Gemeinsame Stellungnahme von ANGA, Buglas und eco an die Bundesnetzagentur zur übersendeten Datei Breitbandmessung.Open.Source.20170727.zip

I. Einleitung und Zusammenfassung

Im Nachgang zu dem am 25.07.2017 durchgeführten Workshop zur installierbaren Version stellte die Bundesnetzagentur Teile des Codes aus dem Tool ihres Dienstleisters als Open Source Code[1] zur Verfügung. Dieser Code soll der Ermittlung der Geschwindigkeit von Breitbandanschlüssen (im Folgenden Breitbandmessung) dienen und für die installierbare Version der Breitbandmessung Verwendung finden.

Er wurde jedoch um proprietäre Bestandteile bereinigt[2] und ist aus diesem Grunde unvollständig und in seiner vorgesehenen Funktion nicht kommentierbar. Die von den Branchenverbänden seit langem geforderte Transparenz in den Funktionalitäten des Messtools kann aus Sicht der Verbände ANGA, Buglas und eco nur durch eine vollständige Offenlegung erreicht werden, auch wenn eine lauffähige Applikation auf Basis des Codes erstellt werden kann. Die zeichnenden Verbände nehmen die angebotene Gelegenheit für eine zumindest partielle Stellungnahme gerne wahr und bedanken sich bei der Bundesnetzagentur für die Möglichkeit der Kommentierung.

Bereits in einer früheren Stellungnahme zu dem „Überblick technische Parameter der installierbaren Version“ vom 07.08.2017 wurde hinsichtlich des Sourcecodes der Server-Komponente das Fehlen

- von allen Angaben zu relevanten Systemvoraussetzungen (z.B. Linux Kernel Version), zum verwendenden Build-Environment des Serverteils für den Sourcecode und zu den verwendeten Bibliotheken und deren Versionsnummern;
- von Anforderungen an eine Testspezifikation (Acceptance Test Plan für die Tiefenprüfung des Systems);
- einer Dokumentation der Netzwerkumgebung sowie
- jeglicher Information zum Zertifizierungs- und Validierungsprozedere der BNetzA

angemerkt (Antwort ausstehend).

Darüber hinaus besteht schon länger die Forderung nach einer Konkretisierung und Vervollständigung des auf der Website der breitbandmessung.de veröffentlichten Konzepts („Technische Spezifikation“ zur Breitbandmessung)[3], gegen die eine inhaltliche Prüfung des Sourcecodes ermöglicht würde. Ohne diese grundlegenden Informationen kann sich die vorliegende Kommentierung nur auf einige formelle Aspekte beschränken. Eine Aussage, ob der Sourcecode sich in der Gesamtbetrachtung für die Erfüllung der ihm zugedachten Aufgabe eignet oder nicht, kann an dieser Stelle daher nicht ergehen. Die weiter mitgeltenden Bedenken und die grundlegende Kritik am Messverfahren und dessen Methodik sind ebenfalls hier nicht Gegenstand, sondern Inhalt vorheriger Stellungnahmen[4].

Die zeichnenden Verbände begrüßen die Ankündigung der Bundesnetzagentur, den Sourcecode auf Ihrer Website zur Verfügung zu stellen. Um der in der Ausschreibung festgelegten Veröffentlichung des Sourcecodes vollumfänglich, entsprechend den Open Source Gepflogenheiten, Rechnung zu tragen, regen die zeichnenden Verbände die zusätzliche oder ersetzende Veröffentlichung und Pflege des vollständigen Sourcecodes auf einer geeigneten Plattform (z.B. GitHub) an. Die Veröffentlichung sollte auch die vorstehend aufgeführten, bisher vermissten Angaben beinhalten, um die Transparenz sicherzustellen.

---

[1] Gemäß enthaltenen Lizenzfiles steht der Code unter verschiedenen Open Source sowie Community Lizenzen.
[2] Mündliche Mitteilung im Workshop vom 25.07.2017
[3] „Technische Spezifikation - breitbandmessung.de.pdf“, MD5SUM d574b5147cd23a41871ff87813add5e5
[4] Siehe auch: http://www.anga.de/infothek/aktuelles/anga-stellungnahme-zum-bnetza-messtool, http://buglas.de/fileadmin/user_upload/Stellungnahmen/Verbaendestellungnahme_Gemeinsamer_Anforderungskatalog_fuer_installierbare_Version_eines_zertifizierten_Messtools_07082017.pdf, https://www.eco.de/wp-content/blogs.dir/gemeinsamer-anforderungskatalog-fuer-installierbare-version-eines-zertifizierten-messtools_07082017.pdf, https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Breitband/Breitbandgeschwindigkeiten/Breitbandgeschwindigkeiten.html

Hinweisen wollen wir an dieser Stelle darauf, dass aufgrund des hier eingesetzten Lizensierungsmodells jegliche Änderungen, Modifizierungen und Anpassungen an Client und Server ebenfalls unter der vorgegebenen Lizenz veröffentlicht werden müssen.

II. Stellungnahme im Einzelnen

a) Angaben zu relevanten Systemvoraussetzungen (z.B. Linux Kernel Version), konkrete Angaben zum Build-Environment des Serverteils für den Sourcecode (sowie die notwendigen Angaben zu den verwendeten Programmbibliotheken[5] (im Folgenden „Libraries“) und deren Versionsnummern sind derzeit nicht verfügbar.

   In den enthaltenen Konfigurationsvorgaben befindet sich zudem ein Verweis auf die Einbindung einer – mutmaßlich proprietären – unbekannt gebliebenen Library. Auf Grund der Namensgebung dieser Library (zafaco) steht zu vermuten, dass es sich hierbei um einen speziellen Code der Firma Zafaco handelt. Welche Aufgaben die darin enthaltenen Programmteile erfüllen oder inwieweit durch diese Library andere Routinen aus den im Sourcecode ersichtlichen und den sonstigen Libraries ersetzt werden, ist nicht abzuschätzen. Zumindest fehlt eine nachvollziehbare Dokumentation der Funktion dieser Library.

   Hinsichtlich der verwendeten angepassten noPoll Library vermissen wir Angaben zu Version, Release-Datum und Patch-Level sowie GitHub Stand[6]. Diese Angaben werden auf der Webseite https://breitbandmessung.de/impressum[7] und in einer der Dateien mit Namen README.md derzeit nicht aufgeführt.

   Die Verwendung von Compilerdirektiven und –Schaltern wie z.B. Optimierungs-Optionen werden automatisch ermittelt und sind nicht transparent dargelegt. Die Auswirkungen auf das ausführbare Programm sind nur sehr schwer abzuschätzen[8]. Wünschenswert wären zudem ein Prozessbild aller Funktionen und eine Übersicht über die Abläufe des Programmes.

   Auf Grund der unzureichenden Angaben waren die zeichnenden Verbände mit dem gelieferten Sourcecode nicht in der Lage, eine belastbare Analyse zu erstellen. Schon das Fehlen der Library (zafaco) sowie deren Headerdateien und die nicht vorhandenen Versionsangaben verhindern eine vollumfängliche Prüfung. Des Weiteren ist die Entwicklung des Linux Kernels so schnell, dass die Angabe der Kernel Version zwingend ist, um eine Referenzarchitektur zu definieren. Die Angabe der verwendeten Architektur (z.B. x86, x86-64) oder der zum Testen verwendeten Linux-Distribution (z.B. Red-Hat oder Debian/Ubuntu basiert) ist unabhängig vom Linux (Kernel). Aus diesen Gründen muss von einer Kommentierung des eigentlichen Codes abgesehen werden.

b) Es fehlt eine Angabe zu den Anforderungen an eine Testspezifikation (Acceptance Test Plan) für die Tiefenprüfung des Systems. Diese ist erforderlich, um eine einheitliche Basis für die Prüfung zu definieren und sicherzustellen, dass Prüfungen und Validierungen immer gegen eine Referenzarchitektur und die Ergebnisse der Prüfungen, jedoch nicht die Interpretation dieser Ergebnisse, herleitbar sind.

c) Hinsichtlich der gesamten Netzwerkumgebung zwischen der Server und Client Applikation fehlt die Dokumentation. Die bereitgestellte Applikation interagiert mit der Netzwerkumgebung in Up- wie auch Downloadrichtung und reicht Pakete an diese weiter bzw. erhält Pakete als Teil des Messverfahrens[9]. Auch hier besteht die Notwendigkeit der Bekanntgabe und Dokumentation um eine Vergleichbarkeit in den Ergebnissen zu erzielen.

   Das Fehlen der Dokumentation betrifft insbesondere:

[5] Gesamtheit mehrerer häufig verwendeter, mit Namen versehener [..] Programmteile, die in einer Datei zusammengefasst sind. (Quelle: http://www.duden.de, abgerufen am 21.08.2017).

[6] Änderungen zum Versionsstand der nopoll Library sind in die verwendete abgeleitete Version derzeit noch nicht eingeflossen.

[7] dort angegebene Open Source Komponenten (ohne Versionsangabe, abgerufen am 29.08.2017): noPoll, json11, jQuery, browser-report, Forge.

[8] siehe z.B. https://lists.debian.org/debian-devel/2017/06/msg00308.html

[9] der bereitgestellte Code scheint im Kern nur den einfachen Teil des Messverfahrens wie Datengenerator und eine Stoppuhr-Funktion zu umfassen.

- die verwendete Hardware, die Implementierung des TCP/IP-Stacks und Einstellungen. Gemäß Begleitdokumentation (README.md) greift die Server Komponente auch auf Fremdcode der Firma Advanced Software Production Line, S.L. zurück (https://github.com/zafaco/nopoll). Diese Library realisiert den Datenaustausch zwischen Client und Server durch Übergabe von Datenpaketen an den verwendeten Linux Kernel. Hinsichtlich der internen Zeitablaufsteuerung zur Weitergabe (Queuing und Scheduling) der Daten an die Netzwerkinterfaces existieren signifikante Unterschiede in den Linux Kernel Versionen. Dies hat einen deutlichen Einfluss auf die zu erzielenden Bandbreiten an den Interfaces. Ebenso haben diese Parameter einen Einfluss auf die Latency, welcher auf Grund der Verwendung von TCP im Tool der Breitbandmessung bekanntermaßen eine erhebliche Bedeutung zukommt

- die Überwachung der Kapazität der Anbindung des eigenen Peerings

- die Evaluierung des Netzwerkpfades, so z.B. Ermittlung der maximalen Paketgröße entlang des Pfades vom Server zum Client oder vom Client zum Server oder Anzahl der Hops vom Server zum Client inkl. der Ermittlung der verwendeten autonomen Systeme auf dem Transportweg. Ist dies Bestandteil des proprietären Codes, so sollte hier eine funktionale Beschreibung geliefert werden

- eine zumindest funktionale Beschreibung der Limitierung der maximalen Anzahl an parallelen Sessions um die maximal verfügbare Bandbreite des Netzwerkinterfaces nicht zu überschreiten

- eine zumindest funktionale Beschreibung der CPU Überwachung und Sicherstellung der zeitgerechten Verarbeitung der eingehenden sowie ausgehenden Pakete

d) Auch das auf der Website breitbandmessung.de veröffentlichte Konzept ist als wesentlicher Bestandteil der Wirkweise des Messtools weiter zu konkretisieren und zu vervollständigen, um den Sourcecode gegen diese zu prüfen (siehe diese und vorherige Stellungnahmen).

e) Da dieses Tool beim Kunden installiert wird und Einfallstore zum Rechner öffnet, ist es aus Sicherheits- und Datenschutzgründen unerlässlich, auch eine ausreichende Deinstallations-Routine vorzusehen, die die installierbare Version der Breitbandmessung rückstandslos von den Kundenendgeräten entfernt, wenn nicht bereits von der BNetzA / Zafaco vorgesehen. Auf die durch die Software geöffneten Eingangstore und die damit verbundenen Sicherheitseinbußen sollte der Nutzer in aller Deutlichkeit hingewiesen werden, damit der Endkunde sich über die möglichen Gefahren bei der BNetzA direkt informieren kann und sich nicht auf Aussagen Dritter beziehen muss.

Die zeichnenden Verbände sind sich aus vielen Gesprächen mit den Endkunden der Netzbetreiber bewusst darüber, dass die installierbare Version des Tools gerade vor dem Hintergrund der Ausweitung der Überwachungsmaßnahmen auf bisher nicht überwachte Dienste und der damit verbundenen Diskussion über den Einsatz von Trojanern von vielen Nutzern argwöhnisch betrachtet werden wird. Diese Diskussion wurde zusätzlich über die Entwicklungen rund um die Vorratsdatenspeicherung entfacht. Wir empfehlen daher die vollumfängliche Offenlegung des Codes, inklusive der bislang als proprietär eingestuften Bestandteile sowie dem Code zu den Installations- und Deinstallationsroutinen. Dies sollte im Rahmen eines Open Source Projektes inklusive der Aufforderung an die Open Source Community zur Prüfung des Codes auch hinsichtlich dessen Sicherheit erfolgen. Ein Beispiel für eine solche Vorgehensweise war im Jahr 2015 die Beauftragung des Fraunhofer Instituts für Sichere Informationstechnologie (SIT) durch das BSI zur Durchführung einer Analyse der auch für Verschlusssachen verwendeten Software Truecrypt mit dem Ziel des Auffindens von Schwachstellen und Backdoors. Das Ergebnis dieser Prüfung ist hier zu finden:
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2015/Sicherheitsanalyse_TrueCrypt_19112015.html

Berlin/Bonn/Köln, den 31. August 2017

Über die ANGA Verband Deutscher Kabelnetzbetreiber e.V.:
Die ANGA vertritt die Interessen von mehr als 200 Unternehmen der deutschen Breitbandbranche, darunter Vodafone, Unitymedia, Tele Columbus, NetCologne und wilhelm.tel sowie eine Vielzahl mittelständischer Anbieter. Über 17 Millionen Haushalte in Deutschland nutzen Kabelfernsehen. Die ANGA-Mitglieder versorgen ihre TV-Kunden mit einer wachsenden Zahl von Fernsehprogrammen, Inhalten in HD, Video on Demand und zeitversetztem Fernsehen. Daneben leisten die ANGA-Netzbetreiber den mit Abstand größten Beitrag zur flächendeckenden Verfügbarkeit von hochleistungsfähigem Internet. Schon heute können sie über 70 Prozent der deutschen Haushalte mit schnellem Internet versorgen. Mehr als 7 Mio. Haushalte machen von diesem Angebot Gebrauch.

Über den Bundesverband Glasfaseranschluss e.V. (BUGLAS):
Im BUGLAS sind die Unternehmen zusammengeschlossen, die in Deutschland Glasfaseranschlussnetze direkt bis in Gebäude beziehungsweise Haushalte (Fiber to the Building/ Home, FttB/H) ausrollen und damit zukunftsgerichtete, hochleistungsfähige Kommunikationsnetze mit dedizierten Bandbreiten bis in den Gigabit pro Sekunde-Bereich errichten und betreiben. Die Mitgliedsunternehmen des Verbands zeichnen für 70 Prozent des gesamten und 85 Prozent des bisherigen wettbewerblichen direkten Glasfaserausbaus verantwortlich und sind damit die Treiber bei der Versorgung Deutschlands mit einer nachhaltig leistungsfähigen Kommunikationsinfrastruktur. Der BUGLAS spricht sich für ein Glasfaser-Infrastrukturziel aus und tritt für investitionsfreundliche Rahmenbedingungen ein, in denen FttB/H-Geschäftsmodelle erfolgreich realisiert werden können. Die über 80 Mitgliedsunternehmen haben bis Ende 2016 rund 1,9 Millionen Haushalte und Unternehmen direkt mit Glasfaser angeschlossen. Bis Ende 2018 wollen sie weitere über 650.000 Haushalte und Unternehmen mit FttB/H versorgen.

Über eco - Verband der Internetwirtschaft e.V.:
eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 1000 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet Service Provider-Verband Europas.