Zertifizierter Pinguin

Mit einer Linux-Zertifizierung will die Bundesregierung die Arbeit des BND erleichtern

Mit einer neuen Software-Richtlinie soll eine Zertifizierung für Linux-Systeme kommen. Die Richtlinie ist jedoch unausgegoren und schwammig formuliert. Sie könnte massive Einschränkungen für deutsche Computernutzer bedeuten.

Von Merlin Schumacher

Zu Beginn konnten wir kaum glauben, was am 17. Dezember 2016 in unsere Hände gelangte: Ein Kollege einer großen deutschen Tageszeitung hatte die Redaktion besucht mit einem brisanten Datenpaket aus dem Bundesministerium für Verkehr und digitale Infrastruktur. Er selbst hatte die offensichtlich geleakten Daten-Container auf seinem Windows-Rechner nicht öffnen können – es handelte sich um mehrere Tar-Dateien – und bat nun um Hilfe der c't-Experten. Insgesamt knapp 1400 Dokumente enthielt der Container, der ihm per Briefpost auf einer zweiseitig beschriebenen DVD von einem anonymen Whistleblower zugegangen war: vieles davon interne Mitteilungen, schon beschlossene Gesetze oder bereits Bekanntes. Nur wenige Inhalte waren tatsächlich vertraulich. Die Sichtung des kompletten Unterlagenberges hat mehrere Redakteure wochenlang beschäftigt.

Die Verifikation der Inhalte stellte die Redaktion vor eine schwierige Aufgabe, denn der ursprüngliche Whistleblower verblieb unbekannt. Zweifel an der Aktualität und Echtheit der Dokumente konnten aber ausgeräumt werden, als Mitte Januar die neue Drohnenverordnung[1] publik wurde – die fast finale Fassung der bis dahin nur als Rohfassung bekannten Verordnung hatte sich in dem Leak befunden.

Zwischen vielen Dokumenten zum Thema Verkehr – darunter eine Rohfassung der Regelung zur Haftbarkeit bei der Nutzung von autonomen Fahrzeugen – fand sich ein Wolf im Schafspelz: Hinter dem Codenamen „RASCHER PILZ“ verbarg sich die „Richtlinie zur Zertifizierung quelloffener Systemsoftware“. Sie soll die Arbeit des Bundesnachrichtendienstes vereinfachen und ist offenbar hauptsächlich auf Bestreben des Innenministeriums entstanden. Der Entwurf sieht vor, dass ab Januar 2018 in Deutschland nur noch vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Linux-Distributionen erlaubt sind. Begründet wird der Vorstoß mit dem Hinweis, dass die „übermäßig starke Verschlüsselung und komplexe Bedienung von Linux-Systemen“ oft genug die Arbeit des Bundesnachrichtendienstes vereitle und laut Innenministerium technisch gewieften Gefährdern in die Hände spiele.

Das Dokument spricht in der Fassung vom 4. Januar von nur drei zu zertifizierenden Distributionen: Ubuntu, openSUSE und Red Hat Enterprise Linux. Diese kleine Auswahl erstaunt, da zum Beispiel Debian fehlt – immerhin eine der populärsten Distributionen. Zudem dient es als Basis von Ubuntu. Die eigentliche Zertifizierung soll das BSI übernehmen.

[lkml] [2016] [Nov] [29] [last100] RSS Feed
Views: [wrap][no wrap] [headers] [forward]

Jeanette Fuller
From Jeanette Fuller <>
Subject [PATCH] crypto: certification patch for german government body
Date Tue, 29 Nov 2016 10:37:24 +0100

```
The Patch has an outrageous size. I don't think it's maintainable.
Also please remove the german comments. I don't know what Uberwachung is.
I wouldn't accept it even in staging.

Signed-off-by: Jeanette Fuller <jfuller@larchprizes.com>
---
 drivers/crypto/bsi/ueberwachung/Kconfig | 3 ++-
 1 file changed, 2 insertions(+), 1 deletion(-)
```

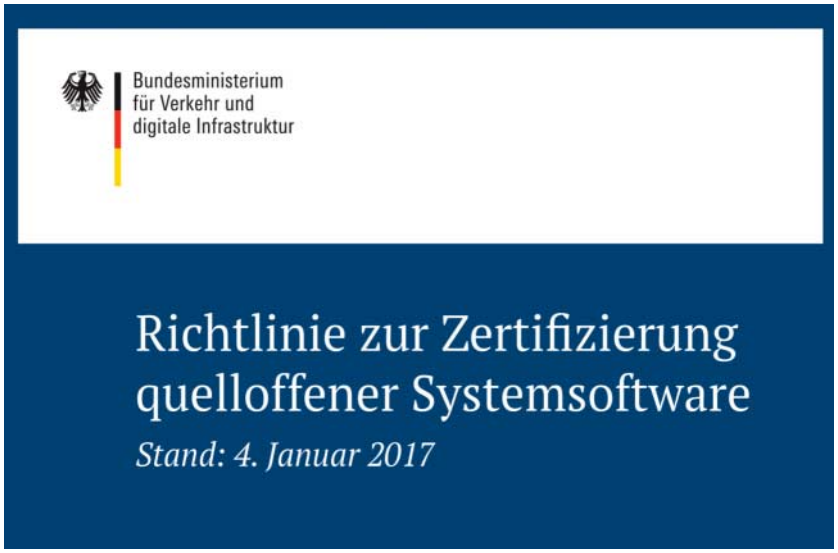
Bereits im November 2016 versuchte der BND einen verdächtigen Patch bei den Linux-Entwicklern einzureichen.

Kernelmodul erforderlich

Das Dokument spricht von einem obligatorischen „nicht quelloffenen Softwaremodul zur Integration in den Betriebssystemkern“. Gemeint ist wohl ein Closed-Source-Kernelmodul. Unter anderem soll das Modul die Entschlüsselung von Laufwerken durch den BND vereinfachen. Zum Einsatz kommen dabei „Schnittstellen, die den Zugriff, im Bedarfsfall über geeignete kryptografische Verfahren gewährleisten“– sprich: Backdoors. Weitere Funktionen, die das Modul implementieren soll, sind Fernüberwachungsfunktionen und das Loggen von Tastatureingaben und IP-Adressen.

Zur Überprüfung laufender Systeme soll eine Website dienen, die dem Nutzer mitteilt, ob auf seinem System das erforderliche Modul läuft. Wie nah die Behör-

den der Fertigstellung sind, zeigt ein bereits gegen Ende November 2016 erfolgter Versuch von Mitarbeitern des BSI, einen undurchsichtigen Kernel-Patch bei den Linux-Entwicklern einzureichen[2]. Er sollte grundlegende Schnittstellen für das Closed-Source-Überwachungsmodul einbringen. Die Kernel-Entwickler lehnten ihn wegen seiner Größe und schlechter Code-Qualität ab. Eine Entwicklerin attestierte dem Patch, dass er unwartbar sei und vermutlich einige Sicherheitslücken enthielt.



Das PDF mit der Richtlinie stammt von Anfang Januar 2017.

Suse und Canonical bereits involviert

Laut Planung sollen Red Hat, Suse und Canonical in Kooperation mit der Bundesregierung erst mal sogenannte DE-Fassungen der zertifizierten Distributionen veröffentlichen. Die Hersteller sollen einen gepatchten Kernel ausliefern, der die geforderten Überwachungsfunktionen bereits enthält. Mit Canonical und Suse gab es wohl bereits Gespräche über die Umsetzung der DE-Fassung. Der Download von nicht zertifizierten Distributions-Images soll dann verboten sein.

Heiß diskutiert ist den Unterlagen zufolge, ob man in einer zweiten Phase eine eigene staatliche Linux-Distribution anbieten wolle. Dieses Bundes-Linux basiert entweder auf Ubuntu oder openSUSE. Bisherige Namensvorschläge wie „Bunduntu“ oder „BUSE-Linux“ wurden verworfen. Die Idee, ein eigenes Bundes-Linux zu entwickeln, stammte aus den Reihen der CSU, die sich Sprachunterstützung für Bairisch gewünscht hatte, welche keine der bisher verfügbaren Distributionen anbietet. Länder wie China oder Nordkorea bieten ihren Bürgern schon länger ein staatliches Linux-System an.

Microsoft macht Lobby

In den Anmerkungen zum Dokument finden sich einige Hinweise auf geführte Gespräche mit Microsoft, das den Unterlagen zufolge seine Software bereits BSI-konform anbietet und den Staat bei seinen Bemühungen unterstützen will. So ist die kürzliche Vorstellung des Linux-Subsystems für Windows 10 vermutlich kein Zufall. Das Subsystem führt typische Linux-Software aus, verwendet aber keinen Linux-Kernel. Das erleichtert Unternehmen den Wechsel zu Windows, die auch nach der Neuregelung auf Linux-Programme angewiesen sind. Ebenso passt die Eröffnung von Microsofts Deutschland-Cloud gut zur Stoßrichtung des Gesetzes.

Wie die Stadtverwaltung München gegenüber heise online bestätigte, hängt das Ende des LiMux-Projekts auch mit einer „zukünftigen Software-Richtlinie des Bundes“ zusammen. Ob es sich um genau diese Richtlinie handelt, bestätigte man jedoch nicht. In Zukunft wolle man sich „aufgrund des geringeren rechtlichen Risikos […] voll und ganz auf Microsoft-Dienste verlassen“.

Durchsetzung diffus

Wie die Bundesregierung das Gesetz durchsetzen will, ist schwer zu sagen. Wer den Download von nicht zertifizierten Linux-Distributionen per Gesetz verhindert, produziert einen Papiertiger: Für jeden halbwegs begabten Anwender stellt die Nutzung eines VPN zur Umgehung von Sperren kein Problem dar.

Ebenfalls ist nicht klar, wie mit bestehender Soft- und Hardware umzugehen ist. In der Theorie müsste die Regierung jeden zwingen, seine Linux-Distribution durch eine zertifizierte zu ersetzen. Zudem bleibt offen, wie die Regelung etwa mit BSD- und anderen Open-Source-Systemen oder alternativen Kerneln wie GNU/Hurd umgeht. Bei Routern und IoT-Geräten ist ebenfalls unklar, wie Anwender diese noch rechtskonform einsetzen können. Dass die Hersteller Firmware-Updates bereitstellen, die für Konformität sorgen, dürfte eher die Ausnahme sein. Einzig Bosch-Siemens-Hausgeräte will dank „remote flashbarer Elektronik“ direkt nach Erlass der Richtlinie alle smarten Haushaltsgeräte rechtlich absichern. Im schlimmsten Fall werden Millionen Tonnen Hardware-Schrott produziert.

Ein großes Fragezeichen bleibt bei Servern. Dort wird Linux primär eingesetzt und ist damit ein essenzieller Bestandteil moderner Web-Dienste. Alle Linux-Server auf deutschem Boden neu zu installieren oder mit dem Kernelmodul zu versehen, wäre eine Aufgabe, die Unternehmen Jahre und Millionen kosten kann. Wie es scheint, arbeitet man inzwischen mit Intel an einer Lösung, die auf der oft kritisierten Fernwartungstechnik ME (Management Engine) basiert.

Unausgegoren, aber bedrohlich

Wie so oft bei IT-Projekten des Bundes erstaunt die technische Unzulänglichkeit des Gesetzes. Dass viele Geräteklassen wie etwa Router auf dem Linux-Kernel basieren, lässt das Dokument außen vor. Die Wahrnehmung beschränkt sich primär auf die Nutzung als Desktop-Betriebssystem. Überraschend ist auch, dass Android nicht im Fokus des Gesetzes steht – sofern die Behörden diese Versorgungslücke nicht schon vorher geschlossen haben, stünden sie bei Mobilgeräten von Google weiterhin blind da. *(mls@ct.de)* c't

Literatur

[1] Axel Kannenberg, Kennzeichen und Kenntnisnachweis: Neue Pflichten für Drohnenpiloten kommen, https://heise.de/-3601385
[2] Thorsten Leemhuis, Kernel-Log, Linux 4.10: Rucklervermeidung und RAID-Cache, c't 5/17, S. 38

Bildschirmhintergrund Bunduntu 17.10 Wilder Wolpertinger: ct.de/yy2d