Themenblätter
im Unterricht

Frühjahr 2004_Nr. 33

extra

Internet-Sicherheit

bpb: Bundeszentrale für politische Bildung

Staat. Gesellschaft. **Wirtschaft. Internationales.** Ethik.

INHALT

Seite 3 – 6	Anmerkungen für die Lehrkraft
Seite 7 – 62	2 Arbeitsblätter im Abreißblock zum Thema: *Internet-Sicherheit.*
Seite 63	Literaturhinweise und Internetadressen

Bestellcoupon auf S. 63/64

Zum Autor:

Ludwig Janssen, Jahrgang 1954, ist ausgebildeter Elektriker, hat an der Gesamthochschule Kassel Sozialarbeit und an der Universität Bonn Politik und Geschichte studiert. Er arbeitet seit 1996 freiberuflich als Autor, Redakteur und Lektor in Köln. Seine Themenschwerpunkte sind Politik und Zeitgeschichte, Neue Medien und Internet, Gesundheit und Psyche sowie Technik. Er arbeitet hauptsächlich für Verlage, Verbände und öffentliche Einrichtungen. Zu seinen kontinuierlichen Projekten gehört das Psychiatrienetz (*www.psychiatrie.de*), das er redaktionell betreut. Für den Cornelsen Verlag und das Projekt „Erinnern für Gegenwart und Zukunft“ (*www.erinnern-online.de*) stellt er regelmäßig Unterrichtsmaterialien zu aktuellen politischen Themen zusammen. Als Lektor hat er zuletzt ein Buch zum Thema Alter und Altern bearbeitet. Für das Buch „HTML und Internet für Lehrer und Schüler“ zeichnet er als Autor verantwortlich. Im Jahr 2003 hat er eine Arbeitshilfe „Psychiatrie und Öffentlichkeitsarbeit“ herausgegeben.
E-Mail: *info@ljanssen.de*, Internet: *www.ljanssen.de*

Themenblätter

➜ *www.bpb.de* >Publikationen (dort auch die vergriffenen)

Nr. 1: Menschliche Embryonen als Ersatzteillager? Bestell-Nr. 5.351
Nr. 2: Die Ökosteuer in der Diskussion Bestell-Nr. 5.352
Nr. 3: Bundestag/Bundesrat (vergriffen)
Nr. 4: Demokratie: Was ist das? Bestell-Nr. 5.354
Nr. 5: Fleischkonsum und Rinderwahn Bestell-Nr. 5.355
Nr. 6: Deutschland, deine Inländer Bestell-Nr. 5.356 (vergriffen)
Nr. 7: Neuer Markt: Internet und Copyright Bestell-Nr. 5.357
Nr. 8: Zivilcourage: Eingreifen statt zuschauen! Bestell-Nr. 5.358
Nr. 9: Pop und Politik Bestell-Nr. 5.359
Nr. 10: Wer macht was in Europa? Bestell-Nr. 5.360
Nr. 11: Geben und Nehmen im Bundesstaat Bestell-Nr. 5.361
Nr. 12: Krieg oder Frieden? Bestell-Nr. 5.362 (vergriffen)
Nr. 13: Terror und Rechtsstaat Bestell-Nr. 5.363 (vergriffen)
Nr. 14: Erinnern und Verschweigen Bestell-Nr. 5.364
Nr. 15: Die Osterweiterung der Europäischen Union Bestell-Nr. 5.365 (vergriffen)
Nr. 16: Mobbing Bestell-Nr. 5.366
Nr. 17: Religion und Gewalt Bestell-Nr. 5.367 (vergriffen)
Nr. 18: Schule und was dann? Bestell-Nr. 5.368 (vergriffen)
Nr. 19: Familie und Frauen-Rollen Bestell-Nr. 5.369
Nr. 20: Der Bundestag – Ansichten und Fakten Bestell-Nr. 5.370
Nr. 21: Hotel Mama – oder die Kunst erwachsen zu werden Bestell-Nr. 5.371
Nr. 22: Lust auf Lernen Bestell-Nr. 5.372
Nr. 23: Koalieren und Regieren. Bestell-Nr. 5.373
Nr. 24: 17. Juni 1953 und Herbst ’89. Bestell-Nr. 5.374
Nr. 25: Heimat ist, wo ich mich wohlfühle. Bestell-Nr.: 5.375
Nr. 26: Bevölkerungsentwicklung und Sozialstaat. Bestell-Nr.: 5.376
Nr. 27: Aktien – Chancen und Risiken. Bestell-Nr. 5.377
Nr. 28: Globalisierung – Ängste und Kritik. Bestell-Nr. 5.378
Nr. 29: Nationale Symbole Bestell-Nr. 5.379
Nr. 30: Arbeitslosigkeit – Ursachen und Abhilfen Bestell-Nr. 5.380
Nr. 31: Zuwanderung nach Deutschland Bestell-Nr. 5.381
Nr. 32: Familienbande Bestell-Nr. 5.382
Nr. 33: Internet-Sicherheit Bestell-Nr. 5.383
Nr. 34: Europa der 25 – Osterweiterung der EU. Bestell-Nr. 5.384
Nr. 35: Staatsverschuldung – Ausmaß und Folgen Bestell-Nr. 5.385
Nr. 36: Präsidentschaftswahlen in den USA Bestell-Nr. 5.386
Nr. 37: 20. Juli 1944: Attentat auf Hitler Bestell-Nr. 5.387
Nr. 38: Jugendbeteiligung in der Demokratie Bestell-Nr. 5.388

Impressum

Herausgegeben von der Bundeszentrale
für politische Bildung/bpb
Adenauerallee 86, 53113 Bonn
www.bpb.de
E-Mail der Redaktion: moeckel@bpb.de

Autor: Ludwig Janssen
Redaktion: Iris Möckel (verantwortlich), Sabine Klingelhöfer

Gestaltung: Leitwerk. Büro für Kommunikation, Köln
Titelbild: Leitwerk
Druck: Neef + Stumme, Wittingen

1. Auflage: April 2004
ISSN 0944-8357
Bestell-Nr. 5.383 (siehe Bestellcoupon S. 63)

Ludwig Janssen

Internet-Sicherheit

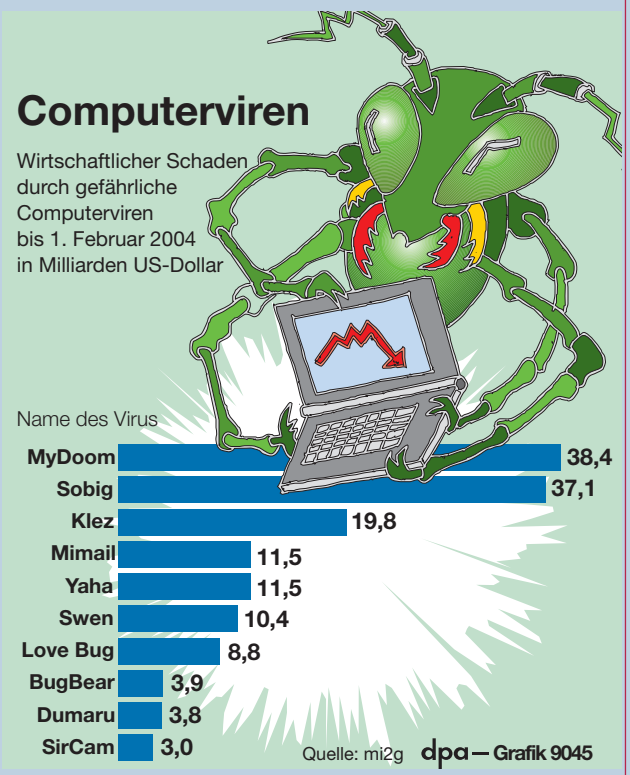
Grundlegende, leicht verständliche Informationen zum Internet und zur Sicherheit im Internet auf der Website des Bundesamtes für Sicherheit im Internet: unter ➜ *www.bsi-fuer-buerger.de*

Das Internet hat in den letzten Jahren eine rasante Entwicklung genommen. Die globale und länderübergreifende Kommunikation hat dazu geführt, dass die Welt näher zusammengerückt ist. Immer mehr private und gesellschaftliche Aktivitäten und Geschäftsprozesse verlagern sich ins Internet. Dazu gehören (insbesondere für Jugendliche) neben der Informationsbeschaffung auch die Kommunikation in öffentlichen Foren, Chats und mit Freunden, Unterhaltung mit internetbasierten Spielen, Beschaffung von Musik, Filmen und Software über Tauschbörsen, Einkauf oder Homebanking.

Es vergeht aber auch kaum ein Tag, an dem die Medien nicht über Datenmissbrauch, Hacker-Angriffe, Computerviren oder horrende Telefonrechnungen berichten. Statt sachlicher Information verbreiten sie jedoch häufig Sensationsgeschichten, die eher Angst, Verwirrung und Verunsicherung auslösen.

Jugendliche bewegen sich sorglos im Internet

Eine Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI: ➜ *www.bsi.bund.de*) aus dem Jahr 2003 belegt, dass es Jugendlichen an der Bereitschaft mangelt, sich aktiv vor Sicherheitsrisiken im Internet zu schützen. In der Studie wird festgestellt, dass beim Thema Sicherheit im Internet „Sorglosigkeit und Ignoranz" vorherrschen. Selbst wer über die Gefahren informiert ist, beschäftigt sich häufig erst damit, wenn Schaden entstanden ist. Auch wenn Mädchen bei der Nutzung des Internets in den letzten Jahren aufgeholt haben: Groß ist immer noch der Wissensunterschied zwischen Mädchen und Jungen beim Thema Internetsicherheit. Während sich jedes zweite Mädchen zwischen zwölf und 18 Jahren mit Internetsicherheit nicht auskennt, ist es bei den Jungen „nur" jeder Vierte.



Spektakuläre Angriffe

Ziele spektakulärer Angriffe auf Rechner von außen sind hauptsächlich große Unternehmen oder öffentliche Einrichtungen. Einen solchen spektakulären Hacker-Angriff gab es beispielsweise im April 1998 auf das US-Verteidigungsministerium. Dabei soll eine Software zur Kontrolle des militärischen Kommunikationsnetzwerks gestohlen worden sein sowie eine weitere, mit der sich die Position von U-Booten feststellen lässt. Allein im Jahr 1999 hat das US-Verteidigungsministerium 22.114 Attacken registriert. Viele spektakuläre Angriffe werden allerdings gar nicht erst bekannt, weil Unternehmen und Einrichtungen kein Interesse daran haben, dass ihre Sicherheitslücken in die Öffentlichkeit gelangen.

bpb: Hrsg.: Bundeszentrale für politische Bildung, 53113 Bonn. Autor: Ludwig Janssen. Verantwortl. Redakteurin: Iris Möckel. Gestaltung: Leitwerk, Köln.

Gefahren für private Anwender

Auf fast jedem Rechner befinden sich Informationen, die in falsche Hände geraten und missbraucht werden können. Sobald der Rechner eine Online-Verbindung herstellt, kann auch von außen darauf zugegriffen werden. Egal, ob man im Internet surft, eine E-Mail verschickt oder Daten austauscht: Der Rechner ist damit Teil eines weltweiten Netzwerkes. Er empfängt und sendet Daten und hinterlässt Spuren.

Malware ist der Überbegriff für Software, deren Zweck es ist, dem Anwender zu schaden. Das Kunstwort setzt sich aus den englischen Begriffen „malicous“ (bösartig) und „Software“ zusammen. Damit sind Computerviren, E-Mail-Würmer, Trojanische Pferde, 0190-Dialer und Spyware gemeint.

Computerviren und E-Mail-Würmer: Mitte 2002 waren weltweit mehr als 90.000 **Computerviren** im Umlauf. Täglich sollen etwa 20 neue hinzu kommen. Sie können sich selbstständig vervielfältigen und beispielsweise harmlose Bilder auf dem Bildschirm einblenden, aber auch die Formatierung der Festplatte zum Ziel haben. Computerviren verbreiten sich mit einer infizierten Datei, die über einen Datenträger oder per E-Mail weiter gegeben wird.

In Zeiten der weltweiten Kommunikation verbreiten sich Computerviren hauptsächlich über **E-Mail-Würmer**. Ihr Ziel ist es, in möglichst kurzer Zeit möglichst viele Rechner zu infizieren. Um sich fortzupflanzen, müssen E-Mail-Würmer keinen fremden Programmcode infizieren. Sie verbreiten sich selbstständig.

Die bekanntesten Computerviren und E-Mail-Würmer haben die Namen „Sobig“, „Michelangelo“, „Melissa“, „Loveletter“, „Code Red“, „Klez“ und „Sapphir“. „Michelangelo“ nistete sich am 6. März 1992, dem Geburtstag des italienischen Malers und Bildhauers, in viele Rechner ein und löschte ihre Festplatten. „Melissa“ nutzte 1999 als erster Computervirus die Adress-bücher von Outlook für seine Verbreitung. „Loveletter“ hat im Mai 2000 innerhalb kürzester Zeit weltweit auf 10 Millionen Rechnern Bild- und Musikdateien zerstört. Der wirtschaftliche Schaden und die Kosten lagen Schätzungen zufolge weltweit bei etwa 50 Milliarden US-Dollar. „Code Red“ befiel im Jahr 2001 binnen weniger Stunden 250.000 Rechner. Im Jahr 2002 nutzte „Klez“ eine Sicherheitslücke von Outlook Express und verbreitete sich über gefälschte E-Mail-Adressen. Im Januar 2003 griff „Sapphir“ (auch „Slammer“ oder „SQ hell“) weltweit zehntausende Server an. Dadurch funktionierten beispielsweise in Seattle an einem Samstag für mehrere Stunden die Notrufnummern von vielen Polizei- und Feuerwehrbezirken nicht. Im Jahr 2003 wurde schließlich Blaster/Loveson freigesetzt, um Microsoft-Server mit Anfragen zu überfluten.

Das Problem von „Monopolen“

Weil etwa 90 Prozent der Privatanwender weltweit mit einem Betriebssystem von Microsoft arbeiten, wird Malware hauptsächlich auch für Microsoft-Produkte entwickelt. Etwa 95 Prozent nutzen den Internet Explorer, und sehr viele bevorzugen als E-Mail-Werkzeug Outlook Express.
Die Dominanz von Microsoft, Sicherheitslücken, Schwachstellen, Standardeinstellungen und die Kombination von Betriebssystem, Browser und E-Mail-Werkzeug von Microsoft ermöglichen es erst, Rechner weltweit innerhalb kürzester Zeit zu infizieren (siehe auch Anhang).

Wer entwickelt und verbreitet Computerviren?

Schon seit 1991 gibt es frei verfügbare Baukästen für die Programmierung von Computerviren, so genannte **Virus Construction Kits**. Damit kann jede/r – auch ohne Programmierkenntnisse – Computerviren erstellen und in Umlauf bringen.
Jugendliche nutzen solche Werkzeuge und entwickeln damit Computerviren – aus Spaß oder um anderen zu imponieren. Andere möchten ihre Fähigkeiten beweisen, um als Programmierer oder Sicherheitsexperten engagiert zu werden. Szene- oder Computerfreaks müssen ihr Können unter Beweis stellen, um in eine Hackergruppe aufgenommen zu werden. Dass sich unzufriedene Mitarbeiter durch die Verbreitung von Viren „rächen“, passiert immer häufiger. Sicherheitsexperten entwickeln Viren, um auf zukünftige Entwicklungen vorbereitet zu sein. Sie analysieren sie und erarbeiten Lösungen für ihre Bekämpfung. Es wird auch gemunkelt, dass die Hersteller von Antiviren-Software neue Computerviren in Umlauf bringen, um ihren Umsatz zu steigern. Beweise dafür gibt es allerdings nicht.

Weitere Gefahren für Privatanwender

Trojanische Pferde (auch: Trojaner) sind in böswilliger Absicht geschriebene Programme, die meistens in einem nützlichen Programm versteckt werden. Nach dem Start des Programms wird das Trojanische Pferd aktiviert und richtet nicht selten erheblichen Schaden an. Mit einem Trojaner können aber auch vertrauliche Informationen wie beispielsweise Passwörter ausspioniert werden. Im Unterschied zu Computerviren können sie sich nicht selbständig weiterverbreiten.

Um den Zahlungsverkehr im Internet zu vereinfachen, wurden Einwahlprogramme, so genannte **0190-Dialer**, entwickelt. Damit können z.B. kostenpflichtige Klingeltöne für das Handy über die Telekom abgerechnet und bezahlt werden. Sie können aber auch zu einer Kostenfalle werden, wenn sie unbemerkt installiert werden. Damit kann – statt der eigenen kosten-

Hrsg.: Bundeszentrale für politische Bildung, 53113 Bonn. Autor: Ludwig Janssen. Verantwortl. Redakteurin: Iris Möckel. Gestaltung: Leitwerk, Köln.

günstigen Verbindung – eine teure Verbindung zum Internet aufgebaut werden. Statt der üblichen 2 bis 4 Cent pro Minute können damit bis zu 1,86 Euro pro Minute anfallen, manchmal sogar 900 Euro pro Einwahl.

Cookies sind kleine Dateien, die auf den Rechner abgelegt werden. Sie können hilfreich und praktisch sein, weil sie einen Besucher beim nächsten Besuch einer Website wieder erkennen, und sie können dazu dienen, Internetseiten auf persönliche Wünsche zuzuschneiden. Mit Cookies kann aber ein sehr genaues Benutzerprofil des Besuchers angelegt werden. Weil sie keine ausführbaren Programme sind, stellen sie kein unmittelbares Sicherheitsrisiko dar, sondern berühren lediglich den Datenschutz.

Statt Cookies werden häufig auch **Webbugs** verwendet. Sie sind nur pixelgroß und unsichtbar in einer Website versteckt. Mit ihrer Hilfe können ebenfalls die Internetgewohnheiten der Benutzer herausgefunden und Benutzerprofile erstellt werden.

Spyware hinterlässt auf dem Rechner eine Identifikationsnummer, spioniert ihn aus und kann ihn eindeutig identifizieren. Sie registriert beispielsweise, welche Websites besucht und welche Dateien heruntergeladen werden oder kopiert E-Mail-Adressen und andere persönliche Daten vom Rechner.

Aktive Inhalte ermöglichen die Einbindung von multimedialen Effekten und Spezialfunktionen in einen Browser. Verbreitete Technologien sind ActiveX, JavaScript und VBScript. ActiveX ist eine von Microsoft entwickelte Technologie, die dafür sorgt, dass Windows-Anwendungen mit dem Internet zusammenarbeiten. Die Nutzer haben allerdings keine Kontrolle darüber, was aktive Inhalte auf dem Rechner machen. Ihr Funktionsumfang kann nicht kontrolliert oder eingeschränkt werden.

Welche Interessen werden verfolgt?

Wer ein Interesse an der Entwicklung von Computerviren und -würmern hat, wurde weiter oben bereits dargestellt.

1. Wenn der Aufwand vertretbar ist, kann es für Kriminelle durchaus lohnenswert sein, über einen Trojaner Passwörter für das Online-Banking oder Zugangsdaten für den Internetzugang auszuspionieren.

2. Die unbemerkte Installation eines 0190-Dialers für eine teure Verbindung bringt dem Urheber innerhalb kürzester Zeit eine große Summe ein. Schließlich merken viele dies erst mit der nächsten Telefonrechnung.

3. Cookies, Webbugs und Spyware werden hauptsächlich eingesetzt, um Nutzerprofile zu erstellen und diese mit den E-Mail-Adressen zu verkaufen, um damit zielgerichtet werben zu können.

Sicherheitsmaßnahmen

Weil in dem Arbeitsblatt konkrete Sicherheitsmaßnahmen in Form einer Checkliste abgefragt werden, wollen wir an dieser Stelle nur allgemein wichtige Sicherheitsaspekte benennen:

- Datensicherung
- Passwortschutz und Datenverschlüsselung
- Schließen von Sicherheitslücken
- Regelmäßige Updates und Installation von Sicherheitspaketen (Patches)
- Konfiguration der Software unter Sicherheitsaspekten
- Einsatz von Antivirensoftware, Firewall und anderen Sicherheits-Werkzeugen
- Im „Ernstfall“ Aktivitäten protokollieren und Angreifer zurückverfolgen.

Ausführliche Sicherheitstipps unter:
➜ ***www.sewecom.de/pc-sicherheitstipps/index.html ;***
dort findet man auch die Datenbank der registrierten Dialer.

Zum Arbeitsblatt

Mit dem Arbeitsblatt sollen in erster Linie der Informationsstand und das Problembewusstsein der Schülerinnen und Schüler erfragt werden. Eine **persönliche Checkliste** dient dazu, das eigene Sicherheitsverhalten kritisch zu hinterfragen und soll Anlass sein, es gegebenenfalls zu verändern.

Die Beschäftigung mit der **Dominanz von Microsoft** bei Betriebssystem und Software soll dazu beitragen, mit den Produkten kritisch umzugehen. Das Beispiel ergibt einen Anlass, über **Monopolbildung** generell, deren Vor- und Nachteile für Betreiber und Benutzer bzw. Nachfrager und Anbieter zu recherchieren und zu diskutieren.

Der Wissensunterschied von Jungen und Mädchen beim Thema Internetsicherheit kann Anlass sein, das Arbeitsblatt geschlechtsspezifisch auszuwerten und die unterschiedlichen Antworten von Jungen und Mädchen zu thematisieren.

Ein Thema, das im Unterricht direkt anschließen könnte, wäre der Bereich „Internet und Datenschutz“.

Karikatur: Martin Guhl

bpb: Hrsg.: Bundeszentrale für politische Bildung, 53113 Bonn. Autor: Ludwig Janssen. Verantwortl. Redakteurin: Iris Möckel. Gestaltung: Leitwerk, Köln.

Anhang

Microsoft
Microsoft ist der weltweit größte Softwarehersteller mit Hauptsitz in Redmond, einem Vorort von Seattle (US-Bundesstaat Washington). Das Unternehmen wurde 1975 von Bill Gates und Paul Allen gegründet, um BASIC-Interpreter zu entwickeln und zu verkaufen (...).
Der Softwarekonzern Microsoft besitzt, seit dem Erfolg des PC durch IBM, im Desktop-Markt für PC-Betriebssysteme eine marktbeherrschende Stellung. Fast jeder neue PC wird mit einem vorinstallierten Windows-System ausgeliefert. In einem Gerichtsverfahren vor einem US-Gerichtshof wurde festgestellt, dass Microsoft seine monopolartige Stellung im Betriebssystemmarkt mittels der nahtlosen Integration des Internet Explorers in das Betriebssystem dazu missbraucht hat, Konkurrenten im Web Browser-Markt, vor allem Netscape vom Markt zu drängen.

Jahr	Angestellte	Umsatz in Mio. US-$
1980	40	8
1985	910	140
1990	5200	1000
2000	50000	25300

Quelle: http://www.net-lexikon.de/Microsoft.html

Monopol
Ein Monopol nennt man eine Marktsituation, in der nur ein Anbieter oder Nachfrager die Preise in einem Marktsegment kontrollieren kann. Das Wort lässt sich auf das griechische „monos“ (allein) und „polein“ (verkaufen) zurückführen (…).

Ausprägungen
Je nachdem, ob nun der Anbieter oder der Nachfrager das Monopol hält, wird zwischen Angebots- und Nachfragemonopol unterschieden. Stehen einem Monopolisten nur wenige statt vieler Nachfrager/Anbieter gegenüber, handelt es sich um ein beschränktes Monopol. Treten auf beiden Seiten nur ein Anbieter und ein Nachfrager auf, spricht man von einem zweiseitigen Monopol.
Der Begriff Monopol wird auch dort angewandt, wo zwar eine gewisse Konkurrenz vorhanden ist, aber der Marktanteil des Monopolisten so hoch ist, dass er als einziger aktiv in die Preisbildung eingreifen kann.

Angebotsmonopole:
- Deutsche Telekom (nach wie vor Quasi-Monopolist, v.a. in den Ortsnetzen und im Analogbereich)
- Deutsche Post AG im Briefversand (siehe auch: Briefmonopol)
- Deutsche Bahn AG
- Microsoft bei Betriebssystemen für Personal Computer

Nachfragemonopole:
(meistens beschränkte Nachfragemonopole):
- meistens bei militärischen Produkten
- Zulieferer für Angebotsmonopole, z.B. Güterzüge für die Bahn

Strategien und Wirtschaftspolitik
Eines der wesentlichen Ziele des Monopolisten ist es, den Markt weiterhin vor möglichen Konkurrenten abzuschirmen und den höchstmöglichen Gewinn abzuschöpfen. Um dies zu erreichen, wird auch zu unlauteren oder marktverzerrenden Mitteln gegriffen. Beispiel einer solchen Praxis ist es, Produkte eine gewisse Zeit zu nicht kostendeckenden Preisen anzubieten, bis der Konkurrent aus dem Markt verdrängt wurde, um anschließend die Preise wieder zu erhöhen. Diese Situation kann auch durch ein Kartell entstehen, oder durch ein Oligopol.

Falls Monopole nicht aus natürlichen Gründen aufgebrochen werden, greift gelegentlich der Staat aus wettbewerbsrechtlichen Gründen ein. Meistens liegt in diesen Fällen ein Verstoß gegen das UWG (Gesetz gegen den unlauteren Wettbewerb) oder das GWB (Gesetz gegen Wettbewerbsbeschränkungen) vor. Beispielsweise wurde Microsoft von der EU-Kommission am 24.3.2004 verurteilt, seine Marktmacht missbraucht zu haben und wurde mit einem Bußgeld von 497 Millionen Euro bestraft.

Quelle: http://www.net-lexikon.de/Monopol.htm

Den aktuellen Stand im Wettbewerbsverfahren der EU-Kommission: ➜ *www.heise.de*

Hrsg.: Bundeszentrale für politische Bildung, 53113 Bonn. Autor: Ludwig Janssen. Verantwortl. Redakteurin: Iris Möckel. Gestaltung: Leitwerk, Köln.

Ludwig Janssen

Internet-Sicherheit

Lückentest

Bei der Definition der folgenden Sicherheitsrisiken fehlen wichtige Begriffe.
Ergänzen Sie diese aus der alphabetischen Liste unten.

1. Ein Computervirus kann sich selbständig ..... und .....
2. Der Funktionsumfang von aktiven Inhalten (ActiveX, JavaScript und VBScript) ist nicht ..... und kann nicht ..... werden.
3. Ein Trojanisches Pferd ..... sich in einer anderen Software und wird heimlich auf den Rechner installiert, um ihn ..... und/oder Daten zu .....
4. Cookies sind kein ..... und erlauben es, die Benutzer beim nächsten Besuch wieder zu ..... und Internetseiten zu .....
5. Ein 0190-Dialer ist ein ....., das sich häufig ..... installiert und eine ..... Verbindung durch eine teure ersetzt.
6. ..... ist eine Software zum ..... der Benutzergewohnheiten.

Ausspionieren	auszuspionieren	eingeschränkt	Einwahlprogramm	erkennen
kontrollierbar	kostengünstige	personalisieren	Sicherheitsrisiko	Spyware
stehlen	unbemerkt	verbreiten	vermehren	versteckt

Der „Loveletter"-Virus

Im Mai 2000 wurde der Computervirus „Loveletter" freigesetzt. Er verbreitete sich innerhalb kürzester Zeit und infizierte Rechner auf der ganzen Welt.

Mit dem Loveletter-Virus wurden weltweit so viele Rechner infiziert:

☐ 2 Millionen
☐ 10 Millionen
☐ 100 Millionen
☐ 300 Millionen

Neben „Loveletter" kenne ich folgende weitere Computerviren:

.....

.....

Wer hat Interesse an der Entwicklung und Verbreitung von Computerviren? Nenne drei Gruppen und ihre Motive:

.....

.....

.....

Die Gesamtkosten des wirtschaftlichen Schadens durch den Computervirus „Loveletter" betrugen nach Schätzungen (in US-Dollar):

☐ 10 bis 20 Millionen
☐ 100 bis 200 Millionen
☐ 1 bis 2 Milliarden
☐ 3 bis 10 Milliarden
☐ 10 bis 50 Milliarden

Karikatur: Erik Liebermann

bpb: Hrsg.: Bundeszentrale für politische Bildung, 53113 Bonn. Autor: Ludwig Janssen. Verantwortl. Redakteurin: Iris Möckel. Gestaltung: Leitwerk, Köln.

Mein eigenes Sicherheitskonzept

Um sich vor Computerviren und E-Mail-Würmer zu schützen, damit sensible Daten nicht in fremde Hände geraten und um Manipulationen am eigenen Rechner zu verhindern, gibt es vielfältige Sicherheitsmaßnahmen. Die wichtigsten sind hier aufgelistet. **Zur eigenen Sicherheit solltest du die Checkliste ehrlich beantworten und die notwendigen Konsequenzen daraus ziehen.**

- ☐ Ich habe immer die neueste Version von Browser und E-Mail-Werkzeug installiert.
- ☐ Ich überprüfe regelmäßig und in kurzen Abständen, ob es neue Sicherheitspakete für Browser und E-Mail-Werkzeug gibt.
- ☐ Ich habe mir die Sicherheitseinstellungen meiner Software angeschaut und sie meinen Bedürfnissen angepasst.
- ☐ Ich arbeite nicht mit dem Internet Explorer und Outlook.
- ☐ Bei der Übermittlung von sensiblen Daten (z.B. Konto- oder Kreditkartennummer) achte ich auf eine sichere Verbindung (z.B. SSL).
- ☐ Ich habe meine Passwörter und Zugangsdaten nicht gespeichert und gebe sie jedes Mal neu ein.
- ☐ Meine Passwörter sind nicht aus dem Lexikon oder leicht zu erraten. Sie bestehen aus Buchstaben, Zahlen und Sonderzeichen.
- ☐ Ich habe für jedes Programm und für jeden Zugang verschiedene Passwörter.
- ☐ Ich habe eine Virensoftware installiert und aktualisiere diese regelmäßig in kurzen Abständen.
- ☐ Ich erstelle regelmäßig und in sinnvollen Abständen eine Sicherheitskopie von meinen wichtigsten Dateien.
- ☐ E-Mails mit wichtigen Informationen verschlüssele ich (z.B. mit PGP).
- ☐ Unbekannte oder unsichere E-Mail-Anhänge lösche ich ungelesen komplett.
- ☐ Werbe-E-Mails ignoriere ich. Ich klicke auch nicht auf Links in Werbe-E-Mails.
- ☐ Ich habe eine Personal-Firewall installiert und an meine individuellen Bedürfnisse angepasst.
- ☐ Ich installiere keine Programme aus unsicheren und/oder unbekannten Quellen.
- ☐ Ich habe eine Dialer-Schutzsoftware installiert und kenne die Datenbank der registrierten Dialer.
- ☐ Ich habe eine Software gegen Spyware installiert.

Was kann jeweils passieren, wenn man sich nicht schützt? (Tipp: ➜ *www.bsi.bund.de*)

USA: Klage wegen Sicherheitslücke in Windows

Microsoft muss sich vor dem kalifonischen Superior Court in Los Angeles wegen Begünstigung der Verbreitung von Viren und Internet-Schädlingen verantworten. Eine Klägerin wirft dem Hersteller vor, nachlässig mit Sicherheitsproblemen seiner Produkte umzugehen und seine Kunden nicht hinreichend über mögliche Risiken zu informieren.
Einem Bericht des „Wall Street Journal“ zufolge beziehen sich die Anschuldigungen auf das Verbraucherschutz-Gesetz des US-Bundesstaats Kalifornien: Aufgrund der Verbreitung seiner Programme lässt Microsoft den Verbrauchern keine andere Wahl, als seine Produkte zu nutzen. In dieser Situation, so schreibt es das Gesetz vor, müsse ein Anbieter alles tun, um Schaden von den Kunden abzuwenden.
Die Kalifornierin führt in ihrer Klageschrift an, durch Sicherheitslücken im Windows-Betriebssystem finanziellen Schaden erlitten zu haben. Außerdem sei ihre Privatsphäre verletzt worden, weil die Schwachstellen in den Microsoft-Programmen unerlaubte Zugriffe auf persönliche Daten möglich gemacht hätten.

Quelle: www.chip.de/news/c_news_10968851.html (chip.de vom 6.10.2003)

Wie würdest Du als Klägerin argumentieren? Wie als Anwalt von Microsoft?
Schreibe jeweils drei Argumente für jede Partei auf.

.....

.....

.....

.....

bpb: Hrsg.: Bundeszentrale für politische Bildung, 53113 Bonn. Autor: Ludwig Janssen. Verantwortl. Redakteurin: Iris Möckel. Gestaltung: Leitwerk, Köln.

Literaturhinweise

· Otto, Alexander: Internet-Sicherheit für Einsteiger. Für Homeanwender und kleine Firmennetze. Sicherheitslücken und Abwehrmaßnahmen, Schritt-für-Schritt-Anleitungen, CD-ROM mit vielen Sicherheits-Tools. Galileo Press, Bonn 2003, ISBN 3-89842-287-9.

· Schoblick, Gabriele und Robert: Sicherheit am PC. Markt + Technik, München 2003, ISBN 3-8272-6536-3.

Zum Thema Internet und Sicherheit sind im Internet selbst viele Informationen zu finden. Diese sind in der Regel viel aktueller als Zeitschriften und Bücher. Viele dieser Informationen stehen auch als PDF-Dateien zur Verfügung. Sie können heruntergeladen und ausgedruckt werden. Deswegen beschränken wir uns auf nur wenige und eher grundsätzliche Literaturhinweise.

Außerdem berichten Computerzeitschriften regelmäßig auch über das Thema PC- und Internetsicherheit. Vielen liegt eine CD bei, auf denen auch kostenlose und/oder Testversionen von Browser, E-Mail-Werkzeugen und Sicherheitssoftware zu finden sind.

Internetadressen

➜ *www.bsi.de*
Auf der Website des Bundesamt für Sicherheit in der Informationstechnik (BSI) sind grundlegende und aktuelle Informationen zum Thema Internetsicherheit zu finden. Das BSI hat die Fachinformationen aber auch für Bürger aufbereitet. Neben einer sehr guten Einführung zum Thema IT-Sicherheit (die auch komplett als PDF-Datei heruntergeladen werden kann) sind dort spezielle Informationen z.B. zum Kinderschutz, zum Thema Einkaufen oder Recht im Internet zu finden. Dort wird auch vielfältige (kostenlose) Sicherheitssoftware vorgestellt, die heruntergeladen werden kann. ➜ *www.bsi-fuer-buerger.de*

1. Informationen über Viren und andere
➜ *www.bsi.bund.de/av/index.htm* (Infos zu Viren, Würmern auf den Internetseiten des Bundesamtes für Sicherheit in der Informationstechnik)
➜ *www.polizei.propk.de/service/sicher/dialer.xhtml* (Informationen zu 0190-Dialern von der Polizei)
➜ *www.dialerschutz.de* und ➜ *www.dialerhilfe.de* (0190-Dialer-Portale)
➜ *www.robinsonlist.de* und ➜ *www.antispam.de* (Informationen zu Spyware und Werbemüll /Spam)
➜ *www.sewecom.de* (Daten- und Verbraucherschutz im Internet)

2. Firewall- Antiviren- und IT-Sicherheitssoftware
➜ *www.firewallinfo.de* (Übersicht)
➜ *www.antivir.de* (H+BEDV)
➜ *www.symantec.de*
➜ *http://de.mcafee.com*
➜ *www.f-secure.de*
➜ *www.tinysoftware.com*
➜ *www.biodata.de*
➜ *www.agnitum.com*
➜ *www.zonelabs.com*
➜ *www.microsoft.com/germany/security*

3. Recht im Internet
➜ *www.bfd.bund.de* (Der Bundesbeauftragte für den Datenschutz)
➜ *www.datenschutzzentrum.de/selbstdatenschutz* (FAQ zum Thema Datenschutz im Internet)
➜ *www.polizei.propk.de* (Das Vorbeugungsprogramm der Polizei u.a. mit dem Thema Internetkriminalität

Bestellcoupon

***Achtung*: Neue Versandbedingungen! Bis 1 kg kostenlos und portofrei, bei 1-15 kg Portobeitrag von ca. 4,60 EUR per Überweisung nach Erhalt.**

Bestell-Nr.: 5.383 _____ Nr. 33: Internet-Sicherheit
Bestell-Nr.: 5.384 _____ Nr. 34: Europa der 25 – Osterweiterung der EU
Bestell-Nr.: 5.385 _____ Nr. 35: Staatsverschuldung – Ausmaß und Folgen
Bestell-Nr.: 5.386 _____ Nr. 36: Präsidentschaftswahlen in den USA
Bestell-Nr.: 5.387 _____ Nr. 37: 20. Juli 1944 – Attentat auf Hitler
Bestell-Nr.: 5.388 _____ Nr. 38: Jugendbeteiligung in der Demokratie

Weitere Themenblätter: siehe Umschlagseite 2!

Bestell-Nr. _____ Exemplare _____
Bestell-Nr. _____ Exemplare _____
Bestell-Nr. _____ Exemplare _____
Bestell-Nr. _____ Exemplare _____

Jede Ausgabe enthält das Arbeitsblatt 27-29 fach!
Alle Themenblätter im Unterricht sind auch im Internet unter ➜ www.bpb.de (Publikationen).

Themenblätter für die Grundschule
Doppelseitiges buntes Wimmelarbeitsblatt; pro Ausgabe 15fach plus Lehrerhandreichung:
Bestell-Nr. 5.350 _____ Nr. 1: Mädchen und Jungen sind gleichberechtigt
Bestell-Nr. 5.349 _____ Nr. 2: Meine Freiheit, deine Freiheit

☐ **Pocket** Politik _____ Exemplare
☐ **Pocket** Wirtschaft _____ Exemplare

Bestell-Nr. 5.340 _____ Methoden-Kiste

☐ Verzeichnis der lieferbaren Unterrichtsmaterialien, Bestell-Nr. 999 (wird ca. alle 6 Wochen aktualisiert)

Timer bitte nicht mit diesem Coupon bestellen!
(Siehe Rückseite)

Liebe Leute,
Im Juni 2004 erscheint der **bpb-Timer für das Schuljahr 2004/2005!**
Vorbestellen kann man ab sofort.

Mitwissen, mitreden, mitmischen: der informative Hausaufgabenkalender der Bundeszentrale für politische Bildung/bpb enthält zu jedem Kalendertag interessante Mitteilungen aus aller Welt, aus Politik und Zeitgeschichte, Gesellschaft und Kultur. Jede der 53 Wochen ist auf je einer Doppelseite im speziellen Timer-Design gestaltet und farbig bebildert. Die Wochentage gibt's in 53 Sprachen von Albanisch und Arabisch bis Vietnamesisch und Walisisch. Dazu gehört ein Serviceteil mit Stundenplänen und Ferienkalendern, Wissenswertem, Landkarten sowie Tipps fürs Überleben in Schule und Gesellschaft. Und einen sorgfältig recherchierten Teil mit Links und Adressen für diejenigen, die noch mehr wissen möchten.

(da isser!)

Bestellen kann man so:
1. Online: ➜ *www.bpb.de/timer*
2. per Fax: 01805- 84 63 72 72 (12 Cent pro Minute)
3. per Postkarte: bpb-Timer, Postfach 810627 in 30506 Hannover
4. per SMS: 84422 *(Muster: timer, einzelexemplar, marie muster, timerweg 1, 88888 musterdorf*); 49 Cent pro SMS; leider nicht aus dem D1-Netz. Kommas nicht vergessen!

Die Bereitstellungspauschale beträgt pro Exemplar 2.- Euro.
Für Sammelbesteller gibt es Rabatt: ab 5 Exemplaren kostet der Timer nur noch 1.- Euro pro Exemplar und ab 100 Exemplaren 75 Cent. Dazu kommen jeweils 3 Euro Porto- und Verpackungspauschale. Die Bearbeitung und Auslieferung besorgt die Firma youngkombi.

Lieferzeit: etwa 7 Tage.
Achtung: Paketversand an Schuladressen **nur** vor und nach den jeweiligen Sommerferien, wenn die Sekretariate besetzt sind (um unnötige und teure Rücksendungen zu vermeiden).

Lieferung leider nur an Inlandsadressen und nur, **so lange der Vorrat reicht.**

Mai-Aktion für Aufgeweckte:
Alle „Multiplikatoren" – das sind zum Beispiel Schulen und Schulsprecher/innen sowie Schülerzeitungsredaktionen – können bis zum 20. Mai ein kostenloses Musterexemplar bestellen.

Alle anderen können aber auch einen neuen Timer gewinnen:
beim **Timer-Online-Quiz** (ebenfalls unter ➜ *www.bpb.de/timer*). Wer sich bis zum 20. Mai mit der richtigen Lösung bei uns meldet, bekommt einen kostenlosen Timer zugeschickt.

.....
Für **Fax-Besteller** (01805- 84 63 72 72 /12 Cent pro Minute):

Bitte senden Sie an folgende Adresse ..... Exemplare des bpb-Timers 2004/2005.

Name:

Schule:

Straße:

PLZ: Ort:

Unterschrift: .....

➜ www.bpb.de/timer

Achtung!
Lieferung nur an Inland-Adressen.

Fax: 0 89-5 11 72 92
E-Mail: infoservice@franzis-online.de

Firma
Franzis' print & media
Postfach 15 07 40

80045 München

Lieferanschrift (nur Inland-Adressen!)

☐ SCHULE ☐ PRIVAT

VORNAME: .....

NAME: .....

KLASSE/KURS: .....

SCHULE: .....

STRASSE: .....

PLZ/ORT: .....