Intermezzo: Wie schütze ich meine Daten?

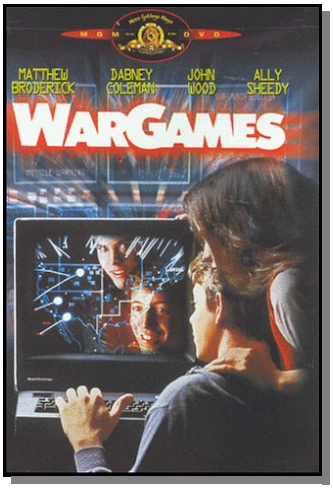

Abb. 1: WarGames

⇨ Der Schüler David Lightman dringt in den Zentralrechner des amerikanischen Militärs ein

⇨ Startsequenzen für Interkontinentalraketen wurden mit Heim-PC ausgelöst

⇨ Thermonuklearer Krieg in letzter Sekunde verhindert

Das sind die Schlagzeilen des Spielfilms „WarGames“. Alles nur blühende Fantasie von Hollywood-Drehbuchautoren, mag man denken, wären da nicht die Gerüchte, dass einige Zeit vor dem Erscheinen des Films ein gewisser K. Mitnick nicht nur in Datenbanken von Online-Shops, Behörden und Militärs eingedrungen sei, sondern eben auch bei NORAD, der Kommandozentrale für die Atomraketen der USA.

Was zunächst sehr spektakulär klingt, war in Wirklichkeit (fast) so einfach wie das Öffnen einer unverschlossenen Tür. Wieso? Nun, die ersten größeren Computernetzwerke entstanden Anfang der Achziger Jahre, als sich in den USA mehrere Universitäten und Forschungseinrichtungen wie z. B. der NASA zusammenschlossen. Ziel war es, einen uneingeschränkten Austausch von Forschungsergebnissen zu realisieren. Insofern ist es nicht verwunderlich, dass kaum ein Gedanke an die Sicherheit der Daten vor ungewünschten Zugriffen verschwendete: Die Daten sollten ja allen frei zur Verfügung stehen. Problematisch wurde die Situation erst, als sich diese Netze mit anderen Netzen, die von militärischen Einrichtungen und Staatsorganen benutzt wurden, zusammenschlossen. Auf diese Weise konnte man über die kaum geschützten Forschungseinrichtungen Zugang zu militärischen Einrichtungen bekommen.

Dies nutzte auch ein deutscher **Hacker**[1] aus Hannover: Im Jahre 1986 verschaffte er sich über die Universität Bremen und das Lawrence Berkeley Laboratory Zugang zu militärischen Computern in den USA. Dort gelangte er an geheime Daten und verkaufte sie an den KGB, den Geheimdienst der Sowjetunion. Er wurde zwar entdeckt und auch verhaftet, musste aber wieder frei gelassen werden, weil es noch keine passenden Gesetze gab.

Auch Banken und Telefongesellschaften wurden das Ziel von Hacker-Angriffen. Manche Hacker verfolgten das ehrliche Ziel, Sicherheitslücken aufzudecken, andere schoben diesen Grund nur vor, um sich selbst zu bereichern. Immerhin wurde deutlich, dass man einerseits den Datenaustausch in Netzwerken sicherer machen musste, andererseits aber auch Gesetze schaffen musste, welche den Umgang mit Daten regeln sollten.

An *deinen* Daten sind Hacker kaum interessiert. Es gibt aber doch Gruppen, die gezielt Daten

[1] Unter einem Hacker versteht man jemanden, der (meist über ein Netzwerk) sich Zugang zu fremden Computern verschafft, diese manipuliert oder dort Daten entwendet. Dabei nutzt er häufig Unachtsamkeiten der Netzwerkverwalter oder Lücken im Sicherheitssystem aus.

von Privatpersonen sammeln. Das sind zum einen Behörden, zum anderen aber auch private Firmen. So sammelt die SCHUFA, eine Schutzgemeinschaft von Kreditinstituten, Handel und anderen Unternehmungen, Daten über die Kreditwürdigkeit von Kunden. Will ein Kunde z. B. eine neue Waschmaschine über Ratenzahlung finanzieren, erkundigt sich der Händler zuerst bei der SCHUFA; sollten dort Hinweise auf eine schlechte Zahlungsmoral des Kunden vorliegen, wird er die Waschmaschine nur gegen Bargeld verkaufen.

Auch viele Rabattsysteme von Warenhäusern sind auf das Sammeln von Kundendaten ausgerichtet. Ziel ist es, das Kaufverhalten genauer zu analysieren, um so Kunden gezielter ansprechen zu können.

Wie werden die Daten heute geschützt?

Daten werden heute auf verschiedene Arten und Weisen geschützt: Zunächst bedient man sich eines so genannten **Firewalls**; dies ist eine Art von Schutzwall, welcher nur bestimmte Arten von Dateien in bestimmte Richtungen und auch nur an bestimmte Adressen hindurch lässt. Bei unzulässigen Versuchen, Daten durch diesen Wall zu schicken oder anzufordern, werden Alarmmeldungen ausgelöst. Der Systemverwalter kann dann nachforschen, wer diese unerlaubten Aktionen versucht hat.

Zum anderen werden wichtige Daten immer häufiger in kodierter Form gesichert und verschickt. Dazu stehen inzwischen zahlreiche zuverlässige Verschlüsselungssysteme zur Verfügung. Wichtig dabei ist, dass das benutzte **Schlüsselwort** für Dritte nicht zu erraten ist: Geburtsdaten sind ebenso tabu wie Namen von Familienmitgliedern. Da es inzwischen auch Kodeknackprogramme gibt, welche sämtliche Worte eines Lexikons austesten, sollte man gänzlich auf die Benutzung von Wörtern verzichten. Empfehlenswert sind sinnlos erscheinende Buchstabenkombinationen wie z. B. HGIWEGZS. Diese Buchstabenkombination findet man garantiert in keinem Lexikon; außerdem ist sie lang genug, so dass sie auch nicht durch Ausprobieren aller Buchstabenkombinationen ermittelt werden kann. Wie aber merkt man sich nun eine solche Kombination? In unserem Fall wurden die Anfangsbuchstaben des Satzes „*H*eute *g*ehe *i*ch *w*ieder *e*inmal *g*ern *z*ur *S*chule“ benutzt.

Aufgaben

1. Wie viele Kombinationen von 3 [8] Großbuchstaben (ohne Umlaute) gibt es?

2. Schätze ab, wie viele Einträge es ungefähr in einem Lexikon von ca. 5000 Seiten gibt? Wie schnell ist ein Kodewort geknackt, wenn jede Kodeüberprüfung eine Millisekunde dauert?

Was sagt das Gesetz heute?

Inzwischen sieht der Gesetzgeber für das Ausspionieren oder Schädigen anderer Computer herbe Strafen vor. Dazu gehören:

§ 202a StGB Ausspähen von Daten
(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.
(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

§ 263 StGB Computerbetrug
(1)Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch Verwendung unrichtiger Einwirkungen auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

§ 303a StGB Datenveränderung
(1)Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

§ 303b StGB Computersabotage
(1) Wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er
1. eine Tat nach § 303a Abs. 1 begeht oder
2. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,
wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.

Auf der anderen Seite haben Privatpersonen durch das **Datenschutzgesetz** aber auch zahlreiche Rechte zur Wahrung ihrer Privatsphäre erhalten. So darf die „speichernde Stelle“ **personenbezogenen Daten** nicht ohne Einwilligung der betroffenen Personen weitergeben; außerdem muss sie für ausreichende Datensicherheit sorgen.

Aufgaben

1. In dem Film „War Games“ verschafft sich der Schüler David Lightman auch Zugang zum Zentralrechner seiner Schule und verändert dort seine Noten. Nach welchem Paragraphen könnte er heute in Deutschland dafür belangt werden? Wie hoch könnte die Strafe ausfallen?

2. Ein Schüler bringt eine mit einem Virus verseuchte Diskette in die Schule... Schreibe eine Geschichte dazu! Versuche am Schluss auch die rechtliche Lage zu erläutern.

3. Welche personenbezogenen Daten sind von dir in deiner Schule gespeichert? Wie wird für ihre Sicherheit gesorgt?

Wie gehe ich mit meinen eigenen Daten um?

Sorgloser Umgang mit den eigenen Daten ist die Hauptursache dafür, dass personenbezogene Daten in falsche Hände gelangen können. In dem folgenden Artikel „WIR WISSEN ALLES ÜBER SIE“ zeigte die Zeitschrift PC Welt im Heft 11/2000, wie ein Herr S. eine Reihe höchst persönlicher Daten preisgab – ohne sich dieser Tatsache bewusst zu sein.

«Im Internet steht mehr über Sie, als Sie denken und als Ihnen vermutlich lieb ist. Wer das Internet aktiv nutzt, hinterlässt nämlich jede Menge Spuren. Aus diesen Mosaiksteinchen lässt sich ein Persönlichkeitsprofil zusammensetzen, das oft mehr über die betreffende Person aussagt, als ihr lieb ist. Viele Internet-Nutzer sind sich nicht bewusst, dass Datenspione – oder beispielsweise auch künftige Arbeitgeber – diese Informationssplitter ohne großen Aufwand noch nach Jahren aufspüren können.

Wir haben einen Praxistest durchgeführt: In der deutschsprachigen Newsgroup de.markt.arbeit.suche – ein Forum für Arbeitsgesuche – pickten wir einen Teilnehmer heraus. Nur mit Hilfe des Internets und von Telefon-CDs versuchten wir, innerhalb einer Stunde möglichst viel über ihn herauszufinden. Das Ergebnis der Recherche lesen Sie im Folgenden.

Die Schilderung unserer Recherchen beruht auf Tatsachen. Den Namen "Hermann Steinbaumer" haben wir allerdings erfunden. Sollte es tatsächlich einen "Hermann Steinbaumer" geben, so hat er nichts mit unserem "Hermann" zu tun. Außerdem haben wir einige Angaben abgewandelt, um Rückschlüsse auf die reale Person unmöglich zu machen. Der Test fand am 29.9.2000 statt.

16:00 Uhr: Wir starten mit unserem Experiment. In unserem Newsreader öffnen wir das Forum de.markt.arbeit.suche und sehen uns einige der Stellengesuche an. Unsere Wahl fällt auf die Nachricht von Hermann Steinbaumer. Er sucht einen neuen Job als Ski- und Volleyball-Trainer. Wir notieren seine Mailadresse – denn die Suche nach seinem Vor- und Nachnamen würde in Suchmaschinen wahrscheinlich zu viele Treffer liefern.

16:06 Uhr: Unter www.deja.comlhome_ps.shtml geben wir als Suchkriterium seine Mailadresse ein. Die Suchmaschine listet zwölf Nachrichten auf, die meisten Fundstellen befinden sich in de.markt.arbeit.suche. Dort hat er in regelmäßigen Abständen gepostet. Der Tenor von Hermanns Nachrichten: "Nach meinem letzten Projekt suche ich nun ein neues. Erfahrungen in Ski- und Volleyball-Kursen. Anfragen beziehungsweise Angebote unter ..." Merkwürdig: Einige Angaben widersprechen sich. In manchen Postings spricht Hermann von "Projekten", dann wieder von Fortbildungsmaßnahmen des Arbeitsamts. Jedenfalls haben wir jetzt schon eine – zumindest grobe – Vorstellung davon, welche Fähigkeiten Hermann hat und dass er schon seit längerer Zeit arbeitslos ist. In einer Antwort auf ein Posting in der Newsgroup de.markt.arbeit.d verrät er sogar sein Alter – 43 Jahre – und seine Handy-Nummer. Hermann ist wohl ziemlich offenherzig.
In einer Nachricht in fido.ger.medizin empfiehlt er ein Antidepressivum, sein Arzt habe ihm das Mittel zur Linderung seiner manischen Depression verschrieben. Wir hoffen für ihn, dass potenzielle Arbeitgeber nicht die gleichen Recherchen anstellen wie wir – sonst sieht es wohl schlecht für Hermann aus. Seit Beginn unseres Tests sind rund 18 Minuten vergangen.

16:18 Uhr: Wir sehen uns die Header der Nachrichten von Hermann an und haben Glück: Er ist T-Online-Kunde. Bei diesen ist häufig in den Headern die Telefonnummer - inklusive Vorwahl enthalten. Das ist auch bei Hermann der Fall. Aus dieser Vorwahl lässt sich natürlich leicht auf den Wohnort schließen, Hermann wohnt also wahrscheinlich in München. Wir surfen zu www.teleauskunft.de, klicken auf "Telefonbuch" und geben Hermanns Vor- und Nachnamen sowie den Wohnort in die entsprechenden Felder ein. Die Suchmaschine spuckt daraufhin brav die Straße aus, in der Herr Steinbaumer wohnt. Selbst wenn Hermann in der Newsgroup einen falschen Namen benutzt hätte, wären wir ihm auf die Spur gekommen. Da wir seine Telefonnummer haben, könnten wir mit einer handelsüblichen Telefon-CD und einem Add-on aus dem Interner eine so genannte Rückwärtssuche durchführen: Das bedeutet, der Anwender gibt nur eine Telefonnummer ein, und das Add-on ermittelt den dazugehörigen Teilnehmer.

Doch auch ohne diese Zusatz-Software liefern Telefon-CDs weitere nützliche Informationen. Mit "Tele-Info 2000" lässt sich beispielsweise leicht herausfinden, ob Hermann in einem Ein- oder Mehrfamilienhaus wohnt. Denn die CD akzeptiert als Suchkriterien auch den Wohnort, die Straße und Hausnummer. Als Ergebnis listet sie bei einer solchen Anfrage alle Bewohner eines Hauses auf – vorausgesetzt, diese haben sich mit ihrer Adresse im Telefonbuch eintragen lassen.
Wir wissen jetzt, dass Hermann in einem Mehrfamilienhaus wohnt. Wie es in seiner Straße aussieht? Auch das ist schnell geklärt: Die CDs "Talk & Show" liefern Bilder und Videos von vielen Gegenden, jedenfalls wenn diese in einer größeren Stadt liegen. Hermann wohnt in einem Altbau, in der Straße stehen ausschließlich Autos der unteren Preisklasse. Gewiss, nur ein Indiz – aber es drängt sich der Verdacht auf, dass es sich nicht um die beste Gegend Münchens handelt und Hermann wahrscheinlich nicht gerade wohlhabend ist.

16:35 Uhr: Das Bequemste wäre natürlich, wenn Hermann eine Homepage hätte – auf der er möglichst viel von sich preisgibt. Da sich jeder Domain-Besitzer normalerweise in einer Datenbank registrieren muss, entschließen wir uns, diese Quelle zu durchforsten: Unter www. ripe.net/cgi-bin/ripedbsearch geben wir "Hermann Steinbäumer Muenchen" ein (die Suchmaschine verträgt keine Umlaute). Hermann tut uns nicht den Gefallen - er hat keine Domain registriert.

16:40 Uhr: Mal sehen, was über Hermann im World Wide Web noch zu finden ist. Wir versuchen es bei www.metacrawler.com, einer der zahlreichen Metasuchmaschinen im Netz. Hermanns Mailadresse ist nicht zu finden - ein Fehlschlag. Keine der Suchmaschinen hat sie erfasst. Uns bleibt also nichts anderes übrig, als seinen Vor- und Nachnamen in die Suchmaschine einzugeben. Metacrawler spuckt rund 30 Seiten aus, auf denen der Begriff "Hermann Steinbaumer" steht - wir müssen also eine Seite nach der anderen abklappern. In einem Web-Forum für Sportinteressierte werden wir fündig: Dort klagt ein "Hermann Steinbaumer" darüber, dass das Fitness-Studio XY ihn nicht mehr als Volleyball-Trainer beschäftigt. Allerdings stimmt die Mailadresse nicht mit der überein, die in seinen Newsgroup-Nachrichten steht. Sie ist von einem Gratis-Mailanbieter und besteht nur aus Zahlen- und Buchstabenkombinationen. Vielleicht hat sich Hermann eine Tarnadresse besorgt? Sicher können wir da nicht sein, aber die Wahrscheinlichkeit ist groß, dass er es ist. Nicht ausgeschlossen, dass er öffentlich über den "bösen" Arbeitgeber jammert. 16:50 Uhr: Wir entschließen uns, noch einmal - jetzt aber mit der vermutlichen Tarn-Mailadresse von Hermann - in Newsgroups nach Beiträgen zu suchen. Unter www.deja.com/home~s.shtml geben wir diese Mailadresse ein. Die Suchmaschine listet 14 Artikel auf, alle im Forum z-netz.alf.erotik.geschichten – der Name der Newsgroup sagt deutlich, worum es geht. Dort hat ein "Markus Maier" – allerdings mit der Mailadresse, die im Web-Forum für Sportinteressierte ein "Hermann Steinbaumer" benutzt – Kommentare zu den erotischen Geschichten abgegeben. Kuschelsex macht ihm offensichtlich am meisten Spaß.

16:58 Uhr: Wir brechen die Recherchen ab. Nicht ohne ein mulmiges Gefühl: Wir wissen jetzt wahrscheinlich mehr über Hermann Steinbaumer, als er uns nach ein paar Gläsern Wein erzählen würde. Der Fall zeigt: Obwohl unsere Testperson Hermann Steinbaumer im Internet nicht übermäßig aktiv war – er hatte etwa keine Homepage –, ließen sich jede Menge Infos über ihn zusammentragen. Selbst die Tarnung mit einem falschen Namen und der Adresse eines Gratis-Maildienstes nutzte in diesem Fall wenig, da er diese Adresse zusammen mit seinem realen Namen benutzt hat.

Das Problem war nicht ein einzelnes Posting, sondern das Bild, das sich aus vielen Mosaiksteinchen zusammensetzen ließ. Online-Datenbanken und Internet-Suchmaschinen übernehmen bei derartigen Recherchen die zentrale Rolle - jeder kann mit diesen Werkzeugen bequem und schnell vom Schreibtisch aus die Informations-Fetzen zusammentragen. Es ist nicht einmal besonderes technisches Know-How notwendig.»

Aufgaben

1. Fasse in einem Steckbrief alle Informationen zusammen, die über Herrn Steinbaumer (in einer einzigen Stunde!) zusammengetragen wurden. Welche dieser Informationen könnten für Herrn Steinbaumer schädlich sein?

2. Überlege, wer (außer deinen Freunden und bekannten) Informationen von dir gesammelt haben könnte.

3. Die im Text erwähnten Telefon-CDs dürfen heute nicht mehr die Möglichkeit bieten, zu einer eingegebenen Telefonnummer Name und Anschrift suchen zu lassen. Warum ist dies (durch das Datenschutzgesetz) untersagt?

4. Es wird behauptet, dass manche Netzbetreiber die Position eines Handys bis auf wenige hundert Meter bestimmen können. Versuche herauszufinden, ob an dieser Behauptung etwas Wahres ist. Schreibe einen Kurzkrimi, in welchem diese Möglichkeit einem Ganoven zum Verhängnis wird.

5. Kopiere das Verzeichnis `source\Datenschutz` auf deine Festplatte. Starte das Programm `glas.exe` von der Festplatte aus und folge den Anweisungen des Programms. Speichere die Ergebnisse im selben Verzeichnis, wenn du mit dem „Test“ fertig bist. Schließe nun das Programm. Schau dir anschließend mit einem Texteditor die Datei `Ergebnis.ini` im selben Verzeichnis an. Was könnte man aus den dort gespeicherten Informationen schließen?
   Ähnliche Programme werden auch manchmal bei Eignungstests benutzt. Nimm Stellung!