Realisierung, Grenzen und Risiken der Online-Durchsuchung

15. DFN-Workshop „Sicherheit in Vernetzten Systemen“
14.02.2008

Dirk Fox
dirk.fox@secorvo.de

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Oder: Der Feind auf meiner Festplatte

15. DFN-Workshop „Sicherheit in Vernetzten Systemen“
14.02.2008

Dirk Fox
dirk.fox@secorvo.de

secorvo
security consulting

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Inhaltsübersicht

- **Hintergrund**
- Klarstellungen
- Technische Realisierung
- Grenzen und Risiken
- Zusammenfassung und Bewertung

Was bisher geschah...

- **Mai 2005**
  - **Verfassungsschutz wird vom BMI zur Durchführung von Online-Durchsuchungen (OD) ermächtigt**
- **25.11.2006 (veröffentlicht am 31.01.2007)**
  - **BGH untersagt heimliche OD als Mittel der Strafverfolgung (fehlende Rechtsgrundlage)**
- **30.12.2006**
  - **Novelle des Verfassungsschutzgesetzes NRW ermächtigt Landesverfassungsschutz zur Durchführung von OD**
- **09.02.2007**
  - **Verfassungsbeschwerde gegen VerfSchG NRW (Winsemann)**
- **02.03.2007**
  - **Verfassungsbeschwerde gegen VerfSchG NRW (Baum)**

Positionen

- **Dieter Wiefelspütz (SPD)**
  - **„Das Internet ist eine Welt, in der jede Sauerei dieser Welt stattfindet. Die Koalition wird daher mit Augenmaß das Erforderliche tun, um diese Sauereien zu bekämpfen.“**
- **Gero von Randow (Die ZEIT)**
  - **„Wer, der ins Netz geht, weiß denn nicht, dass darin letztlich alles öffentlich ist?“**
- **Monika Harms (Generalbundesanwältin)**
  - **„Insbesondere ist das Anwesenheitsrecht [...] gewahrt, weil der Computernutzer während der Übertragung des zu durchsuchenden Datenbestandes an die Ermittlungsbehörde 'online' sein muss.“**

Inhaltsübersicht

- Hintergrund
- **Klarstellungen**
- Technische Realisierung
- Grenzen und Risiken
- Zusammenfassung und Bewertung

Begriffliche Klarstellungen

- **Online-Durchsuchung**
  - Unbemerkter Zugriff von Strafverfolgungsbehörden auf *informationstechnische Systeme* Verdächtiger
  - Online-Durchsicht: Verdeckte elektronische Durchsuchung
  - Online-Überwachung: Verdeckte elektronische Beobachtung
  - „Remote Forensic Software“ (RFS)
- **Quellen-Telekommunikationsüberwachung**
  - Unbemerkter Zugriff auf die Inhalte elektronischer Kommunikation (E-Mail, digitale Telefonie), die herkömmlicher TKÜ-Maßnahme nicht zugänglich sind (Verschlüsselung)
- **Informationstechnische Systeme**
  - Personalcomputer, Laptops
  - PDAs, SmartPhones, MP3-Player, ...
  - Herzschrittmacher? Medizinische Analysegeräte? ...

Perspektive Strafverfolgung

- **Grenzen der Telekommunikationsüberwachung**
  - Anonyme Einträge in Online-Foren, Chats
  - Übermittlung verschlüsselter Daten
  - Verschlüsselte elektronische Kommunikation (E-Mail)
  - Digitale Telefonie über sichere Protokolle (VPN, Skype)
- **Grenzen von Beschlagnahme und Durchsuchung**
  - Gelöschte Nachrichten und Dokumente (sofern nicht nur „oberflächlich“ gelöscht)
  - Verschlüsselt gespeicherte Daten
  - Fehlende Identifikationsmöglichkeit von „getarnten“ Systemen (z.B. missbräuchliche Nutzung von WLANs Dritter)
  - Daten auf leicht zerstör- oder löschbaren Systemen oder Medien (Smartphone mit Sofortlöschung, USB-Stick etc.)
  - Ende aller verdeckten Maßnahmen

Verhältnismäßigkeitsprinzip

- **Zweck: Wird mit der Maßnahme ein *legitimer* und vor allem *konkret benannter Zweck* verfolgt?**
- **Eignung: Ist die *Maßnahme geeignet*, diesen Zweck zu erreichen?**
- **Erforderlichkeit: Ist die *Maßnahme erforderlich*, d.h. gibt es keine mindestens ebenso geeignete Maßnahme, die den Betroffenen weniger belastet?**
- **Angemessenheit: Ist die Maßnahme auch verhältnis-mäßig im engeren Sinne, d.h. *überwiegen die Vorteile* der Maßnahme?**

Inhaltsübersicht

- Hintergrund
- Klarstellungen
- **Technische Realisierung**
- Grenzen und Risiken
- Zusammenfassung und Bewertung

Analyse des Zielsystems

- **Detailkenntnisse des Zielsystems erforderlich**
  - **Betriebssystem (Hersteller, Version, Patch-Stand)**
  - **Internet-Zugang (Einwahl oder DSL, Provider)**
  - **Genutzte Schutzsoftware (Virenschutz, Personal Firewall, Verschlüsselungssoftware etc.; ebenfalls mit Versionsstand)**
  - **Sicherheitskonfiguration (Rechte des Nutzers auf dem System, Konfiguration der Schutzsoftware)**
  - **Genutzte Kommunikationsdienste, verwendete Software (z. B. VoIP, E-Mail, Browser)**
  - **Benutzerverhalten (Art, Zeitpunkt, Häufigkeit der Nutzung des Internet-Zugangs)**
  - **Verbundene Systeme (lokales Netz, Server etc.)**
- **➔ Gewinnung aller erforderlichen Kenntnisse nur bei direktem Zugriff möglich**

Installation OD-Software (1)

- **Entfernte manuelle Installation**
  - Ausnutzung unsicherer Konfiguration des Zielsystems
  - Keine Mitwirkung des Benutzers erforderlich
- **Automatische Hintergrund-Installation**
  - Installation wird in anderem Prozess „versteckt“
  - Unbewusste Mitwirkung des Benutzers erforderlich
  - ➔ Installation über infizierte Webseite
    - Skript-Steuerung, nutzt unsichere Browser-Konfiguration
    - Erfordert Besuch der Webseite durch den Benutzer
  - ➔ Installation über ein Update
    - Manipulation und Zusendung eines Software-Updates
    - Mitwirkung des Benutzers erforderlich

Installation OD-Software (2)

- ➔ Installation über einen E-Mail-Anhang
  - Installation wird beim Öffnen eines E-Mail-Anhangs gestartet
  - Mitwirkung des Benutzers erforderlich
- ➔ Installation über CD/DVD oder USB-Stick
  - Installation über Autostart-Mechanismus
  - Erfordert Mitwirkung des Benutzers

- **Einbau einer „Backdoor“**
  - Verbreitete Standard-Software mit „OD-Schnittstelle“
  - Mitwirkung mindestens eines Herstellers erforderlich
- **Manuelle Installation**
  - Physischer Zugang zum System, Admin-Rechte erforderlich
  - Keine Mitwirkung des Benutzers erforderlich

Schwierigkeiten

- **Identifikation des Zielsystems**
  - IP-Adresse nicht zuverlässig
  - Lokalisierung des Systems ggf. schwierig
  - Mehrere Nutzer möglich
  - Observation und physischer Zugriff erforderlich
- **Ausnutzung von Systemschwachstellen**
  - „Zero Day Exploits“ (unveröffentlichte Lücken) verlängern allgemeine Bedrohung, fördern „schwarzen Markt“
  - Extrem aufwändig
  - Begrenzte Einsetzbarkeit
- **Systemvielfalt**
  - Sehr viele Varianten erforderlich (Individualentwicklung)
  - Qualitätssicherung aufwändig

Ausgestaltung OD-Software (1)

- **Leistungsumfang nach Angaben des BMI**
  - **Systemanalyse (installierte Programme, Benutzeraccounts, ...), Zugriff auf Systemeinstellungen**
  - **Erstellung von Verzeichnisübersichten, Durchsuchen von Verzeichnissen nach bestimmten Dateinamen, Volltextsuche**
  - **Durchsuchen angeschlossener Datenspeicher (USB-Sticks, CDs/DVDs, Flash-Memory, externe Festplatten, zugängliche Netzwerk-Laufwerke/Server-Laufwerke)**
  - **Herunterladen von ausgewählten Dokumenten, Bildern**
  - **Remote-Deaktivierung (unbemerkte Entfernung der Durchsuchungssoftware vom System, Spurenlöschung)**
  - **Tastatur-Logger (Protokollierung aller Tastaturanschläge)**
  - **Automatische Deaktivierung (nach Zeitablauf)**

Ausgestaltung OD-Software (2)

- **Weitere Leistungsmerkmale von „Trojanern“**
  - **Protokollierung von Internetzugriffen (URL, Datentransfers)**
  - **Passwort-Protokollierung (Web-Dienste, Entschlüsselung, ...)**
  - **Einblenden von Meldungen auf dem Zielsystem (um den Nutzer zu bestimmten Reaktionen zu veranlassen)**
  - **Netzwerk-Scan: Analyse weiterer über ein Netzwerk oder ein Kommunikationsprotokoll angeschlossene Geräte**
  - **Übermittlung des Bildschirminhalts („Screen-Shots“)**
  - **Abfangen von gesendeten und empfangenen elektronischen Nachrichten („Quellen-Telekommunikationsüberwachung“)**
  - **Raumüberwachung (Rechnermikrofon, Web-Kamera); nach Angaben des BMI nicht geplant**

➔ **Auswertung aller Daten, Aktivitäten und „Spuren“ früherer Aktivitäten möglich**

Online-Durchsuchung

- **Schutz vor Missbrauch durch Dritte**
  - Verbindungsaufnahme mit einem externen Server
  - Prinzip einer „Inside-Out“-Attacke
  - Verwendung von Verschlüsselungsmechanismen
  - Selbstlöschung von außen oder nach Zeitablauf
- **Datenübermittlung**
  - Datenübermittlung nur während Online-Verbindung möglich
  - Begrenzung der Datenmenge erforderlich
    (geringe „upload“-Bandbreite: 768 kBit/s ≈ 4,5 MB pro Minute)
- **Datenselektion**
  - Nur „syntaktische“ Auswertung möglich (Suchwort)
  - Automatisierte Suche auffällig (Verzögerung, Festplattenzugriff)
  - Manuelle Analyse von Verzeichnissen, Dateinamen

secorvo
security consulting

Inhaltsübersicht

- Hintergrund
- Klarstellungen
- Technische Realisierung
- **Grenzen und Risiken**
- Zusammenfassung und Bewertung

Verhinderung einer OD

- **Technische Schutzmaßnahmen**
  - Patchen des Betriebssystems
  - Restriktive Konfiguration des Systems, des Browsers
  - Nutzung eines Virenscanners
  - Sicherheitssensibler Umgang mit E-Mails
  - Nutzung einer Personal Firewall
  - Wiedereinspielen sauberer System-Images
  - Nutzung von „Virtuellen Maschinen“
  - Booten von einem „sauberen“ Medium (USB-Stick, DVD)
- **Organisatorische Abwehrmaßnahmen**
  - Ständiger Wechsel des Online-Zugangs (WLAN)
  - Nutzung eines mobilen Mediums in wechselnden Systemen

➔ **Online-Durchsuchung ist trivial zu verhindern**

Aufdeckung und Manipulation

- **Hinweise auf eine Online-Durchsuchung**
  - **Warnung der Personal-Firewall bei Verbindungsaufbau**
  - **Warnung des Virenscanners vor Key-Logger**
  - **Ungewöhnliche Datenverbindungen in Protokollen**
  - **Alarmmeldung eines „Honeypots“**
- **Manipulation**
  - **Bereitstellung gefälschter Dokumente mit Schlüsselnamen**
  - **Irreführende Hinweise, falsche Spuren**

➔ **Online-Durchsuchung ist leicht aufzudecken**

Grenzen einer OD

- **Wirksamkeitsgrenzen**
  - Nur Systeme mit und während Online-Verbindung
  - Ergebnisse auf Zielsystem beschränkt
  - Einsatz erfordert aufwändige Vorbereitung
- **Beweiswert**
  - Nicht gerichtsfest (kein sachkundiger Zeuge, nur Protokolleinträge)
  - Zuordnung von Daten und Aktivitäten zu einem Verdächtigen technisch nicht belegbar
  - Manipulation der Ergebnisse durch Verdächtigten nicht auszuschließen

➔ **Kein kurzfristig einsetzbares Ermittlungswerkzeug**

➔ **Liefert nur Hinweise für weitere Ermittlungen**

Kosten und Risiken einer OD

- **Kosten**
  - Informationsgewinnung durch Observation
  - Entwicklung/Anpassung des Installationsmechanismus‘
  - Entwicklung/Anpassung der Durchsuchungssoftware
  - Online-Analyse
  - Auswertung der gefunden Daten
- **Risiken**
  - Weitestgehend spurlose Entfernung möglich
  - Generelle Nutzer-Verunsicherung möglich
  - Zurückhaltung bei Nutzung von Online-Diensten möglich
  - Bei Verwendung von „Zero Day Exploits“
    - Rückgang der Veröffentlichungen von Exploits zu erwarten
    - Unterstützung des „schwarzen Marktes“ für Exploits

Inhaltsübersicht

- Hintergrund
- Klarstellungen
- Technische Realisierung
- Grenzen und Risiken
- **Zusammenfassung und Bewertung**

Zusammenfassung

- **Wirksamkeit**
  - Online-Durchsuchungen lassen sich auf gängigen IT-Systemen trivial verhindern
  - Geringe „upload“-Bandbreite begrenzt Datenmenge
  - Gewonnene Erkenntnisse sind nicht gerichtsfest
- **Eingriffstiefe**
  - Technische Abgrenzung von Quellen-TKÜ und Online-Durchsuchung ist praktisch unmöglich
  - Syntaktische Selektion von „relevanten“ Daten, Dokumenten und Informationen ist unmöglich
  - Eingriff in Kernbereich privater Lebensgestaltung ist technisch unvermeidlich
  - Erreichung des Zielsystems ist erst „ex post“ überprüfbar

Bewertung

- *Zweck*: Befürworter benennen zweifellos legitime, aber unkonkrete und sehr unterschiedliche Zwecke
- *Eignung*: Technische Schwierigkeiten, Grenzen und die Leichtigkeit, mit der die Maßnahme verhindert werden kann, macht Eignung zweifelhaft
- *Erforderlichkeit*: Kein Beleg, dass Erkenntnisse nicht auch mit anderen Mitteln zu gewinnen
- *Angemessenheit*: Hohe Kosten und erhebliche Eindringtiefe in Kernbereich privater Lebensführung stellt Angemessenheit in Frage

Problem der Diskussion

- **Operativer Erfolgsdruck von Strafverfolgung und Nachrichtendiensten**
  - **Zunehmende Bedrohung durch internationalen Terrorismus**
  - **Wachsende Nutzung neuer Medien durch organisierte Kriminalität**
  - **Schwächung von TKÜ-Maßnahmen durch verschlüsselte Kommunikation**
- **Sinkendes Verständnis für rechtstaatliche Grenzen**
  - **Zielgenauigkeit, Augenmaß und Legitimität des eigenen Vorgehens wird von Behörden überschätzt**
  - **Adressat einer Observation ist „möglicher Straftäter“, nicht „verdächtigter Bürger“**

Wer Freiheit um der Sicherheit willen aufgibt, wird am Ende beides verlieren.

Benjamin Franklin

Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe

Tel. +49 721 255171-0
Fax +49 721 255171-100
info@secorvo.de
www.secorvo.de