Überwachung elektronischer Kommunikation

Compass Security Event 2004, 28.04.2004

Dirk Fox
fox@secorvo.de

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail info@secorvo.de
http://www.secorvo.de

Secorvo Security Consulting

- **Unabhängiges Beratungshaus für Informationssicherheit**
- **Ausbildungszentrum für IT-Sicherheit: Secorvo College**





- **Ausbildungspartner von BSI, SAP, T-Systems**
- **Kunden: Schering, BMW, DaimlerChrysler, BASF, Deutsche Bank, Heidelberger, FinanzIT, Michelin, Commerzbank, BSI, Bundesbank, Deutsche Bahn, Deutsche Post, SAP, EZB, Linde, Bosch, ...**

© Secorvo

Inhaltsübersicht

- Telekommunikationsüberwachung
  - Rechtlicher Hintergrund
  - Entwicklung in Zahlen
- Technische Möglichkeiten
- Der IMSI-Catcher
- Internationale Abhörsysteme
- Ausblick

© Secorvo

Inhaltsübersicht

- Telekommunikationsüberwachung
  - Rechtlicher Hintergrund
  - Entwicklung in Zahlen
- Technische Möglichkeiten
- Der IMSI-Catcher
- Internationale Abhörsysteme
- Ausblick

© Secorvo

TK-Überwachung

- **Strafverfolgung**
  - Grundsätzlich richterliche Anordnung erforderlich
  - Beschränkt auf schwere Straftaten (Mord, Menschenraub, ...)
- **Nachrichtendienste**
  - Bundesnachrichtendienst (BND)
  - Militärischer Abschirmdienst (MAD)
  - Verfassungsschutzbehörden (Bund und Länder)
- **Wirtschaftsspionage**
  - „Wir befinden uns heute in einem weltweiten Wirtschafts-krieg. Der Rohstoff, um den gekämpft wird, ist Information.“ (Christian Pierret, franz. Industrieminister, 4/2000)
- **Organisierte Kriminalität**
- **Terrorismus**

© Secorvo

secorvo security consulting

Rechtliche Grundlagen (D)

- **Fernmeldegeheimnis (Art. 10 GG)**
  - „(1) Das Briefgeheimnis sowie das Post- und Fernmelde-geheimnis sind unverletzlich. (2) Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden. (...)“
- **Beschränkung des Fernmeldegeheimnisses**
  - Strafprozeßordnung (StPO): § 100a/b
  - Verbindungsdaten: § 100 g/h StPO (früher § 12 FAG)
  - Außenwirtschaftsgesetz (AWG): §§ 39-43 (28.04.1961)
  - G 10-Gesetz (Neuregelung vom 26.06.2001)
- **Verpflichtungen der Telekommunikationsanbieter**
  - Telekommunikationsgesetz (TKG): § 88 Abs. 1 (Neufassung in Abstimmung zwischen Bundesrat/Bundestag)
  - TK-Überwachungsverordnung (TKÜV) vom 16.08.2002

© Secorvo

secorvo security consulting

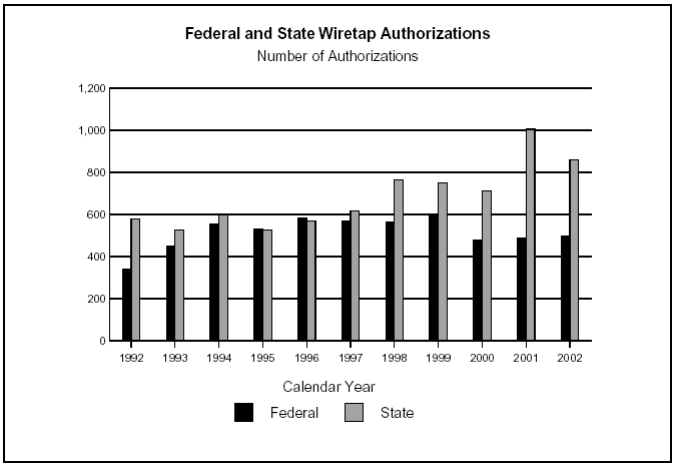
Anforderungen TKG

- **Grundsätze**
  - Bezugspunkt: Kennung einer Telekommunikationsanlage
  - Bereitstellung vollständiger Kopie der Telekommunikation
- **Verpflichtete**
  - Betreiber öffentlicher Telekommunikationsanlagen
  - Ausnahme: Internet-Provider, Spezialdienste, < 1.000 TN
- **Technische Anforderungen**
  - Umsetzung einer Überwachung durch Dritte nicht feststellbar
  - Überwachung durch mehr als eine berechtigte Stelle möglich
  - Daten: Kennungen, Zeit/Dauer, Dienste, Standort (Mobilfunk)
- **Kosten**
  - Vorhaltung und Betrieb der technischen Einrichtungen
  - Eigenverantwortliche Umsetzung der Überwachung

© Secorvo

Überwachung in den USA

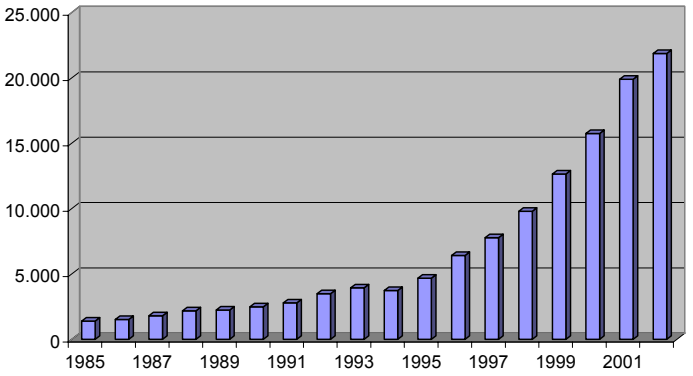
- **Dokumentiert in jährlichen „Wiretap Reports“**



© Secorvo

Überwachung in Deutschland

- **Entwicklung der Telefonüberwachung**
  - **1985: 1.399**
  - **1986: 1.532**
  - **1987: 1.805**
  - **...**
  - **1995: 4.674**
  - **1996: 6.428**
  - **1997: 7.776**
  - **1998: 9.802**
  - **1999: 12.651**
  - **2000: 15.741**
  - **2001: 19.896**
  - **2002: 21.874 = 15 mal so viel wie in den USA!**



© Secorvo

secorvo security consulting

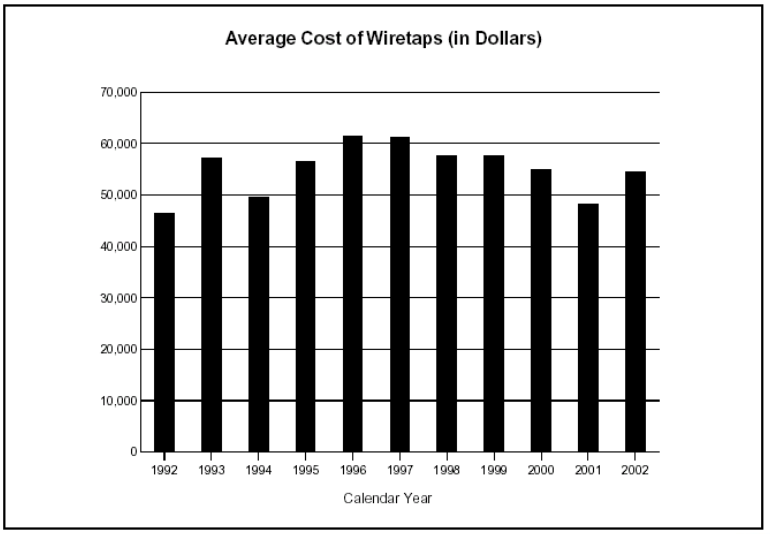
Überwachungspraxis (D)

- **Erwirkung einer Anordnung**
  - **Polizeiliche Ermittlung der Anschlußkennung**
  - **Beantragung durch Staatsanwaltschaft bei Amtsgericht**
  - **Amtsrichterentscheidung auf Grundlage der Begründung**
- **Auswertung von Abhörmaßnahmen**
  - **Wirksamkeit von Abhörmaßnahmen wird nicht ausgewertet (Vorbild USA: „wiretap reports“)**
  - **Amtsrichter erhält keinerlei Kenntnis von Ermittlungen**
  - **Datenvernichtung oft verspätet, unsauber dokumentiert**
  - **Schriftliche Unterrichtung der Betroffenen unterbleibt häufig**
- **Kreis der Betroffenen**
  - **Je Maßnahme durchschnittlich 100 Anschlüsse betroffen**
  - **Pro Jahr mehr als 1 Mio. Anschlüsse abgehört (> 2,5%)**

© Secorvo

secorvo security consulting

Überwachungskosten (USA)



© Secorvo

Inhaltsübersicht

- Telekommunikationsüberwachung
  - Rechtlicher Hintergrund
  - Entwicklung in Zahlen
- **Technische Möglichkeiten**
- Der IMSI-Catcher
- Internationale Abhörsysteme
- Ausblick

© Secorvo

Akustische Überwachung

- Richtmikrofone
- Stethoskope
- Installation von Aufzeichnungsgeräten
- „Wanzen“ in Besprechungsräumen
- Raumüberwachungsfunktion in Anrufbeantwortern, Trojanern
- Freisprecheinrichtung von Nebenstellenanlagen
- Mikrofonfreischaltung in (manipulierten) Handys



© Secorvo

secorvo security consulting

Visuelle Überwachung

- Beschattung (Detektive, Zivilpolizei)
- Überwachungskameras
  - Banken, Sicherheitsbereiche (z.B. Rechenzentren)
  - Öffentliche Plätze
  - Getarnte Mini-Funkkameras
  - ⇨ über 300.000 Großsysteme allein in Deutschland!
- Personenerkennungssysteme
  - Filmaufnahmen von gewalttätigen Demonstranten
  - Aufzeichnungen öffentlicher Plätze
  - ⇨ Beispiel: Football-Meisterschaft „Super Bowl“ („Snooper Bowl“): 19 Verdächtige aus 17.000 Besuchern herausgefiltert

© Secorvo

secorvo security consulting

Elektronische Überwachung

- „Hacking“ von IT-Systemen (Internet, Remote-Access- und Fernwartungszugänge)
- Auswertung von Bildschirm-Abstrahlung (bis 30m)
- Verbreitung „Trojanischer Pferde“
- Anzapfen interner oder externer Vermittlungen
- Ausnutzung von WLAN-Sicherheitslöchern
- Belauschen von Richtfunkstrecken
- Abhören von Satellitenverbindungen (BND: Filterung von 75.000 Verbindungen/Tag = 10%)
- Filterung von Interkontinentalverbindungen (NSA: Systeme „Carnivore“, „Omnivore“)

© Secorvo

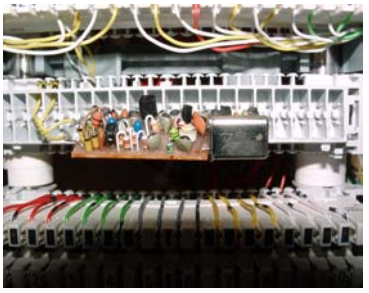
secorvo security consulting

Elektronische Überwachung

- Trojanisches Pferd (sub7en)



- Manipulation von Vermittlungsstellen



© Secorvo

secorvo security consulting

Elektronische Überwachung

- „Key Ghost“
  - Anbringung an Tastaturkabel
  - Speicherung aller Tastatureingaben
  - Kapazität: mehrere MByte





© Secorvo

secorvo security consulting

Inhaltsübersicht

- Telekommunikationsüberwachung
  - Rechtlicher Hintergrund
  - Entwicklung in Zahlen
- Technische Möglichkeiten
- **Der IMSI-Catcher**
- Internationale Abhörsysteme
- Ausblick

© Secorvo

secorvo security consulting

Überwachung im Mobilfunk

- **Grenzen der Observierungsmöglichkeiten**
  - Für den Erlass einer Abhöranordnung fehlt die Teilnehmerkennung
  - Vom Standort einer observierten Person kann nicht mehr auf die Anschlusskennung geschlossen werden
- **Technische Lösung**
  - Gerät zur Feststellung der IMSI (International Mobile Subscriber Number) des Handys einer observierten Person
  - Hersteller: Fa. Rohde & Schwarz (1998)
- **Nutzung des IMSI-Catchers**
  - Einsatz durch BKA seit 1998 in ca. 35 Fällen
  - Seit 01.01.2002: Auch Verfassungsschutz und MAD zur Nutzung berechtigt (§ 9 Abs. 4 BVerfSchG)
  - Seit 06.08.2002: Einsatz legalisiert durch § 101i StPO

© Secorvo

secorvo security consulting

„IMSI-Catcher“

- **Funktionsweise: Simulation einer Basisstation**
- **Produkt der Firma Rohde & Schwarz**
  - GA090: „Maskierung“ einer Basisstation
  - GA900: Unterdrückung der Verschlüsselung
  - Kosten: < 500 TDM
- **Abfrage der IMSI bei eingeloggten Geräten**
- **Betrieb von RegTP nicht genehmigt**



© Secorvo

secorvo security consulting

Wirksamkeit

- **Feststellung der Teilnehmerkennung**
  - Im Rahmen einer Observation: IMSI-Catcher simuliert Funkzelle geringer Leistung (< 1 Watt) und Ausdehnung
  - Gesuchtes Handy muss eingeschaltet sein
  - Netze aller Netzbetreiber müssen simuliert werden
  - Gesuchte IMSI muss herausgefiltert werden
  - Ggf. Mitwirkung ausländischer Netzbetreiber erforderlich
- **Ortung**
  - Bei bekannter IMSI Ortung möglich
- **Abhören**
  - Nur mit Modell GA900 (in Deutschland nicht zulässig)
  - Nur abgehende Anrufe, nur von einem Handy gleichzeitig

© Secorvo

secorvo security consulting

Störungen und Missbrauch

- **Handys im Einzugsbereich des IMSI-Catchers**
  - Mobiltelefone können keine Verbindungen aufbauen (auch nicht zu Notrufnummern)
- **Störungen im Netzbetrieb**
  - Gesprächsabbrüche, Übertragungsfehler durch Interferenzen der Signale der simulierten mit der echten Basisstation
  - Hohe maximale Sendeleistung des IMSI-Catchers (<= 20 Watt)
- **Missbrauchsmöglichkeiten**
  - Verkauf außerhalb Deutschlands zulässig
  - Illegale Nutzung in der Praxis nicht feststellbar
- **Grenzen**
  - UMTS: gegenseitige Authentifikation
  - Aber: bei Störung schaltet UMTS auf GSM!

© Secorvo

secorvo security consulting

Inhaltsübersicht

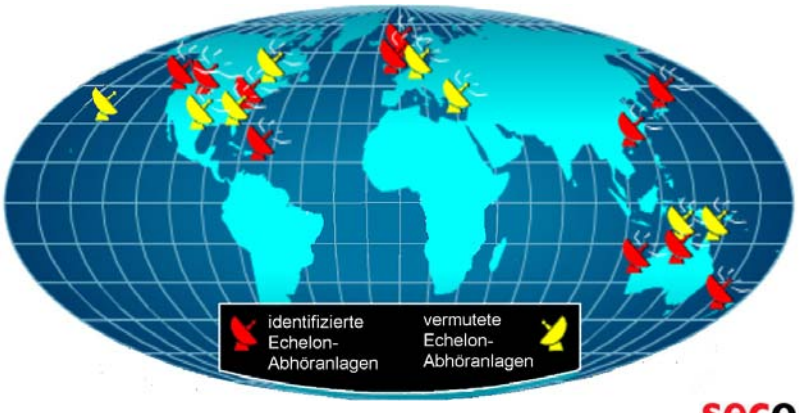
- Telekommunikationsüberwachung
  - Rechtlicher Hintergrund
  - Entwicklung in Zahlen
- Technische Möglichkeiten
- **Internationale Abhörsysteme**
- Schutzmaßnahmen
- Ausblick

© Secorvo

secorvo security consulting

US-Abhörsystem „Echelon“

- **Betrieb durch NSA (60-100.000 MA, 10-15 Mrd. US$/J)**
- **Umfang: 11 bekannte, 8 vermutete Abhörstationen**



© Secorvo

secorvo security consulting

US-Abhörsystem „Echelon“

- **UKUSA-Vereinbarung (1948)**
  - **UK, USA, Kanada, Australien, Neuseeland**
- **Belege**
  - **STOA-Bericht (1998)**
  - **EU-Ausschuß (11.07.2001)**
- **Bad Aibling (Bayern):**
  - **Überwachung des deutschen Fernmeldeverkehrs seit 1952**
  - **etwa 14 Satellitenantennen, ca. 750-1.000 Mitarbeiter**
  - **KI-Inhaltsfilterungssystem: „Memex“ (Schlüsseldaten)**
  - **Einstellung der Tätigkeit: Ende 9/2001**



© Secorvo

secorvo security consulting

Inhaltsübersicht

- Telekommunikationsüberwachung
  - Rechtlicher Hintergrund
  - Entwicklung in Zahlen
- Technische Möglichkeiten
- IMSI-Catcher
- Internationale Abhörsysteme
- **Ausblick**

© Secorvo

secorvo security consulting

Ausblick

- **Wachsende „Begehrlichkeiten“**
  - **Datenabgleich von Strafverfolgungsbehörden mit Nachrichtendiensten**
  - **Technisch stark vereinfachte Zugriffsmöglichkeiten**
  - **Kostensenkung und -abwälzung auf Telekom-Betreiber**
  - **Enfopol: Speicherung von E-Mails, Telefonaten über 7 Jahre**
  - **Einführung der Vorratsspeicherung für ISPs**
- **Zunehmende Verfügbarkeit personenbezogener Daten**
  - **Erhebung von Kundendaten zur Kundenbindung über Kunden-/Rabattkarten (z.B. „miles & more“)**
  - **Gezielte Erforschung von Kundenbedürfnissen (CRM)**
  - **Bewegungsprofile durch RFID-Technologie möglich**
  - **Flächendeckende Erfassung von Bewegungsdaten mit Maut-Technologie möglich**

© Secorvo

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Tel. +49 721 6105-500
Fax +49 721 6105-455
E-Mail info@secorvo.de
http://www.secorvo.de