Im Spannungsfeld von Recht und Technik

Dr. Christoph Wegener
wecon.it-consulting

München, 14. März 2008

Frühjahrs Fach2008 Gespräch

Zur Person: Christoph Wegener

- Mitarbeiter am Horst Görtz Institut für IT-Sicherheit (HGI)
- Gründer der **wecon.it**-consulting
- Gründungsmitglied der Arbeitsgruppe Identitätsschutz im Internet (a-i3)

- Auditor und Sachverständiger
- CISA, CISM, CBP
- Fachautor/-lektor/-gutachter
- Verschiedene Lehrtätigkeiten

- E-Mail: wegener@wecon.net Web: www.wecon.net

Frühjahrs Fach2008 Gespräch

Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
- §§ 113a/113b TKG – die "Vorratsdatenspeicherung"
  - Hintergründe
  - Auswirkungen
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Problemfelder
- Fazit und Diskussion

Frühjahrs Fach2008 Gespräch

Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
- §§ 113a/113b TKG – die "Vorratsdatenspeicherung"
  - Hintergründe
  - Auswirkungen
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Problemfelder
- Fazit und Diskussion

Frühjahrs Fach2008 Gespräch

"Hackerparagraph" Hintergründe (1)

- "European Cybercrime Convention" ETS 185
  - Beschlossen am 23. November 2001
  - Soll noch insgesamt ratifiziert werden
  - Wichtig hier: Art. 6 Abs. 3
- Rahmenbeschluss des Europarates 2005/222/JI
  - Beschlossen am 24. Februar 2005
  - Veröffentlicht im ABl. EG L 69/67
  - Umsetzung bis spätestens 16. März 2007
- § 202c StGB – der Hackerparagraph
  - Teil des 41. Strafrechtsänderungsgesetzes (StrÄndG) vom 30. November 2006
  - Am 6. Juli 2007 verabschiedet,
  - Am 11. August 2007 in Kraft getreten

Frühjahrs Fach2008 Gespräch

"Hackerparagraph" Hintergründe (2)

- § 202c StGB
  "Vorbereiten des Ausspähens und Abfangens von Daten":
  *"(1) Wer eine **Straftat** nach § 202a oder § 202b **vorbereitet**, indem er*
  1. *Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*
  2. ***Computerprogramme, deren Zweck die Begehung einer solchen Tat ist**,*

  ***herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht**, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*
  (2) ..."

- Bezüge zu § 202c StGB in
  - § 202a StGB "Ausspähen von Daten"
  - § 202b StGB "Abfangen von Daten"
  - § 303a StGB "Datenveränderung" (durch Verweis)
  - § 303b StGB "Computersabotage" (durch Verweis)

"Hackerparagraph" Probleme (1)

- Wo liegen die eigentlichen Probleme?
  - Für § 202c StGB ist Vorsatz erforderlich
  - Abgrenzung Hacker-Tools <-> Dual-Use-Tools
- Was heißt "Vorsatz erforderlich"?
  - Was ist "Vorsatz" im rechtlichen Sinne?
    - Absicht
    - Direkter Vorsatz: Täter nimmt mögliche Folge hin
    - Eventualvorsatz ("dolus eventualis"): Eintritt wird für **möglich** gehalten, Täter nimmt das hin
  - Folgerung: Keine Vorbereitungshandlung, wenn ...
    - Keine eigene oder fremde Tat in Aussicht genommen
  - Problem: Zugänglichmachen für (unbekannte) Dritte?
    - Wie konkret muss der Missbrauch durch einen Dritten sein?

"Hackerparagraph" Probleme (2)

- Abgrenzung in Bundestags-Drucksache 16/3656:
  - Hacker-Tools
    - Seite 12: *"[...] Hacker-Tools, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen [...]"*
  - Dual-Use-Tools
    - Seite 12: *"[...] Es reicht, wenn die **objektive** Zweckbestimmung des Tools auch die Begehung einer solchen Straftat ist. [...]"*
    - Seite 19: *"[...] Bei Programmen, deren funktionaler Zweck nicht eindeutig ein krimineller ist [...] oder zu einem legitimen Werkzeug (z. B. bei Sicherheitsüberprüfungen oder im Forschungsbereich) werden (sog. dual use tools), ist der objektive Tatbestand des § 202c [...] nicht erfüllt [...]"*
  - Allgemeine Anwendungsprogramme
    - Nicht näher definiert

"Hackerparagraph" Probleme (3)

- Wie ist es eigentlich gedacht
  - ETS 185, Art. 6, Abs. 1 – Tools müssen in erster Linie für Begehung einer Straftat ausgelegt sein:
    "[...] with intent that it be used for the purpose of committing [...]"
  - ETS 185, Art. 6, Abs. 2 – Klarstellung bezüglich genehmigter Tests / Schutz von Computersystemen
    "This article shall not be interpreted as imposing criminal liability where the production [...]"

- Was machen die anderen Länder
  - Österreich hat eine klarere Regelung – § 126c ÖStgB:
    "[...] ***mit dem Vorsatz*** *herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie* ***zur Begehung einer der in Z 1 genannten strafbaren Handlungen*** *gebraucht werden [...]"*

"Hackerparagraph" Auswirkungen

- Bisher sind eine Reihe von Folgen zu spüren
- Große Verunsicherung der deutschen IT-Akteure
  - Siehe Pressemeldungen BITKOM, eco, CCC, ...
  - (Nicht notwendige) Abwanderung von Webseiten
    - Beispiel: http://www.thc.org
- Klage gegen das BSI
  - 14. September 2007: TecChannel reicht Klage ein
  - 8. Oktober 2007: Klage wird von StA Bonn abgelehnt
  - 31. Oktober 2007: TecChannel reicht Beschwerde ein
- Weiterhin keine "Rechtssicherheit", aber...

Frühjahrs Fach2008 Gespräch

"Hackerparagraph" Schlussfolgerungen

- Keine Panik, keine Panik, keine Panik! :)
  - Unklarheiten lassen sich eingrenzen
- Empfehlungen – aber "ohne Gewähr" ;)
  - IT-Security Audits unbedingt klar definieren (Das sollte sowieso immer der Standard sein!)
  - Keine Werbung für "Systemeinbruchswerkzeuge"
  - Dual-Use-Tools können weiterhin genutzt werden
- Offene Fragen
  - Weitergabe an unbekannten Personenkreis
  - Problem der Abgrenzung Hackertools <-> Dual-Use-Tools

Frühjahrs Fach2008 Gespräch

Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
- §§ 113a/113b TKG – die "Vorratsdatenspeicherung"
  - Hintergründe
  - Auswirkungen
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Problemfelder
- Fazit und Diskussion

Frühjahrs Fach2008 Gespräch

Vorratsdatenspeicherung "Wer, wie, was"

- Warum das Ganze überhaupt?
  - Basiert auf der Richtlinie 2006/24/EG
  - Deutsche Umsetzung in §§ 113a/113b TKG
  - Bemerkenswert: Dauer des Verfahrens
    - Richtlinie vom 15. März 2006
    - Gesetzesentwurf vom 27. Juni 2007
    - Verabschiedet am 9. November 2007
- Wie lange muss gespeichert werden?
  - Mindestens 6 Monate, höchsten 24 Monate
  - Deutschland: 6 Monaten, Großbritannien: 24 Monate
- Ab wann muss gespeichert werden?
  - Telekommunikation ab 1. Januar 2008
    (Aber: Verfolgung von Verstößen erst ab 1. Januar 2009)
  - Internet/E-Mail ab 1. Januar 2009

Vorratsdatenspeicherung Was wird gespeichert? (1)

- Redundantes Speichern: Sowohl bei Absender als auch beim Empfänger wird gespeichert!

- Speicherung der Bestandsdaten bei Kommunikation per
  - Telefonfestnetz, Mobilfunk
  - Internetzugang, Internet-Telefonie, Internet-E-Mail

- Ausdrücklich keine Speicherung von Inhalten!
  - Art. 5, Abs. 2: *"Nach dieser Richtlinie dürfen keinerlei Daten, die Aufschluss über den Inhalt einer Kommunikation geben, auf Vorrat gespeichert werden."*
  - Umgesetzt in § 113a, Abs. 8 TKG

Frühjahrs Fach2008 Gespräch

Vorratsdatenspeicherung Was wird gespeichert? (2)

- Telefonfestnetz:
  - Rufnummer des Anrufenden/Angerufenen, einschließlich der Rufnummern von Weiterleitungen
  - Name und Anschrift des Angerufenen/Anrufenden
  - Datum und Uhrzeit des Beginns und des Endes der Kommunikation
  - Genutzter Telefondienst

- Mobilfunk *zusätzlich*:
  - Teilnehmerkennung (IMSI)/Gerätekennung (IMEI) des Anrufenden/Angerufenen
  - Standortkennung (Cell-ID) bei Beginn und während des Zeitraums der Erfassung einer Verbindung
  - Bei anonymen Diensten: Datum, Uhrzeit und Kennung (Cell-ID) des Standortes der ersten Aktivierung

Vorratsdatenspeicherung Was wird gespeichert? (3)

- Internet-Telefonie:
  - Internetprotokolladresse des Anrufenden/Angerufenen

Vorratsdatenspeicherung Was wird gespeichert? (4)

- Internetzugang:
  - Zugewiesene Internetprotokolladresse
  - Datum und Uhrzeit des Beginns und Endes der Internetnutzung
  - Rufnummer des Wahlanschlusses / des digitalen Teilnehmeranschluss (DSL) für den Zugang

Vorratsdatenspeicherung Was wird gespeichert? (5)

- Kommunikation per elektronischer Post:
  - Versand einer Nachricht
    - Kennung des elektronischen Postfachs / der Internetprotokolladresse des Absenders
    - Kennung des elektronischen Postfachs jedes Empfängers
    - Datum und Uhrzeit des Versandes
  - Eingang einer Nachricht
    - Kennung des elektronischen Postfachs des Absenders und des Empfängers
    - Internetprotokolladresse der absendenden Telekommunikationsanlage
    - Datum und Uhrzeit des Eingangs
  - Zugriff auf das elektronische Postfach
    - Kennung des Postfachs
    - Internetprotokolladresse des Abrufenden
    - Datum und Uhrzeit des Zugriffs

Vorratsdatenspeicherung Datenschutz?

- Art. 7, Satz a): So gut und sicher wie im Netz ;)
  "Die auf Vorrat gespeicherten Daten sind von der gleichen Qualität und unterliegen der gleichen Sicherheit und dem gleichen Schutz wie die im Netz vorhandenen Daten [...]"
- Art. 7, Satz c): Geeignete technische und organisatorische Maßnahmen zum Schutz der Daten
- Art. 7, Satz d): Daten werden am Ende ihrer Vorratsspeicherfrist vernichtet
  Ausnahme: Daten, die abgerufen oder gesichert wurden

Frühjahrs Fach2008 Gespräch

Vorratsdatenspeicherung Verfassungsbeschwerde

- Verfassungsbeschwerde von mehr als 30.000 Personen
- Eingereicht am 31. Dezember 2007
- Acht Beschwerdeführer
- Eilantrag auf Aussetzung

- Verstoß der Vorratsdatenspeicherung gegen:
  - Fernmeldegeheimnis, Recht auf informationelle Selbstbestimmung (Artikel 10 Abs. 1 Var. 3 GG und Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs.1 GG)
  - Berufsfreiheit (Artikel 12 Abs. 1 GG)
  - Eigentumsgarantie (Artikel 14 Abs. 1 GG)
  - Meinungsfreiheit, Informationsfreiheit, Rundfunkfreiheit und Pressefreiheit (Artikel 5 Abs. 1 GG)
  - Allgemeinen Gleichheitssatz (Artikel 3 Abs. 1 GG)

Vorratsdatenspeicherung Aktuelle Folgen

- Umsetzung bisher nicht erfolgt
  - Beispiel Deutsche Telekom
    - Bisher keine Speicherung
    - Noch in "Evaluationsphase" ;)
    - Umsetzung etwa zu Mitte 2008
- Aber: schlechte Stimmung, große Verunsicherung
  - Rückgang der Anrufe bei Telefonseelsorge
  - Patienten widersprechen telefonischer Beratung
  - Verbot der privaten PC-Nutzung am Arbeitsplatz
  - Persönliche Gespräche anstelle von E-Mail/Telefon
  - ...

Frühjahrs Fach2008 Gespräch

Vorratsdatenspeicherung und BVerfG, 1 BvR 370/07 v. 27.2.2008

- Persönlichkeitsgefährdungen bei der Internetnutzung, die nicht nur durch die **Auswertung** von **Kommunikationsinhalten**, sondern auch durch die von **Verkehrsdaten** entstehen können (RZ 179): *"Durch die Speicherung und Auswertung solcher Daten über das Verhalten des Nutzers im Netz können weitgehende Kenntnisse über die Persönlichkeit des Nutzers gewonnen werden."*

- Auch die **Umstände der Telekommunikation** sind bereits durch Artikel 10 des Grundgesetzes (GG) **geschützt** (RZ 183): *"Zudem sind nicht nur die Inhalte [...] geschützt, sondern [...] auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann und wie oft zwischen welchen Personen [...] Telekommunikationsverkehr stattgefunden hat [...]."*

- Ist die Vorratsdatenspeicherung damit schon vor dem Aus?

Vorratsdatenspeicherung: Bemerkenswert ;)

Das kluge Eichhörnchen traut niemandem.

Fühlt sich der Nager beobachtet,
legt er auch Scheinvorräte an.

(In: "Die Welt" vom . Januar 2008)

Frühjahrs Fach2008 Gespräch

Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationsformen
- Richtlinie 2006/24/EG – die "Vorratsdatenspeicherung"
  - Hintergründe
  - Auswirkungen
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Problemfelder
- Fazit und Diskussion

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung Ist das noch ein Thema?

- Entscheidung des Bundesverfassungsgerichts zum "VSG NRW" vom 27. Februar 2008 (BVerfG, 1 BvR 370/07 v. 27.2.2008)
  - Online-Durchsuchung unter strengen Auflagen zulässig
    - Konkrete Gefahr für überragend wichtiges Rechtsgut
    - Richtervorbehalt
    - Schutz Kernbereich privater Lebensgestaltung
  - Neues Grundrecht "Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systemen"
- Technische Umsetzung immer noch offen
- JA, das ist definitiv noch ein Thema!

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung "Wer, wie, was"

- Grundlage im BKA-Gesetz
  - "Online-Durchsuchung" nur ein kleiner Teil
- Was beinhaltet die Online-Durchsuchung?
  - Online-Durchsicht (OD), Online-Überwachung (OÜ)
  - Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)
- Wie wird eine Online-Durchsuchung durchgeführt?
  - Verdeckte, heimliche Maßnahme
  - Einsatz einer "Remote Forensik Software" (RFS)
- Ein Ziel, verschiedene Ziele :)
  - Abwehr "...konkreter Bedrohungen..."
  - Alle denkbaren "informationstechnischen Systeme"
  - Zugriff auf alle [verschlüsselten] Daten

Online-Durchsuchung Entwurf zum BKA-Gesetz

- Online-Durchsuchung (§ 20k):
  "(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen durch den automatisierten Einsatz technischer Mittel aus informationstechnischen Systemen Daten erheben, soweit die Abwehr der dringenden Gefahr oder die Verhütung von Straftaten gemäß § 4a Abs. 1 Satz 2 auf andere Art und Weise aussichtslos oder wesentlich erschwert wäre."

- Außerdem im BKA-Gesetz geregelt:
  - Erkennungsdienstliche Maßnahmen (§ 20e)
  - Besondere Mittel der Datenerhebung (§ 20g)
  - Einsatz technischer Maßnahmen in Wohnungen (§ 20h)
  - Rasterfahndung (§ 20j)
  - Überwachung der Telekommunikation (§ 20l, § 20m)
  - Identifizierung und Lokalisierung von Mobilfunkgeräten (§ 20n)

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung Vorermittlungen?

- "Ermittlungen" vor Start einer Online-Durchsuchung
- Begleitende Telekommunikationsüberwachung
  - Name und Anschrift der Person
  - Standort des Internet-Anschlusses
  - Alle genutzten Mobilfunk-Provider
- Weitere *persönliche Informationen* über diese Person durch "Social Engineering"
- Sinnhaftigkeit als Mittel gegen "konkrete Gefahren"?

Online-Durchsuchung
Wie kann man eine RFS einbringen?

- Zahlreiche Möglichkeiten vorhanden:
  - "Unwissentliche Mitwirkung der Zielperson"
  - Viren, Trojaner und andere Malware
  - Vorhandene Schwachstellen ausnutzen
  - Vergiften von Software-Downloads
  - "Hintertüren ab Werk" in Soft- und Hardware
  - Hinterlegen von Master-Schlüsseln (Key-Escrow)
  - ...
- Zum Teil erhebliche Nebenwirkungen:
  - Vertrauensverlust in IT-Strukturen
  - Verbreitung von "unbekannten" Schwachstellen
  - Haftungsproblematik

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung DOs and DON'Ts

- Was man machen könnte:
  - Nutzen der Kommunikationsinfrastruktur ...
    - zur Informationsgewinnung mittels TKÜ.
    - zum Einschleusen der Überwachungssoftware durch Vergiften -künstlich getriggerter- Software-Downloads.
  - RFS mit Rootkit-Funktionalität vom BIOS/HDD-Firmware/... direkt in den Speicher laden

- Was man besser nicht machen sollte:
  - Nutzen von Remote-Schwachstellen
    - Einfacher Schutz möglich
    - Begrenzte Lebensdauer
    - Gefahr der ungewollten Weiterverbreitung
  - Nutzen von "Phishing"-Methoden
    - Auf Mitwirken der Zielperson angewiesen

Online-Durchsuchung Fiktion und Wirklichkeit

- Eine perfekte RFS ...
  - würde das Zielsystem unbemerkt infiltrieren.
  - wäre (unmodifiziert) wieder verwertbar.
  - hätte eine (ausreichend) "lange" Lebensdauer.
  - wäre unabhängig vom Kommunikationsweg.
  - hätte ein gutes Kosten/Nutzen-Verhältnis.
  - hätte/würde/wäre/...
- Eine realistische RFS ...
  - ist entdeckbar.
  - ist (unmodifiziert) nicht (häufig) wieder verwertbar.
  - hat eine begrenzte Lebensdauer.
  - hat kein gutes Kosten/Nutzen-Verhältnis.
  - ...

Frühjahrs Fach2008 Gespräch

Mögliche Probleme in Bezug auf (heimliche) Online-Durchsuchungen

- Wird überhaupt das gewünschte Ziel durchsucht?
- Wie werden die Daten klassifiziert?
- Was passiert, wenn eine RFS analysiert wird?
- Werden durch eine RFS Schwachstellen eingebracht?
- Sind die Daten vor Gericht verwertbar?
- Verfassungsmäßigkeit heimlicher Maßnahmen?
- ...

Online-Durchsuchung Untersucht die RFS das richtige Ziel?

- Es wird immer nur das informationstechnische Gerät, nicht aber die daran agierende Person identifiziert!

- Lokalisierung (Land / Stadt) des IT-Systems
  - Beispiel: GeoIP von http://www.maxmind.com
  - Genauigkeit mäßig, daher begleitende TKÜ notwendig
  - Probleme bei grenzüberschreitender Kommunikation

- Probleme bei gemeinschaftlicher Nutzung
  - Verwendung von NAT (SOHO-Installationen, ...)
  - Internet-Cafes

Online-Durchsuchung
Wie werden die Daten klassifiziert?

- Eine automatisierte Klassifikation (Daten gehören der Zielperson, Daten sind relevant) auf einem entfernten System ist rein technisch nicht (sicher) möglich.

- Die Daten müssten aber bereits vor dem Versand an den Zentralrechner klassifiziert werden (Datenschutz)!

- Besonders problematisch bei:
  - Gemeinsamer Nutzung eines IT-Systems (zum Beispiel Daten unbeteiligter Privatpersonen)
  - Per Internet eingebundenen Datenquellen Dritter (zum Beispiel Daten des Arbeitgebers)
  - Höchstpersönlichen Daten, die nicht relevant sind

Online-Durchsuchung Neue Schwachstellen?

- Existiert ein offener Port zur Kommunikation?
  - Wäre (auch von außen) identifizierbar
  - Enthüllt Existenz einer RFS
  - Bietet Informationen für Angriff auf eine RFS
- Programmierfehler in einer RFS können nicht ausgeschlossen werden
  - Die RFS kann DIE Schwachstelle eines IT-Systems sein!
- Wer haftet für eventuelle Schäden?
  - Digitale Signatur, E-Commerce, Online-Banking
  - Löschung / Manipulation von Daten Unbeteiligter
  - Haftung durch die Ermittlungsbehörde?
    - Staatshaftung (§ 839 BGB in Verbindung mit Art. 4 GG)?

Online-Durchsuchung Analysierbarkeit einer RFS?

- Analyse einer RFS ist möglich
  - Vollständiger Schutz auch durch Kryptographie unmöglich
  - Analyse durch (Auffälligkeiten im) Netzwerkverkehr
  - Analyse durch (Auffälligkeiten in der) Systemfunktion
- Analyse der RFS zeigt deren Funktion
  - Missbrauch / Nachbau / Modifikation durch Kriminelle
- Sicheres / vollständiges Löschen im Notfall?
  - Bestehendes Backup?
  - Kommunikationsports zur Steuerung?
  - Verwendung von NAT (SOHO-Installationen, ...)?

Online-Durchsuchung Gibt es Schutzmaßnahmen?

- JA, und diese sind zum Teil sehr einfach umzusetzen!
- Zahlreiche Varianten möglich:
  - Booten von "vertrauenswürdigen" Medien
    - Knoppix-CD, USB-Stick, ...
  - Nutzung von zwei getrennten PCs
    - PC-1 am Internet, PC-2 ohne Netzanbindung
  - Nutzung wechselnder, zufälliger Kommunikationswege
    - Wechselnde Internet-Cafes, Handys, ...
  - Nutzung von Open Source Komponenten
  - Nutzung kryptographischer Methoden
  - ...
- Fazit: Wer sich schützen will, kann das tun!

Online-Durchsuchung Es gibt Schutzmaßnahmen!

- Diese sind sehr einfach umzusetzen!
- Zahlreiche Varianten möglich:
  - Booten von "vertrauenswürdigen" Medien
    - Knoppix-CD, USB-Stick, ...
  - Nutzung von zwei getrennten PCs
    - PC-1 am Internet, PC-2 ohne Netzanbindung
  - Nutzung wechselnder, zufälliger Kommunikationswege
    - Wechselnde Internet-Cafes, Handys, ...
  - Nutzung von Open Source Komponenten
  - Nutzung kryptographischer Methoden
  - ...
- Fazit: Wer sich schützen will, muss das tun!

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung Verwertbarkeit der Daten?

- Grundlage der IT-Forensik:
  - Das zu untersuchende System darf nicht mehr verändert werden, es wird nur an binären "1:1-Kopien" gearbeitet
- Erhebliche Probleme:
  - Allein das Einbringen einer RFS verändert das System
  - Das System lebt während der Laufzeit der RFS weiter, Daten werden sich daher laufend verändern
- Authentizität einer RFS?
  - Wie wird dies gewährleistet?
  - Wer kann das überhaupt kontrollieren?
- Allerdings: Präventive *versus* repressive Maßnahmen!

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung Verfassungsmäßigkeit?

- Kernbereich der privaten Lebensgestaltung
  - Eingriff durch Art. 1 Abs. 1 GG verboten
  - Regelung in BKA-Gesetz § 20v: *"[(2) Eine Maßnahme nach § 20k darf nur unter Verwendung von Suchbegriffen angeordnet werden, die nicht zur Erfassung von Inhalten aus dem Kernbereich privater Lebensgestaltung führen.]"*
- Unverletzlichkeit der Wohnung
  - Geregelt in Art. 13 Abs. 1 GG
  - Gilt auch für eine rein technische Überwachung
  - Gilt auch für mit dem Internet vernetzte Computer (vgl. BVerfG, 1 BvR 370/07 v. 27.2.2008 RZ 194)
- Informationelle Selbstbestimmung
  - Offene *versus* verdeckte Durchsuchung
  - Verhältnismäßigkeit des Eingriffs?

Frühjahrs Fach2008 Gespräch

Online-Durchsuchung
Aus aktuellem Anlass :)

- Entscheidung des Bundesverfassungsgerichts zum "VSG NRW" vom 27. Februar 2008 (BVerfG, 1 BvR 370/07 v. 27.2.2008)
  - Online-Durchsuchung unter strengen Auflagen zulässig
    - Konkrete Gefahr für überragend wichtiges Rechtsgut
    - Richtervorbehalt
    - Schutz Kernbereich privater Lebensgestaltung
  - Neues Grundrecht "Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systemen"

- Aber: Technische Umsetzung immer noch offen
- Aber: Viele offene Fragen und Probleme

- JA, das ist und bleibt definitiv noch ein Thema!

Online-Durchsuchung: Ein Blick in die Zukunft ;)

Quelle: vorwärts, Ausgabe 10/2007, Seite 47

Frühjahrs Fach2008 Gespräch

Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerpragraph"
  - Hintergründe
  - Interpretationsformen
- Richtlinie 2006/24/EG – die "Vorratsdatenspeicherung"
  - Hintergründe
  - Auswirkungen
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Problemfelder
- Fazit und Diskussion

Fazit und Diskussion

- Schlussfolgerungen
  - Verunsicherung der IT-Branche
  - "Brüssel macht was es will und keiner bekommt es mit"
- Empfehlungen
  - Informieren, informieren, informieren! ;)
  - Keine Kurzschlussreaktionen!
- Diskussion ist wichtig! :)

Frühjahrs Fach2008 Gespräch

Weitere Informationsquellen (1) Hackerparagraph

- Rahmenbeschluss des Europarates 2005/222/JI
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:DE:PDF
- European Cybercrime Convention ("Budapest Convention")
  http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
- Bundestags-Drucksache 16/3656: Gesetzentwurf zum StrÄndG
  http://dip.bundestag.de/btd/16/036/1603656.pdf

- Stellungnahme des DFN-Vereins zum StrÄndG
  http://www.dfn.de/fileadmin/3Beratung/Recht/Stellungnahme06-11-24.pdf
- Informationsbroschüre der eicar zum StrÄndG
  http://www.eicar.org/press/infomaterial/JLUSSI_LEITFADEN_web.pdf

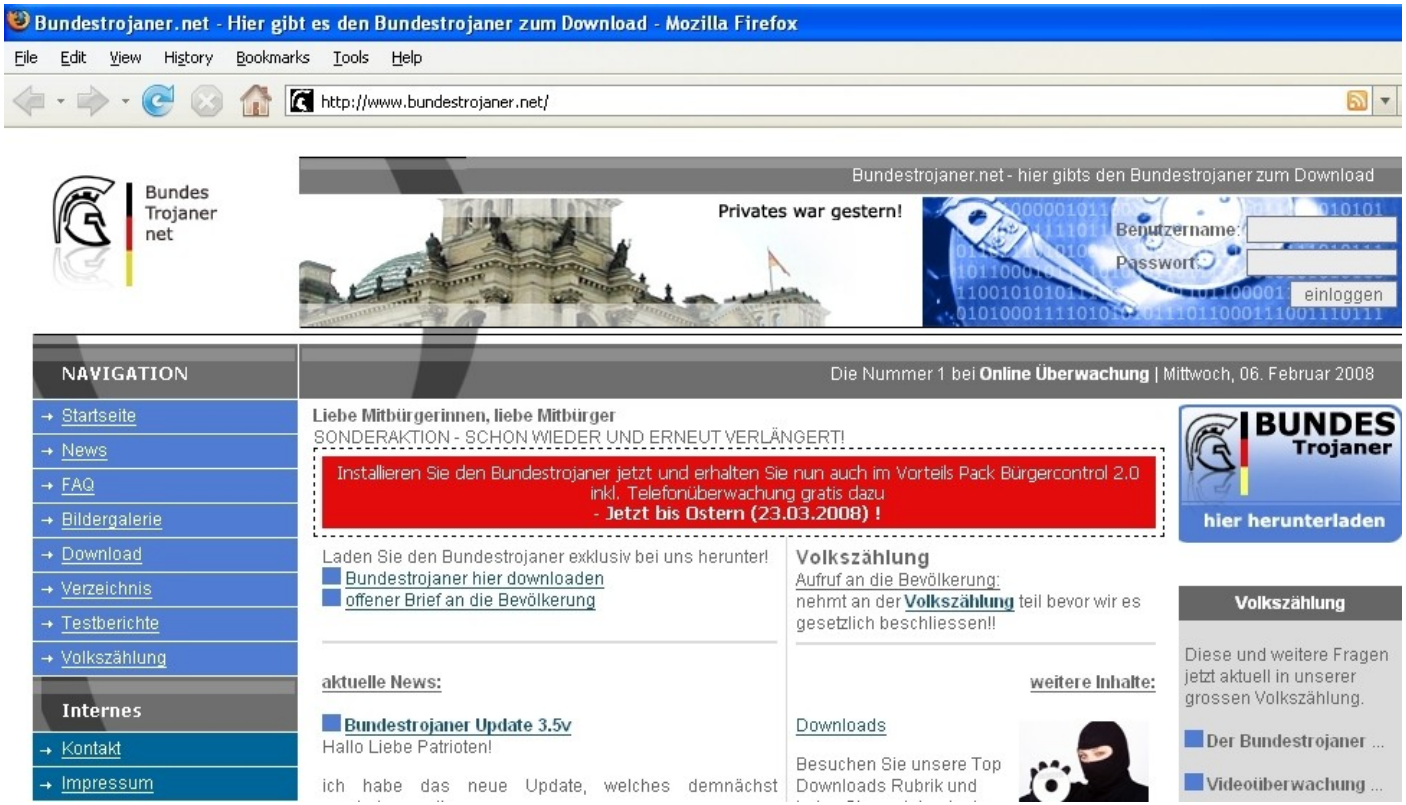
- Borges, G.; Stuckenberg, C.-F.; Wegener, C.: "Zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität". In: DuD – Datenschutz und Datensicherheit 31 (2007) 4, 275-278.

Weitere Informationsquellen (2) Vorratsdatenspeicherung

- Richtlinie 2006/24/EG des Europarats vom 15. März 2006
  http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2006/l_105/l_10520060413de00540063.pdf
- Bundestags-Drucksache 16/5846 vom 27. Juni 2007
  http://dip.bundestag.de/btd/16/058/1605846.pdf
- Verfassungsbeschwerde vom 31. Dezember 2007
  http://wiki.vorratsdatenspeicherung.de/images/Verfassungsbeschwerde_Vorratsdatenspeicherung.pdf

Weitere Informationsquellen (3) Online-Durchsuchung

- Webseite zum Bundestrojaner ;)
  http://www.bundestrojaner.net



Frühjahrs Fach2008 Gespräch

Weitere Informationsquellen (4) Online-Durchsuchung

- Referentenentwurf zum BKA-Gesetz vom 7. Juli 2007
  http://www.ccc.de/lobbying/papers/terrorlaws/20070711-BKATERROR.pdf
- "Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (VSG NRW)"
  http://www.im.nrw.de/sch/doks/vs/vsg_nrw_2007.pdf

- Hansen, M., Pfitzmann, A. und Roßnagel, A.: "Online-Durchsuchungen"
  http://www.heymanns.com/servlet/PB/menu/1226897/index.html
- Pohl, J.: "Zur Technik der heimlichen Online-Durchsuchung".
  In: DuD – Datenschutz und Datensicherheit 31 (2007) 9, 684-688.

- Fragenkatalog des Bundesjustizministeriums
  http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf
- Fragenkatalog der SPD-Fraktion
  http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-SPD.pdf
- Bundestags-Drucksache 16/4997: "Online-Durchsuchungen"
  http://dip.bundestag.de/btd/16/049/1604997.pdf

- Wegener, C.: Hintergründe zum Vorhaben "Online-Durchsuchung"
  http://www.wecon.net/de/downloads/downloads.html?id=14

Danke für Ihre Aufmerksamkeit :)

Haben Sie Fragen?

- Kontakt per E-Mail: wegener@wecon.net
- Mehr Infos im Web: www.wecon.net