Bensberger Gespräche
24.-26. Januar 2011 in Bensberg

Tagungsdokumentation
Dokumentation: Christiane Toyka-Seid

Dienstag, 25. Januar

Input 2 „Virtuelle Sicherheit – Bedrohungen aus dem Internet“
Referenten: Peter Welchering, VoxMundi, Medienanstalt GmbH, Kornwestheim, Sam May, Security Research Lab GmbH, Berlin

Peter Welchering: Der digitale Erstschlag hat vor fast 30 Jahren stattgefunden

Zwei Ausgangsthesen:
a) Die Bedrohung aus dem Internet ist bis jetzt in Sicherheitskreisen noch nicht angekommen
b) Wir haben noch kein Sicherheitskonzept, das zu Ende gedacht ist

Drei Schadensereignisse machen exemplarisch die Brisanz der Gefahren deutlich:
- 1982 Explosion an der Chelyabinsk-Pipeline in Russland
- 2007 Explosion eines Diesel-Testgenerators in den USA und
- 2010 Stuxnet-Computervirusangriff auf Industrieanlage im Iran.

In allen Fällen erfolgten absichtliche Manipulationen an Software-Daten, die neben wirtschaftlichen auch sicherheitsrelevante Auswirkungen hatten.

Drei Daten aus dem militärischem Bereich beleuchten das Problem:
- Oktober 2010: Das Cyber Command der US Streitkräfte nimmt seine Aufgabe auf mit dem Auftrag, cybermilitärische Operationen vorzubereiten und durchzuführen
- November 2010: Die Nato-Staaten diskutieren in Lissabon eine Änderung von Artikel 5 des NATO-Grundlagenvertrags: Soll bei digitalen Angriffen auf die Infrastruktur eines NATO-Mitglieds der Bündnisfall ausgerufen werden?
  Problem: Was ist ein Cyberkrieg? Wann wäre der Beistandsfall gegeben?
- Sommer 2011: Cybereinheit der Bundeswehr soll „aktives Potenzial“ für den Cyberkrieg aufgebaut haben.

Sicherheitslücken und Exploits (kleine Schadprogramme, die Sicherheitslücken ausnutzen)
- Angriffsprogramme nutzen Sicherheitslücken in Betriebssystem-Routinen und vor allen Dingen Kommunikationssoftware aus
- Der Exploit-Markt findet weitgehend auf Auktionen im Internet statt
- 30.000 Schwachstellenanalytiker arbeiten weltweit, davon 10.000 in der VR China
- In Deutschland arbeitet zur Zeit das bekannte „dreckige Dutzend“ an Exploits
- Auftragsproduktionen westlicher Geheimdienste werden seit Sommer 2008 überwiegend in Minsk durchgeführt
- Kooperationsprojekte westlicher Geheimdienste nehmen zu (war vermutlich auch bei Stuxnet der Fall)

Waffen für Cyberkrieg:
- **Remote Forensic Software**: „Bundestrojaner“; Effekte sind: Befehle abfangen und verändern, Mail-Konten können beschlagnahmt werden.
- SQL-Injection: Formulare werden mit einer Datenbank verbunden, die dann ausgewertet werden kann
- Man-in-the-Middle-Attacken: Sender werden zwischen Sender und Empfänger gehängt – z.B. bei Online-Banking werden Daten abgefangen und für Rechner missbraucht

- Denial-of-Service-Attacken: Bestimmte Server werden mit sehr vielen Daten „beschossen“, Schaden entsteht durch die Asymmetrie
- Data Links zu Remote Terminal Units: feste Schnittstellen werden in einen Virus einprogrammiert – dauerhaft werden Links zu bestimmten Daten gelegt.
- **Spezifisch angepasste Malware zur Zerstörung von Infrastruktur:** hier werden passgenaue Störungen intendiert, aber die Versagenswahrscheinlichkeit ist hoch
- (Reverse) honeypots: werden eingesetzt, um Informationen über Angriffsmuster oder Angreiferverhalten zu protokollieren

Die Szenarien
- Lastverteilungsrechner abschalten
- Kommunikationsknotenrechner ausknipsen
- Netzleitrechner stören
- Manipulationen an Frequenzumrichtern
- Druckparameter unzulässig erhöhen
- Embedded Systems mit Metallmigration
- Befehle abfangen und verändern
- Finanztransaktionen manipulieren
- Forschungsergebnisse manipulieren

Konsequenzen: Vorstellbar sind bürgerkriegsähnliche Zustände, wenn der Strom 5 Tage lang ausfällt, es keinen Benzin, keinen Kassenbetrieb in Supermärkten und kein Bargeld mehr gibt.

Schlussbemerkung: Jede Software unterliegt dem „dual use“, kann also als Verteidigungs- und Angriffswaffe im digitalen Krieg genutzt werden. Sicherheitslücken müssen aufgedeckt werden, um wirksamen Schutz entwickeln zu können. Die derzeitig praktizierte Geheimhaltung entdeckter Sicherheitslücken birgt ein erhebliches Sicherheitsrisiko für alle Infrastrukturen.

Sam May: Entwicklung IT-basierter Angriffe, Verteidigung als öffentliche Aufgabe

Digitalisierung hat sich im öffentlichen und Wirtschaftsleben durchgesetzt. Auch die Angriffsaktivitäten haben sich entwickelt, seit 2004 gibt es einen „Qualitätssprung“. Zunächst gab es Angriffe, die große Streuung hatten und über den Masseneinsatz Wirkung erzielen wollten

Angriffe auf kritische Infrastruktur: Seit 2008 gibt es targeted attacks: Software, die auf bestimmte Ziele hin gebaut wird. Wirtschaftsspionage will „intellectual property“ abziehen. Sie wird gezielt eingesetzt.

Mit speziell programmierter Malware rücken kritische Infrastrukturen in den Fokus der Angreifer. Aktuelle Manipulationen zielen dabei auf Sabotage oder Zerstörung. Um effektiv zu sein, braucht es im Vorfeld eine kostspielige Testumgebung, die Spuren müssen verschleiert werden. Es sind sehr aufwendige Attacken (unter Nationalstaaten?)

Die Sicherheit kritischer Infrastrukturen ist ein öffentliches Gut!
Wie kann Verteidigung hier aussehen?

These 1: Es existiert keine marktübliche Lösung für die Sicherheit von kritischen Infrastrukturen.

These 2: Es muss ein Anreiz zur *frühen* Erstellung von sicheren Systemen geschaffen werden („Grüne Bananen“-Politik – Das „Reifen“ von Software darf nicht ermöglicht werden!)
Sicherheitslücken sind umso teurer, je später sie gelöst werden.
Statt Hackertools unter Strafe zu stellen, sollte das Knowhow gefördert werden.

These 3: Ein gesellschaftlicher Diskurs über Sicherheitsniveaus ist notwendig – derzeit herrscht viel Unwissenheit, diffuse Angst, ein Abwägen zwischen den Kosten für Kontrolle und etwaigen Schäden findet nicht statt. Hier braucht es öffentliche Debatten.