Leitstelle511

Chaos Computer Club Hannover e. V.

c/o Stadtteilzentrum Nordstadt/Bürgerschule
Klaus-Müller-Kilian-Weg 2
30167 Hannover
kontakt@hannover.ccc.de

S T E L L U N G N A H M E

zum Antrag „‚Staatstrojaner' stoppen"

Drs. 16/4175 der Fraktion DIE LINKE im niedersächsischen Landtag
(Ausschuß Inneres und Sport)

Hannover, den 25. Januar 2012

Sehr geehrter Herr Kleinwächter,
sehr geehrte Damen und Herren Abgeordnete,

gerne kommen wir Ihrer Bitte um eine Stellungnahme zum Antrag „‚Staatstrojaner' stoppen" (Drs. 16/4175) der Fraktion DIE LINKE nach.

Wir begrüßen jede Diskussion der Staatstrojaner-Thematik im niedersächsischen Landtag. Dabei sehen wir es als erforderlich an, daß eine Diskussion der technischen Hintergründe auf Basis der aktuellen verfassungsrechtlichen Lage stattfindet.

Im Grundsatz basieren unsere Ausführungen auf den bereits durch den Chaos Computer Club veröffentlichten Pressemitteilungen ([1], [2]) sowie dem technischen Analysereport [3].

Für weitere Informationen und Fragen stehen wir Ihnen natürlich gerne zur Verfügung.

Falk Garbsch

Leitstelle511 – Chaos Computer Club Hannover e. V.

Einleitung

Seit dem Beginn des 21. Jahrhunderts entwickeln sich Computer zusehends zu Medien des sozialen Zusammenlebens und damit auch des Austausches von persönlichen Informationen und Daten. Computer werden zunehmend als Ablagemedium privatester und intimster Gedanken genutzt. Vor allem in jüngeren Bevölkerungsgruppen nehmen Computersysteme weniger den Stellenwert eines „Arbeitsgerätes“ ein, sondern entwickeln sich zu einem Instrument zur Auslebung der eigenen Persönlichkeit.

Daher ist es unumgänglich, sowohl auf technischer als auch ethischer Ebene zu diskutieren. Die Diskussion muß sich mit den Gefahren befassen, welche sich durch Eingriffe und Manipulationen in ebendiese privaten Systeme ergeben. Dabei sollte nicht zuletzt die Frage im Fokus stehen, wie weit eine Überwachung und das Ausspähen privatester, persönlichster Daten und Informationen gehen darf und vor welcher Grenze eine solche Überwachung Halt machen muß.

Genau aus diesem Grund hat das Bundesverfassungsgericht in seinem Urteil zur Online-Durchsuchung zur „Quellentelekommunikationsüberwachung“ („Quellen-TKÜ)“ [4] auch festgesetzt, daß „[d]as Gesetz, das zu [der heimlichen Infiltration eines informationstechnischen Systems] ermächtigt, [...] Vorkehrungen enthalten [muß], um den Kernbereich privater Lebensgestaltung zu schützen.“

Die Forderungen im Antrag der Partei DIE LINKE sind im wesentlichen deckungsgleich mit den Forderungen des Chaos Computer Clubs. Die Software der Firma DigiTask hat sich durch die Analysen als unbrauchbar herausgestellt. Eine Verwendung dieser oder einer ähnlichen Software darf unter keinen Umständen weitergeführt werden. Wir bezweifeln, daß es überhaupt möglich ist, die Telekommunikation auf diese Art und Weise verfassungskonform zu überwachen. Bei der Überwachung von Telekommunikation ist zudem jederzeit die Verhältnismäßigkeit zu wahren. Dabei sind zunächst alle Alternativen, die mit deutlich weniger Eingriffen in die Grundrechte auskommen, auszuschöpfen. Beispielsweise könnte das Abhören der Verbindung bei den Anbietern erfolgen, also etwa direkt bei Skype.

Technische Beurteilung des Trojaners

Die Analyse des Behörden-Trojaners weist Funktionen nach, die über das Abhören von Kommunikation weit hinausgehen und die explizite Vorgaben des Verfassungsgerichtes verletzen. So kann der Trojaner über das Netz weitere Programme nachladen und ferngesteuert zur Ausführung bringen.

Es ist nicht einmal versucht worden, softwaretechnisch sicherzustellen, daß die Erfassung von Daten strikt auf die Telekommunikation beschränkt bleibt. Eine Erweiterung der Funktionalität der Computerwanze wurde von vornherein vorgesehen. Dieser Vollzugriff auf den Rechner – auch durch

unautorisierte Dritte – kann etwa zum Hinterlegen gefälschten, belastenden Materials oder Löschen von Dateien benutzt werden.

Es ist jedoch festzuhalten, daß schon die vorkonfigurierten Funktionen des Trojaners ohne nachgeladene Programme besorgniserregend sind. Im Rahmen des Tests hat der CCC eine Gegenstelle für den Trojaner programmiert, mit deren Hilfe Inhalte des Webbrowsers per Bildschirmfoto ausspioniert werden konnten – inklusive privater Notizen, E-Mails oder Texten in webbasierten Cloud-Diensten. Die von den Behörden suggerierte strikte Trennung von genehmigt abhörbarer Telekommunikation und der zu schützenden digitalen Intimsphäre existiert in der Praxis nicht.

Die Analyse offenbarte ferner gravierende Sicherheitslücken, die der Trojaner in infiltrierte Systeme reißt. Die ausgeleiteten Bildschirmfotos und Audio-Daten sind auf inkompetente Art und Weise verschlüsselt, die Kommandos von der Steuersoftware an den Trojaner sind gar vollständig unverschlüsselt. Weder die Kommandos an den Trojaner noch dessen Antworten sind durch irgendeine Form der Authentifizierung oder auch nur Integritätssicherung geschützt. So sind nicht nur unbefugte Dritte in der Lage, den Trojaner fernzusteuern, sondern bereits nur mäßig begabte Angreifer können sich den Behörden gegenüber als eine bestimmte Instanz des Trojaners ausgeben und gefälschte Daten abliefern.

Diese „Quellen-TKÜ“ sollte ausschließlich für das Abhören von Internettelefonie verwendet werden. Dies wäre durch technische und rechtliche Maßnahmen sicherzustellen gewesen. Alternativen zu diesem massiven Grundrechtseingriffen sind vorhanden.

Skype stellt offensichtlich seit 2009 Schnittstellen zum Abhören von VoIP-Verbindungen zur Verfügung [5]. Eine solche Maßnahme wäre deutlich weniger grundrechteinschränkend als die „Quellen-TKÜ“ mittels der von der Firma DigiTask zur Verfügung gestellten Software. Skype schreibt in den Datenschutzrichtlinien [6]: „Skype, der örtliche Skype-Partner oder der Betreiber bzw. Anbieter, der die Kommunikation ermöglicht, stellt personenbezogene Daten, Kommunikationsinhalte oder Verkehrsdaten Justiz-, Strafvollzugs- oder Regierungsbehörden zur Verfügung, die derartige Informationen rechtmäßig anfordern. Skype wird zur Erfüllung dieser Anforderung angemessene Unterstützung und Informationen bereitstellen, und Sie stimmen hiermit einer derartigen Offenlegung zu.“

Nach eingehender Untersuchung des dem CCC zugespielten Staatstrojaners kamen wir zu dem Ergebnis, daß er nicht den rechtlichen Grundlagen entspricht und dessen Einsatz auch in keiner Weise verhältnismäßig und verfassungskonform ist. Darüber hinaus haben wir schwerwiegende Bedenken bezüglich erneuter Pläne, Schadsoftware dieser Art einzusetzen oder zu entwickeln.

Technisch gesehen ist allerdings ein Nachweis nicht möglich, daß eine Software ausschließlich den gestellten Anforderungen an eine verfassungskonforme „Quellen-TKÜ“ entspricht. Wie wir aber gezeigt haben, ist es sehr

wohl möglich nachzuweisen, daß eine Software Funktionen enthält, die nicht verfassungskonform sind.

Daß trotz dieser schwerwiegenden Mängel der Trojaner mehrfach zum Einsatz kam, zeigt, daß es an verläßlichen Prüfungsmechanismen für die Gewährleistung der Einhaltung verfassungsrechtlicher Grundnormen fehlt. Die an Entwicklung und Einsatz des Staatstrojaners beteiligten Behörden haben ihre Informationspflicht gegenüber den demokratischen Kontrollorganen nicht erfüllt. Um dies zukünftig zu verhindern, muß sichergestellt werden, daß Kontrollorgane frühzeitig eingreifen können. Es erweckt bisher auch den Eindruck, als ob die beteiligten Politiker und Kriminalbeamten die Problematik nicht verstehen. Für uns zeigt dies, daß eine weitere Beschäftigung mit der Thematik sowie geeignete Fortbildung der Beteiligten dringend erforderlich ist. Der Chaos Computer Club unterstützt daher den niedersächsischen Landtag gern mit seiner Expertise in dieser Sachfrage.

Der Einsatz dieser Schadsoftware stellt einen unverhältnismäßigen Eingriff in das Persönlichkeitsrecht der Bürgerinnen und Bürger dar. Eine vollständige Aufklärung der Umstände, die zu Entwicklung und Einsatz einer verfassungsrechtlich in keiner Weise abgedeckten Überwachungssoftware geführt haben, ist aus Sicht des Chaos Computer Clubs daher zwingend notwendig.

Nach Berücksichtigung der grundrechtlichen Maßgaben hätte der Trojaner niemals zum Einsatz kommen dürfen, da er gegen geltendes Recht verstößt und zudem die erlangten Daten aus technischer Sicht keine Beweiskraft haben.

Der CCC fordert daher:

> Kein weiterer Einsatz der Trojaner durch Strafverfolgungsbehörden,
>
> Sofortige Offenlegung der Quellcodes und aller Prüfprotokolle über vergangene Einsätze von Trojanern durch deutsche Ermittlungsbehörden,
>
> Zukünftige automatische Offenlegung von Quellcode, Binary und Protokollen des Trojaners nach jedem Einsatz.

Bei einer staatlichen Infiltration eines Rechners muß unwiderruflich die Möglichkeit erlöschen, Daten des infiltrierten Systems gerichtlich zu verwerten, insbesondere auch solche Daten, die sich auf der Festplatte des Systems befinden.

Bei der Überwachung von Telekommunikation ist der Grundsatz der Verhältnismäßigkeit zu wahren. So sind für eine Telekommunikationsüberwachung jederzeit diejenigen Verfahren zu wählen, welche den geringsten Eingriff in die Grundrechte darstellen. Zusammenfassend stimmen wir den Forderungen des Antrags der LINKEN zu:

1. Ein weiterer Einsatz von Software, bei der die Verfassungskonformität nicht gewährleistet ist, darf nicht stattfinden.
2. Der Landtag hat die Öffentlichkeit umfänglich und lückenlos darüber aufzuklären, wie, in welchem Umfang, in welcher Form und auf welcher gesetzlichen Grundlage der Einsatz von Quellen-TKÜ angeordnet und durchgeführt wurde.
3. Es ist darzulegen, wie eine Entwicklung einer verfassungskonformen Software für die Quellen-TKÜ erfolgen, wie diese überprüft und verifiziert werden soll.

Links:

[1] http://www.ccc.de/de/updates/2011/staatstrojaner

[2] http://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner

[3] http://www.ccc.de/system/uploads/76/original/staatstrojaner-report23.pdf

[4] http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

[5] http://www.eurojust.europa.eu/press_releases/2009/25-02-2009.htm

[6] http://www.skype.com/intl/de/legal/privacy/general/#8