Wissen Sie, was in Ihrem Netzwerk wirklich vor sich geht?

In den letzten Jahren macht so genannte „Phone Home Software“ immer mehr von sich reden. Dabei sammelt die Software Daten des Nutzers und versendet diese unbemerkt über das Internet an den Hersteller. Schlimmer als diese Software aber sind Schadprogramme, die „Hintertüren“, „Spambots“ oder „DDoS-Tools“ installieren und Kriminellen so Zugang zu Ihrem PC ermöglichen.

Viele Anwender sind dazu übergegangen, Personal Firewalls auf ihrem Rechner zu installieren, und fühlen sich nun fälschlicherweise sicher. Zwar kann eine solche Firewall anzeigen, ob ein unberechtigter Zugriff von außen stattfindet, jedoch ist es nicht möglich zu sehen, welche Daten über das Netz fließen. Eine solche Firewall versagt auch, wenn es sich um Schadsoftware handelt, die Daten sammelt und dann über andere Programme wie Webbrowser oder Instant Messenger versendet. Diese Programme dienen ohnehin dazu, Daten zu übertragen und sind somit auch in der Personal Firewall freigegeben.

Um derartige Schadsoftware zu überführen, bedarf es anderer Mittel und auch etwas mehr Aufwand und Wissen.

Mithilfe von so genannten Sniffern (z.B. Wireshark) ist es möglich, die Datenströme im Netz zu analysieren und die Daten zu protokollieren. Die einzelnen Datenpakete können anschließend mithilfe von Analyse-Tools genau untersucht werden.

Wireshark ist eine Sniffersoftware, die wichtigste Komponente hierbei ist der Capture Driver: Dieser greift in den Treiber der Netzwerkkarte ein und sorgt dafür, dass alle gesendeten und empfangenen Pakete zwischengespeichert werden. Wireshark bietet außerdem die Möglichkeit, Filter (Netzwerkprotokoll, Quell- und Zieladresse oder TCP-Port) zu setzen, damit die Datensammlung, die später ausgewertet werden muss, überschaubar bleibt.

Die Forward Rate bei einem 100 MBit-Netz liegt pro Port bei bis zu 148.000 Paketen pro Sekunde, bei modernen 1 GigabitNetzwerken verzehnfacht sich die Anzahl der Pakete. Daher sollte der eingesetzte Rechner unbedingt über genügend Rechenleistung verfügen.

Eine Analyse-Komponente findet fehlerhafte Pakete oder Muster, die auf den Einsatz von Hackertools, wie z.B. Portscannern hinweisen. Komfortable Sniffer bringen sogar eine Komponente mit, die das automatische Dekodieren der Pakete übernimmt. Hierbei werden die einzelnen IP-Pakete dem entsprechenden Datenstrom zugeordnet. Es erspart das händische Zusammensuchen der Pakete anhand ihrer Sequenznummern.

Da professionelle Sniffer neben ihren vielfältigen Features und Verwaltungsmöglichkeiten eher für große Netzwerkarchitekturen konzipiert sind, sind sie meist zu teuer für kleine Unternehmen oder Privatanwender. Eine gute Alternative zu kommerzieller Sniffer-Software ist das Freeware-Tool Wireshark (ehemals Ethereal). Es ist für Windows sowie für Unix/Linux verfügbar und unterstützt alle gängigen Protokolle.

Bei der Windows-Variante greift Wireshark auf WinPcap, in der Linuxariante auf libpcap zurück. Bei der Analyse über Wi-L, empfiehlt sich grundsätzlich der Einsatz der Linuxariante da es unter Windows in den meisten Fällen nicht möglich ist, den Promiscuous Mode der WLAN-Karten zu nutzen.

Am Beispiel von Wireshark möchte ich zeigen, wie man den lokalen Netzwerkverkehr überwachtund wie man IP-Kommunikation untersucht, deren Ursache unklar scheint.

Zu Beginn empfiehlt es sich, Filter zu definieren, um den durch die folgende Überwachung entstehenden Datenwust möglichst gering zu halten.

Wireshark kennt grundsätzlich zwei Arten von Filtern. Die Capture-Filter definieren, welche Pakete überhaupt mitprotokolliert werden. Die Display-Filter bestimmen, welche der erfassten Pakete in der aktuellen Analyse berücksichtigt werden.

Etwas unschön ist, dass sich die beiden Filter in ihrer Syntax unterscheiden.

Beim Capture-Filter filtern Sie mit folgender Zeile nach einer MAC-Adresse:
ether host 08:00:08:15:ca:fe

Wollen Sie erst bei der Anzeige nach dieser MAC-Adresse selektieren, filtern Sie mit folgender Zeile:
eth.addr==08.00.08.15.ca.fe

In Wireshark sind bereits einige Filter vordefiniert, so ist es nicht schwer, diese auf die eigenen Bedürfnisse anzupassen.

Vor- und Nachteile der Filter:

Capture-Filter
+ Je mehr Pakete gespeichert sind, desto mehr muss der Display-Filter leisten, um die Analyse des Datenstroms zu ermöglichen.
- Ein einmal ausgefiltertes, also nicht mitprotokolliertes Paket ist weg und kann nicht mehr berücksichtigt werden.

Display-Filter
+ Alle mitprotokollierten Pakete sind nach dem Filtern durch den Display-Filter noch vorhanden und können je nach Bedarf für weitere Auswertungen ein- oder ausgeblendet werden.
- Bei jeder Änderung des Display-Filters muss Wireshark die Pakete des Datenstroms erneut prüfen.

Erste Schritte mit Wireshark

Zu Beginn verschaffen wir uns einen Einblick in die Datenströme, die an unserer lokalen Netzwerkkarte ankommen. Hierzu sollten alle Programme wie Browser, Mailclient und Messenger abgeschaltet werden.

Starten Sie Wireshark öffnen Sie das Menü „Capture“ und wählen Sie „Options…“. Hier wählen Sie die Netzwerkkarte, die die Daten sammeln soll. An dieser Stelle kann man auch die Puffergröße erhöhen, bei Netzen mit hohem Datenaufkommen ist dies empfehlenswert.
Da wir die komplette Kommunikation protokollieren wollen, wird der Haken „Limit each Packet to“ nicht gesetzt und wir verzichten auf die Auswahl eines Capture-Filters. Der Haken „Update list of packets in real time“ kann gesetzt werden, muss aber nicht, denn die Option verbraucht unnötig Rechenleistung.

Sind alle Einstellungen gemacht, starten wir die Protokollierung durch Drücken der Starbuttons. Da wir uns zunächst nur für den allgemeinen Datenverkehr interessieren, lassen wir Wireshark einige Zeit laufen und stoppen das Live-Capture dann.

Im Wiresharkenster sehen wir nun die protokollierten Pakete und die zugehörigen Protokolle. Je nach Netzwerk und verwendeten Geräten erkennen wir eine Reihe von immer wiederkehrenden Paketen. In der Regel sind das ARP-Anfragen über Rechner, die die zu einer IP gehörende MAC-Adresse ermitteln, oder Router, die Pakete versenden, welche zum Austausch von Routing-Informationen dienen.

In meinem Fall erkenne ich, dass eine Netzwerkkomponente NetBIOS-over-IPX-Pakete versendet, was nicht sein sollte, da es sich bei IPX um ein veraltetes und nicht benötigtes Protokoll handelt. Wenn man dieses Paket in Wireshark mit einem Linksklick markiert, so werden im mittleren Fenster weitere Informationen zu diesem Paket angezeigt. Besonderes interessant ist der Teil „Ethernet“. Durch einen Klick auf das Pluszeichen des Eintrags können wir die MAC-Adresse des Rechners erkennen.
Durch einen Rechtsklick auf den Eintrag „Source (MAC-Adresse)“ öffnet sich ein Kontextmenü, über welches sich ein Display-Filter erstellen lässt. Da alle Pakete von dieser oder an diese Station interessant sein könnten, ist hierzu die Option „Apply as Filter / Selected“ zu wählen. Wireshark zeigt nun alle Pakete von dieser oder an diese Station an.

Bei Durchsicht dieser Pakete finden sich glücklicherweise noch zwei BROWSE-Pakete in der Liste, über die es nun möglich ist, nähere Informationen zur versendenden Netzwerkkomponente zu erhalten. Unter anderem findet sich auch der NT-Name des Rechners, in diesem Fall PC1, der zur Domain tec4net gehört. Mit diesem Wissen lässt sich der Rechner nun leicht auffinden und entsprechend neu konfigurieren.

Filtern nach Kriterien

Werden keine Filter gesetzt, liefert Wireshark auch alle Management-Pakete wie ARP-Requests, STP-Nachrichten oder Ähnliches. Diese Informationen sind aber eigentlich nur nützlich, wenn Sie ARP-Poisoning oder einen Fehler beim Spanning Tree Protocol suchen. Um diese Pakete und IP-Broadcasts auszufiltern, ist es möglich, einen Capture-Filter zu definieren, der als Quell- oder als Ziel-IP nur die eigene IP-Adresse erlaubt. Hierzu öffnen Sie den Dialog „Capture / Options“ und tragen im Feld neben dem Button Capture-Filter Folgendes ein:

host <IP-Adresse>

Die <IP-Adresse> ist hierbei die IP der Netzwerkkarte, welche den Datenverkehr protokolliert. Bei bestimmten Verdachtsmomenten hinsichtlich verwendeter Ports ist es möglich, die Filter weiter einzugrenzen, um das Datenaufkommen zu begrenzen. Die folgende Zeile selektiert nur Pakete von der eigenen oder an die eigene Station, die http-Traffic enthalten:

host <IP-Adresse> and tcp port 80

Wie bereits erwähnt, lassen sich entsprechende Pakete aber auch noch später über die Display-Filter für die Anzeige selektieren.

Als Datenschutzexperte müsste ich angesichts der Analyse-Möglichkeiten des Sniffings nun die Hände über dem Kopf zusammenschlagen. Dennoch ist Sniffing sinnvoll und für den störungsfreien Betrieb eines komplexen Netzwerks auch notwendig. Zum einen, um Fehler im LAN zu erkennen und andererseits, um Hacker oder "Phone Home"-Software aufzuspüren.

Werden die beschriebenen Techniken nur zur Fehlerbeseitigung genutzt und anschließend alle Protokolldateien rückstandslos gelöscht, so ist die Balance zwischen technischer Notwendigkeit und den Vorgaben des BDSG eingehalten.

Wie sieht es in Ihrem Unternehmen aus?

Ich berate Sie gerne zu diesen Themen.

Matthias Walter
EDV-Sachverständiger und Datenschutzbeauftragter

tec4net IT-Solutions
Flunkgasse 22
81245 München

http://www.tec4net.com
info@tec4net.com
