1 Malware

1.1 Malware

- **Malware:** Für Malicious (bösartig) Hardware, Software oder Kombination von beiden

1.2 Definition

- **Prozess:** Programm was ausgeführt wird.
- **Betriebssystem:** Erstes Programm was beim Starten ausgeführt wird und dann immer aktiv bleibt.

1.3 Arten von Malware

1.3.1 Klassen von Malware (Joanna Rutkowska)

- **Klasse 0:** Die Malware ändert keinen kritischen Teils des System.
- **Klasse 1:** Malware ändert einen kritischen Bereich, der sich so gut wie nie geändert werden sollte
- **Klasse 2:** Die Malware ändert einen kritischen Bereich der städig geändert werden darf (unwichtig!)
- **Klass2 3:** Überhaupt nicht im System
- **Zu Klasse 0:** Böser Prozess der neben anderen Prozessen exitiert (häufigste Form)
  - Trojaner: sind neue Anwendungen die vom Benutzer ausgeführt werden meistens ohne Wissen, dass es sich um Malware handelt
  - Viren: modifizieren existierende Anwendungen
  - Giftige Eingabe: Nutzen Bugs aus (Exploits) ... wobei nicht kritische Teile des System geändert werden
- **Zu Klasse 1:** Entweder Änderung im Kern des Betriebsystem - oder Änderungen in wichtigen SystempBetrozessen.
  - Rootkits: Einbringen von Malware in den Betriebssystemkernel mit dem Ziel die Malware vollständig zu verstecken
  - Insider Angriffe (Jemand von innerhalb des System): (Achtung ist nicht immer Insiderangriff) Backdoor(Hintertür) manipulierte Software die bestimmmten Leuten Zugriff aus das Betriebssystem ermöglicht
    Logikbombe wird ausgelöst wen bestimmte Bedingungen erfüllt werden (z.B. bestimmtes Datum)
- **Zu Klasse 3:** Z.B. Virtuells System oder Videokamera

1.3.2 Aufspüren von Malware

- Analyse Software
- Analyse Hardware (schwer)
- Analyse Netzwerkverkehr