Arbeitshilfen

Katholisches Filmwerk

Operation Bluebird

Kurzspielfilm, 15 Min.,
Deutschland 1999,
Buch und Regie: Stefan Holtz
Kamera: Paul-Jan Milbers
Musik: Patrick Buttmann
Darsteller: Michael Kausch (Embacher),
Frank Röth (Bark), Tabea Heynik (Hartwig),
Krystof Machowski (Pförtner) u. a.
Produzent: Mario Stefan
Produktion: Fieber-Film in Koproduktion
mit Vide Film / Indigo, Cinemobil, HFF-München

Kurzcharakteristik

Eine Hackergruppe namens „bluebird“ bedroht seit Jahren die internationale Staatengemeinschaft, indem sie Angriffe auf geheime Datenbanken mit Bombendrohungen koppelt: Wenn die Hacker aus dem Netz geworfen werden, explodiert die Bombe. Als es ihnen eines Tages gelingt, über eine belgische Firma und einen russischen Provider ins Pentagon einzudringen, will das amerikanische Militär die Verbindung unterbrechen, auch wenn eine Giftgasbombe in Brüssel explodiert. Für Jürgen Embacher, den Chef der European Network Defense, beginnt ein Wettlauf gegen die Zeit.

Einsatzmöglichkeiten

Schule:
Sek I (ab Jg. 8) und Sek II, in den Fächern Deutsch, Politik/Sozialkunde, Religion, Ethik, Informatik. Der Film bietet sich auch für einen fächerübergreifenden Unterricht an.

Außerschulische Jugendarbeit:
Kinder und Jugendliche wachsen heutzutage mit Computer und Internet auf, sie nutzen mit großer Selbstverständlichkeit die Neuen Medien. Bei allen Freizeiten, Gruppenstunden, Workshops oder Wochenenden, z. B. zur Lebens- und Alltagswelt der Jugendlichen, kann der Film gezeigt werden, um die Jugendlichen für die Gefahren im Umgang mit Computer und Internet zu sensibilisieren.

Erwachsenenbildung:
Bei Veranstaltungen zu Chancen und Risiken der Mediengesellschaft oder Seminaren, die sich mit der Zukunft unserer Gesellschaft beschäftigen, kann der Film als Impulsfilm, z. B. zum Einstieg ins Thema, eingesetzt werden.

Themen: Zukunftsängste, Bedrohung durch Computertechnologie, ethische Auseinandersetzung mit Terrorismus einerseits, mit dem Mythos der Hacker andererseits; das Abwägen von Gütern. Darüber hinaus: Neue Medien, Datenschutz, Cyberterrorismus, digitale Kriegführung, Computerviren, Organisierte Kriminalität, Gefahren des Internet.

Inhalt

Spannende Musik ist in der Einleitungssequenz Bildern unterlegt, die TV-Aufnahmen von militärischen Kampfaktionen zeigen. Dazu wird aus dem Off folgender Kommentar gesprochen, der für Verständnis und Einordnung wichtig ist:
„*War es vor zwanzig Jahren noch die Lufthoheit, die ausschlaggebend für militärische Siege war, so wird im 21. Jahrhundert die Kontrolle der Computertechnologie der Schlüssel zur Macht sein. Deshalb werden Cyberterrorismus und digitale Kriegführung in den kommenden Jahren zur größten Bedrohung der nationalen Sicherheit werden. Ein neuer Krieg hat begonnen.*“

Ein Untertitel zeigt den ersten Handlungsort und die Zeit: Belgien, Brüssel, 14. Juni 1998, 16.05 Uhr. Die Kamera wandert aus der Obersicht auf das Gebäude einer Computerfirma in ein Büro. Die Akteure sprechen Französisch, Untertitel übersetzen, so wirkt das Ganze authentischer. Die Mitarbeiter haben einen Hacker im System entdeckt. Dann werden ihre Gesichter schreckensbleich, als ein blauer Vogel auf dem Bildschirm erscheint mit der Nachricht: „Attention, bluebird is singing." „Merde" (Scheiße!) ist die Antwort und: „Halt, warte! Lass bloß die Leitung in Ruhe. Wir müssen sofort die E.N.D. anrufen" (= European Network Defense).
Norddeutschland, der Chef des E.N.D. liegt mit geschientem Bein im Krankenhaus. Ab jetzt werden die Szenen in Parallelmontage der verschiedenen Handlungsorte gegeneinandergeschnitten. In Brüssel rückt in der Softwarefirma eine Spezialeinheit an. Der Chef im Krankenhaus wird per Telefon von einer Mitarbeiterin seiner Berliner Zentrale informiert. Der Hacker hat sich als Superuser eingeloggt; das Passwort hat er über ein Trojanisches Pferd bekommen. Aber was kann der Hacker im Computersystem dieser kleinen Firma wollen? – Es ist nichts zu machen. Sobald der Großrechner abgestellt würde, fliegt in Brüssel alles in die Luft – das erfährt der Zuschauer aus den Dialogen. Die Kamera zeigt einen Blick in die Bombe. Dunkle Bilder mit bläulicher Lichtstimmung und geheimnisvolle Fachworte steigern die Spannung: „Plastiksprengstoff, Bewegungsmelder, abgeschirmte Kontrolleinheiten, Attrappen und mindestens 10 Kilo Sarin." Die Polizei evakuiert bereits die Innenstadt. Aber der Hacker geht über einen Provider in Pokrowsk, Russland. Dort ist es 0:53 Uhr und nur ein Nachtwächter ist im Dienst, als das Telefon klingelt.
Wieder Brüssel, Berlin und das Krankenhaus in Norddeutschland im Szenenwechsel; natürlich sind die Stationen über Bildtelefon und Computer ver-

bunden. Was will der Hacker? Er öffnet auf einem Rechner ein Programm namens „Transdata“, mit dem alte Computerdaten für neue Betriebssysteme übersetzt werden können. Dann sieht man, wie er sich einloggt; zu entziffern ist „… @ftp.pent.us.gov“, er will sich in den Regierungscomputer im Pentagon einloggen.
In Brüssel packt die Sondereinheit zusammen; sie haben Befehl, die Leitung sofort zu unterbrechen und somit die Explosion der Bombe in Kauf zu nehmen. In Russland muss erst der Chef der IBM-Zweigstelle aus dem Bett geklingelt werden, damit der Nachtwächter Anweisungen bekommt.
Der Chef des EMD hat seine Unterbrechung programmiert, aber die Übertragung macht Probleme, weil ein Gewitter ein Funkloch erzeugt hat. Ein ironisches Element kommt ins Spiel, als der Chef mit dem kranken Bein seine Antenne am Fahnenmast festmacht. Aber das simple Hilfskonstrukt funktioniert. Der Nachtwächter soll den Computer ausschalten, aber er findet natürlich den richtigen Schalter nicht, hat nicht den richtigen Schlüssel für den Serverraum. Im letzten Moment schafft er es, die Sicherungen auszuschalten. Schnell und spannungssteigernd sind in dieser Sequenz die Einstellungswechsel der verschiedenen Orte aneinandergeschnitten.
Am Schluss ist ein beunruhigender und alarmierender Ausblick zu sehen: 5 Monate später – in einem Computer-Kontrollraum entdeckt ein Mitarbeiter wieder die Meldung „Attention, bluebird is singing“: Dann zeigt ein Standbild ein Atomkraftwerk und der Untertitel klärt auf: „AKW Grohnde. 26. November 1998.“

Gestaltungs- und Interpretationshinweise

Durch seine Kürze und eine relativ komplexe Parallelmontage von Handlungssträngen an verschiedenen Orten ist der Film nicht ganz leicht zu verstehen.

Deshalb sind einige Erklärungen vor dem Sehen hilfreich, ohne dass sie etwas vorwegnehmen.
Die Handlungsorte sollten genannt werden: eine Computerfirma in Brüssel; ein Krankenhaus in Norddeutschland, in dem der Chef des European Network Defence liegt; die Zentrale des E.N.D. in Berlin; ein Provider in Russland und am Ende das Atomkraftwerk in Grohnde.
Je nach Altersgruppe und Vorverständnis kann es einige sachliche Verständnisschwierigkeiten geben: Was sind Hacker? – Wo haben sie sich eingeschlichen? Pentagon? Was ist das? – Was ist ein Provider? Je nach Altersgruppe bzw. Voraussetzungen sollten einige Sachbegriffe vorher geklärt werden.

Möglicherweise fallen einigen Zuschauern, gerade den kritischeren, Ungereimtheiten im Film auf: „Unlogisch, dass ein Hacker da reinkommt." – „Wie geht das denn? Ich kann mich doch nicht von hier aus irgendwo einhacken?"
Die Kombination von Hacken und Bombe: „Dann muss er aber doch vorher einmal persönlich da eingebrochen sein, um die Bombe zu installieren." Es handelt sich, mehr kann man dem nicht entgegnen, um einen Fiction-Film; an Agententhriller, z. B. jene mit James Bond, werden solche Anfragen auch nicht gestellt.

Einerseits sollte man also Hilfestellung geben, damit der Film nach einmaligem Sehen richtig verstanden wird. Eine zweite Sichtung ist aber durchaus möglich, z. B. wenn man die Filmsprache analysieren will. Andererseits muss klar sein, dass es nicht auf die Richtigkeit und den Realismus eines jeden Facts ankommt. Schließlich ist „Operation Bluebird" ein Fiction-Film, der auf seine Weise Gefühle und Gedanken anregen will, aber nicht etwas dokumentieren soll. Eine Deutung des Films sollte deshalb vielleicht vom Schluss ausgehen, der signalisiert: So etwas kann jederzeit in unserer Nähe passieren. Die Ein-

schätzung, was passieren kann, welche Ängste wir mit uns herumtragen, kann nicht der Film, sondern muss das Gespräch ergeben.

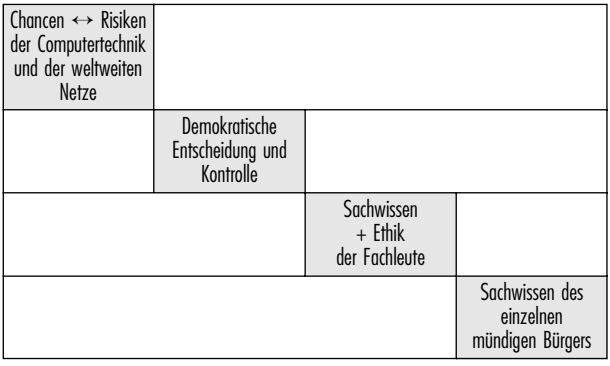
Methodische Anregungen

Ein erster Gesprächseinstieg kann folgendermaßen aussehen: Ist die Szenerie, welche die Filmstory aufbaut, für mich nur unterhaltsame „fiction“, oder weckt sie Unbehagen und Ängste, dass so etwas Ähnliches auch in der Realität passieren könnte? Welche Geschehnisse halten die Zuschauer für vorstellbar, welche für unmöglich?

Einige Beispiele:

- Ist es denkbar, dass eine Bombe hochgeht, wenn eine Computer-Netzleitung gekappt wird?
- Ist es vorstellbar, dass ein Provider in Russland nachts nur mit einem unwissenden Pförtner besetzt ist?
- Ist es vorstellbar, dass sich jemand per Internet in die Sicherheitszentrale eines Atomkraftwerkes einloggt?

Solche Fragen werden kaum letztgültig beantwortet werden können, aber die Diskussion darüber kann eines deutlich machen: der Stand der Informationstechnik ist für die meisten Menschen so undurchschaubar, dass aus der Aura des Geheimnisvollen, die das Internet immer noch umgibt, leicht neue Mythen und Ängste entstehen. Dem könnte sicherlich durch die möglichst weitgehende Information und Aufklärung des Einzelnen entgegengewirkt werden. Aber das ist bei der Menge an Sach- und Detailwissen kaum umsetzbar. Ein zweiter Weg ist, die Entscheidungs- und Kontrollstrukturen bis ins Letzte demokratisch zu gestalten und die verschiedenen Ebenen sachkompetent zu besetzen.



Der Film thematisiert **Zukunftsängste:** Wie sicher sind eigentlich die Daten und die Computernetze unseres Kommunikationszeitalters? Ähnliche Ängste thematisiert der Computerthriller „Matrix“ (USA 1999 von Larry und Andy Wachowski, ebenfalls im Vertrieb des kfw): Der Computer-Hacker Neo entdeckt, dass hinter der vermeintlichen Realität eine böse Welt existiert, die unser aller Leben manipuliert. Weitere Spielfilme zum Thema: „Hackers“ (TV-Movie USA 1996 von Iain Softley), „23 – nichts ist so wie es scheint“ (Deutschland 1998 von Hans Christian Schmid).

Ein weiteres Thema ist die Frage der Erpressbarkeit. Wie leicht sind Staaten zu erpressen, wenn geheime Informationen gefährdet sind oder wenn Menschen bedroht sind?
Erpressung gibt es in meist harmloser Form bereits im zwischenmenschlichen Bereich, besonders auch in Erziehungsfragen: „Wenn du jetzt nicht sofort dein Zimmer aufräumst, dann darfst du nachher nicht …“ oder: „Wenn du mich die Hausaufgaben nicht abschreiben lässt, dann sage ich allen, dass …“ Wo enden eigentlich harmlose „Wenn-dann-Verknüpfungen“, mit denen man etwas bekommen oder erreichen will, und wo fängt Erpressung an?

Für die Erpressbarkeit von Staaten oder Institutionen lassen sich aus der aktuellen Geschichte viele Beispiele finden: Bombendrohungen, Geiselnahmen, Flugzeugentführungen … Das Filmbeispiel ist für die ethische Diskussion vielleicht nicht konkret genug, weil nicht klar ist, welche militärischen Geheimnisse auf dem Spiel stehen. Aber es kann anregend sein, ein vergleichbares Beispiel zu diskutieren: Darf ein Staat einen inhaftierten Schwerverbrecher oder Terroristen auf freien Fuß setzen, wenn damit möglicherweise das Leben einer Geisel gerettet werden kann? Auf den Film bezogen hieße die Frage: Darf die Staatengemeinschaft das Leben vieler Menschen in Brüssel aufs Spiel setzen, um militärische Geheimnisse zu schützen? – Die Diskussion kann in der Gruppe oder Schulklasse anregend als Rollenspiel inszeniert werden; am Entscheidungstisch könnten z.B. sitzen: der Verteidigungs- oder Innenminister (Was wollen sie vor allem schützen?), ein Psychologe (Wie werden die Täter reagieren?), ein Jurist (Welche Position muss die Justiz vertreten?), eine Pfarrerin (Menschenleben ist oberstes Gut.) und zwei direkte Angehörige der gefährdeten Geiseln/Menschen.

Im Film sind sogenannte **„Hacker“** am Werk, die hier allerdings terroristische Ziele verfolgen. Die Computer-„Hacker“ sind aber nicht immer so negativ besetzt, sondern mit ihnen verbindet sich auch der Mythos eines modernen Robin Hood. Ein Thema könnte deshalb auch heißen: Was sind eigentlich „Hacker“? Wie rechtfertigen sie ihr Tun, und wie beurteilen wir das?

Den Mythos spricht folgendes Zitat an: „Hacker, so scheint’s, vermögen die teuflische Macht der Computer und Datenbanken aus den Angeln zu heben. Sie sind die Davids gegen die Goliaths, sie kämpfen stellvertretend für uns alle gegen das Undurchschaubare. Es ist beruhigend, daß es sie gibt – solange solche Husarenstreiche möglich sind, kann es mit dem großen Bruder nicht weit her sein. Gleichzeitig set-

zen sie einen Gestus, eine Idealfigur fort, die in den siebziger Jahren die Jugendkultur geprägt und diverse soziale Bewegungen beeinflußt hat: die Rebellion des einzelnen gegen die anonyme Macht. Die individuelle Subversion gegen die mächtigen Apparate.“ (Matthias Horx, Chip Generation, Reinbek 1984, S. 170.)

Wie Hacker sich selbst sehen, kann man auf den Internetseiten des legendären „Chaos-Computer-Clubs“ (www.ccc.de) erfahren; dort findet man u. a. auch einen ironischen Beitrag zur Frage „Wie werde ich ein Hacker?“. Ernsthafter argumentiert folgender Text: „Zum einen gibt es eine Gemeinschaft, bestehend aus Programmierern und Netzwerk-‚Magiern‘, deren Wurzeln zurück bis in die Zeit der ersten Minicomputer und den frühesten ARPA-Netz-Versuchen reichen. Die Mitglieder dieser Kultur schufen den Begriff ‚Hacker‘. Hacker bauten das Internet, Hacker machten das UNIX Betriebssystem zu dem, was es heute ist, Hacker betreiben das Usenet, Hacker brachten das World Wide Web zum Laufen, Hacker schufen noch viel mehr. Wenn du ein Teil dieser Kultur bist, wenn du zu ihrem Sein und ihrer Entwicklung beigetragen hast, andere Mitglieder wissen wer du bist und dich einen Hacker nennen, erst dann bist du auch wirklich ein Hacker …

Es gibt noch eine andere Gruppe, die sich lautstark als Hacker bezeichnet, diesen Namen aber in keinster Weise verdient. Es sind Menschen (meist pubertierende männliche Wesen), welche einen Spaß daran haben, in Computer einzubrechen und das Telefonnetz zu zerstören. Echte Hacker nennen diese Leute ‚Cracker‘ und wollen mit ihnen nichts zu tun haben. Wirkliche Hacker halten Cracker für ein faules, unverantwortliches und nicht besonders schlaues Pack, denn genauso wenig wie man durch das Knacken von Sicherheitscodes ein Hacker wird, wird man durch das Kurzschließen eines Autos zu einem KFZ-Mechaniker. Unglücklicherweise sind viele Journalisten

und Schreiber darauf verfallen, das Wort Hacker als Beschreibung für Cracker zu verwenden; dies verärgert echte Hacker ungemein. Der grundlegende Unterschied ist: Hacker bauen Dinge auf, Cracker zerstören sie …“ (aus: Eric S. Raymond, Text „How to become a Hacker“, siehe http://koeln.ccc.de/artikel/hacker-howto-esr.html)
Folgende Grundsätze einer **„Hackerethik“** werden dort ebenfalls diskutiert:

- „Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten – fördere Dezentralisierung.
- Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern.
- Mülle nicht in den Daten anderer Leute.
- Öffentliche Daten nützen, private Daten schützen.“

Filmanalytisch bzw. medienpädagogisch kann man den Film unter einer ganz anderen Perspektive betrachten: Wie baut der Film seine Spannung auf? Wie spielen Handlungsebenen/-orte, Schnitt/Montage, Lichtstimmung und Musik zueinander?
Ein solches Projekt hat in der Regel kein großes Budget, um mit großem Aufwand an verschiedensten Orten gedreht werden zu können. Dieses Problem ist in dem Film sehr geschickt gelöst. Es lohnt sich, den Film einmal unter der Frage zu sehen: Wo könnten einzelne Szenen gedreht sein? Wieviel sieht man eigentlich von den jeweiligen Handlungsorten? – Für ganz aktive Gruppen kann die Frage weitergehen: Könnten wir so ein Sujet selbst als Videofilm realisieren?

Literaturhinweise

- „Chancen und Risiken der Mediengesellschaft." Gemeinsame Erklärung der Deutschen Bischofskonferenz und des Rates der Evangelischen Kirche in Deutschland, 1997.
- *Höhns, Martina* (Hg.): Chancen und Risiken der Mediengesellschaft. Ein Lese- und Arbeitsbuch, München: Don Bosco 2000.
- *Zimmermann, Christian:* Der Hacker. Ein Insider packt aus: „Keiner ist mehr sicher", München: Heyne 1998.
- *Power, Richard:* Attacken im Web. Fälscher, Hacker, Datenklauer – die Schattenseiten des Cyberspace, Verlag Markt und Technik.
- Hacking Windows. Wie Hacker in Windows Systeme einbrechen, Verlag dmzsystems.com 2000.

Info: http://www.fieberfilm.de/projekte/abgeschlossen/index.html

Bernward Hoffmann

Kopienverleih: Kirchliche und öffentliche AV-Medienstellen

Kopienverkauf für nichtgewerblichen Einsatz durch:
Katholisches Filmwerk GmbH

Postfach 11 11 52 · 60046 Frankfurt
Ludwigstraße 33 · 60327 Frankfurt

Telefon: (0 69) 97 14 36 - 0 · Telefax: (0 69) 97 14 36 - 13
Internet: www.filmwerk.de · E-Mail: info@filmwerk.de

Herausgegeben vom Programmbereich AV-Medien
Katholisches Filmwerk GmbH, Frankfurt/M.