in: Robert Uerpmann-Wittzack (Hg.): Das neue Computergrundrecht. LIT-Verlag, Berlin 2009, 53-60

Technische Aspekte des neuen Computergrundrechts

Prof. Dr.-Ing. Hannes Federrath

I. Einleitung

In diesem Beitrag geht es um Techniken, mit denen das neue Computergrundrecht verletzt werden kann und den Schutz davor. Im engeren Sinn geht es hierbei um die technischen Grundlagen von Strafverfolgungsmaßnahmen mittels Trojanischer Pferde: Es werden verschiedene technische Möglichkeiten zur Realisierung des sog. „Bundestrojaners“ diskutiert.

Um vertrauliche Daten abzufangen, die mit Hilfe eines Computers ausgetauscht werden, existieren allgemein zwei Angriffspunkte:

- **Angriff von außen:** Der Angreifer hört die Kommunikation auf den Leitungen des Kommunikationsnetzes ab.
- **Angriff von innen:** Es wird innerhalb des Computers angegriffen, auf dem die vertraulichen Daten verarbeitet werden. Damit beschäftigt sich der Hauptteil dieses Beitrags.

Angriffe von außen konzentrieren sich insbesondere auf die Übertragungswege. Sensible Benutzer (auch Kriminelle) werden möglicherweise die Daten vor der Übertragung verschlüsseln, um die Nachrichteninhalte vor einem Angreifer zu schützen. Kryptographische Verfahren sind mittlerweile sehr gut erforscht und in ausreichender Zahl auch in Anwendungen umgesetzt und praktisch für Jedermann sicher nutzbar.

Die damit verbundene Unmöglichkeit, die übertragenen Inhalte zur Strafverfolgung zu nutzen, führte zu dem Wunsch der Strafverfolgungsbehörden, dem Staat die direkte Zugriffsmöglichkeit auf den Computer zu geben, noch bevor die Daten verschlüsselt werden.

Zwar Computer bei Vorliegen der entsprechenden Voraussetzungen beschlagnahmt werden, wenn ein besonders sensibler Benutzer jedoch Verschlüsselung nicht nur bei der Datenübertragung einsetzt, sondern bereits beim Speichern der Daten auf der lokalen Festplatte, sind die beschlagnahmten Daten für Ermittlungszwecke oder als Beweis vermutlich nutzlos. Der Benutzer wird kaum freiwillig den Entschlüsselungsschlüssel (meist ein Passwort) offenbaren. Zudem kann eine Beschlagnahme nicht unauffällig und verdeckt erfolgen. Eine Überwachung künftiger Aktivitäten des Benutzers scheidet mit dieser Maßnahme somit aus.

II. Angriffe von innen

Eine nahe liegende Möglichkeit zum Zugriff auf die (verschlüsselten) Daten und die Kommunikation des Benutzers ist die Manipulation des Computers von innen. Informatiker sprechen hier allgemein von einem Trojanischen Pferd, da dies ohne das Wissen und die Zustimmung des Opfers erfolgt.

Dabei spielt es eine untergeordnete Rolle, ob die Systemveränderung völlig ohne Zutun des Opfers erfolgt (beispielsweise durch Ausnutzen einer Sicherheitslücke in der Anwendungs- oder Systemsoftware) oder ob der Benutzer aus Versehen das Trojanische Pferd selbst installiert hat (beispielsweise bei der Installation eines Computerspiels, das er aus dem Internet herunter geladen hat oder beim Klicken auf einen bösartigen E-Mail-Anhang, siehe Abb. 1). Meistens gelangen Trojanische Pferde von außen über das Internet auf den Computer; seine Wirkung entfaltet das Trojanische Pferd aber innerhalb des Computers. Deswegen handelt es sich um einen Angriff von innen.

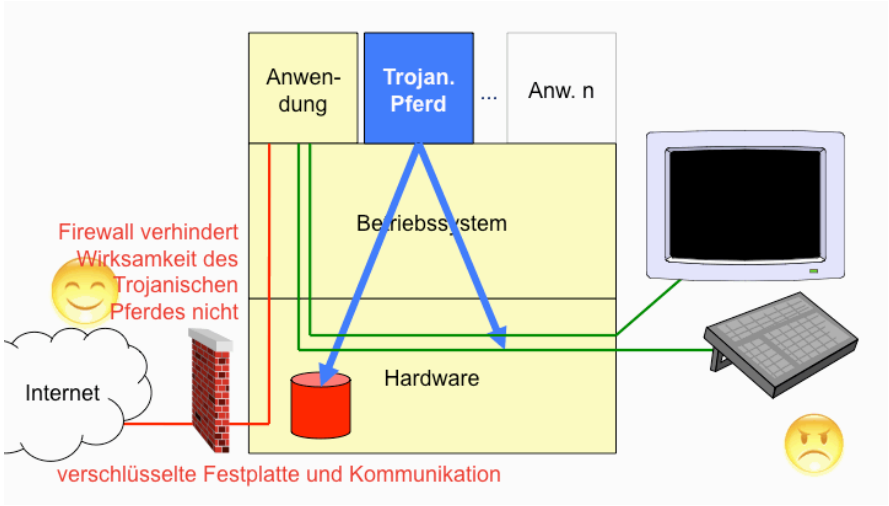

Abb. 1. Bösartige Anwendung könnte alle Daten lesen, auf die der Benutzer Zugriff hat

Angriffe von innen sind geeignet, nicht nur das Schutzziel Vertraulichkeit, um das es hier primär geht, zu verletzen, sondern auch die Schutzziele Verfügbarkeit und Integrität. Insbesondere die Integrität, die hier auch zu verstehen ist als Überbegriff für Unverfälschtheit der Daten, Authentizität, Zurechenbarkeit und Unabstreitbarkeit, kann Probleme bereiten, wenn Daten, die auf dem Computer gefunden oder von ihm empfangen oder verschickt wurden, in einem späteren Gerichtsverfahren als Beweise verwertet werden sollen: Wenn es einem Strafverfolger gelungen ist, in ein fremdes System einzudringen, kann es möglicherweise vorher auch anderen gelungen sein.

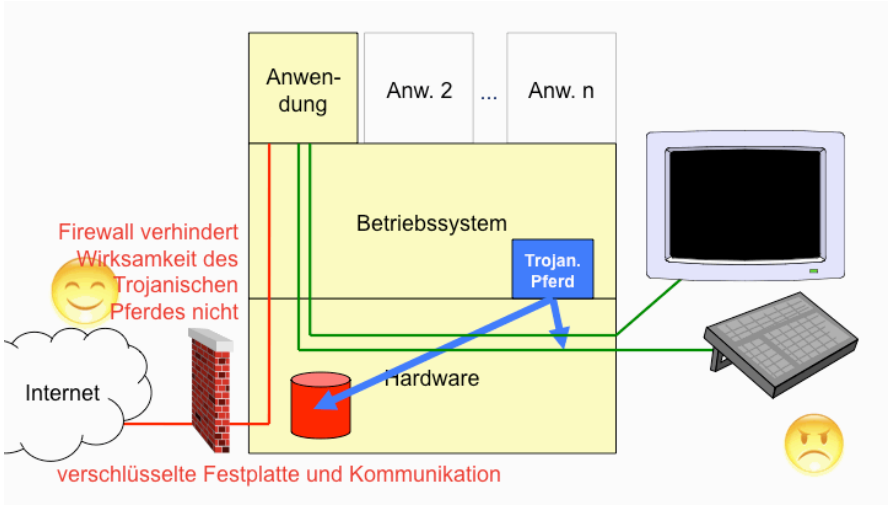

Abb. 2. Bösartige Betriebssystemkomponente (z.B. Treiber) könnte alle Texteingaben abfangen, verschlüsselte Festplatten lesen, usw.

Je nachdem, wo und wie das Trojanische Pferd installiert wurde, stehen dem Angreifer die auf dem Computer gespeicherten und verarbeiteten Daten zur Verfügung. Allgemein verfügt das Trojanische Pferd über diejenigen Lese- und Schreibzugriffsrechte, die der Benutzer ihm verliehen hat (absichtlich oder unabsichtlich).

Besonders dann, wenn sich

1. ein Trojanisches Pferd als nützliches Computerprogramm tarnt oder eine Sicherheitslücke im Betriebssystem ausnutzt, z.B. weil das System nicht auf dem aktuellen Stand ist oder
2. eine Lücke ausgenutzt wird, die zum Zeitpunkt Ihrer Veröffentlichung nur sehr wenigen Hackern bekannt ist (sog. Zero-Day-Exploits), die sich dieses Wissen ggf. teuer bezahlen lassen[1],

kann davon ausgegangen werden, dass dem Angreifer *alle* Daten zur Verfügung stehen. Gleiches gilt für Trojanische Pferde, die sich im Betriebssystem verstecken (siehe Abb. 2) und dort als Systemdienste tarnen (z.B. sog. Root-Kits). Auch hier hilft die Einschränkung von Zugriffsrechten nicht mehr, weil die Zugriffskontrolle Teil des Betriebssystems ist und somit nur vor unberechtigten Zugriffen durch fremde Anwendungen schützt.

Schlimmstenfalls kann ein Trojanisches Pferd auch alle Kommunikation mit Peripheriegeräten (Bildschirm, Tastatur, aber auch beispielsweise Chipkartenleser) vollständig überwachen und manipulieren.

Besonders dreiste Angriffe sind auch denkbar mit Hilfe von Virtualisierungstechnologien. So sind heute alle gängigen Betriebssysteme nicht nur auf physischer Hardware lauffähig, sondern setzen lediglich das Vorhandensein bestimmter Schnittstellen voraus. Jede Hardware-Komponente (Soundkarte, Grafikkarte, Tastatur usw.) hat eine Schnittstelle (z.B. durch festgelegte Speicherbereiche des Hauptspeichers realisiert), über die das Betriebssystem mit der Hardware kommuniziert.

Da es sich hierbei letztendlich aus Sicht des Betriebssystems um eine Software-Schnittstelle handelt, kann ein Betriebssystem nicht (bzw. nicht leicht) erkennen, ob die Schnittstellen auf der Gegenseite tatsächlich in Hardware oder möglicherweise in Software (durch ein Trojanisches Pferd) realisiert sind (siehe Abb. 3). So könnte dem Betriebssystem eine scheinbar harmlose Hardware „vorgegaukelt“ werden.

Weil die Veränderung außerhalb des eigentlichen Betriebssystems erfolgt, erscheint der Computer (aus der Sicht des Betriebssystems und aller Anwendungen) fehlerfrei und nicht manipuliert, so als befände er sich in der wirklichen Welt. Tatsächlich aber läuft er auf einem bösartigen Emulator.

---

[1] http://www.virus.org/news-archive/17-general-security/300-zero-day-auction-site-opens-doors

In Anlehnung an den Kinofilm „Matrix“ wurde ein Proof-of-Concept einer solchen Virtualisierungsschicht *Blue Pill* genannt.[2] Es wurden auch Überlegungen veröffentlicht, wie eine solche Virtualisierungsschicht innerhalb des Betriebssystems erkennbar ist (*Red Pill*[3]).

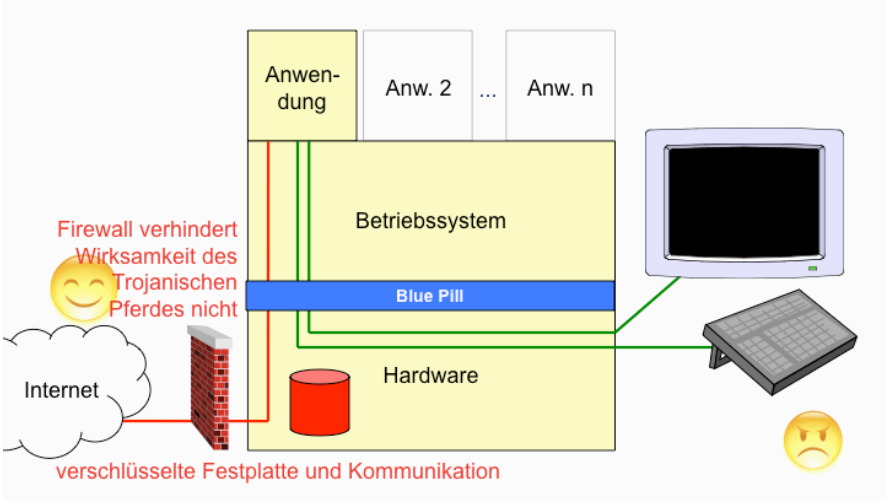

Abb. 3. Bösartige Virtualisierungsschicht (z.B. Blue Pill) könnte dem Betriebssystem einen „sauberen“ Computer vorgaukeln

Eine konkrete Implementierung einer Virtualisierungsschicht zum Überwachen eines Computers könnte z.B. den Bootsektor einer Festplatte so manipulieren, dass beim Hochfahren des Computers zunächst ein minimales eigenes Betriebssystem gestartet wird, das anschließend dem (unveränderten) Betriebssystem eine originale Hardware vorgaukelt. Noch wirkungsvoller wäre es, gleich das BIOS zu modifizieren. Beim Start des Computers wird vor dem Laden des Betriebssystems der Programmcode des BIOS ausgeführt. Das BIOS befindet sich üblicherweise in einem Flash-Speicher auf dem Motherboard des Computers. Selbst nach dem

[2] http://blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf und http://bluepillproject.org/
[3] http://invisiblethings.org/papers/redpill.html

Formatieren der Festplatte und der Neuinstallation des Betriebssystems wäre das Trojanische Pferd somit noch vorhanden.[4]

III. Kommunikation mit der Außenwelt

Über einen verdeckten Kanal, also einen Kommunikationsweg, der für den Benutzer nur sehr schwierig zu erkennen ist, versucht das Trojanische Pferd, die abgefangenen Daten nach außen zu transportieren. Praktisch nützlich ist die Möglichkeit, das Trojanische Pferd von außen fernzusteuern, d.h. ihm auch Anweisungen zu erteilen. Ein solches universelles Trojanisches Pferd eignet sich auch, um nach erfolgreichem Angriff seine Spuren zu verwischen, z.B. indem es sich selbst löscht.

Eine etwa vorhandene Firewall stellt für die Kommunikation nach außen kein Problem dar. Üblicherweise wird die verdeckte Kommunikation in einem Protokoll versteckt, das auf dem Computer wahrscheinlich erlaubt ist (z.B. http). Außerdem wird das Trojanische Pferd mit einer Nutzfunktion (Tarnung) ausgestattet, die auf Kommunikation angewiesen ist. Ist beispielsweise ein vom Opfer genutztes Programm zum Anzeigen von Börseninformationen ein Trojanisches Pferd, dann wird das Kommunizieren mit der Außenwelt (Abruf der Börseninformation) keinen Verdacht erregen.

Für die Fernsteuerung eines Universellen Trojanischen Pferdes kann eine Firewall meist leicht überwunden werden. Wenn Kommunikation von innen nach außen erlaubt ist (siehe vorheriger Absatz), dann kann das Universelle Trojanische Pferd z.B. regelmäßig beim Angreifer „nachfragen“, was es tun soll. Die Kommunikation von außen nach innen wird sozusagen auf die umgekehrte Kommunikationsrichtung zurückgeführt.

Die Programmierung eines Universellen Trojanischen Pferdes ist für einen Informatiker nicht komplizierter als das Schreiben einer normalen Anwendung. Zu Schulungszwecken nutzen wir beispielsweise ein selbst programmiertes Trojanisches Pferd, das sich als Newsticker tarnt. Die Schadroutinen umfassen ca. 70 Zeilen Programmcode. Ein durchschnittlich erfahrener Programmierer kann dies in weniger als 30 Minuten entwickeln. Dass mit wenigen Zeilen Programmcode hoher Schaden angerichtet wer-

[4] http://www.heise.de/newsticker/meldung/print/135171

den kann, wurde im Jahr 2000 deutlich, als der Loveletter-Wurm (ca. 330 Zeilen Code) weite Teile des Internet lahm legte.[5]

IV. Enttarnen und Schutz

Trojanische Pferde und deren verdeckte Kanäle können, wenn sie gut getarnt sind, allenfalls Verdacht erregen durch die ggf. ungewöhnliche Datenmengen, die ins Internet gesendet werden.

Da ein Trojanisches Pferd letztlich Software darstellt, kann bei vorliegendem Verdacht durch Reverse Engineering festgestellt werden, welche Funktionen das Programm ausführt. Ein Schutz des Trojanischen Pferdes vor seinem Opfer ist somit unmöglich.

Dass ein Trojanisches Pferd gewöhnlich Software darstellt, kann sich das Opfer auch zunutze machen. Soweit es sich *nicht* um Trojanische Pferde handelt, die sich der Benutzer aufgrund der für ihn nützlichen Tarnfunktion bewusst installiert hat, können Virtualisierungstechnologien auch ihm helfen: Das Betriebssystem sowie die Anwendungen werden stets aus einem vorher „eingefrorenen“ Systemzustand (Snapshot) gestartet, der sicher ist, d.h. frei von Schadfunktionen. Alle Formen von Manipulationen am Betriebssystem und an Anwendungen gehen somit bei einem Neustart verloren; das System ist wieder frei von Schadsoftware. Selbst die Blue-Pill-Virtualisierung kann damit verhindert werden.

V. Hardware zur Überwachung

Der Vollständigkeit halber muss noch abschließend erwähnt werden, dass neben den hier beschriebenen Möglichkeiten, das neue Computergrundrecht mittels in Software realisierten Trojanischen Pferden zu verletzen, noch eine triviale Möglichkeit existiert, an die verschlüsselten Daten eines Computers zu gelangen: Das Eindringen in den persönlichen Bereich des Computerbenutzers und die Installation eines Hardware-Keyloggers (siehe Abb. 4). Hierzu muss in den Raum eingedrungen werden, in dem der Computer steht und ein kleines Gerät in der Form eines Adapters zwischen PC und Tastatur gesteckt werden.

Dieser Adapter zeichnet alle Tastatureingaben auf, so etwa auch Zugangsdaten, Passwörter für die Festplattenverschlüsselung, aber auch die einge-

[5] http://www.heise.de/newsticker/meldung/print/9390

gebenen Texte. Später wird erneut in den Raum eingedrungen und der Adapter wieder entfernt. Die Zugangsdaten können nun in Ruhe ausgelesen werden. Das Eindringen in den Computer erfolgt dann entweder von außen über das Internet bzw. bei einer etwaigen Beschlagnahme des Computers kann die Festplattenverschlüsselung überwunden werden.

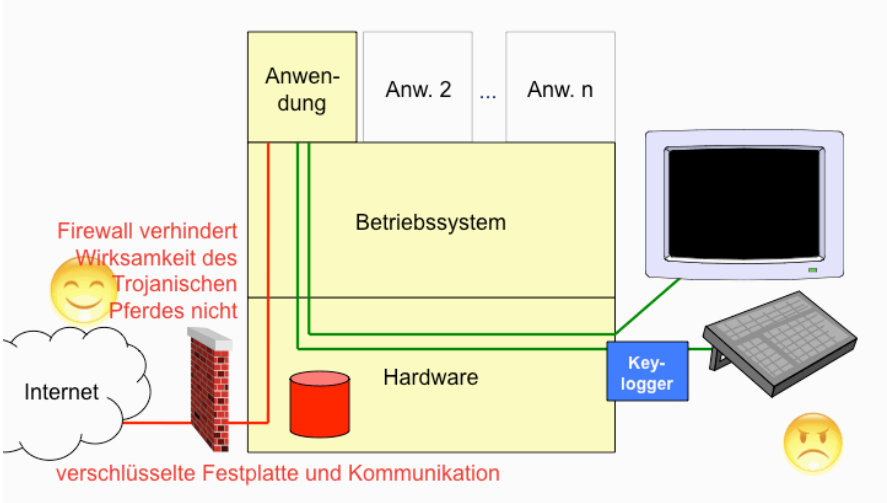

Abb. 4. Bösartige Hardware (z.B. Keylogger) könnte Texteingaben (z.B. Passwort der Festplattenverschlüsselung) abfangen

Ein Video, das einen solchen Angriff anschaulich macht findet sich im Internet unter http://www.youtube.com/watch?v=8FYPHb828f4.

VI. Schlussbemerkungen

Zusammenfassend kann festgestellt werden, dass ein auf einem System installiertes Trojanisches Pferd sowohl verschlüsselte Festplatteninhalte lesen kann, alle Tastatureingaben mitlesen kann (Keylogger), alle Bildschirmausgaben kennt unter Umständen einem Betriebssystem sogar vorgaukeln kann, dass es frei von Schadfunktionen ist.

Problematisch ist die Tatsache, dass derartige Eingriffe in Computersysteme nicht nur die Vertraulichkeit verletzen (was ja aus Sicht eines Strafverfolgers das gewünschte Ziel des Angriffs ist), sondern auch die Integrität

(was möglicherweise zur Unbrauchbarkeit der ermittelten Daten als Beweismittel führt).

Danksagung

Ein herzlicher Dank für Anregungen und Verbesserungsvorschläge sowie für das Korrekturlesen geht an Dr. Claudia Federrath und Dipl.-Wirtsch.-Inf. Florian Scheuer.