Bundestrojaner: Probleme entlang des gesamten Lebenszyklus

2

- Kauf:
  Förderung eines vorrangig durch Kriminelle genutzten „Schwarzmarktes“ für nicht geschlossene Sicherheitslücken
- Auffinden:
  Aufwändig und kostenintensiv

3

- Macht die Software was sie soll?
  (Nur bei Einsatz quelloffener Software durch die Behörde wirklich überprüfbar)

4

- Überwachungssoftware selbst eignet sich unter Umständen als Einfallstor für weitere Angreifer

6

- Die Überwachungssoftware muss dem Zielsystem und den dort vorhandenen Schutzmaßnahmen angepasst werden
- Zwischen Beobachtung des Zielsystems und Installation können Updates das Zielsystem entscheidend verändern
- Zugriff zum Zwecke des Ausspähens bei verschlüsselten Systemen im Standardfall nicht möglich

7

- Trojaner verändert Zielrechner, obwohl dessen Daten als Beweise dienen sollen
- Sicherheit des Zielrechners dauerhaft beeinträchtigt
- Installation verlangt pro Zielsystem (Windows, Mac, iPhone, Android) mindestens eine Sicherheitslücke

9

- Überwachen nicht gesendeter Nachrichten gleicht einer Gedankenüberwachung.
  Noch nicht Gesagtes kann gegen Beschuldigte verwendet werden
- Problem, Beweise dem zu Überwachenden zuzuordnen, wenn mehrere Benutzer einen Computer verwenden

11

- Überwachung kann entdeckt werden und den gegenteiligen Effekt haben
  (z.B. Beweisvernichtung)

12

- Nachladen beliebigen Codes, revisionssicherer Audit-Trail muss geschaffen werden

13

- Kann im Nachhinein neue Befehle bekommen, Beweise zu fälschen, zu platzieren oder zu vernichten

14

- Bei Backup könnte der Trojaner wieder aufgespielt werden
- Systemzeit ist unzuverlässig