StPO).

Das Beispiel lehrt, dass sich auch in Strafanzeigen wegen kleinerer Schäden Teile einer groß angelegten Straftat verbergen können, die nur dann angemessen beurteilt werden kann, wenn ihre Teilakte im Rahmen der Strafverfolgung zusammen geführt werden. Die dazu nötigen Mechanismen, vor allem Melde- und Analysedienste, sind bis heute unvollständig. Allerdings ist die Sensibilität bei den polizeilichen Fachbehörden erheblich gestiegen, so dass jedenfalls erwartet werden kann, dass der klassische Rückruftrick angemessen bearbeitet wird.

2.3 Hacking und Malware

Im Vorgriff auf die besonderen Erscheinungsformen der IuK-Kriminalität müssen die Phänomene und Methoden grundsätzlich betrachtet werden, weil sie in Varianten immer wieder auftauchen.

Noch heute währt eine ideologische Auseinandersetzung über die vor 50 Jahren entstandene Hackerkultur an, wobei sich die Hackerszene von den bedenkenlosen Skript-Kiddies, die unbedacht und skrupellos mit zerstörerischen Werkzeugen hantieren, ohne sie selber entwickelt zu haben oder sie zu beherrschen, von den Crackern, die vor allem Zugangssicherungen zu Programmen und Systemen durchbrechen, um kostenpflichtige Programme oder Dienste ohne Entgelt nutzbar zu machen, und von den Kriminellen abgrenzt, die mit Profitinteresse Malware herstellen, verkaufen und pflegen, Botnetze betreiben, Phishing und andere Formen des Identitätsdiebstahls [41] praktizieren. Darin kommt ein gutes Teil Hilflosigkeit zum Vorschein, weil alle, die „Guten“ wie die „Bösen“, dieselben Methoden, Werkzeuge und Angriffsziele verwenden und sich allenfalls im Motiv unterscheiden. Das zeigt ganz besonders die Auseinandersetzung um das Hackerkollektiv Anonymous [42].

Hacking und Malware stellen die beiden grundlegenden Strategien dar, mit denen die Penetration bei der IuK-Kriminalität betrieben wird. Beim Hacking erfolgt ein individuell gesteuerter Angriff gegen informationsverarbeitende Systeme mit dem Ziel, in sie einzudringen und zu penetrieren. Der nähere Zweck der Einflussnahme orientiert sich an den Motiven des Hackers und kann wegen des technischen Vorgehens offen bleiben.

Die Spannbreite der Akteure und ihrer Motive reicht von berechtigten Auftragsarbeiten von Sicherheitsunternehmen über wohlmeinende, sich aufdrängende Experten bis hin zu Datendieben, Industriespionen und zerstörungswütigen Vanda-

---

41 Siehe: Identitätsdiebstahl und Phishing, in: Dieter **Kochheim**, Cybercrime, 24.06.2010, S. 45.

42 **CF**, IT-Söldner im Kampfeinsatz, 15.02.2011; Dieter **Kochheim**, Eskalationen, 20.02.2011.

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

1976 ist deshalb ein Meilenstein, weil erstmals die Hacking-Kultur einen Namen bekam und ihr spezifischer Sprachgebrauch dokumentiert wurde.

Dieter **Kochheim**, Eine kurze Geschichte der Cybercrime, 23.01.2011, S. 8

len (Hacktivismus [43], Defacement [44], Erpressung, kalter Cyberwar [45]).

Der Einsatz von Malware [46] zeichnet sich dadurch aus, dass ein Programm in das Zielsystem geschleust wird, dessen Sicherheitsvorrichtungen unterläuft und abschaltet und sich schließlich einnistet und tarnt. Die weitere Penetration hängt von der Gestalt des Programms und den Motiven des Entwicklers ab. Die wichtigsten Gestaltungen betreffen den Betrieb eines Botnetzes [47], das Phishing [48] und neuerdings die Industriespionage (Night Dragon [49]).

Neben den Penetrationsstrategien sind im Zusammenhang mit der IuK-Kriminalität weitere Erschei-

Schadcode wird von Kriminellen über mehrere Wege verbreitet: Eine Möglichkeit ist das Hinterlegen von schädlichen Programmen auf Internetseiten. Schon der reine Besuch einer verseuchten Webseite reicht dabei aus, um den Computer über sogenannte Drive-by-Downloads mit Viren, Trojanern, Spionageprogrammen und weiterer Malware zu infizieren. Auf diese tückischen Internetseiten trifft der Nutzer entweder beim Surfen im Netz oder die URLs werden von den Tätern z. B. in sozialen Netzwerken oder durch Nachrichten in Chat-Programmen publiziert. Online-Kriminelle nutzen auch weiterhin Spam-Mails, um Anwender mittels Links auf präparierte Webseiten zu locken oder sie zu animieren verseuchte Dateianhänge zu öffnen. Im Mail-Anschreiben ist dann beispielsweise die Rede von einer vermeintlichen Rechnung oder Mahnung oder es werden exklusive Fotos zu einem aktuellen Ereignis versprochen. Kommen die Anwender der Aufforderung nach, gelangen sie direkt auf die Schadcode-Seiten und fangen sich unbeabsichtigt einen Computerschädling ein.

G Data Security Studie 2011. Wie schätzen Nutzer die Gefahren im Internet ein? 20.06.2011

nungsformen zu beobachten. Sie reichen von verteilten Angriffen (DDoS) über Schutzrechteverletzungen, Verbreitung verbotener Inhalte und von ideologischen Entgleisungen bis hin zur (straflosen) Datenhehlerei und schlichten Betrügereien. Einzelne davon werden noch angesprochen. Zunächst geht es jedoch nur darum, wie eine Penetration abläuft und wie sie als solche strafrechtlich begriffen werden kann.

---

[43] Dieter **Kochheim**, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010

[44] Dieter **Kochheim**, Eskalationen, 20.02.2011, S. 24.

[45] Dieter **Kochheim**, Cybercrime – Cyberwar, 02.07.2011

[46] **CF**, Malware, 12.05.2008

[47] **CF**, Botnetze, 2007

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

[49] **CF**, Night Dragon, 13.02.2011

2.3.1 Malware, Datenträger und Anhänge

Ein informationstechnisches System kann grundsätzlich nur über eine Schnittstelle penetriert werden [50]. Dazu kommen alle Formen von Wechseldatenträgern (Disketten, USB-Sticks, Wechselfestplatten, Speichersticks aus Kameras und Handys und selbst Magnetkarten [51]) in Betracht, vor allem aber die Verbindungen zum Internet selbst, das Funknetz (WLAN) und sogar ein separater Telefonnetzanschluss, wenn er über die Telefonanlage mit der Datenverarbeitung verbunden ist. Schließlich bieten auch alle Formen der Nahfunkverbindungen (Infrarot, Bluetooth und andere) und der Kabelanschluss einen denkbaren Einstieg, sogar das Stromnetz, wenn mit ihm eine Datenverbindung geliefert wird.

Das Transportmittel sind Dateien und Programme, die hier als Malware bezeichnet werden. Sie definiert sich als fremde Software, die die Systemintegrität angreift, um eine bösartige Aktion auszuführen. Die Bösartigkeit kann zerstörerisch sein (Dateien löschen, System unbrauchbar machen), ausforschend (Keylogger, Suche nach persönlichen Daten und Geheimnissen) oder missbräuchlich (▸ modernes Phishing, ▸ Einbindung in ein Botnetz). Von ihrer Form her werden unterschieden:

▷ Viren sind die älteste Form. Sie binden sich in eine bestehende Datei ein und bewirken ihre schädliche Funktion dadurch, dass sie zusammen mit ihr ausgeführt werden. Schon diese einfachsten Formen der Malware wurden mit intelligenten Eigenschaften versehen. Sie konnten sich in den Startvorgang einbinden (Bootviren) und sich tarnen (Stealthviren), indem sie den Zeitstempel der angegriffenen Datei und vor allem ihre Größe erhalten haben [52].

Angriffsebene

- **Systemstart** (BIOS, EPROM)
- **Booten** (Betriebssystem, Kernel)
- **Programmumgebung** (Betriebssystem)
- **Anwenderoberfläche** (Windows, Linux)
- **Anwenderprogramme** (Office, Adobe, Browser)
- **laufender Betrieb** (Java, active X)

▷ Würmer sind selbständige Dateien, die einen laufenden Arbeitsprozess dazu ausnutzen, ihrerseits ausgeführt zu werden.

▷ Trojaner verstecken sich hinter einem nützlichen Dienstprogramm, das oberflächlich ausgeführt wird, und entfalten im Hintergrund ihre bösartigen Aktivitäten.

▷ Kommandostrings (Payload) sind kleine Kommandofolgen, die einen Internet-Browser oder ein anderes Anwenderprogramm dazu veranlassen, die Malware aus dem Internet zu laden.

Für die rechtliche Auseinandersetzung sind solche Definitionen fast ohne Bedeutung. Moderne Malware nutzt alle Erscheinungsformen, wechselt zwischen ihnen und ändert ihre Gestalt. Darauf kommt es rechtlich nicht an, weil nach ihrem Vorgehen und ihren Wirkungen zu fragen ist.

Das IT-Strafrecht orientiert sich an diesen Auswirkungen. So wendet sich § 202a Abs. 1 StGB gegen das Ausspähen von Daten. Trotz der formellen Datendefinition in § 202a Abs. 2 StGB darf nicht unbeachtet bleiben, dass die Vorschrift in dem Abschnitt über die „Verletzung des persönlichen Lebens- und Geheimbereichs“ angesiedelt

---

[50] Alle – auch fernliegenden – Schnittstellen, die ich 2007 angesprochen habe, sind inzwischen zumindest als Übertragungsweg ausprobiert worden. Siehe: **CF**, IT-Sicherheit, Schwachstellen, Angriffe, 2007.
Stuxnet wendet sich destruktiv gegen Industrieanlagensteuerungen und wurde nur über USB-Sticks in die angegriffenen Systeme eingebracht. Die gegenwärtige Entwicklung, vor allem individualisierte Angriffe zum Zweck der Informationsspionage durchzuführen, macht auch „schwierige“ Schnittstellen wie den Nahfunk attraktiv, weil dazu sowieso alle Einzelschritte genau geplant und an die Gegebenheiten des einzelnen Zielsystems angepasst werden müssen. Dass die Tendenz genau in diese Richtung geht, hat der Night Dragon-Angriff gezeigt.

[51] Das ist bislang nur eine theoretische Überlegung. Der Magnetstreifen einer Identifikationskarte verfügt über genügend Kapazität, um einen Starterstring zu beherbergen.

[52] Einzelheiten bei G Data, Malware-Geschichte (drei Teile).

ist und keine Strafbarkeit des Versuchs kennt. Deshalb kommt es nicht nur darauf an, dass der Angreifer überhaupt Daten, *die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind*, erlangt, sondern auch darauf, dass sie grundsätzlich einen gewissen Geheimniswert haben und nicht öffentlich präsentiert werden (Einzelheiten unter ▸ 2.3.3.2).

§ 303a StGB über die Datenveränderung ist hingegen im Sachbeschädigungsrecht angesiedelt. Das führt dazu, dass nicht jede Datenveränderung strafbar ist, sondern nur die, die tatsächlich zu Daten- und Funktionsverlusten führt. Die Computersabotage (§ 303b StGB) lässt jedoch bereits die Zuleitung von Malware als Tathandlung genügen (Einzelheiten unter ▸ 2.3.3.1).

Die Fälschung beweiserheblicher Daten (§ 269 StGB) ist ein Teil des Urkundenfälschungsrechts. Das wiederum hat zur Folge, dass ihre Beweisbedeutung ausschlaggebend ist. Das setzt voraus, dass sie mit einer Person als Aussteller (der Urkunde) in Verbindung stehen müssen, der mit ihnen eine Aussage treffen will, die zumindest mittelbar eine Rechtsfolge betrifft. Daran ändert auch § 268 StGB über die Fälschung technischer Aufzeichnungen nichts. Beide Vorschriften schützen nur verschiedene – menschliche oder automatische – Verarbeitungsprozesse und verlangen gleichermaßen, dass die Daten Bedeutung für Rechtsfolgen haben müssen.

Schließlich wendet sich der Computerbetrug (§ 263a StGB) nicht gegen jede missbräuchliche oder täuschende Datenverwendung, sondern nur gegen die, die das Vermögen des berechtigten Dateninhabers beeinträchtigen kann.

Ausschlaggebend sind also die tatsächlichen und rechtlichen Folgen, die mit dem Einsatz von Malware verbunden sind. Dazu reicht die Tatsache, dass schädlicher Code angeliefert wird, nicht aus. Er muss auch gelesen werden, um zunächst in den Arbeitsspeicher des Zielgerätes zu gelangen (Injektion). Dazu bedarf es Tricks und vor allem einer Ablaufumgebung, in die sich der schädliche Code einbinden und seine eigenen Funktionen

Angriffsprozess:

Über eine ▸ ***Außenverbindung*** muss schädlicher Code in den Hauptspeicher des Zielsystems eingebracht (▸ ***Injektion***) und dort so verarbeitet werden, dass seine Funktionen ausgeführt werden (▸ ***Infektion***). Dazu wird eine Sicherheitslücke missbraucht (▸ ***Exploit***), die die Malware dazu nutzt, sich zu ▸ ***installieren***. Dazu erkundet sie in aller Regel die Umgebungseigenschaften und lädt von einem ▸ ***Command and Control-Server*** im Internet Updates und weitere Programmbestandteile. Anschließend versucht sie sich zu tarnen. Dazu kommen ▸ ***Rootkits*** zum Einsatz, also Programmpakete, die vorhandene Sicherheitseinrichtungen abschalten oder unterlaufen, mit denen die Malware zum jeweiligen Neustart eingebunden (▸ ***Einnisten***) und vor Entdeckung getarnt wird. So präpariert kann die Malware ihre schädlichen Funktionen ausführen, kann das System nach wertvollen Informationen durchsuchen (Lizenzschlüssel, Kontodaten, Zugangscodes), Arbeitsprozesse überwachen (Keylogger) und andere Aktionen steuern (Phishing, Botnetze, DDoS, Spams). Ganz häufig wird dabei auch eine Hintertür eingerichtet (▸ ***Backdoor***), die der Angreifer direkt dazu nutzen kann, das angegriffene System als Konsole für geheime Aktivitäten zu nutzen.

ausführen lassen kann (Infektion). Solche Ablaufumgebungen stellen handelsübliche Computer in reicher Anzahl.

Am Anfang des Starts wird das BIOS ausgeführt [53]. Es lädt die Treiber für die angeschlossene Hardware (Tastatur, Maus, Hauptspeicher [Arbeitsspeicher] und Massenspeicher [Festplatte usw.]) und startet das Betriebssystem. Seine Anweisungen und Einstellungen bekommt das BIOS in aller Regel von einem Speicherchip, der Daten auch ohne Stromversorgung speichern kann (zum Beispiel EPROM [54]). Die Chips sind speicherfähig und bieten damit die erste Gelegenheit, fremden Code in einen Verarbeitungsvorgang einzubringen [55].

---

[53] basic input/output system - BIOS

[54] Erasable Programmable Read-Only Memory - EPROM

[55] Das gilt auch für alle Schnittstellen, zum Beispiel für die Grafik-, Sound- oder TV-Karte, die auf Systemebene betriebsbereit gemacht werden.

Zur Infektion muss mehr geschehen, als den Code nur in den Arbeitsspeicher einzubringen. Der Computer muss auch einen Anlass haben, ihn zu verarbeiten. Die erste richtige Gelegenheit dazu bietet sich beim Booten des Betriebssystems. Es wird, gesteuert vom BIOS, von einem Massenspeicher geladen (interne Festplatte, externe Medien wie CD, DVD, USB-Stick) und richtet die Grundfunktionen des Computers ein. Das geschieht in der Regel zweistufig. Für die Feinsteuerung der Hardware ist der Betriebssystemkern (Kernel) verantwortlich und im zweiten Schritt werden die grundlegenden Programmroutinen installiert. Anschließend erfolgt in aller Regel die Einrichtung der Anwenderoberfläche, das heißt die Einrichtung der grafischen Bildschirmoberfläche, womit die wichtigsten Grundfunktionen des Computer zusammen geführt werden. Zeitgleich oder danach werden auch die Anwenderprogramme eingerichtet, die das Arbeiten (oder den Spaß) am Computer erst ermöglichen (Office, Browser für das Internet, Spiele).

Um aber überhaupt in den Verarbeitungsprozess zu gelangen, muss die Malware eine Sicherheitslücke ausnutzen (Exploit), also einen nicht oder nur schwach überwachten Arbeitsprozess im Computer. Am wenigsten geschützt ist der erste Startvorgang und es hat tatsächlich schon Viren gegeben, die das BIOS überschrieben und zerstörerische Wirkungen entfaltet haben (Festplatte formatieren). Die Möglichkeiten für die Installation und Inbetriebnahme ausgefeilter Malware sind jedoch auf dieser Ebene begrenzt. Moderne Betriebssysteme und Antivirusprogramme überwachen bereits den Bootvorgang im Hinblick auf Unregelmäßigkeiten, ungewöhnliche Ablaufprozesse (Heuristik [56]) und den Start unbekannter Programme. Das ist auch nötig, weil sich besonders ausgefeilte Malware in den Bootvorgang einzubringen versucht, indem Treiberdateien verändert, ausgewechselt oder hinzugefügt werden.

Bevor es dazu kommt, muss die Malware zunächst Ablaufprozesse infizieren und sich als Programm installieren. Am häufigsten werden dazu Exploits auf der Ebene der Anwenderprogramme missbraucht. Dazu werden ganz häufig die Anhänge zu E-Mails genutzt. Sie sind funktionstüchtige Dateien, die mit ihrem Suffix [57] die Anwendungsumgebung anfordern, die sie ausführen kann. Diese Umgebungen lassen vielfach umfangreiche und tiefe Programmabläufe zu, so dass sie dazu missbraucht werden können, ein fremdes Programm zu installieren [58]. Gegenwärtig fußen die meisten Missbräuche auf dem Acrobat Reader von Adobe und auf der Laufzeitumgebung Java von Oracle (vormals Sun) [59]. Die Browserhersteller (MS Outlook, Thunderbird u.a.) haben darauf reagiert und lassen in aller Regel keinen automatischen Start von E-Mail-Anhängen zu.

Ein wichtiges Einfallstor liefern die Browser für die Anzeige von Internetseiten (Internet Explorer, Firefox u.a.). Diese beruhen ganz überwiegend auf der einfachen Skriptsprache Hypertext Markup Language – HTML, die nur wenige Möglichkeiten zum Missbrauch bietet. Eine beliebte davon sind die „iFrames“. Frames bieten die Möglichkeit, verschiedene Seiten zur gemeinsamen Ansicht zu kombinieren, zum Beispiel dazu, einen Bereich des Bildschirms fest zur Navigation zu bestimmen und einen anderen als Textcontainer, der für sich rauf- und runtergeskrollt werden kann. Dazu wird zunächst eine Datei geladen, die Fenster definiert und die ausfüllenden Dateien lädt. Dasselbe geschieht mit eingebetteten Frames, also mit iFrames. Sie definieren auf einer Seite ein Fenster, in dem eine andere Datei angezeigt wird und laden

[56] Antivirenprogramm. Heuristik

[57] Suffix ist die Zeichenfolge, die dem Dateinamen nach einem Punkt rechts angefügt ist. „doc“ steht zum Beispiel für Microsoft Office Word, „pdf“ für den Acrobat Reader von Adobe und „htm“ (html) für eine browserfähige Datei in der Skriptsprache Hypertext Markup Language.

[58] Anschauliche Beispiele für das Einnisten der Malware hat die Zeitschrift c't 2010 in der Artikelserie „Tatort Internet“ vorgestellt. Die Serie wurde 2011 wieder aufgenommen und konzentriert sich jetzt auf die Angriffswege. Bislang ist davon aber nur eine Folge im Internet veröffentlicht worden: Jasper **Bongertz**, Tatort Internet. Nach uns die SYN-Flut, Heise Security 03.08.2011.

[59] Kaspersky-Studie: Adobe-Software größtes Sicherheitsrisiko, Heise online 16.08.2011

diese gleichzeitig [60]. Die Größe der Anzeige lässt sich einstellen und kann auch in Breite und Höhe auf Null gestellt werden. Dann lädt der Browser eine Datei, die nicht angezeigt wird, und es kann sich um Malware handeln, die zunächst den Browser und damit auch den Hauptspeicher mit schädlichem Code injeziert. Daneben lässt HTML auch die Einbindung von Multimedia-Elemeten zu (Bilder, Sounds, Videos, Flash-Animationen), die ihrerseits mit Malware infiziert sein können. Das meiste davon fangen die aktuellen Browser und Antivirenprogramme ab, wenn sie auf aktuellem Stand und die betreffenden Exploits eingestellt sind [61].

Malware – egal zu welchem Zweck – nistet sich in aller Regel durch Exploits im laufenden Betrieb (Internetbrowser, Java), in verbreiteten Anwenderprogrammen (Acrobat Reader) oder in allen Verarbeitungsstufen über Wechseldatenträger ein. Meistens werden dazu die nötigen Programmteile und Updates aus dem Internet geladen und im angegriffenen System installiert. In diesen Fällen kann der schädliche Code in einem relativ kurzen Kommandostring bestehen, der das Anwenderprogramm zum Laden des noch im Internet vorgehaltenen Programms anweist. Erst dann nistet sich die Malware dauerhaft im System ein und das bevorzugt auf der Ebene des Betriebssystems und seltener (aber effektiver) auf der Ebene des Kernels. Dazu trägt es sich zum Beispiel in die Auto-Start-Bereiche der Registry unter Windows, in andere AutoStart-Dateien oder in Laufzeit-Bibliotheken ein, die beim Booten oder dem Start von üblichen Anwenderprogrammen ausgeführt werden. Seine Programmbestandteile versteckt sie mit Hilfe von Rootkits in den System- oder anderen Dateien, von denen erwartet wird, dass sie selten oder nie durchleuchtet werden. Kernfunktionen der Malware, die sich durch ihre Funktionalität verraten könnten, werden dazu häufig verschlüsselt.

---

[60] Das Gästebuch des Cyberfahnders ist ein praktisches Beispiel für einen iFrame.

[61] Bislang ganz unbekannte Schwachstellen werden auch Zero-Day-Exploits genannt. Das bedeutet, dass sie zuvor Null Tage bekannt waren, bevor sie von einer Malware missbraucht werden. Die mangelnde Aussagekraft dieses Begriffes wird von Muttik von McAfee zu recht kritisiert: **CF**, Zero-Day-Exploits und die heile Hackerwelt, 06.11.2010. Auch solche Exploits können anhand ihrer Abläufe und Wirkung erkannt werden (Heuristik).

2.3.2 fortgeschrittene Techniken

Die Beiträge in diesem Kapitel widmen sich aktuellen Erscheinungsformen beim Einsatz von Malware. Ihnen geht es darum, die hohen Entwicklungsstände der Malware-Technik und die detaillierten und professionellen Ablaufplanungen der Angreifer zu veranschaulichen.

Die ersten beiden Erscheinungsformen sind allgemeiner Art und offenbaren besonders die Rücksichtslosigkeit, mit der IuK-Kriminelle Malware zu ihren Zwecken einsetzen.

Das Thema ▸ Phishing beschränkt sich hier auf ein Beispiel des Identitätsdiebstahls beim Onlinebanking und könnte zu vielen Varianten ausdifferenziert werden. Es hebt sich von vielen anderen Beispielen dadurch hervor, dass die kriminelle Aktion nur im Zusammenspiel zwischen einer hochentwickelten Malware auf dem Computer des Betroffenen und einem Command and Control-Server – C&C – abgewickelt wird, ohne dass es seitens des Angreifers noch eines menschlichen Zutuns bedarf. Bei dem Text handelt sich um eine Zusammenfassung vieler Meldungen in Onlinediensten, der Tagespresse und polizeilichen Erfahrungen.

Beim Identitätsdiebstahl geht es immer darum, persönliche (Echt-) Daten mit dem Ziel auszuspähen, 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 [62]. 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, bei Warenhäusern, Informationsdiensten (Fachinformationen, Zeitungen, Wetterdienst), virtuellen Veranstaltungen wie Second Life oder geschlossene Spiele, zu Versanddiensten wie DHL, UPS und Packstationen sowie schließlich zum Onlinebanking und anderen Bezahldiensten wie PayPal, E-Gold und WebMoney. Angegriffen und missbraucht werden alle Dienste, mit denen werthaltige Leistungen ertrogen oder erschlichen werden können.

Die Funktionsweise von ▸ Botnetzen ist schon an anderer Stelle breit beschrieben worden [63], so dass hier nur eine Zusammenfassung und Würdigung erfolgt.

Die vier weiteren Beispiele widmen sich aktuellen Malware-Projekten, die 2010 und 2011 öffentlich bekannt geworden sind. Sie sind hochgradig professionell und richten sich immer ganz gezielt gegen ausgesuchte Unternehmen und Organisationen, wobei nicht nur besonderes Wissen über die Konstruktion von Malware als solche nötig ist, sondern auch über den internen Technikeinsatz, die innere IT-Struktur und die Unternehmensorganisation.

Eine hervorgehobene Rolle spielt dabei ▸ Stuxnet. Diese Malware ist wahrscheinlich mit einem beispiellosen finanziellen Aufwand speziell dazu entwickelt worden, die Atomanreicherungsanlagen im Iran zu sabotieren. Sie hebt sich von kriminellen Angriffen dadurch ab, dass sie sich über Speichermedien verbreitet, mehrere hochwertige Exploits und Rootkits zur Infektion, Einnistung und Ausführung einsetzt und schließlich ganz langfristig und gezielt Industrieanlagensteuerungen der Firma Siemens sabotiert. Der Angriff gegen solche Steuerungen ist bislang beispiellos.

Die übrigen drei Projekte betreffen groß angelegte Formen der Industriespionage, die jeweils Besonderheiten aufweisen. ▸ Shady RAT ist erst im Frühjahr 2011 nach fünf Jahren Laufzeit öffentlich bekannt geworden. Es richtet sich gegen weltweit 72 Unternehmen und Organisationen und hebt sich auch dadurch hervor, dass eine unvorstellbare Datenmenge gestohlen wurde (vermutet in Petabyte-Größe).

▸ Aurora richtete sich Ende 2009, Anfang 2010 ge-

---

62 Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 45, m.w.N.

63 Dieter **Kochheim**, Cybercrime, 24.05.2010, S. 55

gen Google und 30 weitere Unternehmen, die bevorzugt in China engagiert waren. Die Ausführung kann als klassisches Beispiel für einen Malware-Angriff gesehen werden, mit dem sich der Angreifer eine Hintertür (Backdoor) zu Firmennetzen verschafft, um dann Unternehmensgeheimnisse zu stehlen. Wegen seiner Anschaulichkeit wird anschließend anhand des ▸ Aurora-Beispiels das IuK-Strafrechts im engeren Sinne praktisch angewendet.

Den fortschrittlichsten Angriff zeigte der ▸ Night Dragon. Er hebt sich dadurch hervor, dass die Angreifer nicht nur zielgenau in die Firmennetze von petrochemischen Unternehmen eingedrungen, sondern aus dem Innern der Unternehmen heraus über gesicherte VPN-Tunnel direkt auf die Laptops leitender Firmenangehöriger gelangt sind.

2.3.2.1 Phishing

Die Zeiten, in denen unbedarfte Homebanking-Kunden mit E-Mails dazu aufgefordert wurden, ihre Zugangsdaten und TAN zu offenbaren [64], sind längst vorbei. Die dazu verwendeten Überredungstechniken (Social Engineering [65]) kommen heute immer noch in anderen Zusammenhängen zum Einsatz [66]. Modernes Phishing funktioniert hingegen als Man-in-the-Middle-Angriff, bei dem die Malware die zentrale Rolle spielt.

Die eingenistete Malware wartet darauf, dass der Anwender eine der bekannten Homebanking-Webseiten aufruft. Seine Zugangsdaten fängt sie ab und sendet sie an einen Command and Control-Server - C&C, der sich seinerseits mit den Zugangsdaten bei der Bank einloggt. Die heute üblichen Captchas [67], kleine Bilder, die Ziffern und Zeichen nur verzerrt wiedergeben, können den Zugang erschweren, so dass der Anwender die Zugangsdaten auch selber eingeben darf und erst dann gekappt wird. Ganz viele individuelle Daten – Name, Kontonummer, Kontostand und letzter Besuch – offenbaren die Homebanking-Portale von sich aus. Sie sendet der C&C mit der üblichen Begrüßungsseite an den Anwender. Dabei gaukelt er eine sichere „shttp“-Verbindung mit dem Server der Bank vor.

Das weitere Vorgehen variiert. Gelegentlich sendet der C&C jetzt einen Sicherheitshinweis: Wir haben das Homebanking grandios sicher gemacht. Um die neuen Sicherheitsfunktionen nutzen zu können, geben Sie bitte die iTAN Nummer soundso ein! Derweil hat der C&C eine Überweisung an Igor Popow vorbereitet und fragt genau die iTAN ab, die er zur Bestätigung der Überweisung braucht. Die Rückmeldungen der Bank werden vom C&C unterdrückt und die Startseite der Bank so präsentiert, als wäre die

---

64 So noch: **CF**, Phishing, 2007

65 **CF**, Fünf unwichtige Informationen ergeben eine sensible, 01.03.2009

66 Sabrina **Berkenkopf**, Ralf **Benzmüller**, Gefährliche E-Mails, G Data Whitepaper 6/2011, 01.06.2011

67 CAPTCHA

Überweisung nie geschehen.

Der Anwender gibt seine eigenen Überweisungsdaten ein und das böse Spiel wiederholt sich. Der C&C fängt die eingegebenen Daten ab und generiert seine Transaktion an Vladimir Vostok. Die Bank fordert eine neue iTAN und der C&C verwendet die vom Anwender eingegebenen Daten, um ihm die Rückmeldung der Bank vorzugaukeln und zur Eingabe eben dieser iTAN aufzufordern. Damit bestätigt der C&C die Überweisung an Vostok und wandelt die Rückmeldung so um, als wäre des Anwenders Anweisung ausgeführt worden. Das lässt sich beliebig wiederholen. Sobald der Anwender das Homebanking-Portal verlässt, kappt die Malware die Internetverbindung und ändert die lokale DNS-Tabelle (die in die Registry eingebunden ist), so dass beim Besuch der eigenen Bank nur noch eine Fehlerseite aufgerufen wird.

Merken das die Banken nicht? Doch, sie setzen Prüfmechanismen ein und können ungewöhnliche Aktivitäten erkennen. Der C&C steht zwar womöglich in der Ukraine, aber zum Zugang zur Bank nutzt er einen Zombie aus einem Botnetz aus der räumlichen Nähe des Anwenders als Konsole. Zahlungsempfänger ist auch nicht Igor Popow in Odessa, sondern Waltraut Meier in Oberhausen oder Zicherie. Sie leitet das Geld als Finanzagentin auf verschlungenen Wegen an Popow weiter. Ihr Konto wird später mit dem Überweisungsbetrag rückbelastet und sie wegen leichtfertiger Geldwäsche mit Geldstrafe bestraft (§ 261 Abs. 5 StGB). Finanzagenten sind Kanonenfutter und können nur wenige Male eingesetzt werden. Deshalb sind die Täter auch dazu übergegangen, (im Ergebnis erfolglos) Arbeit suchende Polen Bankkontos im Inland eröffnen zu lassen oder Konten unter falschen Identitäten zu errichten. Ausweispapiere, Post-Ident-Unterlagen und Gehaltsbescheinigungen lassen sich dank PhotoShop leicht fälschen und einfach verwenden, wenn die Bank die Übermittlung als Fax-Kopie akzeptiert [68].

[68] Was regelmäßig eine Verurteilung wegen Urkundenfälschung (§ 267 StGB) – Gebrauch einer falschen Urkunde – ausschließt. Die Kopie oder das Abbild eines Fax', die keinen anderen Eindruck erwecken, als eben eine Kopie oder ein Faxausdruck zu sein, sind keine Urkunden mit dem Aussagegehalt des Originals: **BGH**, Beschluss vom 27.01.2010 - 5 StR 488/09.

2.3.2.2 Botnetze

Botnetze [69] sind die mächtigsten Werkzeuge [70], die der Cybercrime heute zur Verfügung stehen [71].

Ein Botnetz, auch Zombie-Netz genannt, ist ein Zusammenschluss von Computern, die mit einem Schadprogramm infiziert sind. Es ermöglicht Cyberkriminellen die Fernsteuerung der befallenen Rechner, ohne dass Anwender etwas davon bemerken. Zombie-Netze können inzwischen auch ohne größeres Fachwissen aufgebaut und gesteuert werden. Sie sind daher lukrativ einsetzbar. Die Folge: die Anzahl von Botnetzen wächst (Namestnikov [72]) mit steigender Tendenz [73].

Genaue Zahlen über die Anzahl von Botnetzen liegen mir nicht vor. Vermutlich sind etwa zwei Dutzend Banden weltweit führend, die sich anhand der eingesetzten Malware, ihrer digitalen Handschriften und Werbestrategien unterscheiden lassen. Durch die zunehmende Verbreitung von Baukästen für die Zusammensetzung von „Botware“ dürfte die Anzahl der kleinen Botnetze noch sprunghaft ansteigen, auf Dauer für die Hersteller von Antivirenprogramme aber kein ernsthaftes Problem darstellen.

Die mit Malware infizierten Zombies verhalten sich

[69] **CF**, Botnetze, 2007

[70] **CF**, mächtige Werkzeuge für die Cybercrime, 24.09.2010;
Zheng **Bu**, Pedro **Bueno**, Rahul **Kashyap**, Adam **Wosotowsky**, Das neue Zeitalter der Botnets, McAfee 19.08.2010.

[71] Sturmwurm-Botnetz sperrangelweit offen, Heise online 09.01.2008;
CF, Basar für tatgeneigte Täter. Botnetze, 11.04.2010

[72] Yuri **Namestnikov**, Schattenwirtschaft Botnetz – ein Milliongeschäft für Cybercriminelle, Kapersky 24.07.2009

[73] Schädlingsbaukästen befeuern Botnetzepidemie, Heise online 17.02.2011;
Damballa, Top 10 Botnet Threat Report – 2010, 11.02.2011

inzwischen sehr zurückhaltend und unauffällig, um den Anwender möglichst wenig zu beeinträchtigen [74]. Das ist der Ökonomie geschuldet. Ein Zombie ist wertvoll und soll möglichst lange unentdeckt und missbrauchsfähig bleiben. Sein behutsamer Einsatz ist keine Freundlichkeit, sondern Kalkül. Hat er seine Schuldigkeit getan, wird er ohne Bedenken geopfert [75].

Mit Botnetzen lassen sich Spams und mit Malware verseuchte Nachrichten versenden. Die Zombies lassen sich ausforschen und zum Phishing missbrauchen. Außerdem dienen sie zu verteilten Angriffen (DDoS), lassen sich zur Erpressung nutzen, als verteilte C&C-Server (Flux-Server), als Speicherplattform für Dropps (abgelegte, ausgespähte Daten) und andere illegale Inhalte, zum Download, zum verteilten Rechnen, um Zugangscodes oder Bitcoins zu knacken [76], und schließlich als Konsole zur verdeckten Kommunikation.

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

Eine solche Anforderungspalette können Einzelpersonen kaum leisten. Paget hat 2010 geschätzt, dass für den Betrieb eines Botnetzes zwei bis drei gute Programmierer nötig sind [77]. Hinzu dürften mindestens zwei Leute für die Logistik kommen, die die Werbung, den Einkauf, die Kundenbetreuung, den Zahlungsverkehr und die interne Qualitätskontrolle abwickeln. Balduan hat schon 2008 über Operating Groups berichtet, die aus mehreren Handwerkern und einem "Kopf" bestehen, der über Aufträge verhandelt, die Arbeit den Handwerkern zuteilt und überwacht und schließlich den Lohn verteilt [78]. Das gilt besonders auch für die Entwicklung von Malware, wobei Balduan Exploit-Händler und Rootkit-Entwickler als unabhängige Zulieferer ansieht.

2.3.2.3 Stuxnet

2010 wurde Stuxnet bekannt und die Firma Symantec hat sich besonders um seine Feinanalyse gekümmert [79]. Über diese besondere Malware lassen sich unter Vorbehalt einige Aussagen treffen:

Stuxnet ist eine Malware, die ganz gezielt zur Sabotage gegen die iranische Atomanreicherungsanlage in Natanz geplant und eingesetzt wurde. An ihrer Entwicklung waren seit 2007 mindestens zwei Entwicklerteams beteiligt, deren „Handschriften“ darauf schließen lassen, dass sie nicht der üblichen Malware-Szene entstammen, sondern dass sie eher Profis aus Israel oder den USA sind. Seit dem Sommer 2009 wurden Mitarbeiter von Firmen, die an dem Bau der Atomanlage beteiligt sind, gezielt mit der Malware ausgestattet, die wahrscheinlich auf USB-Sticks gespeichert war und damit injeziert wurde.

Zur Infektion und Installation wurden mehrere Exploits verwendet, die bis zum Sommer 2010 unbekannt waren (Zero-Day-Exploits) und einen Schwarzmarktpreis im sechsstelligen Bereich er-

---

74 Zum Verhalten von Botnetzen: Tom **Simonite**, Botnetz unter der Lupe, Technology Review 21.12.2010;
CF, Zombies im Labortest, 21.12.2010.

75 Ausführlich zur Funktionsweise: Daniel **Plohmann**, Elmar **Gerhards-Padilla**, Felix **Leder**, Botnets: Detection, Measurement, Disinfection & Defence, ENISA 14.03.2011;
Jens **Tölle**, Botnetze: Erfassung, Messung, Desinfektion und Abwehr, Fraunhofer 2011

76 Trojaner nutzt GPU zur BitCoin-Gewinnung, Heise online 17.08.2011

77 Zum Spamming mit Botnetzen: François **Paget**, Cybercrime and Hacktivism, McAfee 15.03.2010, S. 44.

78 Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.; kostenpflichtiger Download.

79 Nico **Ernst**, Stuxnet greift nur bestimmte Industrieanlagen an, golem.de 15.11.2010

zielen konnten [80]. Auch die eingesetzten Rootkits waren bis zu ihrer Entdeckung unbekannt. Die Entwicklungskosten werden im siebenstelligen Bereich vermutet.

Stuxnet ist in der Lage, ganz gezielt die Industrieanlagensteuerungen der Firma Siemens anzugreifen, die im Iran (dem Vernehmen nach nicht immer lizenzsicher) eingesetzt werden. Auch dazu bedarf es eines ganz besonderen Know Hows und Insiderwissens.

Stuxnet weist somit einige bislang nicht beobachtete Besonderheiten auf:

- die Malware ist extrem teuer in der Herstellung,
- richtet sich ganz gezielt gegen ein Angriffsziel,
- wird nicht über das Netz, sondern über Datenträger verbreitet,
- nutzt mehrere bislang unbekannte Schwachstellen (Exploits) und
- Rootkits und
- greift ganz gezielt Industrieanlagensteuerungen eines führenden Anbieters an.

Damit repräsentiert Stuxnet eine neue Qualität von Gefahr, die ich dem kalten Cyberwar zuordne [81]. Die Grafik oben stammt von McAfee [82] und ist deshalb besonders witzig, weil sie das bekannt gewordene Aufkommen der Malware visualisiert – geballt in Indien und Umgebung, nicht aber im Iran. Ein Schuft …

2.3.2.4 Aurora

Seit Ende 2009 wurden Google und 30 weitere Unternehmen mit einer äußerst professionell programmierten Phishing-Malware angegriffen, die eine erst kurzfristig bekannt gewordene Sicherheitslücke im Internet Explorer ausnutzte [83]. Sie soll besonders darauf ausgerichtet gewesen sein, Zugangsrechte, Passwörter und Unternehmensgeheimnisse auszuspähen [84]. Der McAfee Threat Report für das erste Quartal 2010 [85] hebt die Rolle Chinas im Zusammenhang mit Sicherheitsbedrohungen hervor und sieht in der "Operation Aurora" (S. 12) *den bedeutendsten gezielten Angriff in der Geschichte des Internets*. Kurz zuvor hatte McAfee eine Studie herausgegeben, die sich mit dem Angriff im einzelnen auseinander setzte [86]. Sie zeigt genau die Arbeitsschritte, die oben (▸ 2.3.1) beschrieben werden, also zunächst die Anlieferung [87]:

1. *Ein ins Ziel geratener Benutzer bekam aus einer „vertrauenswürdiger“ Quelle einen Link in einer E-Mail oder in einer Sofortnachricht.*

2. *Der Benutzer klickte den Link an und gelangte so auf eine Webseite in Taiwan, die Schadcode in Form von schädlichem JavaScript-Payload ent-*

---

80 Über € oder $ muss man sich wegen der nahen Wechselkurse keine Gedanken machen.

81 Dieter **Kochheim**, Eskalationen. Stuxnet, 20.02.2011, S. 7, 8 m.w.N.

82 Threat-Report: Drittes Quartal 2010, McAfee Labs 08.11.2010, S. 9.

83 Christoph H. **Hochstätter**, Aurora: Angriff mit IE-Exploit aus China auf Google und den Rest der Welt, zdnet 19.01.2010

84 Marcel **Rosenbach**, Thomas **Schulz**, Wieland **Wagner**, Operation Aurora, Der Spiegel 18.01.2010

85 McAfee Threat-Report: Erstes Quartal 2010, 12.05.2010

86 Schutz für Ihre wichtigsten Ressourcen. Lehren aus „Operation Aurora“, McAfee Labs 12.04.2010

87 Die Zusammenfassungen von McAfee sind bereits so komprimiert, dass sie durch eine Wiedergabe in eigenen Worten an Aussagewert verlieren würden. Sie werden deshalb im Wortlaut zitiert. Auch die Grafik auf der Folgeseite stammt aus der Studie von McAfee.

hielt.

Darauf folgt die Injektion:

3. *Dieses schädliche JavaScript enthielt ein Zero-Day-Exploit für den Internet Explorer und wurde vom Browser des Benutzers heruntergeladen und ausgeführt.*

Bis zu diesem Stadium ist noch nichts Schädliches geschehen. Schließlich folgt die Infektion:

4. *Der Exploit lud dann von Servern in Taiwan einen als Bild getarnten Binärcode herunter und führte den schädlichen Payload aus.*

Danach nistet sich die Malware ein:

5. *Der Payload richtete eine Backdoor ein und verband sich mit einem Botnet in Taiwan.*

Die Schaffung einer „Hintertür“ (Backdoor) ist eine der einfacheren Ausführungsfunktionen einer Malware, aber besonders geeignet zur Industriespionage, weil sie das unbemerkte Ausspähen von Daten im Unternehmensnetz ermöglicht:

6. *Damit hatten die Angreifer vollen Zugriff auf die internen Systeme. Sie hatten es auf geistiges Eigentum und Systeme zum Software-Konfigurations-Management (Software Configuration Management, SCM) abgesehen, auf die sie nun durch die gefährdeten Systeme Zugriff hatten. Das kompromittierte System ließ sich zudem so manipulieren, dass die Angreifer noch weiter in das Netzwerk vordringen konnten.*

Aurora ist ein Beispiel für einen eher klassischen Angriff, bei dem die Malware, anders als bei ▸ Stuxnet oder den ▸ Homebanking-Trojanern, keine dauerhaften, automatisch gesteuerten Aktivitäten ausführt, sondern dem Hacker nur den Zugang zum System verschafft. Das ändert nichts daran, dass hierzu besonderes Expertenwissen und Kenntnisse über das technische Innenleben der angegriffenen Unternehmen nötig war. Diese Kombination aus präzisem Wissen, zielbewusstem Vorgehen und das gleichzeitig gegen eine ganze Reihe von Unternehmen zeichnet Aurora als eine neue Qualität bei den Angriffen im Internet aus.

2.3.2.5 Night Dragon

In einem nur in englischer Sprache verfügbaren White Paper berichtet McAfee über einen seit November 2009 offenbar von China aus geführten, koordinierten und gezielten Cyberangriff gegen globale Öl-, Energie- und petrochemische Unternehmen, dem McAfee den Namen Night Dragon gegeben hat [88]. Mit den Angriffen sollen vor allem Produktions- und Förderdaten, Informationen über Vorräte, Vertragsangebote und Projektkalkulationen erlangt werden.

Das Beispiel belegt, dass nicht nur die zerstörerischen DDoS-Angriffe gezielter werden, sondern auch die Hacking-Angriffe, die der Informationsbeschaffung und der Zerstörung dienen.

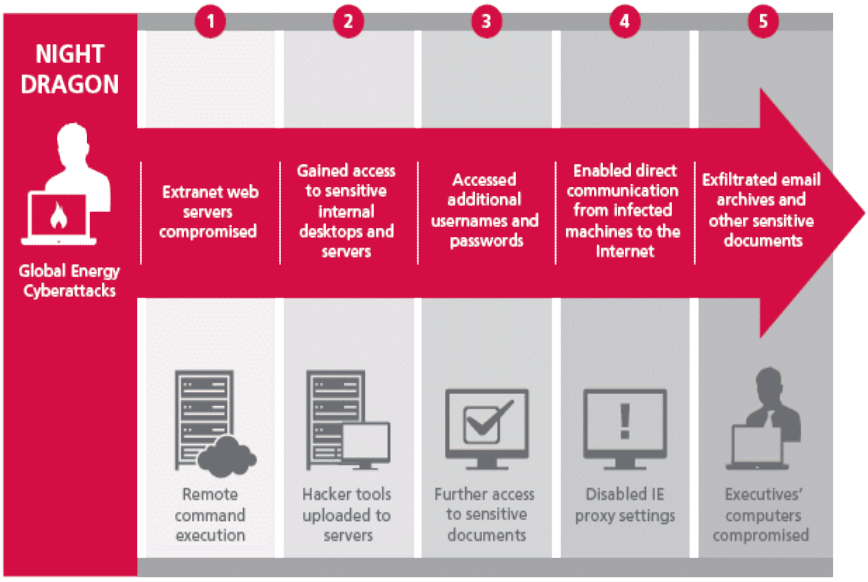
Bei dem Angriff geht es darum, den Fernzugriff auf die Computersysteme der angegriffenen Unternehmen mit entsprechenden Werkzeugen - Remote Access Tools - RAT - zu erlangen. Dazu werden Schwachstellen im Betriebssystem von Microsoft Windows und besonders in der Nutzerverwaltung und Rechtesteuerung - Active Directory - missbraucht.

Zunächst wird der Webserver des Unternehmens mit SQL-Injection-Methoden angegriffen. Dieser Webserver befindet sich noch außerhalb der en-

---

[88] Global Energy Cyberattacks: “Night Dragon”, McAfee Labs 10.02.2011;
Grafik Folgeseite: ebenda;
Stephen **Shankland**, Operation "Night Dragon": Hacker spionieren Ölindustrie aus, zdnet.de 10.02.2011

geren Schutzzone und dient den Kundenkontakten. Aber auch dazu muss er auf Kundendatenbanken, Preislisten und andere interne Informationen zugreifen. Das macht das Gesamtsystem anfällig.



Die SQL-Injektion ist ein einfacher Kommando-String zur Steuerung von Datenbankfunktionen. Gelingt es damit, die Kontrolle über den Webserver zu erlangen, können Hackerwerkzeuge nachgeladen (Infektion), Kontodaten und Zugangscodes ausgespäht oder protokolliert werden. Damit steht der Weg ins Innere des Unternehmensnetzes, alle Server und Desktoprechner offen.

Der Drache nutzt dazu verseuchte Webseiten, die der "eigene" Webserver den Mitarbeitern im Innern sendet, und E-Mail-Anhänge, die er auf dem firmeneigenen E-Mail-Server präpariert.

Um den Fernzugriff vom Command and Control-Server - C&C - des Angreifers durchzulassen, müssen nämlich die Sicherheitseinstellungen im Internet Explorer der firmeninternen Anwender und im Proxy-Server des Unternehmens abgeschaltet werden.

Der Night Dragon war offenbar erfolgreich. Über in China gehostete C&C-Server und Hostspeicher in den USA und den Niederlanden gelang der Eingriff gegen Unternehmen und gegen Führungskräfte in Kasachstan, Taiwan, Griechenland und den USA. Erlangt wurden neben sensiblen Unternehmensdaten auch urheberrechtlich geschützte und vertrauliche Informationen.

Mit neu entwickelten und angepassten Software-Werkzeugen schaffte es der Drache, Firewalls und VPN-Tunnel zu durchdringen, um auf die Laptops der sich sicher glaubenden Mitarbeiter und Führungskräfte zu gelangen.

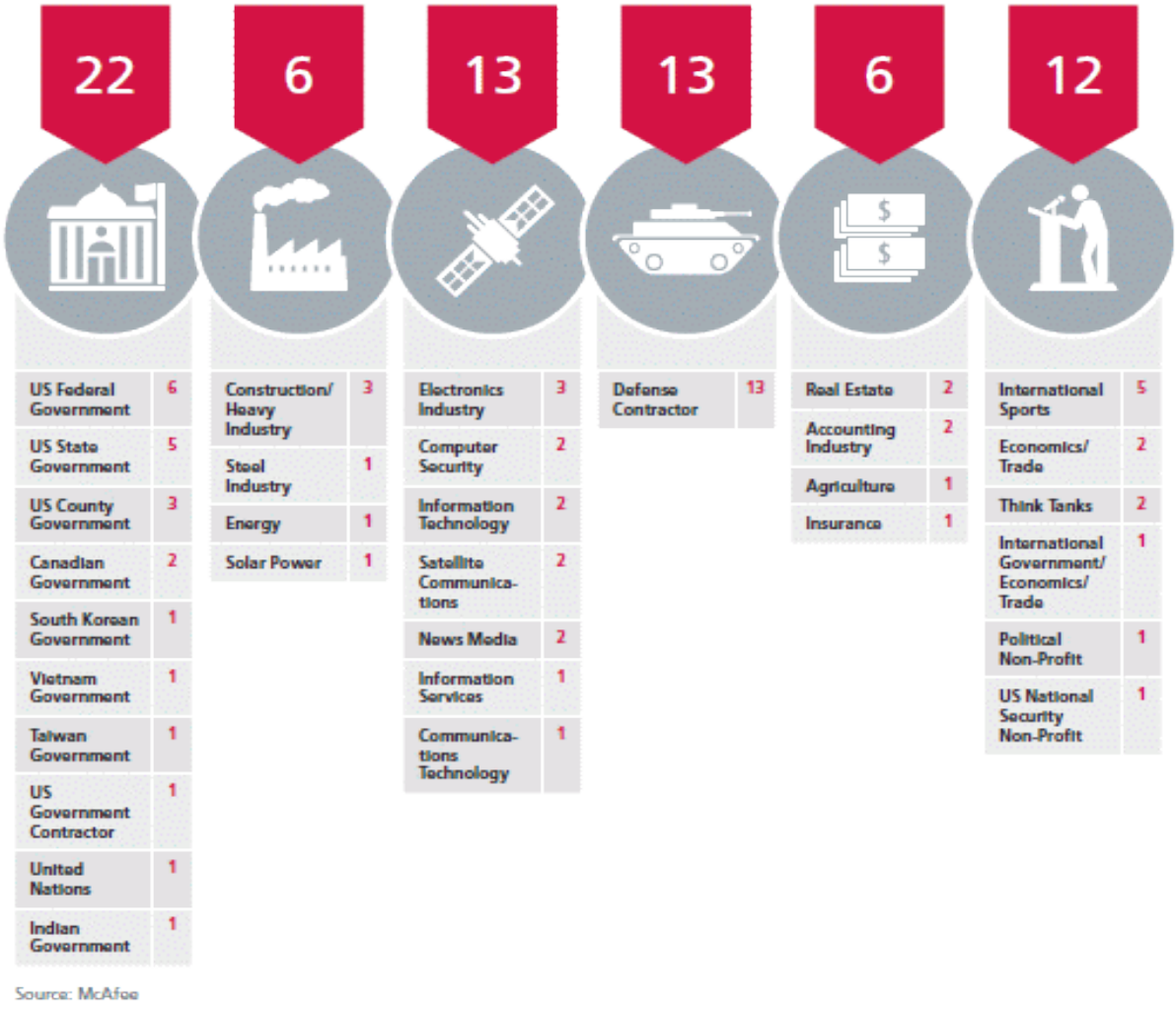
Diese Angriffstiefe ist neuartig. Der Night Dragon gelangte nicht nur in die Firmennetze hinein, sondern schaffte es, die als sicher geltenden VPN-Verbindungen (nicht zu durchbrechen, sondern schlicht) zu umgehen, indem er sie von der Quelle im Unternehmenskern an nutzt. Jede noch so qualifizierte, aber aufgesetzte Sicherheitstechnik kann auf diese Weise ausgehebelt werden.

2.3.2.6 Shady RAT

McAfee hat im März 2011 den Zugang zu den Logfiles eines schon 2009 entdeckten Command and Control Servers – C&C – erlangt, den hungrige Datendiebe bereits seit 2006 als Sprungbrett zu den Datenbanken von insgesamt 72 weltweit verteilten Unternehmen und Organisationen nutzen. Ihre Methode ist einfach und fast schon klassisch zu nennen: Die Angreifen senden an die Mitarbeiter ausgesuchter Unternehmen ("Spear-Phishing") E-Mails mit Anhängen, die eine Download-Routine enthalten. Damit wird die Malware geladen, die eine Hintertür (Backdoor) für den C&C öffnet und den Angreifern den Zugang gibt [89].

Den schon lange dauernden Angriff nennt McAfee "Operation Schattige Ratte", was sich aus dem englischen Sprachgebrauch ableitet, Programme zum Fernzugriff auf fremde Systeme (3) als Ratten (Remote Access Service – RAS ~ Rats) zu bezeichnen. Betroffen sind 72 Organisationen, *darunter ... die ... Regierungen Indiens, Kanadas, Taiwans, Südkoreas, Vietnams und der USA,* <das>

[89] Dmitri **Alperovitch**, Revealed: Operation Shady RAT, McAfee 05.08.2011, S. 3, 4.
Auch die Grafik auf der Folgeseite stammt aus dem Bericht.



IOC, <die> *Vereinten Nationen, ... ASEAN oder* <die> *Antidoping-Behörde sowie ... Hightech-Unternehmen und Rüstungsfirmen, Thinktanks und Medien* [90]. Die Menge der ausgespähten Daten wird in Petabytes geschätzt, also in einer Größenordnung, in der Sony weltweit über Speicherplatz für Videos verfügt [91].

Die Qualität der ausgespähten Daten ist unbekannt, was angesichts der schieren Menge auch unbedeutend ist: Alles, was an Interna und Geheimnisse greifbar ist.

Ungewöhnlich ist: Die Operation dauert schon seit 5 Jahren an und ist kein lockerer Hack, der mal eben zum Spaß durchgeführt wird. Bei der Auswahl der Opfer konzentrieren sich die Angreifer auf Nordamerika (53), Europa ist kaum betroffen (6), etwas stärker der Ferne Osten (8) [92]. Die Dauern der Angriffe sind teilweise kurz und in anderen Fällen reichen sie über Jahre hinweg [93]. Die Ziele als solches lassen kein spezifisches Muster und keinen Schwerpunkt erkennen [94]. Das unterscheidet sie von den Angriffen unter ▸ Aurora vom Anfang 2010.

Die Angreifer scheinen an den Informationen als solche interessiert sein. Es sind keine Erpressungsversuche bekannt geworden. Das spricht für Industrie- und andere Spionage. Deshalb vermutet McAfee die Angriffe aus Russland oder China stammend. Tatsächlich sind beide Länder nicht von ihnen betroffen, wohl aber Südkorea und Tai-

90 Florian **Rötzer**, Bislang größte Cyberhack-Serie entdeckt, Telepolis 03.08.2011

91 **CF**, IT in Zahlen, 08.04.2011

92 McAfee, ebenda, S. 5.

93 McAfee, ebenda, S. 9 bis 13.

94 McAfee, ebenda, S. 7 bis 8.

wan (jeweils 3), Indonesien, Singapore und Hong Kong (je 1). Das lässt eher eine chinesische Handschrift vermuten. Die verwendete Angriffstechnik ist technisch betrachtet solides Handwerk. Ihr fehlt aber das handwerkliche Niveau jüngster Angriffe, mit dem zum Beispiel beim ▸ Night Dragon vorgegangen wurde.

Einzigartig ist hingegen die kaum noch begreifbare Datenmenge, die hier abgegriffen wurde, und die lange Zeit, über die die Aktion lief. Der Zeitfaktor spricht dafür, dass die Angreifer die Daten nicht einfach nur abgesogen, sondern auch in ganzer Tiefe ausgewertet haben.

2.3.3 Malware und IuK-Strafrecht

Das Beispiel von ▸ Aurora zeigt uns anschaulich die Schritte, mit denen sich die Malware einnistet und schließlich ihre schädlichen Funktionen ausführt:

❶ Anlieferung

❷ Injektion

❸ Infektion

❹ Einnisten

❺ Tarnen

❻ Malware ausführen

Besonders die ersten vier Schritte des völlig automatisierten Prozesses (siehe ▸ 2.3.1 und ▸ 2.3.2.4) interessieren für die Frage, ob damit bereits eine Computersabotage (§ 303b StGB) oder ein Ausspähen von Daten vollendet (§ 202a Abs. 1 StGB) wird. Für beide Strafvorschriften gilt, dass sie einen Unrechtserfolg voraussetzen, der einerseits in der Zerstörung von Daten und andererseits in ihrer unberechtigten Wahrnehmung (Ausspähen, Abfangen) besteht. Ein menschliches Zutun bei der Vollendung verlangen sie nicht, so dass als Tathandlung das noch im Vorbereitungsstadium angesiedelte Einrichten von Webseiten oder Präparieren von E-Mails mit Malware als komplettes Programm oder von Startern ausreicht, die den automatischen Download der Malware initiieren sollen [95].

---

[95] Dieses Vorgehen wird schon lange unter dem Begriff Pharming diskutiert (**CF**, Pharming, 2007), wobei die Täter eine Vielzahl von nachgemachten Bankenseiten präsentieren, auf die sie die Kunden verschiedener Banken locken, zu unbedarften Dateneingaben überreden oder von dort schädlichen Code zuspielen. Eine Abwandlung davon besteht darin, dass durch viele miteinander verlinkte Webseiten und die Verwendung häufig nachgefragter Suchworte beste Platzierungen bei den Suchmaschinen erreicht und dadurch die Anwender angelockt werden. Schließlich werden auch die Webserver von frequentierten Angeboten angegriffen und so manipuliert, dass sie die Malware verbreiten.