Techniken der Online-Durchsuchung, ihr Gebrauchs- und Missbrauchspotential sowie resultierende Empfehlungen

Prof. Dr. Andreas Pfitzmann

TU Dresden, Fakultät Informatik, D-01062 Dresden
Tel.: 0351/ 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

28. April 2008

Gliederung

1. Technik der Online-Durchsuchung
   1. Infiltrationsmöglichkeiten
   2. Durchsuchungs- und Manipulationsmöglichkeiten
   3. Speicherung und Übertragung der Ergebnisse
   4. De-Infiltration
2. Gebrauchspotential der Online-Durchsuchung
   1. Heutige IT
      1. Naiver IT-Benutzer
      2. Sensibilisierter IT-Benutzer
   2. Künftige IT
      1. Wie IT sich entwickeln sollte
      2. Wie IT sich entwickeln könnte
3. Missbrauchspotential der für die Online-Durchsuchung entwickelten Technik
4. Empfehlung eines Informatikers zur Online-Durchsuchung
5. Technikverständnis von Wählern, Politikern und Richtern
6. Die Perspektive eines Informatikers auf das Urteil

1. Technik der Online-Durchsuchung

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
De-Infiltration	keine	vielleicht		keine

1. Technik der Online-Durchsuchung

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

Frage und Antwort aus der mündl. Verhandlung

- Woher wissen Sie, dass Sie den richtigen Rechner durchsuchen?

- Wenn wir finden, was wir suchen.

2. Gebrauchspotential der Online-Durchsuchung

Heutige IT – naiver IT-Eigennutzer

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

2. Gebrauchspotential der Online-Durchsuchung

Heutige IT – sensibilisierter IT-Eigennutzer:

Von Firewall bis offline betriebene IT

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

2. Gebrauchspotential der Online-Durchsuchung

Künftige IT – wie sie sich entwickeln sollte:

Deutlich mehr Sicherheit, ohne dass Eigennutzer etwas tun muss

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung	Trojanisches Pferd		
	keine	ja		
Speicherung und Übertragung	keine	ja (Steganographie)		
	physische Abstrahlung	physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

2. Gebrauchspotential der Online-Durchsuchung

Künftige IT – wie sie sich entwickeln könnte:

Unsicherheit, wenn sich Eigennutzer um nichts kümmert

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

3. Missbrauchspotential der für Online-Durchs. entw. Technik

Bedarfsträger

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
			Geeignet für Massenüberwachung	
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung	Trojanisches Pferd		
	keine	ja		
Speicherung und Übertragung	keine	ja (Steganographie)		
	physische Abstrahlung	physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

3. Missbrauchspotential der für Online-Durchs. entw. Technik

Fremde Geheimdienste

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung	Trojanisches Pferd		
	keine	ja		
Speicherung und Übertragung	keine	ja (Steganographie)		
	physische Abstrahlung	physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

Geeignet für Massenüberwachung

3. Missbrauchspotential der für Online-Durchs. entw. Technik

Organisierte Kriminalität: wie fremde Geheimdienste

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
			Geeignet für Massenüberwachung	
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung	Trojanisches Pferd		
	keine	ja		
Speicherung und Übertragung	keine	ja (Steganographie)		
	physische Abstrahlung	physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

3. Missbrauchspotential der für Online-Durchs. entw. Technik

Computer-Kids: wie Bedarfsträger

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
			Geeignet für Massenüberwachung	
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung	Trojanisches Pferd		
	keine	ja		
Speicherung und Übertragung	keine	ja (Steganographie)		
	physische Abstrahlung	physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

4. Empfehlung eines Informatikers zur Online-Durchsuchung

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

4. Empfehlung eines Informatikers zur Online-Durchsuchung

Solange es noch geht und nur wenn unbedingt nötig

Infiltration	keine	physischer Zugriff auf Gerät	über Kommun.-Netz	vom Hersteller eingebaut
Durchsuchungs- und Manipulations-möglichkeiten im Gerät	Beobachtung keine	Trojanisches Pferd ja		
Speicherung und Übertragung	keine physische Abstrahlung	ja (Steganographie) physische Abstrahlung, physischer Zugriff auf Gerät, Kommun.-Netz		
	Offene Beschlagnahme des Gerätes			
De-Infiltration	keine	vielleicht		keine

5. Technikverständnis von Wählern, Politikern und Richtern

- **Wähler:** Nur sporadisches Verständnis. Dies wird als Grenze für eigenes Urteil und Handeln akzeptiert.
- **Politiker:** Nur sehr sporadisches Verständnis, führt zu nahezu blindem Vertrauen in „Experten“ von BKA, ...
  - Dr. Wolfgang Schäuble ist stolz, dass er die IT nicht versteht;
  - Jörg Ziercke macht es nichts aus, dass er die IT nicht versteht;
  - die ihnen Unterstellten sind froh darüber, denn es maximiert ihre Macht.
- **Richter:** Bin von der Bereitschaft der BVerfRichter, die IT zu verstehen, insbesondere im Vergleich zu Politikern, absolut begeistert:
  - Erst verstehen, dann entscheiden, statt der Attitüde der Politiker: Verständnis schränkt den Entscheidungsspielraum nur ein ...

Definitionen für die Schutzziele (aus Informatik-Vorlesung)

Vertraulichkeit (confidentiality)

Informationen werden nur Berechtigten bekannt.

Integrität (integrity)

Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

Verfügbarkeit (availability)

Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

- subsumiert: Daten, Programme, Hardwarestrukturen

- es muss geklärt sein, wer in welcher Situation wozu berechtigt ist

6. Die Perspektive eines Informatikers auf das Urteil

- Verfassungsrichter tun das, was Politiker hätten tun sollen: Sich ein eigenes Urteil über IT erarbeiten und danach Verantwortung übernehmen

- Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als
  - Ausprägung des allgemeinen Persönlichkeitsrechts
  - Und nicht etwa als Ausprägung von Art. 10 oder Art. 13 GG

- „IT-Grundrecht“ reicht weit über Online-Durchsuchung hinaus
  - Klarer, als ich je zu hoffen gewagt hätte
  - Auch von überwältigenden Mehrheiten IT-unverständiger Politiker nicht zu ändern
  - Impliziert Recht auf Selbstschutz bei eigengenutzer IT, u.a. Verschlüsselung, Steganographie und Anonymität
  - Verpflichtet den Staat: Gewährleistung statt nur Respektierung
    ⇒ z.B. Bildungsauftrag: IT-mündige Bürger!

Literaturempfehlungen

- Dirk Fox: Realisierung, Grenzen und Risiken der „Online-Durchsuchung“; DuD Datenschutz und Datensicherheit 31 (November 2007) Seite 827-834.
- Markus Hansen, Andreas Pfitzmann: Technische Grundlagen von Online-Durchsuchung und –Beschlagnahme; Deutsche Richterzeitung, August 2007, Seite 225-228.
- Andreas Pfitzmann: Möglichkeiten und Grenzen der Nutzungsüberwachung von Informations- und Kommunikationssystemen in einer freiheitlichen demokratischen Gesellschaft; Informatik-Spektrum 31/1 (Februar 2008) 65-69.
- Hartmut Pohl: Zur Technik der heimlichen Online-Durchsuchung; DuD Datenschutz und Datensicherheit 31 (September 2007) Seite 684-688.