Secorvo-Forensik
Initiale Checkliste („Schritt #0“)

Stefan Kelm
Secorvo Security Consulting GmbH

Version 1.2
Stand 05. März 2008

(Bitte ggf. ankreuzen)

- **Wie viele Systeme bzw. Festplatten sind betroffen?**
  - ☐ auch RAID, etc.? _____
  - ☐ ungefähre Größe der Festplatten bekannt? _____
  - ☐ externe Platten _____
  - ☐ interne Platten _____
  - ☐ andere Wechselmedien (USB, Flash, SD, etc.) _____
  - ☐ _____

- **Um welche Betriebssysteme handelt es sich?**
  - ☐ Windows (Version: _____)
  - ☐ Linux (Version: _____)
  - ☐ Unix (Version: _____)
  - ☐ _____

- **Kurze Beschreibung der Verdachtsmomente, z.B.**
  - ☐ Vermuteter Hacker-Angriff von Außen
  - ☐ Vermuteter Hacker-Angriff von Innen
  - ☐ Missbrauch eines Systems durch legitimen Benutzers
  - ☐ Missbrauch/illegaler Betrieb von Servern/Diensten
  - ☐ Viren-/Wurm-Befall
  - ☐ _____

- **Zeiträume**
  - ☐ seit wann (ungefähr) bestehen die Verdachtsmomente? _____
  - ☐ wie lange (ungefähr) war das System noch im Einsatz? _____
  - ☐ _____

- **Welche (Sofort-) Maßnahmen sind lokal bereits eingeleitet worden?**
  Anmerkung: Bitte keine unüberlegten Sofortmaßnahmen treffen; hierdurch können wichtige Beweismittel zerstört werden.

  ☐ System wurde "sauber" herunter gefahren, *ODER:*
  ☐ System wurde ohne Herunterfahren (physikalisch) ausgeschaltet
  ☐ System lief weiter
    ☐ wie lange (ungefähr)? _____
  ☐ Ein Systemadministrator hat sich angemeldet
  ☐ Es wurde Analyse-Software installiert: _____
  ☐ Es wurden "verdächtige" Dateien gelöscht/deinstalliert: _____
  ☐ Das System wurde gepatcht: _____
  ☐ Es wurden bereits interne Untersuchungen auf dem System durchgeführt, z.B. Auswertung von Logfiles, Benutzerverzeichnissen, ...
  _____
  _____
  ☐ Es wurden Accounts lokal auf dem System gesperrt/gelöscht: _____
  ☐ Es wurden Prozesse/Dienste gestoppt: _____
  ☐ Es wurde ein Backup vom System gemacht
  ☐ System wurde beschlagnahmt/sichergestellt
    ☐ Wo war das System in der Zwischenzeit? _____
    ☐ Wer hatte Zugang zum System? _____
    ☐ Es wurde ein forensisches Image erstellt
    ☐ Es wurden kryptographische Prüfsummen erstellt
  ☐ _____

- **Wer ist informiert worden?**

  ☐ Betriebsrat
  ☐ Personalrat
  ☐ Konzerndatenschutzbeauftragter
  ☐ IT-Sicherheit
  ☐ Werkschutz
  ☐ _____

- **Weitere Anmerkungen, Kommentare, etc.**

  _____
  _____
  _____