# SAGE/GUUG-Treffen in Hamburg

## Hackerparagraph und Online-Durchsuchung

### aka: Rechtsunsicherheit in der IT-Branche

**Dr. Christoph Wegener**
**wecon.it**-consulting

Hamburg, 8. Mai 2008

# 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

# Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
  - Probleme aus der Praxis
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Technische Möglichkeiten
  - Technische und juristische Probleme
- Fragen und Diskussion

# Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
  - Probleme aus der Praxis
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Technische Möglichkeiten
  - Technische und juristische Probleme
- Fragen und Diskussion

# "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

# "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" Hintergründe (3)

- § 202a StGB – *"Ausspähen von Daten"*:
  *"(1) Wer **unbefugt** sich oder einem anderen Zugang zu Daten, die **nicht für ihn bestimmt** und die gegen unberechtigten Zugang **besonders gesichert** sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.*
  *(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden."*

- § 202b StGB – *"Abfangen von Daten"*:
  *"Wer **unbefugt** sich oder einem anderen unter Anwendung von technischen Mitteln **nicht für ihn bestimmte Daten** (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist."*

# "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 [...]"*

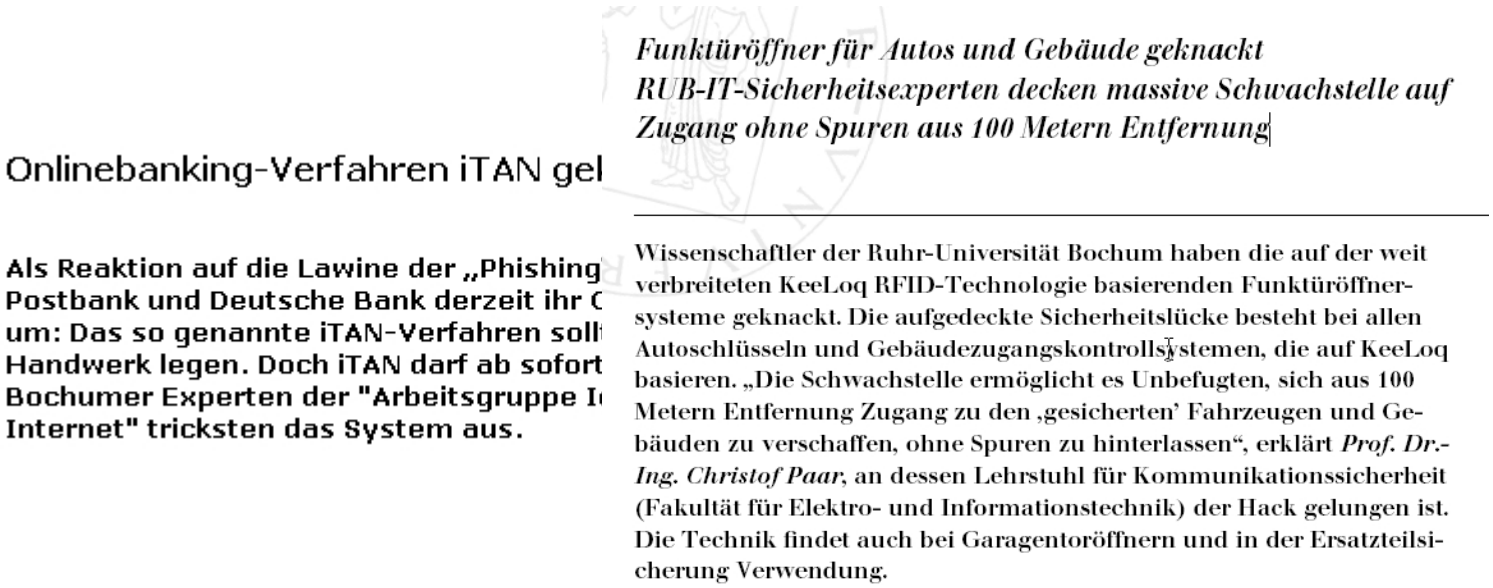
- Was machen die anderen Länder
  - Österreich hat eine klarere Regelung – § 126c ÖStgB:
    *"[...]* ***mit dem Vorsatz*** *herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie* ***zur Begehung einer der in Z 1 genannten strafbaren Handlungen*** *gebraucht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

# "Hackerparagraph" Probleme (4)

- Forschung im Bereich der IT-Sicherheit



Onlinebanking-Verfahren iTAN gel

Als Reaktion auf die Lawine der „Phishing
Postbank und Deutsche Bank derzeit ihr
um: Das so genannte iTAN-Verfahren soll
Handwerk legen. Doch iTAN darf ab sofort
Bochumer Experten der "Arbeitsgruppe I
Internet" tricksten das System aus.

*Funktüröffner für Autos und Gebäude geknackt*
*RUB-IT-Sicherheitsexperten decken massive Schwachstelle auf*
*Zugang ohne Spuren aus 100 Metern Entfernung*

Wissenschaftler der Ruhr-Universität Bochum haben die auf der weit verbreiteten KeeLoq RFID-Technologie basierenden Funktüröffnersysteme geknackt. Die aufgedeckte Sicherheitslücke besteht bei allen Autoschlüsseln und Gebäudezugangskontrollsystemen, die auf KeeLoq basieren. „Die Schwachstelle ermöglicht es Unbefugten, sich aus 100 Metern Entfernung Zugang zu den ‚gesicherten' Fahrzeugen und Gebäuden zu verschaffen, ohne Spuren zu hinterlassen", erklärt *Prof. Dr.-Ing. Christof Paar*, an dessen Lehrstuhl für Kommunikationssicherheit (Fakultät für Elektro- und Informationstechnik) der Hack gelungen ist. Die Technik findet auch bei Garagentoröffnern und in der Ersatzteilsicherung Verwendung.

- Sind §§ 202a|b und/oder 202c StGB einschlägig?
- Was wird die Zukunft bringen?
- Gefahr für den (Forschungs-)Standort Deutschland?

# "Hackerparagraph" Schlussfolgerungen

- Trotzdem: Keine Panik, keine Panik, keine Panik! :)
  - Unklarheiten lassen sich (oft stark) 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
- Aber: Offene Fragen
  - Weitergabe an unbekannten Personenkreis
  - Problem der Abgrenzung Hackertools <-> Dual-Use-Tools
  - Freie Forschung im Bereich der IT-Sicherheit?

# 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.

# Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
  - Probleme aus der Praxis
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Technische Möglichkeiten
  - Technische und juristische Probleme
- Fragen und Diskussion

# 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!

# Hintergründe 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 Forensic Software" (RFS)
- Ein Ziel, verschiedene Ziele :)
  - Abwehr "...konkreter Bedrohungen..."
  - Alle denkbaren "informationstechnischen Systeme"
  - Zugriff auf alle [verschlüsselten] Daten

# Hintergründe Online-Durchsuchung Entwurf zum BKA-Gesetz (16. April 2008)

- "Abwehr von Gefahren des internationalen Terrorismus" (§ 4a)
- Kennzahlen
  - Geplante Personalstellen beim BKA: 130
  - Anlaufkosten: Euro 23,6 Mio, dann pro Jahr: Euro 10,2 Mio
- Unter anderem 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)
  - Sicherstellung (§ 20s)
  - Betreten und Durchsuchen von Wohnungen (§ 20t)

# Hintergründe Online-Durchsuchung Entwurf zum BKA-Gesetz (16. April 2008)

- Online-Durchsuchung (§ 20k):

*"(1) Das Bundeskriminalamt darf **ohne Wissen des Betroffenen** mit **technischen Mitteln** in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass eine Gefahr vorliegt für*

1. *Leib, Leben oder Freiheit einer Person oder*
2. *solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.*

*Eine Maßnahme nach Satz 1 ist auch **zulässig**, wenn sich noch **nicht mit hinreichender Wahrscheinlichkeit** feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt [...]. Die Maßnahme darf nur durchgeführt werden, wenn sie für die Aufgabenerfüllung nach § 4a erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.*

*(2) ..."*

# Vorgehen bei der 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"
- Mittel gegen "konkrete Gefahren"?

# Vorgehen bei der 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)
  - Vor-Ort-Installation
  - ...
- Zum Teil erhebliche Nebenwirkungen:
  - Vertrauensverlust in IT-Strukturen
  - Verbreitung von "unbekannten" Schwachstellen
  - Haftungsproblematik

# Vorgehen bei der Online-Durchsuchung Infektion durch Software-Download

- Voraussetzungen
  - Angreifer kontrolliert den Datenweg des Downloads (Mirror, Proxy, ISP-Netzwerk, ...)
  - Nutzer verwendet keine kryptographischen Prüfsummen (Dazu: Was/wo sind valide Prüfsummen?)

- Vorgehensweise
  - Der Nutzer lädt ein (erzwungenes) Update
  - Angreifer lenkt Download per ARP-/DNS-Spoofing um
  - Angreifer schiebt dem Nutzer eine trojanisierte Datei unter
  - Schadfunktion installiert sich beim Update

# Vorgehen bei der 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

# Vorgehen bei der 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.
  - ...

# 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?
- ...

# Probleme der 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

# Probleme der 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)!
- Das hat auch das BVerfG erkannt (RZ 277 ff)

- 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

# Probleme der 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. 34 GG)?

# Probleme der 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, ...)?

# Probleme der 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!

# Lösungen zur 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!

# Probleme der 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!

# Probleme der Online-Durchsuchung Auswirkungen des BVerfG-Urteils (1)

- Kernbereich der privaten Lebensgestaltung
  - Eingriff durch Art. 1 Abs. 1 GG verboten
  - Regelung in BKA-Gesetz § 20k: *"(7) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch die Maßnahme **allein** Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. **Soweit möglich** ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [...] Daten die den Kernbereich privater Lebensgestaltung betreffen, dürfen **nicht verwertet** werden und sind **unverzüglich zu löschen**. [...]"*

- Regelung entspricht wohl dem Urteil des BVerfG (RZ 280ff)
  - RZ 281: Technischer Schutz, dass Daten nicht erhoben werden
  - RZ 282: Wenn Daten erhoben, sofortige Löschung

# Probleme der Online-Durchsuchung Auswirkungen des BVerfG-Urteils (2)

- 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)

- Aber im Urteil des BVerfG zum VSG NRW (RZ 194):
  *"Art. 13 Abs. 1 GG vermittelt dem Einzelnen allerdings **keinen generellen**, **von den Zugriffsmodalitäten unabhängigen Schutz** gegen die Infiltration seines informationstechnischen Systems [...] Soweit die Infiltration die Verbindung des betroffenen Rechners zu einem Rechnernetzwerk ausnutzt, lässt sie die durch die Abgrenzung der Wohnung vermittelte räumliche Privatsphäre unberührt. Der Standort des Systems wird in vielen Fällen für die Ermittlungsmaßnahme ohne Belang und oftmals für die Behörde nicht einmal erkennbar sein. Dies gilt insbesondere für mobile informationstechnische Systeme wie etwa Laptops, Personal Digital Assistants (PDAs) oder Mobiltelefone."*

# Hintergründe Online-Durchsuchung Urteil des BverfG

- 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
# Schlussfolgerungen und Fazit

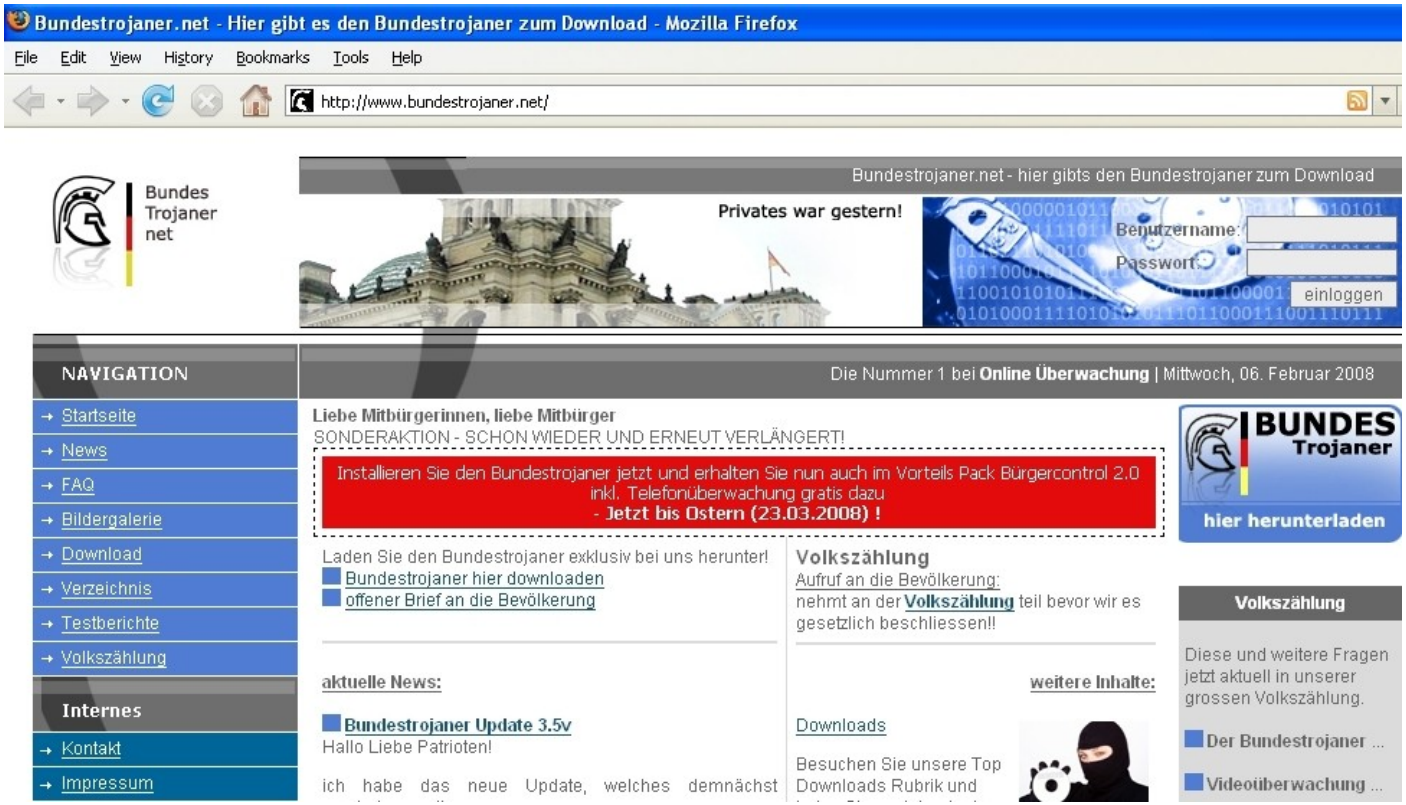
- Zu viele offene Fragen und Probleme
  - Einbringen einer RFS, richtige Zielperson
  - Gibt es zusätzliche Schwachstellen?
  - Verwertbarkeit der Daten, Haftungsfragen
- Heimliche Online-Durchsuchungen nach aktueller Auffassung unter Auflagen verfassungsgemäß!
- Sinnhaftigkeit einer (heimlichen) Online-Durchsuchung nach aktueller Vorstellung aber mehr als fraglich!
- Aber: Schutz ist einfachst möglich
  - Booten von sicheren Medien
  - Nutzung multipler Kommunikationswege

# Zukunft der Online-Durchsuchung: Ein Blick in die Zukunft ;)


Quelle: vorwärts, Ausgabe 10/2007, Seite 47

# Weitere Informationsquellen (1) Online-Durchsuchung

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



# Weitere Informationsquellen (2) 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

- Urteil des BverfG zum VSG NRW vom 27. Februar 2008
  http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

# Was werde ich heute vorstellen?

- § 202c StGB – der "Hackerparagraph"
  - Hintergründe
  - Interpretationen
  - Probleme aus der Praxis
- § 20k BKAG – die "Online-Durchsuchung"
  - Hintergründe
  - Technische Möglichkeiten
  - Technische und juristische Probleme
- Fragen und Diskussion

# Danke für Ihre Aufmerksamkeit :)

Haben Sie Fragen?

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