Dies ist eine erweiterte Version des Beitrages,
der im iX-Sonderheft Security, 2010, erschienen ist.

Onlinedurchsuchung gegen Virenscanner und Persönliche Firewall

Leicht umgangen

Ulrich Greveler, Christian Puls

Seit Anfang 2009 ist die heftig umstrittene Online-Durchsuchung gesetzlich verankert. Unter sehr engen Voraussetzungen ist es den BKA-Beamten nach §20k des BKA-Gesetzes rechtlich möglich, die Computer von Verdächtigen zu durchsuchen. Ob die Durchsuchung in der Praxis auch technisch gelingt, ist bisher nicht bekannt: Die neue Ermittlungsmethode kam bis jetzt nicht zur Anwendung.

Nach Auskunft des Bundesinnenministeriums wurden in den 18 Monaten nach Inkrafttreten des Gesetzes zwar bereits über 680.000 Euro für technische Mittel und Personalkosten aufgewandt, einen Einsatz der zeitweise als „Bundestrojaner“ verspotteten forensischen Software hat es aber bisher nicht gegeben. Die Zurückhaltung der Ermittler ist jedoch nicht der weiten Verbreitung von Virenscannern und *Persönlichen Firewalls* geschuldet. Diese lassen sich tatsächlich leicht umgehen, wie wir im Folgenden zeigen werden.

Verdeckter Eingriff

Die Online-Durchsuchung, die als *verdeckter Eingriff in informationstechnische Systeme* Eingang in die Gesetzgebung gefunden hat, stellt eine legale Kompromittierung eines Systems dar. Der Ermittler wird dazu die Installation einer *Backdoor* bzw. einer *Remote Forensic Software*, RFS, vornehmen, die umfangreiche Möglichkeiten bietet, Daten zu lesen, zu übertragen und auszuwerten. Hilfsweise könnte er sich dazu einer frei erhältlichen Software zur Fernadministration bedienen, die unbeschränkte Zugriffsmöglichkeiten bietet, aber in ihren technischen Möglichkeiten über die juristisch gesetzten Grenzen hinausgeht. Eine Software für den Fernzugriff bietet zumeist Funktionen, um einen Rechner, welcher in diesem Fall als Server fungiert, fernzusteuern oder zu überwachen. Hierzu können Maus- und Tastatureingaben aus der Ferne übernommen werden und der Bildschirm des Servers auf dem entfernten Client angezeigt werden Bekannte Tools, die zur Wartung eines Systems aus der Ferne genutzt werden, sind z. B. *Back Orifice*, *Nuclear RAT*, *SubSeven*, *Bitfrost* oder *NetBus*.

Die potentielle Fähigkeit einer Software, Daten zu verändern, könnte jedoch bei einer Würdigung gewonnener Beweise vor Gericht, kritisiert werden, weswegen einer auch unter juristischen Gesichtspunkten entwickelten RFS der Vorzug gegeben werden sollte. Die Funktionalität der vom BKA entwickelten RFS ist bisher nicht öffentlich bekannt.

Aus Sicht eines Systemanwenders stellt jede Hintertür, die er nicht selbst geöffnet bzw. zugelassen hat, eine Trojanisierung seines Systems dar. In technischer Hinsicht ist es dabei uner-

heblich, ob die Hintertür als „unerwünschte“ Fernadministration, als RFS oder als sonstige Malware gekennzeichnet ist. Der Anwender möchte sein System frei von Malware halten und bedient sich dazu in der Regel technischer Möglichkeiten.

Die im Rahmen einer Abschlussarbeit ermittelten empirischen Ergebnisse über den „Normalfall“ eines privat genutzten Systems bestätigen allgemeine Erwartungen über eine typische Konfiguration und installierte Sicherheitstools [Puls08]. Der PC ist i. a. nicht völlig ungeschützt und wir können von der Verwendung eines Virenscanners und einer *Personal Firewalls* (inkl. so genannten Malware-Detektoren) beim Privatanwender ausgehen. Es ergibt sich ein Referenzmodell eines privaten PCs: Eine Windows-basierte Installation (XP, Vista oder Windows 7), Virenscanner (*Avira, Kaspersky, Norton* sind häufigste Nennungen) und eine *Personal Firewall* (z. B. *Zone Alarm, Sygate*). Dieses Ergebnis deckt sich mit Untersuchungen zu Marktanteilen [Schü08].

Malware und Trojaner

Malware ist ein Oberbegriff für bösartige Software, sowohl selbstreplizierende (Viren) oder nicht selbstreplizierende (z. B. Trojaner, Rootkits). Das Wort Malware setzt sich aus den Wörter **mal**icious (engl. für bösartig) und Soft**ware** zusammen. Selbst wenn die Malware keine beabsichtigten Schadfunktionen bereitstellt, kann schon von einer Beeinträchtigung gesprochen werden, wenn Systemressourcen verbraucht werden, ohne einen vom Nutzer gewünschten bzw. spezifizierten Zweck zu erfüllen.

Unterarten der Malware stellen nicht nur Viren oder Trojaner, sondern auch *Backdoors* und *Rootkits* dar. Eine Backdoor erlaubt es, vorgesehene Authentifizierungsmechanismen und Sicherheitsrichtlinien zu umgehen, um Zugriff auf den Rechner zu erhalten. Backdoors können als eigenständige Programme (wie z. B. *Back Orifice*), Modifikation von bestehenden Programmen oder der Hardware oder durch nur dem Ersteller des Systems bekannte Passwörter bzw. undokumentierte Login-Funktionen auf ein System gelangen. Häufig gelangen Hintertüren als Payload von Viren, Würmern oder Trojanern in ein System.

Das „Einsatzgebiet“ für ein Rootkit ist das Verstecken von Prozessen und Dateien, um Beispielsweise eine Backdoor zu verschleiern oder einen Keylogger zu tarnen. Auch das Überlagern von Systemfunktionen ist möglich, um so beispielsweise den Taskmanager zu deaktiveren oder Tastatur- und Mauseingaben abzufangen. Rootkits bieten gewöhnlich zwei Hauptfunktionen: die Fernsteuerung des Systems und das Ablauschen von Daten. Unter Fernsteuerung versteht man die Kontrolle über Eingabe, Dateien und Prozesse, das Auslösen von Neustarts oder vorsätzliche Systemabstürze.

Digitale Forensik

Eine junge Teildisziplin der Forensik ist die *Digitale Forensik* (auch: *IT-Forensik*). Sie behandelt die Untersuchung verdächtiger Vorfälle im Zusammenhang mit IT-Systemen durch Erfassung und Analyse digitaler Spuren. Erst seit Mitte der neunziger Jahre werden durch *Interpol* Weiterbildungen für polizeiliche Ermittler in Bezug auf die Beweissicherung bei Computerstraftaten angeboten; zu dieser Zeit kam es bei Ermittlungen noch zu schwerwiegenden Ermittlungspannen, weil beispielsweise sichergestellte Disketten zu den Akten geheftet und damit unbrauchbar gemacht wurden [Con97].

Eine Online-Durchsuchung ist als IT-forensische Maßnahme zu betrachten, sofern die verwendete Methode etablierten wissenschaftlichen Ansprüchen genügt. Dabei ist es technisch unerheblich, ob sich die Ermittlungen auf die Aufklärung von Computer-Straftaten (wie Computerbetrug) oder um die Abwehr von Terrorismus-Gefahren (wie es das BKA-Gesetz benennt) beziehen.

„Bundestrojaner“ eine Malware?

Die Hersteller von Anti-Viren-Software gehen davon aus, dass eine Software zur Onlinedurchsuchung von ihren Anti-Viren-Systemen als potenziell gefährlich gemeldet würde. Virenscanner sind insbesondere auch Malwarescanner, und da eine RFS mit den gleichen technischen Mechanismen wie eine Malware arbeitet, soll der Virenscanner diese aufspüren.

Ein Industrievertreter wird während der öffentlichen Debatte zur Online-Durchsuchung mit der Aussage zitiert, dass „*ein Trojaner eine Spionage-Software [ist und bleibt]. Sobald seine Struktur den Software-Herstellern bekannt wird, wird er in das Verzeichnis bekannter Viren aufgenommen und von den Programmen blockiert.*“ Eine Zusammenarbeit mit staatlichen Behörden bei den Online-Durchsuchungen lehnten die Software-Hersteller ab [Gra07].

Die Hersteller-Aussagen könnten zur Annahme Anlass geben, dass der Schutz, der mit Anti-Virus-Produkten erreicht wird, eine Online-Durchsuchung erheblich erschwert bzw. dass die Aufwände, die zur Umgehung des Schutzes notwendig sind, nur mit bedeutenden personellen Ressourcen geleistet werden können. Untersuchungen und praktische Experimente zeigen jedoch, dass diese Annahme unbegründet ist.

Umgehen des Virenscanners

Virenscanner suchen nach allgemeinen Merkmalen, die auf die Gefährlichkeit einer Software hinweisen (heuristische Vorgehensweise), oder nach charakteristischen Codefragmenten (Signatur) bereits bekannter Malware, um diese als Schädling zu identifizieren.

Eine Umgehung des Virenscanners muss daher mindestens diese beiden Erkennungsmethoden berücksichtigen. Dies erweist sich jedoch als mit einfachen technischen Mitteln möglich [GrePu09]. Die Untersuchung, die zu diesem Ergebnis führte, wurde für 36 verschiedene Scanner vorgenommen, die zum Teil nach Herstellerangaben auch eine *Anti-Spyware*-Funktionalität aufwiesen. Die Vorgehensweise wird im Folgenden beschrieben.

Eine Erkennung der Malware mit heuristischen Verfahren basiert zumeist auf der Analyse bestimmter genutzter Funktionen einer Software, welche auf eine schadhafte oder tarnende Funktionsweise hinweisen. Hierzu könnten in verschiedenen Kombinationen der Aufbau von Kommunikationskanälen oder der Zugriff auf Geräte zählen.

Um sowohl die Virensignaturerkennung als auch die heuristische Erkennung zu vermeiden, kann ein einfaches Hex-Editor-Verfahren angewandt werden. Zur Planung einer Intervallschachtelung wird zunächst die erste, dann die zweite Hälfte des Binärcodes byteweise ausgenullt, um eine relevante Offset-Position in der Datei zu ermitteln; dieser Vorgang wird für die Hälften sukzessive wiederholt bis kurze Fragmente (wenige oder einzelne Bytes) ermittelt wurden, die zur Erkennung durch den Scanner relevant sind (siehe Abb. 1).

Nachdem die Fragmente identifiziert wurden, die den Trojaneralarm auslösenden, kann durch Modifikation des Binärcodes eine Erkennung durch den Virenscanner unterbunden werden. Da diese Vorgehensweise direkt den Binärcode verwendet, muss der Ermittler nicht zwingend im Besitz des Quellcodes sein. Jedoch lässt sich so keine genaue Vorhersage treffen, welche Auswirkungen die Veränderung haben wird. Erweiterte man die Intervallschachtelung jedoch um Modifikationen im frei verfügbaren Quellcode einer Fernadministrationssoftware und lokalisierte die „Problemstelle“ dort als Programmzeile (meist handelte es sich beim identifizierten Binärcodefragment um einen Funktionsbezeichner einer DLL-Funktion) kann durch Verwendung eines *Alias*-Bezeichners die Erkennungsproblematik ohne funktionelle Einbußen gelöst werden.

Dazu sind einfache Programmierkenntnisse auf Seiten des Ermittlers erforderlich. Im von den Autoren untersuchten Fall konnte mit Hilfe eines frei verfügbaren PE-Betrachters[1] der gefundenen Offset-Position ein Eintrag in der *Import Name Table (INT)*[2] zugeordnet werden, welcher durch Verwendung eines schon zuvor genannten Alias-Bezeichners umgangen werden konnte. Möchte oder muss man die Funktion trotzdem nutzen, so bietet die Windows-API die Möglichkeit, Funktionen aus DLLs dynamisch zu importieren. Wird die Funktion dynamisch geladen, so kann sie weiterhin genauso verwendet werden wie die direkt aufgerufene Funktion. Nun wird die Funktion jedoch nicht mehr in der *Import Adress Table (IAT)* oder der *Import Name Table (INT)* geführt, was eine Erkennung anhand verräterischer Funktionsaufrufe durch die Heuristik verhindert.

Umgehen der Personal Firewall

Die zweite Hürde, die der Ermittler überwinden muss, wenn er nicht vom Verdächtigen entdeckt werden möchte, ist die *Personal Firewall* (PFW). PFWs sollen i. a. verhindern, dass unzulässige Netzwerkverbindungen nach außen aufgebaut werden bzw. dass ein unerwünschter Serverdienst („offener Port“) gestartet wird. Das PFW-Konzept wird von vielen Experten ohnehin kritisch betrachtet, da es dem Nutzer eine oft nur scheinbar vorhandene Sicherheit vermittelt, die in der Vergangenheit in vielen nachgewiesenen Fällen umgangen werden konnte.[3]

Die Umgehung der PFW gelingt mit einem einfachen Trick ohne nennenswerten Aufwand: Die trojanische Software bestätigt blitzschnell das Dialogfenster mit der Firewall-Warnung und lässt das Öffnen der Backdoor zu Ermittlungszwecken zu. Die PFW-Funktionalität wird also nicht im engeren Sinne unterdrückt; der Verdächtige bemerkt sie aber nicht mehr, da die Bestätigung ohne sein Zutun innerhalb von Sekundenbruchteilen erteilt und auf dem Bildschirm nicht sichtbar wird.

Die Umgehung der PFW macht sich dazu das *Windows Message-System* des Betriebssystems *Windows XP* zu Nutze. Unter XP besitzt jedes Fenster einen eigenen individuellen *Window-*

[1] Ein PE-Betrachter bereitet den Code entsprechend des Portable-Executable-Formats auf.

[2] Die Import Name Table enthält Einträge aller Variablen oder Funktionen einer anderen ausführbaren Datei (so auch DLL) welche in der entsprechenden Anwendung genutzt werden.

[3] „Ein Problem von Desktop-Firewalls [wird] deutlich: Sie wiegen den Anwender in Sicherheit, die sie jedoch letztlich nicht bieten können. Bis jetzt ließ sich mit etwas Phantasie noch jede Personal Firewall umgehen und Daten unerkannt vom Rechner ins Internet senden. Außerdem erhöht jede zusätzliche Software die Komplexität eines Systems und somit auch dessen Fehleranfälligkeit.“ Zitiert aus einer Heise-Meldung vom 18.07.2006 12:55.

Identifier, über den es gezielt angesprochen werden kann. Diese Fenster verfügen über keine expliziten Funktionsaufrufe, um Benutzereingaben zu erhalten, sondern warten darauf, dass das Betriebssystem Eingaben an sie weiterleitet.

Wird nun ein Ereignis ausgelöst, wird eine Nachricht an das jeweilige Fenster versandt. Ereignisse können durch eine Vielzahl von Aktionen sowohl durch User-Interaktion als auch durch das System ausgelöst werden. Beispiele sind das Drücken einer Taste, die Bewegung der Maus oder z. B. das Sichtbarwerden eines Fensters. Auch Anwendungen können Nachrichten erzeugen und an Fenster senden. Der hier ausgenutzte Schwachpunkt dieses Systems ergibt sich daraus, dass keine Prüfung vorgenommen wird, aus welcher Quelle die entsprechende Nachricht stammt. Somit kann eine Anwendung über ein Fenster einer fremden Anwendung vielfältige Aktionen auslösen und nahezu alle Benutzereingaben nachahmen.

Da aktuell verwendete Personal Firewalls auf Nutzereingaben zum Bestätigen oder Ablehnen einer Kommunikationsanfrage warten, kann diese Eingabe durch das System generiert und an das Fenster gesendet werden. Mit Hilfe von Windows-Funktionen lassen sich nun zunächst einige *TAB-Up*-/*TAB-Down*-Events an das Dialogfenster senden um so auf die entsprechenden Buttons (Verbindung zulassen) zu „springen“. Durch das Simulieren eines *Space-Up*-/*Space-Down*-Events wird der entsprechende Button im Dialogfenster anschließend bestätigt. Das in der Abb. 2 dargestellte Dialogfenster wird damit so rasch bestätigt, dass es für den Benutzer nicht sichtbar wird.

Der hier skizzierte Weg für ein XP-basiertes System kann durch einige Zwischenschritte noch weiter verfeinert werden und lässt sich für verschiedene PFWs effektiver anpassen. Eine Übertragung der Vorgehensweise auf Windows Vista bzw. Windows 7 ist ebenfalls möglich wie bei Laborversuchen gezeigt werden konnte.

Aufwände

Die Erstellung einer RFS, die eine umfangreiche Funktionalität für Fernzugriffe auf das zu untersuchende System ermöglicht ist, ist mit geringem Aufwand möglich: Eine Nutzung vorhandener Softwarekomponenten, die über Internetquellen frei verfügbar sind (auf Basis von *Back Orifice 2000*), und eine geringfügige Modifikation des Quellcodes führt bereits bei Laboruntersuchungen zu einem funktionsfähigen RFS-Tool, das von keinem der getesteten Virenscanner erkannt wurde! Zudem ist es der so konstruierten RFS ebenfalls möglich, die Funktionalität der betrachteten *Personal Firewalls* zu umgehen, so dass trotz vorhandener Sicherheitstools einem Fernzugriff nichts mehr im Wege steht.

Die vorliegenden Untersuchungsergebnisse [GrPu09b] lassen eine Aufwandsabschätzung für den Fall zu, dass ein in „üblicher Weise“ konfigurierter PC das Zielsystem darstellt. Die Erstellung des RFS (als Unikat) ist dann mit einem Aufwand von wenigen Personentagen möglich. Eine Übertragung der Ergebnisse auf *Linux*-basierte Systeme ist nur eingeschränkt möglich, da Sicherheitsmechanismen, die eine Kommunikation der RFS mit dem Ermittler behindern, dort nicht mit zuvor beschriebenen Verfahren umgangen werden können. Welche Systemlandschaft bei Terrorverdächtigen vorherrscht, dürfte derzeit nicht bekannt sein.

Einbringung in den PC

Die Einbringung ins Zielsystem stellt den Ermittler vor eine weitere Herausforderung. Es ist zu unterscheiden, ob ein etablierter Kanal der Einbringung zur Verfügung steht (z. B. Implan-

tierung über eine Download-Verbindung in Kooperation mit einem DSL-Provider) oder ob der Verdächtige selbst erfolgreich getäuscht werden kann, so dass er eine Datei ausführt, die die RFS (in verdeckter Weise) enthält. Von einem deutlich höheren Aufwand ist auszugehen, falls ein physikalischer Zugriff (z. B. nach vorheriger Öffnung der Wohnung) erfolgen muss. Da es noch keine dokumentierten Online-Durchsuchungen gegeben hat, ist auch der bevorzugte Weg der Einbringung seitens der Ermittler nicht bekannt.

Eine Zusammenarbeit mit Herstellern von Antivirus- bzw. Antispyware-Produkten ist jedoch in keinem dieser unterschiedenen Fälle nötig, da die Schutzwirkung der Produkte (soweit der Markt von uns betrachtet wurde) unzureichend ist. Aus dem Blickwinkel der Hersteller dieser Sicherheitstools stellt die RFS eine „unerkannte“ Malware da, die ihre Schadfunktion ausführen kann, ohne dass sie von den Sicherheitsmechanismen gehindert wird.

Software für den Einzellfall

Im Vorfeld der gesetzlichen Neuregelung zur Online-Durchsuchung äußerte sich das Bundeskriminalamt zur (geplanten) Vorgehensweise bei Ermittlungen. Der BKA-Präsident Ziercke spricht dabei von einer „*[eigenen] Software, die immer nur für den Einzelfall erarbeitet wird, ein Unikat, das speziell auf die Rechnerumgebung eines Verdächtigen zugeschnitten ist*“ und nennt diese selbst eine *Remote Forensic Software (RFS).*

Die RFS soll für jeden Einzelfall berücksichtigen, welches Betriebssystem der Verdächtige verwendet, welche „*Umgebung*“ (so die Aussage) vorliegt und „*wie [der Verdächtige] kommuniziert*“ [Zie07]. Diese Vorgehensweise erscheint aber nach den dargestellten technischen Untersuchungsergebnissen zumindest für das dort zugrunde gelegte Modell eines privat genutzten PCs realistisch, da die RFS mit geringem Aufwand erstellt werden kann und Software-Unikate nicht von der Erkennung durch Virenscanner auf der Basis von Signaturdatenbanken bedroht sind.

Ob jedoch der auch zukünftig mutmaßlich überschaubare Personenkreis der Verdächtigen (Ziercke spricht von „*maximal zehn solcher Maßnahmen im Jahr*“), die einer solchen Maßnahme unterzogen werden, eine vergleichbare Rechnerkonfiguration verwendet oder auf spezielle Umgebungen ausweicht, wird erst die Praxis der Strafverfolgungsbehörden aufzeigen.

Fazit

Eine Onlinedurchsuchung ist trotz üblicherweise vorhandener Sicherheitstools technisch möglich, nachdem die Einbringung eines RFS vorgenommen wurde. Trotz gegenteiliger Äußerungen seitens der Hersteller von Anti-Virus-Software stellen deren Sicherheitstools keine wirksame Hürde einer Online-Durchsuchung dar.

Dabei kann diese RFS durchaus für den einmaligen Einsatz mit geringem technischen Aufwand (wenige Personentage) erstellt und nur einmalig genutzt werden, um eine Erkennung durch zukünftige Versionen der Virenscanner und ihrer Signaturdatenbanken und Personal Firewalls zu vermeiden. Die Erstellung des RFS gelingt auch einem Ermittler, der über durchschnittliche technische Fähigkeiten und einfache Hilfsmittel verfügt; erhebliche Ressourcen oder spezielles Expertenwissen sind nicht vonnöten, da die benötigten Software-Bestandteile im Internet verfügbar sind.

Für die technische Wirksamkeit der Online-Durchsuchung ist die tatsächliche Systemkonfiguration des zu untersuchenden Systems neben dem Nutzerverhalten des Verdächtigen von erheblicher Bedeutung. Wir können zeigen, dass ein in üblicher Weise konfigurierter PC trotz vorhandener Sicherheitstools unter Nutzung eines RFS-Unikates mit geringem Aufwand einer Online-Durchsuchung unterzogen werden kann, sofern ein etablierter Kanal zur Einbringung der RFS zur Verfügung steht.

Autoren:

Prof. Dr.-Ing. Ulrich Greveler

lehrt Informatik mit dem Schwerpunkt IT-Sicherheit an der Fachhochschule Münster

Christian Puls, MSc

ist Software-Entwickler bei der Advanced Nuclear Fuels GmbH in Lingen

---

Literatur und Quellen

[Con97] Patrick Conley: *Zwischen Festplatte und Fingerabdruck*. Der Tagesspiegel vom 14.8.1997. URL: http://www.tagesspiegel.de/zeitung/Archiv;art1291,2051236

[Gra07] Anna Grabenströer: *„Der Bundestrojaner ist nicht vorstellbar“*. Meldung in *tagesschau.de* vom 29. August 2007 (zuletzt geändert: 15:29 Uhr). URL: http://www.tagesschau.de/inland/meldung488832.html.

[GrPu09] Ulrich Greveler und Christian Puls: Über den Aufwand, Malware auf einem privaten PC zu installieren – Wie einfach lassen sich Virenscanner und Personal Firewalls umgehen? 11. Deutscher IT-Sicherheitskongress des BSI. SecuMedia Verlag. Mai 2009

[GrPu09b] Ulrich Greveler und Christian Puls: Onlinedurchsuchung versus Virenscanner - Eine Aufwandsabschätzung. In Patrick Horster (Hrsg.), D.A.CH Security '09, syssec, ISBN 978-3-00027-488-6

[Puls08] Christian Puls: *Entwicklung und Analyse einer Remote Forensic Software*. Masterarbeit am Fachbereich Elektrotechnik und Informatik der Fachhochschule Münster, Labor für IT-Sicherheit. September 2008.

[Schü08] Anja Schütz: *Vista und Mac OS gewinnen Marktanteile*. Meldung von silicon.de, 8. Juli 2008. URL: http://www.silicon.de/mittelstand/0,39038986,39193148,00 (Stand: 11.12.2008).

[Zie07] Jörg Ziercke (Präsident des Bundeskriminalamts): *„Wir haben nichts zu verbergen“*. Stern-Interview vom 30.08.2007. Elektronisch veröffentlicht vom Bundesministerium des Innern, URL: http://www.bmi.bund.de (Stand: 01.02.2009).

Abbildungen:

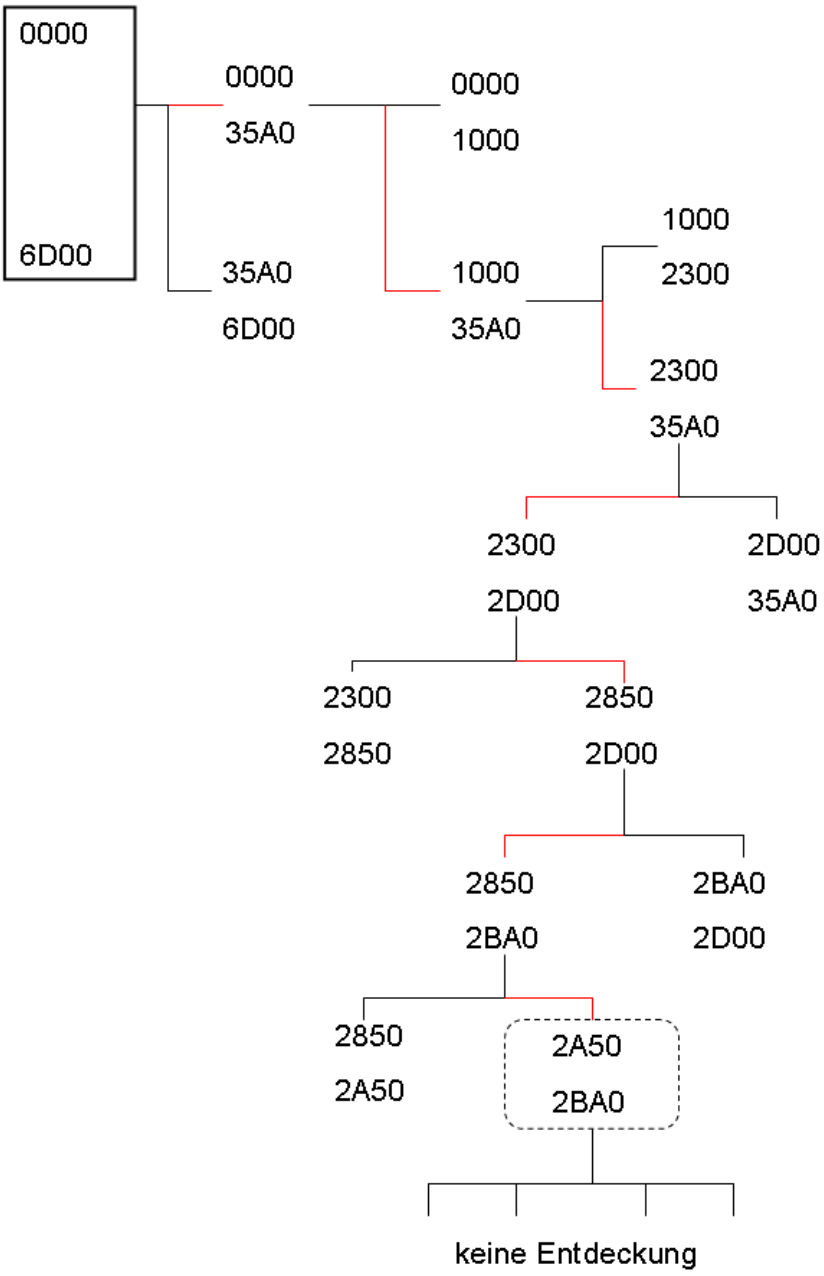

Abb. 1: Intervallschachtelung

Abb. 2: Dialogfenster einer Personal Firewall