Datenschutz und Datendiebstahl am Beispiel des NSA-Skandals

Dr. Christian Becker

15.01.2014

Überblick

Anfänge

- National Security Agency (NSA)
- Existenz der NSA viele Jahre geheim gehalten
- Kürzel NSA vom eigenen Mitarbeiterstab scherzhaft zu *No Such Agency* (Behörde ist nicht bekannt) oder *Never Say Anything* (Sag niemals irgendetwas) umgedeutet
- größter Auslandsgeheimdienst der Vereinigten Staaten
- weltweite Überwachung, Entschlüsselung und Auswertung elektronischer Kommunikation
- gegründet von US-Präsident Harry S. Truman in den 1940er-Jahren als Unterabteilung des Department of Defense
- gegen Ende der 1970er so einflussreich geworden, kaum noch zu kontrollieren

Aktionen vor 2001

- Verbindungen zu anderen Geheimdiensten, nachrichtendienstliche Fähigkeiten der CIA mit technischen Möglichkeiten der NSA
- Saddam Hussein bekam im Ersten Golfkrieg über vier Jahre Geheimdienstinformationen über die Kriegsführung des Iran von der NSA
- NSA unterstützte seit der Regierung Clintons einige Open-Source-Projekte zum Nutzen der Computersicherheit (SELinux)
- Publizierung von Ratschlägen zur Verbesserung der Computersicherheit, seit 2001 jedoch nicht mehr

Situation nach 9/11 I

- Trauma 9/11, Oktober 2001 Anweisung von Vizepräsident Dick Cheney bestehende Gesetze zu umgehen
- am 26. Oktober 2001 Inkrafttreten des PATRIOT Act
- weitreichende Eingriffe in Bürgerrechte für Anti-Terror-Ermittlungen
- Überwachen verdächtigter Personen ohne richterliche Anordnung
- geheimes Abhören von Telefonaten
- Speichern von Verbindungsdaten und Ausspionieren von E-Mail-Kontakten
- Einholen von personengebundenen Informationen bei Versicherungen, Geldinstituten und Arbeitgebern
- Inhaftieren und Ausweisen terrorverdächtiger Ausländer ohne richterliche Prüfung von Verdachtsmomenten

Situation nach 9/11 II

- seit 2011 Bau des Utah Data Center, eines neuen Rechenzentrums
- Speicherung großer Teile der gesamten Internetkommunikation
- mit enormen Rechenressourcen Arbeit an der Decodierung von Verschlüsselungsverfahren
- Kosten des Baus: 2 Milliarden US-Dollar

Auftrag der NSA I

Aufgaben der NSA:

- weltweite Telekommunikation aller Art zu überwachen
- nach nachrichtendienstlich verwertbaren Informationen zu filtern
- diese zu identifizieren, zu sichern, zu analysieren und auszuwerten
- nationales Verschlüsselungswesen
- Schutz eigener nationaler Telekommunikationswege einschließlich der Gewährleistung der nationalen Datensicherheit und Funktion des Cyberspace

Auftrag der NSA II

Tätigkeiten in der Bundesrepublik

- technische Aufklärung fester Bestandteil der US-Dienste in der Bundesrepublik
- bereits Konrad Adenauer unterschrieb Überwachungsvorbehalt zur Kontrolle des in- und ausländischen Post- und Fernmeldeverkehr
- Deutschland Partner dritter Klasse, bei Bedarf Kooperation, dessen Kommunikationsströme aber legitime Angriffsziele
- unter deutschen Diensten schon immer der Bundesnachrichtendienst Hauptpartner, seit 1993 allein

Auftrag der NSA II

- BND übermittellt in großem Umfang Metadaten aus der eigenen Fernmeldeaufklärung an die NSA
- Metadaten sind Verbindungsdaten zu Telefonaten, E-Mails und SMS
- laut Statistik pro Tag Übermittlung von bis zu 20 Millionen Telefonverbindungen und um die 10 Millionen Internetdatensätze
- Filterung dieser Daten vor Transfer um eventuell enthaltene personenbezogene Daten deutscher Staatsbürger

Auftrag der NSA III

- Problem: US-amerikanische Firmen mit Zugriff auf sensible Daten, z. B. IT-Dienstleister Computer Sciences Corporation (CSC), Projekte De-Mail, Aufbau des nationalen Waffenregisters, Überprüfung des Staatstrojaners und der Einführung des neuen Personalausweises
- NSA-Spionage dient auch zur Unterstützung der heimischen Wirtschaft

Ausmaß der Überwachung I

- globale Überwachungs- und Spionageaffäre entstand aus Enthüllungen von als Top Secret gekennzeichneten Dokumenten der NSA
- US-amerikanischer Whistleblower und ehemaliger Geheimdienstmitarbeiter Edward Snowden enthüllt Anfang Juni 2013 das Ausmaß der Überwachung
- Offenlegung diverser spezialisierter Programme

Ausmaß der Überwachung II

- *Bullrun* Programm der NSA, um verschlüsselte Daten im Internet mitlesen zu können, verschiedene Ansätze
- *CO-TRAVELER Analytics* Name eines Programms der NSA zur Sammlung und Auswertung von Standortinformationen aus dem Mobilfunk, Erstellung umfassender Bewegungs- und Beziehungsprofile
- *FAIRVIEW* bezeichnet Ansatz der NSA, auf Daten außerhalb der USA zugreifen zu können, Zusammenarbeit mit US-nationalen TK-Unternehmen, die wiederum mit ausländischen Unternehmen zusammenarbeiten. Unternehmen bestreiten zwar direkte Zusammenarbeit, verweisen aber gleichzeitig auf Gesetze zur Erzwingung der Zusammenarbeit

Ausmaß der Überwachung III

- im Rahmen des *PRISM*-Programms Abschöpfung von Daten von neun großen Internetunternehmen: darunter Apple, Microsoft, Facebook und Google. Unternehmen bestreiten, freiwillig Daten herauszugeben, Zurverfügungstellung nur auf richterlichen Beschluß
- Abteilung der NSA namens *Tailored Access Operations* stellt Werkzeuge ("Otto-Katalog") zur Ausspähung und Manipulation von Computern und Computernetzen her
- *XKeyscore* aus einem Verbund von mehr als 700 Servern in 150 verschiedene Standorte verteilt zur Datenanalyse und Echtzeit-Überwachung

Technische Möglichkeiten: Mobilfunk I

Abhören und Orten von Handys

- Organisation der Mobilfunknetze über Funkzellen mit Basisstationen, eine Funkzelle kann bestimmte Anzahl an Gesprächen vermitteln, in Städten kleines Gebiet, in ländlichen Gegenden größer
- wer Telefonate mithören will, muß den Teilnehmer orten
- wenn Handy empfangsbereit, kann Position genau bestimmt werden, notwendig dazu Telefonnummer des Teilnehmers
- Ermittlung der Nummer über Bewegungsprofil
- Zugriff auf die Informationen der Funkzellen, Ausgabe als Telefongesellschaft und Benutzung des sogenannten SS7 “Signaling System 7“

Technische Möglichkeiten: Mobilfunk II

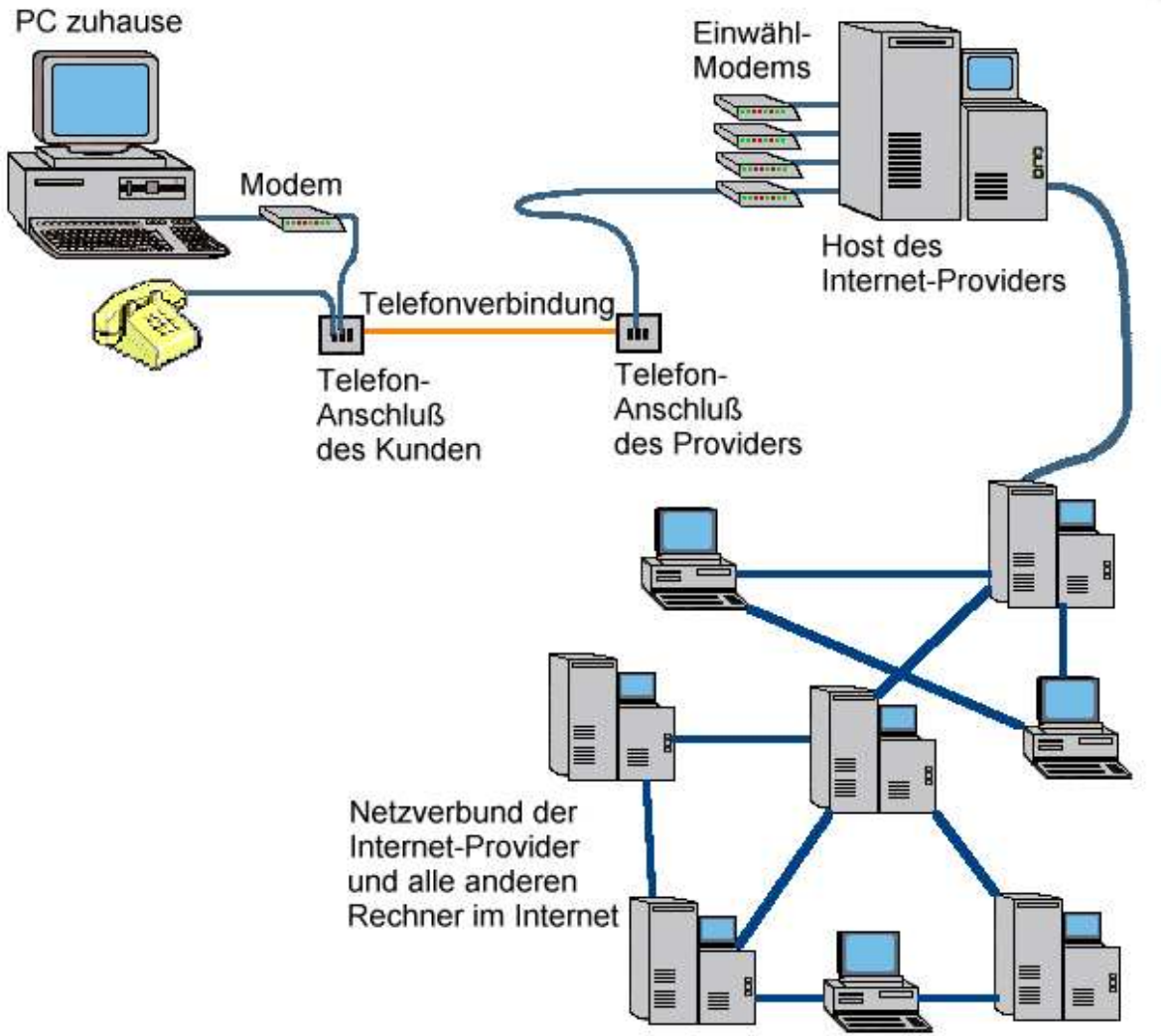
- Registrierung in einem anderen Land irgendwo auf der Welt, Angabe, als Provider auch in Deutschland arbeiten zu wollen. Kostet wenig, Nachweispflichten marginal
- Zuordnung des Teilnehmers über Nummer im *Home Location Register* von jedem Ort aus weltweit, wenn Handy empfangsbereit, genaue Positionsbestimmung möglich
- Zugriff mit sog. IMSI-Catcher, Gerät arbeitet gegenüber Handy wie eine Funkzelle (Basisstation) und gegenüber dem Netzwerk wie ein Teilnehmer

Technische Möglichkeiten: Mobilfunk III

- generell kein Handygespräch in Deutschland unverschlüsselt, aber alte Standards, nicht mehr sicher, Kryptohandies im Moment noch abhörsicher, aber unpraktisch
- Handys surfen automatisch bestimmte Seiten an, sobald sie sich einwählen, Abfang und Umleitung durch IMSI-Catcher, dadurch Übermittlung von Schadcode möglich, um Handy z. B. in eine Wanze zu verwandeln

Angriffspunkte im Netz

Das Internet:



Angriffspunkte im Netz I

Zwei Stoßrichtungen:

- Rastermethode, verdachtsunabhängig $\Longrightarrow$ Gegenmaßnahmen möglich
- zielgerichtet $\Longrightarrow$ "Pech, wenn man auf einer Liste steht" $\Longrightarrow$ de facto keine Gegenmaßnahme möglich

Angriffspunkte im Netz II

"Otto-Katalog":

- Ausnutzen von Schwachstellen "Hacken", Ausnutzung von Programmierfehlern, insbesondere in Webservern und Datenbanken, um Zugriff zu erhalten
- besonders aggressive Spionagesoftware, die sich in das sog. BIOS eines Computers einnistet und so auch Neuinstallation des Rechners überlebt
- präpariertes Monitor-Kabel, mit dem der Inhalt des Bildschirms von außen eingesehen werden kann
- speziell präparierte USB-Sticks, die mittels eingebauter Wanze einen Computer per Funk ausspähen können
- Einbau einer persistenten Backdoor in Internet-Routern, dadurch Fernzugriff auf den Router und Überwachung möglich

Was tun?

- Handy: weit vor einem kritischen Treffen Akku aus dem Handy nehmen
- keine Standardsoftware oder -betriebssysteme verwenden, je exotischer, desto besser
- immer aktuelle Softwareversionen verwenden
- Emails verschlüsseln
- anonym surfen

Emails verschlüsseln I

- E-Mails sind Klartexte, die per Internet versendet werden
- jeder, der diesen Datenstrom abfangen kann (z. B. Systemadministrator) kann mitlesen, Analogie Postkarte
- Verschlüsselung mit einem Schlüssel, unpraktisch
- deshalb einfacher zu handhabendes Verfahren: Schlüsselpaar, öffentlicher Schlüssel und nur dazu passender privater Schlüssel
- mit öffentlichen Schlüssel nur verschlüsseln und Signaturen prüfen, mit privatem Schlüssel nur entschlüsseln und signieren
- öffentlichen Schlüssel verfügbar machen, den privaten Schlüssel kennt nur Besitzer
- damit kann jeder eine Email verschlüsseln, aber nur der Besitzer mit dem passenden privaten Schlüssel kann diese entschlüsseln

Emails verschlüsseln II

Beispiel Thunderbird:

- Thunderbird herunterladen und installieren
- GnuPG (typischerweise als Teil von Gpg4win) herunterladen und installieren
- EnigMail (ein Thunderbird Plugin für Verschlüsselung) über den Addons-Manager von Thunderbird installieren
- mit Thunderbird/EnigMail ein Schlüsselpaar aus Public Key und Private Key und ein Widerrufszertifikat erstellen
- den eigenen Private Key für sich behalten und z.B. auf USB-Stick sichern
- den eigenen Public Key auf einen Schlüsselserver hochladen oder allen Gesprächspartnern mitteilen
- das Widerrufszertifikat ist für Widerrufung (Schlüssel ungültig erklären) gedacht

Anonym surfen I

- TOR-Browser hilft beim Surfen anonym zu bleiben, Kürzel TOR steht für "The Onion Router"
- basiert auf weltweitem Netzwerk aus TOR-Servern
- Browser baut zufällige Verbindung zu einem verschlüsselten TOR-Server auf
- dieser verbindet sich noch zwei Mal mit weiteren Servern im TOR-Netzwerk und verschleiert damit Identität des Surfers
- eingegebene Zieladresse wird an die einzelnen Server weitergeleitet
- jeder Server kennt nur die Adresse seines Vorgängers
- letzter TOR-Server fordert Daten für die gewünschte Webseite an und sendet die Daten zurück

Anonym surfen II

Probleme:

- alle Daten gehen über die Tor-Server, jeder Admin dort hat Vollzugriff auf Daten
- Zugriffsgeschwindigkeit

Aufgabe der Politik?

- Sicherheit vs Freiheit
- drei Stufen
  - verdachtsunabhängig zur Verhinderung
  - verdachtsabhängig zur Aufklärung
  - keine, Verhinderung/Aufklärung?
- Abwägung von Rechtsgütern
- Gefahr des Mißbrauchs, wirksame Kontrolle
- Wirksamkeit der Überwachung, kein Terrorist wird seine Pläne im Klartext verschicken, Möglichkeiten zur Verschleierung, die keine Rasterüberwachung entdecken kann (Steganographie)
- Inkaufnahme von Kollateralschäden
- Gefahr durch organisierte Internet-Kriminalität ebenso gegeben