschlossen wurde (Updates von Betriebssystemen und Virensoftware). Bevorzugt werden dazu Fehler in Programmen, die massenhaft im Einsatz sind, weil sie die größten Erfolgsaussichten bieten (z.B. Betriebssysteme und Büroanwendungen).



A.5 5.4 The Man in the Middle

Jedes einzelne Gerät im Botnetz lässt sich auch individuell steuern. Das ermöglicht es dem Angreifer, sich neben dem Anwender als Administrator auf den Zombie einzuloggen und unter der IP-Adresse und Identität des Anwenders zu kommunizieren und jede im Internet mögliche Aktion durchzuführen.

Der Angreifer kann die Steuerungssoftware so einrichten, dass sie den Internetverkehr eines Rechners besonders wegen Homebanking-Aktivitäten überwacht (im Beispiel A). Ein anderes infiziertes Gerät kann er dann dazu verwenden, als Übertragungsstation (Man in the Middle [367]) zum Kommunikationspartner (im Beispiel B) zu wirken. Dabei kann er die komplette Kommunikation überwachen und im passenden Moment für einen Missbrauch unterbrechen (siehe Beispiel im Zusammenhang mit dem Phishing [368]).

A.5 6. Botnetze, die unerkannte Gefahr

Botnetze lassen sich für jede Gelegenheit einsetzen, bei denen es entweder darauf ankommt, als Angreifer unerkannt zu bleiben, oder für Missbräuche, die große Rechnerkapazitäten erfordern. Somit kommen auch Peer-to-Peer-Netze [369], die Verteilung und Speicherung von Dateien (Computercluster [370]) oder die verteilte Nutzung von Rechenleistung (verteiltes Rechnen [371], Distributed Computing) in Betracht.

Der (auch kranken) Phantasie sind bekanntlich keine Grenzen gesetzt.

Der Betrieb von Botnetzen ist neben der Herstellung von Malware im übrigen und dem Phishing die gefährlichste Erscheinungsform der Cybercrime. Ihre Betreiber verfügen über ein erhebliches Wissen und eine kaum zu überbietende Böswilligkeit.

---

365 Peter **Schill**, Die neuen Herausforderungen der Content Security. Netzwerkfilter auf Applikationsebene, eSafe Januar 2004, benennt etwas versteckt drei Beispiele auf Seite 24 der Präsentation: CODERED, SLAMMER, BLASTER.

366 **WP**, Internet Protocol

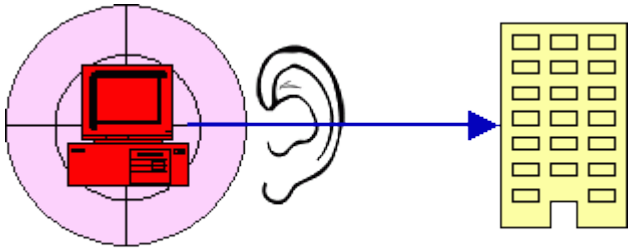
367 **WP**, Man-in-the-middle-Angriff

368 **CF**, Phishing mit Homebanking-Malware, 22.10.2008

369 **WP**, Peer-to-Peer

370 **WP**, Computercluster

371 **WP**, Verteiltes Rechnen



Botnetze lassen sich zu Allem verwenden, was entweder zur Tarnung von Aktivitäten dient oder große Rechenleistungen erfordert. Die häufigste Anwendungsfälle sind der Versand von Spam-Mails und die Durchführung von verteilten Angriffen. Jüngst wurden auch Angebote bekannt, die große Rechenleistungen zum Knacken von Passwörtern erfordern [372].

Botnetze benutzen dieselbe Injektionstechniken, die auch von der Malware im übrigen benutzt werden, also bevorzugt in Form von Anhängen zu Spam-Mails, durch Website-Injection [373] oder als IP-Würmer.

Wie alle anderen Formen der Cybercrime kennen die Betreiber von Botnetzen keine nationalstaatlichen Grenzen, wodurch ihre Verfolgung wenn nicht ausgeschlossen, so doch ganz erheblich erschwert wird.

Über eine internationale Zusammenarbeit der Strafverfolgungsbehörden ist nichts bekannt. Nur private Initiativen haben bisher ein journalistisches Echo erfahren.

Der Wert der Botnetze für billige kriminelle Aktionen wird dafür sorgen, dass sie bleiben, sich allen aktuellen Änderungen der Technik und des Nutzerverhaltens anpassen und weiter verbessert werden.

Das sind keine guten Aussichten.

---

[372] **CF**, Passwort vergessen? Cloud hilft! 19.12.2009; siehe auch: **WP**, Brute-Force-Methode.

[373] **WP**, Cross-Site Scripting

B. Social Engineering

Die technischen Methoden und Tricks, die im ersten Teil beschrieben wurden, haben eine verbindende soziale Komponente. So hinterhältig eine Malware auch programmiert sein mag, sie kann sich in kein technisches System einschleichen, das ihr dazu nicht die Möglichkeit eröffnet. Dazu zählen unüberwachte Schnittstellen, unzureichende Updates, Verzicht auf Virenscanner und Zugangsbeschränkungen sowie unüberlegte Handlungen des Anwenders wie die Gewährung von Administratorenrechten, die unvorsichtige Auswahl von Webadressen oder die fatale Aktivierung von E-Mail-Anhängen.

Die Auseinandersetzung mit der ▸ Malware hat bereits die Techniken der Überredung und Täuschung angesprochen, die in E-Mails und infizierten Webseiten zum Einsatz kommen. Sie sind inzwischen in feiner deutscher Sprache verfasst, treffen den richtigen Ton und suggerieren Vorteile oder drohende Nachteile, die den Anwender zu unbedarften Handlungen veranlassen sollen.

Diese Techniken werden unter dem Begriff des Social Engineering [374] zusammen gefasst und greifen erheblich weiter. Das SocEng kombiniert interaktive und technische Methoden, um seine Zielpersonen auszuspähen, ihre Geheimnisse zu erkunden und schließlich Informationen zu gewinnen, die kombiniert und bewertet werden, um daraus wieder neue Rückschlüsse zu gewinnen.

Der Angreifer handelt immer eigennützig, zielstrebig und gnadenlos, wenn er seine Malware platzieren, Geheimnisse erkunden oder Spionage betreiben will.

Social Engineering benutzt Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, über die sich ein Social Engineer eine gefälschte Identität aneignet. Damit kann der Social Engineer andere zu seinem Vorteil ausbeuten, um mit oder ohne Verwendung von technischen Hilfsmitteln an Informationen zu gelangen.
Kevin Mitnick

Kevin Mitnick [375] ist ein verurteilter Hacker aus den USA. Dem Social Engineering hat er ein wirklich spannendes Buch gewidmet, das er „Die Kunst der Täuschung“ nennt [376]. Die Methoden des SocEng sind klassische Handlungsweisen der Detektive und Spione, die von der Hackerszene entdeckt und für die Penetration informationsverarbeitender Systeme verfeinert wurden. Sie sind bereits begierig aufgenommen worden von den Informationsbrokern und den Industriespionen, die damit ihr Repertoire erweitert haben.

[374] Im Folgenden abgekürzt: SocEng.
WP, Social Engineering (Sicherheit)

[375] **WP**, Kevin Mitnick;
siehe auch: Lothar **Lochmaier**, Risikofaktor Mensch: Die Kunst des Social Engineering, ZDNet.de 27.02.2007

[376] Kevin Mitnick, William Simon, Die Kunst der Täuschung. Risikofaktor Mensch, Heidelberg (mitp) 2003;
CF, IT-Sicherheit, 2008

B.1 Fünf unwichtige Informationen ergeben eine sensible [377]

Beschaffung und Bewertung von Informationen für die Cybercrime

In einer früheren Fassung definierte die Wikipedia das SocEng als die *Kunst, Menschen mittels sozialer Kontakte zu Handlungen zu veranlassen, welche zum Nachteil der Zielperson oder Dritter führen* [378].

"Die Kunst der Täuschung" von Kevin Mitnick [379] ist nicht nur spannend geschrieben, sondern kann als das Standardwerk zum Thema mit der Einschränkung angesehen werden, dass es sich vorrangig um Fallstudien handelt, die nur begrenzt verallgemeinerungsfähig sind.

Mitnick stellt seinem Buch von 2003 eine Definition voran, mit der er das Social Engineering (SocEng) klar von den technischen Methoden des Hackings, dem er sein zweites Buch gewidmet hat [380], und den Überredungstechniken in Spam-Mails und auf Website-Pharmen abgrenzt.

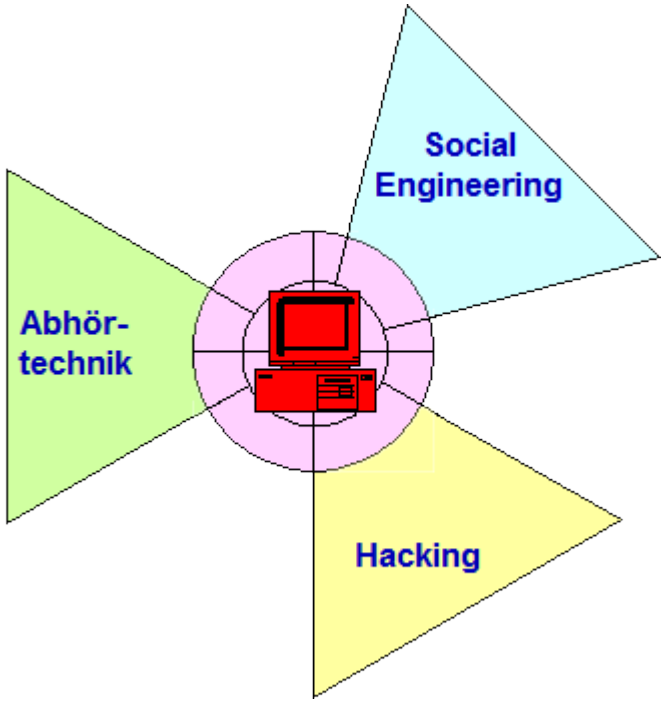
Sie sind wegen ihrer Ähnlichkeiten als SocEng im weiteren Sinne zu betrachten, so dass wir unterscheiden können:

⇨ die kommunikative (sozialpsychologische) Erkundung und Kombination vertraulicher Daten mit dem Ziel, diese zu missbrauchen (SocEng im engeren Sinne),

⇨ den Einsatz von Abhörtechniken und

⇨ den Einsatz von Manipulationsstrategien,

um EDV-Anwender ohne persönliche Ansprache durch Online-Informationsträger zur Offenbarung vertraulicher Informationen (z.B. Phishing) oder zur unbedarften oder heimlichen Installation von schädlichen Programmen (Crimeware [381]) zu veranlassen.



Die Auseinandersetzung mit dem SocEng eröffnet die Chance, die Angreifbarkeit und Sicherheit von Unternehmen und Behörden insgesamt und unter Einschluss der technischen Sicherheit wahrzunehmen, zu bewerten und schließlich Sicherheitsmaßnahmen zu entwickeln.

---

[377] Die erste Fassung dieses Aufsatzes erschien am 01.03.2009.

[378] Jetzt: **WP**, Social Engineering (Sicherheit)

[379] Siehe vorherige Seite.

[380] Kevin Mitnick, William Simon, Die Kunst des Einbruchs. Risikofaktor IT, Heidelberg (mitp) 2006, **CF**, IT-Sicherheit, 2008

[381] Siehe **CF**, gewandelte Angriffe aus dem Netz, 29.11.2008; **CF**, Phishing mit Homebanking-Malware, 22.10.2008; **CF**, Missbrauch fremder Identitäten, 22.11.2008; **CF**, Nummertricks, 21.11.2008.

B.1 1. Security Journal

Dem Schwerpunkt SocEng widmete sich zunächst die englische Fassung des Security Journals von McAfee [382], das später auch auf Deutsch erschienen ist [383].

Die White Papers und sonstigen Publikationen von McAfee werden etwas versteckt im Threat Center [384] präsentiert, aber nicht weiter beworben. Das Security Journal ist die Fortsetzung der jährlichen Berichte über die globalen Sicherheitsbedrohungen, die mich im vergangenen Jahr mit spannenden Länderberichten [385] überrascht haben. Sie sind mit dafür ausschlaggebend gewesen, dass ich zunächst die Theorie von der modularen Cybercrime [386] entwickelt und dann für die modulare Kriminalität [387] verallgemeinert habe.

Die Erfahrungen zeigen (leider), dass ich damit Recht gehabt habe.

B.1 2. Risikofaktor Mensch

Mehr als 60 oder 70 Prozent aller Angriffe gegen Datenverarbeitungssysteme erfolgen nicht von außen, sondern von innen, also von den eigenen Mitarbeitern, die selten aus Böswilligkeit, sondern aus Unwissenheit, aus Unbekümmertheit oder aus Bequemlichkeit Betriebs- und Sicherheitsvorgaben missachten, umgehen oder aushebeln [388]. Dasselbe gilt für Betriebs- und Unternehmensgeheimnisse, die nirgendwo so unüberlegt ausgeplaudert werden wie am Telefon oder in E-Mails an Geschäftspartner.

Angriffe werden zunehmend personalisiert
Die Zahl der interaktiven Angebote im Web wächst ebenso wie die Bereitschaft der Nutzer, persönliche Informationen öffentlich zugänglich zu machen. Immer öfter werden diese Informationen daher auch von Cyberkriminellen missbraucht ...

Auf Social Engineering basierter Spam nimmt zu
Immer öfter verleihen Cyberkriminelle ihren Spam-Nachrichten dadurch Glaubwürdigkeit, dass sie sie mit echten Informationen über die Adressaten anreichern ...

Aktienkursmanipulation schreitet voran
Aktienbetrug per Internet funktioniert üblicherweise nach der Methode "pump and dump". Dabei wird der Kurs von Aktien niedrig bewerteter Unternehmen - sogenannter Pennystocks - durch massenhaft versandte Kaufempfehlungen gezielt in die Höhe getrieben ("pump"), worauf der Betreiber seine zuvor gekauften Anteile unter Ausnutzung des Kurssprungs mit Gewinn auf einen Schlag wieder abstößt ("dump") ...

Betrüger setzen auf die Angst der Anwender
McAfee hat eine zunehmende Verbreitung bösartiger Programme registriert, die sich als Anwendungen von "Sicherheitsanbietern" ausgeben und Internetnutzern mittels Pop-ups angedient werden. Es wird auf eine vermeintliche Infizierung des Rechners hingewiesen, die sich nur unter Anwendung eines bestimmten Programms beheben lässt. Installiert der Nutzer das beworbene Programm, öffnet dieses oft weiterer Malware die Tür …
nach: securitymanager.de

Maßnahmen gegen das SocEng gehören deshalb inzwischen zum Grundschutzstandard für die IT-Sicherheit [389].

Dieser Erkenntnis folgend hat sich bereits in vielen US-amerikanischen Firmen eine Sicherheitsphobie entwickelt, die zu massiven (illegalen) Überwachungen des Telefon- und E-Mailverkehrs geführt hat [390]. Das größte Echo in der Öffentlich-

[382] **McAfee**, Security Journal. Social Engineering (eng.), 09.10.2008;
Internetverbrechen wird persönlich: McAfee Security Journal zum Thema "Social Engineering", securitymanager.de 14.10.2008;
CF, Überredungstechniken, 23.11.2008

[383] **McAfee**, Security Journal. Social Engineering (dt.), 05.10.2008

[384] **McAfee**, Threat Center

[385] **CF**, globale Sicherheitsbedrohungen, 27.07.2008

[386] **CF**, modulare Cybercrime, 07.08.2008

[387] **CF**, modulare Kriminalität, 05.10.2008

[388] IT-Sicherheit: "Interne Mitarbeiter größte Schwachstelle", tecchannel 16.04.2008

[389] **BSI**, Gefährdungskataloge im **BSI**, Grundschutzhandbuch: G 5.42 Social Engineering

[390] Wolf-Dieter **Roth**, Sicherheitsrisiko Mitarbeiter, Telepolis 12.06.2006;
Peter **Mühlbauer**, Trojaner vom Chef, Telepolis 04.04.2006;
Peter **Mühlbauer**, Anonymisieren oder Pseudonymisieren, Telepolis 18.04.2006.

keit erfuhr die interne Untersuchung bei Hewlett-Packard wegen Insiderinformationen aus dem Verwaltungsrat, die an die Medien weitergegeben wurden [391]. In jüngerer Zeit häufen sich aber auch vergleichbare Beispiele aus Deutschland [392].

Studien zur IT-Sicherheit sprechen davon, dass 2005 jeder zwölfte Angriff zum Totalausfall der Firmen-IT geführt hat (8,4 %). In 17,4 % der Fälle waren betriebskritische Anwendungen nicht verfügbar, traten finanzielle Verluste (5,3 %) oder eine Schädigung des Rufes oder der Marke ein (4,2 %). [393]

Als die vier wichtigsten Ursachen, die dem Social Engineering von innen heraus den Boden bereiten, gelten schlechtes Betriebsklima, keine Karrierechancen, Lohndumping sowie mangelnde Fort- und Weiterbildungskonzepte [394].

Dem SocEeng geht es um die Informationsbeschaffung und nicht zwingend darum, die Datenverarbeitung zu stören. Ihr Arsenal besteht aus allen Methoden der Manipulation und Suggestion: „*Täuschung, Bestechung, Erpressung, Einschüchterung, Bedrohung, Appellieren an die Hilfsbereitschaft oder Ausnutzen der Arglosigkeit des Opfers*“ [395].

Die dazu entwickelten Angriffsmethoden reichen vom Durchstöbern von Abfällen nach interessanten Aufzeichnungen bis hin zu psychologisch geschickten Befragungen [396]. Dabei handelt es sich um klassische Methoden der Detektiv- und Spionagearbeit, die an die heutigen Bedürfnisse angepasst werden [397].

Ihr Anwendungsfeld reicht von der klassischen Industriespionage [398] über das Ausforschen behördlicher Geheimnisse [399] und das Abwerben besonders qualifizierter und kenntnisreicher Mitarbeiter [400] bis hin zur Erstellung von Persönlichkeitsprofilen [401], die über Bewerber, Konkurrenten oder potentielle Opfer Auskunft geben [402].

Die Prognosen von Sicherheitsfachleuten sind bereits für 2009 davon ausgegangen, dass sich Hacking- und Malware-Angriffe verstärkt auf einzelne Gruppen, Organisationen und Unternehmen konzentrieren werden [403]. Sie werden gepaart sein mit den Überredungstechniken des Soc-Eng, sei es, um Zugang zu geschützten Organisationen zu bekommen, ihre innere Struktur und ihre Schwachstellen zu erkunden oder um Überwachungstechnik oder Malware zu platzieren [404].

---

391 Beschuldigungen gegen Ex-HP-Verwaltungsratsvorsitzende aufgegeben, Heise online 15.03.2007

392 Siehe: **CF**, viel Feind, viel Ehr, 03.02.2009; **CF**, illegaler Datenhandel, 15.12.2008; **CF**, abgehobener Jargon, 15.02.2009.

393 Angriffe auf IT-Sicherheit: Störfälle nehmen zu, tecchannel 06.10.2005

394 Lothar **Lochmaier**, Risikofaktor Mensch: Die Kunst des Social Engineering, ZDNet.de 27.02.2007: "Human Firewall" beginnt mit klaren Regeln

395 Christoph **Baumgartner**, Social Engineering – trau schau wem, computerworld.ch 05.08.2005

396 Philipp **Schaumann**, Sicherheitsrisiko Mensch. Psychologische Aspekte des Social Engineerings, 31.08.2006

397 **CF**, Schnittstellen zur Datenübertragung, 2007

398 **CF**, erhebliche Schäden durch Industriespionage, 11.03.2008;
siehe auch: **CF**, Eschbach, Der Nobelpreis, 14.02.2009.

399 **CF**, filigraner Angriff, 14.05.2008

400 **CF**, Kopfjäger (Headhunter), 05.09.2008

401 **CF**, Preisgabe des Privaten, 09.07.2008

402 Siehe auch: Sicherheitskultur im Unternehmen, securitymanager.de, besonders das Kapitel "Datenklau für Dummies", S. 58.

403 **CF**, stärkere Ausrichtung auf Neigungsgruppen, 31.12.2008

404 **CF**, Tarnung und Täuschung, 12.05.2008

Verhaltensregeln für die Organisationssicherheit

⇨ *Keine Auskünfte erteilen, zu denen ich nicht ausdrücklich ermächtigt bin. Das gilt für die Arbeitsaufgaben selber, die Arbeits- und Betriebsorganisation sowie für die Zuständigkeit von Kollegen, ihre geänderten Aufgaben und ihre Abwesenheit. Sie sind gerade nicht erreichbar und nicht etwa im Urlaub oder im Mutterschutz.*

⇨ *Kein Zutritt für Fremde in geschlossene Bereiche, von denen ich nicht genau weiß, dass sie dazu berechtigt sind. Höflichkeit ist fehl am Platz!*

⇨ *Schriftliche Aufzeichnungen und Dateien gehören sicher vernichtet. Jede Information kann in der Zusammenschau mit anderen Schlüsse ermöglichen. Das gilt auch für Telefonlisten, Geschäftsverteilungspläne und andere organisatorischen Pläne und Aufzeichnungen.*

⇨ *Offenbar brisante, vertrauliche oder geheime Informationen werden nur mit den Mitarbeitern erörtert, die dazu ermächtigt sind. Das sind Kollegen mit besonderen Aufgaben (Datenschutz, Unternehmenssicherheit usw.) oder die Vorgesetzten. Ihr Ansprechpartner ist Ihr unmittelbarer Vorgesetzter. Er hat die Führungsverantwortung für Sie. Haben Sie Zweifel an der Integrität Ihres Vorgesetzten, können Sie sich auch an dessen Chef wenden.*

⇨ *Aufpassen und melden. Offene Türen, die eigentlich geschlossen sein müssten, technische Vorrichtungen, die bislang nicht vorhanden waren, Personen, die man nicht kennt, oder merkwürdiges Verhalten des PCs. Alles kann darauf hindeuten, dass die Organisationssicherheit bedroht ist.*

⇨ *Seien Sie zurückhaltend mit Auskünften!*

⇨ *Lassen Sie sich nicht unter Druck setzen!*

⇨ *Trauen Sie sich, ein Gespräch zu beenden!*

⇨ *Überprüfen Sie die Identität eines Anrufers!*

⇨ *Sichern Sie sich ab!*

⇨ *Achten Sie auf sensible Dokumente!*

⇨ *Seien Sie schweigsam in der Öffentlichkeit!*

⇨ *Sprechen Sie fremde Personen an!*

⇨ *Sicherheit geht vor Höflichkeit!*

⇨ *Seien Sie auch in der Freizeit wählerisch mit den Gesprächsthemen!*

Schaumann (Secorvo) [407]

B.1 3. Verhaltensregeln für Mitarbeiter

Vorsorge gegen das SocEng ist aber keine reine IT-Aufgabe, sondern eine Maßnahme zur Unternehmenssicherheit. Die Sicherheitskultur, die dazu geschaffen werden muss, lässt sich mit wenigen Regeln (siehe Kasten oben) formulieren [405].

Philipp Schaumann, der zur Sicherheitskultur und Informationssicherheit eine engagierte Webseite betreibt [406], gibt die Regeln in der Form von Merksätzen wieder (siehe oben rechts). Sie reichen bis in den privaten Bereich hinein und stammen von der Secorvo.

Ganz wichtig dabei ist, dass Sicherheit nicht als Kontrolle der Mitarbeiter ausgerichtet wird, sondern als Identität und gemeinsames Anliegen. Dazu gehört auch der kritische Blick auf das auffällige Handeln anderer Kollegen.

Eine richtig verstandene und sensibel organisierte Sicherheitskultur schützt gleichermaßen die IT-Infrastruktur, vor Datenmissbrauch und Korruption. Sie erfordert Schulungen und ein funktionstüchtiges Meldesystem mit geregelten Zuständigkeiten. Ihre Methoden sind die Motivation und der Lob. Sie muss gemeinsam von allen Beteiligten als selbstverständlich gelebt werden.

[405] **CF**, wider dem Tratsch, 13.03.2008; **CF**, Sicherheit durch Monitoring, 14.09.2007.

[406] Philipp **Schaumann**, Secorvo Security Consulting, Video "Social Engineering" (Demo).

[407] Philipp **Schaumann**, Sicherheitskultur und Informationssicherheit; **ders.**, Schutz gegen Social Engineering - neue psychologische Ansätze, Dezember 2008

B.1 4. Vorgehen des Social Engineers

Sven Vetsch [408] beschreibt das Vorgehen beim SocEng in sechs typischen Schritten:

⇨ *Informieren*

Informationen über das Ziel der SocEng-Attacke sammeln, z.B. Im Internet oder per „Dumpster diving“, also das Durchwühlen von Abfällen auf der Suche nach betriebsinternen Informationen wie Organigramme, Telefonverzeichnisse, persönliche Aufzeichnungen. Andere öffentliche Quellen sind z.B. Bibliotheken, Patentschriften, Museen und öffentliche Auftritte auf Messen.

⇨ *Kontakt aufbauen*

mit Anruf, persönlichem Besuch, Brief, E-Mail, Newsgroup, Weblog.

⇨ *Vortäuschung einer Identität*

In eine andere Rolle schlüpfen, z.B. als Vorgesetzter der Kontaktperson, als Endanwender, als Kunde oder als Interviewer bei einer Telefonumfrage.

⇨ *Zielinformationen erarbeiten*

Sich durch verschiedene Fragen an die Zielinformationen herantasten. Beispiele:

⇨ Ich bin neu in der Systemverwaltung und muss Ihre Anwenderdaten überprüfen. Wie war noch Ihre Zugangskennung? Und das Passwort?

⇨ Hier arbeitet doch die Frau Sowieso (Information aus einem Organigramm aus dem Vorjahr). Arbeitet die hier gar nicht mehr?

⇨ Hier Meier, PI Garbsen. Ich habe von meinem Kollegen den Vorgang wegen des Verkehrsunfalls (dort und dort) übernommen. Ist der Vorgang mit dem Führerschein schon bei Ihnen?

⇨ *Kontakt halten*

Wenn man die Zielinformationen hat, soll man den Kontakt möglichst nicht “verlieren“. Die Kontaktperson darf nicht merken, dass sie sensible Daten an einen Social Engineer weitergegeben hat. Gute Kontakte kann man immer wieder verwenden. Der Zugang zu ihm ist leichter, weil man auf die zurückliegenden Kontakte Bezug nehmen kann und die Kommunikation bereits vertraut ist. Der geschickte Angreifer lässt dabei auch immer wieder persönliche Informationen einfließen, die er bei den früheren Kontakten gesammelt hat.

⇨ *Informationen zusammensetzen*

Die Teilantworten müssen sinnvoll miteinander kombiniert werden. Meistens hat man nur nach Teilinformationen gefragt und auch nur solche erhalten. Sie mögen noch so banal erscheinen, können jedoch häufig zu sensiblen Informationen verbunden werden.

Der Social Engineer ist ein intellektueller Angreifer. Er muss nicht nur über Einfühlungsvermögen verfügen, sondern auch gebildet sein. Er muss sein Handwerk verstehen. Dazu gehören nicht nur Kenntnisse über die Zielorganisation, sondern auch über die Sprach- und Handlungsgewohnheiten ihrer Mitarbeiter. Schließlich muss der Social Engineer die Informationen, die er erhalten hat, bewerten, verbinden und wieder feinfühlig bewerten und hinterfragen.

Das ist ein kriminalistisches Vorgehen, das identisch mit der Prüfung des Verdachts [409] im Zusammenhang mit Straftaten ist.

B.1 5. noch einmal: Security Journal

Das Security Journal - SJ [410]- befasst sich *mit der heimtückischsten und allgegenwärtigen Bedrohung – dem Social Engineering* [411]. McAfee ist kein Consulter für die Unternehmensorganisation, sondern ein Anbieter von Sicherheits- und Anti-Malware-Software. Seine Aussage überrascht, weil sie so gar nichts mit dem Vertrieb des Unternehmens zu tun hat.

McAfee's Blickrichtung ist jedoch eine andere als die von Mitnick oder Veitsch, weil die Studie die technischen Angriffsszenen in den Vordergrund stellt und dann erst nach den betrügerischen Strategien fragt, mit denen sie umgesetzt werden.

---

[408] Sven Vetsch, Social Engineering, 21.01.2006, disenchant.ch; nicht mehr verfügbar.

[409] **CF**, Verdacht, 2008; **CF**, Geltung von Beweisen und Erfahrungen, 29.11.2009.

[410] **McAfee**, Security Journal. Social Engineering, 05.10.2008

[411] SJ, S. 3

Dieser Blick auf das SocEng im weiteren Sinne ist genau richtig, weil wir nach den Bedrohungen im Zusammenhang mit der IT fragen und nicht danach, wie man Leute überhaupt betrügen kann [412].

Einen amüsanten Einstieg liefert Hiep Dang, indem er überlieferte Beispiele für das SocEng aus der klassischen Sagenwelt und der Bibel beschreibt [413]. Anschließend zeigt er die Entwicklungen bei der Malware und den Sicherheitstechniken auf.

Die Aufsätze im übrigen beschäftigen sich mit den Erscheinungsformen und Techniken des SocEng.

B.1 5.1 Psychotricks

Karthik Raman schildert die medizinischen und psychologischen Grundlagen für menschliche Entscheidungen und deren Missbrauch [414].

Dazu geht er zunächst auf die Bedeutung emotionaler Entscheidungen ein, die nicht zwangsläufig im Einklang mit rationalen Erwägungen stehen. *Unredliche Politiker, Spione und Hochstapler wissen nur zu gut, dass sie ihre Ziele sehr effizient erreichen können, wenn sie an Emotionen – insbesondere an die Angst – appellieren, um eine emotionale Reaktion auszulösen. Diese Tradition setzen Social Engineers nun fort* [415].

Raman widmet sich sodann verschiedener Spielarten des SocEng. Viele seiner Beispiele sind von Mitnick übernommen worden, was die Darstellung nicht schmälert. Ihm geht es darum, die bekannten Techniken auch bekannt zu machen, um sie durch Sicherheitskonzepte und Schulungen abzuwehren.

> *Kunden der Nordea Bank erhielten (im Januar 2007) eine E-Mail, in der sie gebeten wurden, die darin angegebene „Anti-Spam“-Software herunterzuladen und zu installieren – und da die Nachricht allem Anschein nach von ihrer Bank stammte, kamen 250 Kunden dieser Aufforderung nach. Bei dieser Anti-Spam-Software handelte es sich tatsächlich um einen Trojaner, der Kundendaten sammelte, mit denen sich Kriminelle auf der Website der Bank anmeldeten und Geld stahlen. Es kam zu einem Schaden von 877.000 Euro.*
> Karthik Raman, SJ, S. 9

B.1 5.1.1 Emotionen manipulieren

Hierbei wird auf universale Gefühle wie Angst, Neugier, Gier und Mitgefühl abgezielt. Das Beispiel oben zeigt, wie die Angst instrumentalisiert werden kann. Die Neugier der Mitmenschen wurde im April 2007 ausgenutzt, als die Angreifer auf einem Parkplatz in London USB-Sticks "verloren". Die glücklichen Finder infizierten ihre PCs mit Phishing-Malware (SJ, S. 10).

B.1 5.1.2 Fehlgeleitete mentale Verknüpfungen

Darunter versteht Raman ein Vorgehen, bei dem die Faustregeln des Alltagslebens (Heuristik) durch kognitive Verzerrungen durcheinander gebracht werden.

⇨ *Entscheidungsstützende Verzerrung*

Sie zielt auf Gewohnheiten und Erfahrungen der Anwender. Nachgemachte Webseiten, Spam-Mails, die bekannte Unternehmensinformationen oder Newsletter nachahmen, und Nachrichten von angeblich vertrauten Kommunikationspartnern nutzen diese Methode, um das Opfer zur Preisgabe persönlicher Informationen zu bewegen.

⇨ *Bestätigungsfehler*

Als Beispiel nennt Raman die in vielen Unternehmen übliche Uniformierung von Mitarbeitern. Ein Angreifer in derselben oder in einer nachgemachten Uniform wird vom Opfer ohne Nachfrage als Mitarbeiter jenes Unternehmens identifiziert. Eschbach spricht insoweit von der *Magie von Visitenkarten.*

---

[412] **CF**, Trickbetrüger, 31.12.2008; **CF**, Proll-Skimming, 18.05.2008.

[413] Hiep **Dang**, Die Anfänge des Social Engineering, SJ, S. 4

[414] Karthik **Raman**, Bittet, dann wird euch gegeben, SJ, S. 9

[415] Ebenda, S. 10.

Auf dem Weg dorthin hielt ich an Fotogeschäften, Copyshops und ähnlichen Läden, bis ich einen mit einem Automaten fand, der Visitenkarten druckte. Fünf Minuten später war ich im Besitz von zwanzig frisch gedruckten, erstaunlich gut aussehenden Karten, denen zufolge ich Mats Nilsson hieß und Production Designer einer Filmgesellschaft namens Columbia-Warner Entertainment mit Sitz in Beverly Hills, Los Angeles, war.

Eschbach [416]

⇨ *Mere-Exposure-Effekt*

Der "Effekt der bloßen Darstellung" nutzt die Sensationslust bei spektakulären Ereignissen wie Katastrophen und Unglücke [417]. In ihrer Folge steigt die Zahl der Phishing-Seiten an, die sich dem Thema widmen und ihre Malware platzieren sollen.

⇨ *Ankerheuristik*

Dabei geht es um ins Auge springende Identifikationsmerkmale (Bank-Logo, Kennzeichen von Marken, Corporate Identity), die Vertrautheit bewirken und die Kritikfähigkeit schwächen (nachgeahmte Bankseiten).

B.1 5.1.3 Fehler im Schema verursachen

Sozialpsychologen definieren ein „Schema“ als Abbild der Realität, auf das wir uns beziehen, um Schlussfolgerungen zu unserer Umgebung ziehen zu können (SJ, S. 11). Schemata sind danach aus der Erfahrung gebildete Schablonen für Verhaltensweisen, die als "normal" oder "unauffällig" betrachtet werden. Der Angreifer nutzt sie, um in der Menge unterzutauchen. [418]

Die Kunst der Verkleidung besteht in der Veränderung der zwei entscheidenden Merkmale: Körpersilhouette und Bewegung. ... Nichts übertreiben, darauf kam es an. Völlig durchschnittlich auszusehen und niemandem aufzufallen war das anzustrebende Ideal.

Und bloß nicht schleichen! Schleichen ist verdächtig. Man darf auf feindlichem Gelände niemals ohne Not schleichen, sondern muss sich entspannt bewegen, zielstrebig, so selbstverständlich, als habe man hier zu tun, als gehe man nur seinem mäßig geliebten Job nach. Ich konnte ein Wachmann sein, ein Bote, irgendjemand, der einfach etwas vor die Haustür zu legen hatte.

Mit dieser Haltung war ich einmal sogar von einem großen Firmengelände entkommen, obwohl schon ein von mir versehentlich ausgelöster Alarm in vollem Gange gewesen war. Überall drehten sich gelbe Warnlichter, heulten Signalhupen, doch ich spazierte gelassenen Schrittes am Pförtnerhaus vorbei und brachte es fertig, den Pförtner verwundert zu fragen, was denn da los sei.

Eschbach [419]

⇨ *Attributionsfehler*

Hierbei geht es um gut geübte Schauspielerei. Angreifer können sich sympathisch verhalten, wenn sie eine Bitte äußern, oder dominierend auftreten, wenn sie ihre Opfer zu einer bestimmten Handlung nötigen. (SJ, S.11)

⇨ *Salienzeffekt*

Die Angreifer fügen sich unauffällig wie ein Chamäleon in ihre Umgebungen ein, schließen sich Gruppen an, die verschlossene Eingänge nutzen, und lösen sich von ihnen ebenso unauffällig. Sie geben sich vielleicht als Kunde im Anzug oder als Betreuer in Arbeitskleidung aus, aber nicht als Gaukler auf Stelzen. Die Integration ist dabei nicht nur auf die Kleidung oder das Erscheinungsbild beschränkt – sie kann sich auch auf die Kenntnis von unternehmenseigenem Jargon, firmeninternen Ereignissen sowie Mitarbeitern des Unternehmens und sogar auf die Beherrschung des lokalen Dialekts erstrecken. (SJ, S. 11)

---

[416] Andreas Eschbach, Der Nobelpreis, Bergisch Gladbach (Lübbe) 2005, S. 291

[417] … oder andere Ereignisse wie die Wahl von Obama zum US-Präsidenten: **McAfee**, February 2009 Spam Report, 02.02.2009, S. 6.

[418] Die automatische Erkennung unüblichen menschlichen Verhaltens wird versucht, steckt aber noch in den Kinderschuhen: **CF**, Überwachungskameras. Prävention und Aufklärung, 29.12.2007; **CF**, biometrische Erkennungsverfahren, 01.02.2009.

[419] Eschbach, ebenda, S. 189, 373

Ich glaube nicht, dass Computerkriminelle neue Techniken anwenden. Sie setzen lediglich leicht veränderte Methoden ein, um Menschen zu betrügen. Die aktuellsten und effizientesten Bedrohungen sind meist automatisierte Angriffe, da diese leichter durchgeführt werden können und ein besseres Aufwand-Nutzen-Verhältnis bieten. Sie werden immer die Technik wählen, mit der sie weniger Zeit oder Geld für bessere Ergebnisse investieren müssen.
Matthew Bevan [420]

⇨ *Konformität, Nachgiebigkeit und Gehorsam*

Auch hier geht es um das Auftreten, jedoch gepaart mit Eindruck schindenden Elementen wie Herablassungen, Drohungen oder Versprechungen. So könnte sich ein Social Engineer als Führungskraft auf Geschäftsbesuch ausgeben und sich gegenüber einem jungen Sicherheitsbediensteten durchsetzen, dass er ihm Zugang zum Firmengelände gewährt, obwohl er kein Namensschild trägt. (SJ, S. 11)

B.1 5.2 Geld machen mit Cybercrime

Die Zeit der Unschuld ist vorbei [421]. Das legt auch Markus Jakobsson zugrunde und beschreibt die aktuelle und künftige Cybercrime als geschäftsmäßige Aktivitäten [422].

Die Methoden des Betruges im Internet betrachtet Jakobsson als eine Mischung aus IT und SocEng. Wegen der zunehmenden Strafverfolgung meint er, dass die Cyber-Kriminellen verstärkt dazu übergehen werden, ihre Spuren zu verwischen.

Dazu blickt er zunächst zurück auf den Trojaner Archiveus, eine "Lösegeld-Ware" (Ransomware [423]), mit der die Daten der Opfer verschlüsselt wurden. Anschließend kam die erpresserische Forderung, dass gegen Geld der Schlüssel für die Entschlüsselung geliefert werde. Das Scheitern des Trojaners hatte aber nicht nur technische Gründe: Es gab für die Kriminellen keine Möglichkeit, an das erpresste Geld heranzukommen, ohne dass man ihnen auf die Spur gekommen wäre (SJ, S. 14). [424]

Sodann geht Jakobsson auf die Vandalware ein. Bevor sie zum Einsatz kommt, erwirbt der Angreifer Put-Optionen gegen ein Handelsunternehmen, also Wettscheine auf die Erwartung, dass der Handelswert des Unternehmens sinkt. Dann folgt der Angriff mit dem SocEng, um in dem Unternehmen über Mitarbeiterkontakte die Vandalware zu verbreiten. Wenn das erfolgreich war, dann folgt der zerstörerische Angriff, der zum Beispiel zur Veröffentlichung von Kundendaten auf der Unternehmenshomepage, zum Zusammenbruch der Webshops oder zum Ausfall des Rechnungswesens führt. Die Börsen reagieren darauf unmittelbar, seine Put-Optionen gewinnen an Wert und der Angreifer macht Gewinn (SJ, S. 14).

Schließlich stellt Jakobsson den Klickbetrug vor. Wenn ein Käufer auf eine Werbung klickt, zahlt der Inserent sowohl an den Betreiber der Website, auf der die Werbung angezeigt wird, als auch an das Portal, das die Website mit der Werbung bereitgestellt hat, eine Gebühr. Allein schon bei der Auswahl der Referenzwörter können mehr oder weniger hohe Kosten zu Buche schlagen (Suchwort-Arbitrage). Aber das ist noch kein Betrug (Szenario 2, SJ, S. 15)

Mit angeworbenen Klickern, also Menschen, automatischen Website-Weiterleitungen und Klick-Robotern, also Programmen, die den Seitenaufruf permanent durchführen, können jedoch die Klickzahlen in die Höhe getrieben werden ... und der Gewinn.

Noch besser dazu geeignet sind Botnetze. Jeder Zombie klickt einmal und die Klickzahl geht ins Unermessliche ... dann folgt die nächste Runde. Das zahlungspflichtige Unternehmen hat kaum eine Chance zu beweisen, dass es mit kaufdesinteresierten Zombies betrogen wurde.

---

[420] **McAfee**, Bericht ... zum Thema Virtuelle Kriminalität, Matthew Bevan, S. 4; **McAfee**, Computerkriminalität und Computergesetze, 08.12.2008

[421] **CF**, Hacker: Moral und Unmoral, 07.08.2008

[422] Markus Jakobsson, Social Engineering 2.0: Was bringt die Zukunft? SJ, S. 13

[423] **CF**, hilfsbereite Gauner, 10.01.2010

[424] **CF**, teure Placebo-Software: Scareware, 23.10.2008;
siehe auch: **CF**, Koobface-Gang antwortet, 23.05.2010

Ein feinsinniges Beispiel liefert Jakobsson dafür, wie Preisunterschiede bei den Klickwörtern ausgenutzt werden können. Das Suchwort "Asthma" ist verbreitet und eine Platzierung bei Google kostet etwa 0,10 US-$. Wenn der Täter auf seiner Webseite zum Thema Asthma einen Artikel einstellt, in der die sachlich blödsinnige Frage gestellt wird: „Wussten Sie, dass bei zehn Prozent der Asthmatiker das Risiko besteht, an einem Pleuramesotheliom zu erkranken?“, kann er erwarten, dass sehr viele besorgte Besucher die Werbung zum Suchwort Pleuramesotheliom anklicken. Jeder Klick bringt etwa 63 US-$ (SJ, S. 15).

B.1 5.3 gezielte Manipulationen

An Jakobsons Vandalware schließt Anthony Bettini wegen der Schwachstellen an den Aktienmärkten an [425]. Er betrachtet zyklische und vorhersehbare Aktienkursschwankungen sowie andere Besonderheiten des Aktienmarktes. Am Rande berührt er Spam-Mails, die zum Kauf von Penny-Stocks aufrufen. Wenn sich der Spammer selber eingedeckt hat, dann kann er durch seine Werbung vorübergehend die Kurse ansteigen lassen und rechtzeitig bei (erwartetem) Höchststand verkaufen. Diese Methode ist nicht ganz so brutal wie die von mir geschilderte [426].

Elodie Grandjean analysiert im einzelnen die Spam-Mails und Malware-Angriffe, die 2008 die Olympischen Spiele in China und die politischen Auseinandersetzungen um den politischen Status von Nepal zum Gegenstand hatten [427].

Wir haben bereits erlebt, dass einzelne Mitglieder von Pro-Tibet-Gruppen E-Mails erhielten, die eine mit der Situation in Tibet, China im Allgemeinen oder der Olympiade in Verbindung stehende CHM- (kompilierte Hilfe), PDF-, PPT-, XLS- oder DOC-Datei als Anlage enthielten. Sämtliche dieser E-Mails schienen von einer vertrauenswürdigen Organisation oder Person zu stammen. Die Empfänger waren es gewohnt, solche Dokumente von ihren Unterstützern zu erhalten, und waren deshalb wohl nicht allzu wachsam. Die Anlagen jedoch waren bösartig (SJ, S. 17).

Craig Schmugar hebt die zunehmende Bedeutung von sozialen Netzwerken hervor und weist besonders auf ihre Werbe- und Marketingmöglichkeiten hin [428]. Er beschreibt sodann ihre Anfälligkeit gegen Malware [429] und ihre künftigen Entwicklungen: Integration von GPS für standortabhängige Dienste, Datamining und Auswertung der besonderen Nutzerinteressen.

Social-Websites werden auch cleverer werden und Benutzerinformationen im Web sammeln. Social-Bookmarking-Funktionen wie Digg werden mit sozialen Netzwerken kombiniert und mit selbstlernenden Technologien wie Pandora oder StumbleUpon und Tagging-Funktionen wie Flickr aufgewertet werden. Im Endergebnis steht der Community ein noch umfangreicherer und detaillierterer Strom an relevanten Informationen zur Verfügung, als dies derzeit der Fall ist. Auf Ihrem iPhone werden Sie Empfehlungen zu Filmen aus Ihrem Netzwerk erhalten können. ... (SJ, S. 29)

Ob das alles wünschenswert ist, ist eine zweite Frage. Diese Dienste vergläsern die Anwender und lassen eine genaue Platzierung von Werbung zu. Die von ihnen gesammelten Daten und ihre Auswertungen eröffnen aber auch dem Missbrauch Tür und Tor. Das verkennt auch Schmugar nicht, der breit die "Zunahme von Risiken" anspricht (SJ, S. 30).

---

[425] Anthony Bettini, Schwachstellen an den Aktienmärkten an, SJ, S. 22;
siehe auch **CF**, merkwürdiger Markt, 27.10.2008.

[426] **CF**, Aktienkursmanipulation, 28.11.2008

[427] Elodie Grandjean, Ein ideales Ziel für Social-Engineering-Malware, SJ, S. 16;
siehe auch **CF**, olympische Angriffe, 11.08.2008.

[428] Craig Schmugar, Die Zukunft von Social-Networking-Websites, SJ, S. 28

[429] **CF**, prominente Verführung & Sex, 11.01.2009;
CF, Angriffe aus dem Internet, 22.06.2008;
CF, leichtfertiger Umgang mit sozialen Netzen, 23.10.2008; **CF**, harte Realität, 12.02.2009

Spionageaktionen laufen für gewöhnlich verdeckter ab und sind wesentlich schwerer aufzudecken, als ein aus reinen Profitgründen durchgeführter Angriff. In vielen Fällen waren die Schwachstellen in diesen böswilligen eingebetteten Dokumenten Zero-Day-Angriffe, wodurch diese Dokumente noch schwerer zu entdecken sind, da diese Schwachstellen oft erst gefunden werden, wenn der Schaden bereits entstanden ist. Weil diese Zero-Day-Schwachstellen auf bestimmte Behörden oder militärische Einrichtungen abzielten, kann nicht ausgeschlossen werden, dass ausländische Agenten oder Regierungen diese Angriffe gesponsert haben.
Rahul Kashyap [430]

B.1 5.4 Schwachstellen, Exploits und Fallen

Rahul Kashyap zeigt die Entwicklung der Malware auf und vor allem ihre zunehmende Individualisierung für gezielte Angriffe gegen Unternehmen und Behörden [431].

Er weist zunächst auf die seit 2004 stagnierende und seit 2006 abnehmende Zahl von Malware-Angriffen gegen Server-Produkte von der Firma Microsoft hin, was deren Strategie bestätigt, regelmäßig automatische Updates bereit zu stellen, mit denen Programmfehler und festgestellte Sicherheitslücken (Exploits) behoben werden. Gleichzeitig stieg jedoch die Zahl der Angriffe gegen die Arbeitsplatzrechner (Clients), wobei weniger die Betriebssysteme als die gebräuchlichen Anwenderprogramme missbraucht werden. Das beschränkt sich nicht auf die weit verbreiteten Produkte im Ofice-Paket von Microsoft, sondern betrifft auch *z. B. Adobe, Mozilla und Apple* (S. 32). [432]

Für die Ausnutzung von Client-Schwachstellen sind jedoch Benutzerinteraktionen entscheidend. Malware-Autoren mussten deshalb Wege finden, wie sie Benutzer zum Klicken auf Links und Herunterladen von Bildern sowie Dokumenten aus dem Internet verleiten konnten. Und damit sind wir wieder beim SoEng.

Gleichzeitig habe sich auch die Methodik der Malwareschreiber zur Spionage hin verändert, berichtet Kashyap. Waren die Angriffe zunächst breit angelegt, roh und zerstörerisch, so seien sie immer feiner auf einzelne Einrichtungen, Unternehmen und Behörden ausgerichtet worden [433].

Zwei weitere Trends stellt Kashyap vor: Manipulierte Webserver [434] und Angriffe gegen Router in privaten Heimnetzwerken [435].

B.1 5.5 Typosquatting

Daran schließt Benjamin Edelman an, der sich dem Typosquatting widmet [436].

Zur Vorbereitung dieser schon länger bekannten Methode [437] registrieren die Angreifer für sich Domänennamen mit leichten Abweichungen gegenüber bekannten Markennamen und Internetanbietern. Dazu ist es besonders beliebt, Buchstaben mit solchen auszutauschen, die auf der Tastatur unmittelbar daneben angeordnet sind (z.B. "giiple.com") und damit Erfolg bei "Vertippern" versprechen. Auch das Weglassen von Zeichen gehört dazu, z.B. des Punktes bei "wwwmcafee.com" (SJ, S. 34).

Im Auftrag von McAfee hat Edelmann *80.000 Typosquatting-Domänen allein für die Top 2.000-Websites gefunden* (Mai 2008). Für besonders gefährlich erachtet er solche Vertipper-Seiten, die sich auf besonders von Kindern besuchten Seiten beziehen und ihrerseits pornographische Bilder publizieren.

---

430 Rahul Kashyap, Das neue Gesicht der Schwachstellen, SJ, S. 31

431 Ebenda.

432 Siehe: **CF**, gewandelte Angriffe aus dem Netz, 29.11.2008.

433 **CF**, Massenware und gezielte Spionage, 12.05.2008; **CF**, Cyberwar, 13.12.2008; **CF**, filigraner Angriff, 14.05.2008; **CF**, Umleitungen zu manipulierten Webseiten, 09.12.2008.

434 **CF**, Angriffe gegen Webserver, 21.11.2008; **CF**, SQL-Würmer, 20.09.2008; **CF**, Gegenspionage wider 'ZeuS' und 'Nethell', 19.12.2008; **CF**, Kollisionsangriff gegen Webseitenzertifikat, 15.02.2009.

435 **CF**, Malware. Betriebssystem, 12.05.2008; **CF**, Angriffe auf DSL-Router, 23.01.2008.

436 Benjamin Edelman, Unfreiwillige Abenteuer beim Surfen im Internet, SJ, S. 34

437 **CF**, Typo-Squatting, 29.11.2007; **CF**, Abzocke mit Domain-Tasting, 31.01.2008; **CF**, Domain-Namen-Inflation, 29.01.2009.

David Marcus greift eine Studie von McAfee aus dem Juni 2008 auf und stellt die gefährlichsten Domains vor [438], die mit einer Häufung als Spam-Versender, Malware-Depots oder manipulierten Webseiten auffallen [439]. Die beiden Spitzenreiter sind die USA und Polen.

B.1 5.6 Adware und Spyware

Adware und Spyware sind potentiell unerwünschte Programme - PUP, die wegen ihrer Verbreitung den Begriff "Trojaner" bekannt gemacht haben [440]. Sie waren in aller Regel in ein selbständiges Programm eingebettet, mit denen die Funktionen des PCs erweitert werden konnten (z.B. MP3-Player, Übersetzungsprogramme, Spiele). Mit ihrer Geschichte und Funktion setzt sich Aditya Kapoor auseinander [441].

Als Adware werden Programme bezeichnet, die neben ihrer nützlichen Funktion unvorhergesehen Werbung anzeigen [442].

Im engeren Sinne steht der Begriff Spyware für Überwachungssoftware, die ohne angemessene Kenntnisnahme, Zustimmung oder Kontrolle durch den Benutzer installiert wird. (SJ, S. 38) *Im weiteren Sinne wird Spyware als ein Synonym für (Technologien) verwendet, die ohne entsprechende Zustimmung des Benutzers installiert und/oder implementiert werden ...* (SJ, S. 38)

Es gibt auch Mischtypen davon, etwa Adware, die gleichzeitig das Nutzerverhalten überwacht und auswertet, um dann gezielt ausgewertete Werbung zu übermitteln.

Die PUPs erschienen erstmals 2000, hatten 2005 den höchsten Grad ihrer Verbreitung und gehen seither zurück (SJ, S. 39). Bei ihrer Verbreitung werden zunehmend die Methoden des SocEng genutzt.

Ihre Verbreitung finden die PUPs wegen eines besonderen Vergütungssystems, dem Pay-Per-Installation - PPI, bei dem für jedes installierte PUP eine Provision bezahlt wird. Kapoor nennt ein Beispiel: *ZangoCash zahlt ... für jede installierte Adware in den USA zwischen 0,75 und 1,45 US-Dollar* (SJ, S. 39). Die Installation wird vermittels eines Refferers (Nachverfolger) signalisiert.

Für den Verbreiter kommt es also darauf an, möglichst viele Installationen zu erwirken, so dass sie in häufigen Fällen auf die Anzeige der Endbenutzer-Lizenz verzichten oder die PUPs gleich mit der Malware verbreiten.

Ein anderes Vergütungssystem ist das Pay-Per-Click - PPC.

Einige der gebräuchlichsten Transportmechanismen für PPC-Inhalte sind:

• *Bannerwerbung: Werbeanzeigen werden innerhalb eines Banners oder vordefinierten Bereichs eingeblendet. Wechselnde Inhalte sind möglich.*

• *Pop-Up- oder Pop-Under-Werbung: Die Werbung wird in eigenen Fenstern angezeigt, was von den Benutzern meist als störend empfunden wird.*

• *Flash-basierte Werbung: Ist der Bannerwerbung ähnlich, es werden jedoch Flash-Animationen verwendet, um wechselnde Inhalte anzuzeigen.* (SJ, S. 40)

Im Weiteren referiert Kapoor verschiedene Methoden und Vorfälle der missbräuchlichen Verbreitung von PUPs über Spam-Mails, soziale Netzwerke, Suchmaschineneinträge und gefälschte Webseiten.

---

[438] **CF**, Schurkenstaaten, 20.06.2008;
CF, gefährliche Lokale, 21.02.2008.

[439] David Marcus, Wie gefährlich sind Top-Level-Domains? SJ, S. 44

[440] Heute werden als "Trojaner" vor allem Trägerdateien mit eingebetteten Malware-Funktionen bezeichnet, siehe: **CF**, Malware. Tarnung und Täuschung, 12.05.2008.

[441] Aditya Kapoor, Was ist aus Adware und Spyware geworden? SJ, S. 38;
siehe auch: Anna **Stepanov**, Spyware: Beständiger Wandel, McAfee 02.12.2007

[442] Eine jüngere Spielart davon ist die **CF**, Nörgelsoftware (Nagware), 14.01.2008.

B.1 5.7 Ergebnisse aus dem Security Journal

Die Ergebnisse der Studien wurden in der Meldung über die englischsprachigen Ausgabe veröffentlicht [443].

Der Ansatz von McAfee, im Zusammenhang mit dem SocEng einen besonders intensiven Blick auf die Malware zu werfen, ist sicherlich berechtigt, verkürzt aber das Thema als solches. Richtig daran ist, dass die Verbreitung von Malware und das Locken auf manipulierte Webseiten ohne die mittelbaren sozialpsychologischen Überredungsmethoden des SocEng nicht mehr möglich sind oder jedenfalls nicht in dieser Häufung funktionieren würden. "Mittelbar" deshalb, weil hier vor allem mit Texten, Bildern und dem Layout umgegangen wird, um den Anwender in Vertrauen zu wiegen oder zu übertölpeln.

Das unmittelbare SocEng benutzt keine Medien, sondern findet nur in sozialer Kommunikation statt. Es wird immer auch Mischformen geben, in denen der Social Engineer auch Medien einsetzt oder Abhörtechnik und die Methoden des Hackings.

Die Auseinandersetzung mit dem SocEng, die Karthik Raman nach einer nicht geglückten Einleitung über die medizinischen und psychologischen Grundlagen vollführt, beschränkt sich auf die von Mitnick bekannten Fallstudien und findet keine Verbindung zu den Themen im Security Journal im übrigen. Sein Verdienst ist es, dass er die Methoden der Manipulation in den Zusammenhang zu sozialpsychologischen Schemata stellt und damit besser systematisiert.

Die übrigen Aufsätze liefern gute Zusammenfassungen zu einzelnen Themen und Aspekten. Ihnen fehlt jedoch der Zusammenhang und besonders fehlt eine Systematik der Methoden des mittelbaren SocEng. Außerdem weisen die Aufsätze Lücken auf, weil sie Botnetze und ihre Betreiber unerwähnt lassen und die verschiedenen Formen der Cybercrime sowie die dabei verwendeten Methoden nicht analysieren und systematisieren.

[443] Siehe oben und **CF**, Überredungstechniken, 23.11.2008

B.1 5.8 Fazit: Security Journal

Das Security Journal [444] ist eine wichtige und zum Lesen empfohlene Veröffentlichung. Es bleibt aber hinter meinen Erwartungen zurück.

Der letztjährige Report über die globalen Sicherheitsbedrohungen [445] war nicht nur spannender und exotischer, sondern auch Erkenntnis fördernder. Es ist schade, dass er keinen Nachfolger bekommen hat.

Dabei ist McAfee inzwischen viel weiter, als das Security Journal erkennen lässt. Der Jahresbericht zur Entwicklung der Virtuellen Kriminalität 2008 hat deutliche Worte zur Strafverfolgung [447], zum Cyberwar [448] und zum kriminellen Zahlungsverkehr gefunden. Diese Gesichtspunkte werden im Security Journal nur gestreift, was die Vermutung entstehen lässt, dass sie auch nicht hintergründig eingeflossen sind.

Auch die Prognosen von McAfee sind inzwischen erheblich härter und punktgenauer geworden. Die Voraussagen über die Bedrohungen in 2009 [449] begrüßen den nachhaltigen Rückgang des Spammings nach dem Abschalten der IP-Adressen der als Spammer berüchtigten McColo Corporation und fordern weitere solche Aktionen von Regierungen und Zugangsprovidern (S. 10) [450]. Darüber hinaus erwarten sie neue Formen gefälschter Webseiten mit angeblichen Finanz-

[444] **McAfee**, Security Journal. Social Engineering (dt.), 05.10.2008

[445] **CF**, globale Sicherheitsbedrohungen, 27.07.2008

[446] **McAfee**, Bericht ... zum Thema Virtuelle Kriminalität, **McAfee**, Computerkriminalität und Computergesetze, 08.12.2008

[447] **CF**, Strafverfolgung, 13.12.2008

[448] **CF**, Cyberwar, 13.12.2008

[449] **McAfee**, 2009 Threat Predictions, 13.01.2009

[450] Das Geschäftsfeld wurde inzwischen von Botnetzen übernommen: **McAfee**, January Spam Report, 08.01.2009 (S. 4)

und staatlichen Dienstleistungen (S. 5).

Wünschenswert wäre eine Auseinandersetzung mit dem SocEng als Bestandteil der Erscheinungsformen der Cybercrime insgesamt gewesen. Das könnte ein zu stark wissenschaftlicher Anspruch sein, weil dazu, jedenfalls wegen der aktuellen Ausprägungen, mehr Erfahrungswissen über die Datenspionage und den Cyberwar erarbeitet, gewürdigt und bewertet werden muss.

Aber auch Mitnicks Werk [451] besteht aus Fallstudien und Balduans [452] Bericht musste ich mit anderen Quellen verbinden, bis ich daraus die Theorie von der modularen Cybercrime [453] entwickeln konnte.

B.1 6. Lehren aus den Fallstudien zum Social Engineering

Die von Mitnick und dem Security Journal gelieferten Fallstudien zeigen, dass das Social Engineering keine eigenständige Erscheinungsform der Cybercrime ist. Seine Ursprünge liegen in den Methoden der Rhetorik, der Manipulation und der Suggestion und können ganz verschiedenen Zwecken dienen.

Seine ersten konkreten Ausformungen bezieht das Social Engineering aus den Erfahrungen und Praktiken der Trickbetrüger [454]. Seine selbständige Ausrichtung hat es jedoch durch die Spionage bekommen, die von Kundschaftern, Diplomaten, Spionen und Agenten entwickelt wurden. Wenn sie gut sein und unentdeckt bleiben wollten, mussten sie technisches und sonstiges Wissen mit sozialer Kompetenz und Abgebrühtheit verbinden. Genau das zeichnet den "echten" Social Engineer aus.

Seine Methoden und Machenschaften unterscheiden sich vom Grundsatz her nicht von denen anderer Tätigkeiten, denen es um die Beschaffung geheimer Informationen und den Schlüssen geht, die aus ihnen und öffentlichen Informationen gezogenen werden. Darin unterscheidet er sich überhaupt nicht von Informationsbrokern, Geheimdienstlern und Ermittlern.

Das Social Engineering darf eine gewisse Eigenständigkeit nur in dem Bezug beanspruchen, dass es ihm um die Penetration informationstechnischer Systeme und Daten geht. Seine Ausrichtung geht auf die Informationstechnik und ihre Besonderheiten bestimmen die Ausprägung der sozialpsychologischen Methoden und eingesetzten Techniken.

Die künftige Entwicklung, die vermehrt individualisierte Angriffe und Spionage gegen Einrichtungen, Unternehmen und Behörden erwarten lässt, wird das Social Engineering als eigenständige Erscheinungsform im Zusammenhang mit der Informationstechnik vernichten. Alle anderen Spionage- und Ermittlungsformen werden sich wegen ihrer Methoden angleichen, schnöde und IT-Technik miss- und gebrauchen ähnliche Gedankengänge wegen der Auswertung von Informationen entwickeln.

Das gilt besonders auch für staatliche Ermittler, die technische und soziale Kompetenz verbinden müssen - und bei ihren Methoden an Recht und Gesetz gebunden bleiben.

Das will ich auch nicht anders.

---

[451] Siehe oben.

[452] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.;
siehe: **CF**, Cybercrime: Zusammenarbeit von Spezialisten, 13.07.2008.

[453] **CF**, arbeitsteilige und organisierte Cybercrime, 07.08.2008

[454] **CF**, Trickbetrüger, 31.12.2008

B.2 Beobachten und bewerten

Ein geschickter Angreifer kann allein mit seinen Beobachtungen, mit öffentlichem Allgemeinwissen und überlegten Kombinationen sensible Informationen über eine fremde Organisation, ihren Aufbau und ihren inneren Abläufen sammeln und erschließen. Die ▸ folgenden, erdachten Geschichten zeigen, wie das gemacht werden kann.

B.2 1. einheitliche Organisationssicherheit

Auch in Mitnicks Berichten [455] über das SocEng werden Szenen beschrieben, wie mit belanglosen internen Informationen Vertrauen geschafft und die Gesprächspartner dazu gebracht werden, weitere vertrauliche Informationen bis hin zu personenbezogenen Daten und echten Geheimnissen zu offenbaren. Er beschreibt den Einsatz von Keyloggern, die am PC installiert werden, um die Tastatureingaben zu protokollieren, wie ungesicherte Datensteckdosen zum Eindringen in das EDV-System verwendet und wie die Zugangsdaten von Mitarbeitern missbraucht werden können. Für den Angreifer, der es auf die EDV abgesehen hat, ist es besonders wichtig, einen Zugang mit Administratoren-, also mit vollen Zugriffsrechten zu erlangen, mit denen er auf alle geschützten Informationen zugreifen kann.

Die Sicherheit der Informationstechnik beginnt bei der einfachen Physik. Serverräume müssen verschlossen, klimatisiert und brandgeschützt sein. Verteilerkästen für Datenleitungen müssen abgeschlossen sein; wenn nicht, lässt sich womöglich mit einem Nagelknipser die EDV in mehreren Etagen so sabotieren, dass eine neue Verkabelung installiert werden muss. Datensicherungsbänder gehören in einen Stahlschrank, der sich möglichst in einem anderen Gebäude befindet. Nur dann ist bei einem fatalen Störungsfall (Feuer, Hochwasser, Sabotage) sicher gestellt, dass die Daten mit neuer Technik wieder hergestellt werden können.

Die heutigen Methoden zur technischen IT-Sicherheit sind so verfeinert, dass einfache Angriffe scheitern müssen. Das beginnt bei Datensteckdosen, die nur auf ein bestimmtes Endgerät reagieren, das dort mit seinen individuellen Merkmalen angemeldet ist, und endet bei strikten Regelwerken, die die Installation von fremder Software und damit auch von schädlicher Crimeware am Arbeitsplatz rigoros verhindern. Das Bundesamt für Sicherheit in der Informationstechnik – BSI [456] – hat hierzu ein Regelungswerk geschaffen und verschiedene Studien veröffentlicht, die kaum Lücken offen lassen und neben einem „Grundschutz“ auch „kritische“ Datenverarbeitungsvorgänge [457] im hohen Maße sichern.

Die IT-Sicherheit wird häufig nur als technische Sicherheit angesehen. Die Diskussion um das SocEng zeigt hingegen, dass die IT-Sicherheit immer eingebettet ist in die allgemeine Organisationssicherheit. Die Korruptionsbekämpfung oder die Abwehr von Spionen beschränken sich deshalb heute nicht mehr auf die klassischen Betrachtungsweisen, sondern müssen sich auch den Besonderheiten der Informationstechnik stellen und sie in ihre Konzepte einbinden.

Das Wichtigste bei allen Sicherheitsfragen ist die Ausbildung und die gelebte Sensibilität der Mitarbeiter. Sie lassen sich mit Dienstanweisungen unterstützen, aber nicht ersetzen. Die Mitarbeiter müssen erkennen lernen, wo Unsicherheitsquellen sind und wo ihnen ungewöhnliche oder sensible Informationen abgefragt werden – und sie brauchen Handlungsanleitungen und eine Ansprechstelle, an die sie ihre Beobachtungen und Befürchtungen vorbehaltlos melden können.

Die Überredungstechniken, die das SocEng prägen, haben längst Eingang in andere kriminelle Techniken gefunden. Damit haben sich vor allem die Aufsätze über die ▸ Malware und das ▸ Social Engineering befasst.

---

[455] Siehe oben

[456] **BSI**, IT-Grundschutz-Kataloge
(früher: Grundschutzhandbuch - GSHB)

[457] **BSI**, Veröffentlichungen zum Thema "Kritische Infrastrukturen"

B.2 2. Blick von außen [458]

Die Staatsanwaltschaft liegt unweit des Hauptbahnhofs. Sie ist in einem L-förmigen Gebäude untergebracht, dessen südlicher Teil sieben Stockwerke über dem Erdgeschoss aufweist. Dieser Trakt ist leicht konkav gebogen, wie ein Hohlspiegel. Das Erdgeschoss wird durch ein großes vergittertes Tor unterbrochen, das den Blick zu einem begrünten Innenhof zulässt. Im Hintergrund sind weitere Gebäude erkennbar.

Es ist ein Nachmittag im späten Herbst. Der größere Teil der Fenster ist von innen in verschiedenen Stärken beleuchtet. Je zwei Fenster zeigen immer eine gleichartige Beleuchtung oder sind gar nicht beleuchtet, so dass sie zu jeweils einem Raum gehören.

An verschiedenen Stellen reicht die gleichartige Beleuchtung auch über mehrere Fenster hinweg und man kann auch erkennen, dass einige Leuchtröhren rechts und links über einen Mauersturz hinweg reichen. Sie kennzeichnen größere Räume, in denen entweder mehrere Leute arbeiten oder Archive untergebracht sind.

Ich gehe um den Gebäudeteil links herum und betrachte seine Schmalseite. Es besteht aus massivem Mauerwerk, das in jeder Etage mittig von einem kleineren Fenster unterbrochen wird. Diese Fenster sind höhengleich mit den Fenstern an der Langseite.

Sie liegen also an den Enden von Mittelgängen, von denen beiderseits Räume abzweigen, ohne dass am Ende ein Treppenhaus eingebaut ist. Dies würde sich durch höhenversetzte Fenster oder erkennbare Treppenstrukturen zeigen.

Etwas nach hinten versetzt schließt ein anderes und wahrscheinlich älteres Gebäude an. In diesem Anschlussbereich muss sich ein von außen nicht erkennbares Treppenhaus befinden, weil das die Bauvorschriften verlangen. Der Blick auf die Rückfront ist im wesentlichen verdeckt.

Aus einigem Abstand erkenne ich schließlich eine Richtfunkanlage auf dem Gebäudedach. Es handelt sich dabei um einen Zylinder, oder man kann auch sagen „Blecheimer“, dessen flache Seite in Richtung Nordwesten ausgerichtet ist. Etwa in dieser Richtung befinden sich, wie ich im Stadtplan gesehen habe, eine größere Polizeibehörde und das Landeskriminalamt. Die Größe des „Blecheimers“ zeigt, dass die Richtfunkanlage auf eine Entfernung bis zu etwa 20 Kilometer ausgelegt ist. Sie könnte also auch die Verbindung zu einem entfernteren Behördenteil, zu einer Nebenstelle oder zu einem Archiv herstellen. Um die Ausrichtung der Richtfunkanlage zu klären, müsste ich sie aus einer besseren Beobachtungsposition vermessen (genau gegenüber ist ein Hotel!) und mit Kartenmaterial vergleichen, zum Beispiel von Google Maps.

Ich gehe zurück und zähle dabei meine Schritte. Der konkave Gebäudeteil ist etwa 70 Meter lang. An seinem „Knickpunkt“, wo also das andere Teil des „L“ anschließt, befindet sich ein rundläufiges Treppenhaus, wie man von außen ganz klar erkennen kann. Das anschließende Gebäudeteil ist gradlinig, knapp 100 Meter lang und weist nur fünf Etagen über dem Erdgeschoss aus. Die Raumanordnung entspricht dem, was ich auch am konkaven Gebäudeteil beobachtet habe. Nur eine Besonderheit ist zu sehen: In der ersten Etage führt nach etwa einem Drittel der Strecke eine gläserne „Beamtenlaufbahn“, also eine umschlossene Personenbrücke zum gegenüberliegenden, wilhelminischen Gebäude des Amtsgerichts. In ihr bewegen sich vereinzelt Personen.

Am nördlichen Ende dieses Gebäudeteils schließt das offenbar etwas ältere Landgericht an. Die Anordnung der Fenster variiert etwas, so dass die Etagen beider Gebäude wahrscheinlich mit kleinen Treppen verbunden sind. Von außen ist im Bereich des Gebäudeanschlusses kein Treppenhaus erkennbar.

Das muss innen liegen, weil es vom Baurecht vorgeschrieben ist. Auch dieser Gebäudeteil weist Innengänge auf mit beidseitig anschließenden Büroräumen, wie man sieht.

Am nächsten Vormittag stelle ich mich in besserer Alltagskleidung neben den Eingang rechts neben dem Tor zum Innenhof. Er besteht aus einer

[458] Die Geschichte stammt vom 17.06.2007. Die Sicherheitsmaßnahmen sind seither erheblich verbessert worden.

zweiflügeligen Glas-Schiebetür, die in einer gläsernen Personenschleuse mündet, die zwei Türen hat. Die linke, ebenfalls eine Schiebetür, öffnet sich automatisch.

Hinter ihr befindet sich eine Pförtnerloge, die mit einem „formlos uniformierten" Menschen besetzt ist. Auf seinem Sweatshirt befindet sich die Aufschrift „Justiz".

Ich benehme mich unauffällig, wartend, rauche in Ruhe eine Zigarette. Würde mich jemand ansprechen, würde ich sagen: „Ich warte auf einen Kollegen." Dies ist ein öffentlich zugängliches Gebäude im Innenstadtbereich und deshalb auch ein üblicher Treffpunkt. Die Ausrede zieht immer.

An mir ziehen Menschen vorbei, die sich in fünf Gruppen einteilen lassen.

Das sind zunächst die etwas „abgewrackt" wirkenden Leute mit nachlässiger Kleidung, die häufig auch ungepflegt aussehen. Sie haben fast immer einen Zettel in der Hand – eine Zahlungsaufforderung oder eine Ladung, wie ich vermute – wenden sich immer an den Pförtner und werden von ihm immer nicht ganz freundlich bedient, wie man an der Gestik und den Körperbewegungen sieht. Es handelt sich also um „Kundschaft", die zur Vernehmung, zum Strafantritt oder zu einem Gerichtstermin geladen ist und hier vermittelt wird.

Die zweite Gruppe zeichnet sich dadurch aus, dass sie meist einzeln, aber auch in Gruppen mit einem Pkw vorgefahren kommen und immer Akten in roten Aktenhüllen bei sich trägt. Die meisten dieser Leute sind zivil gekleidet und die anderen tragen Polizeiuniformen.

Auch sie wenden sich immer an den Pförtner und werden von ihm offenbar freundlicher bedient. Schneller als bei der ersten Gruppe greift der Pförtner zum Telefon und sie verschwinden zu den beiden Fahrstühlen, die sie nach oben befördern.

Bei der dritten Gruppe handelt es sich offenbar um Mitarbeiter oder Vertraute. Sie gehen – meistens grüßend – am Pförtner – der zurück grüßt – vorbei und warten vor den Fahrstühlen, bis sie einsteigen können. Sie grüßen auch andere Wartende und sprechen – gelegentlich vertraulich wirkend – mit ihnen.

Ich vermute, dass diese Leute „Schlüsselgewalt" haben und die Zugänge zu den Büroräumen verschlossen sind – sonst würden sich die „Polizisten" nicht artig beim Pförtner melden – nicht alle.

Die vierte Gruppe ist interessant. Sie ist nicht elegant, aber geschäftsmäßig gekleidet. Alle ihrer Vertreter tragen eine mehr oder weniger große Aktentasche und fast alle warten nicht auf den Fahrstuhl, sondern besteigen gruß- und kontaktlos die Wendeltreppe in Richtung erstes Geschoss. Viel höher werden sie nicht steigen. Einerseits machen sie überwiegend einen gehetzten Eindruck (Termindruck? Erledigungsdruck?), andererseits scheinen sie mit den Räumlichkeiten und Anbindungen vertraut zu sein.

Sie müssen offenbar keine verschlossenen Türen passieren und die Laufbrücke, die ich im Bereich der ersten Etage gesehen habe, zeigt, dass hier wahrscheinlich alle drei Behörden miteinander verbunden sind. Nur ganz wenige dieser Leute wenden sich an den Pförtner und lassen sich vermitteln.

Die letzte und kleinste Gruppe besteht aus jüngeren Leuten im Studentenalter, die grußlos (autistisch? unsicher?) und zielstrebig in den hinteren Bereich der Eingangshalle gehen, wo sich, wie ich jetzt sehe, der Eingang zur Bibliothek des Landgerichts befindet.

Ich habe mir Zeit gelassen und weiß jetzt einiges über diese Behörde, ohne einen Schritt in sie gesetzt zu haben:

Nach der Anzahl der Räume, ihrer Anordnung und dem Publikumsverkehr müssen hier mindestens 200, wahrscheinlich mehr als 250 Leute arbeiten.

Es ist eine öffentliche Behörde mit Durchgangs- und Publikumsverkehr. Ihr innerer Bereich ist wahrscheinlich durch verschlossene Flurtüren gesichert.

Sie hat drei Treppenhäuser, davon ein öffentlich zugängliches im „Knickbereich" des L-förmigen Gebäudes und zwei weitere, die baurechtlich vorgeschrieben, aber von außen nicht direkt erkennbar sind.

Eine Standard-Verkabelung für EDV-Anlagen

kann keine Strecken von mehr als 100 Meter überbrücken. Die Flurlängen des Gebäudes zwingen dazu, dass irgendwo im Bereich des sichtbaren Treppenhauses die zentralen Komponenten der EDV zusammen laufen. Wahrscheinlich in der ersten Etage, weil das Erdgeschoss von der Bibliothek und linksseitig offenbar von einem Sitzungssaal eingenommen wird.

Die Richtfunkanlage ist auf hohe Leistung ausgelegt. Sie benötigt eine Wandlungs- und Steuerungsstation in dem Bereich zwischen den zentralen Komponenten und ihrem Standort, weil sonst die Strecke von 100 Metern überschritten wäre. Dazu dürfte ein eigener, zwar kleiner, aber wahrscheinlich abgeschlossener Raum verwendet werden.

Ich werde jetzt meine Aktentasche unter den Arm klemmen und grußlos zum Fahrstuhl gehen, dort werde ich die Taste für die erste Etage drücken, aber dann in den siebten Stock fahren. Zuerst werde ich danach schauen, ob die Flure wirklich verschlossen sind und ob es noch unverschlossene Nebenräume gibt, wo technische Komponenten oder andere interessante Einrichtungen abgestellt oder installiert sind. Dabei lohnt sich immer auch ein Blick auf Blechtüren im Mauerwerk, hinter denen sich häufig die Verteilerkästen für die Telekommunikation und die Datennetze befinden.

Von oben nach unten werde ich das Treppenhaus nutzen, das ist immer unauffällig, weil die meisten Leute mit dem Fahrstuhl nach oben fahren und eher gelassen das Treppenhaus nach unten benutzen. Ich liebe bequeme Leute, die eigentlich verschlossene Türen mit Keilen oder anderen Gegenständen geöffnet halten, um den Zugang zu den Fluren frei halten oder ihren Besuchern den Zugang zu ermöglichen, ohne ihnen einen Schlüssel geben zu müssen.

Besuchergruppen liebe ich sowieso. Ihr Leiter kennt die einzelnen Personen der Delegation in aller Regel nicht, so dass man sich der Gruppe einfach nur unauffällig anschließen muss, um in verschlossene Bereiche zu gelangen.

Unauffälligkeit und Smalltalk sind die wichtigsten Türöffner für geschlossene Bereiche, deren Sicherheit von Niemanden so richtig überwacht wird.

B.2 3. Blick von innen

Kurz vor zwölf Uhr. Mittagszeit. Kolleginnen und Kollegen treffen sich und machen sich auf den Weg zur Kantine. Ich grüße – freundlich und zurückhaltend – und schließe mich der Gruppe an. Man hält mir die Tür auf und schon bin ich in dem „verschlossenen“ Flur. Die Gruppe biegt zu einem innen liegenden Treppenhaus ab (wie ich von außen vermutet hatte!) und ich gehe ein paar Schritte weiter. Schon bin ich wieder unauffällig von der Gruppe getrennt.

Ich gehe zurück zu der Tür, aus der Mann kam, der sich zuletzt der Gruppe anschloss. Sein Name steht auf einem Schild neben der Tür, „Müllermann“, aber die Tür ist verschlossen.

Ich klopfe an der Nachbartür und trete ein. Das Zimmer ist besetzt. „Entschuldigen Sie, ich bin mit Herrn Müllermann verabredet.“ „Der müsste gerade zu Tisch sein“, lautet die freundliche Antwort. Auch die beiden nächsten Türen sind verschlossen. Eine weitere systematische Untersuchung könnte bei dieser Tageszeit zu auffällig sein.

Ich schlendere den Flur zurück. Fast an seinem Ende führt ein dicker aufgeschraubter Kabelschacht quer an der Decke über den Gang. Hier laufen also die Datenleitungen für die Büros des Flures zusammen. Wie ich vermutet hatte, befindet sich der zentrale Raum für die Datenverarbeitung in der Nähe des zentralen Treppenhauses.

Die Flurtüren lassen sich von innen mit einem Türgriff öffnen. Zwei Etagen tiefer habe ich Glück. Die Flurtür ist unverschlossen, weil sie nicht richtig ins Schloss gefallen ist.

Auch hier treffen sich Kolleginnen und Kollegen zum Mittagessen. Eine von ihnen vergisst, ihre Bürotür abzuschließen. Kaum ist die Gruppe aus meinem Blick, bin ich in ihrem Büro. Ich habe jetzt etwa zwanzig Minuten Zeit. Der PC ist eingeschaltet und der Bildschirmschoner oder eine andere Zeitschaltung sind noch nicht aktiv. Ich komme jetzt an alle Informationen, zu denen auch die unvorsichtige Mitarbeiterin Zugang hat.

B.2 4. Nachwort

Inspiriert zu den beiden Geschichten haben mich die kernigen Aussagen von Eschbachs Industriespion [459]: ***Ich komme nicht durch ein Kabel, ich komme durch die Tür. Ich knacke keine Passwörter, ich knacke Schlösser.***

Auch er ist eine fiktive Figur, ebenso wie der Ich-Erzähler in den beiden Geschichten. Sie zeigen jedoch, wie mit Beobachtung, Allgemeinwissen und Kombinationsgabe tiefe Einblicke in eine fremde Organisation gewonnen werden können.

Solche Einblicke lassen sich auch nicht vermeiden. Verhindern lässt sich nur der Missbrauch der gewonnenen Informationen durch ein durchdachtes und konsequent durchgeführtes, mit anderen Worten: gelebtes Sicherheitskonzept.

Diesem Ziel dienen die beiden Geschichten. Sie sollen den Blick dafür schärfen, wie ein Angreifer denken und handeln könnte.

Hacker - also Leute, die sich über Datennetze in fremde Computersysteme einklinken, um dort auf die Suche nach interessanten Daten zu gehen - gibt es wie Sand am Meer. Sie mögen ihre Daseinsberechtigung haben; auf jeden Fall verkörpern sie das Bild, das sich die Öffentlichkeit von einem Industriespion macht. Ich jedoch begebe mich vor Ort, ich weiß, was ich tue, und ich kann einschätzen, was ich zu sehen bekomme. Das ist mein persönlicher Wettbewerbsvorteil.

Denn was ist, wenn sich die interessanten Daten in Computern befinden, die an kein Netz angeschlossen sind? Was, wenn die Unterlagen, auf die es ankommt, überhaupt nicht in digitaler Form vorliegen, sondern als Papiere, Pläne, handschriftliche Notizen? In solchen Fällen schlägt meine Stunde. Ich komme nicht durch ein Kabel, ich komme durch die Tür. Ich knacke keine Passwörter, ich knacke Schlösser. Ich bin nicht darauf angewiesen, dass es einen Zugang gibt zu den Informationen, die meine Auftraggeber interessieren, ich bahne mir meinen Zugang selbst.

Andreas Eschbach

[459] Andreas Eschbach, Der Nobelpreis, Bergisch Gladbach (Lübbe) 2005, S. 160.

C. Underground Economy

Die ersten beiden Teile widmen sich den Methoden der Cybercrime, der dritte Teil beschreibt ihre Akteure und ihre Zusammenarbeit.

Ich gehe davon aus, dass das Massengeschäft der Cybercrime von einer Vielzahl von Einzeltätern geprägt ist, die Malware einsetzen, Identitätsdiebstähle durchführen, Malware programmieren und schließlich Hacking betreiben, um damit Geld zu verdienen. Sie prägen das Bild von einer chaotisch und diffus erscheinenden Cybercrime-Szene.

Dieses Bild verstellt jedoch den Blick auf die professionellen Akteure im Hintergrund. Sie stellen die Infrastruktur für anonyme Hostserver, maskierte DNS-Adressen und Bezahlsysteme zur Verfügung und betreiben Botnetze, das Skimming [460] und das Phishing im großen Stil. Sie sind die organisierten Internetverbrecher, von denen McAfee bereits 2006 gesprochen hat [461].

Die Bekämpfung der Cybercrime muss beide Gruppen im Auge behalten. Wegen der individuellen Täter ist sie ein Massengeschäft und wegen der organisierten Täter ein strategisches.

C.1 Schurken-Provider und organisierte Cybercrime [462]

Russian Business Network - RBN

Russland: Ein sicherer Hafen für die Internet-Kriminalität?

Die wesentlichen Erscheinungsformen der Cybercrime sind immer hinterhältigere Formen der Malware, der schädliche Einsatz von Botnetzen, das Phishing und das Skimming. Sie lassen auf arbeitsteilige und einander unterstützende Strukturen schließen.

Mit den Schurken-Providern und namentlich dem Russian Business Network setzen sich mehrere Veröffentlichungen aus der jüngeren Vergangenheit auseinander. Sie zeigen ein Netzwerk, das in die technische Infrastruktur des Internets eingebunden ist und kriminelle Aktivitäten von der Öffentlichkeit und der Strafverfolgung abschottet.

Die Akteure der Cybercrime haben sich den Herausforderungen der Informationstechnik und des Internets gestellt und verdienen mit ihren kriminellen Aktivitäten offenbar gutes Geld.

Die meiste Malware kommt aus Russland [463], meldete der Cyberfahnder am 21.02.2008 unter Bezugnahme auf tecchannel. Dabei wurde auch *der Zusammenbruch des RBN (Russian Business Network)* erwähnt, der schon bejubelt wurde [464], sich im Nachhinein aber als eine vorübergehende Umstrukturierung heraus stellte.

---

460 **CF**, Arbeitspapier Skimming #2, 02.03.2010; Dieter **Kochheim**, Skimming (Arbeitspapier)

461 **CF**, erste Typenlehre, 27.07.2008

462 Der Aufsatz erschien erstmals am 13.07.2008.

463 **CF**, gefährliche Lokale, 21.02.2008; Russland wieder auf Platz Eins in der Malware-Achse des Bösen, tecchannel 21.02.2008. Jüngere Zahlen wegen Malware-Anhänge an E-Mails lassen Russland eher unverdächtig erscheinen (**CF**, Schurkenstaaten, 20.06.2008). Auch im **CF**, Spam-Monitor von funkwerk (21.06.2008) hat Russland seinen festen Platz, ohne aber auffallend häufig vertreten zu sein

464 **CF**, Russian Business Network ist offline, 07.11.2007

Aufsehen erregte die Untersuchung von David Bizeul [465]. Laut Heise erkundete er seit Sommer 2007 *vier Monate lang in penibler Computer-Detektivarbeit die Struktur des RBN. Auf 406 Servern mit rund 2090 Internet-Adressen fand er so ziemlich alles, was es im Internet nicht geben dürfte: Kinderpornos, Software zum Datendiebstahl, Anwerbeseiten für angebliche Finanzagenten, Drop Zones*. [466]

Im April 2008 beschäftigte sich Gordon Bolduan im Technology Review mit dem RBN und stellt als Aufmacher voran [467]:

Das Internet ist ein mächtiges Werkzeug – sowohl für legale Geschäfte wie auch für Verbrechen. Mittlerweile hat sich im Netz eine gut organisierte kriminelle Subkultur entwickelt, die Milliarden verdienen dürfte und selbst Mittätern Angst macht.

Im Mai 2008 folgte schließlich ein wirklich spannender Artikel in der c't von Frank Faber [468]. Sein Aufmacher lautet:

Wenn Girokonten von Phishern leer geräumt oder Kreditkartendaten missbraucht werden, führen die Spuren oft nach Russland. Mit der Unterstützung von Netzbetrügereien verdienen die Hintermänner des „Russian Business Network" Millionen. Und das augenscheinlich, ohne entscheidend von Strafverfolgungsbehörden gestört zu werden.

[465] David **Bizeul**, Russian Business Network study, bizeul.org 19.01.2008;
CF, Russian Business Network – RBN, 04.05.2008.

[466] Innovation im Untergrund, Heise online 20.03.2008; drop zones: Sichere Speicherorte für kriminell erlangte oder kriminell genutzte Daten.

[467] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.

[468] Frank Faber, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008

C.1 1. Cybercrime in Russland

Bezüge nach Russland tauchen tatsächlich häufiger auf, wenn man die Datenspuren in Spam- und Malware-Mails genauer unter die Lupe nimmt [469].

Schon 2006 hatte Moritz Jäger in tecchannel auf die Verbreitung krimineller Dienste und Dienstleistungen im Internet hingewiesen [470] und mich dazu angeregt, hinter dem Phishing organisierte Strukturen zu vermuten [471]. Über solche Angebote und ihre Preislisten wird immer wieder berichtet [472] sowie über spektakuläre Angriffe, die nicht im Alleingang durchgeführt werden können [473].

Über die informelle und geschäftsmäßige Zusammenarbeit verschiedener Tätergruppen im Internet sind mir Hinweise seit 2005 und nicht erst seit dem allgemeinen Bekanntwerden von Botnetzen geläufig [474]. Auch das breit angelegte Ausspähen von Kontozugangsdaten mit dem Ziel, gefälschte Zahlungskarten zum Missbrauch an Geldautomaten einzusetzen [475], ist nur in einer strukturierten Organisation vorstellbar. Sowohl beim Phishing [476] wie auch beim "professionellen" Skimming [477] müssen verschiedene Arbeitsschritte durchgeführt und Fachleute eingesetzt werden, so dass eine steuernde Instanz zu erwarten ist. Schließlich muss auch wegen der Betreiber von Botnetzen der arbeitsteilige Zusammenschluss von Entwickeln, Systemverwaltern und "Kaufleuten" er-

[469] **CF**, gemeiner Versuch: Zahlungsbestätigung, 21.03.2008

[470] Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006

[471] **CF**, Phishing, organisierte Strukturen, 2007

[472] **CF**, geklaute Daten zum Schnäppchenpreis, 09.04.2008;
CF, Trojanerbaukasten mit Support, 20.06.2008;
CF, qualitätskontrollierter Kontomissbrauch, 09.05.2008.

[473] **CF**, filigraner Angriff, 14.05.2008

[474] Holger Bleich,Trojaner-Sümpfe. DDoS- und Spam-Attacken gegen Bezahlung, c't 1/05, Seite 43; Ferngesteuerte Spam-Armeen. Nachgewiesen: Virenschreiber lieferten Spam-Infrastruktur, c't 5/04, Seite 18

[475] **CF**, arbeitsteiliges Skimming, 18.05.2008

[476] **CF**, Das Unternehmen Phish & Co., 2007

[477] **CF**, steuernde Instanz, 18.05.2008

wartet werden [478].

Mit den Erscheinungsformen der Cybercrime in Russland setzt sich besonders Igor Muttik von den McAfee Avert Labs auseinander [479].

Schon in der Sowjetunion wurden die Ausbildungen in den Naturwissenschaften, der Mathematik und der Informatik erheblich mehr gefördert als die in den Geisteswissenschaften. Muttik sieht heute eine Kombination aus relativ niedrigen Gehältern, einer hohen Arbeitslosenquote und der breiten Verfügbarkeit vernetzter Computer (S. 17) im größten Flächenland der Welt mit mehr als 142 Millionen Einwohnern - ganz überwiegend im europäischen Teil des Landes. Er führt sodann prominente Viren, Virenautoren und führende Kenntnisse aus den Bereichen Datenkompression, Kopierschutz, Fernwartung und Systemanalyse auf, die für die Programmierung von Malware hervorragend missbraucht werden können.

Es gibt ein russisches Sprichwort, das besagt, dass die unbeugsame Härte des russischen Gesetzes nur durch die Unmöglichkeit ausgeglichen wird, es durchzusetzen (Muttik, S. 18). In diesem Zusammenhang referiert er über die IT-strafrechtlichen Vorschriften in Russland, über einige spektakuläre Fälle der Strafverfolgung und über private Organisationen, die sich der Bekämpfung der IT-Kriminalität verschrieben haben.

Muttik hat nach Crimeware-Angeboten in Russland gesucht und ist reichlich fündig geworden: Spam-Adressen, Bot-Software, Spionageprogramme zu verhaltenen Preisen (S. 19, 20) und für Großabnehmer gegen Rabatt (S. 20).

Sein Fazit (S. 21): Russland verfügt - ebenso wie *China, ... Brasilien und die Ukraine* - über hoch qualifizierte IT-Fachleute ohne Perspektive am legalen IT-Markt. Selbst wenn sie Arbeit haben, sind die Einkommen, die durch kriminelle Programme und ihren Einsatz erwartet werden können, ein ganz erheblicher Anreiz.

Über die innere Struktur der Botnetzbetreiber gibt es nur Spekulationen. Ich bin bisher davon ausgegangen, dass sie eher als Einzelpersonen handeln. Das mag falsch sein, weil auch insoweit verschiedene logistische Aufgaben bewältigt werden müssen, die eine Arbeitsteilung geradezu aufdrängen:

⇨ *Softwareentwicklung und -pflege.*

⇨ *Vertrieb der Malware zur Verbreitung der Zombieprogramme durch Spam-Aktionen [480] und Infiltration fremder Webseiten [481].*

⇨ *Vertragsverhandlungen wegen des Einsatzes des Botnetzes.*

⇨ *Administration des Botnetzes.*

⇨ *Finanzverwaltung.*

Für die Annahme, dass auch der Einsatz von Botnetzen durch arbeitsteilige Gruppen erfolgt, sprechen vereinzelte Meldungen. [482]

Seine Beispiele für die Strafverfolgung beschränken sich auf Einzelfälle, die teilweise im Ausland erfolgten. Ein "Marktdruck durch Strafverfolgung", wie ich es nennen würde, scheint nicht vorhanden zu sein, so dass das eher geringe Verfolgungsrisiko die Bereitschaft, Cybercrime zu praktizieren, besonders fördern dürfte.

Das Thema "individuelle Spionagesoftware" spart Muttik aus. Es kann bedeutungslos, angesichts der Perspektive von McAfee als Anbieter von Anti-Malware-Software ein vereinzeltes Problem oder bewusst ausgeblendet worden sein.

Ich glaube, dass die zweite Antwort zutrifft. Perspektivisch werden sich aber McAfee und alle anderen IT-Security-Unternehmen auch um die individuellen Malwareformen zur Industriespionage und zur Ausforschung privater Geheimnisse kümmern müssen, weil diese Angriffe mit Sicherheit zunehmen und einen Bedarf des Marktes hervorrufen werden.

Muttiks Prognosen klingen sehr allgemein und zurückhaltend. Er erwartet, dass der russische

---

478 Tom **Espiner**, Harald **Weiss**, Sicherheitsexperten: Storm-Botnet wird bald verkauft, ZDNet 17.10.2007

479 Igor **Muttik**, Die Wirtschaft und nicht die Mafia treibt Malware voran, McAfee 12.02.2008

480 **CF**, Anatomie des Sturm-Wurms, 06.03.2008; **CF**, Kraken-Bot, 08.04.2008

481 **CF**, Massenhacks von Webseiten werden zur Plage, 14.03.2008

482 **CF**, Cybercrime. Botnetze, 07.08.2008

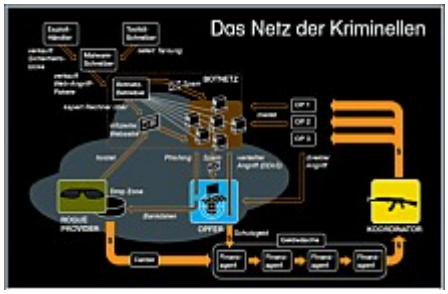
DDoS-Angriff auf Estland

Im April und Mai 2007 gab es einen großen DDoS-Angriff, der auf viele Regierungswebsites in Estland gerichtet war. Ermittler gehen davon aus, dass der Angriff durch die Umsetzung des „bronzenen Soldaten“ veranlasst wurde, einem Denkmal für einen unbekannten russischen Soldaten im Zweiten Weltkrieg. Estnische Behörden hatten beschlossen, das Monument vom Zentrum Tallins auf einen vorstädtischen Militärfriedhof zu versetzen. Dieser Beschluss löste unter der Bevölkerung Tallins Unruhen aus, bei denen eine Person getötet wurde. Später, kurz vor dem Jahrestag des Sieges (zur Beendigung des 2. Weltkriegs, der in Estland am 9. Mai gefeiert wird), begann ein mehrere Tage andauernder DDoS-Angriff. Viele große estnische Websites standen während dieser Zeit nicht zur Verfügung. Unter Sicherheitsexperten herrscht die Meinung vor, dass dieser Angriff von einer Gruppe von Einzelpersonen durchgeführt und von deren patriotischen Gefühlen angeheizt wurde. ... Es konnten keine Hinweise auf eine Beteiligung der russischen Regierung an diesen Angriffen gefunden werden, und selbst wenn es eine Verbindung gäbe, würde diese mit sehr großer Wahrscheinlichkeit nicht entdeckt werden. Nach dem Vorfall beschuldigten sich beide Seiten gegenseitig der Cyber-Angriffe. [483]

Staat die IT-Kriminalität verstärkt verfolgen und damit zurückdrängen wird. Für eine Entwarnung sei jedoch kein Platz, weil andere Regionen der Welt nachdrängen werden.

Wenn aber in Russland das technische Wissen besonders konzentriert ist und gleichzeitig große soziale Spannungen und Verteilungskämpfe bestehen, dann dürfte Muttiks Einschätzung mehr als fraglich sein. Ich befürchte, dass der russische Bär auch bei der Cybercrime noch gehörig mitwirken wird.

Muttik erwähnt die russische Mafia am Rande und erkennt, dass sie ein wirtschaftliches Interesse an der Förderung der Cybercrime haben könnte. Ich bin ganz sicher kein Experte für die Einschätzung dieser Situation, befürchte aber auch, dass solange solche kriminellen Strukturen frei oder relativ frei agieren können, das profitable Geschäft mit der Cybercrime einen besonders "sicheren Hafen" haben könnte. Frei von Strafverfolgung und unter



stützt von sprudelnden kriminellen Einnahmen.

Keiner hackt mehr heute zum Spaß, das ist knallhartes Business geworden. [484]

C.1 2. Zusammenarbeit von Spezialisten

Gordon Bolduan [485] stellt in das Zentrum seiner Betrachtung die modernen Botnetze, die er zutreffend als das mächtigste kriminelle Werkzeug ansieht, das zur Verfügung steht. Die von der Bot-Malware infizierten Rechner lassen sich nicht nur nach persönlichen Daten und Zugangscodes ausforschen, sondern in ihrer Gemeinschaft zu allen Massenerscheinungen im Internet missbrauchen. Die wichtigsten Formen sind das werbende Spamming, die Verbreitung von Malware mittels E-Mail-Anhänge, das Phishing und schließlich verteilte Angriffe (DDoS). Allein schon die Drohung mit einem solchen Angriff kann zur Erpressung zu Schutzgeld eingesetzt werden.

Wegen der Leistungsfähigkeit der Botnetze ist zu ergänzen, dass die Zombie-Software zumeist modular aufgebaut ist, so dass sie immer wieder aktualisiert und sich wandelnden Bedürfnissen angepasst werden kann.

Einzelne Geräte aus dem Botnetz können zudem als Webserver für die Verteilung von Software-Updates, zur Steuerung kleinerer Gruppen von infiltrierten Rechnern und zu ihrer Überwachung verwendet werden. Einzelne Varianten der Botsoftware gehen sogar sehr behutsam mit den infiltrierten Rechnern um, um nicht aufzufallen und den Zombie möglichst lange missbrauchen zu

[483] Muttik, S. 21

[484] Balduan, Digitaler Untergrund, Technology Review 4/2008, S. 28

[485] Gordon Bolduan, S. 26 ff.

können [486].

Bolduan bleibt nicht bei der Beschreibung des Botnetz-Phänomens, sondern widmet sich vor alem dem Netzwerk der Cyber-Kriminellen.

Die beteiligten Spezialisten lassen sich nämlich wegen ihrer Aufgaben und Tätigkeiten unterscheiden und dürften teilweise in Bandenstrukturen organisiert sein.

C.1 3. organisierte Botnetze

Malware missbraucht Sicherheitslücken. Die Zombie-Software zum Betrieb eines Botnetzes ist eine spezialisierte Form von Malware, die ihrem Einsatzzweck angepasst ist.

In der frühen Hackerkultur war es üblich, Sicherheitslücken zu veröffentlichen, um die Hersteller von Hard- und Software unter Druck zu setzen, damit sie Gegenmaßnahmen treffen. Daneben hat sich inzwischen ein Markt für unbekannte und eben nicht veröffentlichte Sicherheitslücken entwickelt. Diese Händler nennt Bolduan ***Exploit-Händler*** (Exploit Vendors), die ihre Kenntnisse an die Entwickler von Malware verkaufen.

Mit den ***Toolkit-Schreibern*** identifiziert er eine zweite Gruppe von Spezialisten. Sie liefern die Funktionen zur Tarnung der infiltrierten Software.

Die ***Malware-Schreiber*** führen die Zulieferungen der Exploit-Händler und Toolkit-Schreiber zusammen. Sie produzieren entweder ein fertiges Programm oder entwickeln Malware-Baukästen, die sie vermarkten [487].

Bereits Moritz Jäger hat darauf hingewiesen, dass in dieser Szene Verrechnungskonten auf der Basis von Edelmetallen sehr beliebt seien [488]. Sie lassen die verzögerungsfreie Verrechnung geldwerter Forderungen zu und sind nur etwas zögerlich bei dem Transfer zu nationalem Geld. Der Anbieter E-Gold führt zum Beispiel für jeden der Beteiligten ein Guthabenkonto in der Verrechnungseinheit "Gold", womit die gegenseitigen Forderungen ab- und zugebucht werden können [489].

Bolduan [490] benennt als Alternative den Bezahldienst WebMoney (wmz), *dessen Webadresse auf eine WebMoney Corporation in Japan registriert ist und der als Support-Kontakt eine Adresse in Moskau angibt; auf einer Liste der WebMoney akzeptierenden Händler finden sich hauptsächlich Online-Kasinos, Kreditkartendienste und Goldbörsen – und dazu ein ukrainisches Programmierer-Team.*

Botnetze richten sich meistens gegen eine Vielzahl von Opfern [491], wenn nicht ein verteilter Angriff oder eine Spionageaktion gegen ein einzelnes Ziel gerichtet wird.

Einzelne Zombies fallen immer wieder aus, weil sie vorübergehend aus dem Netz genommen werden, eine Antiviren-Software die Malware aufgespürt und unschädlich gemacht oder das Opfer sich einen neuen PC zugelegt hat [492]. Zum Erhalt seines Botnetzes muss der Betreiber deshalb immer wieder Malware verteilen, um durch neue Zombies den Bestand zu erhalten oder auszubauen. Solange dabei E-Mail-Anhänge verwendet werden, lässt sich zur Verteilung das schon bestehende Botnetz nutzen.

Die Kenntnisse der Anwender und die Sicherheitsfunktionen in den PCs haben zugenommen, so dass die Malwareverbreitung vermehrt dazu übergegangen ist, Injektionsverfahren einzusetzen, die beim Surfen im Internet oder beim Öffnen bislang als harmlos geltender Dokumente zum Zuge kommen.

Die inzwischen sehr häufig eingesetzten infiltrierten Webseiten bedürfen eines Speicherplatzes, von dem aus sie abgerufen werden können. Dazu kann ein infiltrierter Rechner aus dem Botnetz verwendet werden. Das ist jedoch ineffektiv, weil die Zombies in aller Regel über ihre Zugangsprovider dynamische IP-Adressen zugewiesen bekommen und der belastende Datentransfer zu

---

[486] **CF**, Anatomie des Sturm-Wurms, 06.03.2008

[487] **CF**, Trojanerbaukasten mit Support, 20.06.2008

[488] **CF**, neuartige Finanzdienste, 2007

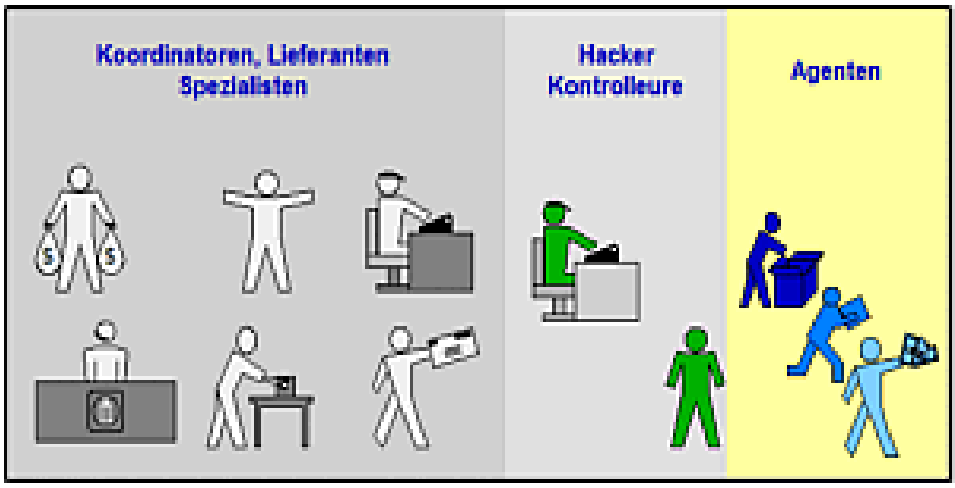
[489] **CF**, Verrechnungssysteme auf der Basis von Edelmetallen, 2007

[490] Balduan, S. 32

[491] **CF**, Botnetze: Wirkung wie DDoS, 17.10.2007

[492] Weihnachten ließ Botnetze schrumpfen, Heise online 28.12.2006

auffällig wäre.



Sinnvoller ist es, dafür einen Server zu verwenden, bei dem der zusätzliche Traffic (Datendurchsatz) nicht weiter auffällt oder vom Anbieter toleriert wird. Die erste Wahl für die Installation infiltrierter Webseiten sind gekaperte, also gehackte Hostserver, zumal ihre statische Internetadresse nach jedem - spätestens zweiten - Missbrauch "verbrannt" und in die üblichen Spamming- und Malware-Abwehr-Datenbanken aufgenommen ist. Dasselbe gilt für die Ablage der Update-Versionen für die Zombie-Software.

Wenn der Täter nach der Guerilla-Strategie verfährt, sind gekaperte Hostserver tatsächlich die beste Wahl. Sie werden missbraucht und sogleich wieder aufgegeben. Langfristige Planungen bedürfen jedoch "sicherer Häfen". Nur hier können aufwändige Website-Farmen und konspirative, geschlossene Benutzergruppen eingerichtet und kriminelle Daten gehostet werden. Sie bedürfen der schützenden Hand eines starken und souveränen Türstehers, der sowohl neugierige Nachfragen wie auch die Nachstellungen von Strafverfolgungsbehörden abprallen lässt. Sie nennt man ***Schurken-*** oder ***Rogue-Provider*** und das ***Russian Business Network - RBN*** - dürfte das bekannteste von ihnen gewesen sein.

C.1 4. Spezialisierung

Nach Balduan lassen sich verschiedene Personengruppen definieren, die sich durch ihre besonderen Fertigkeiten und Aufgaben unterscheiden.

C.1 4.1 Drop Zones

Im System der Cybercrime hat der Rogue-Provider eine zentrale Rolle, weil er die sicheren und abgeschotteten Drop Zones zur Datenhaltung liefert. Hier werden die Farmen und die Malware-Updates gespeichert, bevor sie in das Botnetz zur weiteren Verbreitung eingespeist werden, sowie die von den Opfern ausgespähten Daten zwischengelagert. Außerdem ist er der bevorzugte Lieferant für Kommunikationsplattformen und geschlossene Benutzerkreise zum Informations- und Datenaustausch mit Inhalten, die nicht für die Öffentlichkeit und schon gar nicht für die Strafverfolgung bestimmt sind.

C.1 4.2. Carder

Als Carder wird ein Krimineller bezeichnet, der geklaute Kreditkartendaten kauft und diese zu Bargeld macht [493].

Wie alle anderen Hauptpersonen auch bleibt der Carder im Hintergrund und kann sich verschiedener Methoden bedienen. Beim Phishing sind das im wesentlichen drei Methoden:

⇨ mit Hilfe eines Hackers werden die Kontozugangsdaten eingesetzt, um Überweisungen vorzunehmen,

⇨ das Homebanking des Opfers wird online überwacht und im entscheidenden Moment eine Überweisung umgeleitet,

⇨ die infiltrierte Malware verändert während eines Überweisungsvorgangs die Zieldaten mit denen des Carders.

Die vierte Methode ist das Kopieren von Zahlungskartendaten auf Rohlinge. Sie ist im wesentlichen vom Skimming bekannt.

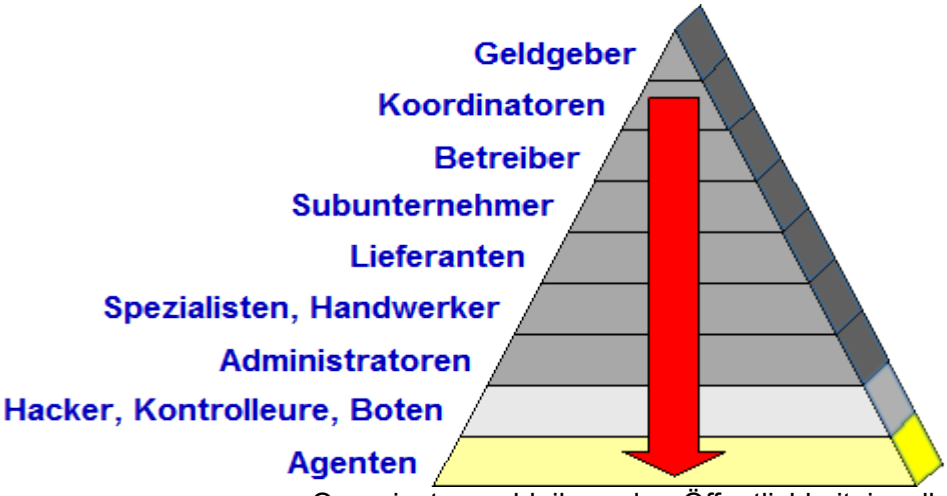
---

[493] Bolduan (4), S. 30:
... die damit Kreditkarten fälschen oder hochwertige Wirtschaftsgüter im großen Stil bestellen.

C.1 4.3 Agenten

Die Agenten sind die Klinkenputzer der Cybercrime. Sie handeln in der Öffentlichkeit und werden mit verschiedenen Aufgaben eingesetzt.

Am bekanntesten sind seit dem Phishing die Finanzagenten. Auf ihre Girokonten werden die Überweisungen umgeleitet und sie sollen per Bargeld-Transfer oder mit anderen Methoden die kriminellen Gewinne zu den Hinterleuten bringen.



Organisatoren bleiben der Öffentlichkeit in aller Regel verborgen (Schaubild auf der Vorseite). Die Agenten müssen in der Öffentlichkeit arbeiten und unterliegen einem mehr oder weniger großem Entdeckungsrisiko. In dem Bereich dazwischen sind die Hacker beim Phishing, die Unterhändler, z.B. zum Anwerben von Agenten, und die Kontrolleure angesiedelt, die die Agenten überwachen und die Erlöse einsammeln. Sie müssen mit zurückhaltendem Risiko in der Öffentlichkeit auftreten.

In arbeitsteiligen Organisationen ist damit zu rechnen, dass die handelnden Personengruppen streng voneinander getrennt sind. Die Hinterleute lassen sich deshalb kaum feststellen.

Beim Skimming werden verschiedene Agenten eingesetzt. Die erste Gruppe muss die Überwachungstechnik installieren und schließlich wieder abbauen und die zweite in einem anderen Land die nachgemachten Zahlungskarten einsetzen. Dabei ist die Tätigkeit des Cashing, also der Einsatz gefälschter Zahlungskarten am Geldautomaten, verhältnismäßig einfach, aber wegen des Entdeckungsrisikos gefährlich.

Zu den Agenten können auch die Hacker gezählt werden, die fremde Bankkonten manipulieren (Phishing).

C.1 4.4 Spezialisten

Von den Agenten muss man die Spezialisten unterscheiden, die das kriminelle Handwerkzeug liefern. Das sind die Malwareschreiber und Adressenlieferanten für Spamaktionen, die Texter für Webseiten und Spams, die den richtigen Jargon treffen und fremdsprachensicher sein müssen, die Webdesigner für das Pharming und die Administratoren für Botnetze.

Im Zusammenhang mit dem Skimming kommen auch richtige Handwerker zum Einsatz, die einerseits die Überwachungstechnik her- oder zusammenstellen und andererseits Zahlungskarten fälschen. Es werden vereinzelt Fassaden eingesetzt, deren Herstellung großes handwerkliches Geschick erkennen lässt.

Die Lieferanten, Spezialisten, Koordinatoren und

C.1 4.5 Koordinator. Operation Group

Die zentrale Figur jedoch ist ... ein „Independent Business Man“ – eine Person, die Kontakte zur Unterwelt pflegt und zwischen Bot-Herdern, Hackern, Malware-Schreibern und Spammern koordiniert. ... mithilfe der Botnetz-Infrastruktur kann der Koordinator Unternehmen mit verteilten Massenangriffen auf ihre Webseiten drohen und so Schutzgeld erpressen, Spam-Wellen mit Werbung für überteuerte Produkte oder Aktien lostreten oder tausendfach persönliche Informationen wie Bankzugangsdaten ergaunern. [494]

Nach einem von Bolduan zitierten Gewährsmann soll es sich bei den Koordinatoren in aller Regel um frühere KGB-Leute und / oder Angehörige der

[494] Bolduan, S. 30

russischen Mafia handeln [495]. Diese Leute seien auch erfahren in der Geldwäsche.

Der Koordinator betreibt Cybercrime-Management und hat dafür gewisse Gestaltungsfreiräume, je nach dem, welche Aufgaben er an Subunternehmer outsourcen kann und will.

Um zum Beispiel eine Phishing-Aktion durchzuführen, braucht er ausgespähte Kontozugangsdaten. Die kann er kaufen, selber erheben oder die Erhebung und den Missbrauch in eine kombinierte Malware-Aktion einbinden.

Mit dem Einkauf von Kontodaten, anderen Diensten oder Modulen, die der Koordinator benötigt, kann er national tätige ***Operation Groups*** [496], also Subunternehmer oder Vermittler beauftragen.

Sobald er über diese "veredelten" Daten verfügt, braucht er noch Hacker für den Kontomissbrauch und Agenten für die Sicherung der kriminell erlangten Gewinne.

Die "Hacker" müssen mehr vertrauenswürdig als kompetent sein. Der Aufruf eines Homebanking-Portals und der Missbrauch von Kontozugangsdaten einschließlich "normaler" Transaktionsnummern nach dem alten TAN-Verfahren ist eine eher banale Sache.

Komplizierter wird es, wenn die ausländische Herkunft des Angriffs verschleiert werden muss. Dann muss der Hacker einen Anonymisierer benutzen, der allerdings dem Rechenzentrum der angegriffenen Bank ebenfalls auffallen könnte.

Die Alternative dazu ist die Nutzung eines unauffälligen Rechners, dessen Standort im Zielland ist. Dazu muss sich der Hacker entweder bereits dort befinden oder ein infiltriertes Gerät nutzen. Dazu wiederum eignen sich entweder gehackte Einzelgeräte oder Zombies aus einem Botnetz.

Schließlich benötigt der Koordinator noch Agenten, die ihre Girokonten zur Verfügung stellen und den kriminellen Gewinn zu ihm übertragen.

Die übrigen Erscheinungsformen der Cybercrime weichen wegen ihrer Anforderungen von diesem Beispiel ab. Das Grundmodell bleibt immer gleich:

Auf der Ebene unterhalb der Koordinatoren sind die Betreiber angesiedelt, die über Botnetze oder Drop Zones (Rogue-Provider) verfügen.

Sie sind ihrerseits auf Subunternehmer angewiesen, die ihnen die nötige Malware liefern oder für bestimmte "Geschäfte" besonders spezialisiert sind (z.B. Carder, Operation Groups).

Die Zulieferung besonderer Informationen (Adressen, Sicherheitslücken, Bankkonten) oder Modulen (Rootkit, Hardware) erfolgt durch Zulieferer. Sie bleiben ebenso wie die Spezialisten und Handwerker im Hintergrund, die z.B. die Überwachungstechnik und die Dubletten für das Skimming oder Webseiten und Texte für das Phishing herstellen.

Die Administratoren kümmern sich um den laufenden Betrieb von Botnetzen und Pharmen.

Hacker im hier verwendeten Sinne werden für den Online-Missbrauch beim Phishing oder für das Ausspähen bei der Industriespionage benötigt. Auf dieser Ebene sind auch die Kontrolleure (Vorarbeiter) für die Agenten angesiedelt, die deren Einsätze abstimmen oder Finanzagenten betreuen.

Die Basis stellen schließlich die Agenten, die sich im Licht der Öffentlichkeit bewegen müssen.

C.1 4.6 Rogue Provider

Schurken-Provider betreiben wie andere Anbieter im Internet auch eine normale technische Infrastruktur. Sie sind autonome Systeme, also in sich geschlossene technische Netzwerke, die mit anderen internationalen Netzen und Carriern durch Verträge verbunden sind [497].

Ihre Netzdienste sind dieselben, die auch andere Host- und Zugangsprovider bieten: Die Verwaltung von DNS-Adressen [498], Speicherplatz (Hostspeicher) und Kommunikationsplattformen (Chat, geschlossene Benutzergruppen).

Sie unterscheiden sich hingegen wegen ihres Geschäftsmodells, weil sie ihre Kunden gegenüber

[495] Balduan, ebenda

[496] Balduan, ebenda

[497] **CF**, autonome Systeme und Tiers, 2007

[498] **CF**, Auflösung von DNS-Adressen, 2008;
CF, Kontakte. Tier-1. DeCIX, 2007

In einer ... Grauzone operieren die sogenannten Rogue Provider, die mit „bullet proof hosting“ werben, also im Prinzip versprechen, dass sie Ermittlungen von Strafverfolgern nicht übermäßig unterstützen und dass sie auf Missbrauch-Beschwerden nicht reagieren. ...

Das ... Geschäftsmodell des RNB war simpel und dreist: Je mehr eine Domain in den Fokus der Öffentlichkeit geriet, je mehr Beschwerden an die E-Mail-Adresse für Missbrauch geschickt wurden, desto mehr Geld verlangten die Russen von ihren Kunden.

Bolduan, S. 32

der Öffentlichkeit und vor allem vor den Strafverfolgungsbehörden abschotten. Dazu werden Scheinfirmen eingerichtet, die als Inhaber von Domänen geführt werden, oder Fantasie- und Aliasnamen benutzt. Solche schurkischen Dienste schließen es aus, dass die Betreiber und Hinterleute aus Registern oder anderen öffentlichen Quellen identifiziert werden können (Bullet Proof Domains [499]). Zum Zweck der Abschottung werden vereinzelt auch technische Tricks eingesetzt, die den technischen Standort des Rogue-Servers verschleiern [500].

antispam.de nennt diese Art von Unternehmen *beschwerdeignorante Provider und Hoster* [501] und benennt einige von ihnen aus China, Korea, Russland und den USA. In Bezug auf Russland sind das informtelecom.ru [502] und das Russian Business Network [503]. Auch Deutschland ist nicht frei von zögerlich reagierenden Providern.

Das Russian Business Network (RBN) ist ein russischer Internetdienstanbieter mit Sitz in St. Petersburg, Levashovskiy Prospekt 12. Ein großes Netz von Tochterfirmen haben u.a. ihren Sitz auf den Seychellen, in Panama, Türkei, China und Großbritannien. Als Carrier sind RBN-Rechner teilweise mit denen von Firmen wie AkiMon sowie SBT-Tel vernetzt, deren Uplink Silvernet über Anschlüsse an großen Rechnerknoten wie MSK-IX verfügen. Die Zeitschrift c't ordnet den Provider der Gruppe der Rogue ISPs zu, die ihre kriminellen Kunden vor dem Zugriff von Justizbehörden schützen und welche deren Dienstleistungen auch dann weiter betreiben, wenn sich Beschwerden häufen. Zu den Angeboten von Kunden von RBN gehören Affiliatensysteme wie iFramecash.net, Rock-Phish-Crew. Zu den Techniken gehören teilweise Innovationen wie Fast Flux-botnet (schneller Wechsel), welche IP-Spuren verwischen sollen. Schadsoftware wie MPack-Kit, Sturmwurm-Bot, Gozi-Bot, Torpig oder 76Serve, (vermietbare Bot-Armee-Software, die zur Ausspähung von Kreditkarten oder Identitäten dient), wird von RBN gehostet.

Wikipedia [504]

---

499 Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007; ders. ebenda: ... Bullet Proof Domains

500 Russian Business Network bekannt? tecchannel 17.10.2007

501 beschwerdeignorante Provider und Hoster, antispam.de

502 *informtelecom.ru: Dieser russische Webhoster ist seit einigen Jahren schon immer wieder durch Hosten von Phishing-/Muli-Webseiten, Warez-Piracy-Seiten, Casino-Spam-Seiten, Bride-Scam-Seiten u.a. aufgefallen.*

503 *RBN: Man erfreut sich offensichtlich bester Beziehungen zur russischen Regierung, der Betrieb geht seit Jahren unbehelligt in dieser Richtung weiter. Der gesamte IP-Adressbereich dieses russischen Providers steht auf der Blackliste von Spamhaus.org.*

504 **WP**, Russian Business Network - RBN

C.1 5. Russian Business Network - RBN

Heise nennt die Betreiber des RBN *die "Bösesten der Bösen im Internet"* [505] und meldete im Herbst 2007, dass es sich aus dem Internet zurück zöge: *Fast alle bekannten Autonomous Systems (AS) des RBN sind seit Kurzem aus den globalen Routing-Tabellen verschwunden: RBN-AS, SBT-AS, MICRONNET-AS, OINVEST-AS, AKIMON-AS, CONNCETCOM-AS und NEVSKCC-AS. Einzig CREDOLINK-ASN ist im Moment noch in den Tabellen, obwohl deren Netze ebenfalls nicht mehr erreichbar sind.* [506]

Dank Bizeuls Untersuchung [507] kam etwas Licht in die Geschäftsaktivitäten des RBN und seiner Leitungspersonen. *An der Spitze des RBN steht nach Bizeuls Recherchen ... ein Mann mit dem Decknamen "Flyman"* [508]. *Der Firmensitz des nirgendwo registrierten und seit 2005 tätigen Unternehmens ist in St. Petersburg, Levashovskiy Prospekt 12* [509]. *Von flyman wird behauptet, er sei der Neffe eines hochrangigen Politikers aus Sankt Petersburg. So ließe sich erklären, warum der Bandenkopf offensichtlich unbehelligt seinen Geschäften nachgehen kann* [510]. Faber identifiziert einen weiteren Akteur: *Ging es um Domains von RBN oder SBT-Tel und AkiMon, fand sich oft der Name Nikolay Ivanov* [511].

Faber beschreibt in groben Zügen die Anbindungen des RBN [512], die Ursprünge seiner kriminellen Aktivitäten (das Verbreiten von Kinderpornographie, die Verbreitung von Schadcode und die aktive Beteiligung am Phishing; Rock-Phish-Crew) bis hin zur aktuellen Vermietung von Botnetzen, die für das Phishing optimiert sind: *Die Monatsmiete pro Bot konnte je nach dem, wie lange er bereits installiert ist, schon mal 1000 US-Dollar betragen. Je frischer der Bot, desto teurer ist er* [513].

Schließlich bringt Faber das RBN mit den Betreibern des Sturmwurm-Botnetzes [514] in Verbindung, weil die über manipulierte Webseiten verbreitete Malware (MPack-Kit) bei RBN gehostet war [515]. Faber: *Es scheint so, als fungiere das Russian Business Network als Katalysator, als jenes fehlende Teil, das zum Aufbau einer regelrechten Schattenwirtschaft im IT-Bereich nötig gewesen war* [516].

Das Verschwinden des RBN im November 2007 war nur vorübergehend, wie schon Frank Ziemann im Februar 2008 zurückhaltend berichtete: *St. Petersburg gilt als Hochburg der organisierten Online-Kriminalität. Auch das berüchtigte Russian Business Network (RBN), eine Art Internet-Provider für Online-Kriminelle, war bis vor wenigen Monaten dort angesiedelt, soll mittlerweile jedoch umgezogen sein.* [517]

Faber [518]: *Nur einen Tag später tauchten die ersten Sites wieder auf, gehostet allerdings in China und Hong Kong. ... In der Tat war wenig später zu beobachten, dass das RBN zwar weiterhin in Sankt Petersburg residiert, seine Services aber auf verschiedene Länder verteilt. ...*

RBN habe seine Niederlassungen in Panama und der Türkei ausgebaut.

Das RBN ist also Mitte 2008 keineswegs Geschichte, sondern aufgrund der neuen Strategie lediglich wesentlich schwerer zu entdecken. [519]

---

505 Die "Bösesten der Bösen im Internet" isoliert, Heise online 07.11.2007

506 Ebenda

507 David **Bizeul**, Russian Business Network study, bizeul.org 19.01.2008;
CF, Russian Business Network – RBN, 04.05.2008

508 Innovation im Untergrund, Heise online 20.03.2008

509 Frank Faber, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008

510 Ebenda, S. 93.

511 Ebenda.

512 Kasten auf der Vorseite; ebenda S. 93.

513 Ebenda, S. 94.

514 **CF**, Anatomie des Sturm-Wurms, 06.03.2008

515 Frank Faber, ebenda, S. 95.

516 Ebenda; unter Bezugnahme auf Muttik.

517 Frank **Ziemann**, Sturm-Wurm-Bande bald hinter Gittern? PC-Welt 04.02.2008

518 Frank Faber, ebenda, S. 96.

519 Ebenda.

C.1 6.Fazit

Bizeuls Recherchen zeigen, dass beharrliche Forschungen in Verbindung mit Erfahrungswissen verdeckte Strukturen und Zusammenhänge erhellen können. Das Russian Business Network zeigt dabei beispielhaft, wie mit der Kombination aus technischem Wissen, technischer Infrastruktur und den Methoden der Geldwäsche sowie der Verschleierung geschäftlicher Aktivitäten sichere Häfen für kriminelle Machenschaften im Internet aufgebaut und dauerhaft erhalten bleiben können.

Die Annahme von Bolduan, Rogue-Provider in der Form des RBN hätten keine Zukunft und würden völlig von Botnetzen abgelöst, teile ich nicht. Botnetze sind ein schlagkräftiges und wandlungsfähiges Instrument für kriminelle Aktivitäten, können aber Drop Zones für die Lagerung krimineller Inhalte, die kontinuierliche Kommunikation zwischen Lieferanten, Subunternehmer usw. und geschlossene Benutzerkreise nicht ersetzen. Sie werden sich wandeln, aber nicht verschwinden.

Die Auseinandersetzung mit dem RBN hat eine Reihe neuer Begriffe wie Rogue-Provider, Carder, Koordinator oder Exploit-Händler zu Tage gefördert. Sie bergen in sich die Gefahr, die ganze Cybercrime-Szene als differenzierte Veranstaltung von Fachleuten anzusehen. In ihr werden sich sicherlich einige hoch qualifizierte und spezialisierte Einzelpersonen bewegen, die sich besonders mit technischen Einzelheiten befassen.

Wegen der geschäftsmäßigen Präsenz ist jedoch eine Unternehmensstruktur erforderlich, wie sie auch im Wirtschaftsleben bekannt ist. Auch dafür ist das RBN ein Beispiel.

Andererseits zeigt sich die Cybercrime-Szene auch nicht als geschlossenes Ganzes, sondern doch eher als ein geschäftlicher Verbund. Anders sind die offen angebotenen Dienste von Spezialisten nicht zu deuten.

Die Malware-Schreiber dürften sich in aller Regel als Einzelkämpfer herausstellen und die Betreiber als bandenförmige Gruppen. Dasselbe gilt für die Operation Groups, bei denen ich eine strenge Führung vermute.

Das RBN und andere Schurkenprovider können nur dort existieren, wo sie politisch unterstützt werden oder das behördliche und gesellschaftliche Bewusstsein über ihre Gefährlichkeit unterentwickelt ist. Insoweit gebe ich Muttik recht, auch wenn ich nicht glaube, dass sich Russland alsbald aus der Cybercrime verabschiedet.

Sicherlich werden sich andere Schurkenprovider in Schwellenländern ansiedeln. Sie brauchen aber zweierlei: Eine leistungsfähige technische Netzstruktur, an die sie sich anschließen, und eine gesellschaftliche Umgebung, in der sie sich frei bewegen können. Beides bietet Russland.

C.2 arbeitsteilige und organisierte Cybercrime

Der klassische Blick auf die Kriminalität in der Informationstechnik und dem Internet ist der von Technikern und Informatikern geprägte auf die Erscheinungsformen, Sicherheitslücken, Infiltrationswege und Funktionen. Das ist der Security-Blick, dessen Ziele die Sicherung informationstechnischer Systeme, die Datensicherheit und die Abwehr von Angriffen sind.

Diesen Blick haben auch Sicherheitsunternehmen, die ihre Firewall-, Antiviren- und sonstige Sicherheitsprogramme verkaufen wollen. Daran ist nichts Falsches, wenn es um die technische IT-Sicherheit, um betriebliche Abläufe und ihre Gefahrenquellen geht.

Die Grundlage für eine rechtliche und strategische Befassung mit der Cybercrime ist die, dass man zunächst die Grundzüge verstehen muss, wie sie und ihr technisches Umfeld funktionieren. Diesem Blick auf die Erscheinungsformen widmet sich auch der Cyberfahnder, wenn er sich mit den ▸ Angriffspunkten und -methoden, mit der Netztechnik [520] und den kriminellen Erscheinungsformen [521] auseinander setzt.

Die strategische und kriminalpolitische Auseinandersetzung mit der Cybercrime muss jedoch die handelnden Personen, ihre Motive und ihre Ziele betrachten.

Dabei hilft auch der Blick auf die Details, wenn es um handwerkliches Können und die Vorschusskosten geht, die aufgebracht werden müssen, um kriminelle Gewinne zu erzielen. Ganz wesentlich ist jedoch die Frage danach, wie die Steuerung arbeitsteiliger Prozesse, die Bezahlung und die Sicherung der Beute funktionieren. Nur so lassen sich Strukturen erkennen und zerschlagen.

Solche Fragen hat der Cyberfahnder immer wieder angesprochen, meistens aber ohne das Gesamtbild zu betrachten [522].

Dieser Aufsatz führt die (journalistischen) Quellen und Überlegungen zusammen, um die Cybercrime wegen der handelnden Personen und ihre Motive zu betrachten.

Die grundlegende These lautet:

Je aufwändiger und arbeitsteiliger die Cyber-Kriminellen vorgehen, desto mehr sind sie davon motiviert, eine lohnende und dauerhafte Einnahmequelle für kriminelle Gewinne zu schaffen und zu nutzen.

C.2 1. der IT-typische Blick auf die Erscheinungsformen

Findet ein IT-ler (oder ein Marketing-Mensch) eine neue Lösung, ein neues Design, eine isolierte Aufgabe, die er er aus einem Paket gelöst hat, oder eine neue Erscheinungsform einer Malware, so bekommt sie einen eigenen Namen. So entsteht ein Zoo vielfältiger Namen, die vieles trennen, aber nichts verbinden.

Wenn es um die Kriminalität im Internet geht, ist das nicht anders. Wir haben mindestens zwei "Skimmings", das alte [523] und das POS-Skimming [524]. Aber auch das "alte" hat so viele Erscheinungsformen, dass (selbst) ich zwischen dem Proll-Skimming [525] und dem arbeitsteiligen Skimming [526] unterschieden habe.

Das klassische Phishing [527] versuchte, mit nachgemachten Nachrichten bekannter Geschäftsbanken - also direkt über E-Mails - die Kunden zur Preisgabe ihrer Zugangsdaten zu bewegen. Dazu boten sich Eingabefelder in der E-Mail oder ein Link an, mit dem auf ein nachgemachtes Bank-

---

[520] **CF**, Telekommunikation und Internet (Themenseite)

[521] **CF**, Cybercrime und IT-Strafrecht, 08.08.2008

[522] Die arbeitsteiligen Strukturen beim Phishing (**CF**, Das Unternehmen Phish & Co., 2007) und beim Skimming (**CF**, steuernde Instanz, 18.05.2008) wurden mit den Erscheinungsformen behandelt und im Zusammenhang mit der **CF**, Führung: Cybercrime (07.08.2008) zusammen gefasst. Die jüngeren journalistischen Quellen lassen ein umfassendes Bild erkennen:

CF, Schurkenprovider und organisierte Cybercrime, 13.07.2008;

CF, globale Sicherheitsbedrohungen, 27.07.2008

[523] **CF**, Skimming, 2008

[524] **CF**, POS-Skimming, 2008

[525] **CF**, Proll-Skimming, 2008

[526] **CF**, arbeitsteiliges Skimming, 2008

[527] **CF**, Ausforschung von Kontozugangsdaten, 2007

portal geführt wurde. Weil die Täter gleich mehrere Portale fälschten und auf einem gekaperten Server bereitstellten, wurde das in Anlehnung an eine "Farm" [528] als Pharming [529] bezeichnet.

Auch die Methoden zur Tatausführung haben sich dahin gehend gewandelt, dass beim alten Phishing eine zeitliche Trennung zwischen dem Einsammeln der Daten und ihrem Missbrauch bestand. Das "moderne" Phishing führt beide Arbeitsschritte zusammen, indem eine Automatik – nur noch selten ein Mensch - nach der Art des Man-in-the-Middle [530] in den Überweisungsvorgang direkt eingreift oder eine Malware mit vordefinierten Daten diesen Vorgang manipuliert. Das heißt dann, jedenfalls in Brasilien, PWS-Banking [531].

Beim Grabbing [532] geht es darum, begehrte Domainnamen zu registrieren und damit für andere zu blockieren, um dann über einen guten Preis für die Übertragung des Namens zu verhandeln. Die Rechtsprechung nennt das Erpressung und Markenverwässerung, wenn es dabei um Firmennamen und Marken geht, was heute als Cybersquatting [533] bezeichnet wird.

Um die Frage, wie sich eine Malware transportieren lässt, sind Grabenkämpfe geführt worden. Infiziert sie sich in eine Programm- oder Kommandodatei und ist ein Virus? Lässt sie sich gleichsam huckepack von einer Anwendungsdatei tragen und ist sie deshalb ein selbständiger Wurm? Oder doch eher ein Trojaner, weil sie in eine Anwendungsdatei eingebettet ist, die etwas anderes zu sein scheint?

Darin zeigt sich ein kurzsichtiger Blick auf die Erscheinungsformen und die Infiltrationstechniken und nicht auf das, worauf es ankommt: Was bezweckt die Malware und warum wird sie eingesetzt?

Sicherheitsunternehmen sprechen deshalb ganz überwiegend nur noch von Malware. Hervorzuheben ist McAfee, wo man sich immer mehr dafür interessiert, welche Menschen Malware programmieren und einsetzen.

Diese auf das Ergebnis ausgerichtete Betrachtung äußerte sich zunächst dadurch, dass der Begriff Crimeware eingeführt wurde. Darunter werden alle Programme zusammen gefasst, die ausdrücklich dazu bestimmt sind, kriminellen Zwecken zu dienen.

C.2 2. was ist Cybercrime?

Eine allgemeingültige Definition ist nicht in Sicht. Die Wikipedia verweist auf den Oberbegriff Computerkriminalität [534] und schließt sich der Polizeilichen Kriminalstatistik - PKS [535]- an. Danach werden folgende Fallgruppen im Einzelnen erfasst [536]:

⇨ Betrug mittels rechtswidrig erlangter Kreditkarten mit PIN

⇨ Computerbetrug (§ 263a StGB)

⇨ Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten

⇨ Fälschung beweiserheblicher Daten,

⇨ Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB)

⇨ Datenveränderung, Computersabotage (§§ 303a, 303b StGB)

⇨ Ausspähen [und Abfangen] von Daten (§§ 202a, 202b StGB)

⇨ Softwarepiraterie
  ⇨ private Anwendung z.B. Computerspiele, oder
  ⇨ in Form gewerbsmäßigen Handelns

⇨ Herstellen, Überlassen, Verbreiten oder Verschaffen sogenannter „Hacker-Tools“, welche darauf angelegt sind, „illegalen Zwecken zu dienen“ („Hackerparagraf“, § 202c StGB)

Es handelt sich um eine sehr formalisierte Betrachtung, mit der Fallzahlen bewältigt werden

[528] **CF**, Phishing - neue Tendenzen, 30.08.2007
[529] **CF**, Pharming, 2007
[530] **CF**, The Man in the Middle, 2007
[531] **CF**, Länderstudie. Brasilien, 27.07.2008
[532] **CF**, Grabbing, 2007
[533] **CF**, Grabbing, 2007

[534] **WP**, Computerkriminalität
[535] **WP**, Polizeiliche Kriminalstatistik (Deutschland)
[536] **CF**, Anstieg der Internetkriminalität, 23.05.2010; **BMI**, Polizeiliche Kriminalstatistik 2009, 18.05.2010; **BMI**, Polizeiliche Kriminalstatistik 2009, 29.04.2010

können. Ihre Stärke ist die Fortschreibung. Indem das jährliche Aufkommen anhand von definierten Fallgruppen mit den früheren Zahlen verglichen wird, können Entwicklungen, besonders Steigerungen und Rückgänge, ausgelotet werden. Das hilft bei der Bemessung des Erfolges gesetzgeberischer und polizeilicher Maßnahmen und Schwerpunkte.

Die Cybercrime ist jedoch eine junge und äußerst dynamische Erscheinungsform der Kriminalität, die sich dadurch der statistischen Erfassung entzieht.

Eine ebenso formalisierte Betrachtung hat der Cyberfahnder präsentiert, indem er vom IT-Strafrecht [537] im engeren [538] und weiteren Sinne spricht [539].

Diese Unterscheidung macht Sinn, wenn man Cybercrime als eine Kriminalitätsform ansieht, die sich zu ihrer Vorbereitung oder Ausführung der Informations- und Kommunikationsnetztechnik bedient. Das Bundesverfassungsgericht spricht insoweit zusammen fassend von Informationstechnischen Systemen – itS [540].

Ein itS ist eine technische Einrichtung, die digitale Informationen herstellt, verarbeitet oder übermittelt. Der Chip in der Zahlungskarte ist ebenso ein itS wie das Innenleben einer digitalen Uhr und das Internet als Ganzes.

Für die Herangehensweise des BVerfG ist diese Definition nahe liegend und nicht zu kritisieren. Es hat die Gestalt und Grenzen eines neuen Grundrechts [541] definiert und dazu auf die Allgegenwart von itS zurück gegriffen, um einen individuellen Vertrauensschutz einzuführen. Auch das BVerfG wird in den nächsten Jahren erkennen, dass gegen die kriminellen Formen des Gebrauchs und Missbrauchs von itS gleichwertige Handlungsermächtigungen der Strafverfolgung erforderlich sind. Sein Befreiungsschlag gegen eine ausufernde Onlinedurchsuchung schafft rechtsstaatliche Grundlagen, die mit Leben ausgefüllt werden müssen.

[537] **CF**, IT-Straftaten, 2007

[538] **CF**, IT-Strafrecht im engeren Sinne, 08.08.2008

[539] **CF**, IT-Strafrecht im weiteren Sinne, 08.08.2008

[540] **CF**, Informationstechnische Systeme, 05.04.2008

[541] **CF**, Gestalt und Grenzen eines neuen Grundrechts, 05.04.2008

Alle drei Varianten zur Definition entstanden, um eine Aussage zu einer spezifischen, aber jeweils anderen Frage zu treffen.

Die polizeiliche Statistik fragt nach den Entwicklungen und ist ein Instrument für die Kriminalpolitik.

Das materielle IT-Strafrecht fragt danach, welche Handlungen strafbar sind und welche nur mit den Mitteln der IT oder auch mit den Mitteln der Informationstechnik begangen werden können.

Die verfassungsrechtliche Betrachtung fragt nach dem Einfluss und die Bedeutung der IT für die Gestaltung und den Schutz persönlicher Freiheitsräume.

Die kriminalistische Frage nach den Beweggründen bleibt damit unbeantwortet.

Typenlehre nach McAfee [542]

Innovatoren	*geringe Gefahr*
ruhmgierige Amateure	*mittelmäßige Gefahr*
Nachahmer	*mittelmäßige Gefahr*
Insider	*hohe Gefahr*
organisierte Internetverbrecher	*hohe Gefahr*

C.2 3. Hacker: Moral und Unmoral

Was unterscheidet den klassischen Hacker, wie er gelegentlich noch im Chaos Computer Club - CCC [543]- auftritt, von dem Sasser-Programmierer? [544] Der klassische Hacker hat noch eine Moral, eine Vorstellung von gut und richtig. Dort begann auch der Sasser-Programmierer, als seine Malware zunächst nur andere schädliche Malware beseitigen sollte. Sein Spieltrieb und seine mangelnde Weitsicht brachten ihn aber dazu, die Folgen seine Würmer nicht mehr abzuschätzen, nicht mehr wahrzunehmen und schließlich immer mehr Böswilligkeiten in sie einzubauen.

Zusammen mit den Script-Kiddies [545], die fertige

[542] **CF**, erste Typenlehre, 27.07.2008

[543] **CF**, Wir sind die Guten! 20.01.2008

[544] **CF**, neue Herausforderungen, 2007

[545] **CF**, Länderstudie. USA, 27.07.2008

Toolkits [546] für ihre gefährlichen Spielereien einsetzen, markiert der Sasser-Programmierer die Typen "ruhmgierige Amateure" und "Nachahmer", wie sie von McAfee bezeichnet wurden [547].

Die Programmierer von Toolkits [548] sind hingegen Grenzgänger: Teilweise noch "Innovatoren" und teilweise schon Internetverbrecher, um in der Typenlehre von McAfee zu bleiben.

Klassische, innovative Hacker, die nach Sicherheitslücken suchten und ihre Erkenntnisse den Verantwortlichen berichteten, konnten für sich in Anspruch nehmen, jedenfalls insgesamt der IT-Sicherheit zu dienen.

Sie taten das gelegentlich auch öffentlich und setzen damit nicht nur die Hersteller von Hard- und Software unter Zugzwang, sondern eröffneten auch der Schar der Nachahmer ein neues Spielfeld.

Ist dieses Handeln noch "moralisch", wenn Nachahmer geradezu dazu motiviert werden, itS zu penetrieren, auszuforschen und zu sabotieren?

Die Veröffentlichung von Sicherheitslücken ist keine Anstiftung (§ 26 StGB) zum Ausspähen von Daten (§ 202a StGB) oder zur Computersabotage (§§ 303a, 303 StGB), weil es an an der Aufforderung zu einer bestimmten Straftat fehlt, kann aber eine Anleitung zu Straftaten sein, wenn damit ausnahmsweise gemeingefährliche Verbrechen ermöglicht werden (§ 130a StGB [549]).

Ein Cracker ist jemand, der Zugriffsbarrieren von Computer- und Netzwerksystemen umgeht [550]
Cracking ist die Tätigkeit, ein Computerprogramm zu analysieren, um den Kopierschutz zu entfernen [551]

Im Jargon der Hackerkultur wird gerne zwischen den "guten" Hackern und den nicht so sauberen Crackern unterschieden. Die Definitionen sind jedoch nicht einheitlich, weil sich das Cracking auf verschiedene Schwerpunkte beziehen kann.

Worin unterscheiden sich Hacker, Cracker und Exploit-Händler ? [552]

Sicherlich nicht in ihren Methoden. Sie betreiben Hacking, indem Sie Netzzugänge oder andere Sicherungstechniken aushebeln, brechen oder zu umgehen versuchen.

Damit machen sie sich auch vom Grundsatz her strafbar.

"Moral" ist kein hinreichendes Kriterium dafür, Kriminalität zu definieren [553]. Sie kann die Schuldschwere beeinflussen, nicht aber das "Ob". Wenn der Betreiber von IT Sicherheitslücken erkunden lassen will, so rechtfertigt das den Einsatz des Hackings. Will er das nicht, dann gibt es jedenfalls keine strafbefreiende Begründung dafür.

Der Exploit-Händler wird jedoch vom Streben nach Gewinn getrieben. Darin unterscheidet er sich tatsächlich vom Hacker und vom Cracker. Das macht ihn auch zu einer neuen Form von Kriminellen.

C.2 4. Einzeltäter

Kein Einzeltäter handelt ohne gesellschaftlichem Hintergrund und ohne Einbindung in eine Bezugsgruppe. Man sucht sich, findet sich, unterstützt sich, streitet und kämpft miteinander. Die Experten für Exploits, Toolkits und Malware dürften überwiegend späte Nachfahren der Kosmos-Experimentierkasten-Generation sein, mit der ich aufgewachsen bin. Sie sind keineswegs asozial, sondern durchaus kommunikativ. Man hört aufein-

[546] **CF**, Trojaner für Dummies, 03.01.2008
[547] **CF**, erste Typenlehre, 27.07.2008
[548] **CF**, Trojanerbaukasten mit Support, 20.06.2008
[549] **CF**, strafbare Bombenbau-Anleitungen im Internet, 2007
[550] **WP**, Cracker (Computersicherheit)
[551] **WP**, Crack (Software);
Eine bemühte **WP**, Abgrenzung zum Begriff ‚Cracker'
[552] Der Exploit-Händler verkauft die von ihm entdeckten oder gekauften Sicherheitslücken:
WP, Exploit-Händler. 13.07.2008
[553] Die Rechtsoziologie unterscheidet zwischen der individuellen Moral als Handlungsprinzip, der gruppenbezogenen Sitte und dem staatlichen Recht. Starke Sitten können das Recht im Einzelfall beeinflussen, wenn es im Widerspruch zu ihm steht. Das ist aber kein Freibrief zum rechtswidrigen Handeln.
CF, neue Knäste braucht das Land, 27.122007

ander und lernt voneinander. Echte Zusammenarbeit kennen sie nur mit höchst vertrauten Kumpeln. Arbeitsteilung, Prozessplanung und -überwachung sind ihnen nicht unbekannt, aber fremd.

Sie achten es, wenn Andere diese Fertigkeiten haben, und nutzen sie, wenn sie sie brauchen. Ihr Ding machen sie aber lieber alleine.

Das ist keine Analyse, sondern eher eine subjektive Einschätzung.

Ich glaube tatsächlich, dass Bolduans [554] Darstellung zutrifft, dass die IT-Handwerker im Bereich der Cybercrime eher Einzeltäter sind. Man unterwirft sich einem Auftraggeber für ein Projekt, arbeitet rund um die Uhr und liefert irgendwann ein gutes, vielleicht auch geniales Ergebnis ab.

Bertold Brecht hat gesagt: *Erst kommt das Fressen und dann die Moral*.

Was ist, wenn man nicht mehr zuhause bei den Eltern wohnt, nicht mehr Vaters Flatrate benutzen kann und Hotel Mama den Dienst verweigert?

Dann muss man Geld verdienen mit dem, was man am besten kann.

Zusammenarbeit, Diskussion und Kommunikation sind alltägliche soziale Prozesse. Gefährlich werden sie, wenn eine In-Group-Sitte entsteht mit abweichenden Sitten- und Rechtsvorstellungen, die ganz schnell zu einer Wagenburg-Identität werden können, die alles Äußere als falsch und bekämpfenswert ansehen.

In-Group-Prozesse sind gut und richtig, wenn sie eine Identität und das Rückgrat der Mitglieder fördern. Sie sind falsch und "sektisch", wenn sie sich zur Außenwelt abgrenzen und keine vernünftige Kommunikation mit ihr mehr zulassen und sie zur Feindwelt wird.

Die virtuelle Welt befriedigt aber keine realen Bedürfnisse.

Wohnen, Essen, Trinken, Internet, Sex und die Katze, die um die Beine streicht, verlangen nach Geld.

Individualisten bekommen es von Kontaktpersonen, die die Aufträge erteilen, die Ergebnisse abholen und das Geld bringen. Damit sind wir in dem klassischen Bild von den Geld- und Ausweisfälschern.

Gute Individualisten in diesem Sinne müssen sich auf ihre Fertigkeiten konzentrieren und brauchen um sich herum Vermarkter, Buchhalter für das Inkasso und eine Firma, die sie vom Alltagsgeschäft entlasten.

Damit ist die mittelständische organisierte Cybercrime geboren.

Ihre Vertreter verdienen die Strafverfolgung. Das ist aber nur Marktbereinigung, weil neue Anbieter sofort wieder nachwachsen werden.

Richtig gefährlich sind ihre Auftraggeber.

C.2 5. Malware-Schreiber, Zulieferer und Auftraggeber

An den Anfang der "Produktionskette" stellt Balduan [555] die Malware-Schreiber, die zwei Zulieferungen benötigen: Vom Exploit-Händler erhalten sie die Beschreibung einer Sicherheitslücke, auf der sie die Malware aufsetzen können, und vom Toolkit-Schreiber erhalten sie die aktuellen Instrumente zum Tarnen der Malware.

Bevor jedoch die geeigneten Werkzeuge ausgewählt und beschafft werden können, bedarf es eines Auftraggebers und dessen Vorstellungen über die Funktionsweise der Malware.

Als Auftraggeber kommen vor Allem Botnetzbetreiber, Botnetznutzer, Phisher und Informationshändler in Betracht. Sie haben sehr unterschiedliche Bedürfnisse.

Botnetzbetreiber haben ein besonderes Interesse an der Pflege, dem Erhalt und der Erweiterung des ▸ Botnetzes. Bei der Pflege und dem Erhalt geht es darum, die Zombierechner und ihre Steuerungssoftware mit den neuesten Methoden zur Tarnung und zur Steuerung auszustatten. Wegen der Tarnung kommen die Toolkit-Schreiber mit ins Boot, die sich auf dem Markt der Antivirensoftware auskennen und immer neue Methoden entwickeln, wie man die installierte Malware vor

[554] **CF**, Botnetz-Software und -Betreiber, 13.07.2008

[555] Ebenda

der Enttarnung bewahren kann. Um die Funktionstüchtigkeit zu erhalten, sind Kenntnisse im Zusammenhang mit Peer-to-Peer-Netzen und der Fernwartung erforderlich. Insoweit ist eine Zusammenarbeit mit den Fachleuten der Botnetzbetreiber nötig oder mit freien Fachleuten, deren Wissen eingekauft werden muss.

Der Einsatz der neuesten Tarnungen ist auch für die Erweiterung des Botnetzes von Bedeutung. Hierbei kommt es jedoch besonders darauf an, neue Zombies zu gewinnen, also auf die Verteilung der Malware (Methoden), Infiltration und Übernahme von PCs.

Die Palette der Anforderungen an eine Bot-Software lässt es kaum erwarten, dass nur ein einzelner Malware-Schreiber zum Einsatz kommt. Im Gegensatz zu "normaler" Malware soll der Zombie möglichst lange erhalten bleiben, so dass die Steuerung und die Beeinträchtigung behutsam sein sollen [556].

Die Malware muss deshalb beherrschen:

⇨ Infiltration und Übernahme

⇨ modularer Aufbau und Update

⇨ Tarnung

⇨ Steuerungsfunktionen, Betriebsüberwachung

⇨ Einsatzsteuerung

Diese Vielfalt bedarf eines Projektmanagements und der Leitung durch einen Koordinator.

Die Anforderungen der Auftraggeber im Übrigen sind vielleicht nicht ganz so umfassend, aber auch nicht unbedeutend. Phisher benötigen eine präzise Steuerung zum Missbrauch des Homebankings und Industriespione eine präzise Funktion zur Ausforschung des Zielrechners.

Erst wenn die Aufgabe mit ihren besonderen Anforderungen bekannt ist, kann der Malware-Schreiber die geeigneten Exploits und Toolkits auswählen und seine Software zusammenstellen.

Maßgeblich für die weitere Auftragsabwicklung ist die Bezahlung. Insoweit kommen vor Allem Bargeld und Bezahlsysteme auf der Grundlage von Edelmetallen in Betracht [557]. Wegen der Barzahlung ist eine "unechte" Hawala denkbar, bei der Boten die Geldübergabe besorgen. Der Einsatz von Operation Groups, von dem Balduan berichtet, lässt das nahe liegend erscheinen.

C.2 6. spezialisierte Zwischenhändler

Die Funktionsvielfalt der Malware lässt Zweifel an der Einzeltäterannahme aufkommen. Warum sollte sich ein begnadeter Malware-Schreiber eine kleine Firma schaffen, die sich um seine Vermarktung kümmert? Warum sollte er Marktforschung betreiben, um sich die geeigneten Exploits und Toolkits zu beschaffen? Unter marktwirtschaftlichen Gesichtspunkten liegt es viel näher, anzunehmen, dass sich für jede dieser Aufgaben spezialisierte Zwischenhändler herausbilden, die ihre eigenen Zulieferer für Exploits, Toolkits und andere Spezialformen von Software haben.

Ein Blick auf das Skimming [558] macht die Sinnhaftigkeit des Einsatzes von Spezialistengruppen mit unterschiedlichen Qualifikationen besonders deutlich:

⇨ echte Handwerker bauen Skimmer, Überwachungskameras, Vorsatzgeräte und Steuerungsprogramme

⇨ Installateure bauen die Überwachungstechnik in eine Bankfiliale ein und bauen sie später auch wieder ab

⇨ Fälscher stellen die Dubletten von Zahlungskarten her

⇨ Läufer setzen die Dubletten an Geldautomaten ein

⇨ andere Agenten transportieren die Dubletten und die Beute

Die Installateure brauchen Geschick, die Fälscher Zeit und die richtige Ausstattung und die Läufer einfach nur Dreistigkeit. Gute Handwerker entstehen nicht dadurch, dass sie 'mal eine Überwachungskamera bauen und mit einem Sender ausstatten. Sie brauchen Übung und Erfahrung, die

[556] **CF**, Anatomie des Sturm-Wurms, 06.03.2008

[557] Beispiele dafür sind **CF**, E-Gold (2007) und **CF**, WebMoney, 13.07.2008.

[558] **CF**, arbeitsteiliges Skimming, 18.05.2008

sie nur bekommen, wenn sie ihre Geräte immer wieder und für verschiedene "Projekte" anbieten.

Auch beim Phishing werden besondere Kenntnisse benötigt, wenn es darum geht, "gute" Webseiten oder E-Mails herzustellen, unauffällige Texte und gute Übersetzungen [559].

Das, was ich Zwischenhändler nenne, bezeichnet Balduan als Operation Groups [560]. Sie haben ihre Kontakte und Leute, auf die sie bei jedem Auftrag zurück greifen können. Sie und besonders ihre leitenden Unternehmer erleichtern das Geschäft für alle Beteiligten. Die Spezialisten müssen sich nicht um ihre Vermarktung kümmern und die Auftraggeber nicht darum, den richtigen Spezialisten oder Zulieferer zu finden.

Durch den Einsatz von Zwischenhändlern bekommt die Cybercrime eine neue Gestalt. Sie organisiert sich dadurch arbeitsteilig und marktmäßig - um Straftaten zu ermöglichen und durchzuführen.

C.2 7. kriminelle Unternehmer

Organisierte Internetverbrecher im Sinne der Typenlehre von McAfee [561] sind die Unternehmer, also die Botnetzbetreiber und die Rogue-Provider, sowie die "Projektleiter", also Koordinatoren.

Botnetzbetreiber bieten unter Marktgesichtspunkten eine auf Dauer angelegte Dienstleistung. Ihr Produktionsmittel ist das Botnetz, das sie eingerichtet haben und pflegen, und ihre Dienstleistung der Gebrauch des Botnetzes.

Ein Botnetz lässt sich vielfältig einsetzen, zum Beispiel zum Versand von Spams. Diese Dienstleistung werden die Betreiber selber durchführen und sich dazu die zu verbreitende Nachricht übermitteln lassen. Die Zieladressen werden entweder vom Kunden geliefert, die Versender greifen auf ihre eigenen Bestände zurück oder kaufen Adressenlisten gezielt ein [562]. Das dürfte Verhandlungssache sein und letztlich eine Frage des Preises.

Es ist kaum vorstellbar, dass die Botnetzbetreiber Erpressungen im Zusammenhang mit verteilten Angriffen, Phishing-Kampagnen und die Kontrolle von Malware in eigener Regie durchführen, weil dazu jeweils spezielles Wissen und besondere Maßnahmen zur Beutesicherung nötig sind.

Sie werden sich deshalb darauf beschränken, ihr Werkzeug projektbezogen einzusetzen oder zeitweilig zu vermieten [563].

Während die Botnetz-Betreiber im Verborgenen bleiben, sind die Schurken-Provider (Rogue-Provider) ganz offiziell in die technischen Strukturen des Internets eingebunden. Ihr bekanntester Vertreter ist das Russian Business Network - RBN.

Das Geschäftsmodell der Rogue Provider unterscheidet sich nur etwas von den sonstigen Zugangs- und Hostprovidern, weil sie ihre Kunden nachhaltig von der neugierigen Öffentlichkeit abschotten. Das RBN verwendet Scheinfirmen für DNS-Eintragungen, liefert sichere Speicherorte [564] für Malware, Pharmen, "geheime" Webauftritte und ausgekundschaftete Kontozugangsdaten, geschlossene Benutzergruppen und damit einen Handelsplatz für alles, was als illegale Inhalte und Kommunikationen im Internet möglich ist.

Das Geschäftsmodell ist einfach: Je mehr Anfragen von Geschädigten, Neugierigen und Strafverfolgern abgewimmelt werden müssen, desto teurer wird der Dienst.

Das funktioniert nur solange keine effektive Rechts- und Strafverfolgung gegen den Rogue-Provider erfolgt. Befürchtet er Schadenersatz oder sogar Strafe, dann strukturiert er sich um, wie das RBN gezeigt hat: RBN lebt [565].

---

559 **CF**, Malware lernt die deutsche Sprache, 27.07.2008

560 **CF**, Operation Groups, 13.07.2008

561 **CF**, Hacker: Moral und Unmoral, 07.08.2008

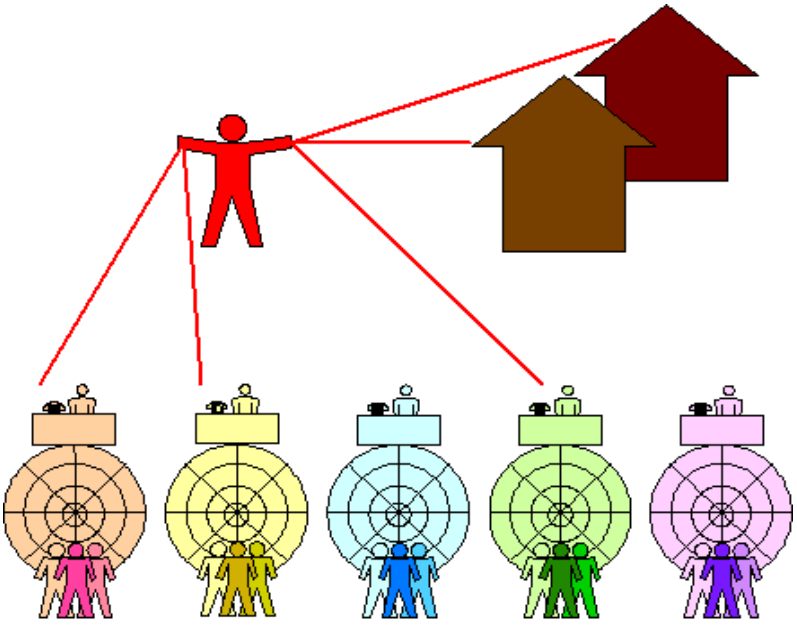
562 Siehe: **CF**, Zusammenarbeit der Szenen, 2007; **CF**, Spam-Discounter, 13.10.2007; **CF**, geklaute Daten zum Schnäppchenpreis, 09.04.2008; **CF**, qualitätskontrollierter Kontomissbrauch, 09.05.2008; **CF**, neue Herausforderungen, 2007; **CF**, Forderung nach Übertragungsgebühren, 08.12.2007.

563 Frank Faber, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008; **CF**, Russian Business Network – RBN, 13.07.2008.

564 **CF**, Drop Zones, 13.07.2008

565 **CF**, RBN lebt, 13.07.2008

C.2 8. Koordinatoren



Von den kriminellen Unternehmen, die darauf ausgelegt sind, dauerhaft zu handeln und sich sozusagen zu etablieren, unterscheiden sich die Koordinatoren [566]. Sie planen kriminelle Einzelaktionen, kaufen die dazu nötige Infrastruktur (Botnetz, Drop Zone), das Fachwissen und die nötigen Leute ein. Sie sind sozusagen die Projektmanager der Cybercrime.

Es gibt Gerüchte, dass die Koordinatoren häufig aus dem Kreis des früheren KGB stammen.

Auch die Koordinatoren werden sich auf bestimmte "Projekte" spezialisieren und durch sie Erfahrungen sammeln. So bauen sie Erfahrungswissen über Zwischenhändler und die Qualität ihrer Dienste auf, das ihnen bei jedem neuen "Projekt" zugute kommt.

Ob sie alleine handeln, ist unklar. Wahrscheinlich werden sie sich nach und nach einen kleinen Stab aufbauen, der bei der Abwicklung der Projekte hilft.

Im Übrigen bleiben sie im Verborgenen - wie die Spezialisten und Zwischenhändler auch.

Über die Auftraggeber ist ebenfalls nichts bekannt. Komplexe Projekte werden aber ohne eine Vorschussfinanzierung nicht durchführbar sein.

C.2 9. Zwischenergebnis

Die organisierte Cybercrime wird von Unternehmern ausgeführt, die die dauerhaft benötigten Werkzeuge wie Botnetze und Drop Zones zur Verfügung stellen. Soweit sie in der Öffentlichkeit agieren wie die Rogue-Provider, ist es ihr Bestreben, ihre zahlenden Kunden von der neugierigen Öffentlichkeit abzuschotten.

Für die kriminellen Projekte sind in aller Regel Koordinatoren zuständig, die die nötigen Geräte, Programme und das Spezialistenwissen einkaufen und zusammen führen. Dabei rekrutieren sie wahrscheinlich ganz überwiegend keine einzelnen Zulieferer und Programmierer, sondern bevorzugt Zwischenhändler, die ihrerseits über einen Stamm von Zulieferern, Experten oder "Laufburschen" verfügen.

Große Cybercrime-Projekte haben eine Komplexität erreicht, dass sie von Einzeltätern nicht mehr bewältigt werden können. Sie werden vereinzelt auftreten als Hacker (Exploits, Adressdaten) und Programmierer (Toolkits, Malware) und ihre Dienste werden sie wahrscheinlich immer häufiger über Zwischenhändler verkaufen, die für bestimmte Segmente des kriminellen Marktes spezialisiert sind.

C.2 10. Organigramm der Cybercrime

Die bereits an anderer Stelle aufgenommenen Hinweise [567], die hier zusammen gefasst und angereichert wurden, lassen eine arbeitsteilige Struktur erkennen, in der vor Allem kriminelle Unternehmen (Botnetzbetreiber und Rogue-Provider), Zwischenhändler (Operation Groups) und Koordinatoren für einzelne kriminelle Projekte handeln (siehe Grafik oben).

In diesem Modell spielen die Handwerker, Spezialisten und Laufburschen (Finanzagenten beim Phishing, Geldabheber und Installateure beim Skimming) zwar die Basis der kriminellen Handlungen. Ihr Einsatz und die Zusammenführung ihrer Arbeitsergebnisse wird in diesem Modell je-

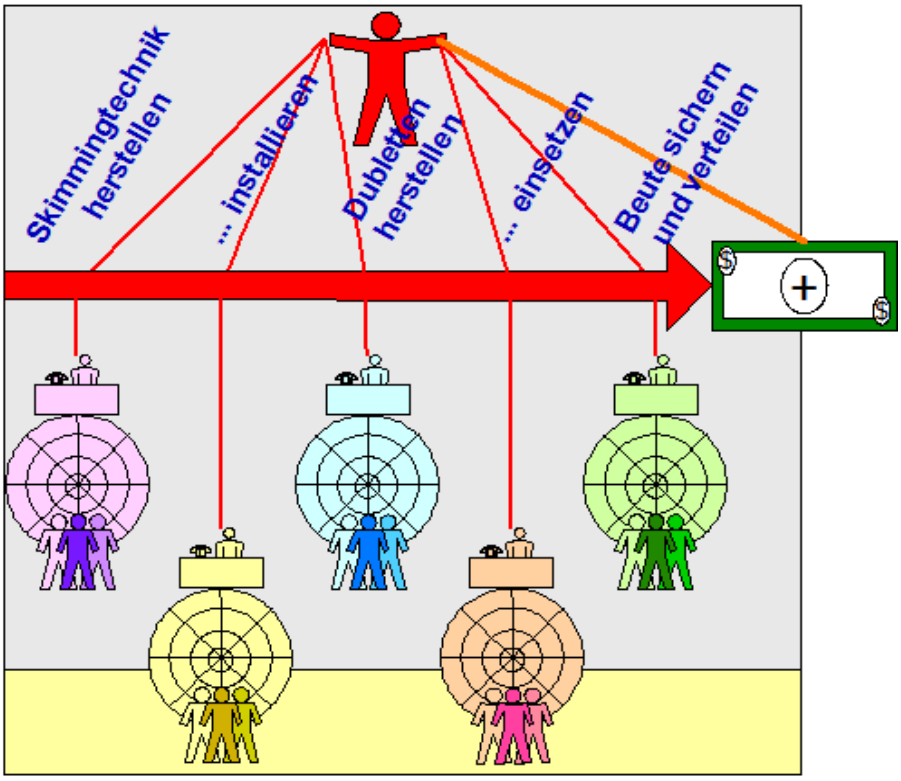
[566] **CF**, Koordinator, 13.07.2008

[567] **CF**, Schurkenprovider und organisierte Cybercrime, 13.07.2008

doch von den Zwischenhändlern und den Koordinatoren organisiert.

Außerhalb des Organigramms bleibt viel Raum für die "einfache" Cybercrime. Zu ihr gehören die Script-Kiddies mit ihren zusammen gebastelten Trojanern, die keinen nennenswerten Schaden anrichten, die Lügner bei Onlineauktionen, die Nutzer von Raubkopien und viele andere Massenerscheinungen. Sie bilden das kriminelle Massengeschäft, das von der Strafverfolgung abgearbeitet werden kann und das Moden unterworfen ist.

Eine neue Qualität ist jedoch wegen der arbeitsteiligen und teilweise bereits organisierten Cybercrime entstanden, die das Organigramm abbildet.



C.2 11. neue Definition der Cybercrime

Für die ***arbeitsteilige Cybercrime*** bietet sich deshalb folgende Definition an:

⇨ *Die arbeitsteilige Cybercrime ist 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* (wie Botnetze und Rogue-Provider) *und Gruppen mit Spezialisten* (Operation Groups) *zurück, deren Dienste und Handlungen sie zur Erreichung des kriminellen Zieles zusammenführen.*

Einzelne Zwischenhändler, die Botnetzbetreiber und die Rogue-Provider dürften für sich bereits die Bedingungen für eine ***organisierte Cybercrime*** erfüllen:

⇨ *Organisierte Cybercrime ist die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von IT-Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig*

a. unter Verwendung gewerblicher oder geschäftsähnlicher Strukturen,

b. unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder

c. unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.

C.2 12. modulare Cybercrime

Der IT-typische Blick auf die Erscheinungsformen der Cybercrime stellt die öffentlich handelnden Akteure in den Vordergrund.

Am Beispiel des Skimmings sind das aber nur die wegen ihrer Dreistigkeit qualifizierten Installateure und die Läufer, die schließlich die Dubletten missbrauchen. Die wirklichen Spezialisten für die Zusammenstellung der Skimmingtechnik, die Fälscher und die Beutesicherer bleiben dabei aus dem Blick.

Das arbeitsteilige Skimming ist hingegen zielorientiert. Die Methoden zur Datengewinnung sind ihm völlig gleichgültig. Ihm kommt es auf die Beute an. Die Module, die für die Zielerreichung eingesetzt werden, sind austauschbar. Sowohl die Handwerker wie auch die Installateure können eingespart (und damit die Namensgeber für diese

Form der Cybercrime), wenn die Zahlungskartendaten auf andere Weise beschafft werden können, oder outgesourced werden, um dann nur mit den Arbeitsergebnissen weiterzuarbeiten.

Andere Formen der Cybercrime ließen sich ganz ähnlich darstellen.

Phishing: Es ist egal, wie die Kontozugangsdaten beschafft werden, ob durch ein E-Mail-Formular, einer Webseite, POS-Skimming oder einer Keylogger-Malware. Das Ergebnis zählt. Die in irgendeiner Form ausgespähten Daten sollen missbraucht und die Beute gesichert werden. Der Weg dahin ist eine Zusammenstellung von Modulen, die eine Weile funktionieren und dann wieder ausgetauscht werden müssen.

So betrachtet müssen die Namen für die besonderen Formen der Cybercrime neu bedacht werden, weil sie sich bislang an dem Beschaffungs- und nicht an dem Verwertungsprozess orientieren:

⇨ nicht Skimming, sondern Zahlungskartenmissbrauch,

⇨ nicht Phishing, sondern Homebankingmissbrauch,

⇨ nicht Botnetze, sondern Missbrauch von PC-Clustern.

C.2 13. Fazit

Die Cybercrime ist IT-Kriminalität. Es handelt sich um Straftaten unter Einsatz der Informationstechnik und des Internets.

Ihre allgemeinen Formen zeigen sich in Massenerscheinungen wie Betrügereien in Auslobungsplattformen, z.B. bei eBay, oder die Verbreitung und Nutzung urheberrechtlich geschützter Werke. Besondere Ausprägungen sind die Verbreitung rechtswidriger Inhalte (Kinderpornos, Beleidigungen, Boykottaufrufe, Bombenbauanleitungen), das Amateur-Hacking (Nachahmer) und der Identitätsdiebstahl, um Andere zu schädigen oder in Misskredit zu bringen.

Ihre Gefährlichkeit soll nicht kleingeredet werden, weil sie im Einzelfall furchtbare Schicksale hervorrufen oder vertiefen (z.B. Kinderpornographie).

Als Ausprägungen schwerer und organisierter Kriminalität zeigen sich hingegen die Erscheinungsformen der Botnetze, des Phishings und des Skimmings.

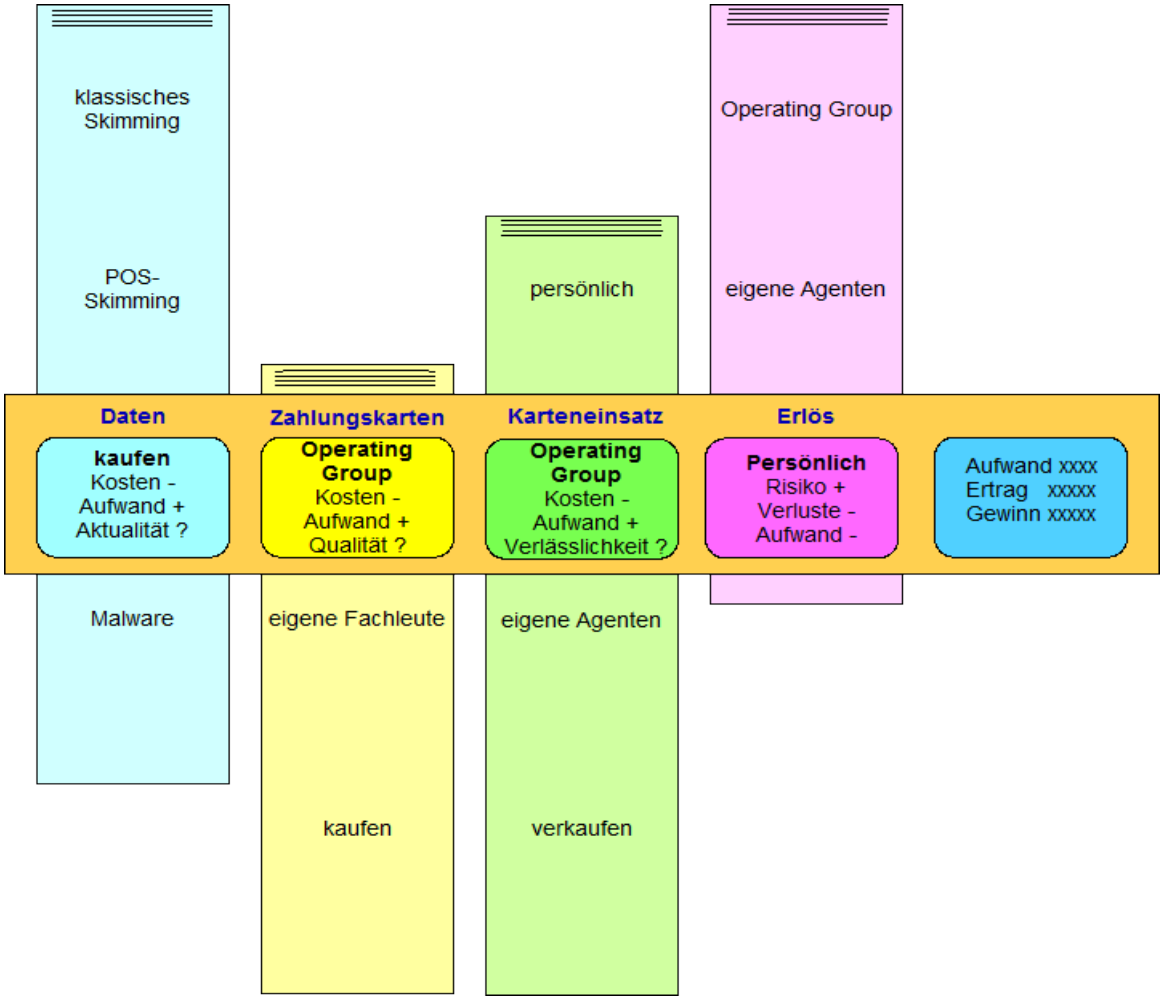
Diese Kriminalitätsformen sind zielorientiert und verfolgen den Zweck, kriminelle Gewinne zu verwirklichen. Dabei orientieren sie sich auf den Missbrauch bestimmter Formen der Technik wie Zahlungskarten, das Homebanking oder von PC-Clustern. Die dabei eingesetzten Methoden des Missbrauchs sind gleichgültig. Sie sind modular und werden zweckverfolgend ausgewechselt oder modifiziert.

Entstanden ist deshalb eine arbeitsteilige Cybercrime-Szene, die sich wegen einzelner Erscheinungsformen als Organisierte Kriminalität darstellt.

In dieser Struktur haben Einzeltäter noch eine vereinzelte Bedeutung, wenn sie mehr oder weniger unersetzbare Spezialisten sind.

Ansonsten sind sie austauschbar. Vor Allem die mehr dreisten als kenntnisreichen Läufer, die notgedrungen in der Öffentlichkeit auftreten müssen, sind ersetzbar und können jederzeit geopfert werden. Sie sind die Finanzagenten beim Missbrauch des Onlinebankings und die Installateure und die Läufer bei Einsatz gefälschter Zahlungskarten.

Ihre Handlungen sind zwar namensgebend für die betreffende kriminelle Erscheinungsform gewesen, für die Zielerreichung sind die öffentlich handelnden Personen aber nur funktional bedeutsam und ansonsten austauschbar.



C.2 14. modulare Kriminalität

Das Bild von der ▸ modularen Cybercrime lässt sich auf jede Form der Kriminalität übertragen [568]. Die modulare Kriminalität ist geprägt von der Technik des Projektmanagements, zielt auf eine effektive Gewinnerzielung und hat als wesentliche die Parameter Aufwand und Gewinn sowie, nur darin unterscheidet sie sich von üblichen Projekten, dem Entdeckungsrisiko. Das versinnbildlicht am Beispiel des Skimmings die Grafik oben. Ich nenne sie die „Messlatte des Koordinators“ [569].

Der eine oder andere Koordinator mag besondere Erfahrungen, Kontakte und Quellen für ein einzelnes Kriminalitätsfeld haben und deshalb besonders gut darin sein. Kennzeichnend für die modulare Kriminalität ist jedoch, dass sie wegen der kriminellen Methode und wegen der Erreichung der Meilensteine völlig offen ist. Ihre Maßgabe ist der erwartete Gewinn.

Das liegt vor allem daran, dass die modulare Kriminalität vorfinanziert werden muss. Sie verzichtet auf einen Mitarbeiterstamm, wenn es im Ergebnis schneller und besser: billiger ist, Daten, Werkzeuge und Dienste von spezialisierten Fachleuten einzukaufen.

Das führt zu einer Schattenökonomie mit kriminellen Halbfertigprodukten.

Kein "ordentlicher" Handwerker, der gute Fassaden für das Skimming bauen kann, setzt sich ohne Not dem Stress aus, diese auch für das Ausspähen von Zahlungskartendaten zu installieren und wieder abzubauen.

Die modulare Kriminalität ist eine logische Fortsetzung der Arbeitsteilung zwischen Dieb und Hehler, nur dass die Arbeitsteilung noch weiter segmentiert ist.

Möglich ist das nur, wenn es die Mittelsleute und spezialisierte Subunternehmer gibt, die über Sze-

[568] **CF**, modulare Kriminalität, 05.10.2008

[569] **CF**, Kriminalität aus dem Baukasten, 21.09.2008

nekenntnisse, Kontakte und mehr oder weniger locker angebundene Mitarbeiter verfügen. Sie und ihre Zuarbeiter bilden die Operating Groups, von denen erstmals Bolduan spricht. Sie liefern die kriminellen Halbfertigprodukte in Form von Geräten, Daten oder Diensten, also zum Beispiel für die Installation von Skimming-Hardware, für den Missbrauch von gefälschten Zahlungskarten, für den diskreten Transport oder Versand von Geld oder anderen Werten und so weiter.

Der Koordinator ist zunächst ein Kalkulator. Seine Entscheidungsparameter sind, wie gesagt, wirtschaftlicher Art und betreffen Aufwand, Profit und Entdeckungsrisiko. Nur der dritte Eckpunkt ist von der Kriminalität geprägt.

C.3 Basar für tatgeneigte Täter

Wie organisieren sich arbeitsteilige Täter in der Underground Economy?

Die Cybercrime verfügt mit dem Internet über eigene Mechanismen der Kommunikation und des Austausches ihrer kriminellen Dienstleistungen. Das gängige Bild geht von einer diffusen, chaotisch anmutenden Vielzahl von Einzelpersonen aus, die sich sporadisch binden und ihre Werkzeuge und Kenntnisse gegen andere Werte tauschen. Ich nenne sie die Crämer. Ihre Schattenwelt wird üblicherweise als die Underground Economy bezeichnet.

Die Crämer sind die kleinen Kriminellen, die ihren Lebensunterhalt auf den Basaren in der Underground Economy verdienen.

Im Hintergrund agieren die Organisierten Internetkriminellen, die richtige Beute machen.

Die Arbeitsweisen der Cybercrime und der "normalen" Kriminalität vermischen sich dabei allmählich. Während die herkömmlichen Täter das Internet immer mehr als ihre anonym erscheinende Kommunikationsplattform nutzen, professionalisieren sich Teile der Cyber-Kriminellen und übernehmen dazu auch die Strukturen und Methoden, die das Verbrechen im Übrigen kennt.

C.3 1. Hacker-Märkte

Die Kommunikation und die kriminellen Geschäfte erfolgen bevorzugt in geschlossenen Boards (Foren). Die dort ablaufenden Prozesse werden vor allem von Ester und Benzmüller beschrieben [570].

C.3 1.1 Ende eines Hackerboards

Im November 2009 zerschlugen die Staatsanwaltschaft Bonn und das Bundeskriminalamt eine Tätergruppe, die nicht nur ein Forum für jederlei kriminelle Leistungen betrieb, sondern auch ein Botnetz, mit dem Kritiker und Konkurrenten angegriffen wurden [571].

Die etwa 18.000 Teilnehmer im Elite-Forum boten u.a. *Kreditkarten- und Kontodaten, illegal beschaffte Passwörter oder selbst programmierte schädliche Software wie Trojaner* zum Tausch und Kauf an [572]. Sie verdienen ihren Lebensunterhalt in der Underground Economy [573], ohne dass die meisten von ihnen dadurch reich geworden wären.

Das Beispiel passt zu den schon älteren Erfahrungen, über die Jäger 2006 berichtet hat [574]. Er fand Preislisten für Botnetze, Malware, Schwachstellen (Exploits) und Rootkits (Tarnmechanismen gegen Virenscanner) [575], also für alles, was man zum Herstellen von Malware braucht. Im einzelnen beschreibt schon Jäger den Basar für tatgeneigte Einzeltäter [576].

Die Spuren, über die 2008 zum Beispiel Muttig berichtet hat, führten nach Russland [577]. Den Anreiz dafür, sich kriminell zu betätigen, sieht Muttig darin, dass Russland einerseits über Leute mit hervorragendem Wissen verfügt, die andererseits kaum legale Erwerbsmöglichkeiten haben [578].

Balduan hat - ebenfalls 2008 - die Underground Economy als allgemeine Erscheinung angesehen, in deren Zentrum die Betreiber von Botnetzen stehen [579].

---

570 Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009;
dieselben, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

571 **CF**, D-AU-Netz zerschlagen, 25.11.2009;
BKA geht mit Großrazzia gegen Botnetz-Betreiber vor, Heise online 25.11.2009

572 Razzia bei Internetforum "Elite Crew", Hamburger Abendblatt 28.11.2009

573 **CF**, Schattenwirtschaft im Internet, 24.11.2008;
CF, Schwarzmarkt, 19.12.2008

574 Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006

575 **CF**, geklaute Daten zum Schnäppchenpreis, 09.04.2008; **CF**, Trojanerbaukasten mit Support, 20.06.2008; **CF**, qualitätskontrollierter Kontomissbrauch, 09.05.2008.

576 **CF**, professionelle Einzeltäter, 05.10.2008

577 **CF**, Cybercrime in Russland, 13.07.2008;
Igor **Muttik**, Die Wirtschaft und nicht die Mafia treibt Malware voran, McAfee 12.02.2008

578 **CF**, Fachleute und geringe Löhne, 05.10.2008

579 **CF**, Zusammenarbeit von Spezialisten, 13.07.2008; Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.; kostenpflichtiger Download.

Er hat recht behalten. Nicht nur damit, dass sich die Botnetze zu den mächtigsten kriminellen Werkzeugen entwickelt haben [580], sondern auch damit, dass die Cybercrime zu einem knallharten Geschäft geworden ist, in dem professionelle Täter richtig Geld verdienen, nicht zu ihrem Spaß handeln und schon gar nicht aus hehren moralischen Beweggründen.

Die Crämer, die illegale Inhalte, einzelne ausgespähte Kontodaten und Programme zum Kauf anbieten, sind in aller Regel die mittelmäßig gefährlichen Amateure und Nachahmer, von denen McAfee bereits 2006 gesprochen hat (siehe unten). Sie agieren unter ihren szenetypischen Pseudonymen auf Black Markets, also auf Kommunikationsplattformen (Boards) mit einer Offenheit und Unbekümmertheit, die jeden Rest von schlechtem Gewissen vermissen lässt. Sie wähnen sich sicher und die Erfahrungen sprechen für sie.

Die Crämer bilden aber nur die sichtbare Oberfläche, den Basar. Die geschützte Umgebung für den Basar stellen Schurkenprovider und professionelle Kriminelle zur Verfügung, die weitaus gefährlicher sind.

C.3 1.2 verstärkte Abschottung

Im Anschluss an ihren bemerkenswerten Bericht über die Schattenwirtschaft im Internet vom August 2009 [581] haben Ester und Benzmüller die Basare weiter beobachtet und jetzt ihr "Update 04/2010" veröffentlicht [582].

Nachdem das Elite-Forum zerschlagen worden ist (auch: „1337 Crew“), haben sich neue Boards gebildet, um dessen Nachfolge anzutreten. Die Crämer setzen ihre Geschäfte unvermittelt fort. Eine aktuelle Preisliste belegt, dass gehackte Spiele-Accounts für 5 bis 18 €, SIM-Karten im Bundle für 1 € das Stück und PayPal-Konten für wenig Geld (20 € bei einem Guthaben von 1.290,71 €) zu haben sind. Am teuersten sind gehackte Packstationen [583] für den Warenbetrug, die bis zu 50 Euro kosten [584]. Bedruckte Kreditkartenrohlinge mit Hologrammen kosten zwischen 45 und 150 US-$, Kartendrucker von 450 bis 3.500 US-$ und ganze Skimming-Sets bis zu 10.000 US-$ [585].

Um die Nachfolge des Elite-Forums wurden erbitterte Kämpfe geführt. Die Konkurrenten schossen sich teilweise gegenseitig ab [586].

Um sich besser gegen die Strafverfolgung und Betrüger in den eigenen Reihen (Scammer [587]) zu schützen, wurden Aufnahmegebühren oder Referenzen gefordert [588]. In einzelnen Fällen wurden auch keine neuen Mitglieder mehr aufgenommen [589].

Die Autoren beschreiben interessante Einzelheiten über die Geschäftspraktiken eines Boards [590]. Neben der Aufnahmegebühr für jedes Mitglied (zum Beispiel 10 € per PaySafeCard) konnten sie bislang zwei verschiedene Arten von Verkaufslizenzen im Board erwerben:

⇨ **Monopollizenz** (Patent); berechtigt zum exklusiven Verkauf einer Warengruppe (zum Beispiel gehackte Kreditkarten) und kostete mehrere Hundert Euro.

⇨ **Shop-Lizenz**; berechtigt zum Verkauf beliebiger Leistungen mit Ausnahme der Monopol-Dienste und war günstiger zu bekommen.

Mittlerweile gibt es nur noch normale Händlerlizenzen. Die so genannten Verkaufspatente wurden abgeschafft. Nun muss jeder Verkäufer einen Betrag zahlen, um die Verkaufsberechtigung zu erhalten. Das Prinzip spült Geld in die Board-Kasse und soll vor internen Scammern, Betrü-

---

580 Sturmwurm-Botnetz sperrangelweit offen, Heise online 09.01.2008;
CF, einfach abschalten, 11.01.2009.

581 Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009

582 Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

583 **CF**, Carding, 22.11.2008

584 Ester/Benzmüller 2010, S. 4; Grafik bei G Data.

585 Ester/Benzmüller 2010, S. 5; Grafik bei G Data.

586 **CF**, Hacker cracken Carder-Forum, 23.05.2010; Hacker cracken Carder-Forum, Heise online 19.05.2010

587 **CF**, der Basar, 11.04.2010

588 Ester/Benzmüller 2010, S. 9.

589 Ester/Benzmüller 2010, S. 8.

590 Ester/Benzmüller 2010, S. 8.

gern, schützen. [591]

Es seien neue Webshops entstanden, schreiben die Autoren, und einige "etablierte" seien weiterhin tätig. Ihre Betreiber könnten die Betreiber der Boards selber oder jedenfalls in deren Umfeld angesiedelt sein [592].

Am Fall des „1337 Crew“ Forums haben viele Mitglieder im Untergrund erkannt, dass sie nicht so sicher sind, wie es wohl viele von ihnen gedacht hatten. Viele Onlinekriminelle haben sich auch aus dem Untergrund-Tagesgeschäft zurück gezogen, vielleicht nur temporär, um nicht „mit laufendem Rechner“ von der Polizei erwischt zu werden. [593]

> *Die Grenze zwischen Internetkriminalität und Internetkrieg verschwimmt heute immer mehr, weil manche Staaten kriminelle Organisationen als nützliche Verbündete betrachten. Einige Nationen zeigten bereits, dass sie bereit sind, Angriffe auf gegnerische Ziele durch kriminelle Organisationen und Privatpersonen zu tolerieren, zu fördern oder sogar gezielt einzusetzen.*
>
> *Karnik u.a.* [594]

C.3 2. Wandlung der Erscheinungsformen

Die Formen der Cybercrime haben sich in den letzten Jahren verfeinert und professionalisiert. Sie wurden bereits im Einzelnen beschrieben, so dass hier nur auf die Entwicklungen und Veränderungen eingegangen wird. Sie zeigen, dass das Fachwissen und handwerkliche Qualität der Kriminellen einen erschreckend hohen Stand erreicht haben. Diese Tendenzen haben eine gewisse Ähnlichkeit mit der Geschichte der gewerblichen Informationstechnik. Während am Anfang eine Garagenwerkstatt [595] ausreichte, um die ersten Computer zusammen zu schrauben, „schmutzige“ Betriebssysteme [596] zu programmieren und einfache Spiele zu vermarkten [597], wurden aus diesen Werkstätten später internationale Konzerne mit klingenden Namen wie Microsoft, Apple und viele andere.

Auch die Informationstechniker mussten sich professionalisieren, kaufmännisches Denken lernen und ein eigenes Marketing entwickeln.

Die Cybercrime zeigt eine ähnliche Entwicklung. Sie vereinigt inzwischen sehr unterschiedliches Fachwissen, so dass ihre Organisation in aller Regel auf Arbeitsteilung und gewerbliche Strukturen beruhen muss, um die gezeigte Qualität zu bekommen. Geschickte Einzeltäter mögen die dazu nötigen Zulieferer finden und beauftragen können. Der Stand der Cybercrime lässt hingegen kleinere und größere Unternehmen erwarten, deren Mitarbeiter flukturieren, aber vom Grundsatz her kontinuierlich zusammen arbeiten.

C.3 2.1 Phishing

Den stärksten Wandel hat das ▸ Phishing erfahren. Als ich mich 2007 erstmals mit ihm beschäftigte, basierten seine Methoden [598] allein auf dem Versand von Spam-Mails. Mit ihnen wurden Finanzagenten [599] geworben und schließlich, zunächst noch mit groben Methoden des ▸ Social Engineerings, Bankkunden dazu überredet, ihre Zugangsdaten und besonders ihre Transaktionsnummern - TAN - zu offenbaren.

Schon vor zwei Jahren stellte das Sicherheitsunternehmen McAfee fest, dass die in Deutschland verbreitete Malware mit einer perfektionierten Sprache daherkommt [600]. Das gilt nicht nur für die

---

[591] Ester/Benzmüller 2010, S. 8.

[592] Ester/Benzmüller 2010, S. 9.

[593] Ester/Benzmüller 2010, S. 9. Einigen Beschuldigten ist es bei der Elite-Razzia tatsächlich passiert, dass sie am PC sitzend von der Polizei bei ihren Geschäften im Board erwischt wurden.

[594] Abhishek **Karnik**, Avelino C. **Rico**, Jr., Amith **Prakash**, Shinsuke **Honjo**, Erkennung gefälschter Sicherheitsprodukte, McAfee 04.01.2010

[595] Von den Gründern der Apple Inc. (Steve Jobs, Steve Wozniak und Ronald Wayne) ist überliefert, dass sie ihre ersten Computer in der elterlichen Garage produzierten.
WP, Apple. Geschichte

[596] Die ersten Versionen des Disk Operating System – DOS – von Microsoft wurden spaßhaft auch als „Quick and Dirty Operating System“ bezeichnet;
WP, PC-kompatibles DOS

[597] Ich denke dabei an Pong von 1972;
WP, Computerspiel

[598] **CF**, Phishing: Zusammenfassung krimineller Methoden, 2007

[599] **CF**, Finanzagenten, 2007

[600] **CF**, Länderberichte. Deutschland, 27.07.2008;

häufig grausame Rechtschreibung und Grammatik aus der Anfangszeit, sondern auch für den Jargon [601]. Darin unterscheiden sich die neuen Täter von der Nigeria-Connection, aber auch die lernt dazu [602].

Das Phishing hat subtile Formen angenommen [603], nutzt Malware und hat das Ausspähen der Nutzerdaten automatisiert [604]. Dabei wendet es die Methode des Man-in-the-Middle an [605] und gaukelt dem Anwender sogar gefälschte Kontobewegungen vor, damit er die von der Bank angeforderte iTAN offenbart [606]. Der Betrieb von Botnetzen und der Einsatz von Phishing-Malware sind dabei zusammen gewachsen [607].

Das Phishing war die erste spezialisierte Form des Identitätsdiebstahls, wobei sich die Täter auf das Ausspähen von Kontozugangsdaten beschränken. Heute werden alle individuellen Netzdienste penetriert, wenn sie versprechen, Gewinn machen zu können oder Kontakte herzustellen, die ihrerseits Gewinn versprechen.

C.3 2.2 Identitätsdiebstahl

Seit mehreren Jahren nehmen die Fälle zu, dass mit ausgespähten oder auf Tarnidentitäten lautende Waren- und Handelskonten Missbrauch getrieben wird [608]. Wie beim Phishing besteht hierbei die Schwierigkeit in der Beutesicherung, so dass Warenagenten zum Einsatz kommen, die Wertgegenstände umverpacken und weitersenden, Tarnadressen, Paketstationen u.a. [609]. Die Kreativität der Täter ist beachtlich und führt zum Beispiel zu neuen Formen der Aktienmanipulation [610] und gezielten Angriffen auf Unternehmen [611]. Sie zeigen, dass die Täter nicht nur mit der Informationstechnik umzugehen wissen, sondern auch besondere Marktmechanismen missbrauchen können.

Der angekündigte Trend zu individualisierten Angriffen und vermehrter Industriespionage [612] ist eingetreten. Zudem verwischen sich die Grenzen zwischen privater Cybercrime und staatlichem Cyberwar [613]. Der Bundesverfassungsschutz spricht insoweit von einer deutlichen Zunahme der "elektronischen Angriffe" zum Zweck der Spionage und vor allem der Industriespionage [614].

Schließlich vermengen sich auch kriminelle Erscheinungsformen miteinander. Ein markantes Beispiel dafür ist der Angriff auf die Kundenkonten des Finanzdienstleisters RBS World Pay, wobei die Methoden des Hackings und des Cashings zusammengeführt wurden, um neun Millionen Dollar Beute zu erzielen [615]. Dieses Beispiel

---

Toralv **Dirro**, Dirk **Kollberg**, Deutschland: Malware lernt die Sprache, McAfee Februar 2008

601 **CF**, Salienzeffekt, 01.03.2009;
CF, filigraner Angriff, 14.05.2008;
CF, infizierte Webseite, 14.05.2008.

602 **CF**, (Fast) 30 Jahre Spam aus Nigeria! 14.08.2007;
CF, Evergreen: Vorschussbetrug nach Nigeria-Art, 17.03.2008.

603 **CF**, Angriffe aus dem Internet, 22.06.2008;
Daniel Bachfeld, Dunkle Flecken. Neuartige Angriffe überrumpeln Webanwender, c't 11/2008, S. 83

604 **CF**, Phishing mit Homebanking-Malware, 22.10.2008

605 **CF**, The Man in the Middle, 2007;
CF, Man-in-the-Middle (Grafik), 2007.

606 **CF**, sicheres Homebanking, 19.12.2008;
Daniel **Bachfeld**, Zahl oder Karte. Sicherer Zugriff aufs Online-Konto, c't 17/2008, S. 94

607 Daniel **Bachfeld**, Einzelne Bande war für zwei Drittel aller Phishing-Angriffe verantwortlich, Heise online 17.05.2010

608 **CF**, Sicherheitsstudien von G Data und McAfee, 03.10.2009;
Dennis **Elser**, Micha **Pekrul**, Das Geschäft der Kennwortdiebe: Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er? McAfee 05.08.2009

609 **CF**, Online-Warenhäuser, 22.11.2008;
CF, Berichte und Studien zur IT-Sicherheit, 26.08.2009;
François **Paget**, Finanzbetrug und Internet-Banking: Bedrohungen und Gegenmaßnahmen, McAfee 10.07.2009

610 **CF**, Aktienkursmanipulation, 22.11.2008

611 **CF**, Emissionsrechte, 07.02.2010

612 **CF**, Perspektiven. Cybercrime, 31.12.2008;
Abhishek **Karnik**, Avelino C. **Rico**, Jr., Amith **Prakash**, Shinsuke **Honjo**, Erkennung gefälschter Sicherheitsprodukte, McAfee 04.01.2010

613 **CF**, Analysen zum Cyberwar, 11.01.2010;
François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010, S. 8.

614 **CF**, Verfassungs- und Wirtschaftsschutz, 25.05.2009;
BMI, Verfassungsschutzbericht 2008, Vorabfassung 19.05.2009, S. 285

615 **CF**, Skimming-Coup, 06.02.2009

brachte mich dazu, das Skimming [616] als eine (Rand-) Erscheinung der Cybercrime anzusehen. Seine Täter handeln im globalen Maßstab [617] und verfeinern ständig ihre Methoden [618].

> *Bot-Netze sind die wichtigsten Werkzeuge krimineller Banden, die jährlich viele Millionen durch Betrug und Erpressung abkassieren*.
>
> Heise online [619]

C.3 2.3 Botnetze

Moderne ▸ Botnetz-Malware geht behutsam [620] mit dem Wirtsrechner um, damit die Aktivitäten der Malware unerkannt und der Zombie dem Botnetz möglichst lange erhalten bleibt. In aller Regel wird sie von infizierten Webseiten in den Browser injiziert, wobei es sich zunächst nur um einen kleinen Loader [621] handelt. Er sorgt dafür, dass die Malware - auf neustem Stand - geladen wird. Dann geht es darum, die Malware auf dem Wirt zu installieren und zu tarnen. Dazu erforderliche Komponenten werden aus dem Internet nachgeladen.

Im nächsten Schritt wird der Wirt erforscht. Sein Betriebssystem, seine Hardware und die eingesetzten Programme werden automatisch erfasst und seine Online-Verfügbarkeit gemessen. Diese Daten sendet die Malware an ihren Kontrollserver, der sich regelmäßig hinter ebenfalls gekaperten Zombies mit besserer Leistung versteckt [622]. Ausgeforscht werden aber auch die persönlichen Daten des Anwenders, nicht nur für das Homebanking, sondern auch für eBay und andere Verkaufsplattformen, für soziale Netzwerke und alles, was zu finden ist. Alles lässt sich auch zu Geld machen.

Die Leistungsmerkmale und Online-Verfügbarkeit entscheiden über die Eignung des Wirts als Zombie im Botnetz.

Die Botnetzsteuerungen sind fein und präzise geworden. Sie sorgen für die Aktualisierung der Malware und steuern die kriminellen Aktivitäten [623] des Botnetzes, also vor Allem den Versand von Spam, von E-Mails mit Malware-Anhängen, verteilte und auf Neigungsgruppen und Einzelpersonen ausgerichtete Angriffe [624]. Die Täter im Hintergrund können sich jederzeit auf einen Zombie begeben und von ihm aus kommunizieren, Geschäfte abschließen oder kriminelle Einzelaktionen ausführen. Die dabei hinterlassenen Netzspuren verweisen immer nur auf den Inhaber des infiltrierten Zombies.

C.3 2.4 Skimming

Mit dem Skimming im Einzelnen befasst sich ein gesondertes Arbeitspapier [625]. Hier werden deshalb nur die Entwicklungstendenzen dieser Kriminalitätsform angesprochen.

Die klassischen Skimming-Täter treten in zwei Tatphasen öffentlich auf, beim Ausspähen von Daten (Skimming im engeren Sinne) und abschließend beim Missbrauch von Zahlungskarten (Cashing). Anlässlich dieser öffentlichen Auftritte erfolgen auch erfahrungsgemäß die polizeilichen Zugriffe. Der Fälschungsvorgang selber wird nach den bisherigen Erkenntnissen vorwiegend im osteuropäischen Ausland unternommen.

Wie jede kriminelle Mode wandelt sich auch das Skimming, wobei verfeinerte Methoden zum Einsatz kommen. Während zunächst selbst gebaute Kameras dazu eingesetzt wurden, um die Tastatureingaben der Bankkunden zu beobachten, kommen inzwischen auch handelsübliche Digitalkameras [626], Handys mit Kamerafunktion und handwerklich hochwertige Tastaturaufsätze zum

---

[616] **CF**, Zwischenbilanz: Skimming, 14.11.2009

[617] **CF**, internationale Skimming-Bande zerschlagen, 14.11.2008

[618] Dieter **Kochheim**, Skimming #2, März 2010, S. 12

[619] Sturmwurm-Botnetz sperrangelweit offen, Heise online 09.01.2008

[620] **CF**, Anatomie des Sturm-Wurms, 06.03.2008; siehe auch: Christoph **Alme**, Web-Browser: Eine neue Plattform wird angegriffen, McAfee Juni 2009.

[621] **CF**, Phishing mit Homebanking-Malware, 22.10.2008

[622] **CF**, dezentrale Steuerung, 2007; Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007, S. 76

[623] **CF**, verteilte Angriffe (u.a.), 2007

[624] **CF**, Koobface-Gang antwortet, 23.05.2010

[625] Dieter **Kochheim**, Skimming #2, März 2010

[626] **CF**, Kamera, 13.04.2009

Einsatz [627], die auf den Typ des angegriffenen Geldausgabeautomaten angepasst sind, oder ganze Fassaden (Front Covering) [628], in die sowohl die Tastatur wie auch der Skimmer zum Auslesen der Magnetstreifen von Zahlungskarten eingebaut sind.

Seit zwei Jahren mehren sich die Fälle des POS-Skimming [629]. POS bedeutet Point of Sale. Gemeint sind die handlichen Terminals an den Kassen im Einzelhandel, die gleichzeitig die Kartendaten auslesen und über ihre Tastatur die PIN aufnehmen [630]. Alle notwendigen Daten durchlaufen diese Geräte. Wenn die Täter es schaffen, sie entsprechend umzurüsten, dann speichern oder senden sie die Dumps [631] an die Täter.

In Russland wurden unlängst die Geldautomaten selber gehackt, um die Dateneingabe vollständig aufzuzeichnen [632]. Vermutlich wurde dazu eine technische Schnittstelle an den Geräten genutzt, die zur Wartung, Funktionsprüfung oder Aktualisierung der Software bestimmt ist.

Beide Beispiele zeigen, dass die Beschaffung der Kartendaten und PIN auf mehreren Wegen erfolgen kann. Sie ist zwar wichtig für den Taterfolg, am Ende zählt aber das erbeutete Geld und nicht die Methode, mit der die Täter an die Daten gelangten. Die Arbeitsteilung bei dieser Kriminalitätsform lässt auch spezialisierte „Subunternehmer“ zu, die sich auf die Beschaffung der Daten beschränken und ihre „Rohstoffe“ an andere Spezialisten verkaufen, die sich um das Fälschen und das Cashing kümmern.

Besonders heimtückisch gingen die Hacker vor, die Ende 2008 in die Datenhaltung einer US-amerikanischen Bank eindrangen und die Kartendaten einschließlich PIN von 100 Kunden ausspähten [633]. Gleichzeitig erhöhten sie deren Auszahlungslimit. Am 08.11.2008 wurden weltweit und gleichzeitig an 130 Geldautomaten in 49 Städten die gefälschten Zahlungskarten eingesetzt und damit 9 Millionen US-$ erbeutet.

Dieses Beispiel zeigt, wie sich die Methoden der Cybercrime in den Formen des Hackings, des Ausspähens und des Verfälschens von Daten mit denen anderer Kriminalitätsformen vermengen.

Das Skimming ist von seiner Herkunft her eher beim Trickdiebstahl und -betrug angesiedelt [634], weil es ihm ursprünglich nur um das Stehlen von Zahlungskarten und ihre Fälschung ging. Es verlangt handwerkliche Fertigkeiten bei der Herstellung der eingesetzten Geräte, besonderes Wissen wegen der Auswahl der Geldautomaten und Standorte, die sich einerseits zum Ausspähen der erforderlichen Daten und andererseits zum Missbrauch der gefälschten Zahlungskarten eignen, sowie logistisches Geschick bei der Installation der Überwachungshardware. Die verschiedenen Arbeitsschritte im Tatplan, ihre wechselnden Anforderungen an die Fähig- und Fertigkeiten der Täter [635] und die grenzüberschreitende Logistik des Gesamtplans sprechen für eine Arbeitsteilung mit einer zentralen planenden und steuernden Instanz.

C.3 2.5 Social Engineering

▸ Phishing, ▸ Identitätsdiebstahl, ▸ Malware im Allgemeinen und ▸ Botnetze sind ohne ▸ Social Engineering nicht denkbar. Es handelt sich um eine (offene) Sammlung von Methoden, um andere Menschen zur Preisgabe von Informationen oder zu einem unbedachten Handeln zu veranlassen, die bei Bedarf um Spionagetechnik ergänzt werden. Dabei folgt es dem Prinzip, das jeder Spionagetätigkeit zugrunde liegt: ***Fünf unwichtige Informationen ergeben eine sensible***, wenn

627 **CF**, Tastaturaufsatz, 13.04.2009;
CF, Tastaturblende, 13.04.2009

628 **CF**, Skimming, Juli 2007

629 **CF**, POS-Skimming, 18.05.2008;
CF, Datenklau und -missbrauch, 19.08.2008

630 **CF**, BKA: Lagebild OK. Manipulation von POS Terminals, 01.11.2008

631 vollständige Kartendaten einschließlich PIN;
CF, Fachworte, April 2007

632 **CF**, Skimming an der Quelle, 20.03.2009

633 **CF**, Skimming-Coup, 06.02.2009

634 **CF**, Proll-Skimming, 18.05.2008;
CF, Beobachtung. Trickdiebstahl, Juli 2007.

635 **CF**, Grafik, Juni 2008. Wegen der Herstellung von Skimmern (Kartenlesegeräte) fehlt noch der Hinweis auf § 149 StGB. Die Diskussion um die Strafbarkeit wegen des Umgangs mit diesen Geräten wurde erst ab Herbst 2008 öffentlich.

man sie geschickt kombiniert und mit Alltags- und Fachwissen interpretiert.

Ende 2008 hat McAfee das Social Engineering als eine der gefährlichsten Erscheinungsformen der Cybercrime beschrieben [636], ohne aber seine ganze Dimension zu erfassen. Das Sicherheitsunternehmen hat zu stark die Malware im Blick und vernachlässigt die Organisationssicherheit [637] sowie die unmittelbare Interaktion (Suggestion, Manipulation) zwischen Menschen, die Kevin Mitnick hervorragend herausgearbeitet hat [638].

Beim Social Engineering geht es nicht allein darum, Malware zu platzieren, sondern auch darum, öffentliche Quellen, Abfälle und Fachpublikationen auszuwerten sowie aus dem direkten Kontakt mit Menschen Informationen zu beziehen, die zu einem gewinnträchtigen Informationsdiebstahl missbraucht werden können. Ich habe das am Beispiel meines Arbeitsumfeldes demonstriert [639] und finde immer noch Eschbachs Industriespion köstlich, der sich auf die handwerklichen und Sozialtechniken der Spionage beschränkt [640].

> *Wie in den meisten Gemeinschaften erfolgreicher Krimineller sitzen tief im Inneren einige streng abgeschirmte Köpfe, die sich auf die Mehrung ihrer Gewinne mit beliebigen Mitteln konzentrieren. Sie umgeben sich mit den menschlichen und technischen Ressourcen, die dies ermöglichen.*
>
> McAfee [641]

C.3 3. der Basar

Im zerschlagenen Elite-Forum und ähnlichen Plattformen haben sich Neugierige, kriminelle Anfänger ab Kindesalter und Profis getummelt. Ihre Geschäfte konnten sie abgeschottet und anonym abschließen. Dazu gehören Wartungsverträge für Malware, qualitätsgeprüfte Kontodaten und Gewinnbeteiligungen bei kriminellen Aktionen.

2006 unterschied McAfee die Beteiligten nach den mittelmäßig gefährlichen ***ruhmgierigen Amateuren*** und ***Nachahmern*** sowie den seltenen, aber wenig gefährlichen ***Innovatoren*** [642]. Gefährlich hingegen seien die (verärgerten) ***Insider*** [643] und hoch gefährlich die ***Organisierten Internetverbrecher***.

Eine systematische Analyse der Underground Economy haben 2009 Marc-Aurél Ester und Ralf Benzmüller vorgestellt [644]. *Die Szene und ihre Strukturen* <zeigen>, *dass es sich hier um keine harmlose Minderheit handelt, sondern um organisierte Betrüger und Diebe* (S. 3).

Von zentraler Bedeutung sind dabei die Boards, also die geschlossenen Diskussionsforen, die zielgruppengerecht sowohl für *Script Kids, die gerne einmal Hacker spielen wollen* (S. 3), wie auch für abgebrühte Kriminelle angeboten werden. Für sie wird im Board häufig ein Marktplatz angeboten, der Black Market, auf dem vor Allem Kreditkartendaten, E-Mail-Adresslisten, Botnetze und Raubkopien zum Handel angeboten werden. Die Verhandlungen und die Kommunikation mit dem Provider erfolgt in aller Regel mit abgeschotteten Instant Messaging Diensten (S. 4) [645]. Zur Anonymisierung kommen vor Allem Proxy-

---

636 **CF**, virtuelle Kriminalität 2008, 13.12.2008; Bericht von McAfee zum Thema Virtuelle Kriminalität (ZIP), McAfee 08.12.2008

637 **CF**, Organisationssicherheit, 07.02.2010

638 Kevin Mitnick, William Simon, Die Kunst der Täuschung. Risikofaktor Mensch, Heidelberg (mitp) 2003

639 Dieter **Kochheim**, Social Engineering, 17.06.2007

640 **CF**, Nobelpreis, 26.06.2007; Andreas **Eschbach**, Der Nobelpreis (Zitate)

641 **CF**, Organisierte Kriminalität im Internet, 05.10.2008; Zweite große europäische Studie über das Organisierte Verbrechen und das Internet, McAfee Dezember 2006 (ZIP)

642 Ebenda

643 Siehe auch: **CF**, Schutz nach innen, 29.08.2009; Christian **Böttger**, Der Feind im Inneren, Technology Review 28.08.2009

644 Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009; siehe auch: **CF**, Sicherheitsstudien von G Data und McAfee, 03.10.2009;

645 **WP**, Instant Messaging

Aus den Hackern, die nur zum Spaß in fremde Systeme eindrangen, entwickelten sich organisierte kriminelle Strukturen, die auf Gewinn aus sind.

Im Internet haben sich zahlreiche Online-Börsen für geraubte Daten etabliert.

Zum Einsatz kommen größtenteils Forensysteme, auf denen zahlungswillige Käufer nahezu alle illegalen Dienstleistungen erhalten, die das Internet bietet.

Auch die notwendige Hardware zum Erstellen gefälschter Karten und Ausweise wird hier gehandelt, ebenso so genannte Drops, das sind sichere Orte, an die sich mit gestohlenem Geld gekaufte Ware liefern lässt.

Auch Hacker, Cracker und Virenschreiber bieten ihre Dienste an. So kann ein Kunde beispielsweise komplette Bot-Netze mieten.

Einen Großteil der angebotenen Ware machen zudem Trojaner, Keylogger und andere Schadsoftware aus.

Denn zu jedem der einzelnen Viren erhält der Kunde eine sechsmonatige Support-Phase, in der er sich mit Problemen an den Verkäufer wenden kann.

Das Geld für die angeforderten Artikel wird dabei einem vertrauenswürdigen Dritten, meist dem Forenbetreiber, überwiesen.

Besonders beliebt ist die Micropayment-Lösung E-Gold. Diese setzt ... nicht auf eine Währung, sondern sichert das im Umlauf befindliche Geld mit Gold und anderen Edelmetallen.

Zudem kümmern sie sich neben dem eigentlichen Verkauf um den „Nachwuchs“. Nahezu jede Seite enthält eine Tutorial-Sektion, in der erfahrene Nutzer ihr Wissen an neue Mitglieder weitergeben.

Eine gut geschriebene Anleitung kann den Bekanntheitsgrad des Erstellers deutlich steigern. Außerdem kann sich der Autor damit eine Art Loyalität neuer und künftiger Phisher sichern. Beide Aspekte kommen anschließend wieder dem Autor bei seinen Geschäften zugute.

Alle Zitate von Jäger [646].

Dienste (S. 9) und Anonymisierer [647] zum Einsatz.

Professionelle Anbieter betreiben daneben häufig offen zugängliche Webshops, in denen Käufer von *Schadcode wie in einem regulären Onlineshop einkaufen können* (S. 5). Szene-übliche Bezahl-

Innerhalb der Board-Szene tobt ein Kampf darum, wer die Nummer 1 ist. Nicht selten werden Boards von Konkurrenten defaced (optisch verändert) oder sogar Überlastangriffen ausgesetzt. Gerne kopieren diese „Mitbewerber“ auch die Datenbanken der jeweiligen Foren und veröffentlichen diese dann auf anderen Boards. Auf diese Weise möchten sie einen erfolgreichen Angriff beweisen und dafür Anerkennung in der eigenen Community erhalten. Meist wird die Webseite zudem signiert, um zu zeigen, dass man sie gehackt hat.

Ester, Benzmüller [648], S. 4

dienste sind *Western Union* [649], *Paysafecard* [650], *E-Gold* [651] *oder auch Webmoney* [652] (S. 6). Wer sich nicht die Mühe machen will, einen Webshop und das Bezahlsystem zu pflegen, kann dazu einen Offshoring-Dienst mieten, der allerdings bis zu einem Drittel des Umsatzes als Provision verlangt (S. 7).

Betrüger, die schlechte Waren liefern oder gegen Vorkasse nichts, werden Scammer genannt und in eigenen Forenbereichen "geflamed", also bloßgestellt und geächtet (S. 8). Solche Bewertungssysteme sind auch von eBay und Amazon bekannt, nur dass dort eher keine kriminellen oder Hehlerwaren angeboten werden.

Gefragt sind Informationen, mit denen sich Accounts anlegen, Identitäten übernehmen oder sonstige, für die Szene nützliche und nötige Dinge tun lassen (S. 9). Dazu gehören besonders auch die Adressen von Cardable Shops, *bei denen Online-Käufer mit ihren gestohlenen Kreditkartendaten aufgrund von mangelnder Überprüfung leicht Waren bestellen können. Denn je mehr Angaben ein Shop verlangt, desto mehr Daten muss der Betrüger erbeuten oder kaufen. Je*

646 Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006

647 **CF**, Anonymisierer, 09.07.2008

648 Ester, Benzmüller, siehe oben.

649 **CF**, Auslandszahlungen per Bargeldtransfer, 2007

650 **CF**, Bezahlen im Internet, 19.06.2008;
Matthias **Sternkopf**, Moritz **Jäger**, Neue Bezahlverfahren im Internet. Was leisten PayPal, giropay, Moneybookers und Co? Tecchannel 12.06.2008;
siehe auch: **CF**, Betrug mit Porno-Vorwurf, 07.03.2010.

651 **CF**, Verrechnungssysteme auf der Basis von Edelmetallen, 2007

652 **CF**, Botnetz-Software und -Betreiber, 13.07.2008

vollständiger die Datensätze bei Kreditkarten sind, desto wertvoller sind sie daher auch (S. 9).

C.3 4. Organisierte Internetverbrecher

Einen besonderen Raum nehmen die Angebote von Botnetzbetreibern ein, die ihre Dienste in den Boards anbieten. *Bevorzugt werden infizierte Computer in Westeuropa, Nordamerika und Australien gesucht. Es ist davon auszugehen, dass dies sehr wahrscheinlich mit der guten Internet-Infrastruktur innerhalb dieser Länder und mit der hohen Verbreitung des Netzes zusammenhängt* (S. 10). *Der Versand von 1.000.000 Spam-E-Mails kostet ca. 250 bis 700 US-Dollar bei einem Botnetzbesitzer* [653] (S. 12).

Ester und Benzmüller gehen auch auf das Carding, die Beutesicherung, das sie Cashout nennen, und Einzelheiten beim Betrieb von Botnetzen sowie Bullet Proof-Diensten ein, von denen noch zu sprechen sein wird. Dabei bleiben sie jedoch auf der Erscheinungsebene, ohne sich mit den Personen und Strukturen zu befassen, die Black Markets oder andere der angebotenen Dienste betreiben.

Dazu besteht jedoch ein dringender Anlass. Es ist etwas anderes, geklaute Daten oder andere kriminelle Dienste in einem Board anzubieten, als die Infrastruktur für das Board, den Proxy, den anonymen Hostspeicher oder den "all inclusive" Webshopdienst zu betreiben. Die Betreiber haben echte Investitions- und Betriebskosten, die sie nicht zum Vergnügen oder aus Altruismus aufbringen.

Sie sind die, die von McAfee als Organisierte Internetverbrecher bezeichnet werden, die sich mit menschlichen und technischen Ressourcen umgeben, um Gewinn zu machen.

Der von McAfee gewählte Begriff ist plakativ, aber nicht besonders trennscharf.

Die allgemein anerkannte Definition für Organisierte Kriminalität [654] liefert die Anlage E [655] zu den

> *Eine weitere sehr gefragte Ware sind Dokumente: Das Interesse liegt in diesem Bereich auf gefälschten Führerscheine oder Studentenausweisen ebenso wie auf gestohlenen Personalausweisen. Begehrt sind alle Dokumente, die dabei helfen, seine eigene Identität geheim zu halten oder eine andere zu übernehmen. Besonders auf russischen Boards blüht ein starker Handel mit solchen Dokumenten.*
> Ester, Benzmüller [656]

RiStBV [657]. Der Periodische Sicherheitsbericht des BMI von 2006 [658] hebt besonders die Abschottung gegenüber Außenstehenden hervor [659] und spricht von *professionellen Tätergruppen und Organisierter Kriminalität* [660].

Das Kriterium der Abschottung gilt für alle strukturierten Formen der Cybercrime. Zu ihnen zähle ich die ***Betreiber*** von

⇨ Boards für kriminelle Dienste,

⇨ Offshore-Diensten (Webshops, Bezahldienste),

⇨ Botnetzen,

⇨ spezialisierten Proxy-Servern,

⇨ Bullet Proof-Infrastruktur (vor Allem Hostspeicher, Drop Zones) und

⇨ anonymisierenden DNS-Servern

sowie die ***Programmierer*** von spezialisierter Malware zum Betrieb von Botnetzen und zur individualisierten Spionage.

Die Nutzer der Boards sind die Amateure, Nachahmer, Insider und Spezialisten, von denen McAfee gesprochen hat. Für sie gilt überwiegend der erste Anschein, dass es sich um eine diffuse Menge tatgeneigter Einzeltäter handelt.

---

653 Ester, Benzmüller, siehe oben.

654 **CF**, Organisierte Kriminalität, 2007

655 **CF**, Gemeinsame Richtlinien der Justizminister/-senatoren und der Innenminister/-senatoren der Länder über die Zusammenarbeit von Staatsanwaltschaften und Polizei bei der Verfolgung der Organisierten Kriminalität

656 Ester, Benzmüller, S. 10.

657 Siehe auch: **BKA**, Lagebild Organisierte Kriminalität 2005 Bundesrepublik Deutschland (Kurzfassung, S. 8)

658 **BMI**, Zweiter Periodischer Sicherheitsbericht, November 2006

659 **BMI**, 4.3 Professionelle Tätergruppen und Organisierte Kriminalität, 15.11.2006

660 **CF**, Professionelle Tätergruppen und Organisierte Kriminalität, 2007

Die Betreiber zeigen hingegen ein anderes Kaliber. Sie benötigen gewerbliche Strukturen, hinter denen sie ihre kriminelle Tätigkeit verbergen. Dazu sind Einzeltäter in aller Regel nicht in der Lage. Sie brauchen entweder feste oder jedenfalls dauerhafte Partner, mit denen sie zusammenarbeiten.

Heute können mehr als 75 Prozent der russischen Wissenschafts- und Ingenieur-Studenten nach dem Abschluss des Studiums keinen Job finden. Sie oder Ihre Tutoren eröffnen inzwischen Shkola Hackerov ("Hacker-Schulen"). Dort bieten sie Schulungen in Hacking und führen ihre Schüler direkt zur Kriminalität, wo sie zwei bis drei Mal mehr verdienen als wenn sie ehrlich arbeiten würden.
Paget [663]

C.3 5. kriminelle Programmierer

Eine unklare Stellung nehmen die professionellen Programmierer von ▸ Malware ein. Ich vermute, dass sie vor Allem allein arbeiten, aber rege und abgeschottete Kontakte zu Zulieferern und anderen Fachleuten pflegen, von denen sie auch im Einzelfall Unterstützung erhalten, ohne dass sie gemeinsam eine gewerbsähnliche Struktur aufbauen.

Dafür sind folgende Annahmen Ausschlag gebend:

Der Erfolg von Malware hängt von der Qualität der verwendeten Sicherheitslücken (Exploits), der Tarntechnik (Root Kits) und der Malware selber ab, die alle Komponenten verbindet. Einfache Malware, also Massenware, kann längst mittels "Baukästen" zusammengestellt werden [661].

Professionelle Malware dürfte hingegen eine Einzelanfertigung sein, die zwar auf erfolgreichen Komponenten aufbaut, aber letztlich die intellektuelle Leistung eines oder mehrerer Programmierer erfordert.

Das gilt besonders für Botnetz-Malware, die profunde Kenntnisse über Peer-to-Peer-Netze und Fernwartung voraussetzt. In diesem Bereich mag es Einzeltäter geben. Die Anforderungen an die Malware-Komponenten lassen jedoch eher erwarten, dass vertraute Gruppen zusammen arbeiten.

Professionelle Kriminelle wissen, wo ihre Grenzen sind, und schließen sich deshalb in aller Regel mindestens zu lockeren Verbünden zusammen, die ständig und arbeitsteilig zusammen arbeiten.

Es gibt - auch in Deutschland - Hinweise darauf, dass bei ihrer Zusammenarbeit die Methoden des Projektmanagements [662] zum Zuge kommen. Sie umfassen den Projektauftrag, die Meilensteine, um das Projektziel zu erreichen, und nicht zuletzt einen Zeitplan. Diesen erfordert die "Kritische Kette". Sie bedeutet nichts anderes als die pünktliche Ablieferung der Komponenten, mit denen der nächste Projektteilnehmer zwingend weiter arbeiten muss.

Bei den professionellen Programmierern wird man deshalb beide Erscheinungsformen finden, den begnadeten Einzeltäter ebenso wie die streng organisierte Kleingruppe mit spezialisierten Teilnehmern. Von da ist es kein weiter Schritt zur Operation Group mit einer eigenen Leitungsstruktur.

Auf dem Basar werden sich alle Interessierten tummeln, die Einzeltäter ebenso wie die, die sich an eine Operation Group angeschlossen haben. In ihm bewegen sich schließlich auch die Agenten, die Spezialisten und die Kleinunternehmer, die deren Dienste einkaufen, um sie für kriminelle Projekte zu verwenden.

---

[661] Frühes Beispiel: **CF**, Trojanerbaukasten mit Support (Turkojan), 20.06.2008

[662] **CF**, kritische Projekte, 2008

[663] François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010, S. 8.

C.3 6. Operation Groups

Schon Balduan hat von den Agenten und Spezialisten gesprochen sowie von den Operation Groups [664]. Bei ihnen handelt es sich um Kleinunternehmer, die Einzelleistungen für kriminelle Projekte zur Verfügung stellen und dazu auf die nötigen Spezialisten zurückgreifen können.

Es ist gut denkbar, dass besonders Malware-Schreiber in solchen kleinen Gruppen arbeiten und nicht am operativen Geschäft selber teilnehmen. Als Zulieferer sprachlich perfekter Texte für Spams und Webseiten kann ich mir eher Einzelpersonen als Experten vorstellen.

Meine Vorstellung von dem Unternehmen Phish & Co. [665] scheint auf die moderne Zusammenarbeit zwischen Operation Groups nicht mehr anwendbar zu sein.

Im Bezug auf das Phishing muss jetzt davon ausgegangen werden, dass unterschiedliche Personengruppen Finanzagenten anwerben und betreuen und andere das Phishing als solches durchführen. Die Szene hat sich spezialisiert.

Auch in Bezug auf andere Kriminalitätsformen muss immer mehr von selbständigen Spezialisten ausgegangen werden. Bei gescheiterten Skimming-Angriffen sind inzwischen so viele baugleiche Tastaturaufsätze aufgetaucht, dass von einer Serienproduktion durch einen oder mehreren versierten Handwerkern ausgegangen werden muss, die ihre Waren für teures Geld verkaufen.

> *Die zentrale Figur jedoch ist ... ein „Independent Business Man“ – eine Person, die Kontakte zur Unterwelt pflegt und zwischen Bot-Herdern, Hackern, Malware-Schreibern und Spammern koordiniert. ... mithilfe der Botnetz-Infrastruktur kann der Koordinator Unternehmen mit verteilten Massenangriffen auf ihre Webseiten drohen und so Schutzgeld erpressen, Spam-Wellen mit Werbung für überteuerte Produkte oder Aktien lostreten oder tausendfach persönliche Informationen wie Bankzugangsdaten ergaunern.*
>
> Bolduan, S. 30

C.3 7. Koordinatoren

Auch von den Koordinatoren hat Balduan berichtet. Sie planen kriminelle Einzelprojekte nach Maßgabe des Projektmanagements und den üblichen wirtschaftlichen Messgrößen:

⇨ Aufwand,

⇨ Gewinn und

⇨ Entdeckungsrisiko.

Der Basar, die Operation Groups und die Koordinatoren sind typische Erscheinungsformen der Cybercrime. Sie werden in ähnlicher Weise auch in Bezug auf andere kriminelle Erscheinungsformen auftreten, nicht aber als gängiges Organisationsmodell für alle kriminellen Aktivitäten.

Ein Beispiel dafür sind die kurzen zeitlichen Abstände zwischen dem Skimming und dem Cashing, die sich im vergangenen Jahr auf bis zu zwei Tage verkürzt haben. Das spricht eher für eine auf Dauer angelegte Zusammenarbeit zwischen den arbeitsteiligen Tätergruppen und nicht dafür, dass spezialisierte Ausspäher ihre Erzeugnisse erst auf einem Schwarzmarkt anbieten müssen, um sie an spezialisierte Fälscher und Casher abzusetzen.

Klassische Einbrecher werden ebenfalls eher nach einem eingefahrenen Muster mit Vertrauten zusammen arbeiten und nicht für jede einzelne Tat neue Komplizen suchen. Nach aller Erfahrung haben sie auch Kontakte zu spezialisierten Hehlern, die einen kontinuierlichen Absatz versprechen.

---

[664] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 30;
Cyberkriminelle entwickeln sich zu Unternehmern, tecchannel 15.07.2009

[665] **CF**, Das Unternehmen Phish & Co., 2007

> *Das ... Geschäftsmodell des RNB war simpel und dreist: Je mehr eine Domain in den Fokus der Öffentlichkeit geriet, je mehr Beschwerden an die E-Mail-Adresse für Missbrauch geschickt wurden, desto mehr Geld verlangten die Russen von ihren Kunden.*
>
> Bolduan, S. 32

C.3 8. Schurkenprovider

Der bekannteste Rogue Provider [666] (Schurkenprovider [667]) ist das Russian Business Network - RBN [668]- in Petersburg gewesen, das sich Ende 2007 aus der Öffentlichkeit zurück gezogen hat. Über seine Aktivitäten haben vor Allem Bizeul [669], Bolduan [670] und Frank Faber berichtet [671].

Das Kerngeschäft des RBN und anderer Schurkenprovider besteht darin, ihre zahlenden Kunden für ihre heiklen oder kriminellen Aktivitäten Abschottung, also einen "sicheren Hafen" zu bieten. Das verlangt nach

⇨ anonymisierten Speicherstandorten,

⇨ einer anonymisierten Adressverwaltung (Maskierung von DNS-Eintragungen),

⇨ komfortablen Anbindungen an das Internet und

⇨ eine Niederlassung, in der der Schurkenprovider ohne Angst vor Repressalien handeln kann.

Die ersten drei Voraussetzungen lassen sich nur erfüllen, wenn der Schurkenprovider ein Autonomes System - AS [672]- betreibt. Dabei handelt es sich um ein selbständiges Netzwerk, das über mindestens zwei Außenverbindungen zu anderen Netzen verfügt, über die es Verbindungen zum Internet hat. Jedem AS wird von der Internet Assigned Numbers Authority - IANA [673]- eine eindeutige, fünfstellige Autonomous System Number - ASN - vergeben [674]. Für den europäischen Bereich ist diese Aufgabe auf das Réseaux IP Européens Network Coordination Centre - RIPE NCC [675]- übertragen worden.

C.3 9. Tarnung und Abschottung der Kunden

Ein AS kann sich im Internet nicht verstecken. Es ist anhand seiner AS-Nummer eindeutig erkennbar und sein physikalischer Standort genau zu orten.

Was in seinem Inneren geschieht, ist eine andere Sache.

C.3 9.1 Whois Protection

Das AS ist berechtigt, eine eigene Adressenverwaltung durchzuführen. Dahinter verbirgt sich nichts anderes als ein DNS-Server [676], der dazu da ist, für eine beschreibende Internetadresse den physikalischen Standort anhand der nummerischen Adresse des Internetprotokolls zu melden [677]. Darüber hinaus liefert der DNS-Server die persönlichen Angaben über den Inhaber der DNS-Adresse.

Damit verfügt jedes AS über ein mächtiges Werkzeug. Mit seinem DNS-Server kann es die gespeicherten Domänennamen zu jedem beliebigen physikalischen Standort leiten und in der Datenbank im Übrigen jeden Unfug über den Inhaber bereit halten [678].

In Fachkreisen wird das als "Whois Protection" bezeichnet [679]. Es ist nichts anderes als die Verschleierung der Betreiberdaten, um ihn vor den

---

666 **CF**, Rogue Provider, 13.07.2008

667 **CF**, Schurkenprovider, 05.10.2008

668 **CF**, Russian Business Network – RBN, 13.07.2008

669 **CF**, Schurken-Provider und organisierte Cybercrime, 13.07.2008;
David **Bizeul**, Russian Business Network study, bizeul.org 19.01.2008

670 Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008;
CF, weitere Nachweise, 13.07.2008

671 **CF**, Russian Business Network – RBN, 13.07.2008;
Frank Faber, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008

672 **CF**, verwirrende Beziehungen, 2007

673 **WP**, Internet Assigned Numbers Authority

674 **WP**, Autonomes System. Verwaltung

675 **WP**, RIPE Network Coordination Centre

676 **WP**, DNS-Server

677 Schematische Darstellung: **CF**, Auflösung von DNS-Adressen, 2007.

678 **CF**, IP-Adressen ohne Beweiswert, 16.05.2010

679 **CF**, Auskunftsdienste im Internet, 06.12.2009

Nachstellungen der Strafverfolgung oder von Abmahnern zu schützen.

In offenen Foren findet man dazu euphorische Lobhudeleien: Endlich keine Abmahnungen und teure Anwaltsforderungen mehr!

C.3 9.2 anonyme Server

Das zweite mächtige Werkzeug, das dem AS zur Verfügung steht, ist die Anonymisierung von Servern.

Mit dem einfachen Kommando "Ping" [680] lässt sich die technische Erreichbarkeit einer Netzadresse überprüfen. An ihr kann sich ein Netzknoten befinden (Router, Switch, Gateway) oder ein Endgerät, das Dateien (Hostspeicher, FTP) oder Datendienste (Webserver, Datenbanken) birgt. Auf das Ping-Kommando meldet das angeschlossene Gerät seine Identität.

Ping richtet sich an nummerische Adressen des Internetprotokolls nach dem Muster xxx.xxx.xxx.xxx . Vom Anspruch her sollen die beiden linken Ziffernfolgen den geographischen Standort der IP-Adresse widerspiegeln.

Auch die IP-Adressen werden von der IANA einzeln oder blockweise vergeben. Die Ziffernfolge offenbart im Ergebnis nur das AS, an das sie vergeben wurde, nicht aber den physikalischen oder geographischen Standort, an dem sie eingesetzt wird. Diesen kennt nur das AS selber.

Das AS hat mehrere Möglichkeiten, auf die Rückmeldungen des Endgerätes Einfluss zu nehmen. So kann es alle Rückmeldungen unterbinden, wenn es an seinen Eingängen Firewalls betreibt, die die Meldungen nicht durchlassen.

Der Betreiber der Endgeräte, also das AS, kann auch genau vorgeben, was sie an die Gegenstellen senden. Das kann jeder Quatsch sein.

Wenn ein Schurkenprovider über ein eingetragenes AS verfügt, das an zwei Endpunkten an andere AS angeschlossen ist, über geographisch weit verstreute IP-Adressen und über ein Rechenzentrum mit hinreichend leistungsstarken Rechnern verfügt, dann kann er die informationstechnischen Aktivitäten, die auf den Rechnern stattfinden, so tarnen, dass jedem Außenstehenden vorgegaukelt wird, dass die betreffenden Internetangebote nicht lokalisierbar sind oder irgendwo auf der Welt stattfinden, aber nicht dort, wo sie tatsächlich sind.

Das hübsch bunte Geotracing [681] lässt sich damit herrlich in die Irre führen.

C.3 9.3 Detektion

Dennoch kann man die geographischen Standorte von getarnten DNS-Adressen und Servern auch von außen eingrenzen und lokalisieren. Verantwortlich dafür ist das Internetprotokoll selber und das Netzwerkwerkzeug Traceroute [682].

Die Architektur des Internets folgt technischen und wirtschaftlichen Logiken. Die großen internationalen Netzbetreiber (Tiers [683]) können die Datenströme steuern und zum Beispiel möglichst lange in der eigenen Netz-Infrastruktur belassen, um sie erst am Zielort an einen regionalen Endanschluss-Betreiber zu überlassen. Diese Strategie wird als "cold potato" bezeichnet und IBM [684] ist besonders bekannt dafür, so zu verfahren. Andere Carrier [685] ohne oder mit schwachen überregionalen Leitungen verfahren nach der "hot potato"-Methode und versuchen, ihre Daten äußerst schnell an andere Partner zu übergeben.

Das Internetprotokoll toleriert die Vorgaben der Carrier und lässt Umwege bei der Signalübertragung zu. Sie können darauf beruhen, dass die direkte Strecke überlastet ist, so dass zum Lastausgleich Umwege schnellere Verbindungen versprechen. Was die Carrier hingegen nicht zulassen, sind unwirtschaftliche Zick-Zack-Wege im weltweiten Netz.

Mit Traceroute können die Zwischenstationen eines Signals im Internet gemessen werden. Sie verraten, wo etwas Merkwürdiges im Signallauf

680 **CF**, Suchmaschinen und -techniken. IP- und DNS-Adressen, 29.12.2008

681 **CF**, Lokalisierung. Geotracing, 06.12.2009

682 **CF**, Auskunftsdienste im Internet, 06.12.2009

683 **CF**, autonome Systeme und Tiers, 2007

684 **CF**, Besonderheit: IBM, 2007

685 **CF**, verwirrende Beziehungen, 2007

passiert, wenn man als Anwender ausreichende Kenntnisse über die Physik des Internets hat.

Auch dem Tracerouting werden falsche und getarnte Endpunkte vorgegaukelt. Anhand der markanten Zwischenstationen lässt sich jedoch erkennen, wo die Verschleierung einsetzt.

Wenn von Bulgarien aus ein Server in der Türkei erreicht werden soll, dann folgt das Signal einem der Seekabel, die durch das Schwarze Meer zwischen beiden Staaten verlegt sind. Es läuft nicht erst zum Mittelmeer, um über Italien und den deutschen Internetknoten in Frankfurt zu einer Provinzhauptstadt zu gelangen, wonach es plötzlich einen Zielort in der Nordtürkei anzeigt.

Bei genauer Betrachtung ergibt sich nämlich, dass alle Zwischenstationen sehr schnell durchlaufen werden. Erst in der Nähe der Provinzhauptstadt durchläuft das Signal eine lange Verarbeitungszeit, um dann einen Zielort an einem ganz anderen Ende der Welt anzuzeigen. Wenn das Signal getunnelt [686] und getarnt durch ein Virtual Private Network [687] gejagt wird, kann das sogar möglich sein. Nicht aber, wenn man das nächste Tracerouting aus der geographischen Nähe des Zielortes startet und das Signal dennoch den Weg über die Provinzhauptstadt nimmt.

Das AS des Schurkenproviders verrät sich also durch die Zwischenstationen beim Tracerouting, an denen angeblich etwas passiert, was der Netzlogik widerspricht.

C.3 9.4 heimlicher Betrieb

Die Anonymisierung von Servern und die Tarnung von DNS-Adressen sind technische Tricks, um die Veranstalter von illegalen Diensten und Inhalten unkenntlich zu machen. Sie erhalten vom Bullet Proof-Provider einen "sicheren Hafen" für ihre illegalen Aktivitäten, die Bizeul am Beispiel des RBN erkundet hat. Ester und Benzmüller bestätigen seine Aussagen (siehe rechts oben).

Der Betrieb des AS findet aber nicht im Virtuellem statt, sondern in der realen Welt. Neben der getarnten Technik muss deshalb etwas hinzukommen: Der Betreiber muss in einer Umgebung handeln, in der er sich frei von Angriffen, Restriktionen und staatlicher Macht fühlen kann. Für das RBN war das zunächst der Fall. Es galt als beschwerdeignoranter Provider und Hoster [689], von dem weder in ihren Rechten Betroffene noch Strafverfolgungsbehörden die geforderten Auskünfte bekamen.

So kann nur handeln, wer wirklich von seiner staatlichen Umgebung geschützt wird oder wer sich selber so stark tarnt, dass zwischen ihm als Person und seiner schurkischen Veranstaltung keine Verbindung hergestellt werden kann. Das ist keine leichte Aufgabe.

In jüngerer Zeit treten verstärkt betrügerische Webshops mit attraktiven Warenangeboten auf, die es auf die Vorauszahlungen ihrer Kunden absehen. Sie bedienen sich in aller Regel der angesprochenen Offshoring-Dienste, die ohne getarnte Umgebungen keine Abschottung der Anbieter leisten können. Die dazu erforderliche Technik betreiben sie entweder selber oder mieten sie von spezialisierten Schurkenprovidern.

> *Hier finden alle ein Zuhause, die Drop Zones für die Daten ihrer Botnetze suchen, illegale Shops betreiben, Command & Control (C&C)-Server sicher unterbringen wollen und dergleichen mehr. Unter Dropzones ist in diesem Zusammenhang ein Server zu verstehen, auf dem beispielsweise die auf dem Rechner des Opfers installierte Spyware ihre gesammelten Daten ablegen kann. Das Produktportfolio reicht hier wie bei jedem seriösen Anbieter vom kleinem Webspace-Angebot, über virtuelle Server bis hin zu ganzen Serverclustern, je nach Geldbeutel und Anforderungen.*
>
> Ester, Benzmüller [688]

[686] **CF**, Verschlüsselung. Tunnelung, 30.03.2008

[687] **CF**, Overlay-Netze und VPN, 30.03.2008

[688] Ester, Benzmüller, S. 11

[689] antispam.de, beschwerdeignorante Provider und Hoster

c.3 9.5 IP-Adressen und Domain-Entführer

Manuel Schmitt kritisiert [690], die Strafverfolgungsbehörden würden sich zu sehr auf die IP-Adressen [691] verlassen und dabei die Routing-Prokolle der großen Provider außer Acht lassen [692], greift fehl. Anlass geben ihm das Border Gateway Protocol – BGP [693]- und die Meldung, dass im April 2010 ein chinesischer Provider einen Teil des Internets entführt hat [694].

Was ist passiert [695]? Der chinesische Internet-Provider IDC China ist ein autonomes System - AS [696]- und betreibt einen BGP-Router, der dem Internet meldet, mit welchen anderen Partnern er verbunden ist [697]. Diese Meldungen nehmen die Netzknoten auf und speichern sie. Mit diesen Daten arbeitet das BGP und die Netzknoten senden an das AS Nutz-Datenpakete, weil sie davon ausgehen, dass dieses Zwischennetz sie an das richtige Ziel weiter leitet. Das ging aber schief, weil das AS falsche Partnernetze meldete und die angelieferten Datenpakete irgendwo in China versandeten. Das erfolgte unkontrolliert, weil das BG-Protokoll keine Kontrolle, sondern Vertrauen voraussetzt.

Der böswillige Einsatz einer BGP-Manipulation kann dazu führen, dass bestimmte Ziele im Internet vorübergehend nicht erreichbar sind. Das kann für kriminelle oder kriegerische Kampagnen durchaus von Interesse sein.

Dauerhaft ist dieser Zustand aber nicht, weil das Internetprotokoll auch die Rückantwort erwartet, dass die Datenpakete vollständig am Ziel angekommen sind. Die falsche Verbindung löst dadurch eine vermehrte Netzlast wegen der Fehlermeldungen aus. Sie führen schließlich dazu, dass das fehlerhafte AS umgangen und die Signale über andere Wege geleitet werden.

Die böswillige BGP-Manipulation eignet sich zur Verschleierung der Netzstationen nur, wenn am Ende tatsächlich gemeldet wird, dass alle Datenpakete angekommen sind. Das machen sich die Schurkenprovider zunutze, die getarnte Hostspeicher betreiben, deren Standort vor der Öffentlichkeit, Abmahnern und der Strafverfolgung verschleiert werden sollen [698]. Diese Fälle fallen dadurch auf, dass die Standortmeldungen, die mit dem Tracerouting oder anderen Werkzeugen auf der Grundlage des Internetprotokolls ermittelt werden, unsinnig sind, weil sie der physikalischen und wirtschaftlichen Logik des Weltnetzes widersprechen [699].

Schmitts Warnung gilt nur für die Fälle, dass ein Schurkenprovider die Identität seines Kunden tarnt, um ihn der Verfolgung zu entziehen. Es ist nicht zu erwarten, dass dadurch Unschuldige verfolgt werden, weil das Whois Protection und die Tarnung von Servern Standorte und Identitäten verschleiern, nicht aber anderen Handelnden unterschieben.

Geniale Verbrecher könnten hingegen auf die Idee kommen, den Internetauftritt eines Opfers komplett nachzubauen und gezielte Veränderungen daran vorzunehmen. Mit einer BGP-Umleitung könnte dann auf den manipulierten Internetauftritt umgeleitet werden.

Das geht aber nur, wenn das Opfer selber ein AS ist, weil sich die BGP-Umleitung auf andere Netzknoten. Ein einzelner Teilnehmer innerhalb eines AS - also ein Host-Kunde neben anderen - kann jedenfalls von außen nicht so ohne weiteres angegriffen werden. Der Angreifer müsste ganz gezielt die Hostadresse des Opfers filtern und auf die gefälschte Präsenz umleiten. Mit größerem Aufwand ginge auch das.

Für die Strafverfolgung stellt sich das Problem nicht in dieser Brisanz. IP-Adressen sind ganz überwiegend von Interesse, weil sie von einem Zugangsprovider aus seinem Bestand seinem Kunden zugewiesen wurden (Bestandsdatenabfrage), der damit Böses veranstaltete. Dabei geht es nicht um die Ziel-, sondern um die Ausgangs-

690 Manuel **Schmitt**, IP-Adressen nur mit sicherem Routing eindeutig, Heise online 13.05.2010

691 **WP**, IP-Adresse (Internet Protokoll)

692 **CF**, verwirrende Beziehungen, 2007 (Tiers, Carrier)

693 **WP**, Border Gateway Protocol

694 Chinesischer Provider "entführt" kurzzeitig Teile des Internets, Heise online 12.04.2010

695 **CF**, IP-Adressen ohne Beweiswert, 16.05.2010

696 **WP**, Autonomes System

697 **CF**, Routing über den Globus, 16.05.2010

698 **CF**, anonyme Server, 11.04.2010

699 **CF**, Detektion, 11.04.2010

adresse. Deren Manipulation bei einem TK-Unternehmen kann zunächst in dem Bereich der Legende angesiedelt werden.

Dennoch ist Schmitts Warnung berechtigt. Mit Routing-Manipulationen lassen sich Fehlinformationen verbreiten, die Andere in echte Schwierigkeiten bringen können. Jedenfalls dann, wenn der Angreifer über ein AS, über tiefes Wissen und über die Ressourcen verfügt, kann er mit großem Aufwand ganz gezielt die Subadresse seines Opfers umleitet, um ihm unlautere Aktivitäten unter zu schieben.

C.3 10. Crämer und große Kriminelle

Kriminelle Crämer wie die, die ihre Waren und Beuten in Boards anpreisen, sind nicht die großen Nummern im kriminellen Geschäft. Sie sind lästig, dreist und gehören nachhaltig in ihre Grenzen verwiesen.

Viel bedenklicher sind die Betreiber, die den Crämern ihren Markt erst bieten. Sie gilt es richtig zu bekämpfen.

McAfee nennt sie die Organisierten Internetverbrecher und dem kann ich nicht widersprechen. Es handelt sich dabei um die Bullet Proof-Provider und die anderen Schurken, die ich benannt habe.

Das Bild von der diffusen und ungreifbaren Wolke tatgeneigter Täter gilt nur für die Crämer und ist oberflächlich. Sehr lange hat die Strafverfolgung einzelne Trugbilder der Cybercrime betrachtet, ohne sich die wirklich wichtige Frage zu stellen: Wer steckt dahinter und macht das dunkle Treiben erst möglich?

Die professionellen Hinterleute sind es, die nachhaltig und grenzüberschreitend verfolgt werden müssen. Wenn sie nicht mehr frei agieren können, dann bricht auch der Markt für die Crämer weg.

PaySafeCard.com unter DDoS
Published on 02-18-2010 17:14
Nach dem PaySafeCard.com PSC's mit Passwort fast wertlos machten , da man nun den Bon brauchte um das PW zu ändern bzw. mit PW zu benutzen , wollte sich das einige Mitglieder dieser Scene nicht gefallen lassen und schlagen nun zurück. Zum DDoS auf http://www.paysafecard.com/ wird aufgerufen, egal wie groß das Botnetz ist. [700]

C.3 11. Beutesicherung

Die Beutesicherung ist die wichtigste Voraussetzung für kriminelle Geschäfte jeder Art. Eine traurige Berühmtheit hat insoweit Western Union [701] erlangt. Es handelt sich - neben Money Gram - um den bekanntesten Dienst für den Bargeldtransfer, der auch die unbekanntesten Ecken der Welt erreichen kann. Für viele Migranten ist er ein Segen, weil sie nur mit seiner Hilfe ihre Angehörigen in der Heimat unterstützen können.

Finanz- und Warenagenten sind nach wenigen Einsätzen verbrannt. Außerdem reagieren die Banken zunehmend sensibel auf ungewöhnliche Auslandsüberweisungen [702].

Paysafecard, E-Gold und Webmoney sind Bezahlsysteme, die sich für die Beutesicherung im kleinen Stil eignen [703]. Paysafecard ist ein anonymer Bezahldienst, bei dem der Empfänger nur über den Code auf dem vom Versender gekauften Gutschein verfügen muss, um den Auszahlungsbetrag zu erhalten. Dagegen sind E-Gold und Webmoney Verrechnungssysteme nach dem Vorbild von Geschäftskonten (Girokonto). "Echte" Auszahlungen sind möglich, aber schwierig und gelten bei Webmoney als zu teuer.

"PaySafeCard" - PSC - ist keine Karte im her-

---

700 Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010, S. 7, Grafik bei G Data.

701 **CF**, Auslandszahlungen per Bargeldtransfer, 2007

702 Erfolg gegen international organisierte Online-Kriminelle, BKA 13.09.2007;
Haftstrafen im Bonner Phishing-Prozess, Heise online 04.09.2008;
Großrazzia in USA und Ägypten gegen „Phishing"-Betrüger, Hamburger Abendblatt 08.10.2009

703 **CF**, grenzüberschreitender Vermögenstransfer, 2007

kömmlichen Sinne, sondern ein Guthabenkonto aufgrund einer Einmalzahlung [704]. Sie wird an einer Verkaufsstelle geleistet, an einer Tankstelle, Kiosk, Post, Lotto-Annahmestelle oder Automat. Dafür bekommt der Einzahler eine 16-stellige PIN genannt, die meistens auf einem Bon ausgedruckt ist.

Das Guthaben berechtigt zum Einkauf in den Webshops, die sich PSC angeschlossen haben. Dem Kunden entstehen keine zusätzlichen Transaktionskosten. Nur dann, wenn er sich das Guthaben wieder auszahlen lassen will, kostet das eine Bearbeitungsgebühr von 5 €.

PSC ist aber ein echtes, also anonymes PrePaid-System, so dass das Guthaben beliebig gehandelt und übertragen werden kann. Das macht PSC in der Schattenwirtschaft so beliebt. Unabhängig von Grenzen und Entfernungen kann der Einzahlungsbetrag einfach dadurch übertragen werden, dass dem Empfänger die PIN der "Card" mitgeteilt wird. Unterstützt wird das durch ein Sicherheitssystem, das PSC anbietet. Der Erwerber des Guthabens kann mit der PIN ein Webportal aufrufen und dort die PIN mit einem zusätzlichen Kennwort schützen. Bei der Übertragung übermittelt er dann nicht nur die PIN, sondern auch das Kennwort. Der neue Inhaber kann jetzt das Kennwort ändern und ist dadurch der exklusive Inhaber des Einzahlungsbetrages [705]. Auch in der Szene gilt: Vertrauen ist gut, Kontrolle ist besser. Erst wenn der neue Inhaber das Kennwort geändert hat, kann er sicher sein, dass der alte Guthabeninhaber nicht doch lecker einkauft und das Guthaben verbrät.

Dieses Verfahren hat PSC am 18.02.2010 abgeschlossen. Das Kennwort konnte seither nicht mehr nachträglich geändert werden, wenn sich der Inhaber nicht mit dem ausgedruckten Bon legitimiert [706]. "Sicherer" Zahlungsverkehr durch Übertragung des Guthabens ist dadurch eingeschränkt.

Die Hackerszene reagierte empört und rief zum DDoS-Angriff gegen PSC auf [707]. *Es kam zu längeren Ausfallzeiten (Downtime) der PSC-Homepage, wobei jedoch nicht bekannt ist, ob es schlussendlich durch die Angriffe begründet war, oder durch Wartungsarbeiten, wie offiziell verlautbart*. [708].

Nur einen Tag nach den DDoS-Aufrufen, am 19.02.2010, revidierte der Bezahldienstleister seine neue Passwortpolitik. Zum 22.2.2010 sollte eine Einrichtung und Änderung eines Passworts auch wieder ohne die Einsendung des Kassenbons möglich werden [709]. Das wurde von der Szene freudig begrüßt [710].

Die Fakten sprechen für sich: Ein verteilter Angriff gegen PSC scheint wirklich stattgefunden zu haben und das Unternehmen ist danach eingeknickt.

Western Union, PayPal und PaySafeCard sind keine kriminellen Unternehmen, die sich auf Geldwäsche und die Sicherung krimineller Gewinne ausgerichtet haben. In der Rückschau belegen sie aber, dass ihre Folgenabschätzungen entweder leichtfertig und unbedarft oder so waren, dass sie im Interesse ihres Erfolges Bedenken beiseite geschoben haben. Ihre Dienste lassen sich zur Geldwäsche und von der Schattenwirtschaft nutzen. Dessen ungeachtet haben sie keine oder kaum Vorkehrungen getroffen, um dem vorzubeugen. Western Union hat schon vor einigen Jahren darauf reagiert und verlangt jedenfalls in Deutschland die Identifikation seiner Kunden. PSC hat jetzt erfahren, wie gefährlich das Umfeld ist, auf das sich das Unternehmen eingelassen hat.

Die Bezahlsysteme eignen sich gut für das Tagesgeschäft. Große, gleichzeitig anonyme und dennoch öffentliche Geschäfte lassen sich nur in der realen Schattenwirtschaft abwickeln. Dazu eignen sich am besten Scheinfirmen [711] oder gleich die Gründung einer Offshore-Bank, die eigene Zahlungskarten herausgeben kann [712].

C.3 12. fließende Grenzen

Die Cybercrime-Szene besteht offenbar aus ver-

[704] **WP**, Paysafecard

[705] Grafik bei G Data.

[706] Ester/Benzmüller 2010, S. 6 f.

[707] Kasten auf der Vorseite; Grafik bei G Data.

[708] Ester/Benzmüller 2010, S. 7.

[709] Ester/Benzmüller 2010, S. 7.

[710] Ester/Benzmüller 2010, S. 8.

[711] **CF**, Phishing-Aktion, Vorbereitungen, 2007

[712] (keine Satire) Gründung von Vermögensverwaltungsgesellschaften und Banken (Einlagenkreditinstitute) EWR-Schweiz-USA und Offshore, firma-ausland.de

schieden organisierten Beteiligten.

Die Masse besteht aus kaltschnäutzigen, selbstsicheren und bedenkenlosen Geschäftemachern und Trittbrettfahrern, also Einzelpersonen, die keine Skrupel haben, kriminelle Dienste zu nutzen und im kleinen Stil auch anzubieten. Das geschieht außerhalb der Webshops in den Foren, die den Hauptteil des Basars bilden.

Die Web-Kaufleute verdienen ihren Lebensunterhalt mit illegalen Angeboten - meistens mehr schlecht als recht. Sie sind bereit, in ihre Verkaufsplattformen zu investieren, und handeln damit auf längere Sicht. In anderen Worten: Gewerbsmäßig.

Unter den Web-Kaufleuten scheint es auch richtig erfolgreiche zu geben, quasi Großhändler. Sie benötigen nicht nur eine Plattform, sondern auch eine gewerbsmäßige Struktur. Es dürfte sich bei ihnen um Operating Groups handeln, die aus mehreren Personen bestehen, die ihrerseits eine Kleinbande bilden. Diese Gruppen haben einen fließenden Übergang zu den organisierten Internetverbrechern.

Organisierte Internetverbrecher in diesem Sinne sind hingegen die Betreiber der Boards und ihr "Umfeld", worauf Ester und Benzmüller zart hingewiesen haben. Sie richten sich im Internet so ein, dass sie selber ungestört kriminelle Geschäfte betreiben oder aus den Straftaten anderer ihren Gewinn ziehen können.

Der Basar muss nicht zwingend im Internet stattfinden. Er kann auch in intensiven Gesprächskontakten in geschlossenen Teilnehmergruppen bestehen, zwischen Personen, die sich kennen, vertrauen und zu einzelnen - meistens Absatzgeschäften - in immer wieder wechselnden Konstellationen zusammen kommen.

Auch bei diesen Beteiligten liegt eine grundsätzliche Bereitschaft zur kriminellen Zusammenarbeit vor. Sie steht unter dem Vorbehalt, nur bei einer besonders günstigen Gelegenheit zusammen zu arbeiten und nicht bei jeder sich bietenden. Gewinn wollen die Beteiligten aber auch machen.

Die Cybercrime, die sich im Wesentlichen in der virtuellen Welt bewegt, braucht spätestens zur Beutesicherung Schnittstellen zur realen. Darin unterscheidet sie sich nicht von der herkömmlichen Kriminalität. Umgekehrt nutzen auch klassische Kriminelle verstärkt das Internet, um sich zu verständigen und Kontakte zu knüpfen oder die dort gebotenen Möglichkeiten zur Verschleierung von Zahlungswegen zu nutzen.

Die Grenzen werden mehr und mehr verschwimmen [713].

[713] Siehe auch: G Data: eCrime-Ausblick 2010.

C.4 Publikationen zur Cybercrime

Der Aufsatz über den ▸ Basar für tatgeneigte Täter verweist auf eine Reihe von Veröffentlichungen im Internet mit grundlegender Bedeutung. Hier folgt ein zusammenfassender Überblick

Die meisten Veröffentlichungen stammen von dem Sicherheitsunternehmen McAfee [714]. Es setzt sich intensiv mit den kriminellen Strukturen im Internet auseinander, ohne die Einzelheiten zu vernachlässigen.

Die wichtigsten Veröffentlichungen von McAfee sind nach meinem Eindruck die Zweite große europäische Studie über das Organisierte Verbrechen und das Internet vom Dezember 2006, die Länderberichte vom Februar 2008 und Studie über das Social Engineering vom Oktober 2008.

Das Sicherheitsunternehmen G Data tritt erheblich weniger in Erscheinung. Für den Bericht über die Underground Economy vom August 2009 gibt es nichts vergleichbares.

In Bezug auf die Schurkenprovider und das RBN ist der Artikel von Gordon Bolduan [715] von höchstem Erkenntniswert.

McAfee, Sicherheitsbedrohungen
1, Open Source, Juli 2006
2, Cyber-Kriminalität, April 2007
3, Ein Internet, viele Welten, Februar 2008
4, Social Engineering, Oktober 2008
5, Risiko-Management und Compliance, Juli 2009

[714] Wegen der Nachweise siehe unten.

[715] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008;
kostenpflichtiger Download.

C.4 1. McAfee. Analysen zu globalen Sicherheitsbedrohungen

Das Sicherheitsunternehmen McAfee veröffentlicht seit 2006 seine regelmäßigen Analysen über globale Sicherheitsbedrohungen, die seit 2008 als Security Journal fortgeführt werden.

Der erste Report erschien im Juli 2006 und nahm sich zum Schwerpunkt die Open Source-Software und Sicherheitsprobleme, die in ihrem Zusammenhang gesehen werden [716]: Der Preis für die Vorteile von Open Source. Die ablehnende Haltung dürfte von den tatsächlichen Entwicklungen überholt worden sein.

Im April 2007 folgte ein Bericht, der sich ausdrücklich der Cyber-Kriminalität widmete [717]: Die Zukunft der Cyber-Kriminalität. Er greift die Themen aus dem ersten Report wieder auf und aktualisiert sie im Hinblick auf Handyviren, Voice over IP, das Vordringen von Spyware, das unbedarfte Umgehen mit sozialen Plattformen im Internet, das seinerzeit neue Vista von Microsoft und weiteren Themen.

Mich am meisten beeindruckt hat die dritte Analyse zu den globalen Sicherheitsbedrohungen [718]: Ein Internet, viele Welten.

Einzigartig an ihr ist, dass sie in verschiedenen Länderberichten die regionalen Besonderheiten der Cybercrime herausarbeitet und in einen globalen Zusammenhang stellt. Davon hätte ich mir Fortsetzungen gewünscht.

Im Oktober 2008 erschien das Security Journal,

[716] **CF**, globale Sicherheitsbedrohungen, 27.07.2008;
Der Preis für die Vorteile von Open Source, McAfee Juli 2006

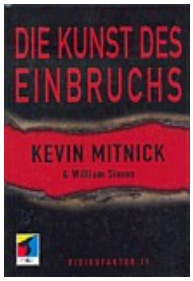
[717] **CF**, Cybercrime, 27.07.2008;
Die Zukunft der Cyber-Kriminalität, McAfee April 2007

[718] **CF**, Länderberichte, 27.07.2007;
Ein Internet, viele Welten, McAfee Februar 2008

Social Engineering in englischer Fassung [719]. Es bildet eine der wesentlichen Grundlagen für meinen Aufsatz über das ▸ Social Engineering.

Dabei handelt es sich um Methoden der Kommunikation, Manipulation und Suggestion - im Bedarfsfall angereichert um Ausspähtechnik, die andere Menschen zu unbedachten Äußerungen oder Handlungen bringen sollen.

Die wichtigsten Ergänzungen zu dem Thema liefern die beiden Bücher von Kevin Mitnick [720].



Das zunächst letzte Security Journal erschien im Juli 2009 [721]: Risiko-Management und Compliance.

McAfee, virtuelle Kriminalität
1, Organisierte Verbrechen und das Internet, Dezember 2006
2, Virtuelle Kriminalität, Dezember 2008
3, Cybercrime and Hacktivism, März 2010

C.4 2. virtuelle Kriminalität und Cyberwar

Außer der Reihe erschien McAfee's Zweite große europäische Studie über das Organisierte Verbrechen und das Internet [722]. Sie lieferte die erste Typenbeschreibung für die Internetkriminalität, die auch im Basar angesprochen wird [723]. Sie stellt nach meinem Eindruck den ersten ernsthaften Versuch dar, die Cybercrime im Zusammenhang mit den handelnden Personen zu bewerten.

Im Dezember 2008 folgte der Bericht von McAfee zum Thema Virtuelle Kriminalität [724]. Er verweist auf die Zunahme staatlicher Auseinandersetzungen im Internet (Cyberwar) und fordert eine koordinierte, grenzüberschreitende Strafverfolgung.

Die beiden Berichte werden ergänzt von der detaillierten Studie vom März 2010, die bislang nur in englischer Sprache vorliegt: François Paget, Cybercrime and Hacktivism [725]. Paget liefert viele Beispiele für mafiöse Strukturen in der Internetkriminalität und für die Verschmelzung von Krimina-

[719] Siehe: **CF**, Überredungstechniken, 23.11.2008;
CF, Security Journal. Social Engineering. 01.03.2009;
Security Journal. Social Engineering, McAfee Oktober 2008

[720] Kevin Mitnick, Die Kunst der Täuschung. Risikofaktor Mensch, Heidelberg 2003;
ders., Die Kunst des Einbruchs. Risikofaktor IT, Heidelberg 2006

[721] Risiko-Management und Compliance, McAfee 10.07.2009;
CF, Berichte und Studien zur IT-Sicherheit, 26.08.2009

[722] Zweite große europäische Studie von McAfee über das Organisierte Verbrechen und das Internet, McAfee Dezember 2006 (ZIP)

[723] Die Grafik zeigt das Titelblatt der von McAfee veröffentlichten Studie. Es handelt sich auch an dieser Stelle um ein Zitat (§ 51 UrhG), das McAfee würdigt und der Berichterstattung dient (§ 50 UrhG). Nutzungsbeschränkungen werden in dem PDF-Dokument von McAfee nicht angegeben. Wegen der Veröffentlichung der Grafik wurde im Sommer 2009 versucht, den Cyberfahnder abzumahnen und eine exorbitante Geldforderung durchzusetzen.

[724] Bericht von McAfee zum Thema Virtuelle Kriminalität, McAfee 08.12.2008

[725] François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010.

lität und staatlich unterstützten Angriffen im Internet.

McAfee, einzelne Studien
Identitätsdiebstahl, Januar 2007
Virtualisierung und Sicherheit, Oktober 2008
Web-Browser, Juni 2009
AutoRun-basierte Malware, Juni 2009
Finanzbetrug und Internet-Banking, Juli 2009
Kennwortdiebe, August 2009
Mapping the Mal Web, November 2009
gefälschte Sicherheitsprodukte, Januar 2010

Neben den umfassenden Studien werden von McAfee auch einzelne Themen aufgegriffen, die die Organisations- und die technische Sicherheit betreffen. Ohne Anspruch auf Vollständigkeit werden hier die Beiträge genannt, die den stärksten Bezug zur Cybercrime haben.

François **Paget**, Identitätsdiebstahl, McAfee 04.01.2007 (ZIP)

Dennis **Elser**, Micha **Pekrul**, Das Geschäft der Kennwortdiebe: Wer ist an Identitätsdiebstahl beteiligt, und wie funktioniert er? McAfee 05.08.2009 [726]

François **Paget**, Finanzbetrug und Internet-Banking: Bedrohungen und Gegenmaßnahmen, McAfee 10.07.2009 [727]

Christoph **Alme**, Web-Browser: Eine neue Plattform wird angegriffen, McAfee Juni 2009

Vinoo **Thomas**, Prashanth **Ramagopal**, Rahul **Mohandas**, Die Zunahme der AutoRun-basierten Malware, McAfee Juni 2009 [728]

Abhishek **Karnik**, Avelino C. **Rico**, Jr., Amith **Prakash**, Shinsuke **Honjo**, Erkennung gefälschter Sicherheitsprodukte, McAfee 04.01.2010 [729]

Zheng **Bu**, Rahul **Kashyap**, Ahmed **Sallam**, Joel **Spurlock**, Rafal **Wojtczuk**, Virtualisierung und Sicherheit, McAfee 31.10.2008 [730]

Shane **Keats**, Dan **Nunes**, Paula **Greve**, Mapping the Mal Web, McAfee 03.11.2009 [731]

Passend zum Thema sind drei Artikel aus der Zeitschrift c't hervorzuheben:

Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007, S. 76

Daniel **Bachfeld**, Dunkle Flecken. Neuartige Angriffe überrumpeln Webanwender, c't 11/2008, S. 83

Daniel **Bachfeld**, Zahl oder Karte. Sicherer Zugriff aufs Online-Konto, c't 17/2008, S. 94

Das Netz der Phisher, September 2006
Underground Economy, August 2009
Update: Underground Economy, April 2010

Die umfassendste und informationsreichste Studie zur Underground Economy im Internet stammt von G Data [732]:

Marc-Aurél **Ester**, Ralf **Benzmüller**, G Data Whitepaper 2009. Underground Economy, 19.08.2009

Das jüngst erschienene „Update“ hat die Strukturen der Schattenwirtschaft noch weiter durchdrungen [733]:

Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

[726] **CF**, Sicherheitsstudien von G Data und McAfee, 03.10.2009
[727] **CF**, Berichte und Studien zur IT-Sicherheit, 26.08.2009
[728] **CF**, Angriffstechniken, 03.07.2009
[729] **CF**, gefälschte Sicherheitsprodukte, 07.02.2010
[730] **CF**, Abwehr und Angriff mit virtuellen Maschinen, 08.03.2009
[731] **CF**, Gefahrenzonen, 04.12.2009
[732] **CF**, Sicherheitsstudien von G Data und McAfee, 03.10.2009
[733] **CF**, neue Hacker-Boards schotten sich ab, 23.05.2010

Lobend muss insoweit auf Jäger hingewiesen werden, der die Grundzüge der Schattenwirtschaft im Internet bereits 2006 beschrieben hat:

Moritz **Jäger**, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.09.2006

Mit dem bekanntesten ▸ Schurkenprovider, dem ▸ Russian Business Network – RBN, setzen sich auseinander:

David **Bizeul**, Russian Business Network study, bizeul.org 19.01.2008

Gordon **Bolduan**, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.;

Frank **Faber**, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008

IT-Sicherheit in Deutschland 2009, März 2009
Verfassungsschutzbericht 2008, Mai 2009

Mit der Sicherheitslage im Allgemeinen setzen sich auseinander:

BSI, Die Lage der IT-Sicherheit in Deutschland 2009, BSI 03.03.2009

BMI, Verfassungsschutzbericht 2008, Vorabfassung 19.05.2009

D. Schluss

D.1 Lehren

⇨ Grundsätzlich ist jede Schnittstelle zu einem Netz oder zum Anschluss von Peripheriegeräten für physikalische oder netzbezogene Angriffe geeignet. Das gilt besonders dann, wenn die Schnittstelle über eigene Verarbeitungskomponenten (Betriebssystem, Prozessor) und Massenspeicher verfügt.

⇨ Netzbezogene Angriffe erfolgen in aller Regel unter Ausnutzung von Schwachstellen (Exploits) oder mit Dateien, die über das Netz oder externe Datenträger zugeliefert werden.

⇨ Injektion (Zulieferung), Infektion (Grundinstallation) und Installation (Einbindung, Tarnung, Update) von Malware nutzen neben technischen Schwachstellen auch menschliche Schwächen aus, um technische Sicherungsmaßnahmen (Rechtesteuerung, Firewall, Virenscanner) zu überwinden und Umzurüsten (Deaktivierung von Virenscannern, Reservierung von Ports, Veränderung der internen Host-Tabelle).

⇨ Der persönliche Zugang zu Mitarbeitern dient auch dazu, Interna zu erkunden, die entweder für sich von Wert sind (Geschäfts- und sonstige Geheimnisse) oder dazu genutzt werden können, Zugang zu geschützten Bereichen zu erlangen (Passwörter, Peripheriegeräte, Hintertüren, Zugangsrechte).

⇨ Malware dient fast immer auch dazu, persönliche Geheimnisse zu erforschen (Botsoftware) oder unmittelbar zu missbrauchen (Phishing). Die häufigsten Erscheinungsformen dienen dem Auskundschaften – vor Allem im Zusammenhang mit dem Online-Banking – und zur Übernahme in ein Botnetz.

⇨ Handelswert haben alle persönlichen Daten und vor Allem Zugangsdaten zu persönlichen Konten, mit denen Geschäfte oder die Kommunikation abgewickelt werden (geschlossene Nutzerkreise, Handelsplattformen, Warenverkehr).

⇨ Die Cybercrime-Szene scheint stark differenziert zu sein. Neben vielen Einzelpersonen, die eher als Trittbrettfahrer tätig sind, haben sich Spezialisten herausgebildet, die auch eigene Strukturen der ständigen Zusammenarbeit entwickelt haben (Operation Groups). Dazu gehört vor Allem die Entwicklung von Malware, bei der Exploit-Händler, Toolkit-Entwickler und die Programmierer der Malware zusammenarbeiten, und von Bot-Software.

⇨ Botnetze sind das mächtigste Werkeug, das den Cyber-Tätern zur Verfügung steht. Sie verlangen nach einer ständigen Aktualisierung nicht nur im Hinblick auf ihre Funktionalität, sondern auch zur Tarnung. Außerdem bedürfen Botnetze der Administration, Wartung und der Einrichtung für kriminelle Einzelaktionen. Das macht eine ständige und arbeitsteilige Zusammenarbeit mehrerer Personen nötig, wobei sich weitere Spezialisten um die Vermarktung und Beutesicherung kümmern dürften.

⇨ Auch wenn sich die Underground Economy von der Öffentlichkeit abschottet (Boards), muss die Infrastruktur für Kommunikationsplattformen, Webshops, Drob Zones und Datenspeicher von spezialisierten Schurkenprovidern zur Verfügung gestellt werden. Sie tarnen sich und ihre Kunden, sind aber zwangsläufig an das Internet und in wirtschaftliche Beziehungen eingebunden, so dass sie darüber identifiziert werden können.

⇨ Ebenso wie die Täter im Bereich der Cybercrime muss auch die Strafverfolgung grenzüberschreitend sein. Die bereits gemachten Erfahrungen lehren, dass das möglich, aber aufwändig ist.

D.2 Cyberfahnder

Seit 2007 berichtet der ▸ Cyberfahnder über die Informations- und Kommunikationstechnik, die Cybercrime und die Ermittlungen gegen sie. Dieses Arbeitspapier stellt die wichtigsten Beiträge aus der Webseite vor, die sich mit der Technik, den Erscheinungsformen und den Strukturen der Cybercrime befassen.

Eine Reihe von Aussagen sind spekulativ und werden aus nur wenigen Fakten, ihrem Zusammenspiel und Erfahrungswerten abgeleitet. Die schnelllebige Entwicklung der IKT und der Cybercrime erfordern ein solches Vorgehen, um Abwehrstrategien und Vorsichtsmaßnahmen zu entwickeln. Bereits die dreijährige Erfahrung zeigt, dass viele Prognosen, die sich besonders auf die für Angriffe geeigneten Schnittstellen bezogen haben, bewahrheitet haben.

Ein weiterer Schwerpunkt des Cyberfahnders ist das Skimming [734], dem ein eigenes Arbeitspapier gewidmet ist:

Dieter **Kochheim**, Arbeitspapier Skimming #2, März 2010 [735]

Ältere Arbeitspapiere beschäftigen sich ebenfalls mit besonderen Aspekten der Cybercrime [736]:

Dieter **Kochheim**, Phishing, 22.01.2007 [737]

Dieter **Kochheim**, Grenzüberschreitender Transfer von Vermögenswerten, 15.05.2007 [738]

Dieter **Kochheim**, IT-Strafrecht. Zusammenfassung, 02.11.2007 [739]

Dieter **Kochheim**, Onlinedurchsuchung, 11.03.2007 [740]

---

[734] **CF**, arbeitsteiliges Skimming, 08.05.2008

[735] **CF**, Zwischenbilanz: Skimming, 14.11.2009

[736] **CF**, Cybercrime und IT-Strafrecht, 08.08.2008

[737] **CF**, Phishing, 2007

[738] **CF**, grenzüberschreitender Vermögenstransfer, 2007

[739] **CF**, IT-Straftaten, 2007;
CF, IT-Strafrecht, 2007

[740] **CF**, Onlinedurchsuchung, 2007;
CF, Bundesverfassungsgericht: Onlinedurchsuchung, 05.04.2008