15. DFN-Cert Workshop "Sicherheit in vernetzten Systemen"

Hintergründe zum Vorhaben Online-Durchsuchung

Überflüssig oder unverzichtbar?

Dr. Christoph Wegener
Horst Görtz Institut für IT-Sicherheit

Hamburg, 14. Februar 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, CBP
- Fachautor/-lektor/-gutachter
- Verschiedene Lehrtätigkeiten

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

Was werde ich Ihnen vorstellen?

- "Wer, wie, was" der Online-Durchsuchung
  - Begriffsdefinitionen
  - Zielsetzung einer Online-Durchsuchung
- Technische und juristische Aspekte
  - Installation und Funktion
  - Schutzmaßnahmen
  - Problemstellen
    - Gerichtsverwertbarkeit der Daten
    - Haftungsproblematik
    - Online-Durchsuchung im Ausland
    - Verfassungsmäßigkeit heimlicher Maßnahmen
- Schlussfolgerungen und Fazit

Hintergrund (1)
"Wer, wie, was" der Online-Durchsuchung

- 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

Hintergrund (2)
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)

Hintergrund (3)
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"?

Technische Aspekte (1)
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

Technische Aspekte (2)
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

Technische Aspekte (3)
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
- Praxisdemo

Technische Aspekte (4)
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 (1)
Untersucht eine RFS das gewünschte 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 (2)
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

Probleme (3)
Neue Schwachstellen durch eine RFS?

- 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 (4)
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 (5)
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 (1)
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 (6)
Verwertbarkeit der Daten vor Gericht?

- 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 (7)
Verfassung und heimliche Maßnahmen?

- 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

- Informationelle Selbstbestimmung
  - Offene *versus* verdeckte Durchsuchung
  - Verhältnismäßigkeit des Eingriffs?

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 wohl nicht verfassungsgemäß!
- Sinnhaftigkeit einer (heimlichen) Online-Durchsuchung nach aktueller Vorstellung mehr als fraglich!
- Aber: Schutz ist einfachst möglich
  - Booten von sicheren Medien
  - Nutzung multipler Kommunikationswege

Ein Blick in die Zukunft ;)

Quelle: vorwärts, Ausgabe 10/2007, Seite 47

Weitere Informationsquellen (1)

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

Weitere Informationsquellen (2)

- 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

Danke für Ihre Aufmerksamkeit :)

Haben Sie Fragen?

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