Die politische Aufarbeitung des jüngst entdeckten Staatstrojaners lässt die Öffentlichkeit in einen Abgrund aus Fahrlässigkeit, Inkompetenz und Ignoranz gegenüber der Verfassung blicken. Was eigentlich ein großer Skandal sein sollte, droht jedoch im technischen Kleinklein unterzugehen. Nicht nur die Politik und die Sicherheitsbehörden haben Defizite beim Verständnis der Risiken moderner Informationstechnologie, auch die meisten Journalisten und Bürger sind sich deren Tragweite nicht bewusst. Von Jens Berger

In Deutschland kommt es pro Jahr rund 16.000 mal vor, dass eine Genehmigung zur Telekommunikationsüberwachung erteilt wird. Das Grundgesetz schützt zwar das Fernmeldegeheimnis, sieht jedoch explizit Ausnahmen vor, bei denen der Staat dieses Grundrecht aushebeln darf. Zwischen den Ermittlungsbehörden und dem Bürger steht in diesem Falle lediglich ein Richter, der die Maßnahmen absegnen muss. Wie die Zahlen zeigen, ist die Überwachung von Telefongesprächen mittlerweile in der Strafverfolgung eine gängige Praxis. Natürlich nutzen Personen, die im Fokus strafrechtlicher Ermittlungen stehen, auch moderne Kommunikationstechniken, wie beispielsweise die Möglichkeit, Gespräche über das Internet zu führen. Dies stellt die Behörden vor technische Probleme, da es nach bisherigen Erkenntnissen nicht möglich ist, Gespräche, die über eine VOIP-Software wie beispielsweise Skype geführt werden, „im Netz“ abzuhören, da die Datenpakete verschlüsselt übertragen werden.

Quellen-TKÜ

Um Telefonate, die über den Computer geführt werden, abhören zu können, sind daher Maßnahmen notwendig, um das Gespräch am Computer des Verdächtigen mitschneiden zu können – also zu einem Zeitpunkt vor der Verschlüsselung durch die VOIP-Software. Diese sogenannte Quellen-TKÜ (Telekommunikationsüberwachung) ist jedoch rechtlich heikel, da sichergestellt werden muss, dass ausschließlich die Kommunikation aufgezeichnet wird, die der Verdächtige über VOIP-Software tätigt. Ein simples „Anzapfen“ des Mikrophons am betreffenden Rechner ist nicht gestattet, da auf diese Art und Weise auch persönliche Gespräche mitgeschnitten werden können, die nicht den Charakter der Telekommunikation haben und zum verfassungsrechtlich besonders geschützten Kernbereich der privaten Lebensgestaltung zählen. Eine Quellen-TKÜ, die diesen strengen Anforderungen nicht genügt, wäre eine Überwachungsmaßnahme, die analog zur Wohnraumüberwachung zu sehen ist, vor die das Bundesverfassungsgericht weitaus größere Hürden gesetzt hat.

Um den Behörden die Quellen-TKÜ zu ermöglichen und gleichzeitig die Grundrechte der Verdächtigen zu schützen, hat das Bundesverfassungsgericht technische Richtlinien formuliert, nach denen Software, die zur Quellen-TKÜ eingesetzt werden darf, ausschließlich die Telekommunikationsinhalte übertragen darf, die vergleichbar zu

herkömmlichen Telefongesprächen sind. Diese Software gelangt ohne Wissen des Verdächtigen auf seinen Rechner und ist in ihrer Arbeitsweise vergleichbar mit einem sogenannten „Trojaner“ – daher ist in der Presse auch meist von einem „Staatstrojaner“ die Rede, wenn es um Software zur Quellen-TKÜ geht. Es ist kein großes Geheimnis, dass diese Software von den Landes- und Bundesbehörden bereits eingesetzt wird, jedoch war bis vor kurzem unbekannt, welche Software die Behörden einsetzen.

Der Fund des CCC

Dies änderte sich erst, als dem Chaos Computerclub (CCC) vom Anwalt eines Verdächtigen, auf dessen Rechner das bayerische LKA eine Quellen-TKÜ-Software geschleust hatte, die Festplatte seines Mandaten zur Analyse übergeben wurde. Wie der CCC herausfand, war die eingesetzte Software wesentlich mächtiger als die Richtlinien des Bundesverfassungsgerichts hergeben. So kann die analysierte Variante des Staatstrojaners beispielsweise Photographien vom Bildschirminhalt anfertigen [PDF – 11.7 MB]. Diese Funktion ist jedoch vergleichbar mit einer herkömmlichen Videoüberwachung im nicht-öffentlichen Raum, die jedoch immer noch verboten ist. Ebenfalls unvereinbar mit den Vorgaben des Bundesverfassungsgerichts ist die Möglichkeit, den Trojaner bei Bedarf online mit zusätzlichen Modulen zu bestücken – so könnten die Überwacher beispielsweise über ein Videomodul auf die in einem Laptop eingebaute Kamera zurückgreifen, mit einem Dateienmodul könnten sie nach Belieben die Inhalte der Festplatten auslesen und modifizieren. Letzteres wäre ein Element der „Online-Durchsuchung“, die zwar ebenfalls vom Bundesverfassungsgericht gestattet ist, die aber – analog zur Wohnraumüberwachung – an sehr rigide Auflagen gebunden ist.

Ermittlungsunterlagen aus dem Umfeld des Trojanereinsatzes, der vom CCC analysiert wurde, beweisen, dass die bayerischen Behörden von den verfassungsrechtlich verbotenen Funktionen des Trojaners regen Gebrauch gemacht haben – und dies wohlgemerkt gegen die expliziten Einschränkungen, die der genehmigende Amtsrichter erteilt hatte [PDF – 723 KB]. Die Praxis zeigt, dass Möglichkeiten, die vorhanden aber rechtlich untersagt sind, von den Ermittlungsbehörden dennoch genutzt werden – ob der Verfassungsbruch dabei vorsätzlich oder fahrlässig aufgrund mangelnder Rechtskenntnisse erfolgte, ist dabei unerheblich.

Wie der Antivirensoftware-Hersteller Kaspersky Labs gestern mitteilte, existiert neben dem vom CCC untersuchten Trojaner, der offenbar ein älteres Exemplar ist, auch eine modernere, noch leistungsfähigere Variante des Staatstrojaners, die auch auf aktuellen Systemen zum Einsatz kommen kann.

Offenbarungseid der Politik

Die einzige Möglichkeit, die verfassungsrechtlichen Einschränkungen sinnvoll umzusetzen, ist es, die Trojaner so zu programmieren, dass sie erst gar keine Daten weiterleiten können, die einen gesonderten verfassungsrechtlichen Schutz genießen. Zahlreiche Experten sind der Meinung, dass dies überhaupt nicht möglich sei. Wenn dem so sein sollte, dann kann die Antwort darauf nur der komplette Verzicht auf eine Quellen-TKÜ sein. Auch der nun angekündigte Vorstoß, künftige Versionen des Trojaners selbst zu entwickeln, kann hier nicht überzeugen. Wie soll der Staat, der heute noch nicht einmal das Know how hat, den Quellcode eines Staatstrojaners zu lesen, morgen ein eigenes Programm entwickeln?

Noch erschreckender als der Einsatz des Trojaners selbst ist jedoch die Reaktion der beteiligten Politiker und Beamten. Wie sich in der aktuellen Fragestunde des Bundestages am Mittwoch herausstellte, hatten die Behörden offenbar keinen blassen Schimmer, was ihr Staatstrojaner alles kann. Der aktuelle Trojaner stammt wahrscheinlich aus einem Auftrag, den das Zollkriminalamt in Köln für mehr als zwei Millionen Euro an die Firma Digitask vergeben hat. Was Digitask den Behörden geliefert hat, war jedoch – wenn man den Behörden glauben darf – eine Art Black Box, bei der die Ermittler sich nur dafür interessierten, was als verwertbares Ergebnis auf ihrem Schreibtisch landete. Sie hatten – nach eigenen Angaben – nie Einblick in den Quellcode des Trojaners und haben sich bei der Abnahme auf eine Funktionsüberprüfung verlassen. Eine solche Überprüfung ist jedoch keinesfalls ausreichend, wenn es um derart verfassungsrechtlich sensible Zusammenhänge geht.

Sollte die Schilderung der Behörden der Wahrheit entsprechen, können sie überhaupt keine Angaben machen, ob die von ihnen eingesetzte Software korrekt funktioniert. Sie können auch gar nicht wissen, ob sie verfassungskonform ist. Um dies beurteilen zu können, müssen sie die „Schaltpläne“ der Software kennen – sie müssen also den Quellcode analysieren.

Dies hörte sich in den Werbekampagnen des BKAs ganz anders an. 2007 stellte BKA-Präsident Ziercke sogar in Aussicht, den Quellcode des Trojaners den Gerichten und dem CCC zur Verfügung zu stellen. In der Realität kennt noch nicht einmal das BKA den Quellcode. Dies ist nicht nur intransparent und ein Verstoß gegen die Auflagen des Bundesverfassungsgerichts, sondern auch brandgefährlich. Nicht nur die Behörden, sondern jeder Hacker, der Zugriff auf den Trojaner hat, kann ihn nach eigenem Gusto fernsteuern. Es ist sogar möglich, dass sich Dritte zwischen den Verdächtigen und die Behörden schalten und die abgefangen Daten manipulieren. Dass diese Gefahr nicht nur theoretisch besteht, belegen die Analysen vom CCC und verschiedenen Antivirensoftware-

Herstellern, die dem Staatstrojaner von Digitask eine miserable Sicherheit attestieren.

Eigentlich sollte eine solche Serie von Pleiten, Pech und Pannen die Behörden und die Politik wachrütteln. Das Gegenteil ist jedoch der Fall. Sowohl der bayerische Innenminister Herrmann als auch der Bundesinnenminister Friedrich (beide CSU) sind sich weder einer Schuld noch eines Fehlers bewusst und lassen jegliche Kritik an sich abperlen. Friedrich besaß sogar die Dreistigkeit, gar nicht erst zur aktuellen Stunde im Bundestag zu erscheinen. Auch die Unionsfraktion spielt den Skandal lieber herunter und beweist damit nicht nur, dass sie sich um die technischen Einzelheiten nicht schert, sondern auch, dass sie die Vorgaben des Bundesverfassungsgerichts nicht interessiert. Niemand verlangt, dass die Politik auf jedem Gebiet hochqualifizierte Fachleute besitzt. Es ist jedoch beileibe kein Ruhmesblatt für den Parlamentarismus, wenn selbst die auserkorenen Fachleute der Regierungsparteien CDU und CSU noch nicht einmal eine Grundkompetenz in den Technologien besitzen, die heute bereits das wirtschaftliche Rückgrat unseres Landes bilden. Dabei ist noch nicht einmal die Absicht zu erkennen, sich auf diesem Feld weiterzubilden. Wie kann es sein, dass selbst ein parlamentarischer Staatssekretär im Innenministerium, wie Ole Schröder (CDU), offenbar ungebrieft und komplett ahnungslos in eine aktuelle Fragestunde des Bundestages geht und dabei allenfalls zum Fremdschämen einlädt? Nicht nur die Inkompetenz, sondern mehr noch die gezeigte Ignoranz ist bemerkenswert.

Ginge es im konkreten Fall nicht um Informationstechnologie, sondern um etwas „Greifbares“, wären Herrmann, Friedrich und auch Ziercke wahrscheinlich längst nicht mehr im Amt. Die Gefahren der modernen Technologien für unsere verfassungsrechtlich garantierten Freiheiten sind jedoch nicht nur für Politiker und Spitzenbeamte, sondern auch für die Medien oft ein Buch mit sieben Siegeln. Einzig und allein die FAZ glänzt hier mit einer sehr lobenswerten Berichterstattung [PDF – 11.7 MB], während der Rest der Medien dem Thema entweder hinterherläuft oder es offensichtlich für weniger relevant hält. Es ist dabei schon bezeichnend, dass die Opposition im Bundestag den Verantwortlichen kritischere und vor allem fachkundigere Fragen stellte als die versammelte Journalistenschar.

Je geringer der Wissensstand über moderne informationstechnologische Fragen ist, desto größer ist die Gefahr, dass politische Hardliner unsere Grundrechte auf diesem Gebiet aushebeln. Von der noch größeren Bedrohung dieser Grundrechte seitens der Privatwirtschaft ist hierbei noch nicht einmal die Rede.