



Open Source im Unternehmen

Doris Gottstein

Von Ethereal zu Wireshark

Von offenen Quellen und offenen Märkten

Was geschieht, wenn der Hauptentwickler einer Open-Source-Software die Firma wechselt, der alte Arbeitgeber jedoch eine komplette Infrastruktur um die Software aufgebaut hat und die Namens- und Markenrechte nicht hergeben will? Die Community hinter dem freien Netzwerkscanner Ethereal zog an einem Strang und machte weiter – unter einem neuen Namen.

Im Mai dieses Jahres wechselte Gerald Combs, Schöpfer und Hauptentwickler des erfolgreichen quelloffenen Netzwerkscanners Ethereal, den Arbeitgeber. Seit den späten neunziger Jahren bei Network Integration Services (**NIS[1]**) beschäftigt, hat er jetzt ein neues Tätigkeitsfeld bei **Cace Technologies[2]** gefunden. Die noch junge kalifornische Firma entwickelt System-, Sicherheits- und Netzwerktools.



Selbst erstellt: Das Logo für Wireshark gehört Gerald Combs – wie auch die Marke.

Geschäftsführer Robert Jewell von NIS hatte 2004 den Namen Ethereal als Markenzeichen eintragen lassen. Combs' alter Arbeitgeber war nicht bereit, die Marken- und Namensrechte an der Software an Combs abzutreten. Seitdem segelt das Open-Source-Projekt unter neuer Flagge und nennt sich nun Wireshark. Das von Combs selbst erstellte neue Logo zeigt einen stilisierten Hai. In treffender

Weise symbolisiert die Wahl das, was Netzwerker immer schon an dem Tool schätzen: Intelligenz, Reaktionsstärke, Flexibilität, Schnelligkeit und ein hervorragender Spürsinn werden dem Tier zugesprochen. Ein gutes Vorbild, erschnüffelt er Verdächtiges doch über Meilen hinaus.

Das über die ganze Welt zerstreute Entwicklerteam um den freien Netzwerkscanner reagierte gelassen auf die Weigerung von NIS, den Namen Ethereal freizugeben. Alle Kern-Entwickler des Projekts hielten Combs die Treue. "Just change the name and let's go on", war die Devise.

Erfolgsfaktor Open Source

Bei der Entwicklung von Ethereal orientierte sich Combs an **Sniffer[3]** von **Network General[4]**. Als Student an der Universität von Kansas City war er für die Netzwerkadministration zuständig und lernte dort das Referenzprodukt und den damaligen Marktführer kennen: "Anfang der 90er schafften wir einen Sniffer an, und als System Administrator war ich für Installation und Troubleshooting verantwortlich". Zwischen 40.000 und 80.000 US-Dollar habe so ein Tool damals gekostet, "ein ziemlich hoher Betrag für ein Gerät, das man nur ein- bis zweimal im Monat braucht".

Combs fand Gefallen an Sniffer und hätte bei Unicom, seinem nächsten Arbeitgeber, gern weiter damit gearbeitet. Da sich der kleine ISP ein solche Investition jedoch nicht leisten konnte, fing der Entwickler Ende 1997 damit an, in seiner Freizeit einen eigenen Protokoll-Decoder zu schreiben. Im Sommer 1998 war das erste Release des auf den Namen Ethereal getauften Tools fertig. Als dankbarer Benutzer von diversen Open-Source-Programmen entschied sich Combs, die Software unter die GNU General Public License (GPL) zu stellen.

Das anfänglich kleine Programm baute auf den bereits als Open Source verfügbaren Analyse-Tools LibPcap und Tcpdump auf, lief unter Linux und Solaris und eignete sich zur Protokoll-Analyse von IP, TCP und UDP. Die erste Version bestand aus nur 20.000 Programmzeilen; mittlerweile umfasst das aktuelle Release mehr als eine Million. Combs' Augen strahlen, wenn er über das spontane Feedback der Entwickler und Technologie-Aspekte spricht: "Es war erstaunlich, dass sie so viel zum Projekt beitrugen, und zeigt, dass sie dieselben Bedürfnisse hatten wie ich."

Das halbe Dutzend Leute, das Combs in den frühen Anfängen zur Seite stand, ist über die Jahre zu einer Community beträchtlichen Umfangs herangewachsen. Etwa 400 bis 500 Entwickler besitzen das Copyright an den zahlreichen Protokoll-Decodern oder Plugins, die die Software so universell einsetzbar machen. Das über viele unterschiedliche Parteien verteilte Urheberrecht schützt das Open-Source-Projekt effektiv gegenüber den Interessen Einzelner, das Programm zu Geld zu machen.

Aus Ethereal wird Wireshark

1998 wechselte Combs von Unicom zu NIS. Offensichtlich sah der neue Arbeitgeber Potenzial in dem Projekt Ethereal, denn schon bald danach wurde die Tochterfirma Ethereal Inc. aus der Taufe gehoben. Das wenig später ebenfalls von NIS gegründete **Etherealsoft[5]** bietet Entwicklungsdienstleistungen, Schulung und Support rund um das Netzwerk-Analyse-Werkzeug.

Fällt das Firmengebilde, mit dem der Sicherheitsspezialist den Geschäftsfeldern rund um das Ethereal-Projekt ein Zuhause gab, mit Combs' Entscheidung für Cace Technologies nun wie ein Kartenhaus zusammen? Combs, der den Wechsel mit persönlichen Motiven begründet, weiß es nicht. Auch wenn er den "ätherischen" Namen, den Netzwerk-Administratoren spontan mit Ethernet in Verbindung bringen, samt Marke zurücklassen musste, schätze er seine bisherige Firma und die Kollegen sehr, lässt er diplomatisch vernehmen.

Robert Jewell, der Geschäftsführer von NIS, bedauert das Weggehen des Ethereal-Entwicklers. Auch ihm lässt sich jedoch keine konkrete Antwort entlocken. "Wir fühlen uns dem Open-Source-Konzept verpflichtet und werden unsere Trainingsangebote für Ethereal, Wireshark und andere Open-Source-Produkte weiter ausdehnen", so die Aussage. Wie dieses Angebot jedoch aussehen soll und ob NIS selbst Pläne zur Weiterentwicklung von Ethereal hat, bleibt im Dunkeln.

Mit jedem neuen Release baut Wireshark seinen Entwicklungsvorsprung aus. Version 0.99.1 erschien mit dem Umzug der Website, aktuell ist 0.99.2. In wenigen Monaten sollen mit Release 1.0 eine Menge neuer Features kommen. Die Chancen für alternative proprietäre oder parallel entwickelte Software-Produkte stehen schlecht: "20 bis 40 Mannjahre Arbeit stecken alleine in der Entwicklung der verschiedenen Protocol Dissectors", rechnet Combs vor. Mit dem Wechsel des kompletten Entwickler-Teams zu Wireshark gibt es kaum Bedenken mehr: die Zukunft gehört Wireshark.



Wireshark-Gründer Gerald Combs (in der Kansas City Central Station, in der gerade für die Shark Exhibition erworben wird).

Neue Ausblicke

Gerade ist der **AirPcap[6]** von Cace, ein kleiner Wireless-Adapter in Form eines USB Memory Sticks, erschienen. "Der Wireless-Markt wächst dynamisch", meint Combs. Ein großes Potenzial sieht der Neue im Cace-Team auch in weiteren Produktentwicklungen. Mit Highspeed Appliances und Network Probes beschäftigen sich die Entwickler um Loris Degoiani und Gianluca Varenni derzeit. Das Zusammenwachsen der Angebotspalette rund um Wireshark verspricht spannend zu werden.

Nicht nur deshalb fühlt sich Combs, der bis zum Umzug ins kalifornische Davis noch über einen Fernzugang arbeitet, wohl im neuen Job. Das Entwickler-Team seines neuen Arbeitgebers denkt so wie er, spricht seine Sprache und genießt den Fun-Faktor der Arbeit.

Geläutert durch die Erfahrung mit NIS hat der Programmierer das Namens- und Markenrecht an Wireshark zunächst für sich selbst gesichert. Er könne sich aber auch gut vorstellen, das Projekt bei einer Stiftung zu beheimaten, die nicht nur über das Copyright wacht, sondern das Fortbestehen der Open-Source-Software dauerhaft sicherstellt.

URL dieses Artikels:

<http://www.heise.de/open/artikel/77199>

Links in diesem Artikel:

[1] <http://www.netisinc.com/>

[2] <http://www.cacetechnology.com/>

[3] http://www.networkgeneral.com/Product_Home.aspx

[4] <http://www.networkgeneral.com/>

[5] <http://www.etherealsoft.com/>

[6] [http://www.cacetechnology.com/products/airpcap.htm?](http://www.cacetechnology.com/products/airpcap.htm?utm_source=Wireshark&utm_medium=banner&utm_term=vertical&utm_campaign=Airpcap)

[utm_source=Wireshark&utm_medium=banner&utm_term=vertical&utm_campaign=Airpcap](http://www.cacetechnology.com/products/airpcap.htm?utm_source=Wireshark&utm_medium=banner&utm_term=vertical&utm_campaign=Airpcap)