in: Forschung & Lehre 8 (2013) 614-616
http://www.forschung-und-lehre.de/wordpress/?p=13961

# Computerüberwachung

## Methoden und Möglichkeiten

Hannes Federrath

*Die US-amerikanische NSA mit dem Überwachungsprogramm PRISM und auch der britische Nachrichtendienst mit einem Spionageprogramm namens Tempora spähen die Kommunikation von europäischen Staaten und Bürgern aus. Mit welchen technischen Methoden tun sie dies? Wie werten sie die ausgespähten Daten aus?*

Die National Security Agency (NSA) gilt zurecht als einer der mächtigsten Nachrichtendienste der Welt. Bereits vor mehr als 25 Jahren wurde mit Unterstützung seiner Verbündeten globale Überwachung betrieben. Das Satellitenüberwachungssystem Echelon wurde von der westlichen UKUSA-Alliance betrieben und lieferte seit etwa 1970 Informationen über die Lage im Ostblock. Obwohl Deutschland der UKUSA-Alliance nicht angehörte, wurde auch von deutschem Boden aus abgehört. Die inzwischen stillgelegte Bodenstation in Bad Aibling zeugt davon.

Zwölf Jahre nach dem Mauerfall beschäftigte sich das EU-Parlament mit Echelon und stellte in seinem „Bericht über die Existenz eines globalen Abhörsystems“ (AZ: A5-0264/2001) fest, „. . . dass nunmehr kein Zweifel mehr daran bestehen kann, dass das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, . . . “. Interessant an dem Bericht des EU-Parlaments ist, dass man damals vor zwölf Jahren feststellte, „. . . dass die technischen Kapazitäten dieses Systems wahrscheinlich bei Weitem nicht so umfangreich sind, wie von den Medien teilweise angenommen“ (http://tinyurl.com/A5-0264).

Allerdings stellte bereits 2001 die stellvertretende Vorsitzende des Echelon-Untersuchungsausschusses im EU-Parlament Ellie Plooij (Niederlande) fest: „Geheimdiensten sind, was das Abhören betrifft, durch nationale Gesetze Grenzen gesetzt. Es gibt aber keine Regeln für grenzüberschreitendes Abhören. Das ist ein großer Mangel beim Schutz der internationalen Kommunikation. Wir müssen diesbezüglich internationale Abkommen schließen, zunächst innerhalb der EU, dann in größerem, internationalem Rahmen“ (http://tinyurl.com/Plooij).

## Neue technische Möglichkeiten

Die Größenordnungen, in denen die NSA auch deutsche Kommunikationsverbindungen überwachen soll – hier ist die Rede von bis zu 500 Millionen Datensätzen pro Monat – zeigen, dass die heutigen technischen Möglichkeiten in vollem Umfang genutzt werden (http://tinyurl.com/xkeyscore).

Für den Überwacher stellen sich dabei zwei Probleme. So muss er erstens zur Datengewinnung nah genug an die für ihn relevanten Kommunikationsverbindungen kommen. Dann

kann er sowohl Verbindungsdaten, d.h. wer wann und ggf. von wo aus mit welchen Kommunikationspartnern wie lange kommuniziert hat, als auch die Inhaltsdaten der Kommunikation mitlesen. Während die Verbindungsdaten nur wenige hundert bis tausend Byte umfassen und damit im vollen Umfang alle Verbindungsdaten aller Nutzer für immer gespeichert werden können, ist die Speicherung aller Inhaltsdaten aller Kommunikationsverbindungen weder möglich noch sinnvoll, auch wenn teilweise in den Medien (http://tinyurl.com/BildPRISM) berichtet wurde, die NSA speichere alle Inhaltsdaten für wenigstens drei bis sechs Monate. Dementsprechend erfolgt zweitens eine Datenfilterung in Echtzeit: Die für den Überwacher interessanten Inhaltsdaten werden aus den gigantischen Datenströmen z.B. anhand von Schlüsselwortlisten, nach Sender- und Empfängeradressen, genutzten Diensten (E-Mail, Chat, aufgerufene Webseiten) herausgesucht und gespeichert.

Eigentlich ist die Verschlüsselung und damit der Schutz sensibler Inhaltsdaten inzwischen technisch recht einfach lösbar, zumindest bei der E-Mail-Kommunikation. Voraussetzung ist, dass sich die Kommunikationspartner vorher auf ein Verfahren wie S/MIME oder GnuPG einigen und kryptographische Schlüssel miteinander austauschen. S/MIME ist bereits in den meisten E-Mail-Programmen enthalten, allerdings haben private Nutzer meist Probleme beim Erzeugen und beim Austausch der Schlüssel. Beim GnuPG-Verfahren muss zusätzliche Software auf dem Rechner installiert werden, dafür ist die Schlüsselerzeugung unkomplizierter als bei S/MIME. Auch das verschlüsselte Websurfen gelingt inzwischen problemlos: HTTPS ist wie S/MIME oder GnuPG Ende-zu-Ende-verschlüsselt, d.h. niemand kann auf den Leitungen oder den Routern mitlesen.

Während Inhaltsdaten durch Ende-zu-Ende-Verschlüsselung (sofern sie eingesetzt wird) heute gut geschützt werden können, gelingt der Schutz der Verbindungsdaten nicht annähernd so gut. Zwar ist es technisch möglich, alle Kommunikationsleitungen und Funkstrecken komplett zu verschlüsseln, also sowohl Inhaltsdaten als auch Verbindungsdaten vor Außenstehenden zu schützen; damit wäre eine Überwachung der Kommunikationsleitungen für einen Nachrichtendienst eigentlich wenig gewinnbringend. In der Praxis werden jedoch aus Unvorsichtigkeit noch immer genügend viele Inhalts- und Verbindungsdaten unverschlüsselt übertragen und stehen somit auch Außenstehenden zur Verfügung (http://tinyurl.com/TAT14).

Alle Router zwischen den Kommunikationspartnern benötigen für ihre Funktion die unverschlüsselten Verbindungsdaten (Adressen). Hier setzt das heute bekannte Überwachungsszenario von Nachrichtendiensten an: Neben der Überwachung der Kommunikationsverbindungen von außen, wie sie bereits bei Echelon praktiziert wurde, werden mit Wissen und Unterstützung der Netzbetreiber auch Daten innerhalb der Kommunikationsnetze erhoben und gespeichert. Hierzu laufen auf den Routern und Servern des Netzbetreibers sog. Sniffer-Programme, die alle Verbindungsdaten speichern und die o.a. Datenfilterung vornehmen.

Der Einsatz von Sniffer-Programmen durch sog. Bedarfsträger (Sicherheitsbehörden und Strafverfolger) wird ebenfalls schon seit vielen Jahren praktiziert. In Deutschland kann ein Richter auf der Grundlage der §§ 100a,b der Strafprozessordnung (StPO) die zeitlich begrenzte Überwachung der Telekommunikation eines Anschlusses anordnen. Im Internetzeitalter betrifft dies natürlich neben dem (Mobil)-Telefon auch die gesamte Internetkommunikation. In Deutschland werden z.B. sog. SINA-Boxen zur Überwachung eingesetzt. Bei den großen Internet Service Providern administriert und konfiguriert teilweise von staatlichen Stellen abgeordnetes Personal diese Geräte direkt vor Ort.

In den USA wurde wenigstens bis 2001 bei der Überwachung mit dem sog. Carnivore-System gearbeitet, zudem kam auch kommerzielle Software zum Einsatz (http://tinyurl.com/bu34sht).

Spezielle technische Vorkehrungen zur Überwachung müssen vom Netzbetreiber heute kaum noch getroffen werden. Die Betriebssysteme von Servern und Routern verfügen von jeher über technische Protokollierungs- und Überwachungsfunktionen zur Fehleranalyse. Mit den staatlichen Überwachungsanforderungen wurden außerdem internationale technische Schnittstellendefinitionen geschaffen, die von den Netzbetreibern umzusetzen sind; andernfalls erhalten diese keine Netzbetreiber-Lizenz (http://tinyurl.com/k65ys4g).

Da die heute verfügbaren Hacker-Tools im Internet nicht nur kostenlos, sondern auch sehr leistungsfähig sind, werden sie vermutlich auch von Sicherheitsbehörden eingesetzt. Allerdings ist es extrem unwahrscheinlich, dass eine Überwachung von deutschen Kommunikationsverbindungen und bei deutschen Netzbetreibern durch (ausländische) Sicherheitsbehörden im großen Stil ohne deren Wissen und mit Hackermethoden erfolgt, d.h. durch unbemerktes Eindringen in die Server und Router des Netzbetreibers: Die Ausleitung der überwachten Daten zum Bedarfsträger verursacht erkennbare Netzlast, die jedes Frühwarnsystem (Intrusion Detection) melden würde. Außerdem erfordert eine effektive Überwachung die fortlaufende Nachsteuerung der Datenfilterung.

### Grenzen der Überwachung

Obwohl nach den Enthüllungen der geheimen NSA-Spähprogramme der Eindruck entstehen mag, staatliche Stellen könnten heute uneingeschränkt jede Kommunikation weltweit mitlesen, sind die Möglichkeiten der konkreten Strafverfolgung teilweise erschreckend gering. Dies hat zwei Ursachen:

Erstens sammeln die Überwachungsprogramme Daten massenhaft verdachtsunabhängig, aber eben auch unspezifisch. So wurden beispielsweise auch in Deutschland legal und für kurze Zeit auf der Grundlage der EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung für sechs Monate alle Verbindungsdaten von Nutzern gespeichert. Nachdem das Bundesverfassungsgericht im Jahr 2010 die Umsetzung der Vorratsdatenspeicherung für verfassungswidrig erklärt hatte, wurde deren Wirkung auf die Strafverfolgung wissenschaftlich untersucht und festgestellt, dass sie keinen messbaren Einfluss auf die Aufklärungsquoten von Straftaten hat (http://tinyurl.com/73a7oxn).

Zweitens können sich Straftäter ebenso wie unbescholtene Bürger der Totalüberwachung mit Hilfe von Selbstschutzwerkzeugen wie Verschlüsselung (GnuPG, S/MIME) und Anonymisierungsdiensten (TOR, JonDos) recht wirkungsvoll entziehen. Da dies auch der Gesetzgeber erkannt hat, wurde mit der Neufassung des BKA-Gesetzes im Jahr 2008 in § 20k die Möglichkeit einer sog. Online-Durchsuchung eingeführt. Hierbei geht es um die Datenbeschaffung an der Quelle (bzw. Senke) einer Kommunikation (sog. Quellen-Telekommunikationsüberwachung, kurz: Quellen-TKÜ) (http://tinyurl.com/BKAG20k).

Das Bundesverfassungsgericht hat 2008 der Online-Durchsuchung mittels „Bundestrojaner“ sehr enge Grenzen gesetzt und ein neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Computergrundrecht) formuliert. Demnach darf präventiv nur überwacht werden, wenn dies zur Abwehr einer konkreten Gefahr für ein überragend wichtiges Rechtsgut richterlich angeordnet ist

(http://tinyurl.com/BvR37007).

Hintergrund ist die Absicht der Sicherheitsbehörden, die verschlüsselte Kommunikation noch vor dem Verschlüsseln (bzw. nach dem Entschlüsseln) beim Verdächtigen oder seinem Kommunikationspartner mitzulesen. Hierzu muss jedoch in einen fremden Rechner eingebrochen werden, um die Spähsoftware direkt dort zu betreiben. Ein Abhören der Daten beim Netzbetreiber wäre wirkungslos, da diese verschlüsselt sind.

### Alle Möglichkeiten werden genutzt

Carnivore, Echelon und PRISM zeigen, dass die jeweils aktuellen technischen Möglichkeiten zur Computerüberwachung durch US-amerikanische staatliche Stellen auch tatsächlich genutzt werden. Auch deutsche Sicherheitsbehörden verfügen über ähnliche technische Möglichkeiten zur Überwachung der Kommunikation. Nahezu unbegrenzter preisgünstiger Speicher führt schon heute zur dauerhaften Speichermöglichkeit von Verbindungsdaten.

Angesichts der massiven Bedrohungen durch Schadsoftware und Schnüffelprogramme gehört der Umgang mit Risiken heute ganz selbstverständlich zum Computeralltag. Wichtig ist es, Risiken zu vermeiden, wann immer dies möglich ist, immer alle Softwareupdates einzuspielen, technische Mechanismen wie Verschlüsselung und Anonymisierung einzusetzen, wo dies sinnvoll ist, und selbst dann muss man darauf hoffen, dass es keine verborgenen Sicherheitslücken gibt. Ursache ist die hohe Komplexität der Systeme, die kaum beherrschbar ist. Dies macht es Hackern und Überwachern meist viel zu leicht.

---

### Autor

Professor Hannes Federrath ist Leiter des Arbeitsbereichs Sicherheit in Verteilten Systemen am Fachbereich Informatik der Universität Hamburg. Seine Forschungsinteressen umfassen die Sicherheit mobiler Systeme, Kryptographie, Datenschutztechniken im Internet sowie technische und organisatorische Aspekte der Informationssicherheit.