Risikoabwägung von TCG

Hunderprozentige Sicherheit durch TCG?

Schutz vor wem?

Andy Müller-Maguhn,

andy@ccc.de

Symposium "Trusted Computing Group"

Berlin, 03.07.2003

Zum Chaos Computer Club

- Geschichte, Aufgabe und Funktion
  - seit 1981 Treff von Computerfreaks und Datenreisenden; Diskussionsrunde rund um elektronische Netze
  - seit 1984 Herausgabe Zeitschrift Datenschleuder und Veranstaltung des jährlichen Chaos Communication Congress [1]
  - 1986 Gründung des Chaos Computer Club e.V. [2] u.a. als Konsequenz des 2. WiKG (Regelung von Verantwortlichkeiten)
- Vereinsziele
  - Einsatz für ein Menschenrecht auf zumindest weltweite ungehinderte Kommunikation
  - Förderung von Informationsfreiheit und Transparenz (z.B. maschinenlesbare Regierung, Zugang zu Akten..)
  - Auseinandersetzung mit den Wechselwirkungen zwischen Technologie & Gesellschaft (Risiken & Chancen)
- Praktische Arbyte / Organisationsform
  - Bundesweiter Verein & galaktische Gemeinschaft, organisiert in Dezentralen, Erfa-Kreisen und Chaos-Treffs
  - Themenbasierte Arbeitsstrukturen und Betrieb von Kommunikationsstrukturen und Medien (Listserver, Web, FTP, Radio, CD-ROM)
  - Durchführung & Teilnahme von/an Veranstaltungen (Congress & Camp, Workshops, Anhörungen, ..)
  - Mitglied der Global Internet Liberty Campaign GILC [3] sowie Gründungsmitglied von European Digital Rights EDRI [4]

---

[1] http://www.ccc.de/congress/

[2] http://www.ccc.de/club/statutes

[3] http://www.gilc.org/

[4] http://www.edri.org/

Kategorien von Angreifern & Ihren Motivationen

- Hacker
  - Neugier, Förderung von Informationsfreiheit & Transparenz
- Cracker
  - Befreihung eingesperrter Bits (Kopierschutzmechanismen)
- Crasher
  - Vandalismus/Kaputtwillspaß als Frust-Ableiter ("I HATE TO GO TO SCHOOL")
- (Wirtschafts-) Kriminelle
  - "materielle Interessiertheit" = "unberechtigte Verschaffung von Vermögensvorteilen"; mehr oder weniger klar abgrenzbare Bereiche
- Spione
  - Zugang und Verfälschung von Information
- Militärs und andere kriegsführende Organe
  - Information Warfare: Ausspähung, Manipulation und Zersetzung von IUK-Systemen

---

Angriffsperspektive I

- Sicherheit ist die Sicherheit des schwächsten Punktes.
- Angriffsökonomie: der Weg des geringsten Widerstandes

  Angriff als individueller, dynamischer Prozess
- Konzeptionelle schwäche statischer Abwehrkonzepte

  Beispiel: Angriff über Wavelan - Accespoints im Intranet in einem Firewall Abwehr-Paradigma

Abwehrperspektive I

- Technische Möglichkeiten im Kontext der Umsetzung in wirtschaftlichen Realitäten

  "Das Ziel von Sicherheitsmaßnahmen kann nur sein, zwischen dem Aufwand zur Sicherung
  und dem Aufwand zum Durchbrechen dieser Sicherung ein Ungleichgewicht zuungunsten des Angreifers herzustellen"

  - Beispiel: Die daraus resultierende Vorgehensweise von SWIFT / die NIMBY Stratgie.

- Betriebswirtschaftliche Optimierung von Arbeitsabläufen vs. Aufwand zur Berücksichtigung der Sicherheit

  - Beispiel: Der "I-LOVE-YOU" Virus und die wirtschaftlichen Hintergründe in den verschiedenen Dimensionen:

    - 1. Einsatz und Konfiguration von Werkzeugen

    - 2. Featurewahnsinn und Gewichtung von Funktionalität vs. Sicherheit bei Programmierung

---

Angriffsperspektive II

- Szenario: Kontinuierlicher betriebswirtschaftlicher Optimierungsdruck bei gleichzeitig kontinuierlicher Vernachlässigung [1] der Sicherheit
- Angriffsform: Assimilierung von Strukturelementen durch Subventionierung des Endkundenpreises
  - **Injizierung von Angriffswerkzeugen ("trojanischen Pferden") u.a. legendiert als "Sicherheitsinstrumente"**

    Mögliche Beispiele: Firewall Installation der EU in Brüsse1996 [2], Comverse Infosys (heute: Verint) [3]
  - **Abgriff von Verkehrsströmen durch Gestaltung von Netzinfrastruktur - Datenpfaden**

    Mögliches Beispiel: Gestaltung der AT:M-Netzpfade bei der Anbindung des Africe-One Glaserfasernetzes [4]
  - **Zugriff auf Daten durch Verlagerung im Rahmen von kostengünstigsten Outsourcing-Dienstleistungen**

    Mögliches Beispiel: Amdocs [5]
- Die verschiedenen Ebenen der Jurisdiktionsproblematik:
  - 1. Unternehmen, die Sicherheitsprodukte herstellen, müssen sich an die Gesetze Ihre Landes halten.
  - 2. Punkt 1 gilt auch für Unternehmen, die in Ihrem Land Daten für Unternehmen aus anderen Ländern verarbeiten.
  - 3. Zivilrechtliche Verträge und Safe-Harbour Rahmenverträge schränken 1. und 2. nicht ein.
  - 4. Technische Realitäten und Zugriffsmöglichkeiten stehen nicht zwangsläufig in Kompatibilität mit juristischen Realitäten (Enforcement).

---

[1] Vernachlässigung definiert als: Priorität auf betriebswirtschaftlicher Optimierung, nicht auf Sicherheit

[2] http://www.islandone.org/Politics/LondonTimes-19960804.html

[3] http://www.contramotion.com/updates/org/comverse

[4] http://www.africaone.com/

[5] http://www.contramotion.com/updates/org/amdocs man beachte aber auch die Kundenlisten http://www.amdocs.com/

Abwehrperspektive II

- Identifizierung möglicher Angriffspunkte und Einschränkung der diesbezüglichen (Angriffs-)Handlungsoptionen
- Berücksichtigung der Jurisdiktionsopportunität von
  - Komponenten bzw. Ihren Herstellern
  - Outsourcing-Dienstleistungen bzw. den Dienstleistern
  - Genutzten Pfaden bei transnationalen Datenübertragungen
- Abgleich der verschiedenen Realitäts-Komponenten:
  - Umfang von Funktionen, Dienstleistungen und Sachzwängen in den betreibenden Entitäten
  - Komponenten-Funktionalität und sich ergebende Handlungsoptionen ("hidden agendas")
  - Technische Konzepten und technische Realitäten (Datenhoheit)

"Trusted Computing" ?!

"What do you mean by trust?

The ability to feel confident that the software environment in a platform is operating as expected.

This is done by reliably measuring and reliably reporting (using aliasing) information about the platform"

Punkt 12 in der TCPA FAQ Version 0.5 vom 03.07.2002

"A platform can be trusted if it behaves in the expected manner for the intended purpose."

Joe Pato, Hewlett-Packard

- Gegenargument gegen diese Definition:

Angriffsformen, die darauf beruhen, daß neben den erwarteten und gewollten Programmfunktionen zusätzliche (ungewollte) Programmfunktionen ausgeführt werden können sind nicht abgedeckt.

Vertrauenswürdig ist Technologie nur, wenn deren Funktionalität Überschaubar **und** Beherrschbar ist.

Grundsätzliche Fragen im Bezug auf TC (PA) etc.*

- Konzeption, Entwicklung, Implementiertung: Sicherheit für wen?
  - Wer kontrolliert die Schlüssel?
    - Erzeugung der Schlüssel und mögliche Einbehaltung im Kontext von Key-Recovery Funktionen
    - Datenschutzfragen im Bezug auf die Zuordnungsoptionen generierten Schlüssel durch die in der CA anfallenden Datensätze.
  - Kontrolle über die (in der hardware implementierten) Software?
    - Überprüfbarkeit der softwaremässigen Implementierung in Hard- und Software
    - Fragen im Bezug auf Transparenz, Zertifizierungsmechanismen und Hoheit über den Code
  - Kontrolle über die Anwendungssoftware im praktischen Einsatz (OS Ebene, also z.B. Palladium*)
    - Konzeption (Policy) kann derzeit nicht als Ergebniss eines Interessenausgleichs betrachtet werden.
    - Hardware kontrolliert Software kontrolliert Benutzer: nicht andersrum, d.h. keine Kontrolle durch Benutzer (Ausnahme: Ausschaltoption)
- Gefahren im praktischen Einsatz
  - **Nachschlüssel, mindestens aber gewaltiges Mißbrauchspotential durch die in der CA auch ohne Key Recovery anfallenden Daten**
  - **Zugriff auf (geheime) Anwenderschlüssel durch verdeckte Kanäle (nicht-transparente Zertifizierung nicht-öffentlichen Codes)**
  - **Einzug fremd-opportuner Soft- und Hardwareelemente in der dominanten PC Hard- und Softwareplattform**

---

* oder wie das unter dem Namen TCPA angefangene Projekt, dessen Implementierung bei Microsoft ursprünglich Paladium heißt, diese Woche korrekt bezeichnet wird

Parameter der (Un-)Sicherheit

- Bereiche
  - Schlüsselgenerierung und Verwaltung
  - Konzeptionierung, Softwareerstellung
  - Spezifizierung und Produktion Hardware
- Parameter
  - Akteure und Handlungsoptionen, Ausmass und Grenzen der Kontrollierbarkeit
  - Wirtschaftliche Umstände und Abhängigkeiten
  - In welcher Jurisdiktion und unter welcher Opportunität?

Mögliche Entschärfungen der Problembereiche

- Schlüsselgenerierung und Verwaltung unter PC-unabhängiger Kontrolle des Anwenders
  - Option Smartcard
- Zertifizierungsoption etwaiger Vertrauenswürdigkeit von Soft- und Hardware durch vollständige Transparenz
  - Auch für den Anwender

Weitere Informationen

http://www.ccc.de/digital-rights/

mail@ccc.de