52. UKW-Tagung Weinheim

Sicherheit im Internet – Typische Angriffsszenarien

Dipl.-Ing. Erich H. Franke, DK6II

erich.franke@afusoft.com

Die Probleme durch Schadprogramme beschäftigt Insider schon lange Jahre. Ich habe bereits 1990 auf dieser Tagung einen Vortrag zu diesem Thema gehalten [EHF_90]. Vieles aus meinem damaligen Beitrag ist heute zwar im Detail vielleicht überholt, doch die grundlegende Plage durch Schadprogramme aller Art hat sich bis heute vervielfacht und kostet die Anwender zunehmend Nerven, Zeit und auch viel Geld. Lassen Sie uns anschauen, welche Probleme heute *en vogue* sind.

Königsbach-Stein, im Juli 2007

Motivation

Die Grundlagen der „klassischen“ Viren reichen schon sehr weit in die Computergeschichte zurück. Studien über Programme, die sich selbst vervielfältigen können sind bereits in den siebziger Jahren angestellt worden, damals jedoch im universitären Bereich und nicht als Träger von Schadroutinen.

Computersicherheit war im Zeitalter von Zentralrechnern mit angeschlossenen Terminals im „Time sharing“ Betrieb und in eben diesem universitären Umfeld noch nicht wirklich relevant.

Das Wort „Hacker“ war noch nicht in aller Munde, jedoch war die Neugier für Computerleute schon seit jeher eine starke Triebfeder: „Mal schauen, was es in den Rechnern denn so alles gibt!“

Wer die „magischen Fähigkeiten“ hatte, seine Druckjobs zu beschleunigen, mehr von der wertvollen Rechenzeit zu ergattern oder dem einen oder anderen eine Spaßnachricht auf das Terminal zu schicken, war bei Freunden und Kommilitonen hoch angesehen. Dazu brauchte man nur gute Insider-Kenntnisse und die richtigen Passworte, dann war alles klar.

Mit zunehmender Verbreitung vernetzter Rechner begannen immer mehr Leute sich für fremde Computer zu interessieren. Es gab zwar keinen festgeschriebenen Kodex, jedoch jeder „Datenreisende“[1] war darauf erpicht, dass sein „Besuch“ in einem fremden Rechner möglichst unentdeckt blieb. Man wollte ja die Administratoren nicht dazu provozieren, die Sicherheitsmaßnahmen zu verändern.

„*Real Hackers don’t mess with data*! “[2] war einer der Leitsprüche dieser Epoche.

Doch diese unschuldigen Zeiten sind längst vorbei.

Mehr und mehr verbreiten sich vorgefertigte Angriffsprogramme in Form quietschbunter „Virenbaukästen“ oder als ausführbare „Skripte“, die ohne eigenes Know-How von jedermann auch ohne eigene Kenntnisse angewandt werden können. Damit tummeln sich die „*Skript Kiddies*“ in den Netzen, Hacker der untersten Kaste, die mangels eigenen Wissens nur vorgefertigte Angriffe starten können. Die Gefahr die von diesen Leuten ausgeht ist jedoch immens. Sie besteht hauptsächlich darin, dass diese ihre Befriedigung häufig nur aus purem Vandalismus ziehen und damit großen Schaden anrichten.

Computerspezialisten die über eigenes Know-How verfügen, beginnen hingegen in zunehmendem Maße auf dem Freien Markt ihr spezialisiertes Wissen zu Geld zu machen. Das ihnen in der heutigen leistungsorientierten Gesellschaft auch nicht zu verdenken.

Zum Beispiel verdingt sich ein Teil der Hacker als so genannte „*White Hat*“[3] als Berater in der Sicherheitsindustrie, schreiben zum Teil exzellente Fachartikel oder produzieren selbst Sicherheitssoftware.

Hingegen ist ein nicht kleiner Teil der restlichen Hackergemeinde als *Black Hats*“[4] inzwischen in die Kriminalität abgewandert.

---

[1] Ich bin mir dessen nicht sicher, doch ich glaube der CCC in Hamburg prägte diesen Begriff

[2] Wirkliche Hacker verändern keine Daten

[3] White Hat-> Der weiße Hut der „guten“ Cowboys im Western

[4] Black Hat-> Den tragen im Western meistens die Schurken

Allerdings sind die Wenigsten davon reine Vandalen. Sie haben sich vielmehr zur Unterstützung kriminelle Aktivitäten verdungen, wie zum Beispiel zum *Spamming* (Unerwünschte Massen-Mails), Ausspähen kommerzieller Daten oder zum so genannten „*Phishing*“[5] oder ganz einfach zum massenweise „*Cracken*“[6] von Medien, Spielen und Programmen.

Diese Aktivitäten sind für die Mehrheit der Computeranwender äußerst lästig und erzeugen inzwischen ganz erheblichen wirtschaftlichen Schaden.

Um als *Black Hat* in der Szene und bei seinen zwielichtigen Kunden anerkannt zu sein, muss dieser über eine entsprechend große Plattform „gecrackter“ Computer verfügen, deren Leistung er dann am Markt verkauft. Diese Rechnernetze nennt man auch „*Bot-Nets*“[7]. Die gecrackten Rechner in einem Botnet werden meistens als *Drohnen*[8] bezeichnet.

Der Speicherplatz gecrackter Computer wird besipielsweise gerne zur Archivierung illegalen Materials wie „*Moviez*“ (gecrackte Filme und Musik), „*Warez*“ (gecrackte Software und Spiele) oder einfach für Hardcore-Porno benutzt. Hat ein Hacker beispielsweise eine Serverfarm eines Internetproviders kontaminiert, so können illegale Daten dort lange lagern und aus der Fangemeinde abgerufen werden, ohne dass Rückschlüsse auf den eigentlichen Verursacher gezogen werden können. Im Zweifelsfall bekommt der Betreiber des Servers Ärger, obgleich er von diesen Dingen meist gar nichts weiß.

Zum anderen sind Systeme mit dauernder Internetanbindung für den *Black Hat* interessant. Ein kontaminierter Rechner kann als Relais für Massen-Mails (*Spam*) dienen. Dies ist für die Anbieter dieser Plage besonders beliebt, da diese verteilten Quellen nicht so einfach verstopft werden können. Im Zweifelsfall gerät der unschuldige und unwissende Computerbetreiber in das Visier der Fahnder und der *Black Hat* und seine Auftraggeber bleiben im Dunkeln.

Mit Spionage müssen vor allem Industrieunternehmen rechnen. Ist das Ausspähen militärischer Geheimnisse weitgehend in den Hintergrund getreten, besteht eine nicht zu vernachlässigende Bedrohung durch das Ausspähen kommerziellen und wissenschaftlichen Know-Hows von Unternehmen. Die Dunkelziffer ist verständlicherweise recht hoch, doch Behörden nehmen dieses sehr ernste [BSI].

Selbstverständlich wird kein *Black Hat* vom eigenen heimischen PC aus aktiv um in einen Firmenrechner einzudringen! Die Gefahr einer Entdeckung und Rückverfolgung wäre viel zu hoch! Auch hier wird er sich seines Botnets als Relaisstelle bedienen.

Daher sind die *Black Hats* ständig bestrebt, weitere Rechner aufzuspüren und unter ihre Kontrolle zu bringen. Dazu stehen ihnen zahlreiche Mittel zur Verfügung.

Bedrohungsszenarien

Das älteste Infektionsverfahren ist der „klassische“ Virus. Seine Hochphase war in der Vergangenheit, als nur wenige Rechner miteinander vernetzt waren und daher das Medium „Diskette“ zur Übertragung notwendig war. Ich habe darüber bereits ausführlich geschrieben [EHF_90]. Lassen Sie uns kurz Revue passieren.

Ein Virus „befällt“ ein gespeichertes Programm bzw. eine „aktive Komponente“ indem es sich in diesem Programm einnistet. Somit verbreitet sich ein Virus zwar auf einem Computer meist von selbst. Zum Sprung von Computer zu Computer benötigt er jedoch den Menschen – wörtlich genommen – als Daten-Träger.

Bis Anfang 2000 sind klassische Viren praktisch verschwunden. Inzwischen regt es sich wieder an der Virusfront. Die Verwendung von USB-Speichersticks als Transportmedium macht es möglich. Ebenso die Tatsache, dass in modernen Betriebssystemen zahlreiche Dateiformate multi-mediale und sogenannte „aktive“ Inhalte besitzen können.

Ein Virus ist immer darauf angewiesen, dass das infizierte Medium in irgendeiner Weise „ausgeführt“ wird, d.h. die Kontrolle über die CPU erhält. Dann werden der Fortpflanzungs- sowie der Schadanteil wirksam und das Drama beginnt.

Die dabei verwendeten Techniken stammen zwar aus der Vergangenheit, sind aber immer noch aktuell und gefährlich.

---

[5] Abfischen von Kundendaten. Das „Ph“ ist Jargon und hat eine lange Historie bei den Freunden des U.S.-amerikanischen Telefon-Netzes

[6] Das (strafbewehrte) Entfernen der Kopier- oder Nutzungssperre

[7] Als Abkürzung von Robot Network

[8] In *Startrek* werden die Mitglieder des Borg-Kollektivs ebenfalls als Drohnen bezeichnet

Polymorphe Viren verändern sich bei jedem Fortpflanzungszyklus selbst und versuchen damit, sich vor den statischen Signaturen der Virenscanner zu verstecken. So genannte „Stealth"-Viren verhindern ihre Entdeckung, indem sie Betriebssystemsroutinen manipulieren und damit versuchen, diese zu blenden. Eine ähnliche sekundäre Technik wird in den sogenannten Root-Kits verwendet. Hierin steckt eine Menge krimineller Energie, die inzwischen auch schamlos – mithin illegal – von der Musik- und Filmbranche zu radikalen Kopierschutzmaßnahmen verwendet wird [KFILM]. Wir werden dies später eingehend diskutieren.

Im Gegensatz zum Virus, der auf einen Überträger angewiesen ist, bewegt sich der „*Wurm*" selbsttätig durch Netzwerke. Würmer sind darauf programmiert, Sicherheitslücken im Opferrechner zu nutzen. Der Wurm-Code stellt auf dem Zielrechner eine Kopie von sich selbst her um sie dort auszuführen. Damit beginnt von dort das Spiel von Neuem.

Ein Wurm alleine stellt zwar im eigentlichen Sinne noch keine Bedrohung dar. Doch in den allermeisten Fällen dient er als Träger einer Schadroutine, die wiederum sehr unterschiedliche Auswirkungen haben kann.

Der erste bekannt gewordene Virus-Zwischenfall legte am 2.11.1988 in den U.S.A. ca. 2600 Rechner lahm. Robert Tappan Morris Jr. gelangte hierdurch zu einer zweifelhaften Berühmtheit [MWORM]. Der Wurm fiel nur dadurch auf, dass der Mechanismus, der die Re-Infektion ein und desselben Rechners verhindern sollte aufgrund eines Softwarefehlers versagte. Doch das Design enthielt eine Menge an krimineller Energie, wie z.B. Stealth-Techniken und war dazu geeignet, das erste Botnet aufzubauen.

Moderne Varianten wie „*Sasser*" [SASS] der im April 2004 im Feld auftrat, *phatbot* („fat bot", fetter Roboter), und *Netsky* waren noch wesentlich ausgefuchster. Die Würmer verbreiten sich unter Ausnutzung von Schwachstellen im Betriebssystem ohne Zutun der Benutzer durch direkte IP-Kommunikation. Die Programmierer sind zum Teil recht hoch qualifiziert jedoch mit viel Freizeit gesegnet.

Die Täter werden in der Presse leider häufig zu Unrecht glorifiziert [NETSKY]. In Wirklichkeit sind diese Produkte keine technische Spielerei sondern dienen den *Black Hats* als wichtiges Einbruchswerkzeug. Der Wurm ist also eher etwas wie das Brecheisen oder der Vorschlaghammer in den Händen eines Einbrechers. Hierdurch wird für den Täter der Prozess des Crackens automatisiert und damit beschleunigt, was bei der Größe normaler Botnets von tausenden von befallenen PCs erforderlich ist.

Als Detail ist am Rande anzumerken, dass phatbot ein gutes Beispiel dafür ist, welcher mörderische Konkurrenzkampf zwischen vielen *Black Hats* tobt. Phatbot entfernt bestimmte konkurrierende Würmer um den Rechner für sein eigenes Botnet sicherzustellen. Letztendlich geht es dabei eben um Geld!

Die allfälligen email-Würmer sind fast zu simpel für eine eingehende Diskussion. Emails enthalten in ihren Anhängen ausführbare Anteile, die, wenn sie durch unvorsichtiges Öffnen aktiviert wurden, sich die Adresseinträge des email-Programmes schnappen und in Kopie an all diese Email-Empfänger versenden.

Dadurch, dass es den Menschen bzw. dessen Neugierde oder Ängste benötigt – die email öffnet sich ja nicht von selbst – klassifiziert man diese Art gerne unter der Rubrik „Trojanisches Pferd".

Der Name Trojanische Pferd geht auf die Sage mit dem Holzpferd zurück, welches die Trojaner aus eigener Kraft in ihre Stadt gezogen hatten und das eine unerwartete und unerwünschte Überraschung enthielt.

Genau so verhält es sich mit der digitalen Variante. Verspricht Ihnen der email-Inhalt auch billiges Viagra oder die Nacktphotos der Nachbarin, oder werden Sie in horrend schlechtem Deutsch mit einem Strafbefehl oder einer exorbitant hohen Rechnung konfrontiert, so sollten Sie den Anhang dieser Nachricht nicht einmal mit einer Beißzange anfassen! Selbst Text- oder Bilddokumente können – passend verfälscht – aktive Inhalte auf Ihrem Computer freisetzen sobald sie geöffnet und damit aktiviert wurden. Und die einmal gerufenen Geister wird man dann nicht mehr so leicht los.

Ebenso grob fahrlässig ist es, Software aus nicht zweifelsfrei identifizierbaren Quellen zu laden und auszuführen. „Never accept software from strangers!"[9] Dieser alte Satz gilt heute umso mehr!

Es ist nicht sinnvoll, sich alleine auf einen Virenscanner zu verlassen. Die Scanner können Bedrohungen nur melden, wenn diese in den Signaturen bereits berücksichtigt sind. Da jedoch die Analyse neuer Bedrohungen, besonders bei polymorphen Inhalten eben seine Zeit dauert, sind selbst die bes-

[9] Nehmen Sie von Fremden keine Programme an!

ten Scanner blind und taub, so lange diese nicht auf den „allerneuesten“ Stand gebracht wurden. Und das kann im weltweiten Kontext allen Versprechungen zum Trotz durchaus Wochen dauern.

Die „logische Bombe“ ist ein Schadprogramm, welches sich nicht verbreitet, sondern mit Absicht beispielsweise durch einen Innentäter hinterlegt wird. Die Szenarien reichen vom „frustrierten Angestellten“ der sich an seinem Arbeitgeber rächen will und Datenbestände manipuliert bis hin zur internen Vorbereitung eines späteren Einbruchs von außen.

Unter die technisch sekundären Bedrohungen zählt das gefährliche „Phishing“. Unter Vortäuschung einer falschen Identität versuchen Täter ihre Opfer zur Preisgabe von PIN-Codes, Kreditkartennummern etc. zu bewegen.

Dies erfolgt häufig über verfälschte Mails bzw. Websites. Hierin steckt noch ein immenses Gefahrenpotential. Selbst für informierte und ausgebildete Benutzer sind diese Fälschungen nicht in jedem Fall zweifelsfrei zu erkennen. Selbst mit dem allergeringsten Aufwand können auf den ersten Blick glaubhaft erscheinende Falsifikate erstellt werden, wie eine Gruppe meiner Studenten im Rahmen einer Projektarbeit untersucht hat [PHIS].

Bei der Menge der weltweit durchgeführten Phishing-Angriffe genügt bereits eine geringe Erfolgsquote um großen Schaden hervorzurufen.

Die Ergebnisse – Datenbanken mit Kreditkartennummern, Pin-Codes etc. – werden auf dem freien Markt angeboten. Mit ihnen können „Hit-and-Run“10-Täter hohen Schaden verursachen.

Eine weitere sekundäre Technik beinhaltet das Unterbrechen des Betriebs einer Site oder eines Teilnetzes. Es gibt eine Reihe von Angriffstechniken, um Computer kurzzeitig am Netzbetrieb zu hindern. Manchmal genügt dies, um eine kriminelle Handlung durchzuführen oder einfach nur Vandalismus zu betreiben.

Ist das Unterbrechen einer ebay-Auktion vielleicht nur ein kleinkrimineller Akt, so kann die Unterbrechung eines DNS-Servers mit kurzzeitiger Übernahme der DNS-Funktion durch einen Piratenserver zwecks anschließender „Vergiftung“ der DNS-Caches angeschlossener Computer zur Vorbereitung einer ernsthaften Straftat dienen.

Angriffswege und -ablauf

Der überwiegende Anteil der Angriffe auf Rechner muss zwangsläufig „von außen“, d.h. über die normalen Netzwerkschnittstellen erfolgen.

Im Regelfall wird der Angreifer mit Hilfe automatisierter Skripte versuchen, im Betriebssystem oder den laufenden Anwenderprogrammen auf diesen Rechnern eine Schwachstelle zu finden, die er ausnutzen kann. Man nennt diese ausnutzbaren Schwachstellen auch „*exploits*“[11].

Er muss unter den unzähligen Computern im Netz erst einmal einen geeigneten Kandidaten für seine Angriffe finden.

Hierzu dient gewöhnlich ein sogenannter *Port Scan* mit anschließender Klassifikation. Hierfür gibt es eine Reihe von Programmen, die mit verblüffender Treffsicherheit die Art des Betriebssystems und dessen Version aus den Antworten auf unschuldig wirkende Pakete ablesen können.

Dies ist für die nächste Phase, nämlich das Analysieren der Schwachstellen eminent wichtig. Meistens passen „exploits“ wie Schlüssel in ein Schloss nur für eine ganz bestimmte Version von Betriebssystemen, nämlich die, die auch wirklich die dem exploit zu Grunde liegende Schwachstelle enthält.

Diese Analyse und die Überwindung einer solchen potentiellen Schwachstelle sind heutzutage voll automatisierte Prozesse. Das Bild das Hollywood und die Regenbogenpresse von dem feisten Menschen zeichnet, der zwischen Coladosen und Pizzakartons virtuos auf seiner Tastatur spielt hat weitgehend ausgedient. Wie in allen Bereichen unserer Gesellschaft ist Effizienz gefordert und der Konkurrenzdruck zwingt demnach auch *Black Hats* zur Automatisierung und Rationalisierung.

Es gibt auch Alternativen zur reinen Exploits. Unter „Social Engineering“ versteht man, menschliche Schwächen – Freundlichkeit und Hilfsbereitschaft bis hin zur schlichten Dämlichkeit – dazu auszunutzen, an für den geplanten Einbruch relevante Informationen zu gelangen. In dem sehenswerten Kinofilm „War Games“ [WARG] wird ziemlich glaubhaft dargestellt, wie der Hauptdarsteller zu seinem

---

[10] Zuschlagen und weglaufen

[11] Engl. To exploit: ausnutzen, ausbeuten

Passwort kommt. Dies liegt nämlich in der obersten Schreibtischschublade und ist fein säuberlich aufnotiert.

Dieses Szenario ist vollkommen realistisch. Bei Sicherheits-Audits findet man immer wieder Passworte auf einem Notizzettel auf den Monitor geklebt, wo es von jedem Besucher gesehen und notiert werden kann.

In dem Film wurde auch das Erraten eines anderen Passwortes völlig glaubhaft dargestellt. Die Hauptperson beschaffte sich persönliche Informationen aus verschiedenen Quellen und kam damit auf das gesuchte Wort, in diesem Fall der Name des Sohnes des Opfers. Auch heute noch werden von vielen Nutzern einfach die Namen von Angehörigen, Haustieren oder auch von Filmgestalten gerne als Kennworte benutzt.

Die meisten Angriffsprogramme führen ganze Bibliotheken mit derartigen Begriffen mit sich. Diese so genannte „Dictionary Attack“ kann sehr viel schneller - und mithin effizienter – ausgeführt werden wie ein „Brute Force“[12]-Angiff auf die Passworte, bei denen einfach alle Zeichen permutiert werden.

Ich würde auch nicht völlig ausschließen wollen, ob nicht vielleicht auch ein freundlich-hilfloser Anruf beim Systemadministrator mit Bitte um Rücksetzen des Kennwortes positiv ausgeführt wird.

Die meisten „Rückfragen“ die dann gestellt werden sind eher ein Scherz denn eine Sicherheitsmaßnahme. Da wird oft nach dem Geburtsdatum gefragt, oder nach Namen und Abteilungsbezeichnung oder der Adresse. Dies sind alles Informationen, die sich ein Angreifer im Vorfeld aus offenen Quellen leicht beschaffen kann.

Selbstverständlich werden wir absolute Sicherheit nicht erreichen können. Doch indem wir jede Information als vertraulich behandeln, machen wir einem potentiellen Angreifer das Leben schwerer indem wir die Messlatte höher hängen. „*Don’t give the hacker any clue!*“[13] ist ein gutes Leitmotto.

Selbst wenn der Administrator das Kennwort nur an einen bestimmten Benutzer als email sendet ist keine Hilfe, wenn der Angreifer physischen Zugang zum Netzwerk oder gar zu dem anzugreifenden Computer hat.

Damit kommen wir zum physischen Angriff: „*Boot access is root access*!“[14] Wenn der Angreifer auch nur kurze Zeit unbeobachtet über den Computer verfügen kann, verhilft die mitgebrachte Knoppix-CD oder der entsprechend präparierte USB-Stick per Neustart dem Angreifer zu allem was er benötigt.

Selbstverständlich lassen sich verschlüsselte Festplatten und Ähnliches so einfach nicht knacken. Manchmal ist auch die Funktion zum Hochfahren des Rechners von USB-Speichern, CD und Diskette - falls es so etwas noch gibt – auch schlichtweg abgeschaltet. Doch werden in vielen Fällen aus Kostengründen einfache Standard-PC verwendet und ohne die genügende Sorgfalt eingesetzt. Und genau dies gibt diesem Angriff eine ordentliche Erfolgswahrscheinlichkeit.

Ist der Angreifer einmal „drin“ so geht es in den meisten Fällen nur noch darum, Administrator- bzw. root-Rechte zu erlangen. Unter dem Begriff „*raise of privilege*“[15] versteht man diese Technik. Da der Angreifer die volle Kontrolle über das System benötigt, braucht er möglichst weit reichende Rechte.

Hier ist der Angreifer von Außen sogar ein wenig im Vorteil. Wie schon der Moore-Wurm [MWORM] attackieren exploits meistens anfällige Betriebssystemsprozesse durch Techniken wie beispielsweise die altehrwürdige „*Buffer Overflow*“[16]-Attacke. Gelingt es nun einen Betriebssystemsprozess zu zerschießen und zu übernehmen, so läuft das Angreiferprogramm nun mit den Rechten des Opfers – in den meisten Fällen also im Kontext des Betriebssystems, ein El Dorado für jeden *Black Hat*.

Nun gilt es noch, sich den Zugang für spätere Besuche zu sichern. Passworte können sich ändern. Und der Angriff auf das Betriebssystem geht häufig auch nicht spurlos vorbei. Prozesse können vorzeitig beendet werden oder Logbucheinträge wurden erstellt, aus denen der Systemadministrator vielleicht Rückschlüsse auf einen Angriff ziehen kann. Das wäre dem *Black Hat* nicht recht.

Hat sich ein Schädling erst einmal eingenistet, so öffnet er Kommunikationsverbindungen, über die er sich – im Falle des Wurms – fortpflanzen kann um mit seinem Herrn und Meister Kontakt aufzunehmen. Damit teilt er ihm dann mit, dass die neue Drohne in das Kollektiv eingegliedert worden ist. Na-

---

[12] „Brutale Gewalt“: Der Angreifer probiert einfach jede Zeichenkombination durch. Dagegen helfen lange Passworte.

[13] Gib dem Hacker keinen Anhaltspunkt

[14] Grob übersetzt: „Wenn Du den Rechner selbst hochfahren kannst, hast Du damit auch Administratoren-Rechte

[15] Erhöhung der Berechtigungsstufe

[16] Puffer-Überlauf

türlich geht das nicht über direkte Wege. Meistens werden Chats dazu missbraucht, derartige Informationen weiter zu leiten.

Ältere Programme, aber auch noch *sasser* und *phatbot* öffneten noch „wilde Ports“ um zu kommunizieren. Doch vergleichbar mit einer Funkstation, die außerhalb üblicher Bänder sendet fällt dies heute meistens gerade auf.

Daher benutzen mehr und mehr Schadprogramme als Hintertür unauffällige Ports wie 80 (http[17]) oder gar 443 (https). Mit letzterem ist der Verkehr sogar verschlüsselt, so dass der Angreifer ungestört kommunizieren kann. Ein zentraler „Corporate Firewall“ kann den Verkehr des Schädlings nicht von beispielsweise einer Update-Sitzung oder normalem Browsen unterscheiden.

Über diese Protokolle sind öffentliche Chats problemlos erreichbar und das Schadprogramm kann sogar einfach auf Befehle seines Meisters warten, die in Form unschuldig aussehender Texte hinterlegt sind. Diese konspirative Arbeitsweise macht die Situation heute gefährlicher denn je.

Glücklicherweise installieren inzwischen viele Nutzer einen „Personal Firewall“, freie Produkte wie Zone Alarm [ZAL, kommerzielle Produkte wie [SYMAN] oder verwenden – sofern sie ein Windows-Betriebssystem nutzen den eingebauten Microsoft Firewall.

Der Trick dabei ist, dass im Gegensatz zum zentralen „Corporate Firewall“ der „Personal Firewall“ Kenntnis über den Absender-Prozess auf dem System hat.

Sollte Ihr Firewall also plötzlich melden, dass http-Verkehr von einem unbekannten Programm ausgeht und Sie nicht surfen, sollten Sie sehr misstrauisch werden!

Insgesamt wird das Schadprogramm versuchen, sich auf Ihrem Rechner so unauffällig wie möglich zu verhalten, so dass Sie als Nutzer oder als Administrator nicht misstrauisch werden und den Schädling vorzeitig entdecken, denn Ihr Rechner soll ja schließlich als Drohne im Botnet des *Black Hat* dienen.

Somit schließt der Angriff häufig damit, dass alle verräterischen Spuren beseitigt werden. Im einfachsten Fall werden Logdateien manipuliert, so dass suspekte Einträge einfach nicht mehr auftauchen oder durch nichts sagende Texte ersetzt werden. Kein schweres Problem.

Die Königsklasse allerdings stellen die „*Root-Kits*“[18] dar. Auch diese Technik ist schon recht alt doch immer noch aktuell.

Alle Betriebssysteme, von CP/M über MS-DOS bis hin Windows und Unix besitzen interne Datenstrukturen, über die die Dienste auf unterer Ebene gesteuert werden.

Bei CP/M hieß das noch BDOS, bei Windows ist es die „*Service Allocation Table*“. Darin enthalten sind Zeiger, über das die höheren Betriebssystemsfunktionen die Arbeitsdienste aufrufen. Beispielsweise benutzt der Explorer zur Anzeige des Verzeichnisses einige dieser „low-level“-Funktionen.

„Klemmt“ sich nun ein Programm zwischen diese Schichten, so kann es Aufrufe und Antworten nach Belieben manipulieren.

Es könnte so problemlos die Anzeige bestimmter Dateinamen einfach unterdrücken. Das funktioniert nicht nur für Dateien sondern auch für alle anderen Aufrufe, bis hin zu Netzwerkzugriffen, die dann an allen Sicherungen vorbei quasi aus dem vegetativen Nervensystem heraus erfolgen. Ade Firewall, ade Virenscanner! Das *Root-Kit* bildet eine fast perfekte Tarnkappe.

Mit dieser Technik arbeiten mehr und mehr Schädlinge. Perfiderweise hat neuerdings auch die Film- und die Musikindustrie das „*Root-Kit*“ entdeckt. In einem bekannt gewordenen Fall hat ein Filmunternehmen ein Root-Kit zur Tarnung eines radikalen Kopierschutzes benutzt [KFILM]. Durch konzeptuelle Fehler in dieser „Schutz“-Software wird ein Computer, der eine legale Kopie dieses Films abgespielt hat in seiner Funktionsweise eingeschränkt, so dass selbst lange nach Auswurf der Film-CD das „Brennen“ von Daten-CDs behindert wird.

Zwar erkennen moderne Scanner die Urform dieses Root-Kits, doch verbesserte Versionen wären von Viren-Scannern nicht mehr entdeckbar.

Auf UNIX- bzw. LINUX-Systemen funktionieren Root-Kits sogar noch viel eleganter. Da durch das Open-Source-Konzept alle Quellcodes aller Systemteile jedermann zugänglich sein müssen [GNUGPL], kann ein potentieller Angreifer für ihn kritische Betriebssystemsdienste einfach so verändern, dass dieses gegenüber dem Schadprogramm blind ist. Im Service *ps*[19] beispielsweise genügt

---

[17] http: Hypertext Transport Protocol, das grundlegende auf TCP basierende Protokoll zum Web-Surfen

[18] Von *root*, dem Unix-Äquivalent zum Administrator bei Windows

[19] *ps* gibt unter UNIX / LINUX die Liste der aktuell geladenen Prozesse aus

eine Handvoll Manipulationen am Quellcode, dass ein bestimmter Prozessname nicht mehr angezeigt wird. Man nennt diese Technik anschaulich auch „*Trojaned Services*“.

Unsere Gegner

Von Alarmanlagen kennt man, dass der wirkliche Feind nicht etwa der Einbrecher ist. Es ist viel mehr der Fehlalarm und die Schlamperei. Auf der Seite der Computer ist die Situation vergleichbar.

Von den „technischen Schwachstellen“ kennen wir als prominenten Vertreter den „*Buffer Overflow*“. Es gibt noch ein gutes Dutzend anderer Schwachpunkte, die meist mit der Möglichkeit zusammenhängen, Code in aktiven Elementen auszuführen.

Häufig sind nicht abgefangene Wertebereiche bei Variablen an Schnittstellen die Quelle des Übels. Kein Hacker wird sich an Schnittstellenkonventionen hält sondern vielmehr versuchen, durch sorgfältig und gezielt falsch formatierte Werte das System zum fehlerhaften Arbeiten zu bringen und die Instabilität dann auszunutzen.

Es gibt zahllose Erfahrungen über Daten die an Schnittstellen versehentlich zum Vorschein kommen, wenn man diese nur lange genug und bewusst falsch stimuliert.

Doch diese technischen Schwachstellen decken nur einen Aspekt ab.

Fehlkonfigurationen stellen den anderen Teil dar: Viele Systeme werden unter Zeitdruck und Stress „*Out-of-the-Box*“[20] mit Standardwerten konfiguriert. Darunter können durchaus auch Passworte sein. Internet-WLAN-Router sind dabei ein ganz gutes Beispiel.

Oft genug wird das Gerät einfach aufgestellt, angeschlossen – und gut ist’s. „Ich bin drin! Es ist doch ganz einfach!“ Die Auslieferungswerte funktionieren sofort, daher werden sie nicht mehr verändert.

„Das ist doch egal. Der Kasten steht doch eh’ nur bei mir!“ Hin und wieder werde ich mit diesem Argument konfrontiert. Doch ganz so einfach ist das nicht.

Eine Reihe von Produkten besitzen nämlich die Fähigkeit, über das drahtgebundene Netz und die WAN[21]-Schnittstelle umprogrammiert zu werden und dies sogar über einen offenen Dienst (telnet).

Fördert ein Port-Scan des DSL-Nummernbereiches nun solch einen Router zu Tage, so kann jeder der das Standard-Passwort kennt damit herumspielen. Diesen Umstand halte ich nicht für erstrebenswert, denn im Internet werden die Standard-Passworte für die meisten Geräte veröffentlicht.

Hat man nun sogar physischen Zugang zu dem Gerät genügt meist ein kleiner Druck auf die Taste auf der Rückseite – und schwupp – das Gerät nimmt wieder seine Standard-Passworte ein. Hand aufs Herz! Wann haben Sie zum letzten Mal Ihren WLAN-Router überprüft?

Administratoren von Rechnernetzen haben dieses Problem zuhauf. Hier muss man aus praktischen Gründen häufig mit einheitlichen Passworten arbeiten. Doch wenn mehrere Leute diese kennen (müssen), dann besteht immer die Gefahr des Verrates – absichtlich oder unabsichtlich – social engineering lässt grüßen!

Gleiches gilt für den Netzwerkzugang, für ftp-Upload-Accounts und so weiter. Dies alles setzt voraus, dass ausgebildete Menschen das System überprüfen und dass das System wiederum periodisch auf seine Wirksamkeit hin überprüft werden muss. Man nennt diese Überprüfungen auch „Audit“

Hier kommen wir vom rein technischen hin zur Diskussion der organisatorischen Maßnahmen. Schließlich hat die Computernutzung und auch das Problem mit Schadprogrammen mehr mit dem Verhalten von Menschen zu tun als mit Problemen bei Maschinen.

Wir müssen zu Menschen „kompatible“ Verfahren und Abläufe festlegen. Dieser Aspekt stellt den Schlüssel für einen wirksamen Schutz dar:

Ein gutes Beispiel dafür ist die Wahl der Passworte. Selbstverständlich stehen Gandalf, Frodo, Neo und so weiter in jedem besseren Wörterbuch von Angriffsskripten, ebenso so ziemlich jeder angloamerikanische weibliche und männliche Vorname. Die zu nutzen ist keine gute Idee!

Doch was ist, wenn Sie von Ihren Mitarbeitern oder Ehepartnern Kennworte wie „*k7&e%v2$$y*“ abverlangen? Das einzige was Sie damit erreichen ist, dass sie an den Monitoren kleine gelbe Zettel vorfinden werden, auf denen die Passworte fein säuberlich notiert sind. Auch keine wirklich gute Idee!

---

[20] Grob Übersetzt: „Direkt aus der Verpackung“, daher „ohne eigene Kenntnis“

[21] Wide Area Network. Im Falle des Internet-Routers ist das eben das Internet…

Ein Tipp sind so genannte „Pass Phrases“, also Sätze an die man sich erinnern kann. Die “verfälscht“ man dann nach einem einfach zu merkenden, möglichst nicht standardisierten Schema:

Ein Beispiel. Kann sich ein Fan der Serie Simpsons gut an folgenden Satz erinnern: „*Homer hat ein Spider Schwein*“. Dann lässt er einfach die Vokale weg und erhält „*HmrhtnSpdrSchwn*“. Oder man lässt alternativ jeden zweiten Buchstaben weg, oder, oder...

Das, was dabei herauskommt ist sicherlich nicht perfekt – Perfektionisten fordern in Passworten aus gutem (technischen) Grund zusätzlich Sonderzeichen und Ziffern – doch besser als beispielsweise „*Trinity*“ ist das allemal!

Funktionieren Programme auf dem Computer nicht richtig, dann wird sich jeder Benutzer dem Problem nach Möglichkeit entziehen. Liegt die Ursache an den fehlenden Zugriffsrechten einer lieblos ausgeführten Installation, dann wird im Alltag jeder zukünftig eben als Administrator arbeiten.

Hier lohnt sich eine fachgerechte Analyse sehr, denn durch Arbeiten mit Administrator-Rechten ebnet man den Schädlingen geradezu den Weg.

Genauso problematisch sind zu restriktive Proxies und Firewalls. Menschen sind nun einmal schlau! Braucht ein Mitarbeiter das Internet für seine Arbeiten, hat dafür aber keine eigene Berechtigung, so wird er eben einfach den Account eines Kollegen nutzen. Im Ernstfall arbeitet er vielleicht über einen privaten email-Provider, was sämtliche Schutzmaßnahmen hinterrücks aushebelt.

Die kritischste Konstellation die mir in diesem Zusammenhang begegnete befand sich in einem Bürohaus mit mehreren kleinen Firmen.

In dem einen Betrieb war jedweder Zugang zu http und https durch den Firewall grundsätzlich blockiert. Die Mitarbeiter hatten lediglich ein Intranet zur Verfügung.

Diese lösten pfiffig das Problem, indem sie auf dem „kleinen Dienstweg“ das Netz mit dem eines Nachbarbetriebs, welcher liberalere Einstellungen pflegte, verbanden – eine Lösung, die jedem Sicherheitsbeauftragten die Haare zu Berge stehen lassen!

Hier hilft nur, geschickte Lösungen unter Einbeziehung der Mitarbeiter zu finden und deren Bewusstsein für den Nutzen zu schärfen, den sie aus höherer Sicherheit des Betriebes ziehen.

Das gleiche gilt im privaten Einsatz.

Ein unverschlüsseltes WLAN mit Richtantennen zur Freundin zu „verlängern“ rächt sich spätestens dann, wenn auf dem benachbarten Parkplatz ein „*Bad Guy*“ mit seinem Laptop steht, der über diesen bereitwillig geöffneten Weg seine Kinderporno aus dem Netz zieht oder Angriffe auf ebay fährt.

Im Zweifelsfall werden sich die Ermittler an die Person halten, die zu diesem Zeitpunkt die DSL-Verbindung bzw. die IP-Adresse inne hatte. Einen Nachweis, dass die Straftat von einem unbekannten Mit-Surfer per WLAN ausgeführt wurde, dürfte gerichtsverwertbar nicht zu erbringen sein. Pech gehabt!

Übrigens stellt auch die Standard-Verschlüsselung WEP[22] mit 104/128 Bit keinen Schutz mehr dar. Der Rekord mit 51 Minuten, den Shamir 2000 beschrieb ist heute auf wenige Minuten geschrumpft. Da auch hier wieder Angriffsprogramme für jedermann anwendbar im Netz stehen hat man praktisch keine andere Möglichkeit als alte WLAN-Knoten einzumotten.

Was können wir tun?

Ok! Absolute Sicherheit ist nicht zu erzielen. Grundsätzlich ist alles gut, was einem Angreifer die Arbeit erschwert. Denn wenn ein Black Hat bzw. dessen Angriffssoftware Ihr System überhaupt nicht findet, lässt er es in Frieden und wendet sich dem nächsten zu. Das Sankt-Florian-Prinzip auf Elektronisch!

Daher gilt: „Don‘t give the hacker any clue! “

Vermeiden Sie die Veröffentlichung interner Netz-Strukturen und technischer Details. So etwas gehört nicht ins Internet. Auch wenn Sie in Newsgroups technische Fragen stellen: Sie müssen gewahr sein, dass einer der Forumsteilnehmer seinen schwarzen Hut im Schrank liegen hat und jede Information begierig aufnimmt. In jedem Krieg ist Information eine der wichtigsten Größen.

Gleiches gilt für Serverbetreiber: Vermeiden Sie vollmundige Login-Meldungen, wie sie früher mancher Administrator voller Stolz präsentierte, in der Art von: „*Willkommen auf dem Entwicklungsrechner*

---

[22] Wire Equivalent Privacy. Vollmundiges Versprechen, die WEP-verschlüsselte Funkverbindung sei so sicher wie eine Drahtverbindung

der Abteilung 3 der XYZ AG." Ihre Kollegen werden das kaum lesen, jeder interessierte Außenseiter ist davon jedoch sicherlich begeistert, denn jetzt hat er ein interessantes Ziel! Also weg damit!

Nicht so bekannt ist, dass jeder Server, sei es nun Apache mit http und https, FTP und sogar telnet in den so genannten „Banner" für Hacker wertvolle Informationen absondert. Betriebssystem-Typ und Version, Serverversion usw. Alles Daten, die die Klassifikation und die Auswahl von passenden Exploits erleichtern. Legale Programme fangen damit gewöhnlich nichts an. Weg damit!

Einfach aber wirksam: programmieren Sie den Firewall wenn möglich so, dass er Verbindungsversuche auf ungeöffneten Ports nicht abweist sondern kommentarlos ignoriert. Dies zwingt dem Analyseprogramm des *Black Hat* Wartezeiten auf und verlangsamt und behindert die Klassifikation. Lassen Sie am Besten nicht einmal Pings in Richtung des Internet zu. Manches Hackerskript prüft per Ping die Anwesenheit eines Computers auf einer IP-Adresse. Doch was das Skript nicht weiß macht es nicht heiß!

Erschweren Sie den unautorisierten Zugangs von und zum WAN, d.h. aus Ihrem Netz nach Außen. Ein „personal firewall" ist noch immer eine gute Idee und sollte auf Ihrem Rechner nicht fehlen! Sie sollten weiterhin Ihren Computer nicht direkt mit dem DSL verbinden, obgleich das immer noch propagiert wird. Ein Router für unter 100 Euro wehrt bereits „out-of-the-box" eine Menge Probleme ab.

A propos WLAN: benutzen Sie mindestens WPA, wenn nicht WPA2 zur Verschlüsselung. Achten Sie weiterhin auf eine möglichst geringe Reichweite des Knotens! Wohin die Hochfrequenz nicht reicht, von dort kann auch kein Angriff erfolgen.

Zwar sind „war driver"[23], so nennt man die Leute die im Auto durch die Stadt fahren um nach offenen WLAN zu suchen manchmal mit Richtantennen ausgestattet und können über den Antennengewinn auch aus größerer Entfernung in Ihr Netz eindringen, doch immerhin: Auch diese Maßnahme hängt die Messlatte höher.

Für Server-Betreiber: Nutzen Sie möglichst verschlüsselte Dienste. Bieten Sie gegebenenfalls keine „offenen" Dienste mehr an.

Ohne weiteres kann man ftp durch sftp, tenet durch ssh und http durch https ersetzen.

Sie sollten zudem erwägen, keine anonymen Uploads zuzulassen. Sie wissen nie, welche Laus Ihnen jemand in den Pelz setzt. Wenn Ihre Server beschlagnahmt werden, da sich Pornographie oder „*warez*" darauf finden ist es meistens zu spät.

Fremde Software mit Misstrauen zu betrachten. „Don't accept software from strangers!" Dies beachtet heute vermutlich jeder.

So bleibt am Schluss noch, die Rechnerhardware unter Verschluss oder Aufsicht zu halten, dass Unbefugte den Computer nicht manipulieren können.

Zum Schluss: Gute und schlechte Betriebssysteme – Gibt es das?

In die Folklore der Computergemeinde gehört unweigerlich die Diskussion über das Für und Wider bestimmter Betriebssysteme. Wie der Autofahrer am Stammtisch mit glühenden Worten seine bevorzugte Marke verteidigt gibt es bei den Computernutzern genau so Adepten, welche mit religiösem Eifer das eine oder andere System verteidigen und nicht davor zurückschrecken, Abweichler wegen ihres Unglaubens auch einmal übel zu beschimpfen.

Wir haben an der Hochschule die Verteilung der Betriebssysteme, deren Einsatz und die verschiedenen Bedrohungen gegenübergestellt und dabei keine wirklich signifikanten Unterschiede gefunden. Für weit verbreitete Betriebssysteme gibt es eben mehr Schadsoftware – die Nachfrage regelt das Angebot – doch selbst für Exoten wie für Handy-Betriebssysteme sind bereits „exploits" bekannt geworden.

Wichtiger als der Typ des Computers und des Betriebssystems sind die richtige Anwendung von Schutzmaßnahmen sowie ein Quäntchen an gesundem Menschenverstand.

Abkürzungen und Begriffe

AJAX — Asynchronous Javascript and XML. Eine „Technologie" aus dem Bereich Webseiten-Programmierung die unter Anwendung dieser Sprachen Webseiten nur an den notwendigen Stellen „asynchron" aufdatiert.

---

[23] Grob übersetzt „Kriegs- oder Angriffs-Fahrer".

ASCII	American Standard Code for Intermation Interchange. Wohlbekannter 7-Bit-Code aus der Urzeit amerikanischen Fernschreibens. Nicht umzubringen!
C3I	Eigentlich C^3I: In zivilen Quellen: „Command, Control, Communication and Information“ oder im militärischen Umfeld „Command, Control, Communication and Intelligence“. (Systeme) zur Kombination von Kommandostrukturen, Kommunikation und Information- bzw. Aufklärungsinformation zur Verbesserung der Lagebeurteilung zur Erzieleung einer besseren „Situation Awareness“.
DNS	„Domain Name Service“; Internet-Dienst, der Domain-Namen in IP-Adressen umschlüsselt.
DoS	„Denial of Service“; (gezielte) Unterbrechung des Betriebs eines Systems, Sabotage.
EGNOS	European Ground Navigation Overlay System. Euriopäische Initiative zur Übertragung von GPS-Korrekturdaten über geostationäre Satelliten im Rundstrahldienst.
HTML	Hypertext Markup Language. Sprache zur Beschreibung von Inhalten im Internet.
HTTP	Hypertext Transfer Protocol. Protokoll oderhalb von TCP. Meist genutzt zur Übertragung von HTML-Inhalten.
IP	Internet Protocol. Unterstes Übertragungsprotokoll für Daten im Internet. Höhere Protokolle wie TCP und UDP bauen darauf auf..
LAMP	Linux, Apache, MySQL, PHP. Eine „Technologie“ aus der LINUX-Welt, die Web-Seiten unter Anwendung eben dieser Programmpakete dynamisch macht.
TCP	„Transmission Control Protocol“. Ist ein verbindungsorientiertes Protokoll des IP-Stacks. Kein Schutz gegen Datenverlust. Keine kryptologische Funktion. Großer Overhead..
UDP	„User Datagram Protocol“. Ist ein verbindungsloses Protokoll des IP-Stacks. Schutz gegen Datenverlust. Keine kryptologische Funktion. Geringer Overhead.
UTF-8	8-bit Unicode Transformation Format. Codierungsvorschrift für UNICODE-Zeichen, die neben den lateinischen auch kyrillische, hebräische, arabische, koreanische etc. Schriftzeichen enthält. UTF-8 codierte Zeichen können bis zu 4 Byte umfassen und können durch das trickreiche Codeschema bis zu 1.114.112 Zeichen codieren.
XML	Extensible Markup Language. HTML-ähnliche Codierung strukturierter Daten.

Quellen

[AKTA]	Jochen Helfrich, Thomas Bünz und Patrick Keil ; „Aktuelle Angriffsszenarien auf Rechnernetzwerke“, Vorlesung Sicherheitstechnik HS Darmstadt, 2004
[BSI]	Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de
[C3I]	Blair, Sir Ian; „Command, Control, Communication and Information“; www.met.police.uk/c3i/
[DOD_OR]	“Orange Book”, DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria", 1985
[EHF_90]	Franke, Erich H.; “Unheimliche Begegnungen der Elektronischen Art - Computerviren und was man dagegen tun kann“; Skriptum zum Vortrag am 17.9.90 auf der 35. UKW-Tagung in Weinheim.; http://www.afusoft.de/website/medien/hamradio/publications/UKW90.pdf
[GNUGPL]	GNU General Public License, Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301, USA
[KFILM]	Kinowelt Home Entertainment GmbH; “Mr. und Mrs. Smith”; ISBN 4-006680-034744; Der Film enthält ein durch ein Root-Kit geschütztes Kopierschutzverfahren, welches den Rechner langfristig behindert.
[MWORM]	„Der Morris-Wurm“; http://www.kossakowski.de/kap222.htm#FN3
[NETSKY]	Interview mit dem Autor von Netsky http://stern.de/computertechnik/computer/index.html?id=525454&nv=ct_cb&eid=501069
[PHIS]	Josiane Wouega, Florian Zimmermann, Nils Maier; „Password-Phishing“; Projektarbeit zur Vorlesung Sicherheitstechnik; HS Darmstadt, 2005
[SASS]	„Beschreibung : W32.Sasser.Worm“; http://www.bsi.de/av/vb/sasser.htm
[SASS1]	http://de.wikipedia.org/wiki/Sasser
[SYMAN]	http://www.symantec.com/index.jsp
[WARG]	„War Games“ R:John Badham, Spielfilm 113 min
[ZAL]	http://www.zonealarm.com/store/content/home.jsp