Medienbildung/ICT und Medien für Sek I und Sek II

# Netwars – Krieg im Netz

52:00 Minuten

**Einführung**
**00:00** Hacker dringen in die Netzwerke von Infrastrukturanlagen und Unternehmen ein, nicht selten im Auftrag von Regierungen. Welche Nationen sind führend im Cyber War? Und wie steht es um die Sicherheit der Strom- und Wasserversorgung in einer deutschen Kleinstadt?

**Stuxnet**
**03:27** 2010 wurde auf Computern im Iran das Schadprogramm Stuxnet entdeckt, das Steuerungsprogramme für Industrieanlagen infizieren konnte und die Möglichkeit eröffnete, von aussen direkt Produktionsprozesse zu sabotieren.

**Iranisches Atomprogramm**
**07:17** Zwei Jahre später enthüllte der amerikanische Journalist David Sanger, dass die US-Regierung die Schadsoftware eingesetzt hatte, um das iranische Atomprogramm auszubremsen. Bis zu seiner Entdeckung brachte Stuxnet die Urananreicherung im Iran nahezu zum Erliegen.

**Trinkwasser- und Stromversorgung**
**09:21** In Ettlingen, einer deutsche Kleinstadt am Rand des Schwarzwalds, versorgen die Stadtwerke 20 000 Haushalte mit Trinkwasser und Strom. Die Stadt hat einen professionellen Hacker beauftragt, das Gefahrenpotenzial eines elektronischen Eindringens in ihre Anlagen zu prüfen.

**Israels Iron Dome**
**14:59** Der Iron Dome, das modernste Flugabwehrsystem der Welt, schützt die Menschen in Israel vor Raketenangriffen. Parallel dazu hat der israelische Staat schon vor 15 Jahren begonnen, einen digitalen Iron Dome zu installieren, der Verkehrsleitsysteme und die Versorgung mit Strom und Wasser vor Cyberangriffen schützt.

**Wettrüstens im Cyberspace**
**21:18** Für die Industrie in Europa bedeutet das Wettrüsten im Cyberspace eine neue Bedrohungssituation. Anders als in Israel, gibt es etwa in Deutschland und Frankreich keine bindenden Cybervorschriften. Industrielle Anlagen sind europaweit ungeschützt mit dem Internet verbunden.

**Social Engineering**
**22:36** Maximal fünf Tage braucht der Profihacker, um den Ettlingern den Strom auszuknipsen. Ein gezielter Angriff beginnt meist mit Social Engineering, dem Einschleusen von Schadsoftware über Mitarbeiter.

**Israels IT-Technologie**
**24:46** Israels boomende IT-Technologie entwickelt weltweit führende Sicherheitsprodukte. Die meisten Programmierer sind ehemalige Geheimdienst-Mitarbeiter und Militärs aus Cyber-Einheiten, die ihre erworbenen Kenntnisse verkaufen und für Regierungen Produkte für digitale Überwachung entwickeln.

**Asymmetrische Kriegsführung**
**28:20** Cyberkriege zeichnen sich durch asymmetrische Kriegsführung aus. Dem Angreifer reicht eine Schwachstelle in Millionen Zeilen Code. Die Cyberverteidigungszentrale der Nato in Belgien verzeichnet pro Jahr etwa 2 500 schwerwiegende Cyberattacken.

| | |
|---|---|
| **IT-Sicherheitskonferenz Las Vegas** | **33:40** Die IT-Sicherheitskonferenz in Las Vegas steht ganz im Zeichen der NSA-Enthüllungen. Die Berichte von Edward Snowden zeigen das Ausmass des Cyberkriegs. Die USA führen pro Jahr über 200 Cyberangriffe durch, die der Auslandüberwachung und der Bekämpfung des Terrorismus dienen. |
| **Chinesische Hacker** | **39:37** Chinas IT-Boom hat ein Heer patriotischer Hacker hervorgebracht, die unter Kontrolle der Regierung dem feindlichen Amerika den Kampf angesagt haben. |
| **Industriespionage** | **42:20** China betreibt Cyberspionage in Unternehmen, um die eigene Industrie aufzubauen. Bekanntestes Beispiel ist die Firma Huawei, deren Produkte mittlerweile besser und billiger sind als die amerikanischer Konkurrenten wie Cisco. |
| **Showdown in Ettlingen** | **45:37** In Ettlingen suchen drei Profihacker nach Hintertüren und ungeschützten Zugängen in die Steuerung für Strom und Wasser. Im Gästehaus der Stadtwerke werden sie fündig, lenken die Sekretärin ab, zapfen eine Netzwerkdose an, entern das System und könnten nun mit einem Knopfdruck den Strom einer ganzen Stadt ausschalten. |
| **Entnetzung** | **49:05** Trotz der weltweiten Bedrohung IT-gestützter Anlagen setzen führende Anbieter wie Siemens auf noch mehr Vernetzung. Unabhängige Experten bezweifeln jedoch, dass die heutige Technologie angriffssicher angelegt ist und fordern deshalb eine Entnetzung, z.B. das Abkoppeln von Infrastrukturanlagen vom Internet. |