



Prof. Dieter Kempf
Mitglied des BITKOM-Präsidiums

Innere Sicherheit und Hightech

BITKOM - Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Berlin, 28. November 2007

Sicherheit und Hightech: Drei Dimensionen

Schwerpunkt heute: Staatliche Überwachung



Bereitstellung von Sicherheitselektronik

Videoüberwachung

Biometrie, z.B. E-Pass

Verteidigung u.a.

Staatliche Überwachung von Kommunikation

TK-/Internetüberwachung

Vorratsdatenspeicherung

Online-Durchsuchung

Anwender-Schutz gegen Gefahren

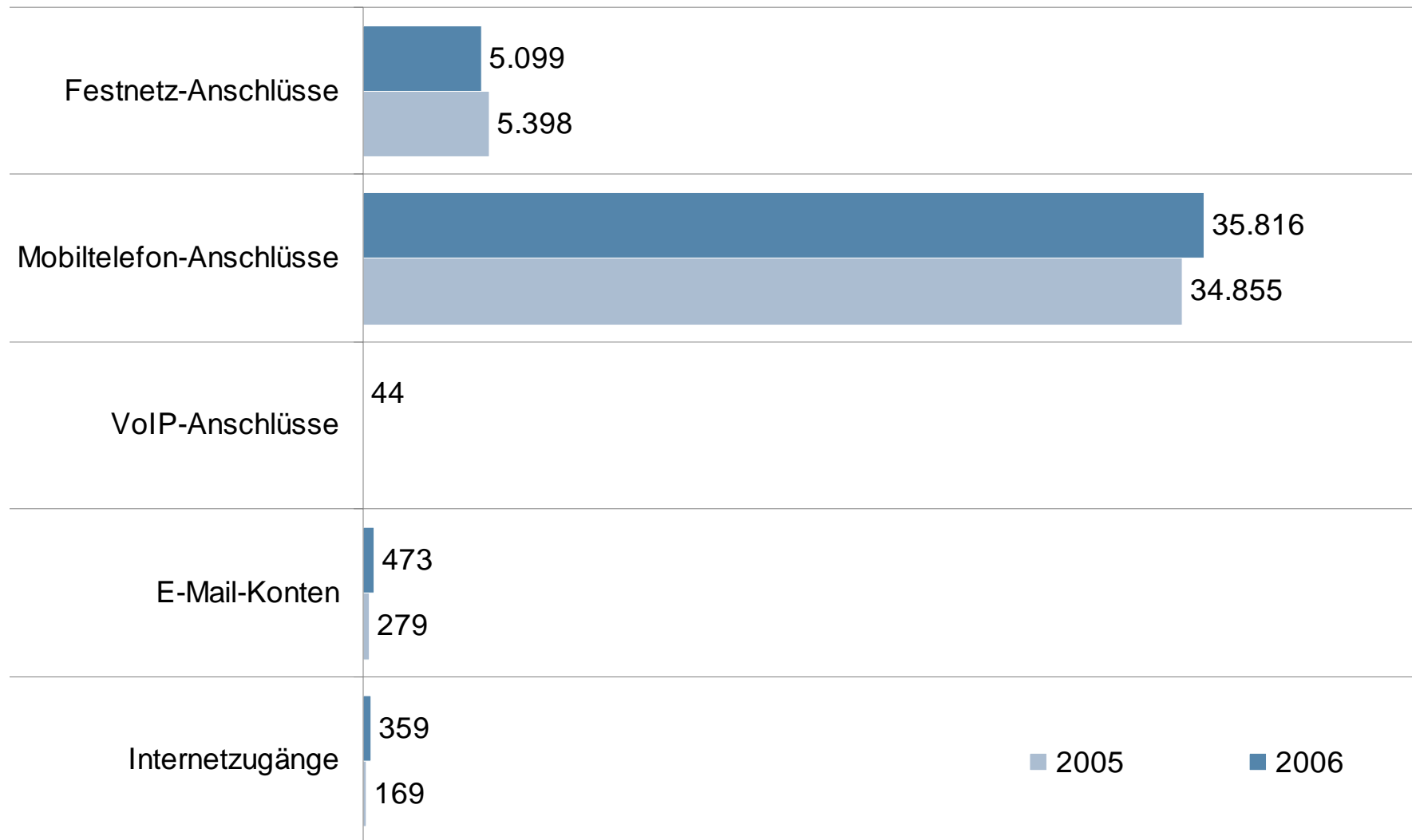
Schadprogramme/Viren

Phishing

Hacker

Der Staat hört mit

Überwachung zur Strafverfolgung, § 110 Abs. 8 TKG



Quelle: Bundesnetzagentur

Überwachung von Gesprächsinhalten und Daten

Gesetzliche Bedingungen nach §§ 100 ff. StPO



	Bisher	Neu
Telefon, Handy, VoIP, SMS, E-Mails	<ul style="list-style-type: none">▪ Enger Straftatenkatalog▪ Nur wenn andere Wege aussichtslos▪ Irrelevantes löschen, Betroffene informieren▪ Richtervorbehalt, bei Gefahr im Verzug StA	<ul style="list-style-type: none">▪ Erweiterter Straftatenkatalog▪ Z.B. Steuerdelikte, Menschenhandel, Doping▪ Geplant ab 01.01.2008

Kommunikation: Speicherung Verbindungsdaten

Gesetzliche Bedingungen bei Telefon und Internet



	Bisher	Künftig (geplant ab 1.1.2008 bzw. 1.1.2009)
Telefon, Handy, VoIP, SMS	<ul style="list-style-type: none"> ▪ Keine generelle Speicherpflicht ▪ Max. 6 Mon. Speicherung für Rechnungszwecke ▪ Auf Kundenwunsch Löschung mit Re.-Versand ▪ Auskunft an Ermittler bei erheblichen Straftaten 	<ul style="list-style-type: none"> ▪ Generelle Speicherpflicht 6 Mon. ▪ Inkl. Standortdaten und IP-Adressen ▪ Auskunft an Ermittler bei mehr Straftaten ▪ Betriebskostenentschädigung geplant
Internet-Zugang, E-Mail	<ul style="list-style-type: none"> ▪ Keine generelle Speicherpflicht f. IP-Adressen ▪ Auch nicht für E-Mail-Verbindungsdaten ▪ Max. 6 Mon. Speicherung für Rechnungszwecke ▪ Auskunft an Ermittler bei erheblichen Straftaten 	<ul style="list-style-type: none"> ▪ Internet-Einwahldaten 6 Mon. speichern ▪ Inkl. IP-Adresse und Anschlusskennung ▪ Mail-Verbindungsdaten 6 Mon. speichern ▪ Inkl. Mail-Adressen, Absender-IP, Zeiten ▪ Auskunft an Ermittler bei mehr Straftaten ▪ Betriebskostenentschädigung geplant

Unterstützung für Ermittler

- Bekämpfung von Kriminalität und Terror ohne Branchen-Mitarbeit undenkbar
- Verlässlicher Kooperationspartner auf gesetzlicher Basis

Pragmatischer Ansatz

- Balance zwischen Schutz der Gesellschaft und Schutz der Privatsphäre
- EU-Vorgaben sind sinnvolle Richtschnur
- Straftatenkatalog überprüfen (z.B. Beleidigung per Telefon/Internet)

Faire Bedingungen

- Beginn für Sprachtelefonie zum 1.1.2008 zu kurzfristig (technische Umsetzbarkeit kaum machbar: nur wenige Wochen zur Umsetzung nach Beschluss im Bundestag)
- Generelle Übergangsfrist bis 2009 für technische und personelle Umstellung wäre besser
- Entschädigung für Investitionen in Technik von 50 bis 75 Millionen Euro
- Entschädigung für jährliche Betriebskosten in zweistelliger Millionen-Höhe

Entschädigungszahlungen für die VDS

Geplante Änderungen und BITKOM-Position



Alte Regelung

- TK-Unternehmen bezahlt wie Tatzeugen: 17 €/h
- Aufwand für Kostennachweis höher als Erstattung.
- Folge: Viele Unternehmen verzichten auf Kostenerstattung.

Regelung der Entschädigungen im verabschiedeten Gesetzesentwurf:

Positiv

- Endlich: Verabschiedeter Gesetzesentwurf erkennt Belastungen der TK-Unternehmen an
- Daher generell: Großer Schritt nach vorn
- Dank pauschaler Sätze kein Kostennachweis mehr nötig

Negativ

- Pauschale Sätze zu niedrig – auch im internationalen Vergleich

Entschädigungszahlen im Vergleich I

Österreich, Schweiz, Deutschland: Beispiel 1



1. Telefonüberwachung: analoger Standardanschluss, 90 Tage

- Österreich: 2.393,20 Euro
(Einrichtung: 128 Euro, Übermittlung pro Tag: 25 Euro, Sekretariatspauschale 15,20 Euro)
- Schweiz: 794 Euro (umgerechnet)
(Einrichtung und Betrieb: 794 Euro)
- Deutschland (bei dezentraler Anforderung): 325 Euro
(Einrichtung 100 Euro, Übermittlung pro 30 Tage: 75 Euro)
- Deutschland (bei zentraler Anforderung): 305 Euro
(20 Prozent Rabatt auf Einrichtungspreis)
- BITKOM-Forderung: Statt Abschlag bei zentraler Anforderung ein Zuschlag bei dezentraler Anforderung auf den Grundpreis

Entschädigungszahlen im Vergleich II

Österreich, Schweiz, Deutschland: Beispiele 2 und 3



2. Überwachung eines DSL-Anschlusses

- Österreich: 2.393,20 Euro
- Schweiz: Keine Pauschale, Erstattung nach Aufwand
- Deutschland (dezentral): 700 Euro
- Deutschland (zentral): 680 Euro

3. Auskunft zu bei Providern gespeicherten Verkehrsdaten (Rufnummern, IP-Adressen, Standorte)

- Österreich: Auskunft über 1 Tag pro Kennung: 85,70 Euro
Auskunft über 90 Tage: 664,20 Euro
- Schweiz: Auskunft pauschal: 322 Euro (umgerechnet)
- Deutschland: Auskunft pauschal: 30 Euro

Überwachung von Gesprächsinhalten und Daten

Gesetzliche Bedingungen nach §§ 100 ff. StPO



	Bisher	Künftig
PCs u. Festplatten	<ul style="list-style-type: none"> ▪ Kein Bundesgesetz f. Online-Durchsuchung ▪ Zugriff nur bei Hausdurchsuchung ▪ Hausdurchsuchung bei allen Straftaten mögl. ▪ Richtervorbehalt, bei Gefahr im Verzug StA 	<ul style="list-style-type: none"> ▪ Informeller Entwurf zur Online-Durchsuchung ▪ Alle Endgeräte und Mail-Server mögl. Ziel ▪ Abwehr „dringender Gefahren“/Terrorismus ▪ Richtervorbehalt, notfalls durch BKA-Präsid.
Wohnung	<ul style="list-style-type: none"> ▪ Großer Lauschangriff (Gespräche innerhalb) ▪ Enger Straftatenkatalog, bes. hohe Hürden ▪ Pers. Kernbereich muss ausgeschlossen sein ▪ Strenger Richtervorbehalt, nicht durch StA 	<ul style="list-style-type: none"> ▪ Keine Änderungen in Sicht

Eng begrenzter Einsatzbereich

- Hohe Hürden wie bei der Wohnraumüberwachung
- Orientierung an Leitlinien des BVerfG zum Großen Lauschangriff
- Wenige Fälle pro Jahr (Gefahrenabwehr/Terrorismus)

Problematisch bei Software-Schnittstellen

- Nationaler Ansatz für Hintertüren wenig sinnvoll
- Nachteile für Anbieter in Deutschland
- Bei wenigen Fällen pro Jahr besser individueller Zugriff

Problematisch bei E-Mail-Servern

- Nationaler Ansatz wenig sinnvoll
- Nutzer können auf ausländische Anbieter ausweichen

Online-Durchsuchung

Varianten und offene Fragen



Technisch

- Programm: Trojaner, Key-Logger oder andere Technik
- Zugriff: Individuell oder über obligatorische Software-Schnittstelle
- Installation: Direkt/manuell, über E-Mail-Anhang, Webseite oder Software-Update
- Sog. „Bundestrojaner“ müsste Firewalls und Virens Scanner umgehen
- Programm soll nicht irrtümlich auf weitere Rechner übertragen werden

Rechtlich

- Gelten für Festplatten ähnliche Schutzkriterien wie für Wohnräume?
- Lassen sich strafrechtlich Relevantes und persönlicher Kernbereich trennen?
- Sind Erkenntnisse auch vor Gericht zur Strafverfolgung nutzbar?
- Dürfen Firmen in Deutschland Schutzprogramme gegen Online-Durchs. anbieten?

Online-Durchsuchung

Beispiele aus dem Ausland



Österreich

- Kabinett hat Regelung beschlossen, gilt voraussichtlich ab Herbst 2008
- Nicht nur zur Gefahrenabwehr, sondern auch zur Strafverfolgung
- Straftaten mit 10 Jahren Mindestfreiheitsstrafe und dringender Tatverdacht
- Richtervorbehalt und gesonderte Beobachtung durch Rechtsschutzbeauftragten
- Nach Angaben des Justizministeriums ein bis zwei Einsätze jährlich geplant

Schweiz

- Gesetzliche Regelung zur Gefahrenabwehr geplant
- Einsatzfelder: Terrorismus, Spionage, Waffenhandel, illegaler Technologietransfer
- Richtervorbehalt, bei Gefahr im Verzug Anordnung durch zuständiges Bundesamt

USA

- FBI hat bisher in Einzelfällen Spähprogramme eingesetzt, die namentlich bekannt sind
- Funktionen: Ausspähen von Systemdaten, besuchten Webseiten sowie IP-Adressen
- Laut FBI keine Erfassung von Kommunikationsinhalten



Prof. Dieter Kempf
Mitglied des BITKOM-Präsidiums

Innere Sicherheit und Hightech

BITKOM - Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Berlin, 28. November 2007