Virtuelle Sicherheit –

Bedrohungen aus dem Internet

Oder: Der digitale Erstschlag hat vor fast 30 Jahren stattgefunden

Vortragender: Peter Welchering

WELCHERING:

Drei Schadensereignisse

1982: In Russland explodiert eine Verdichtungsstation an der Chelyabinsk-Pipeline – Ursache: Ein Softwarefehler der von Programmierern der CIA in die kanadische Steuerungssoftware eingebaut worden war, um Softwarediebstähle zu verhindern

2007: Im US-Bundesstaat Idaho explodiert ein Diesel-Testgenerator. Das Department of Homeland Security hatte einen Test im Labor des Energieministeriums gefahren, in dem mit einer Man-in-the-Middle-Attacke die Steuerdaten vom Maschinenleitstand abgefangen wurden und völlig überhöhte Werte an den Generator geschickt wurden.

2010: Mit dem Computervirus Stuxnet werden Industriesteuerungen manipuliert. U.a. werden Zentrifugen in einer iranischen Urananreicherungsanlage in Natans durch Stuxnet so heruntergedrosselt, dass die Herstellung von waffenfähigem Uran massiv verzögert wird.

Drei Daten aus dem militärischen Bereich

Im Oktober 2010 nimmt das Cyber-Command der amerikanischen Streitkräfte den Betrieb auf. Die Mission: Vorbereitung und Durchführung umfassender cybermilitärischer Operationen

Im November 2010 diskutieren die NATO-Mitgliedsstaaten auf ihrem Gipfel in Lissabon eine Änderung von Artikel 5 des NATO-Grundlagenvertrags. Bei digitalen Angriffen auf die Infrastruktur eines NATO-Mitglieds soll der Bündnisfall ausgerufen werden können.

Im Sommer 2011 soll die Cybereinheit der Bundeswehr, die Computer- und Netzwerkkooperation, CNO, in der Tomburg-Kaserne in Rheinbach bei Bonn „aktives Potenzial“ für den Cyberkrieg aufgebaut haben

Sicherheitslücken und Exploits

- Angriffsprogramme nutzen Sicherheitslücken in Betriebssystem-Routinen und vor allen Dingen Kommunikationssoftware aus
- Exploit-Markt findet weitgehend auf Auktionen im Internet statt
- 30.000 Schwachstellenanalytiker 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 mit israelischen Entwicklern nehmen zu

Waffen für den Cyberkrieg

- Remote Forensic Software
- SQL-Injection
- Man-in-the-Middle-Atacken
- (Distributed) Denial-of-Service-Attacken
- Data Links zu Remote Terminal Units
- Spezifisch angepasste Malware zur Zerstörung von Infrastruktur
- (Reverse) honeypots

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

Die Konsequenzen

Prof. Dr. Hartmut Pohl

Carsten Casper

Schlussbemerkungen

- Jede Software unterliegt dem „dual use“
- Jede „Verteidigungswaffe“ im digitalen Krieg ist auch immer eine Angriffswaffe
- Wirksamen Schutz garantiert nur die rückhaltlose Veröffentlichung aller entdeckten Sicherheitslücken
- Die derzeitige Verteidigungsdoktrin für den Cyberwar basiert auf Geheimhaltung entdeckter Sicherheitslücken; dadurch wird ein erhebliches Sicherheitsrisiko für alle Infrastrukturen geschaffen