Wege zum Identity-Management
Fahrlässiges Arbeiten oder gezielte Angriffe der Mitarbeiter sind eine Gefahr für das Firmennetz. Gefragt ist ein Identity- und Access-Management. Single-Sign-on hat sich dafür als Einstieg bewährt.
SEITE 24

Tuning-Tipps für App-Server
Verteilte Anwendungen werden heute vielfach komponentenorientiert auf Basis von J2EE gebaut. Dabei gilt es einige Regeln etwa für den Datenbankzugriff und die Behandlung von Transaktionen zu beachten.
SEITE 30

COMPUTERWOCHE.de

Zukunft der IP-Netze
Die Tage pauschaler Angebote sind gezählt.
www.computerwoche.de/581548

Blades reduzieren Komplexität
Vorteile und Probleme der Kompakt-Server.
www.computerwoche.de/576960

COMPUTERWOCHE.de

Wireshark – günstige Sniffer-Alternative

Der Open-Source-Analyzer bringt die etablierten Anbieter von Netz-Tools zunehmend in Bedrängnis.

VON DORIS GOTTSTEIN*

Für viele IT-Verantwortliche sind sie in Zeiten knapper Kassen ein Muss: „Open Source"-Lösungen, um die Kosten zu senken. Im Networking-Bereich ist dies Wireshark – alias Ethereal –, das sich als freies Netzwerkanalyse-Tool einen Namen machte. Die Software ist nicht nur unter Kostenaspekten interessant, sondern bietet hinsichtlich Bedienerfreundlichkeit und Aktualität erhebliche Vorteile gegenüber den lizenzpflichtigen Konkurrenten.

Protokoll-Decoder als Trumpf

In wenigen Jahren hat sich Wireshark/Ethereal so vom Do-it-yourself-Programm zum führenden Netzwerkanalyse-Tool für Profis entwickelt. Bedingt durch den Firmenwechsel zu Cace Technologies in Davis, Kalifornien, musste der Softwaregründer Gerald Combs allerdings den ursprünglichen Namen Ethereal aufgeben, denn die Namensrechte verbleiben bei seinem ehemaligen Arbeitgeber. Deshalb heißt das Erfolgsprodukt nun Wireshark.

Netzwerkern hilft das Tool vor allem beim Troubleshooting. Zudem wird das Profi-Werkzeug für die Software- und Protokollentwicklung eingesetzt. Die große Stärke von Wireshark liegt in den zahlreichen Protokoll-Decodern, die das Tool unterstützt. Dadurch besitzt es Features, die andere gängige Produkte nicht bieten können. Als einziges Produkt läuft die Software übrigens auf allen bekannten Rechner-Plattformen wie Unix, Linux, Solaris, Mac OS X, Windows und diversen BSD-Versionen.

Hier lesen Sie ...

- was ein Open-Source-Netz-Tool wie Wireshark leistet;
- wo seine Vorteile im Vergleich zu kommerziellen Produkten liegen;
- warum die Protokoll-Decoder essentielle Bedeutung haben;
- für welche Einsatzzwecke Wireshark geeignet ist.

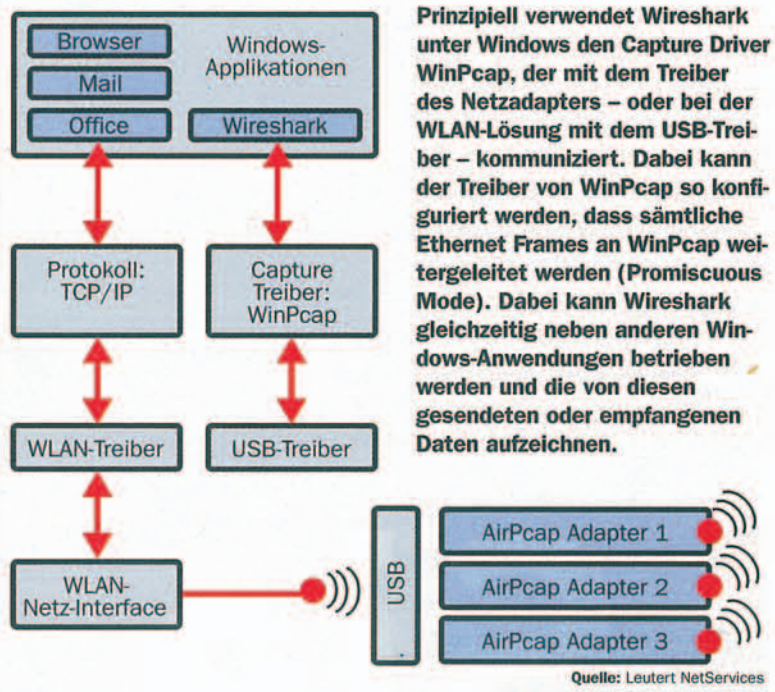
Zum Erfolg des Tools trugen laut Combs unter anderem die zahlreichen internationalen Entwickler bei, die schon 20 bis 40 Mannjahre alleine in die Arbeit für die Protokoll-Decoder gesteckt haben, mit denen die Datenpakete lesbar gemacht werden. Ein Zeitvorsprung, den selbst kommerzielle Anbieter kaum aufholen können. So überholte das Tool schnell den seit Ende der 80er Jahre marktführenden „Sniffer" in der Gunst der User. Dazu tragen allerdings auch die Premium-Preise bei, die Sniffer-Produzent Network General für jedes einzelne Tool pro Computer-Installation verlangt. Beim Einsatz mehrerer Lizenzen können schnell mehrere Tausend Euro pro Jahr allein für Updates wie etwa neue Protocol-Decoder zusammenkommen – den Anschaffungspreis von mehreren Tausend Euro pro Lizenz nicht eingerechnet.

Dass der hohe Sniffer-Preis das Überholmanöver heraufbeschwor, entbehrt nicht einer gewissen Ironie. Als Systemadministrator habe er schon an der Universität von Kansas City mit einem Sniffer gearbeitet, erklärt Combs, jedoch habe sich sein nächster Arbeitgeber, der US-amerikanische ISP Unicom, ein so teures Tool damals nicht leisten können: „Ich musste mir deshalb etwas einfallen lassen." Das Programm namens Ethereal, das Combs dann selbst entwickelte, basierte auf den beiden bereits verfügbaren Analyse-Tools LibPcap (Library Packet Capture) und TCPdump (Transmission Control Protocol).

Verteilte Entwicklung

LibPcap nutzte Combs, um Signale anzuzapfen, und das ursprünglich für Unix entwickelte Hilfsprogramm TCPdump, um die damals noch in Textform dargestellten Daten für die spätere Analyse zu speichern. Anfänglich lief Ethereal auf den Betriebssystemen Linux und Solaris und eignete sich zur Protokoll-Analyse von IP, TCP, UDP und natürlich von Ethernet, dem Namenspaten. Nur 20 000 Progammzeilen habe sein allererstes Release umfasst, sagt er, „heute sind es über eine Million".

Wireshark-Funktionsweise



Prinzipiell verwendet Wireshark unter Windows den Capture Driver WinPcap, der mit dem Treiber des Netzadapters – oder bei der WLAN-Lösung mit dem USB-Treiber – kommuniziert. Dabei kann der Treiber von WinPcap so konfiguriert werden, dass sämtliche Ethernet Frames an WinPcap weitergeleitet werden (Promiscuous Mode). Dabei kann Wireshark gleichzeitig neben anderen Windows-Anwendungen betrieben werden und die von diesen gesendeten oder empfangenen Daten aufzeichnen.

Quelle: Leutert NetServices

Das spontane Feedback der Entwickler zeigt, dass Combs Arbeit an einem eigenen Network Analyzer zur richtigen Zeit, und seine Entscheidung, ihn unter der GNU General Public Licence öffentlich zugänglich zu machen, vielen Bedürfnissen entgegen kam. Ein halbes Dutzend Leute hätten anfänglich mitgearbeitet, heute seien es 400 bis 500 Entwickler, die das Copyright an den, von ihm „Dissectors" genannten Decodern besäßen. Über mehr als 750 solcher Protocol-Dissectors verfügt Wireshark inzwischen, und mit jeder neuen Anwendung, wie etwa der Internet-Telefonie VoIP, kommen weitere hinzu. Die hohe Decoder-Zahl ist denn auch einer der Pluspunkte des Open-Source-Produkts. „Das A und O eines Protocol Analyzers sind Anzahl und Decodierungsgrad der analysierten Protokolle", kommentiert Rolf Leutert, Netzwerkanalyse-Experte der ersten Stunde.

FOTO: GOTTSTEIN

Zur richtigen Zeit das richtige Produkt: Gerald Combs gründete das Open-Source-Projekt Wireshark/Ethereal.

Mehr als ein Analyse-Tool

Einen weiteren Grund für die hohe Akzeptanz in der Networking-Szene führt Erwin Rol, Inhaber der gleichnamigen Software-Engineering-Firma aus Holzkirchen, an: „Wireshark ist nicht nur ein Tool zur Ethernet-Analyse", meint er unter Hinweis auf den früheren Namen, „es unterstützt vielmehr Hardware." Wie viele aus der Entwicklergemeinde stieg der freiberuflich arbeitende Systemsoftware-Ingenieur beim Schreiben von Netzwerksoftware in das Projekt ein: „Ich nutzte Ethereal zum Debuggen, und weil das verwendete Protokoll nicht weit verbreitet war, schrieb ich selbst ein Plugin." Auch künftig will er am Wireshark-Programm mitwirken, denn „bei der Entwicklung von Networking-Software ist eine kleine Erweiterung des Tools manchmal eine sehr große Arbeitshilfe."

Die WLAN-Variante

Mit dem Wechsel von Combs zum kalifornischen Startup-Team um Loris Degoianni und Gianluca Varenni, die für den Packet-Capture-Treiber „WinPcap" verantwortlich zeichnen, gehen weitere Entwicklerwünsche in Erfüllung. Team-Mitglied Rol dürfte nicht der Einzige sein, der sich über den „interessanten Ansatz freut, per USB Daten zu ‚sniffen'". In diesem Monat wurde der „AirPcap", ein kleiner Wireless-Adapter in Form eines USB-Memory-Sticks, in den Markt eingeführt. Der innovative Bruder des WinPcap ermöglicht es, auch drahtlos übermittelte Datenpakete einzufangen. Im Gegensatz zu PCI-Steckkarten – bei den meisten Notebooks ohnehin auf eine oder zwei begrenzt –, kann ein USB-Port mit Hilfe entsprechender Hubs einfach auf mehrere erweitert werden, was den Anschluss von mehr als nur zwei der neuen „Wireless Capture Sticks" erlaubt.

Ideale Problemlösung

Leutert findet das genial, denn „es bedeutet, dass bis zu 13 Kanäle mitgelesen werden können, so viele wie WLAN in Europa hat". Zudem wären damit im so genannten ‚Promiscuous Mode' auch Wireless Management- und Kontroll-Frames zu sehen, und zweitens könnten mehrere solche Adapter parallel in allen Kanälen Daten mitschneiden. Bislang ermöglichten selbst neuere eingebaute Karten nur ein begrenztes Aufzeichnen der Frames – sofern die Karte nicht aktiv von anderen Anwendungen wie etwa einem Browser belegt sei, erläutert der Netzwerk-Profi. Daher sei der AirPcap für Netzwerker im Wireless-Umfeld die ideale Problemlösung.

Im Verbund mit Wireshark liegen die Vorteile des innovativen Wireless-Adapters auf der Hand: Zum einen ist Wireshark selbst

ein Tool für alle möglichen Protokoll-Varianten und damit universell einsetzbar. Durch die Vielzahl an Protokollen, die Aktualität der entsprechenden Decoder und die schnelle Verfügbarkeit neuer Decoder können zudem viel mehr Informationen aufgezeichnet und ausgewertet werden. Während der in den meisten mobilen Computern vorinstallierte WLAN-Adapter weiter zum Arbeiten verwendet werden kann, ermöglicht die Installation von einem oder mehreren AirPcap-Adaptern das gleichzeitige Aufzeichnen zusätzlicher Daten aus einer oder mehreren Zellen. Im Gegensatz dazu verwenden die meisten am Markt verfügbaren Alternativprodukte den bereits vorinstallierten Wireless-Adapter, was nur eine von zwei Optionen offen lässt: Entweder wird die Verwendung eines Adapters für die normale Arbeit eingeschränkt oder wichtige Management- und Kontroll-Frames lassen sich zur Analyse nicht aufzeichnen.

Die leichte Portabilität des AirPcap USB-Adapters auf ein anderes Notebook markiert einen weiteren Vorteil: Selbst wenn dieses über keinen eingebauten Adapter verfügt, wird es dadurch schnell zu einem voll einsatzfähigen WLAN-Analyzer. Für rund 200 US-Dollar ist die innovative Hard-/Software-Kombination ab sofort über die Wireshark-Homepage zu erwerben. Ein großes Potenzial sieht Combs in weiteren Produktentwicklungen. Mit Highspeed Appliances und Network Probes beschäftigt sich das Cace-Entwicklerteam derzeit. Und auf der Wunschliste der Core Developer stehen weitere interessante Aspekte wie etwa Security, noch bessere Usability oder Decryption. Sie könnten sich genauso schnell zu Einzigartigkeiten entwickeln, die kostenpflichtige Mitbewerbs-Programme das Fürchten lehren.

Bei allen Vorzügen sollte aber eines nicht vergessen werden: Wer alle Möglichkeiten von Wireshark ausschöpfen will, kommt angesichts der Komplexität heutiger Netze kaum um entsprechende Schulungen herum. Während der Network Analyzer der Open-Source-Philosophie verpflichtet bleibt, buhlen verschiedene Anbieter derzeit um das Trainingsgeschäft. Vor knapp zwei Jahren bot Combs ehemaliger Arbeitgeber NIS unter dem eigens dafür gegründeten Firmenkonstrukt Ethereal Inc. und EtherealSoft die ersten Schulungsangebote an. Aber auch Combs neuer Arbeitgeber ist am Geschäft rund um das Analyse-Tool interessiert: Bei Cace Technologies wird gerade fieberhaft an einem Trainingskonzept gearbeitet. Und selbst in Europa mehren sich die Angebote, den perfekten Umgang mit Wireshark zu lehren. Einer der ersten Kursanbieter, Leutert NetServices, legt gerade ein Schulungsprogramm auf. Der Wettbewerb um die Dienstleistungen, die das frei verfügbare Softwareangebot kommerziell ergänzen, hat gerade erst begonnen. So ist zu erwarten, dass die kommenden Trainings-Offerten sich wohl im Rahmen marktüblicher Kursgebühren entwickeln werden. *(hi)*

***DORIS GOTTSTEIN** ist freie Wirtschaftsjournalistin in St. Blasien.

Rund um Wireshark

Schulungsanbieter und weitere Informationen zu dem Werkzeug sind unter anderem auf folgenden Internet-Seiten zu finden:

www.wireshark.org
www.cacetech.com
www.netisinc.com
www.ethereal.com
www.mnex.biz
www.wireshark.ch
www.erwinrol.com
www.sniffer.com (das kommerzielle Konkurrenzprodukt)

Mehr zum Thema

www.computerwoche.de/

575409: Open-Source-Tools prüfen IT-Sicherheit;
1214325: Gutartige Netzschnüffler.