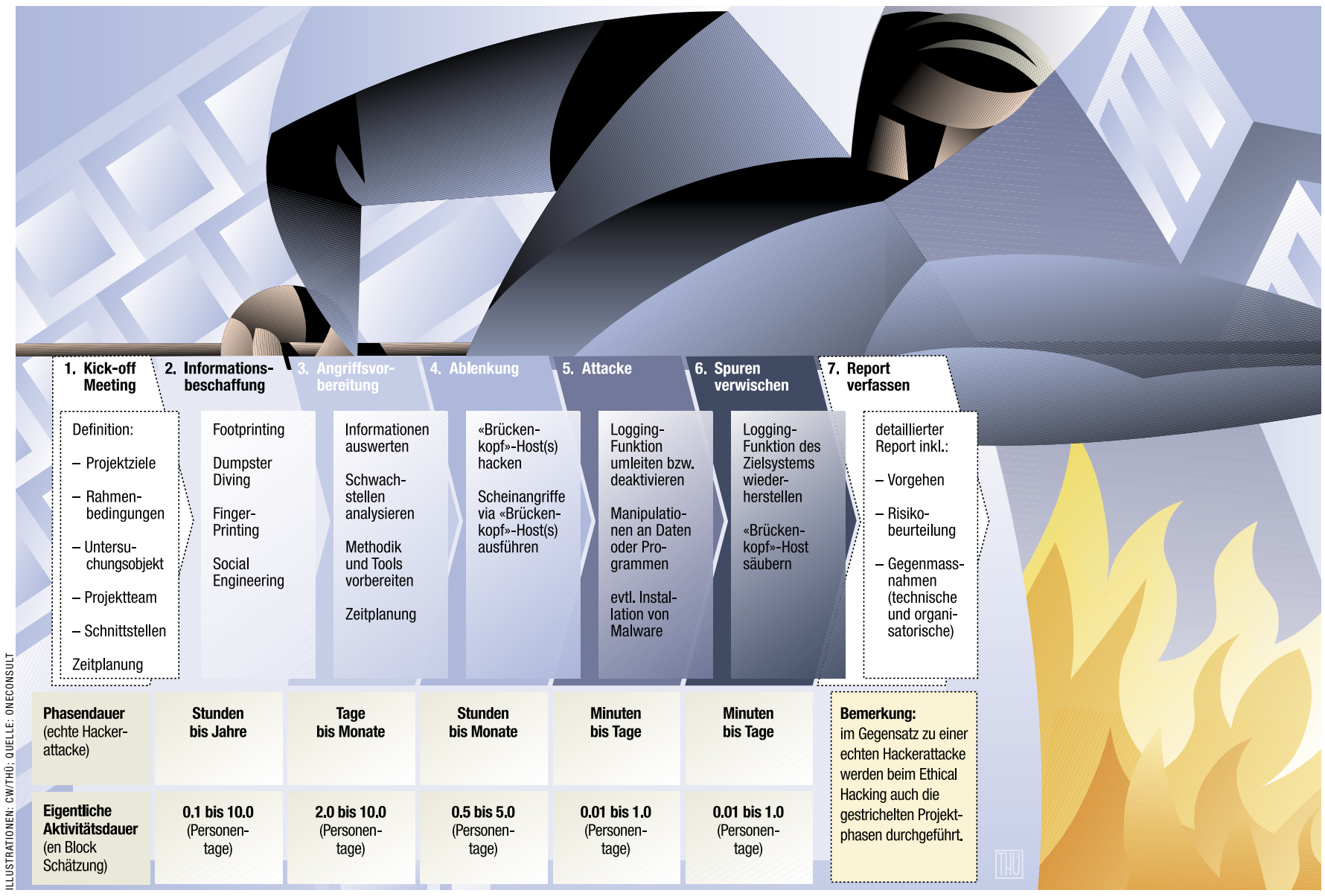
Computerworld Dossier IT-Security

Hacker im Visier: Aktion statt Resignation

Systemangriffe Vor Hackerattacken ist heutzutage kein Unternehmen mehr sicher. Internationale Studien haben gezeigt, dass selbst kleine und mittlere Unternehmen von Hackern systematisch ausspioniert oder sabotiert werden. Dieser Artikel zeigt Merkmale und Ablauf typischer Hackerattacken auf, mit dem Ziel, aus Sicht des Angegriffenen situationsgerecht agieren zu können.

Christoph Baumgartner*



Ein typischer Hackerangriff erstreckt sich über fünf Phasen. Beim Ethischen Hacking kommen zwei weitere Phasen hinzu: Das Kickoff-Meeting sowie das Abfassen eines Reports.

Leider werden dem Begriff «Hacker» unterschiedlichste Bedeutungen zugeordnet. In den siebziger Jahren bezeichneten sich sehr versierte Programmierer als Hacker, weil sie Problemstellungen «quick and dirty» in Form eines «Hacks» lösten. Ab 1990 bekam der Begriff Hacker eine neue Deutung. Journalisten bezeichneten damit Personen, die ohne Erlaubnis in Computernetzwerke eindrangen und die betroffenen Systeme aushorchten oder manipulierten. Um die Jahrtausendwende haben sich folgende Bezeichnungen etabliert: Als «Skript Kiddie» wird eine Person bezeichnet, die über relativ wenig Computer- und Netzwerkfachwissen verfügt, aber unbedarft automatisierte Hackertools einsetzt und damit teilweise massiven Schaden verursachen kann (etwa 90 Prozent der in den Logfiles der Computersysteme erfassten Hackerattacken werden von Skript Kiddies verursacht). Ein Hacker/Cracker, auch «Black Hat» genannt, bricht ohne Erlaubnis des Systemeigners meist via Computernetze in Computersysteme ein oder knackt das Lizenzsystem von Computerprogrammen. Dafür umgeht oder bricht er bewusst Sicherheitsmechanismen. Die Beweggründe sind Ehrgeiz, möglicher finanzieller Profit, Geltungssucht, Idealismus oder Zerstörungswille, wobei Idealismus die gefährlichste Triebfeder ist, da derartig motivierte Leute am meisten Engagement und Zeit einbringen.

Ein «Ethical Hacker», auch als «White Hat» oder Auftragshacker bezeichnet, ist ein Computer- und Netzwerkspezialist, der im Auftrag des Systemeigners nach Systemverwundbarkeiten sucht, die ein Hacker/Cracker ausnutzen könnte. Im weiteren Verlauf dieses Artikels ist mit dem Begriff Hacker immer eine Person mit unlauteren Absichten gemeint. Aus Gründen der Vereinfachung wird jeweils nur die männliche Form gewählt.

Informationsbeschaffung

In dieser Phase möchte sich der Hacker möglichst umfassende Informationen über das Opfer und dessen Infrastruktur beschaffen. Dazu werden verschiedene Methoden angewandt, welche sich bezüglich der zu erhaltenden Informationen und des Entdeckungsrisikos, in das sich der Hacker begibt, unterscheiden. Beim Footprinting wird im Internet nach Informationen über das Zielobjekt und dessen technische Beschaffenheit gesucht. Dabei werden hauptsächlich Websites und Newsgroups mittels Tools durchforstet. Das Opfer kann derartige Aktivitäten nicht erkennen. Beim Dumpster Diving wird der Abfall des Opfers systematisch nach relevanten Informationen wie User-ID, Passwortlisten oder internen Projektpapieren durchsucht. Diese Aktivität kann mit etwas Glück vom Opfer erkannt werden. Beim Fingerprinting werden die vom Internet her erreichbaren Systeme mittels Tools wie Port- oder Securityscannern untersucht. Hacker erhalten dabei Informationen über erreichbare Systeme, offene Ports, angebotene Dienste, Betriebssystem- und Applikationsversionen oder das Verhalten der Firewall. Dieses Fingerprinting kann an Hand der Einträge in Logfiles auf der Firewall vom Opfer erkannt werden.

Als Social Engineering werden sämtliche Informationsbeschaffungsmethoden bezeichnet, bei denen Menschen im Spiel sind und deren Schwächen systematisch ausgenutzt werden. Beispielsweise kann sich ein Hacker am Telefon oder vor Ort als vermeintlicher Systemtechniker des Opfers ausgeben und so an gewünschte Passwortinformationen gelangen. Oftmals funktioniert diese Technik nach dem Puzzle-Prinzip. Der Hacker bekommt bei jedem Kontakt mit einem Angestellten des Opfers eine Information, welche er dann bei einer anderen Stelle quasi als Echtheitsbeweis weiter verwenden kann, um seinem Ziel etwas näher zu kommen. Beim Social Engineering ist die Entdeckungsgefahr für den Hacker gross, denn nicht immer lassen sich die Mitarbeiter durch vorgetäuschte Hilflosigkeit, Komplimente oder Einschüchterung zur Preisgabe vertraulicher Informationen bewegen. Aus diesem Grund werden die Methoden des Social Engineerings nur dann eingesetzt, wenn der Hacker nicht mit anderen, für ihn weniger gefährlichen Möglichkeiten an die benötigten Informationen gelangt.

Angriffsvorbereitung

In der Angriffsvorbereitungsphase werden die in der vorherigen Phase erlangten Informationen ausgewertet. Auch Hacker möchten sich die Arbeit nicht schwieriger als nötig gestalten. Deshalb suchen sie nach Schwachstellen, die sie zur Zielerreichung ausnutzen können. Wenn Wirtschaftsspionage das Ziel ist, kann der Hacker beispielsweise zum Schluss kommen, lieber einen geeigneten Mitarbeiter des Opfers zu erpressen oder zu bestechen, als sich die Mühe zu machen, die technischen Sicherheitsmechanismen in einem langwierigen Prozess zu umgehen oder zu durchbrechen. Falls sich der Hacker für die Computernetzwerk-basierte Methode entschlossen hat, legt er sich die dafür benötigten Tools oder technisches Equipment zurecht und programmiert speziell auf diesen Angriff abgestimmte Hilfsmittel wie Exploits, die in der Informationsphase erkannte Schwachstellen auf dem Zielsystem ausnutzen, um damit beispielsweise Administrationsrechte auf den Zielsystemen zu erlangen. Zum Abschluss dieser Phase erfolgt die Zeitplanung. Das Opfer hat in dieser Phase keinerlei Chance, die drohende Hackerattacke zu erkennen.

Es ist übrigens kein Zufall, dass Hackerattacken oft in den frühen Morgenstunden, an Wochenenden und Feiertagen stattfinden. Zu diesem Zeitpunkt werden die Systeme des Opfers meistens von einer personell stark reduzierten Rumpfmannschaft betreut, was die Gefahr der frühzeitigen Entdeckung der Hackerattacke und die Einleitung geeigneter Gegenmassnahmen stark einschränkt.

In diesem Beitrag

- Wie Hacker an umfassende Informationen über ihre Opfer kommen und auf welche Weise sie sich auf ihre Attacken vorbereiten
- Mit welchen Ablenkungsmanövern Angreifer Security-Chefs auf die falsche Fährte locken
- Welche präventiven Massnahmen Angriffe auf das System verhindern oder zumindest vereiteln können

Ablenkung

Die Ablenkungsphase ist optional, wird aber oftmals von Hackern durchgeführt, die es auf gut gesicherte Umgebungen wie beispielsweise Banken oder militärische Einrichtungen abgesehen haben. Um das Interesse der Sicherheitsverantwortlichen des Opfers auf eine falsche Fährte zu locken, werden vom Hacker so genannte «Brückenkopf»-Hosts unter Kontrolle gebracht. Potenzielle Kandidaten dafür sind Systeme aus dem universitären Umfeld, welche einerseits tendenziell schlechter geschützt werden als Systeme von mittleren und grossen privatwirtschaftlichen Unternehmen und andererseits mittels beeindruckenden Bandbreiten (welche für bestimmte Denial-of-Service (DoS)-Attacken benötigt werden) ans Internet angeschlossen sind. Der Hacker gelangt mit-

Fortsetzung auf Seite 14

*Christoph Baumgartner ist Geschäftsführer und Senior Consultant bei der auf Informationssicherheit (IT Security) und strategische Beratung spezialisierten OneConsult GmbH.

Dossier: IT-Security

Es mangelt am Bewusstsein

Claudia Bardola

Die Security-Spezialisten hatten im letzten Jahr alle Hände voll zu tun: 2004 wurden über 10 000 neue Viren, Würmer und Trojaner aufgespürt und die Anzahl der Phishing- und Hackattacken ist massiv angestiegen. In einer Studie der Marktbeobachterin Mummert geben denn auch zwei Drittel der Schweizer und der deutschen Unternehmen an, wesentlich mehr Angriffe auf ihre IT-Infrastruktur ausgemacht zu haben als im Jahr zuvor.

Trotzdem will bei den befragten IT-Chefs der Groschen offenbar nicht so recht fallen: Die Hälfte von ihnen stuft das Sicherheitsrisiko in ihrem Unternehmen als gering ein. Angesichts dieses fehlenden Security-Bewusstseins erstaunt es wenig, dass lediglich magere 13 Prozent der interviewten Firmen ihre Sicherheitsmassnahmen und -ziele in einer Policy festgehalten haben. Bei 27 Prozent der Betriebe gibt es bloss informelle Richtlinien, jedes fünfte Unternehmen hat gemäss der Studie überhaupt keinen Plan.

Eine schlampige Sicherheitspolitik kann aber teuer zu stehen kommen: Experten schätzen, dass beispielsweise ein durch Viren lahm gelegter Rechner durchschnittlich Kosten in der Höhe von 7500 Franken verursacht. Zwingen Hacker ein komplettes System in die Knie, so kann der Schaden, nicht zuletzt infolge des Produktionsausfalls, schnell in die Hunderttausende gehen.

Fortsetzung von Seite 13

tels eines Passwortcrackers oder durch Abhören des Netzwerkverkehrs (Sniffing) an das Passwort eines gültigen Accounts und kann sich auf dem entsprechenden System einloggen.

In der Folge kann er mittels der kopierten digitalen Identität des rechtmässigen und ahnungslosen Benutzeraccount-Besitzers quasi in dessen Namen agieren um beispielsweise via diverse Brückenköpfe Scheinangriffe auszuführen. In der Praxis werden oft ganze Ketten von Brückenköpfen quer über alle möglichen Länder und Kontinente eingesetzt, damit das so genannte Tracing des echten Ursprungs der Hackerattacke erschwert wird und der Hacker besser getarnt ist. Scheinangriffe sind vom Opfer von echten Angriffen nicht zu unterscheiden.

Spuren verwischen

Nachdem alle benötigten Vorarbeiten vom Hacker erledigt wurden, kann die eigentliche Attacke beginnen. Als erstes wird versucht, das Anfallen und die Aufzeichnung jeglicher echter Spuren zu verhindern. Dies geschieht einerseits mittels des Einsatzes von Brückenköpfen und andererseits durch systematisches Umleiten oder Deaktivieren der Logging-Funktion der Zielsysteme. Anschliessend kann der Hacker seinen eigentlichen Auftrag erledigen und beispielsweise Daten und Programme manipulieren. Nach getaner Arbeit installieren Hacker oft noch Hintertürchen wie beispielsweise Trojaner (siehe auch nachfolgende Artikel) auf den kompromittierten Systemen, die es dem Hacker in Zukunft vereinfachen, erneut Zugriff auf das System zu bekommen. Sollte es dem Hacker nicht gelingen, die Kontrolle über das Zielsystem zu erlangen, führt er oftmals als Frustreaktion eine Denial-of-Service-Attacke aus, welche bei Erfolg die Verfügbarkeit des angegriffenen Systems negativ beeinträchtigt. Nachdem der Angriff abgeschlossen ist, werden möglichst alle Spuren verwischt und die Logging-Funktion des Zielsystems wieder hergestellt. Allfällig eingesetzte Brückenköpfe werden ebenfalls von Spuren gesäubert.

Gegenmassnahmen

Obwohl während einer relativ langen Zeitspanne Informationen über das Zielobjekt gesammelt werden, findet der eigentliche Angriff innerhalb eines eng bemessenen Zeitfensters statt (siehe Grafik). Es ist also von entscheidender Bedeutung, einen geplanten Hackerangriff möglichst früh zu erkennen und abzuwehren. Die wohl wirkungsvollste Massnahme ist die Steigerung der Security Awareness der Mitarbeiter. Denn wer sich bewusst ist, dass sämtliche Informationen einen Wert haben, welche im Web, im Gespräch oder auf dem Schreibtisch liegend aktiv oder passiv an andere weitergegeben werden, der überlegt sich, ob, wem und vor allem was er an andere kommuniziert. Dieses gesteigerte Sicherheitsbewusstsein der Mitarbeiter erschwert Unberechtigten die Informationsgewinnung massgeblich und vereitelt manche geplante Hackerattacke bereits in einer frühen Phase.

Weitere präventive Massnahmen sind regelmässige Sicherheitsüberprüfungen und Vulnerability Management-Systeme. Falls der Hackerangriff dennoch in die heisse Phase der laufenden Attacke geht, so soll die Attacke raschestmöglich erkannt und der Hacker in die Irre geleitet werden, um wertvolle Zeit für Gegenmassnahmen zu gewinnen. Um Attacken zu erkennen, haben sich in der Praxis Intrusion-Detection und Prevention-Systeme bewährt, welche Alarm schlagen und allenfalls selbständig Gegenmassnahmen wie das Kappen einer bestimmten Verbindung einleiten können.

Sogenannte Honeypots sind echt aussehende, aber mit falschen Daten gefütterte Systeme, welche dem Hacker ein interessantes System vortäuschen, in dem er sich dann bewegt und damit schliesslich Zeit vergeudet. Es gibt also durchaus Mittel, Hackerangriffe mittels Prävention zu verhindern oder zumindest deren Erfolg zu vereiteln. Dank richtigen Aktionen des vermeintlichen Opfers resigniert am Schluss nur einer – der Hacker. ■

Workshop – Hack yourself

Ethical Hacking Gewiefte Hacker platzieren Trojaner, um Computersysteme über das Internet fernzusteuern. Diese Systeme dienen meist als so genannter «Brückenkopf» für weitere Angriffe. Lesen Sie, wie Hacker dabei vorgehen und testen Sie mit einem Trojaner, ob Ihr Netzwerk vor derartigen Angriffen gefeit ist.

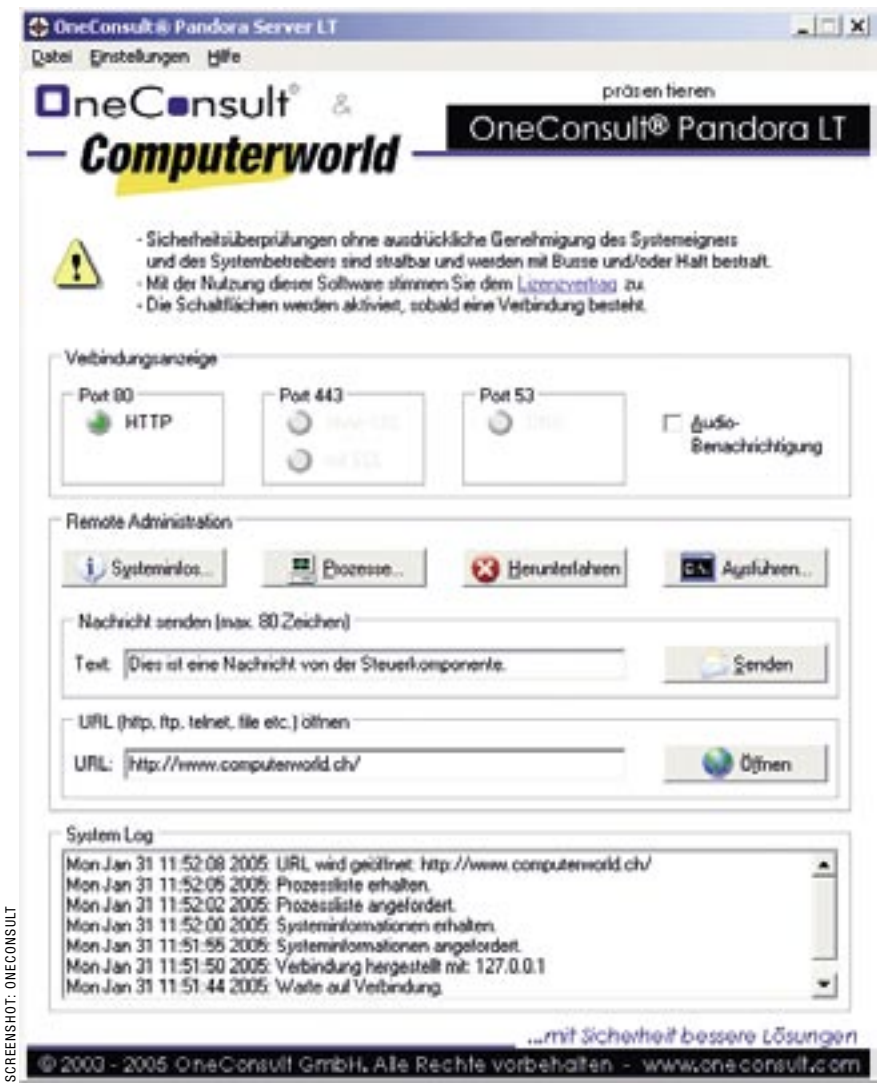
Simon Wepfer*

Sicherheitskonzepte, die sich auf eine harte Schale verlassen, dabei allerdings die Sicherheit der inneren Systeme vernachlässigen, werden im Fachjargon mit dem Begriff «Candy-Sicherheit» umschrieben. Mit den Süssigkeiten sind konkret die M&M's Bonbons gemeint, deren weicher Kern sich dann offenbart, sobald die Glasur mit einem kräftigen Biss oder geduldigem Lutschen durchdrungen ist. Tatsächlich ist einem Hacker die Firewall an sich egal. Verschiedene Dienste wie Mail-, DNS- oder Webserver müssen vom Internet her erreichbar sein. Ein Hacker wird denn auch versuchen, den Hebel eher dort anzusetzen, als sich an einer Firewall die Finger zu verbrennen.

Die zur Verfügung stehenden Dienste nutzen auch Trojaner aus: Die Programme verbinden sich durch die Firewall hindurch mit einer Steuerkomponente oder loggen sich auf einem IRC-Kanal (Internet Relay Chat) ein, um von dort Steuerbefehle zu erhalten. Auf diese Weise lässt sich ein Rechner in einem geschützten Netzwerk fernsteuern – trotz Firewall. Der Datentransfer sieht dann etwa wie eine herkömmliche Verb indung mit einem Webserver aus, doch statt Webseiten werden Steuerbefehle, Finanzdaten oder Passwörter übertragen.

Ein Rootkit ist eine Weiterentwicklung der Trojaner: Es versteckt sich und seine Aktivitäten durch Modifikationen am Betriebssystem. Besonders perfid gehen dabei die so genannten «Kernel Rootkits» vor. Sie werden beispielsweise in Form eines Gerätetreibers geladen und nisten sich tief im Betriebssystem ein. Das Kernel Rootkit setzt Filterfunktionen (Dateien/Verzeichnisse, Prozessl iste, Netzwerkverbindungen) direkt bei den entsprechenden Systemfunktionen ein, um sich zu verbergen. So kann auch eine Desktop-Firewall nicht erkennen, dass soeben eine vom Anwender unerwünschte Netzwerkverbindung hergestellt worden ist.

*Simon Wepfer ist Consultant bei der auf Informationssicherheit (IT Security) und strategische Beratung spezialisierten OneConsult GmbH.



SCREENSHOT: ONECONSULT

Mit der von Oneconsult entwickelten Client-/Server-Anwendung Pandora LT lässt sich überprüfen, ob das eigene Netzwerk anfällig auf Hackerattacken ist. .

Hack yourself

Wir möchten Sie einladen, Ihre eigene Netzwerkinfrastruktur mittels indirektem Ansatz zu überprüfen. Es handelt sich hierbei um einen von vielen Sicherheitstests, die bei einer technischen Sicherheitsüberprüfung vorgenommen werden: Es wird versucht, einen PC im LAN (Local Area Network) durch die Firewall hindurch remote zu administrieren. Hierfür stellen wir unter http://www.oneconsult.com/downloads/downloads.html die Software «OneConsult Pandora LT» zur Verfügung. Pandora ist eine Client-/Server-Anwendung und besteht aus dem Trojaner (Clientkomponente) und der Steuerkomponente.

Falls keine entsprechenden Schutzmechanismen installiert wurden, sollte es möglich sein, das mit der Clientkomponente «infizierte» System über die Serverkomponente remote zu steuern. Dies funktioniert oft auch durch eine Hardware-Firewall hindurch. Das Tunneling findet bei Pandora LT über das http-Protokoll statt. Schlägt eine direkte Verbindung fehl, versucht der Trojaner diese über einen Proxy Server aufzubauen.

Pandora wird voraussichtlich von Ihrem Anti-Virenprogramm nicht erkannt. Dies bedeutet aber nicht, dass Ihr Anti-Virenprogramm versagt hat. Anti-Virenprogramme erkennen bekannte Viren an Hand von Signaturen (Bit-Mustern). Da es sich bei Pandora LT nicht um ein schon länger im Umlauf befindliches, potenziell gefährliches Tool handelt, wird dessen Bit-Muster (noch) nicht erkannt.

1. Notieren Sie sich die Firewall-Konfiguration auf den Systemen, auf welchen Sie OneConsult® Pandora LT verwenden möchten.
2. Stellen Sie sicher, dass die auf dem zu steuernden System installierte Software-Firewall ausgehende Verbindungen auf TCP Port 80 (http) zulässt.
3. Stellen Sie sicher, dass auf dem System, auf dem die Steuerkomponente gestartet werden soll, eingehende und ausgehende Verbindungen auf TCP Port 80 (http) erlaubt sind.
4. Starten Sie das Programm OneConsult-Pandora-Server.exe. Die Steuerkomponente ist nun bereit und wartet auf eine Verbindung.
5. Starten Sie auf dem zu steuernden System das Programm OneConsult-Pandora-Client.exe: Es öffnet sich ein DOS-Fenster, in welchem Sie den Systemnamen oder die IP-Adresse der Steuerkomponente eingeben müssen.
6. Sobald die Verbindung mit der Steuerkomponente aufgebaut wurde, können Sie auf der Steuerkomponente die vom Frontend unterstützten Befehle ausführen.
7. Sie können die Programme der Client- und Serverkomponente jederzeit durch das Schliessen der zugehörigen Fenster beenden.

Eine ausführlichere Bedienungsanleitung wird mit der Software mitgeliefert. Falls die Desktop-Firewall auf dem zu steuernden Rechner den Verbindungsaufbau nicht gestattet, ist der Rechner vor herkömmlichen Trojanern (ohne Rootkit-Funktionalitäten) ge-schützt. In diesem Fall sollten Sie den Zugriff trotzdem gewähren, um zu testen, ob weitere Komponenten im Netzwerk die Verbindung verhindern können.

Fazit

Sicherheitsrichtlinien und Mitarbeiter mit gesteigerter Security-Awareness in Kombination mit einem mehrschichtigen, technischen Schutzkonzept (Zwiebelschalen-Modell) bieten einen guten Schutz vor derartigen Angriffen. So wird aus einem knackigen M&M eine harte Zwiebel, wo keiner zweimal hineinbeissen möchte. ■

Info/http://www.oneconsult.com

Praxisbericht: Ethical Hacking

Hacking Der direkte Ansatz im Ethical Hacking verfolgt das Ziel, ein System ohne aktive Mithilfe des Besitzers zu manipulieren. Im Gegensatz zum indirekten Ansatz ist der Aufwand schwerer abzuschätzen. Dieser Bericht zeigt aus der Angreifer-Perspe k-tive den praktischen Ablauf eines ethischen Hackings.

Simon Wepfer

Ich schreibe meinem Freund J. eine E-Mail und frage ihn, ob er sich für einen Hackversuch an seinem Heimnetz begeistern könne. Eine halbe Stunde später trifft seine Erlaubnis ein. Genau genommen hat der Angriff bereits mit meiner Anfrage begonnen: Ich schaue mir die Header-Informationen der E-Mail an und erfahre so die IP-Adresse des Zielsystems.

Um warm zu werden beginne ich mit einem Traceroute und einigen DNS- und Whois-Abfragen. Dann starte ich einen Portscan auf die TCP Ports 1-80. Hierfür verwende ich das Open-Source-Tool nmap. Der Syn-Scan (-sS) sendet Kommunikationsanfragen an Zielports, ohne eine Protokoll-konforme Verbindung herzustellen:

- nmap -sS -O -T Polite -P0 -vvv -p 1-80 ziel-ip

Die Option -O versucht das Betriebssystem am Verhalten zu erkennen (OS Fingerprinting). Der Scan selbst benötigt einige Minuten. An Hand des Outputs ist erkennbar, dass es sich vermutlich um ein Zyxel Produkt handelt und der FTP- und Telnet-Dienst aktiv sind. Nebenbei betrachte ich natürlich ständig den Netzwerkverkehr mit ethereal oder tcpdump.

Standard-Passworte

Ich versuche zunächst mit dem Standard-Passwort der Zyxel-Produkte die Herrschaft über den Router zu erlangen. Ich rufe eine Telnet-Session auf und gebe das Passwort «1234» ein. Leider schlägt der Versuch fehl. Ich versuche das Passwort noch mit einigen Schüssen ins Blaue zu erraten – ohne Erfolg. Scheint doch nicht ganz so einfach zu sein.

Verwundbarkeiten

Nachdem die aktiven Dienste bekannt sind, starte ich den Security-Scanner «Nessus», um das Zielsystem nach Sicherheitslücken zu untersuchen.

- nessus-update-plugins
- nessusd -D
- nessus

Zuerst aktualisiere ich die Test-Plugins. Anschliessend starte ich den Nessus Daemon. Dabei handelt es sich um den Dienst, welcher die Tests ausführt. Mit dem dritten Befehl starte ich schliesslich das GUI. Ich wähle sämtliche passenden Plugins aus (ausser den DoS-Tests) und definiere die bekannten Zielports sowie die Ziel-Adresse. Nur wenige Minuten später ist der Test bereits beendet, der Report zeigt jedoch leider keine ausnutzbaren Verwundbarkeiten.

Dictionary Attacke

Ich entscheide mich, eine so genannte Dictionary Attacke auf den FTP-Dienst zu starten. FTP eignet sich für solche Fälle besonders gut. Hat das Opfer ein simples Passwort gewählt, verspricht dieser Angriffstyp nämlich hohe Erfolgschancen. Hierfür wird ein Tool benötigt, das selbständig Benutzernamen- und Passwort-Kombinationen ausprobieren kann. Gängige Tools sind beispielsweise Hydra, TeeNet oder Brutus.

Die zahlreichen Passwortlisten sind im Internet schnell gefunden. Nach lediglich 330 Versuchen ist das Passwort geknackt: homer. Darauf hätte ich

Weitere Links:

Nmap Portscanner: **http://www.insecure.org/**
Nessus Vulnerabiliy Scanner: **http://www.nessus.org/**
OneConsult Pandora LT: **http://www.oneconsult.com/downloads/downloads.html**