Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB
Melde- und Analysestelle Informationssicherung MELANI

Cyber-Bedrohung, -Risiken und Informationssicherung

Marc Henauer

Beer Talk, 21. März 2013

1. Einleitung - Risiken und Bedrohungen in der Welt der Informationen
2. Der Untergrundmarkt
3. Von der IT-Sicherheit zur Informationssicherung
4. Schlussfolgerungen

Risiken und Bedrohung

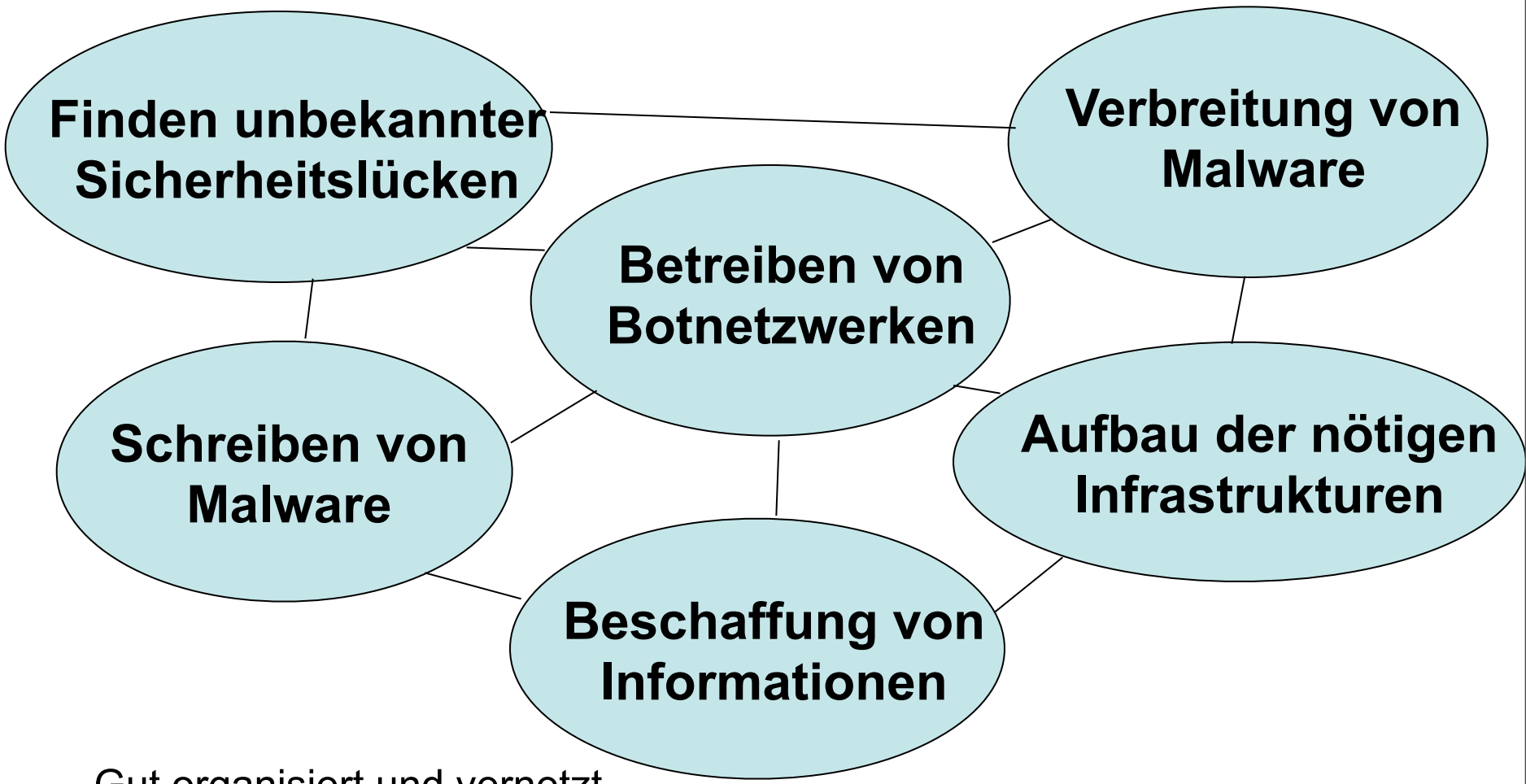
- Zunahme der Bedeutung der Informationstechnologie für Geschäftsprozesse und Finanztransaktionen
- Zunahme der Teilnehmer an diesen Prozessen, zunehmende Vernetzung
- Zugang zu immer mehr wertvoller Information wird möglich

Zunahme der Möglichkeiten für Betrug, Spionage, Erpressung, Sabotage

Auftreten neuer Akteure (z.B. Organisierte Kriminalität, Staaten)

Anpassung der Motive und Methoden bestehender Akteure: kommerzieller Gewinn, Know-how Transfer, politische Motive

Arbeitsteiligkeit und „freier“ Markt



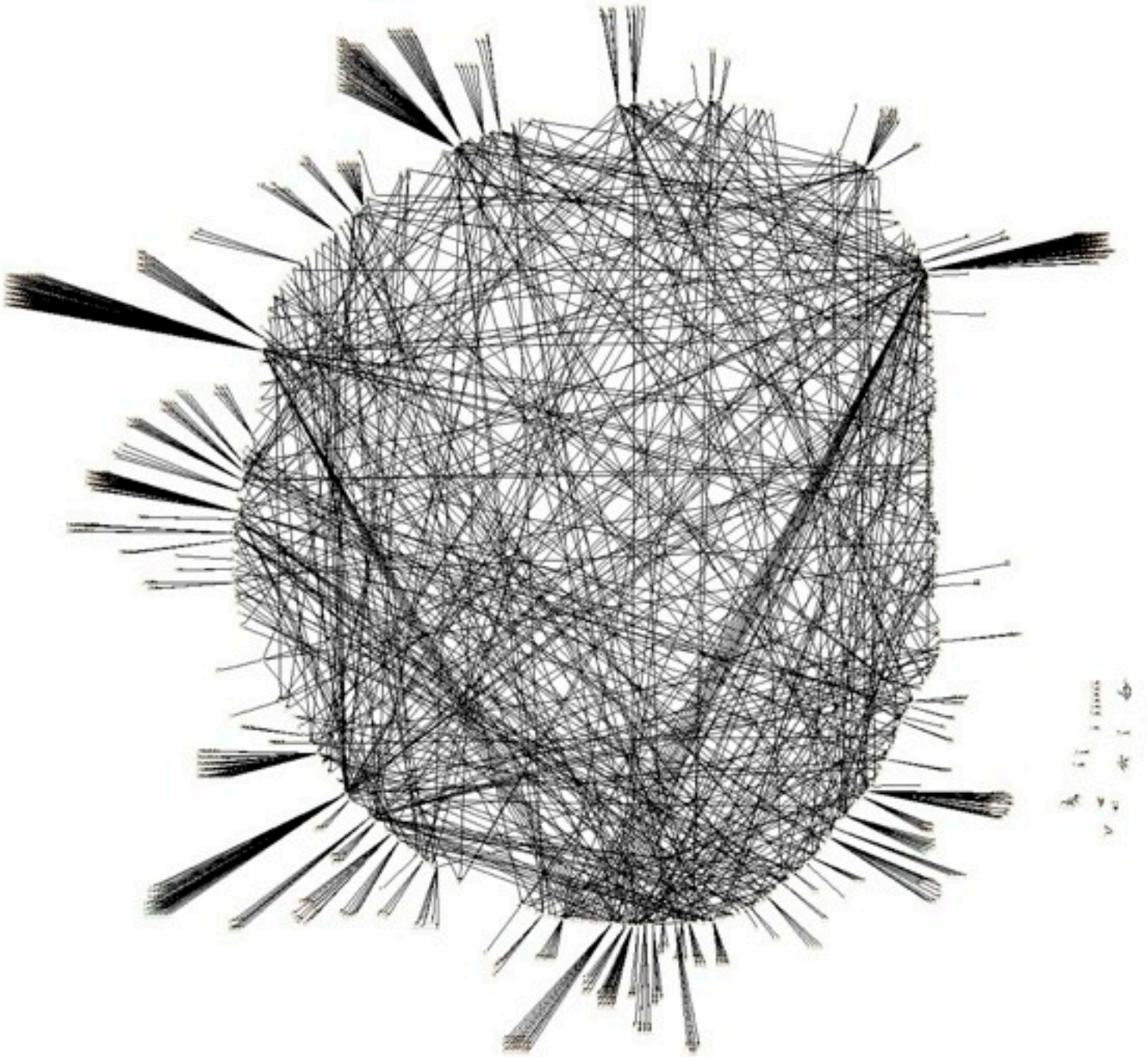
Gut organisiert und vernetzt

- über den Markt kann alles beschafft und organisiert werden.
- Verbindendes Element ist dabei die finanzielle Absicht

Arbeitsteiligkeit und „freier“ Markt Software mit EULA

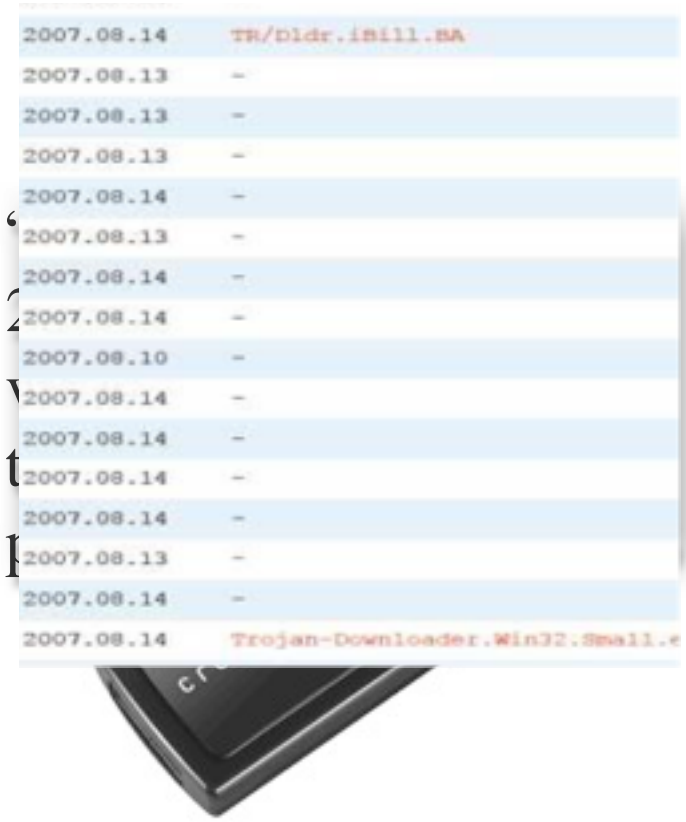
- **Der Verkäufer:**
- Leistet qualifizierten technischen Support via Internet.
- Trägt keine Verantwortung für:
  - Datenverlust
  - Schliessung/Abschaltung von Servern
  - Traffic-Kosten
- Verpflichtet sich, Fehler, die in der Funktionsweise **der Software** gefunden wurden, zu korrigieren und binnen kürzester Fristen Updates ohne finanzielle Gegenleistung zuzusenden.
- Verpflichtet sich, beliebigen Vorschlägen/Meinungen/Rückmeldungen zur Funktionsweise **der Software** Gehör zu schenken und angemessene Entscheidungen zu treffen.
- 2. **Der Kunde:**
  - Ist nicht berechtigt, **die Software** zu irgendwelchen kommerziellen oder nicht-kommerziellen Zwecken zu verbreiten, die nicht den Interessen des Verkäufers entsprechen.
- ist nicht berechtigt, den binären Code des Bots und des Builders zu disassemblieren/analysieren.
- Ist nicht berechtigt, das Steuerungspanel zur Verwaltung anderer Botnets oder zu irgendwelchen anderen Zwecken zu verwenden, die in keinem Zusammenhang mit **der Software** stehen.
- Ist nicht berechtigt, absichtlich irgendwelche Teile **der Software** an Antiviren-Software-Hersteller oder andere, ähnliche Einrichtungen zu senden.
- Verpflichtet sich, den Verkäufer für jede Erneuerung **der Software** zu bezahlen, die nicht mit Fehlern in dessen Funktionsweise in Zusammenhang steht, ebenso für die Ergänzung um jede zusätzliche Funktionalität.

- *Wird gegen diese Vereinbarung verstossen und dieser Verstoss entdeckt, gehen Sie jedweder technischen Unterstützung verlustig. Darüber hinaus wird der Bot Ihrer Zusammenstellung unverzüglich den Antiviren-Software-Herstellern zugesandt.*



Was nicht (mehr) alleine genügt

- Antivirensoftware
- Updates für Betriebssysteme und Applikationen
- Off-Line-Netzwerke



Von der IT-Sicherheit zur Informationssicherung

- Wenn keine 100% Sicherheit existiert, müssen Risiken minimiert und die Sicherheit optimiert werden.
- Dabei spielen mehrere Faktoren eine Rolle:
  - Kosten für zusätzliche IT-Lösungen
  - Kosten für zusätzliche physische und personelle Lösungen
  - Kosten der Effizienzeinbussen, welche jede zusätzliche, einschränkende Sicherungsmassnahme mit sich bringt.

Informationssicherung = Personell, Physisch und IT

- Wer hat Zugriff auf was? Und wie werden diese Mitarbeiter genau ausgewählt, überprüft und allenfalls überwacht?
- Existieren Klassifizierungen? Wo sind unterschiedlich klassifizierte Daten gespeichert? Und wer hat die Verantwortung dafür? (Cloud-Services)
- Welche Kanäle werden gebraucht, um welche Daten zu senden oder um sie verfügbar zu machen?
- Welche Daten werden öffentlich oder intern publiziert? (Facebook: Social Engineering)

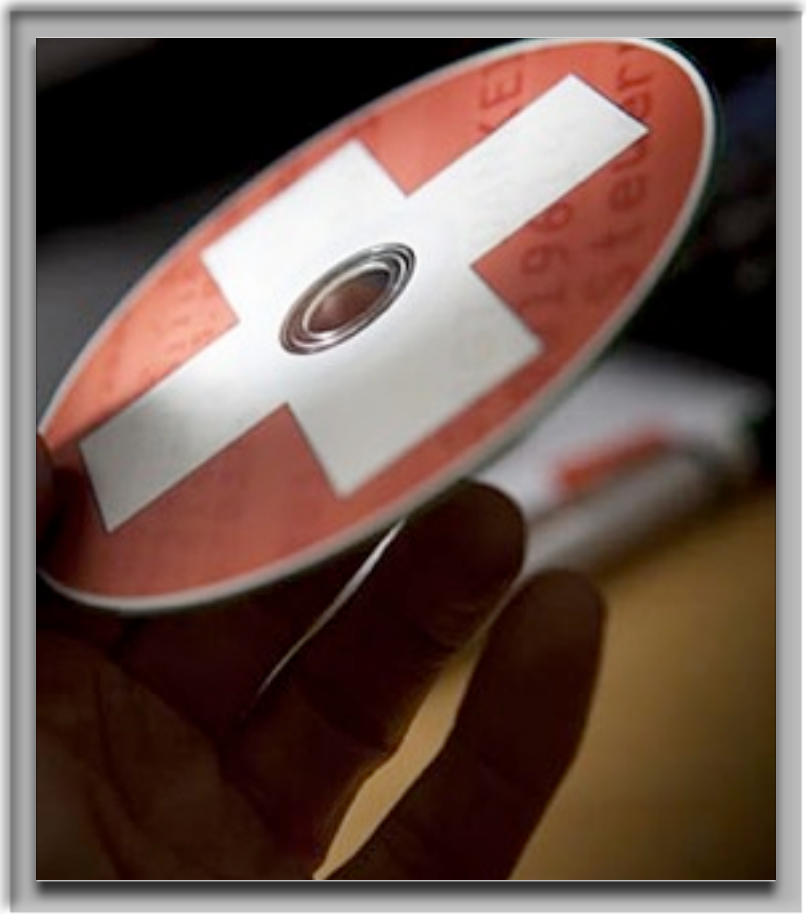
Das Schutzbedürfnis der Information diktiert das entsprechende Schutzniveau. Dieses soll unter Einbezug und Austarierung aller Risikofaktoren erreicht werden.

Schlussfolgerungen

- Prinzipiell gilt: Wenn ein Markt oder Wille existiert, wird Information gestohlen.

- Informationssicherheit ist nicht gleich IT-Sicherheit. Nur ein integraler, Risikomanagement basierter Prozess kann zu einem besseren Informationsschutz führen.

- Risikomanagement ist Aufgabe der Geschäftsleitung. Der Staat unterstützt dies, in dem er seine Informationen im Cyber-Bereich zentralisiert und bedarfsgerecht zur Verfügung stellt . Compliance und Auflagen nur dort wo branchenspezifisch identifiziert (Kernpunkt NCS).



Fragen?

Besten Dank für Ihre Aufmerksamkeit.