5. Malware

5.1. EINLEITUNG

In den Anfangszeiten des Internets war es noch Spaß, sich Zugang zu fremden Computern zu verschaffen. Diese ersten „Hacker“ traten für Informationsfreiheit ein und wollten mit ihren „Hacks“ beweisen, dass es ohnehin nichts gibt, was man dauerhaft geheimhalten könne. Sie waren bestrebt, bei ihren „Einbrüchen“ keinen Schaden anzurichten. Oft informierten sie die Gegenseite über ihre gelungenen Einbrüche und die gefundenen Sicherheitslücken. Doch es gibt nur noch wenige von diesen „Gentlemens mit weißer Weste“, die sich als „White Hat“-Programmierer bezeichnen. Das Internet wird heute überschwemmt mit Betrügern und „Black Hat“-Kids, denen es nur darauf ankommt, viel Geld zu ergaunern.

Im Internet kursieren Millionen Schadprogramme, und zehntausende Schadprogramme kommen jeden Tag dazu. Die Internet-Mafia „erwirtschaftet“ einen Gewinn, welcher den Gewinn der Drogenmafia um ein Vielfaches übersteigt. Es ist nahezu sicher, dass ein völlig ungeschützter PC schon nach wenigen Stunden Surfen mehrfach infiziert ist. Die Hersteller von Antivirenprogrammen stimmen in ihren Jahresberichten immer wieder darin überein, dass mehr als ein Drittel aller deutschen PCs verseucht sind. Das Internet wird zunehmend gefährlicher und die Attacken werden professioneller.

„Hacker“ wird als Sammelbezeichnung für alle „bösen Buben“ verwendet.

Wenn in diesem Buch von Viren gesprochen wird, ist meist das ganze Spektrum von Schädlingen gemeint.

Mit „Antivirenprogramm“ ist das ganze Spektrum von Schutzprogrammen gemeint, von denen die einfachsten nur vor den klassischen Viren einigermaßen schützen und alle E-Mail-Bedrohungen ignorieren, während die komplexeren Sicherheitsprogramme auch eine Firewall, heuristische Suche, Kindersicherung usw. enthalten und die vor vielen Arten von Malware schützen.

Ihre Sicherheit wird bedroht:

- Viren, Würmer, Trojaner, Spyware, Backdoors, Ransomware und andere Schädlinge versuchen unbemerkt in Ihren Computer einzudringen. Der Sammelbegriff für diese Schadsoftware ist „Malware“ (**Mal**icious Soft**ware**, deutsch „bösartige Software“).

  (Mehr darüber siehe `http://de.wikipedia.org/wiki/Malware`).
- Ihre persönlichen Daten werden gesammelt: Bankverbindungen, Hobbys, Adressen von Bekannten. Ihre E-Mails werden ausgewertet, Ihre Einkäufe registriert, Ihr Surfverhalten wird protokolliert. Teils geschieht das durch Ihre eigene Unachtsamkeit, teilweise durch Spionageprogramme.

Welcher Schaden kann daraus für Sie entstehen?

- Ihr PC wird langsamer, funktioniert nur eingeschränkt und stürzt ab. Daten können verloren gehen. Die Reparatur kann Stunden oder Tage dauern und hunderte Euro kosten.
- Ihr PC wird ohne Ihr Wissen missbraucht, um Werbung zu versenden und um Angriffe auf Ihre Firma und Ihre Bekannten zu starten. Die werden sich freuen!
- Ihr PC wird ohne Ihr Wissen für kriminelle Aktionen missbraucht, beispielsweise zur Zwischenlagerung von pornografischem Material oder für Angriffe auf andere PCs.
- Ihr Leben wird ausspioniert. Die Daten werden für Werbung gebraucht und um Sie besser betrügen zu können. Dossiers für ihre potenziellen Arbeitgeber werden erstellt.
- Ihre Kinder geraten in Gefahr.

Welche Schäden können für eine Firma entstehen, zusätzlich zu den bereits genannten?

- Arbeitszeitausfall von Stunden und Tagen, Produktionsausfall, Lieferverzögerungen bis zum Bankrott,
- Diebstahl von Forschungsergebnissen und Fertigungsunterlagen,
- Einsicht in Finanzunterlagen, Kalkulationen, Ausschreibungen und Verträge.

5.1.1. Niemand ist ganz sicher

Sie haben Ihren PC hinter einer Hardware-Firewall versteckt, das beste Antivirenprogramm installiert und halten es stets auf dem neuesten Stand? Sie installieren alle Updates? Sie glauben, nun sind Sie völlig sicher? Das ist ein Irrtum. **Niemand ist jemals ganz sicher.** Wieso?

Leider besitzen die Virenprogrammierer nicht die Freundlichkeit, ihre neuesten Angriffsprogramme zwecks Begutachtung vorab an die Antivirenhersteller zu schicken. Deshalb erfahren die Antivirenhersteller von neuen Schädlingen erst dann, wenn sie bereits eine gewisse Verbreitung erreicht haben. Die Antivirenhersteller stellen Computer als Fallen auf, sogenannte „Honeypots" (Honigtöpfe), und sie lassen sich von den bei ihren Kunden installierten Antivirenprogrammen alle verdächtigen Aktivitäten melden. Wer als erster einen neuen Virus findet, gibt ihm einen Namen und informiert die anderen Antivirenhersteller. Manchmal finden mehrere Hersteller einen neuen Virus gleichzeitig, dann trägt er mehrere Namen.

Auf jeden Fall vergehen einige Stunden, bis der Schädling gefunden und analysiert ist, bis eine Abwehrmethode programmiert und als Update bereitgestellt ist. Dann muss das Update noch auf Ihren PC heruntergeladen werden. Es vergehen also immer ein bis drei Tage, bis Ihr Antivirenprogramm Ihren PC vor den neuesten Entwicklungen schützen kann. Umgekehrt bedeutet es, dass sich neue Viren einige Tage fast ungehemmt ausbreiten können.

Natürlich dürfen Sie deshalb nicht auf ein Antivirenprogramm verzichten, denn ein gutes Programm wehrt 99 % der Attacken ab. Wie kann die verbleibende Sicherheitslücke geschlossen werden? Ganz klar: Nur durch Ihr Verhalten. Die wichtigste Antiviren-Software befindet sich zwischen Ihren Ohren. Ihr Wissen um Funktionsweise und Ausbreitungsmethoden der Schädlinge, Ihre Vorsicht und Aufmerksamkeit kann die Gefahr abwehren oder zumindest in ihren Auswirkungen mildern. Dieses Buch soll Ihnen das notwendige Wissen vermitteln.

Übrigens gibt es eine einfache Methode, die Erkennungsrate Ihres Antivirenprogramms zu steigern: Schalten Sie Ihren PC eine Viertelstunde früher als sonst ein und lassen Sie ihn nach der Anmeldung für zehn Minuten im Leerlauf. Dadurch erhält das Antivirenprogramm die nötige Zeit, die neuesten Virendefinitionen herunterzuladen. Auch Windows und Anwendungsprogramme gewinnen Zeit, eventuell bereitstehende Sicherheitsupdates zu installieren. Danach ist der PC besser gerüstet, auch den allerneuesten Bedrohungen zu begegnen. Und wenn Sie nicht so viel Zeit haben für zehn Minuten Leerlauf: Beginnen Sie den Tag **nicht** mit dem Empfang von E-Mails. Erledigen Sie in der ersten Viertelstunde nur solche Aufgaben, für die Sie das Internet nicht brauchen.

5.1.2. Warum gibt es Malware?

In den 1970er Jahren wurde das erste Programm erfunden, das sich selbsttätig von Computer zu Computer verbreiten konnte. 1982 gab es den ersten Virus für den Mac-Computer von Apple, 1986 tauchte der erste Virus für IBM-kompatible Computer auf. Einen Virus zu programmieren war damals eine hochinteressante Übung für gute Programmierer. Viren richteten keinen nennenswerten Schaden an, hauptsächlich dienten sie dazu, die Benutzer zu necken. Ihre Verbreitung war gering, nur wenige Computer waren vernetzt. Das Internet gab es noch nicht. Windows in der Version 3.0 gab es erst seit 1990, bis dahin lief auf fast allen PCs das Betriebssystem DOS, und damals war es noch einfach, einen Virus zu entfernen.

Die Zahl der Viren nahm allmählich zu, und es tauchten die ersten bösartigen Viren auf. Die ersten Antivirenprogramme kamen auf den Markt. Einen Virus zu programmieren, der von den gängigen Antivirenprogrammen nicht erkannt wird, wurde von Hackern als sportliche Herausforderung angesehen. Einen der oberen Plätze in der Liste der meistverbreiteten Viren zu erreichen, erhöht das Selbstwertgefühl und die Anerkennung im Computer(hacker)klub.

Besonderen „Ruhm" hatte im Jahr 2000 der Virus „I love you" erreicht. Er verbreitete sich rasend schnell, weil viele Anwender und auch viele Systemadministratoren die Gefahr unterschätzt und ihre Systeme ungenügend gesichert hatten. Die Schweizer Rückversicherungsgesellschaft Swiss RE hat im Jahr 2001 eine Statistik über Katastrophen und deren direkten und indirekten wirtschaftlichen Schaden veröffentlicht. Die ersten acht Plätze sind von Vulkanausbrüchen, Erdbeben und anderen Naturkatastrophen belegt. In dieser Statistik nimmt „I love you" den neunten Platz ein. Ein Virus im Rang einer Naturkatastrophe!

Heute werden nicht mehr viele Viren „aus Lust und Laune" entwickelt. Die große Masse der Viren und anderer Malware wird mit dem Ziel entwickelt, Gewinn zu machen. Die Programmierung wird immer professioneller.

Malware nimmt pro Jahr um 20 bis 30 % zu. Den größten Zuwachs gibt es beim Ausschnüffeln von Identitätsinformationen. Lesen Sie:

- „Einmal Gott sein“, DER SPIEGEL 20/2000 http://www.spiegel.de/spiegel/print/d-16409510.html
- „Geschichte der Computerviren“ http://www.itespresso.de/2012/10/18/die-geschichte-der-computerviren/

5.1.3. Wer entwickelt die Malware?

Unter den Hackern sind die Arbeitsteilung und die Zusammenarbeit gut organisiert. Über das Internet haben sie verschlüsselte Netzwerke organisiert, um auf wechselnden virtuellen „Marktplätzen“ ihre Leistungen anzubieten und Verträge abzuschließen.

- Gestohlene Kreditkartendaten, Bankverbindungen, Adresslisten usw. werden versteigert.
- Für 6000 Dollar können Sie US-Bürger werden: Sie bekommen Pass, Führerschein, Geburtsurkunde und andere Papiere, einschließlich Eintrag in alle wichtigen amtliche Datenbanken. Deutsche Pässe sind billiger.
- Spezialgeräte werden angeboten, z. B. Kreditkartendrucker und Spionagewerkzeuge.
- Es gibt „Virenbaukästen“ mitsamt Anleitung zu kaufen, wie man aus bewährten Malware-Komponenten etwas Neues für den eigenen Bedarf zusammenbauen kann.
- Botnetze oder Teile davon (z. B. nur deren deutsche PCs) kann man mieten. Mit einem Botnetz kann man massenhaft Spam versenden, Malware verteilen oder DoS-Angriffe („**D**enial **o**f **S**ervice, deutsch: Dienstblockade, siehe nächste Seite) durchführen.
- Die höchstqualifizierten Spezialisten suchen nach unbekannten Schwachstellen. Für eine gefundene Sicherheitslücke wird ein Konzept für den Angriff entworfen, dann wird das Schadprogramm programmiert und getestet. Größere Vorhaben werden mit professionellem Projektmanagement angegangen.
- Schadprogramm-Rohlinge kann man kaufen, mitsamt Anleitung und Komplettservice. Der Käufer trägt nur noch seine Kontonummer für die erpressten Gelder ein und verfasst in der Sprache jedes Ziellandes einen geeigneten Text. Ein Beispiel dafür ist der „BKA-Trojaner“, von dem Dutzende Varianten im Umlauf sind.

Dmitry Fedotov, unter Hackern bekannt als „Paunch“, ist als Entwickler des Hacker-Tools „Blackhole“ berühmt. Blackhole ist eine Art Webanwendung für die Verbreitung von Malware, die Hacker gegen eine Abo-Gebühr von 1500 US-Dollar pro Jahr mieten können. Der Hacker versorgte Blackhole mit Updates über neue Schwachstellen, bis er 2012 in Russland verhaftet und zu zehn Jahren Gefängnis verurteilt wurde.

Jeremy Jaynes stahl 90 Millionen E-Mail-Adressen aus einer AOL-Datenbank und versandte Spam-E-Mails. Das brachte ihm eine halbe Million US-Dollar pro Jahr ein. Er wurde zu neun Jahren Haft verurteilt.

Vladimir Leonidovich Levin konnte der Citybank 10 Millionen US-Dollar stehlen. Er wurde zu drei Jahren Gefängnis und zu einer Geldstrafe von über 240 000 US-Dollar verurteilt.

Mittlerweile finden sich Hacker zu großen Teams zusammen. Von professionellen Projektmanagern geleitet werden hochkomplexe Angriffe programmiert. Einige Beispiele:

- Ein Programm „Stuxnet“ arbeitete sich zielstrebig voran bis zu den Uranzentrifugen des iranischen Atomprogramms. Stuxnet infizierte deren Steuerung und zerstörte etwa tausend Zentrifugen. In einigen Industriesteuerungen anderer Länder wurde Stuxnet ebenfalls gefunden, doch er richtete außer im Iran nirgends Schäden an. Es wird vermutet, dass Stuxnet ein Gemeinschaftsunternehmen der USA mit Israel war.
- „Night Dragon“ (deutsch „Drache der Nacht“) hatte die Öl-, Gas- und Industriekonzerne der USA zum Ziel. Finanzdokumente und Daten zu Fördermengen, Kapazitäten und Pipelines wurden gestohlen. Überwachungssysteme für Industrieanlagen und Fernwartungssysteme wurden gehackt.

  Night Dragon wurde 2009 entdeckt. McAfee meinte, das Programm wäre schon seit vier Jahren aktiv. Sabotage konnte nicht festgestellt werden, das Programm hatte nur Informationen beschafft – was für spätere Angriffe sehr nützlich wäre. China ist höchst verdächtig, der Urheber zu sein.
- Als „Operation Aurora“ werden Hackerangriffe auf Google, Microsoft und andere US-Firmen bezeichnet. China hatte (vermutlich erfolgreich) nach Gmail-Konten von chinesischen Menschenrechtsaktivisten gesucht. Noch viel spektakulärer ist die Erbeutung der Liste, gegen wen gerichtlich angeordnete Überwachungsaktionen laufen. Damit sollte wohl ermittelt werden, welche chinesischen Agenten bereits von den USA enttarnt wurden und seitdem beobachtet werden.

Angriffe wie diese werden „Advanced Persistent Threats“ genannt: fortschrittliche, langlebige Bedrohungen. Die infizierten Computer senden Informationen über Monate oder Jahre an die Hintermänner. Bei solchen Angriffen sind hohe Gewinne zu erwarten bzw. eine hohe Ausbeute an geheimen Informationen.

Der Forensik-Spezialist Alexander Hutton sagte: *„Wir wissen nicht, wie gut diese Teams sind. Eventuell wurden Aurora und Night Dragon von der B-Mannschaft programmiert und wir entdecken die Angriffe der besseren Cyber-Gangster gar nicht.“*

Einen Angriff auf das Boden-Computernetz der Fluggesellschaft „LOT“ im Juni 2015 kommentierte der Sicherheitsexperte Frank Kölmel: *„Weltweit beobachten wir rund 400 Gruppierungen, die in der Lage sind, Systeme mit Advanced Persistent Threats über Monate hinweg unbemerkt anzugreifen. Wichtige Teile der Infrastruktur wie Fluglinien sind nicht selten Ziel dieser Angriffe. Auf der ganzen Welt versuchen Kriminelle und staatlich unterstützte Akteure immer wieder, Infrastruktureinrichtungen anzugreifen und sich Zugang zu ihren Systemen zu verschaffen.“*

5.1.4. Wie kann mit Malware Geld verdient werden? Einige Beispiele

Kreditkartenbetrug

Der Diebstahl von Kreditkartendaten und deren Verkauf ist hoch professionalisiert. Auf einem wohlorganisierten Schwarzmarkt werden Kartendaten für vier Dollar pro Person gehandelt. Kartendaten mit geprüfter Bonität und aktuellem Kontostand sind deutlich teurer. Mit Zugangsdaten zu PayPal kann man ebenfalls ein Konto leerräumen. 10 Kreditkartenrohlinge im Wunschdesign sind ab fünf Dollar erhältlich, sogar mit Hologramm. Wenn man eine größere Mengen Karten braucht, kauft man für weniger als 1000 Dollar einen Drucker, der neutrale Rohlinge mit dem Layout der gewünschten Bank bedruckt. Die gestohlenen Daten speichert man auf dem Rohling und geht mit der neuen Kreditkarte einkaufen.

Diebstahl

Die Zugangscodes für die Packstationen der Post sind für 30 bis 50 Euro zu haben. Es ist zwar Zufall, was man im Postfach findet, doch bei eBay oder im An- und Verkauf wird man fast alles los.

Erpressung mit gestohlenen Daten

Der Hacker stiehlt einer Firma wichtige Finanzdaten, Kundendaten oder Forschungsunterlagen. Dann präsentiert er der Firma die gestohlenen Daten und droht, diese zu veröffentlichen oder an die Konkurrenz zu verkaufen. Nur wenn die Firma ein üppiges „Beratungshonorar“ zahlt, erfährt sie, wie die Sicherheitslücke geschlossen werden kann. Die Firmen zahlen, um negative Publicity zu vermeiden.

Zombies bilden Bot-Netze

Einen PC, der ohne Wissen seines Benutzers über das Internet ferngesteuert werden kann, nennt man „Zombie“ oder „Bot“ (Abkürzung vom „Robot“). Ursache ist meist eine unentdeckte Infektion durch spezielle Trojaner. Die Gesamtheit der von einem Hacker gesteuerten Zombies bezeichnet man als Botnet. Botnets werden zum Versand von Spam, für Angriffe auf PCs und Netze und für andere kriminelle Aktivitäten genutzt. Antivirenhersteller und andere Experten schätzen, dass weltweit zwischen 10 % und 50 % aller Internet-PCs Teil eines Botnetzes seien. In Deutschland sei etwa jeder vierte PC ferngesteuert.

Erpressung mit DoS-Angriffen

Bei einem „**D**enial **o**f **S**ervice“-Angriff (deutsch: Dienstblockade) wird die Webseite einer Firma oder Institution von feindlichen Rechnern mit einer solchen Menge (sinnloser) Anfragen bombardiert, dass der Server überlastet wird. Die Anfragen der normalen Benutzer können nicht mehr beantwortet werden oder die Webseite ist nicht mehr erreichbar. Erst wenn der Betreiber der Webseite zahlt, wird der Angriff beendet. Wenn am Angriff eine große Anzahl PCs (eines Botnetzes) beteiligt sind, spricht man von einem „**D**istributed **D**enial **o**f **S**ervice“-Angriff (Distributed = verteilt). DDoS-Attacken werden von Cyber-Kriminellen sogar als Service angeboten. Die Webseite eines lokalen Konkurrenten lahmzulegen kostet etwa 150 Dollar pro Tag. Bei Großfirmen wird es teurer.

Manche Angriffe sind politisch oder ideologisch motiviert. Als sich im Dezember 2010 mehrere Banken weigerten, Spenden an WikiLeaks und Julian Assange weiterzuleiten und die Konten sperrten, starteten Aktivisten der Gruppe Anonymous die „Operation Payback“: Sie führten erfolgreiche DDoS-Angriffe auf die Bank of America, Visa, Mastercard, Amazon und die schweizerische PostFinance durch. Nur die Amazon-Server brachen nicht zusammen.

SPAM

Zwar lesen nur wenige Leute die Spam-Mails, und noch viel weniger kaufen dann tatsächlich die beworbene Ware. Andererseits ist der Versand von Millionen Mails pro Stunde kein Problem, da für den Versand vorzugsweise „gekaperte" PC verwendet werden. Bei einer Flatrate fallen keine Versandkosten an, und sonstige Kosten sind vernachlässigbar gering. Deshalb wird Spam als Geschäftsmodell weiter stark wachsen.

Im Jahr 2006 waren täglich 60 Milliarden Spam-Mails unterwegs, 2012 waren es 145 Milliarden und 2016 werden es voraussichtlich 190 Milliarden sein. Die Angriffe werden zunehmend gezielter. Der Spam-Anteil beträgt in zahlreichen Firmen bereits 90 % bis 97 % des E-Mail-Eingangs, eine Steigerung auf bis zu 99 % wird erwartet.

Abgesehen davon, dass Spam Zeit und Nerven kostet, ist Spam ungefährlich, solange Sie die Spam-Mail nicht öffnen. Denn Links im Spam führen teilweise auf verseuchte Seiten, und eventuelle Anhänge sind oft infiziert.

Wenn man einige Vorsichtsmaßnahmen beachtet, wie am Anfang des Kapitels „Infektionswege" beschrieben, kann man den Spam-Anteil gering halten. In meinem seit 12 Jahren bestehendem Firmen-Postfach habe ich etwa 15 % Spam, in meinem seit 1996 bestehenden privaten E-Mail-Fach weniger als 5 %.

Anfang 2014 habe ich ein Facebook-Konto eingerichtet. Trotz aller mir bekannten Vorsichtsmaßnahmen ist die Zahl der Spam-Mails auf 20 pro Monat angeschwollen, abgesehen von den ständigen „Kennen Sie ...?". Ich habe vorsorglich ein extra E-Mail-Konto für Facebook eingerichtet, die Spammer kennen mein „normales" Konto nicht.

Betrügerische Überweisungen

Ein Hacker kann Bankverbindungen samt Passwort und TAN für weniger als 10 Dollar kaufen. Dann zieht er von tausend Konten je 20 € per Lastschrift ein und gibt einen unverdächtigen Zahlungsgrund an (z. B. Danke für Ihren Einkauf bei Edeka!). Das ergibt einen netten Tagesverdienst. Die meisten Leute holen ihre Kontoauszüge nur einmal monatlich ab und achten kaum auf kleine, Wochen zurückliegende Buchungen oder denken, der Partner hätte eingekauft.

Sie haben den Betrug bemerkt und wollen das Geld zurückbuchen lassen? Das wird kaum gelingen.

Haben Sie schon einmal eine Annonce gelesen „Leichter Nebenverdienst – mehrere hundert Euro pro Tag!"? Wer sich auf so ein Angebot meldet, bekommt eine Geschichte aufgetischt, z. B. dass eine ausländische Firma ihren deutschen Kunden die umständlichen und teuren Überweisungen ins Ausland ersparen möchte und deshalb einen einheimischen „Finanzagenten" sucht. Er müsse nur ein Konto eröffnen und 90 % der eingehenden Zahlungen täglich per Western Union an den Hacker transferieren (weil Transfers über Western Union nicht zurückverfolgt werden können). Die restlichen 10 % dürfe er für seine „Mühe" behalten. Für schlichte Gemüter klingt das wie leicht verdientes Geld. Wer darauf hereinfällt, wird im Hackerjargon als „money mule" (Geldesel) bezeichnet. Welch schöne Doppeldeutigkeit!

Nach ein paar Tagen oder Wochen klingelt die Polizei. Dann wird der „Esel" als Hehler verurteilt, es sei denn, er kann einen Psychologen überzeugen, dass er ein Vollidiot und lebensuntüchtig ist. Dann bekommt er einen Vormund oder geht in die geschlossene Anstalt. Das gestohlene Geld muss der Geldesel in beiden Fällen ersetzen. Da bleibt nur der Antrag auf Privatinsolvenz, mindestens sieben Jahre eines kärglichen Lebens sowie schlechte Karriere- und Jobaussichten.

Ein kleines Sortiment weiterer Tricks:

- Eine Möglichkeit, Diebesgut gefahrlos in Empfang zu nehmen: „Wir mieten Ihren Briefkasten für 99 € im Monat. Sie müssen nur unseren Namen unter Ihren Namen schreiben und uns den Zweitschlüssel geben."
- Die Gauner bieten eine interessante, leerstehende Immobilie oder einen Urlaubs-Bungalow an. „Gegen Überweisung von 500 € Kaution senden wir Ihnen den Schlüssel zu."
- „Sie haben eine Million Euro gewonnen! Teilen Sie uns Ihre Kontodaten mit und überweisen Sie vorab die Notargebühr, damit wir den Gewinn auszahlen können!"
- „Sie haben einen Ferrari gewonnen! Sie können ihn am ... um 10 Uhr im Werk Mailand persönlich abholen, oder uns vorab die Überführungsgebühr von 590 Euro überweisen."

Verkauf persönlicher Informationen

Persönliche Informationen sind hoch begehrt. Alles wird gesammelt: Was Sie im Internet bestellen, was Sie im Chat schreiben, in welchen Communities Sie sich betätigen. Selbst die Webseiten, die Sie anklicken, und wie lange Sie auf dieser Seite bleiben bis zum Weiterklicken, liefern wertvolle Daten zu Ihrem Profil. Ihr Haus wird von Satelliten und von vorbeifahrenden Kamerawagen fotografiert. Ihre E-Mails werden analysiert (die **N**ational **S**ecurity **A**gency liest mehr als 90 % aller in Europa versandten E-Mails mit). Glauben Sie bloß nicht, irgendetwas würde geheim oder unbemerkt bleiben, was Sie im Internet tun. Glauben Sie nicht, irgendeine Information würde früher als in hundert Jahren gelöscht werden.

Wofür sind diese Daten nutzbar? Drei Beispiele:

- Die Werbebranche ist an persönlichen Daten sehr interessiert. Kennt man die Hobbys und Kaufgewohnheiten, werden diese Daten an interessierte Firmen verkauft. Diese können gezielter und damit erfolgreicher werben. Wenn beispielsweise eine Firma Rettungsringe verkaufen will – was ist wohl sinnvoller: Eine Sendung an alle Haushalte oder ein gezielter Versand der Werbung nur an Leute, die sich irgendwann für Boote und Zubehör interessiert haben?
- In den USA gibt es seit mehreren Jahren professionelle Agenturen, die Bewerberprofile im Auftrag von Personalchefs erstellen. Die Kenntnis von Vorlieben, Hobbys, Bekanntenkreis, früheren Arbeitsstellen, Gerichtsverfahren und Steuerabrechnungen sind wichtig für Einstellung und Karriere. Ihr Gesundheitszustand und eventuelle chronische Krankheiten sind hochinteressant für potenzielle Arbeitgeber. Sie haben wegen Alkohol die Fahrerlaubnis abgeben müssen? Sie sind mal ein paar Monate auf Bewährung verurteilt worden, weil Sie dem bösen Nachbarn eins ausgewischt haben oder Ihnen „die Faust ausgerutscht“ ist? Die Musik- oder Softwareindustrie hat Sie als „Raubkopierer“ erwischt? Die Polizei streicht das nach ein paar Jahren aus ihren Akten, die Datensammler ganz sicher nicht. Begraben Sie die Aussicht auf einen Traumjob und auf Karriere.
- Das süddeutsche Apothekenrechenzentrum hat im August 2013 anonymisierte Patientendaten an Pharmaunternehmen verkauft. Die Anonymisierung war ungenügend, ohne großen Aufwand konnten die Versichertennummern rekonstruiert werden. Die Firma pharmafakt/Gesellschaft für Datenverarbeitung (GFD) hatte ähnliches im Februar 2012 getan. Für die Arzneimittelhersteller ist es hochinteressant, von welchen Ärzten die Patienten mit chronischen Krankheiten behandelt werden. Die Pharmaunternehmen können dadurch ihre Vertreter gezielter zu den Ärzten schicken, um ihre teuren Medikamente anzupreisen. Auch Krankenversicherungen dürften an diesen Daten sehr interessiert sein. Es gibt Patienten, welche aus ihrer Krankenkasse herausgeflogen sind, z. B. wegen Beitragsrückstand. Und nun finden sie keine Kasse, die sie aufnimmt. Ob wohl die Krankenversicherungen schon die Daten der Online-Apotheken auswerten? Kennt die Kasse die verschriebenen Medikamente, kann sie die Aufnahme von Menschen mit teuren, chronischen Krankheiten ablehnen.

Vielleicht fragen Sie sich jetzt: Ist das für die Datenkraken nicht schrecklich teuer, so viele Daten zu speichern? Nein. Heutige Festplatten sind gigantisch. Ein Gigabyte reicht aus, um entweder 1500 Fotos in mittlerer Qualität oder den Text eines 10 Meter hohen Aktenstapels zu speichern. Angenommen, es gäbe die technische Möglichkeit, jedes Wort mitzuschreiben und zu speichern, welches Sie im Laufe Ihres Lebens sprechen. 4000 Worte pro Tag mit durchschnittlich 8 Buchstaben ergibt etwa 1 MByte pro Monat. In 1000 Monaten (83 Jahren) ist das nur ein Gigabyte. Bei einem Preis von 80 Euro für eine Festplatte von 2000 GB (Mai 2015) entspricht 1 GByte einem belegten Speicherplatz im Wert von 4 Cent. Wenn man den Text komprimiert, bleiben nur etwa 2 Cent, und der Preis pro Gigabyte fällt jedes Jahr um etwa 30 %.

Amazon hat im Dezember 2013 ein Patent über ein „System zum antizipatorischen Paketversand“ angemeldet. Um die Lieferzeiten zu verkürzen, will Amazon die Waren abschicken, noch bevor der Kunde sie bestellt hat. Nach der Auswertung früherer Bestellungen, Bewertungen, Produktsuchen, Wunschzettel, Warenkorbinhalten, Rücksendungen und Berücksichtigung der Zeit, wie lange der Mauszeiger auf einem Produkt geruht hat, ist sich Amazon sicher, aus den gesammelten Daten das Kaufverhalten seiner Kunden vorhersagen bzw. manipulieren zu können ...

5.1.5. Wie viel Geld kann mit Malware verdient werden?

Im September 2007 verkündete der Geschäftsführer (CEO) von McAfee, dass mit Malware ein jährlicher Umsatz von 105 Milliarden Dollar erwirtschaftet wird – mehr als im internationalen Drogenhandel. Eine Richterin am US-Finanzministerium nannte für 2007 einen ähnlichen Gewinn. Neuere, verläßliche Zahlen konnte ich nicht finden. Doch ganz sicher wächst die Computerkriminalität weitaus schneller als die Drogengewinne.

Der weltweit tätige Finanzdienstleister Cybersource schätzte den Schaden durch E-Commerce-Betrug für die US-Wirtschaft auf 3,6 Milliarden Dollar im Jahr 2007, das war ein Anstieg von 20 % gegenüber dem Vorjahr. Symantec nannte für 2013 nur für Deutschland allein einen Schaden von 24 Milliarden Euro.

Programmierer, die imstande sind, Programme für gezielte Angriffe gegen Firmen zu entwickeln, gehören zu den Spitzenverdienern.

5.1.6. Ist die Gefahr zu stoppen?

Die Qualität der Malware steigt von Jahr zu Jahr. Immer neue Angriffsmethoden werden entwickelt. Beispielsweise gibt es zunehmend zweistufige Attacken: Nicht die Spam-Mails sind verseucht, sondern sie enthalten Links auf infizierte Seiten. Gegen zehntausende hochmotivierte Hacker verlieren die vergleichsweise wenigen Mitarbeiter der Antiviren-Hersteller zunehmend an Boden. Alle 8,6 Sekunden wird ein neuer Schadprogrammtyp entdeckt, meldete GData. „Gespräche mit Chief-Technology-Officers von Anti-Malware-Herstellern zeigten, dass die Experten selbst davon ausgehen, den Kampf gegen die Schädlinge zumindest auf Code- und Desktop-Seite zu verlieren." Bald wird es nicht mehr möglich sein, einen einigermaßen ausreichenden Schutz zu erhalten für „nur" 30 Euro, die das Jahresabonnement eines Antivirenprogramms üblicherweise kostet. Es wird zunehmend wichtiger, durch vorsichtiges und umsichtiges Verhalten im Internet den Gefahren aus dem Weg zu gehen. Antiviren- und andere Schutzprogramme haben noch nie einen vollständigen Schutz bieten können, und die Schutzwirkung nimmt weiter ab.

Im ersten Halbjahr 2013 gab es laut GData 10000 neue Schadprogrammtypen pro Tag. 99,9 % davon zielen auf Windows-Betriebssysteme. Doch für die Besitzer eines Apple und die Fans von Linux ist das kein Grund, sich entspannt zurückzulehnen. 0,1 % von 8000 macht acht Angreifer pro Tag, die auf Apple bzw. Linux spezialisiert sind.

Panda Security zählt nicht die Malware-Typen, sondern die Exemplare. Im Bericht von Panda Security zum dritten Quartal 2014 werden 227 747 neue Malware-Exemplare pro Tag genannt. Im ersten Halbjahr 2014 waren es „nur" 160 Tausend. In Deutschland sind 26 % aller PC infiziert, in China 50 %. Trojaner stellen einen Anteil von 78 % (in zweiten Quartal noch 58 %) und Viren 9 % von der gesamten Malware.

- Analyse von GData: Preisliste für kriminelle Dienstleistungen im Jahr 2009
  `http://www.cio.de/i/detail/artikel/898319/1/680045/EL_12530230711784181416114/`
- Kriminelle Dienstleistungen (2012): Wer nicht hacken kann, muss hacken lassen
  `http://www.spiegel.de/netzwelt/web/trend-micro-nennt-preise-im-russischen-hacker-untergrund-a-865571.html`
- Virenreport von GData für das erste Halbjahr 2014
  `https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/GData_PCMWR_H1_2014_DE_v2.pdf`

5.1.7. Malware und das Militär

Schon seit Jahren ist klar: Ein Cyber-Angriff auf Elektro-, Gas- und Verkehrsnetze kann Schäden verursachen, die zu landesweiten Ausfällen und in der Folge zu humanitären Katastrophen führen können. Das Nato-Bündnis hat auf seiner Tagung in Wales im September 2014 festgestellt: *„Cyber-Angriffe können einen Punkt erreichen, an dem sie Wohlstand, Sicherheit und Stabilität auf nationaler und euro-atlantischer Ebene gefährden. Ihre Auswirkungen können für die modernen Gesellschaften so schädlich wie konventionelle Angriffe sein."* Die Nato hat unmissverständlich festgestellt, dass Computerangriffe auf Nato-Mitglieder künftig „je nach Fall" wie ein militärischer Angriff behandelt werden, der die Beistandspflicht des Artikels 5 des Nato-Vertrages nach sich zieht.

Das ist eine ebenso überfällige wie scharfe Warnung an Länder wie Russland, China oder Nordkorea, die bisher glaubten, sie könnten straflos mit solchen Attacken davonkommen.

5.1.8. Interview mit einem Hacker

Der amerikanischen Sicherheitsfirma WhiteHat Security ist es 2013 gelungen, ein Interview mit einem ehemaligen Hacker zu führen, der jetzt als Sicherheitsberater arbeitet. Nachfolgend einige Aussagen des Hackers:

„Mit einem Botnetz Geld zu verdienen ist einfacher als Zähneputzen."

Mit dem *„Aufbau von Botnetzen ... lässt sich das meiste Geld verdienen – mehrere Tausend Dollar am Tag!"*

„Die größte Zahl an Bots, die ich jemals gleichzeitig kontrolliert habe, lag bei 570 000."

„Viele Nutzer wissen ja nicht einmal, dass ihre E-Mail-Adressen über ihre Facebook-Profile öffentlich einsehbar sind und sich wunderbar an Spammer verkaufen lassen. Das Abgreifen lässt sich natürlich automatisieren und damit Geld verdienen."

Startup-Unternehmen ohne qualifizierten Administrator haben meist *„ihr DNS nicht im Griff, was den Schutz vor Cache Poisoning angeht. Ein geräuschloser Einbruch in deren Datenbank ist in weniger als einer Stunde vollzogen."*

„Denken Sie immer daran, dass der Kriminelle dem, was es an Sicherheitstechnologie zu kaufen gibt, zehn Schritte voraus ist. Wenn eine Zero-Day-Schwachstelle öffentlich wird, ist sie bereits seit Monaten im Einsatz gewesen."

Wie empfinden Sie die Gefahr, doch einmal ins Gefängnis zu müssen? *„Es ist sehr schwierig, die Beweise für unsere Schuld zusammenzubekommen – das gestohlene Geld ist sogar unmöglich zu finden."*

Nachzulesen:

`http://www.computerwoche.de/a/mit-einem-botnetz-geld-zu-verdienen-ist-einfacher-als-zaehneputzen,2540793`

Interessant ist auch die Meinung des IT-Sicherheitsexperten Dan Kaminsky: „Niemand weiß, wie man Computer wirklich sicher macht".

`http://www.zeit.de/digital/datenschutz/2015-06/bundestags-hack-it-sicherheit-dan-kaminsky`

Eine Analyse des Dark Web vom Antiviren-Spezialsten trendmicro:

`http://www.trendmicro.de/media/wp/tl-forschungspapier-deep-web-whitepaper-de.pdf`

5.1.9. Einige englische Fachbegriffe

Exploit
: ein Befehlscode, der eine Sicherheitslücke oder Fehlfunktion einer Anwendung ausnutzt (vom englischen „to exploit = ausnutzen)

Vulnerability
: Sicherheitslücke

Cross-Site-Scripting (XSS)
: „Webseiteübergreifendes Scripting": Bösartiger HTML-Code wird in eine vertrauenswürdige Webseite eingefügt.

Cache Poisoning
: wörtlich: Cache-Vergiftung. Ein DNS-Server merkt sich in seinem Cache-Speicher die Antworten der übergeordneten DNS-Server, um wiederholte Anfragen schneller beantworten zu können. Durch Einschmuggeln falscher Einträge können Nutzer des DNS-Servers auf gefälschte Webseiten umgeleitet werden.

Honeypot
: Die Bezeichnung basiert auf der Idee, dass man einen Bären mit Honig anlocken bzw. von anderen Zielen ablenken kann. Analog verwendet man PCs oder Server, die so programmiert sind, dass sie ein attraktives Ziel für Malware darstellen. Beispielsweise kann ein ungeschützter, unbenutzter Honeypot-PC in einem großen Firmennetzwerk eingesetzt werden, in dem alle anderen PCs gut geschützt sind. Ein Angreifer, der das Netz auf Schwachstellen untersucht, wird zwangsläufig den Honeypot zuerst angreifen. Da der Honeypot-PC im Netzwerk keinerlei Aufgaben hat, ist jede Aktivität auf dem Honeypot-PC das Ergebnis eines Angriffs. Dadurch kann ein Angriff erkannt und analysiert werden.

5.1.10. Die Sicherheitslücke „Buffer Overflow“

„Buffer Overflow“ (Zwischenspeicher-Überlauf) ist eine der häufigen Ursachen für Sicherheitslücken und sei hier beispielhaft erklärt. Die Bezeichnung stammt aus der Programmierung und bezeichnet im Wesentlichen einen Programmfehler, bei dem ein Programmierer für bestimmte Daten weniger Speicher zur Verfügung gestellt hat, als maximal benötigt werden könnte. Wenn eine unerwartete große Menge Daten ankommt, so ist der zur Verfügung gestellte Puffer nicht ausreichend groß: er läuft über. Was sich hinter dem Ende des Puffers befindet – ob Programmcode oder Daten – wird von den überzähligen Bytes überschrieben, d. h. zerstört. Wenn es sich bei den überzähligen Bytes nicht um ein zufälliges Muster, sondern eine sorgfältig ausgesuchte Bytefolge handelt, kann dem Betriebssystem ein Stück Schadcode untergeschoben werden.

Ob Betriebssystem oder Anwendungsprogramm – jedes Programm besteht aus einer gewaltigen Anzahl von Unterprogrammen, die aus kleineren Unterunterprogrammen bestehen, welche aus noch kleineren Unterunterunterprogrammen zusammengesetzt sind usw. In der Regel wurde jedes Unterprogramm von einem anderen Programmierer(team) geschrieben. Die am häufigsten benötigten, mehrfach nutzbaren Unterprogramme werden zu Standardprogrammbibliotheken zusammengefasst.

Wenn alle Unterprogramme fertig programmiert sind, werden Sie von einem „Compiler“ in Maschinensprache übersetzt und zusammengefügt. Jedes Unterprogramm besteht aus einem Code-Teil (Befehle) und einem Daten-Teil (Konstanten, Variablen und Bereiche für Daten). Im fertigen Programm wechseln sich Code- und Datenteile ab.

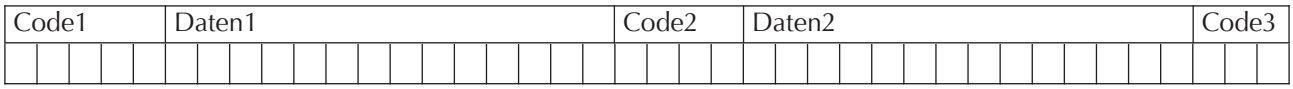

Abb. 5.1: Abfolge von Code und Daten in einem Programm

Nehmen wir an, das Unterprogramm Code1 des Browsers kopiert eine Webadresse in den Datenbereich Daten1, der Platz für maximal 14 Zeichen hat. Anschließend wird das Unterprogramm Code2 aufgerufen.

Was passiert, wenn die Webadresse länger als 14 Zeichen ist und der Programmierer von Code1 vergessen hat, die Länge der Adresse zu prüfen? Das Programm Code2 würde überschrieben werden, und wenn die CPU das Programm Code2 ausführt, stehen dort falsche Befehle.

Man kann einer Bytefolge nur selten ansehen, ob es sich um Befehlscode oder Daten handelt. Und die CPU kann das schon gar nicht unterscheiden. Wenn sie Daten vorfindet, wo ein Befehl stehen müsste, interpretiert sie die Daten als Befehle – was auch immer dadurch geschieht. In der Regel stürzt das Programm (der Browser) ab.

Die höchstqualifiziertesten Hacker untersuchen monatelang Byte für Byte den Code des Browsers und anderer Programme nach möglichen Problemen. Wenn ein Hacker diese Sicherheitslücke (die fehlende Längenkontrolle) entdeckt hat, würde er sich eine überlange Webadresse ausdenken, deren erste 14 Byte den Bereich Data1 füllen. Ab Byte 15 würde er ein kleines Programm unterbringen, welches anstelle von Code2 ausgeführt wird. Dann müsste er nur noch jemanden finden, der diese speziell ausgetüftelte Webadresse mit seinem Browser aufruft.

Was würden Sie denken, wenn Sie den folgenden Text auf einer Webseite oder in einer HTML-Mail sehen?

Über den Link http://www.microsoft.de/demos/A3265 können Sie Windows 10 zum Einführungspreis von 20 € bekommen.

Sie denken vermutlich: „Das ist eine Adresse von Microsoft, also vertrauenswürdig, und das Angebot ist toll!“

Doch schauen Sie sich den Quelltext an:

Über den Link http://www.microsoft.de/demos/A3265 können Sie Windows 10 zum Einführungspreis von 20 € bekommen.

Der Microsoft-Link ist nur Fassade! Beim Anklicken würde die Adresse www.1 └ë┬╢WW╡HT│?╨!sσ╚LΛ!æ12Ł4L┘11 angesteuert. Könnte es eine russische oder chinesische Webseite sein? Das wäre möglich. Der Browser würde eine solche Zeichenfolge nicht beanstanden, und ein Antivirenprogramm auch nicht. Doch tatsächlich ist in dieser Zeichenfolge ein kleines Programm in Maschinensprache versteckt:

```
100 31C0     XOR     AX,AX
102 89C3     MOV     BX,AX
104 BA5757   MOV     DX,5757
```

```
107 B94854   MOV     CX,5448
10A B43F     MOV     AH,3F
10C CD21     INT     21
10E 730F     JNB     0120
110 B8024C   MOV     AX,4C02
113 CD21     INT     21
115 B93132   MOV     CX,3231
118 B534     MOV     CH,34
11A 89C1     MOV     CX,AX
11C BE3131   MOV     SI,3131
11F 90       NOP
```

Mit einer Befehlsfolge in dieser Länge (32 Byte) könnte man beispielsweise eine auf Festplatte befindliche Datei einlesen und auf eine genau ausgewählte Stelle im Arbeitsspeicher schreiben. Webadressen dürfen 127 Byte lang sein. Um ein Schadprogramm aus dem Web herunterzuladen und unbemerkt zu installieren, sind diese 127 Byte mehr als ausreichend.

Das ist nur ein Beispiel von unzähligen Möglichkeiten.

Bleibt die Frage: Wie kann ich überprüfen, ob hinter einer vertrauenswürdig scheinenden Adresse (wie im obigen Beispiel) eine andere Adresse versteckt ist? Wenn man im Firefox, Chrome oder Internet Explorer mit der rechten Maustaste auf einen leeren Teil einer Webseite oder einen Text klickt, kann man im Kontextmenü den „Quellcode anzeigen“ bzw. „Seitenquelltext anzeigen“ lassen. Es geht auch über „Ansicht“ → „Quelltext anzeigen“. Beim Firefox-Browser funktioniert zusätzlich die Tastenkombination Strg-U. Doch im Quelltext einer kompletten Webseite etwas Verwertbares zu finden ist fast unzumutbar. Viel einfacher ist es, mit der rechten Maustaste auf einen Link zu klicken und sich dann die „Eigenschaften“ anzeigen zu lassen.

Wie man sich den Quelltext einer HTML-Email ansehen kann, ist in Kapitel 6.1.6. „Verdächtige Mail gefahrlos prüfen“ beschrieben.

In welchen Programmen wurden die meisten Sicherheitslücken gefunden? Kaspersky zitiert aus der Datenbank des „National Institute of Standards and Technology“ von 2012: 42 % Adobe Reader, 27 % Java, 2 % Adobe Flash. Alle andere Software zusammengenommen: 29 %.

Quelle: `http://www.kaspersky.com/de/internet-security-center/infografiken/software-sicherheitsluecken`