7 Was wir nicht brauchen: Unerwünschtes und Unnötiges

Spam und Schadsoftware

Spam

Als **Spam** oder auch **Junk** werden unerwünschte Werbe-E-Mails bzw. unerwünschte Nachrichten bezeichnet. Der Ursprung des Begriffs „Spam" ist nicht ganz klar, steht jedoch vermutlich in Zusammenhang mit dem Akronym des Dosenfleischs **Sp**iced H**am** der Firma **Hormel Foods**.[1] Die britische Komikergruppe **Monty Python** verwendete dann 1970 das Wort in einem Sketch in derartigem Übermaß, dass es wohl zum Synonym für die massenhafte und unerwünschte Verbreitung von etwas wurde.[2] „Junk" hingegen kommt aus dem Englischen und bedeutet schlicht „Abfall" oder „Müll".

Spam-Mails lohnen sich für die Absender, denn zum einen ist der Mail-Versand kostenlos und zum anderen öffnen Nutzer noch immer – versehentlich oder bewusst – Werbe-Mails. Einige Spam-Mails sind nicht nur nervig, sondern können auch Schaden anrichten: Durch vireninfizierte Spam-Mails kann der Computer des Adressaten ohne dessen Wissen Teil eines sog. **Botnets** werden. Das ist ein Netz bestehend aus mehreren Computern, die von Dritten ferngesteuert werden können, um bspw. Spam-Mails zu versenden oder gar andere Computer zu attackieren.[3] Diese automatisierten Computerprogramme werden in Anlehnung an das englische Wort für Roboter (**robot**) als **Bots** bezeichnet.

Spam-Mails sind meist nicht mehr bloß allgemein gehaltene unerwünschte Werbebotschaften.
Viele Spam-Mails sprechen den Adressaten persönlich an – bspw. durch die Verwendung des Vor- und Nachnamens – und sind attraktiv gestaltet.

Spam kann in unterschiedlichen Kontexten auftauchen und verschiedene Formen annehmen.

Formen von Spam

Spam-Mail
Unerwünschte Werbe-Mails sind die wohl häufigste Spam-Form. Das amerikanische Software-Unternehmen **Symantec** hielt in seinem Bericht für den Monat Juni 2015 fest, dass 49,7 % des gesamten erfassten E-Mail-Verkehrs Spam war.[4] Spam-Mails können in drei Arten differenziert werden:

- **Scam**
  Scam (zu Deutsch „Betrug") bezeichnet E-Mails, die Angebote für besonders günstige, einmalige Waren oder Geschäfte enthalten und den Adressaten auffordern, diese zu kaufen. Der Käufer erhält nach der Überweisung des Geldes das versprochene Produkt jedoch nicht.[5]

- **Hoax**
  Hoax (zu Deutsch „Täuschung" oder auch „Falschmeldung") bezeichnet eine Spam-Mail, die in Form eines Kettenbriefes versandt wird und die Aufforderung beinhaltet, die E-Mail an möglichst viele Freunde und Bekannte weiterzuleiten. Inhaltlich geht es in den Hoax-Mails meist um Warnungen, Einladungen oder Aufrufe. Hoaxes werden natürlich nicht nur per E-Mail versandt. Sie kursieren auch in Sozialen Netzwerken wie bspw. Facebook.[6] Meist sind die Hoaxes schlicht nervig – einige allerdings enthalten auch Viren, die den Computer des Empfängers infizieren, schlimmstenfalls ausspionieren oder gar fernsteuern können.

- **Phishing**
  Phishing setzt sich zusammen aus den beiden englischen Begriffen „Password" und „Fishing" und bezeichnet das kriminelle Abgreifen wichtiger Passwörter. Betrüger schicken gefälschte Nachrichten an Nutzer, um an deren Zugangsdaten, bspw. für das Bankkonto zu gelangen. Die Mails verlinken auf Seiten, die vorgeben von seriösen Kreditinstituten zu sein und greifen so die Bankdaten derjenigen Nutzer ab, die auf diesen Seiten aktiv sind.[7]

Spam dieser Art findet sich nicht nur in E-Mails, sondern auch in Sozialen Netzwerken. Dort gibt es auch weitere Arten von Spam: So finden Nutzer auf ihrer Pinnwand bspw. Posts vor, die ihr Interesse wecken sollen, z.B. mit einer spannenden Aussage oder einem verlockenden Privat-Video eines Stars. Wird dieser Post dann angeklickt, gelangen die Nutzer meist nicht auf den erwarteten Inhalt. Stattdessen wird den Freunden des Nutzers angezeigt, dass er oder sie besagten Post **geliked** hat. Auf diese Weise werden solche Posts schnell verbreitet und mit ihnen schlimmstenfalls auch Viren. Facebook bietet hier bspw. die Möglichkeit an, derartige Beiträge zu melden und als Spam zu deklarieren.

Suchmaschinen-Spam
Suchmaschinen-Spamming bezeichnet den Versuch, das Ranking einer Webseite innerhalb der Suchergebnisse mittels unlauterer Methoden zu verbessern. Das funktioniert auf verschiedenen Wegen: bspw. durch die unnatürlich häufige Verwendung eines Suchbegriffs im Text der Webseite, deren Ranking verbessert werden soll. Oder es werden eigens Seiten generiert, die ausschließlich Links auf die Seiten enthalten, die optimiert werden sollen. Hintergrund ist hier, dass Suchmaschinen die Relevanz einer Webseite nicht zuletzt auch an der Menge und Qualität der Verlinkungen durch andere Seiten messen. Suchmaschinen-Anbieter identifizieren solche Seiten aber immer effektiver als Spam und strafen sie durch Ausschluss aus ihrem Such-Index ab.[8]

Mobile Spam
Da das Smartphone ein medialer Alleskönner ist und viele Funktionen, wie z. B. E-Mail, Internet und damit auch Dienste wie Soziale Netzwerke auf sich vereint, sind auch die Spam-Formen nicht grundlegend neu: Spam kann in Form von Spam-Mails oder SMS-Spam auftreten und birgt die gleichen Gefahren wie auch für Desktop-Computer (z. B. Viren, Botnets). Auch über die verschiedenen Apps, wie z. B. **WhatsApp**, **Snapchat** oder **Instagram** können unerwünschte Werbebotschaften versendet werden. Meist ist es möglich, diese dem Anbieter direkt zu melden.

Spam: Was sagt das Gesetz?
In Deutschland ist das unaufgeforderte Zusenden von Werbung laut § 1 des Gesetzes gegen den unlauteren Wettbewerb (UWG) dann verboten, wenn die Werbung in unzumutbarer Weise belästigt.[9] Aus diesem Grund verschicken Spammer ihre Botschaften ent-weder über Internetanbieter aus dem Ausland oder über Botnets. Wenn Spam im Postfach gelandet ist, muss der Adressat diesen gemäß Artikel 10 des Brief-, Post- und Fernmeldegeheimnisses selbst löschen bzw. durch entsprechende Programme automatisch löschen lassen.[10] Auch in § 6 des Telemediengesetzes (TMG) findet sich eine konkrete Regelung über die „kommerzielle Kommunikation": Eine E-Mail darf ihren werblichen Charakter in Absender- und Betreffzeile nicht verschleiern und muss für den Nutzer klar erkennbar sein.[11] Art. 13 der europäischen Datenschutzrichtlinie über die elektronische Kommunikation (2002/58/EG) sieht überdies vor, dass das Versenden von Werbung nur mit vorheriger Einwilligung zulässig ist (Opt-in-Verfahren).[12]

Schutz vor Spam
Spam ist meist ärgerlich, aber harmlos. Kritisch wird es, wenn Spam mit Viren infiziert ist oder auf entwicklungsbeeinträchtigende Inhalte, wie z. B. Webseiten mit problematischen Gewalt- oder Sexualdarstellungen, verlinkt. Um Spam vorzubeugen und dessen Anzahl zu beschränken, sind folgende Maßnahmen hilfreich:

1. *Mit der eigenen E-Mail-Adresse bedacht um-gehen und evtl. eine zweite E-Mail-Adresse im Sinne einer „Wegwerfadresse" anlegen*

Viele Dienste-Anbieter im Internet, seien es Shops, Newsletter, Portale etc. verlangen bei der Registrierung die E-Mail-Adresse des Nutzers. Da diese Adress-Daten leicht in die Hände von Werbetreibenden geraten können bzw. die Daten ganz bewusst von einigen Dienste-Anbietern weitergegeben werden, lohnt es sich, eine zweite E-Mail-Adresse anzulegen. Diese kann immer dann angegeben werden, wenn man keinen Wert auf News, Benachrichtigungen über Sonderangebote etc. seitens des Dienste-Anbieters legt. Einige E-Mail-Provider bieten sogar spezielle E-Mail-Accounts an, die nur für kurze Zeit gültig sind und die eingehende E-Mails nach einem bestimmten Zeitraum automatisch löschen. Anbieter, die solche **Wegwerf**-Adressen bereitstellen, sind u. a.: **https://www.trash-mail.com/**

http://www.wegwerfemail.de/ oder **http://spoofmail.de/**. Selbst große E-Mail-Provider wie bspw. **Yahoo!** bieten ihren Nutzern die Möglichkeit, unter der eigenen (richtigen) E-Mail-Adresse, Wegwerf-Adressen einzurichten.

❷ *Nicht auf Spam reagieren, d. h. keine Anhänge / Links öffnen*

Wichtig ist, nicht auf Spam zu reagieren und sich weder beim Absender der Nachricht zu beschweren, noch Anhänge oder Links zu öffnen. Letztere könnten mit Viren verseucht sein und damit den Computer infizieren. Die Rückmeldung beim Absender des Spams bestätigt diesem die Richtigkeit der Adresse, was schlimmstenfalls zu noch mehr Spam-Mails führen kann! **Wichtig:** Dieses Prinzip gilt auch für die Abwesenheitsnotiz bei Urlaub. Diese muss unbedingt nach dem Spam-Filter geschaltet werden, da sonst die Spammer ebenfalls wissen, dass die E-Mail-Adresse korrekt ist.

❸ *Spam-Filter und Schutzprogramme installieren*

Spam-Filter sind entweder direkt auf dem Computer des Nutzers installiert (z. B. im Fall von Outlook) oder aber sie liegen auf dem Server des E-Mail-Providers. In letzterem Fall kann der Nutzer den Filter nicht weiter beeinflussen und muss auf ausreichenden Schutz vertrauen. In dem Falle eines eigenen Filters ist der Nutzer für das regelmäßige Update des Spam-Filters selbst verantwortlich, kann allerdings auch Einstellungsänderungen selbst vornehmen. Neben einem Spam-Filter sollte jeder Computer zudem über ein funktionsfähiges Virenschutzprogramm verfügen, das in regelmäßigen Abständen aktualisiert wird. Auch eine sog. **Firewall**, zu Deutsch „Brandschutzmauer", ist sinnvoll – sie überprüft alle Daten, die der User aus dem Netz lädt sowie die Daten, die von dem Computer ins Netz geschickt werden.

❹ *Spam-Filter „trainieren"*

Alle deutschen E-Mail-Provider haben einen Spam-Filter integriert. Dieser sorgt dafür, dass verdächtige E-Mails in einem separaten Spam-Ordner landen. Wenn sich doch noch die eine oder andere Spam-Mail im regulären Posteingang findet, kann diese dem E-Mail-Anbieter als Spam gemeldet werden. So kann der Anbieter das nächste Mal besser reagieren und ähnliche E-Mails direkt im Spam-Ordner ablegen.

❺ *Wachsam sein bei dubiosen Nachrichten*

Ist der Absender einer Nachricht nicht bekannt oder erscheint die Betreffzeile seltsam, dann sollte die Nachricht sowie auch ihre Anhänge oder Links nicht geöffnet werden.

❻ *Eigene E-Mail-Adresse verschleiern*

Es gibt keine Möglichkeit, die eigene E-Mail-Adresse z. B. im Impressum der eigenen Webseite sicher zu verschleiern. Es kann nur versucht werden, das Ausfindigmachen der richtigen E-Mail-Adresse für Bots zu erschweren. „@" durch „at" zu ersetzen gehört zu den einfach zu knackenden Lösungen. Schwieriger ist es für Bots hingegen, bspw. sog. **Captchas** zu entschlüsseln. Hinter „Captcha" verbirgt sich die Phrase „**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part" – Tests also, mittels derer zwischen Menschen und Programmen unterschieden werden soll. Man kennt sie in Form von Zahlen- und/oder Buchstabenkombinationen, die auf einem Bild zu sehen sind und die dann durch den Nutzer in ein separates Feld eingegeben werden müssen.[13]

❼ *Eintragung in Robinsonliste*

In die Robinsonliste können sich Verbraucher eintragen, die keine weitere unerwünschte Werbung via Post, Telefon, E-Mail, Mobil oder Fax erhalten wollen: **https://www.robinsonliste.de**.
Werbetreibende Unternehmen können die Robinsonliste mit ihrer Empfängerliste abgleichen und so sicherstellen, dass Verbraucher, die keine Werbung wünschen, auch keine erhalten. Die Eintragung in die Liste bietet allerdings keinen vollkommen sicheren Schutz vor unerwünschter Werbung, denn nicht alle Werbetreibenden halten sich an den Wunsch des Verbrauchers.

❽ *Benutzerprofile*

Auf Geräten sollte generell als normaler Benutzer und nicht als Administrator gearbeitet werden. Auf diese Weise kann Schaden, den Schadsoftware anrichten kann, beträchtlich vermindert werden.

Tipp: *Spam und rechtswidrige Online-Inhalte können an die Internetbeschwerdestelle gemeldet werden:*
http://www.internet-beschwerdestelle.de/

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/themen/kommunizieren/spam/
Hier finden sich weiterführende Informationen zu Spam.

www.vz-nrw.de/home
Auf der Seite der Verbraucher-Zentrale finden sich umfassende Informationen rund um das Thema Werbung, E-Commerce, Datenschutz u. v. m.

www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Spam/Schutzmassnahmen/schutzmassnahmen_node.html
Informationsseite zu Spam vom Bundesamt für Sicherheit in der Informationstechnik.

www.lehrer-online.de/it-sicherheit.php
Informationsseite für Lehrer zu vielen verschiedenen Themen – u. a. über IT-Risiken.

http://praxistipps.chip.de/wegwerf-email-adressen-diese-anbieter-gibts_1674
Hier sind noch weitere Anbieter von sog. Wegwerf-Adressen aufgeführt.

www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/version.htm
Hier finden sich genaue Informationen zur Verschlüsselung von E-Mails mittels des Pretty-Good-Privacy-Verfahrens.

www.internauten.de/index.html?mission=E-Mail_Spam/index.html
Ein Online-Spiel, das sich an Kinder richtet und verschiedene Internetrisiken als Missionen aufbereitet – u. a. auch E-Mail und Spam.

www.youtube.com/watch?v=anwy2MPT5RE
Spam-Sketch von Monty Python aus dem Jahr 1970.

Endnoten

[1] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Spam-Definition.* Aufgerufen am 10.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Spam/spam_node.html

[2] ebd.

[3] BENDRATH, R. (2009, 18. Dezember). *Botnets, Internetanbieter und Politik – auf sanften Sohlen zu neuen nationalen Strukturen der Internet-Regulierung?* [Blog-Beitrag] Aufgerufen am 10.07.2015 unter https://netzpolitik.org/2009/botnets-internetanbieter-und-politik-auf-sanften-sohlen-zu-neuen-nationalen-strukturen-der-internet-regulierung/

[4] SYMANTEC. (2015, 16. Juli). *Symantec Intelligence Report: June 2015* [Blog]. Aufgerufen am 20.07.2015 unter http://www.symantec.com/connect/blogs/symantec-intelligence-report-june-2015

[5] TECHFACTS. (2014, 15. Mai). *Was ist Scam?* Aufgerufen am 10.07.2015 unter http://www.techfacts.de/ratgeber/was-ist-scam

[6] ZIEMANN, F. (2015, 18. Juli). *TU-Berlin: Hoax-Liste.* Aufgerufen am 20.07.2015 unter http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

[7] VERBRAUCHERZENTRALE NRW. (2015, 21. Januar). *Spam: E-Mail-Müll auf der Datenautobahn.* Aufgerufen am 10.07.2015 unter http://www.vz-nrw.de/spam#arten

[8] LAMMENETT, E. (2007). *TYPO3 Online-Marketing-Guide. Affiliate- und E-Mail-Marketing Keyword-Advertising, Suchmaschinen-Optimierung mit TYPO3.* Wiesbaden: Verlag Dr. Th. Gabler.

[9] GESETZ GEGEN DEN UNLAUTEREN WETTBEWERB (UWG). Aufgerufen am 18.11.2014 unter http://www.gesetze-im-internet.de/uwg_2004/

[10] GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND (GG). *Artikel 10.* Aufgerufen am 20.07.2015 unter http://www.gesetze-im-internet.de/gg/art_10.html

[11] TELEMEDIENGESETZ (TMG). Aufgerufen am 20.07.2015 unter http://www.gesetze-im-internet.de/tmg/

[12] DATENSCHUTZRICHTLINIE FÜR ELEKTRONISCHE KOMMUNIKATION. (2002, 12. Juli). Aufgerufen am 18.11.2014 unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32002L0058&from=DE

[13] GOOGLE. (k. A.). *reCAPTCHA: Tough on bots easy on humans* (Absatz 3). Aufgerufen am 19.11.2014 unter http://www.google.com/recaptcha/intro/

Schadsoftware

Schadsoftware wird oft auch als **Malware** bezeichnet. Dieser Begriff setzt sich zusammen aus dem englischen **mal**icious (zu Deutsch: boshaft) und Soft**ware**. Damit sind Programme gemeint, die Schaden an Computersystemen (PCs, Chips, Handys, Smartphones etc.) anrichten, Daten ausspionieren oder sich Zugang zu privaten Computersystemen verschaffen wollen.[14] Der erste **Wurm** (s. u.) war wohl der sog. **vampire worm**, den die beiden Programmierer des **XEROX**-Unternehmens John Hepps und John Shock in den 80er Jahren programmierten: Das kleine Programm war eigentlich dazu entwickelt worden, über Nacht automatisch Prozesse abzuwickeln, die tagsüber aufgrund der hohen Auslastung des Prozessors durch das Tagesgeschäft nur schwer möglich waren. Der **vampire worm** legte jedoch eines Tages bedingt durch einen Prozessfehler alle Computer des Unternehmens lahm und musste daher entfernt werden.[15]

Als erster **Virus** (s. u.) gilt wohl die Schadsoftware **Brain**, die von zwei pakistanischen Brüdern entwickelt wurde.[16] Sie infizierte bestimmte Bereiche einer Diskette, wodurch der Zugriff auf diese extrem verlangsamt wurde. Eine Infizierung blieb durch die Nutzer in vielen Fällen unbemerkt. Seither haben verschiedene, weitaus schädlichere Malware-Programme immer wieder öffentliches Aufsehen erregt: darunter **Marburg, LoveLetter, Sasser, Flame** u. v. w. m. Es gibt verschiedene Arten von Malware:

- **Virus**
  Ein Virus ist ein Schadprogramm, das sich selbstständig vervielfältigen kann und auf diese Weise schnell verbreitet. Der Virus heftet sich an andere Programme und kann so ohne Wissen des Nutzers beim Download von Dateien aus dem Internet, über USB-Stick etc. den eigenen Computer infizieren. Die Größe des Schadens, den Viren anrichten, variiert stark: von harmlosen sinnlos ausgegebenen Textstücken bis hin zur Löschung der gesamten Festplatte.[17]

- **Wurm**
  Würmer sind dem Virus sehr ähnlich: Auch sie können sich selbstständig vervielfältigen, nachdem sie einmal ausgeführt wurden. Anders als Viren infizieren Würmer aber keine fremde Dateien und auch nicht den Startsektor eines Laufwerks. Würmer werden meist über infizierte E-Mails oder Links verbreitet. Würmer verbrauchen viele Netzwerkressourcen und können einen Computer so lahmlegen.[18]

- **Trojaner**
  Der Begriff ist angelehnt an das Trojanische Pferd der griechischen Mythologie. Entsprechend bezeichnet der Trojaner im Kontext der Schadsoftware ein Programm, das sich in scheinbar vertrauenswürdigen, seriösen Programmen versteckt.[19] Der Trojaner kann darüber unbemerkt auf dem Computer installiert werden. Oft sind Trojaner sog. **Spyware**.

- **Spyware**
  Unter Spyware sind Programme zu verstehen, die unbemerkt auf dem PC installiert werden und vertrauliche Daten, Passwörter, Surfverhalten, Informationen über benutzte Programme etc. des infizierten Computers ausspionieren (auf Englisch: „to spy"). Diese Informationen können dann einerseits für die Abzocke genutzt werden oder kommen Werbefirmen zugute, die auf dieser Basis zielgenau Werbung ausbringen können.[20]

- **Scareware**
  Scareware setzt sich zusammen aus den beiden englischen Begriffen **scare** (zu Deutsch: jmd. erschrecken) und Soft**ware**. Darunter zu verstehen sind Schadprogramme, die beim Nutzer durch gefälschte Warnmeldungen, z. B. über eine Virenifektion, Ängste schüren sollen. Dies soll den User dann dazu verleiten, eine bestimmte (Schad-) Software zu installieren.[21]

- **Ransomware**
  „Ransom" bedeutet übersetzt „Erpressung". Diese Art der Schadsoftware versucht den Nutzer zu erpressen, indem die Nutzung des Computers gesperrt und der Nutzer dazu aufgefordert wird, einen bestimmten Geldbetrag zu zahlen, um wieder auf den Rechner zugreifen zu können.[22]

- **Dialer**
  Programme, die eine Telefonverbindung oder den Versand von SMS über hochpreisige Dienste herstellen.

Aus der Praxis
Zu diesem Thema können sich die eher technisch interessierten SchülerInnen verwirklichen. Vielleicht bietet sich die Gelegenheit, ein ***Live-Hacking*** *zu besuchen – eine Veranstaltung, auf der demonstriert wird, wie leicht Hacker an Daten gelangen und Dritte ausspionieren können. Alternativ gibt es unter diesem Stichwort sehr anschauliche Vorführungen in* ***YouTube****.*

Schadprogramme: Wirtschaftlicher Schaden
Für den betroffenen Nutzer sind Schadprogramme lästig, denn es kostet Zeit, Nerven und oftmals Geld, sich der Schadprogramme zu entledigen, einen sicheren Schutz zu installieren und beständig zu aktualisieren. Laut einer Studie der Sicherheitsfirma **Norton** aus dem Jahr 2012 haben Privatpersonen durch Malware weltweit einen finanziellen Schaden von insgesamt ca. 88 Milliarden Euro erlitten.[23]

Sehr häufig infizieren Nutzer ihre Geräte unbewusst während des Surfens auf seriösen, aber gehackten Seiten bzw. auf speziell erstellten Angriffs-Webseiten. Diese Art der Infektion wird **Drive-by-Download** genannt: Hacker integrieren den Schadcode in eine Webseite, woraufhin sich dann der Nutzer alleine durch den Besuch der Website automatisch und ohne es zu wissen, mit der Malware infiziert. **Drive-by-Downloads** stellen die am weitesten verbreitete Art der Infektion mit Malware dar.[24]

Suchmaschinen-Anbieter wie Google versuchen Webseiten, die Malware enthalten, zu erkennen. Wird eine Webseite als infiziert erkannt, wird dem Nutzer, der auf die Seite zugreifen möchte, eine Warnung angezeigt.[25]

Smartphone & Schadware
Im Grunde sind mobile Endgeräte von den gleichen Schadprogrammen bedroht wie Desktop-PCs.
Durch die nahezu flächendeckende Ausstattung mit Smartphones und Tablets hat sich jedoch immer mehr Schadsoftware gezielt auf die mobilen Endgeräte spezialisiert: Es gibt Schadprogramme, welche unbemerkt Kamera und Mikrofon eines Smartphones aktivieren und die Daten aufzeichnen, Malware, die auf Standortdaten eines Gerätes zugreift und alle getätigten Aktionen nachverfolgt etc.[26]

Android-Geräte sind eher anfällig für Malware.[27] Das liegt zum einen an der hohen Verbreitung von Android-betriebenen Geräten und zum anderen daran, dass Google es seinen Nutzern relativ leicht ermöglicht, neben dem offiziellen Google-Play-Store auch weitere Stores zu nutzen, um Apps zu beziehen. Diese App-Stores von Dritten haben teilweise eine fragwürdige Sicherheitspolitik und Malware findet daher leicht Eingang. Apple verfolgt eine restriktivere Politik und prüft jeder App auf deren Sicherheit, ehe diese im App-Store eingestellt wird.

Tipp:
Das ***Bundesamt für Sicherheit in der Informationstechnik*** *bietet einen aktuellen Informationsservice und spricht Virenwarnungen aus, wenn dies eine kritische Masse deutscher Nutzer betrifft:* ***https://www.buerger-cert.de/***
Außerdem gibt es auch auf den Seiten der Antiviren-Hersteller regelmäßig Informationen über neue Bedrohung z. B. von ***Kaspersky*** *unter* ***http://www.viruslist.com****.*

Schutz vor Schadprogrammen
Um sich vor Schadprogrammen zu schützen, sind folgende Maßnahmen und Übergelungen sinnvoll:

1. ***Antivirenprogramm / Firewall installieren & aktualisieren***

Auf jedem Gerät sollten ein Antivirenprogramm und eine Firewall installiert sein. Es gibt gute kostenlose und gute kostenpflichtige Software. Gleich, für welche man sich entscheidet: es ist unbedingt notwendig, diese Software regelmäßigen Updates zu unterziehen, denn Viren verändern sich beständig und schnell ist die Anti-Viren-Software nicht mehr auf dem neuesten Stand.
Firewalls sind meist in das Antivirenprogramm integriert. Eine Firewall schützt ein Gerät vor Angriffen und unberechtigten Zugriffen aus dem Internet. Die Firewall sollte niemals ausgeschaltet sein!

❷ *Betriebs- und Anwendersoftware aktualisieren*

Nicht nur die Anti-Viren-Software und die Firewall sollten regelmäßig aktualisiert werden. Auch Betriebs- und Anwendersoftware muss laufend auf den neuesten Stand gebracht werden, damit Viren nicht durch etwaige Sicherheitslücken eindringen können. Aber Vorsicht: Die Updates sollten nur von seriösen Quellen bezogen werden, denn Updates von gängiger Software (z. B. Adobe Flash, Adobe Reader) können von Schadsoftware verseucht sein.

❸ *Risiko-Webseiten meiden*

Ein hohes Risiko, das eigene Gerät mit Malware zu infizieren, besteht beim Besuch kostenloser Pornoseiten.[28] Aber auch Streaming-Portale – Seiten, die Filme zum direkten Ansehen im Browser bereitstellen – stehen im Verruf für Malware-Attacken genutzt zu werden.[29] Aber: Ein Großteil der Malware stammt von seriösen Seiten, die von Cyberkriminellen gehackt wurden.

❹ *Nachrichten / Daten kritisch prüfen*

Nachrichten und deren Anhänge sollten nur geöffnet werden, wenn der Absender bekannt und vertrauenswürdig ist, die Betreffzeile seriös klingt und die Nachricht erwartet wurde. Das ist wichtig, da auch die Möglichkeit besteht, dass die Rechner von Freunden/ Bekannten vorab infiziert wurden. Empfehlenswert ist es daher, die Anhänge vor dem Öffnen vom Antivirenprogramm auf Bedrohungen scannen zu lassen.

❺ *App-Berechtigungen kontrollieren*

Vor dem Installieren einer App kritisch prüfen, welche Berechtigungen sie zum Funktionieren wirklich benötigt: Warum verlangt z. B. eine Taschenlampen-App Zugriff auf Kontaktdaten? Bei iOS (Apple-Betriebssystem) können Berechtigungen einzeln abgelehnt werden. Hier gilt es jedoch zu beachten, dass die betreffende App ohne Zugriffsrechte möglicherweise nicht benutzt werden kann. Bei Android (Google-Betriebssystem) war das Ablehnen von Berechtigungen lange nicht möglich. Erst mit der neuen Version 6.0 des Android Betriebssystems hat sich dies geändert: der Nutzer kann nun bei einigen Berechtigungen selbst entscheiden, ob er den Zugriff darauf erteilt oder verweigert. Jedoch gilt dies nicht für alle Berechtigungen, so dass bei allzu datenhungrigen Apps die Suche nach alternativen nach wie vor sinnvoll ist.

❻ *Benutzerprofile*

Geräte sollten immer als normaler Nutzer und nicht als Administrator genutzt werden, denn letzterer ist mit weitreichenden Berechtigungen ausgestattet. Wird das Gerät mit Malware infiziert, kann der Schädling in der Administrator-Einstellung mit Berechtigung zur System-Konfiguration weitaus größeren Schaden anrichten.

❼ *Dateien regelmäßig sichern*

In regelmäßigen Abständen sollten von den wichtigsten Dateien Sicherungskopien auf externe Festplatten angefertigt werden. Im Fall eines massiven Schadsoftware-Befalls sind diese Daten nicht verloren.

❽ *Wachsam sein*

Nutzer sollten im Internet immer auf der Hut vor Malware sein und auf den gesunden Menschenverstand vertrauen: Meldungen, Nachrichten und Aufforderungen sollten nicht blind vertraut werden.

Erkennen von Schadprogrammen

Woran kann man ein von Schadprogrammen befallenes Gerät erkennen? Am Desktop-PC lässt sich das u. U. durch folgende Indikatoren feststellen:[30]

- Verringerte Computerleistung
- Hohe Prozessorauslastung
- Langsame Internetverbindung
- Programme starten/schließen sich automatisch
- Vermehrte Werbeeinblendungen

Bei mobilen Endgeräten ist ein Virenbefall, neben der Prüfung durch eine Antiviren-Software, u. U. auch anhand folgender Indikatoren feststellbar:[31]

- Langsame Internetverbindung, hoher Datenverbrauch
- Hohe Prozessorauslastung
- Hoher Energieverbrauch
- Überhöhte Telefonkostenabrechnung: Abo-Gebühren, teure Premium-Nummern etc.

Links und weiterführende Informationen

Webseiten

www.av-test.org/de/antivirus
Hier finden sich detaillierte Testberichte zu Antivirenprogrammen auf Desktop-PCs und mobilen Endgeräten.

www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass.html
Der Sicherheitskompass der Polizei beschäftigt sich mit den 10 häufigsten Sicherheitsrisiken.

www.bka-trojaner.de
Hier gibt es Hilfestellung zur Beseitigung diverser Ransomware.

http://praxistipps.chip.de/bin-ich-teil-eines-botnetzes-so-finden-sies-heraus_12330
Auf dieser Seite kann getestet werden, ob das eigene Gerät Teil eines Botnets ist.

www.lehrer-online.de/it-sicherheit.php
Hier finden sich Unterrichtseinheiten und Hintergrundinformationen rund um das Thema „IT-Sicherheit".

www.lehrer-online.de/viren-wuermer-trojaner.php
Hier gibt es Informationen und Unterrichtseinheiten zum Thema "Viren" und "Trojaner".

www.internauten.de/index.html?mission=Download/index.html
Auf dieser Seite findet sich ein Spiel zu Viren und Trojanern, das sich an jüngere Kinder richtet.

www.blinde-kuh.de/viren
Diese Seite bietet kindgerechte Informationen rund um das Thema „Viren".

Endnoten

[14] SPRINGER GABLER VERLAG (Hrsg.). (k.A.). *Gabler Wirtschaftslexikon, Stichwort: Malware.* Aufgerufen am 20.07.2015 unter http://wirtschaftslexikon.gabler.de/Archiv/1408508/malware-v4.html

[15] BRENTON, C. & Hunt, C. (2003). *Network Security. The Expertise You Need to Protect Your Network from Common Threats* (2. Auflage). Alameda, CA: Sybex.

[16] MILOŠEVIĆ, N. (k. A.). *History of malware*. [Blog] Aufgerufen am 19.11.2014 unter http://www.inspiratron.org/HistoryOfMalware.php

[17] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Viren.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Viren/viren_node.html

[18] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Würmer.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Wuermer/wuermer_node.html

[19] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Trojaner.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/TrojanischePferde/trojanischepferde_node.html

[20] BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI). (2015). *Schadprogramme: Spyware.* Aufgerufen am 20.07.2015 unter https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/Schadprogramme/Spyware/spyware_node.html

[21] PURSCHE, O. (2013, 05. Juni). Schadprogramme täuschen Virenbefall nur vor. *welt.de*. Aufgerufen am 19.11.2014 unter http://www.welt.de/wirtschaft/webwelt/article116828024/Schadprogramme-taeuschen-Virenbefall-nur-vor.html

[22] POLIZEI-PRAEVENTION.DE. (k. A.). *PC gesperrt? Ransomware.* Aufgerufen am 20.07.2015 unter http://www.polizei-praevention.de/themen-und-tipps/pc-gesperrt-ransomware.html

[23] NORTON. (2012). *2012 Norton Cybercrime Report*. Aufgerufen am 20.07.2015 unter http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

[24] MCCORMACK, C. (2011). *SOPHOS: Die vier Grundsätze für umfassenden Web-Schutz.* Aufgerufen am 21.07.2015 unter http://www.sophos.com/de-de/medialibrary/Gated%20Assets/white%20papers/sophos4rulescompletewebprotectionwpna.pdf?la=de-DE.pdf

[25] IHLENFELD, J. (2012, 20. Dezember). *Google warnt vor gehackten Webseiten.* golem.de. Aufgerufen am 19.07.2015 unter http://www.golem.de/1012/ 80227.html

[26] VILSBECK, C. (2014, 05. März). *Android ist Ziel von 97 % der mobilen Malware.* techchannel.de. Aufgerufen am 19.07.2015 unter http://www.tecchannel.de/kommunikation/news/2053774/android_ist_ziel_von_97_prozent_mobiler_malware/

[27] WINTERER, A. (2013, 07. Juli). *Viren-Attacken: Android-Smartphones in Gefahr?* [Blog-Beitrag]. Aufgerufen am 19.07.2015 unter http://blog.zdf.de/hyperland/2013/07/viren-attacken-android-smartphones-in-gefahr/

[28] SCHISCHKA, S. (2013, 18. April). *Gefährliche Malware auf kostenlosen Pornoseiten.* pcwelt. Aufgerufen am 19.07.2015 unter http://www.pcwelt.de/news/Gefaehrliche_Malware_auf_kostenlosen_Porno-Seiten-Gefahr_im_Web-7839179.html

[29] ZOLLONZ, A. (2013, 05. Juni). *Virus auf movie2k: Streaming-Plattform verbreitet Malware.* netzwelt.de. Aufgerufen am 20.07.2015 unter http://www.netzwelt.de/news/96091-virus-movie4k-streaming-plattform-verbreitet-malware.html

[30] ZELCH, B. (2013, 08. April). *Ist mein Computer infiziert? 5 Symptome bei einem Malware-Befall.* (Absatz 1-4). Aufgerufen am 07.12.2014 unter https://www.austrosec.at/2013/04/ist-mein-computer-infiziert-5-symptome-bei-einem-malware-befall/

[31] T-ONLINE. (2013, 19. November). *Ist Ihr Smartphone gehackt?* (Absatz 1–5). Aufgerufen am 07.07.2015 unter http://www.t-online.de/handy/smartphone/id_62854486/trojaner-test-ist-mein-smartphone-gehackt-.html

Arbeitsblatt	**AB 1**	**AB 2**
Titel	**Spam-Mails – wie schützt du dich?**	**Ein ganzer Zoo im Computer und auf dem Handy?**
Kompetenzen	Die Schülerinnen und Schüler erarbeiten die Möglichkeiten zum Schutz vor unerwünschten E-Mails (sogenannten Spam-Mails).	Die Schülerinnen und Schüler lernen verschiedene Formen von Schadsoftware kennen und können eine Übersicht anfertigen.
Methoden	Einzelarbeit, Partnerarbeit, Unterrichtsgespräch, Ergänzungs-Übung	Partnerinterview, Plakat, Experte (optional), Partnerarbeit, Einzelarbeit
Material	Arbeitsblatt	Arbeitsblatt
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja (nur für das Video von Monty Python notwendig)	ja

Hinweise für die Durchführung

AB 1: Spam-Mails – wie schützt du dich?

Anhand dieses Arbeitsblattes sollen die Schülerinnen und Schüler die drei „goldenen" Regeln des E-Mailing kennen lernen und begründen können. Die Form des E-Mailing kann dabei gewählt werden, wenn die Möglichkeiten dazu bestehen, ansonsten lassen Sie die Begründung vielleicht einfach als zusammenhängenden Text schreiben.

Die Ergänzungen zu den Sätzen soll eine kleine Wissensabfrage zum E-Mailing sein, denn oft beherrschen Schülerinnen und Schüler das E-Mailing, wissen aber nichts mit CC oder BCC o. ä. anzufangen:

Mögliche Antworten:

- Der Betreff einer E-Mail ist wichtig, weil … der Empfänger daran sofort sehen kann, ob es eine Spam-Mail ist oder nicht, auch ohne sie zu öffnen.
- Wenn ich mehrere Empfänger habe, mache ich Folgendes … Ich schreibe sie in die Empfängerzeile, getrennt durch ein Komma (Dies kann von Programm zu Programm variieren).
- Das BCC beim E-Mailing steht für … Blind Carbon Copy, also eine „blinde" Kopie. Die anderen Empfänger der E-Mail können diesen BCC-Empfänger nicht sehen.
- Anhänge öffne ich nur von ... Bekannten oder Freunden oder wenn ich weiß, von wem er stammt.
- Große Dateien über 10 MB verschicke ich nur, wenn … es unbedingt notwendig ist und ich beim Empfänger nachgefragt habe.
- Ich habe zwei E-Mail-Adressen, weil … ich eine private benutze für meine Freunde und Bekannten.
- Eine andere gebe ich öffentlich weiter. Die privaten E-Mail-Adressen bekommen nur … meine Freunde und Bekannten.
- Das mache ich mit blöden E-Mails … Ich lösche sie sofort oder ich markiere sie als SPAM.
- E-Mails von Unbekannten behandele ich so: Ich öffne nie Anhänge und bin vorsichtig mit dem Inhalt. Wenn mir etwas komisch vorkommt, lösche ich sie. Vor allem antworte ich nicht ohne weiteres.
- Auch in E-Mails bin ich höflich, weil … auf der anderen Seite keine Maschinen, sondern Menschen sitzen.

AB 2: Ein ganzer Zoo im Computer und auf dem Handy?

Die Auflistung möglicher Schädlinge für digitale Geräte ist didaktisch reduziert (s. Sachinformationen), bietet aber einen guten Einstieg in das Thema. Die Schülerinnen und Schüler sollen im ersten Arbeitsauftrag eine eigenständige Recherche auf den Seiten von klicksafe und dem Bundesamt für Sicherheit in der Informationstechnik – das sie auf diese Weise kennenlernen – vornehmen. Hier ist vielleicht etwas Hilfestellung und Vorarbeit notwendig, da diese Seiten sehr umfangreich sind und immer wieder aktualisiert werden.
Im zweiten Arbeitsauftrag sollen die Schülerinnen und Schüler nach der Informationsbeschaffung ihren Partner/ihre Partnerin informieren. Dies kann in Form eines „Partnerinterviews" geschehen: Als Synthese soll dann eine Seite mit den wichtigsten Informationen entstehen. Vielleicht besteht die Möglichkeit, auch andere Klassen über das Problem in Form eines Stationenlernens zu informieren.

Spam-Mails – wie schützt du dich?

„Spam-Mails sind eine wahre Plage, oder? Bestimmt hast du auch schon solche unerwünschten E-Mails bekommen. Der Name stammt wahrscheinlich von „SPiced hAM" (englisch für „gewürzter Schinken") was früher der Name eines Dosenfleischs war. Als Begriff für „massenhaft" und „unerwünscht" soll das Wort aus einem alten Fernsehsketch der Komikergruppe „Monty Python" stammen.
Du kannst dir den Spot hier anschauen: **http://bit.ly/19PeUMn**

Spam-Mails sind nicht nur lästig, sondern können auch gefährlich werden. Deshalb gibt es drei goldene Regeln des E-Mailing:

- niemals auf eine Spam-Mail reagieren
- den Spam-Filter „trainieren"
- die E-Mail-Adresse nicht überall angeben und immer eine zweite E-Mail-Adresse anlegen

Arbeitsaufträge:

1. Überlege, warum diese Regeln sinnvoll sind! Schreibe eine E-Mail an eine Freundin/einen Freund, in der du ihr/ihm diese Regeln erklärst. Wenn du keine Möglichkeit hast eine E-Mail zu schreiben, schreibe die Erklärung auf die Rückseite des Arbeitsblattes!

2. Aber es gibt noch weitere wichtige Dinge, die man beachten sollte. Hier findest du Hinweise, ergänze sie zu ganzen Sätzen:

Der Betreff einer E-Mail ist wichtig, weil …

Wenn ich mehrere Empfänger habe, mache ich folgendes …

Das BCC beim E-Mailing steht für …

Anhänge öffne ich nur von …

Große Dateien über 10 MB verschicke ich nur, wenn …

Ich habe zwei E-Mail-Adressen, weil …

Die privaten E-Mail-Adressen bekommen nur …

Das mache ich mit blöden E-Mails …

E-Mails von Unbekannten behandele ich so:

Auch in E-Mails bin ich höflich, weil …

Ein ganzer Zoo im Computer und auf dem Handy?

Ein wenig digitale Biologie?
Auf unserem Computer, Smartphone oder Tablet können sich zahllose Schädlinge tummeln.

Computerviren
Darunter sind solche Dinge gefasst wie Bootviren (dann startet der Computer erst gar nicht mehr), Makroviren (weit verbreitet in Office-Programmen), Datei-Viren (sie starten mit einem Programm), Polymorphe Viren (sie heißen so, weil sie sich gut verkleiden können und ständig verwandeln) und die Tarnkappen-Viren (die sich besonders gut verstecken können).

Rogueware
Rogueware ist besonders perfide: Diese Software gaukelt vor, andere Schadsoftware zu entfernen, tut aber das Gegenteil.

SpyApps
SpyApps zeichnen unbemerkt die Kommunikation auf, schalten Mikrofon und Kamera ein oder leiten den Standort des Handys weiter.

Scareware werden gefälschte Warnmeldungen u. ä. bezeichnet, die den Nutzer verunsichern und dazu verleiten sollen, andere Software zu installieren.

„Würmer"
Ein Wurm kann sich selbst vervielfältigen und automatisch Kopien verschicken. Er braucht auch kein anderes Programm (wie ein Virus), sondern arbeitet ganz selbstständig.

„Trojaner" – Trojanische Pferde
(Kennst du die Sage vom Trojanischen Pferd?) Ein Trojaner benutzt einen gemeinen Trick. Das Virus gibt vor, etwas anderes zu sein (z. B. ein Spiel oder nützliches Programm): Kaum hast du es aufgerufen, befällt es deinen Computer. In diesen Trojaner kann auch ein Spionageprogramm versteckt sein, das deinen Computer auskundschaftet (und deine Passwörter munter weiterleitet).

Hoaxes
Ein Hoax (zu Deutsch: „Jux", „Schabernack" oder „Schwindel") ist nichts anderes als eine Falschmeldung, die von Person zu Person verbreitet wird (z. B. via SMS, WhatsApp- oder Facebook-Nachricht). Ein Hoax besteht meist aus drei Elementen; einem Aufhänger, der Echtheit vermitteln soll, gefolgt von einer Aufklärung über die aus dem Internet drohende Gefahr und der abschließenden Bitte, diese Information an so viele Internetnutzer wie möglich weiterzuleiten. Echte Virus-Warnungen werden nie auf diese Weise verschickt.

Und wie kommen diese Viren, Würmer, Trojaner und Hoaxes auf deinen Computer und in dein Handy? Und wie kannst du dich davor schützen?

Arbeitsaufträge:

1. Informiere dich über das Problem auf den folgenden Seiten:

klicksafe: **www.klicksafe.de/themen/technische-schutzmassnahmen/den-pc-schuetzen/**
Bundesamt für Sicherheit in der Informationstechnik: **https://www.bsi-fuer-buerger.de/**

2. Wie sieht ein wirksamer Schutz aus? Erkläre es deiner Nachbarin/deinem Nachbarn und umgekehrt!

3. Erstelle eine Übersicht mit den wichtigsten Informationen über Viren und den Schutzmaßnahmen! Versuche doch bitte, Symbole und Bilder in deine Übersicht einzubringen.
Erstelle in einem Textbearbeitungsprogramm ein Merkblatt mit Symbolen!

Hoaxes, Kettenbriefe und Shitstorms

Hoaxes

„Hoax" kommt aus dem Englischen und bedeutet „Scherz", „Schabernack" oder auch „Schwindel". Als Hoax wird eine Falschmeldung bezeichnet, die über Soziale Netzwerke, wie bspw. Facebook, WhatsApp etc. schnell an viele Personen weitergeleitet wird.[1] Da der Inhalt der Hoaxes meist nicht völlig abwegig ist, ist es vor allem für Kinder und Jugendliche nicht immer einfach, sie als Falschmeldungen zu enttarnen. Meistens sind Hoaxes witzig bzw. nervig und harmlos. Immer wieder kommt es aber vor, dass über Hoaxes Viren eingeschleppt und Phishing-Attacken geschickt getarnt werden.

Hoaxes haben in der Regel einen reißerischen Inhalt: z. B. wird für einen Leukämiekranken dringend eine bestimmte Blutgruppe gesucht oder es wird gemeldet, dass Handys während des Aufladens explodierten und den Nutzer verletzen können, oder es wird entrüstet auf das traurige Schicksal der Bonsai-Katzen hingewiesen.[2]

Ein technischer Schutz ist angesichts des viralen Verbreitungsweges von Hoaxes nicht möglich. Umso wichtiger ist es daher, Kinder und Jugendliche über Hoaxes aufzuklären und sie so dazu zu befähigen, Falschmeldungen als solche zu erkennen.

***Tipp:** Die Technische Universität Berlin führt eine Hoax-Liste, die ständig aktualisiert wird:*
http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Kettenbrief

Kettenbriefe funktionieren nach dem Schneeballprinzip: Ein Empfänger erhält eine Nachricht mit einer mehr oder minder expliziten Aufforderung, diese an eine Mindestanzahl von Freunden und Bekannten weiterzuschicken.[3] Diese leiten sie dann wiederum an ihre Kontakte weiter. So verbreitet sich ein Kettenbrief innerhalb kürzester Zeit an eine große Personenzahl.

In einigen Kettenbriefen wird dem Empfänger mit Unglück, Tod etc. gedroht, wenn er die Nachricht nicht weitersendet. Andere Kettenbriefe versprechen dem Nutzer Glück, Geld etc., sollte die Nachricht weitergeleitet werden. Wieder andere setzen den Nutzer unter moralischen Druck. Gerade für junge Nutzer ist nicht immer erkenntlich, dass es sich bei dem Inhalt eines Kettenbriefes um einen (schlechten) Scherz handelt: Ende 2013 kursierte in WhatsApp eine Sprachnachricht, in der eine Computerstimme damit drohte, den Empfänger und dessen Mutter umzubringen, wenn die Nachricht nicht an mind. 20 weitere Personen weitergeleitet wird. Viele Kinder fühlten sich durch die Botschaft bedroht und wandten sich daraufhin an Eltern, Lehrer und Polizei.[4]

Eine neuere Entwicklung im Bereich der Kettenbriefe ist die Nominierung einer Person mittels WhatsApp oder Facebook, sich einer bestimmten Herausforderung zu stellen: Im Sommer des Jahres 2014 kursierte in den Sozialen Medien die sog. **ALS Ice Bucket Challenge**, an der selbst Prominente aus Politik, Sport, Gesellschaft etc. teilnahmen. Der Nominierte hatte die Aufgabe, sich einen Kübel eiskaltes Wasser über den Kopf zu schütten und dann drei weitere Personen zu nominieren, dies ebenfalls zu tun. Die Aktion sollte zudem gefilmt und das Video als Beweis im Internet bereitgestellt werden. In die Welt gesetzt wurde die **Ice Bucket Challenge** für den Zweck, auf die seltene Krankheit **Amyotrophe Lateralsklerose** (ALS) hinzuweisen. Ursprünglich war angedacht, dass sich nur diejenigen Personen der Ice Bucket Challenge unterziehen sollten, die nicht bereit waren für den guten Zweck zu spenden. Mit zunehmender Popularität der Challenge beteiligten sich viele Personen nicht nur mit einer Eiswasserdusche, sondern auch an der Spende.[5]

Bedenklich werden derartige Kettenbriefe bzw. Challenges vor allem dann, wenn zu riskanten Aktionen aufgerufen wird. Dies ist aber nicht immer der Fall: In den Sozialen Netzwerken lässt sich aktuell noch eine weitere Form des Kettenbriefes identifizieren: Nutzer nominieren zwei Freunde oder Bekannte, die dann ihre 10 Lieblingsbücher, -songs etc. angeben müssen. Diese nominieren dann wiederum je zwei Personen etc.

INFO: *Bekannterweise werden nicht nur schadhafte Inhalte in viraler Form über das Internet verbreitet. Eine neue, durch das Internet entstandene Sonderform der Kommunikation sind sog.* ***Memes****. Dabei handelt es sich um Bilder und kurze Videos, die vielfach verbreitet und dabei z. B. kopiert, erweitert, neu betitelt oder fast komplett verändert werden. Doch so schnell wie die einzelnen Memes aufgetaucht sind, so schnell sind sie meist auch wieder verschwunden. Dennoch entwickeln sich auf diese Weise interessante Dynamiken bezüglich dessen, worüber gesprochen wird und was gerade von allgemeinem Interesse ist. Einen kurzen Überblick über die Entstehung und Bedeutung von Memes findet sich hier:*
www.thegap.at/rubriken/stories/artikel/wie-das-meme-zum-meme-wurde/

Shit- und Candystorm

„Shitstorm" ist eine neudeutsche Wortschöpfung, im Englischen ist stattdessen der Begriff **„Online-Firestorm"** gebräuchlich. Ein Shitstorm ist eine Empörungswelle in Form von massenhafter Schmähkritik gegen eine Person oder eine Sache via Soziale Netzwerke, Messenger etc. Nach Sascha Lobo, einem bekannten deutschen Blogger, ist ein Shitstorm ein „Prozess, wo in einem kurzen Zeitraum eine subjektiv große Anzahl von kritischen Äußerungen getätigt wird, von denen sich zumindest ein Teil vom ursprünglichen Thema ablöst und stattdessen aggressiv, beleidigend, bedrohend oder anders attackierend geführt wird"[6]. Die Dynamik, die ein solcher Shitstorm entfalten kann – wie viele Nutzer sich daran beteiligen und ob, bzw. wie er medial aufgegriffen wird – ist kaum abzuschätzen.

Ein Shitstorm kann begründet oder unbegründet sein, kann Einzelpersonen oder Unternehmen, Verbände, Parteien etc. betreffen. Für eine Einzelperson kann ein Shitstorm – gleich ob begründet oder unbegründet – schlimme psychische Folgen haben (siehe **Kapitel 6_1 Cyber-Mobbing**). Für ein Unternehmen, einen Verband oder eine Partei, die sich einem Shitstorm ausgesetzt sehen, besteht die begründete Befürchtung eines Image-Verlustes mit den damit verbundenen negativen Auswirkungen auf Verkaufs- bzw. Mitgliederzahlen:

- Die Firma Henkel sah sich 2011 massiven Anfeindungen im Netz gegenüber: Sie hatte zu einem Designwettbewerb für das Pril-Etikett im Rahmen einer limitierten Edition aufgerufen, aber nicht mit den absurden Vorschlägen gerechnet, die von den Online-Nutzern eingingen. Als Henkel die Gewinnerliste bereinigte, kam es zum Shitstorm.[7]

- Der Deutsche Fußballbund veröffentlichte via Twitter anlässlich des 100. Länderspielsieges ein Foto zweier deutscher Fußballspieler aus dem Jahr 1942, auf deren Trikots ein Hakenkreuz zu sehen war. Der DFB sah sich genötigt, das Bild nach einem Shitstorm wieder zu löschen.[8]

- Die Partei Bündnis 90/Die Grünen erlebten vor der Bundestagswahl 2013 einen Shitstorm. Die Partei hatte sich für die Einführung eines sogenannten Veggie-Tages ausgesprochen. An einem Tag in der Woche sollten Kantinen nur fleischlose Kost anbieten. Die Grünen wurden daraufhin u. a. als Ökofaschisten bezeichnet.[9]

Problematisch an den Shitstorms ist u. a. auch, dass potenziell die Möglichkeit besteht, diese bewusst loszutreten und zu befeuern – bspw. durch gefälschte Posts etc. – um Konkurrenten zu schaden.

Nicht immer besteht diese Art von Massenphänomen aus negativer Kritik. Es gibt sie auch unter umgekehrtem Vorzeichen: Der Adressat wird dann mit positivem Zuspruch überhäuft.[10] Diese Form wird als **„Candystorm"** bezeichnet. Geprägt wurde dieser Begriff von Twitter-Nutzern und Grünen-Mitgliedern, die dem Aufruf von Volker Beck (Die Grünen) folgend dessen Kollegin Claudia Roth dazu ermunterten, weiterhin Parteivorsitzende zu bleiben. Neben Claudia Roth kamen bislang einige Politiker, Prominente und Unternehmen in einen Candystorm.

Shit- und Candystorms können ein enormes Machtpotenzial entfalten: Unternehmen, politische Entscheidungsträger, Einzelpersonen etc. können nicht sicher davon ausgehen, dass (vermeintliches) Fehlverhalten unbemerkt und ungestraft bleibt. Auf der einen Seite können Shit- und Candystorms daher als Korrektiv zum Aufzeigen und Anprangern von Missständen fungieren. Auf der anderen Seite ist klarzustellen, dass ein Shit- bzw. ein Candystorm keine Mehrheitsmeinung abbilden, emotional geführt werden und daher unter Umständen die Möglichkeit für eine konstruktive Auseinandersetzung verbauen.

Links und weiterführende Informationen

Webseiten

http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml
Die Technische Universität Berlin führt eine Hoax-Liste, die ständig aktualisiert wird.

http://www.feinheit.ch/media/medialibrary/2012/04/shitstorm-skala_2.pdf
Shitstorm – Skala, die von der Social Media Expertin Barbara Schwede und Daniel Graf entwickelt wurde.

www.fr-online.de/digital/claudia-roth-und-der-candystorm,1472406,20860688.html
Ein Artikel zum neuen Phänomen „Candystorm".

Endnoten

[1] TERNIEDEN, H. (2009, 17. Dezember). *Jahrzehnt des Hoaxing: Unglaublich, aber falsch.* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/panorama/gesellschaft/jahrzehnt-des-hoaxing-unglaublich-aber-falsch-a-666310.html

[2] ZIEMANN, F. (2014, 10. November). *TU Berlin: Hoax-Liste*. Aufgerufen am 07.07.2015 unter http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

[3] ZIEMANN, F. (2014, 19. November). *TU Berlin: Hoax-Info Service*. Aufgerufen am 07.07.2015 unter http://hoax-info.tubit.tu-berlin.de/hoax/#8

[4] MILDE, S. (2015, 10. Januar). *WhatsApp: Vorsicht vor diesen Kettenbriefen.* chip.de. Aufgerufen am 07.07.2015 unter http://praxistipps.chip.de/whatsapp-vorsicht-vor-diesen-kettenbriefen_37162

[5] SUEDDEUTSCHE.DE. (2014, 25. August). *Was Sie über das Phänomen Eiskübel wissen müssen*. Aufgerufen am 03.07.2015 unter http://www.sueddeutsche.de/panorama/ice-bucket-challenge-was-sie-ueber-das-phaenomen-eiskuebel-wissen-muessen-1.2102571

[6] LOBO, S. (2010, 21. April). *How to survive a shitstorm* [Video]. Aufgerufen am 02.12.2014 unter https://www.youtube.com/watch?v=-OzJdA-JY84

[7] BREITHUT, J.(2011, 20. Mai). *Soziale Netzwerke: Pril-Wettbewerb endet im PR-Debakel.* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/netzwelt/netzpolitik/soziale-netzwerke-pril-wettbewerb-endet-im-pr-debakel-a-763808.html

[8] GLINDMEIER, M. (2014, 22. November). *Tweet zeigt Siegbild von 1942: DFB blamiert sich mit dem Foto aus Nazi-Zeit.* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/sport/fussball/dfb-twittert-nazi-bild-von-1942-a-1004449.html

[9] VON BOEHN, V. H. (2013, 05. August). *Gründe Pläne für Vegetarier-tag lösen Shitstorm aus.* derwesten.de. Aufgerufen am 06.07.2015 unter http://www.derwesten.de/politik/gruene-plaene-fuer-vegetarier-tag-loesen-shitstorm-aus-id8278629.html

[10] TAGESSPIEGEL.DE. (2012, 12. November). *Candystorm statt Shitstorm auf Twitter*. Aufgerufen am 10.07.2015 unter http://www.tagesspiegel.de/politik/gruenen-chefin-claudia-roth-candystorm-statt-shitstorm-auf-twitter/7376754.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Falschmeldungen – nicht immer harmlos**	**Shitstorm**
Kompetenzen	Die Schülerinnen und Schüler erkennen die Strukturmerkmale von Falschmeldungen, die als „Hoaxes" bekannt sind.	Die Schülerinnen und Schüler erkennen Merkmale des Internet-Phänomens „Shitstorm" und Möglichkeiten der Bewertung. Sie beurteilen die Legitimität solcher Aktionen.
Methoden	Gruppenarbeit, versch. Präsentationsmöglichkeiten	Gruppenarbeit, Internet-Recherche, Mind-Map
Material	Arbeitsblatt (je nach Präsentationsform versch. Materialien wie Papier, Stifte, Kleber)	Arbeitsblatt, (evtl. großes Papier für große Mind-Map)
Zeit (in Minuten)	90	90
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Falschmeldungen – nicht immer harmlos	Hoaxes laden für den aufgeklärten Betrachter oft zum Schmunzeln ein, trotzdem darf man ihre Bedeutung nicht unterschätzen. Die Schülerinnen und Schüler sollen hier einige der modernen Sagen („urban legends") aus dem Internet unter dem Begriff der „Hoaxes" kennenlernen und sich mithilfe der Internet-Adresse der Technischen Universität Berlin über den aktuellen Stand informieren. Hier könnten Sie eine Phase einbauen, in der die Schülerinnen und Schüler über ihre eigenen Erfahrungen berichten, aber auch über ihre Ängste sprechen können. Gerade jüngere Schülerinnen/Schüler können von bspw. Gewaltandrohung sehr verängstigt sein. Wie immer bei diesen Themen gilt es, sensibel zu reagieren. Mit dem letzten Arbeitsauftrag sollen die Schülerinnen und Schüler ihre Erkenntnisse kreativ umsetzen und damit das Gelernte festigen.
AB 2: Shitstorm	Sascha Lobo bezeichnet sich selbst als Autor, Blogger, Microblogger und Strategieberater und ist vielfach in den Neuen (wie auch in den alten) Medien präsent. Seine Definition eines Shitstorms ist nicht wissenschaftlich, kennzeichnet aber trotzdem sehr anschaulich das Phänomen. Auf der Grundlage der Beaufort-Skala zur Einteilung von Windstärken (die den Erdkunde-Kolleginnen und -Kollegen geläufig sein dürfte) versuchen Schwede und Graf eine Einteilung der Shitstorms. Hier dürfen Sie sehr leistungsstarke Schülerinnen und Schüler gerne zum kritischen Hinterfragen einer solchen Einteilung auffordern. Sie soll dazu dienen, den Shitstorm nicht pauschal zu verurteilen, sondern auch qualitativ zu bewerten. In der Mindmap sollen die Schülerinnen und Schüler ihre Erkenntnisse darstellen und sie sich gegenseitig präsentieren. Im letzten Arbeitsauftrag gehen die Schülerinnen und Schüler noch einen Schritt weiter mit der Frage, ob ein Shitstorm nicht auch positive Seiten haben kann, zum Beispiel als demokratisches Instrument der Meinungsäußerung. **Quellen** Definition: Lobo, S. (2012, 21. April). *How to survive a shitstorm* [Video]. Aufgerufen am 02.12.2014 unter **https://www.youtube.com/watch?v=-OzJdA-JY84** **Bildquelle:** „Sascha Lobo" von Matthias Bauer (flickr: Matthias Bauer) - originally posted to Flickr as Sascha Lobo. Lizenziert unter CC BY-SA 2.0 über Wikimedia Commons - **https://commons.wikimedia.org/wiki/File:Sascha_Lobo.jpg#/media/File:Sascha_Lobo.jpg**

Lust auf mehr?
Moderne Mythen oder urban legends sind ein schier unerschöpfliches Thema, das sich im Internet kongenial unterbringen lässt. Dazu gehören ganze Gebilde von Verschwörungstheorien, die früher in Büchern und Zeitschriften nur ein kleines Publikum fanden, nun aber weltweit ausgebreitet werden. Für historisch interessierte Schülerinnen und Schüler könnte als Beispiel hier die These von der „Nicht-Mondlandung" der Amerikaner kritisch hinterfragt werden.

Falschmeldungen – nicht immer harmlos

Hoaxes nennen Experten die vielen Falschmeldungen, die im Internet kursieren. Beliebte Hoaxes sind u. a.:

- Personen mit bestimmte Blutgruppe für einen Leukämie-Kranken gesucht
- Vorsicht! Handy explodiert beim Aufladen!
- Spritzen-Nadeln von HIV-Infizierten im Kinositz versteckt!
- Die Flugnummer Q33NY einer der Maschinen, die am 11.09.2011 ins World Trade Center flog, ergibt in der Schriftart **Wingdings** folgende Botschaft:

Q33NY

▽

Wingdings

▽

Quelle: The Museum of Hoaxes (www.hoaxes.org)

Die meisten Hoaxes sind schlicht witzig oder nervig. Einige jedoch spielen ganz bewusst mit Emotionen wie der Angst vor Tod oder Krankheit, Rachegefühlen etc. Unter folgender Adresse kannst du eine ständig aktualisierte Liste von Hoaxes finden, die von der Technischen Universität Berlin betreut wird:
http://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Arbeitsaufträge:

1. Teilt euch in 4er-Gruppen auf. Zwei von euch informieren sich über Hoaxes allgemein. Die anderen beiden informieren sich über Kettenbriefe, die per E-Mail, über Soziale Netzwerke oder Messenger-Apps verschickt werden. Sucht jeweils 2–3 Beispiele heraus, die ihr besonders interessant findet.

2. Tauscht euch in der Gruppe aus und stellt euch die Ergebnisse gegenseitig vor!

3. Denkt gemeinsam darüber nach, warum diese Hoaxes und Kettenbriefe in Umlauf gebracht werden und welche Folgen sie haben können.

4. Überlegt und recherchiert, wie man sich schützen kann! Erstellt Tipps zum Schutz für jüngere SchülerInnen. Ihr dürft eine der folgenden Präsentationsformen wählen:

   A einen Aufkleber
   B max. zehn einfache Sätze
   C ein Symbol / Piktogramm
   D ein Werbeplakat
   E einen Reim / ein Gedicht
   F ein Maus-Pad

Shitstorm

„Als Shitstorm wird ein Internet-Phänomen bezeichnet, bei dem innerhalb eines kurzen Zeitraums eine subjektiv große Anzahl kritischer Äußerungen getätigt wird, von denen sich zumindest ein Teil vom ursprünglichen Thema entfernt und stattdessen aggressiv, beleidigend oder bedrohend sind“

(nach Sascha Lobo, 2012).

Foto: Matthias Bauer

Die Wissenschaftler Barbara Schwede und Daniel Graf versuchten gar eine Skala zu beschreiben für die Stärke eines Shitstorms: Von 0 (keine kritischen Rückmeldungen) über 4 (Herausbildung einer vernetzten Protestgruppe. Wachsendes, aktives Follower-Publikum auf allen Kanälen) bis Stufe 6 (ungebremster Schneeball-Effekt mit aufgepeitschtem Publikum. Tonfall mehrheitlich aggressiv, beleidigend, bedrohend.).

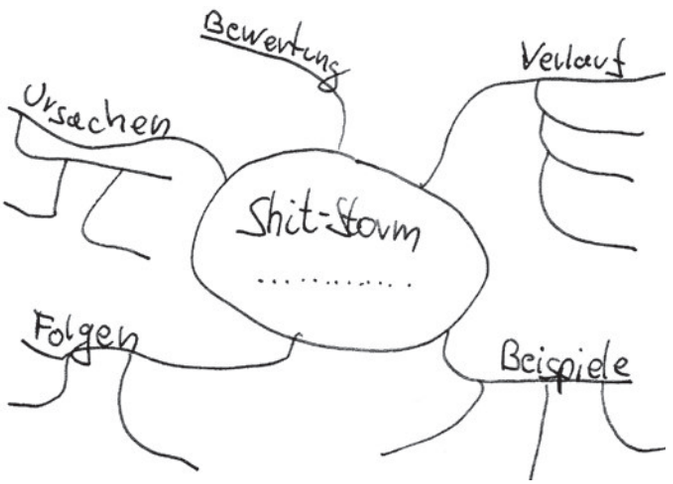
Arbeitsaufträge:

1. Informiert euch über einen Shitstorm aus dem vergangenen Jahr. Versucht herauszufinden, warum und wie er entstanden ist, wie er verlaufen ist was die Folgen waren. Versucht, den ausgewählten Shitstorm in der Skala von Schwede und Graf zu verorten. Diese ist zu finden unter

   http://www.barbaraschwede.ch/blog.html bzw.

   http://tinyurl.com/038ug8g

2. Stellt eure Ergebnisse in Form einer Mind-Map dar:



3. Shitstorms können auf der einen Seite für Einzelpersonen, Unternehmen, Verbände etc. problematisch sein und sie schädigen. Auf der anderen Seite können Shitstorms durch ihr Machtpotenzial auf Missstände hinweisen und sogar darauf hinwirken, diese zu beheben. Diskutiert diese zwei Seiten eines Shitstorms in der Klasse. Versucht, Regeln aufzustellen, wann ein Shitstorm in Ordnung wäre.

Illegale Downloads und Tauschbörsen

Illegale Downloads

Rechtslage

Aktuelle Blockbuster noch vor dem offiziellen Kinostart sehen, die neuste CD der angesagten Band herunterladen, benötigte Software aus dem Internet ziehen? Das ist mit ein wenig technischem Know-how nicht weiter schwer. Viele Personen laden illegal hochgeladene Daten aus ominösen Internetquellen auf den eigenen Computer herunter. In Deutschland laden laut einer gemeinsamen Studie des **Bundesverbands der Musikindustrie** (BVMI), des **Börsenvereins des deutschen Buchhandels** und der **Gesellschaft zur Verfolgung von Urheberrechtsverletzungen** (GVU) 3,7 % der Nutzer illegal Medieninhalte herunter.[1] Am häufigsten werden einzelne Musiktitel heruntergeladen, dicht gefolgt von Spiel- und Kinofilmen, Musikalben und TV-Serien.[2]

Wer Medieninhalte hochlädt, ohne deren Urheber zu sein, macht sich nach dem Urheberrecht strafbar, denn das Recht ein Werk zu vervielfältigen und zu verbreiten liegt alleine bei diesem selbst. Dies ist im Urheberrechtsgesetz (UrhG) Abs. 4, § 16 und § 17 geregelt. Auf einen Verstoß gegen das Urheberrecht können empfindliche Geldstrafen fällig werden (siehe **Kapitel 5_2 Urheberrecht und Open Content**). Das Herunterladen der Mediendaten ist grundsätzlich erlaubt, wenn die Kopien ausschließlich zu privaten Zwecken genutzt werden. Voraussetzung dafür aber ist, dass die Kopien nicht aus „offensichtlich rechtswidrigen" Quellen stammen dürfen.[3] User, die dabei ertappt werden, illegal Mediendateien hochzuladen bzw. aus dem Internet herunterzuladen, werden von beauftragten Anwaltskanzleien dazu aufgefordert, eine Unterlassungserklärung abzugeben und Schadenersatz zu zahlen. Die dabei verlangte Schadenersatzsumme ist meist sehr hoch angesetzt und teilweise auch scheinbar überzogen, um mögliche Folgetäter abzuschrecken.

Gefahren

Problematisch sind die Quellen zum illegalen Download nicht nur aus urheberrechtlicher Sicht: Über diese Portale sind auch Inhalte zugänglich, die bspw. in Deutschland bestimmten Altersgruppen eigentlich nicht zur Verfügung stehen dürfen. Darunter fallen bspw. gewalthaltige Filme oder solche mit pornographischen Inhalten. Jugendschutzrechtliche Bestimmungen und somit der Schutz von Kindern und Jugendlichen vor solchen Inhalten, werden auf diese Weise untergraben (vgl. **Kapitel 5_1 Jugendmedienschutz**).

Neben Jugendschutzrechtsverletzungen bergen illegale Downloadportale darüber hinaus die Gefahr, die Geräte der Nutzer mit Schadsoftware und Werbeprogrammen zu infizieren.

***Tipp:** Es ist wichtig, SchülerInnen frühzeitig für die Urheberrechts-Thematik zu sensibilisieren und mit ihnen den Wert von Filmen, Musikclips etc. zu diskutieren.*

Illegale Tauschbörsen

Filesharing

In den Medien ist häufig von Tauschbörsen die Rede. Gemeint sind damit sog. „Filesharing"-Systeme. **Filesharing** bezeichnet die Weitergabe oder den Tausch (engl. „sharing") von Dateien (engl. „files") zwischen Internetnutzern (engl. „**Peer-to-Peer**" bzw. „**P2P**"). Für das Filesharing ist bestimmte Software erforderlich, die zuerst auf dem Rechner herunter geladen werden muss. Mittels der Software ist es dann möglich, nach einer bestimmten Mediendatei zu suchen.[4] Bei einer Suchanfrage werden diejenigen Nutzer angezeigt, welche die Mediendateien zum Download bereitstellen. Da die übertragenen Dateien häufig groß sind und damit den Download verlangsamen, werden einzelne Datenpakete von verschiedenen Anbietern heruntergeladen. Häufig wird der Nutzer, der die Dateien auf seinen Rechner lädt, bereits selbst als Anbieter der besagten Mediendatei gelistet (z. B. bei **BitTorrent**).[5] Daneben kann jeder Nutzer auch ganz gezielt eigene Dateien zum Download anbieten.

Filesharing ist nicht grundsätzlich illegal. Urheberrechte werden nur verletzt, wenn ein Nutzer Mediendateien hochlädt, deren Urheber er nicht ist oder an denen er keine entsprechenden Rechte besitzt (s. o.). Stellt ein Nutzer einen Link zum Download auf eine geschützte Datei online, begeht er somit eine Urheberrechtsverletzung.

Share- oder Filehoster

Während beim Filesharing Mediendateien von anderen Nutzern heruntergeladen werden, erfolgt der Download in anderen Fällen über sog. „**Sharehoster**" bzw. **„Filehoster"** – also über die Server eines Diensteanbieters wie z. B. **RapidShare, Megaupload**. Eine Anmeldung, um den Dienst nutzen zu können, ist hier nicht erforderlich: Jeder Nutzer kann auf die Webseite des Diensteanbieters zugreifen und Dateien hoch- bzw. herunterladen. Auch hier gilt: Sharehoster sind nicht per se illegal. Allerdings wird diese Infrastruktur auch dazu verwendet, urheberrechtlich geschützte Mediendateien zu verbreiten.[6]

Streaming

Unter „**Streaming**" wird das Abspielen von Filmen im Browser verstanden – der Film wird dabei nicht heruntergeladen. Es gibt seriöse Anbieter, die das Streaming gegen eine monatliche Gebühr ermöglichen, wie z. B. **Watchever** oder **Amazon Prime**. Abseits dieser seriösen Anbieter bewegt sich das Streaming in einer rechtlichen Grauzone.[7] Der Europäische Gerichtshof entschied in seinem Urteil von 2014, dass das Zwischenspeichern von Filmen – wie es beim Abspielen im Browser der Fall ist – keine Urheberrechtsverletzung darstellt.[8] Die Anbieter der einschlägigen illegalen Downloadquellen (z. B. **kinox.to**, **video2k** oder **Movie2k)** hingegen begehen klar eine Urheberrechtsverletzung und können dafür belangt werden. Spektakulär war der Fall der Webseite **kino.to**, dessen Betreiber verhaftet und später verurteilt wurde.[9] Die Seite wurde im Juni 2011 zwar vom Netz genommen, allerdings erschien nur einige Wochen später ihr Nachfolger **kinox.to**. Durch die sich ständig ändernden technischen Möglichkeiten des Internets ist jedoch nicht klar, wie sich die Rechtslage hier weiter entwickeln wird.

Links und weiterführende Informationen

Webseiten

www.klicksafe.de/service/fuer-lehrende/zusatzmodule-zum-lehrerhandbuch/#c1519
Das klicksafe-Zusatzmodul *Nicht alles, was geht, ist auch erlaubt* bietet umfassende Information zum Thema „Urheberrecht" sowie Unterrichtsmaterialien.

www.klicksafe.de/service/materialien/broschueren-ratgeber/nicht-alles-was-geht-ist-auch-erlaubt-urheber-und-persoenlichkeitsrechte-im-internet/
Die Broschüre ist zusammen mit iRights entstanden und beschäftigt sich mit Urheber- und Persönlichkeitsrechten im Internet.

www.klicksafe.de/themen/rechtsfragen-im-netz/
Auf klicksafe.de finden sich umfassende Informationen zu Rechtsfragen im Netz.

http://irights.info/
Auf dieser Seite finden Sie umfassende Informationen zu Rechtsfragen im Netz.

http://internet-abc.de/kinder/wwg-musik-autor-urheber-recht.php
Hier finden sich kindgerechte Erläuterungen rund um das Thema „Urheberrecht".

Endnoten

[1] GESELLSCHAFT FÜR KONSUMFORSCHUNG (GfK). (2013). *Studie zur digitalen Content-Nutzung (DCN-Studie) 2013* [PowerPoint Präsentation]. Aufgerufen am 21.07.2015 unter http://www.gvu.de/wp-content/uploads/2015/08/DCN_Studie-2013.pdf

[2] STATISTA. (2014). *Anzahl von illegalen Mediendownloads aus dem Internet im Jahr 2010*. Aufgerufen am 21.07.2015 unter http://de.statista.com/statistik/daten/studie/200320/umfrage/illegale-downloads-von-medieninhalten/

[3] VERBRAUCHERZENTRALE NIEDERSACHSEN. (k. A.). *Urheberrechtsverletzungen und ihre Folgen*. (Absatz 4). Aufgerufen am 11.08.2015 unter http://www.verbraucherzentrale-niedersachsen.de/internet-urheberrechtsverletzung-und-seine-folgen

[4] KLICKSAFE. (k. A.). *Was sind Tauschbörsen? Was ist Filesharing?* Aufgerufen am 07.07.2015 unter http://www.klicksafe.de/themen/rechtsfragen-im-netz/tauschboersen/p2p-filesharing-tauschboersen-was-ist-das/

[5] KLICKSAFE & IRIGHTS. (2014). *Nicht alles, was geht, ist auch erlaubt! Urheber- und Persönlichkeitsrechte im Internet.* Aufgerufen am 07.07.2015 unter http://www.klicksafe.de/service/materialien/broschueren-ratgeber/nicht-alles-was-geht-ist-auch-erlaubt-urheber-und-persoenlichkeitsrechte-im-internet/

[6] MÖLLEKEN, J. (2010, 14. September). *Filehoster: Hehler oder Helfer?* spiegel.de. Aufgerufen am 10.07.2015 unter http://www.spiegel.de/netzwelt/web/filehoster-hehler-oder-helfer-a-717333.html

[7] PLÖGER, S. (2014, 09. Oktober). *So gefährlich sind die illegalen Download-Portale.* welt.de. Aufgerufen am 11.07.2015 unter http://www.welt.de/wirtschaft/webwelt/article133101871/So-gefaehrlich-sind-die-illegalen-Download-Portale.html

[8] FOCUS.DE. (2014, 11. Juni). *Endgültiges Aus für Redtube-Abmahner? EU-Gericht erklärt Streaming für legal.* Aufgerufen am 20.07.2015 unter http://www.focus.de/digital/internet/endgueltiges-aus-fuer-redtube-abmahner-europaeischer-gerichtshof-streaming-ist-keine-urheberrechtsverletzung_id_3912287.html

[9] REIßMANN, O. (2011, 08. Juni). *Kino.to: Ermittler verhaften Betreibern mutmaßliche Betreiber von Raubkopie-Seite.* spiegel.de. Aufgerufen am 20.07.2015 unter http://www.spiegel.de/netzwelt/netzpolitik/kino-to-ermittler-verhaften-mutmassliche-betreiber-von-raubkopie-seite-a-767375.html

Arbeitsblatt	**AB 1** ▶●	**AB 2** ▶▶
Titel	**Musik aus dem Internet?**	**Up- und Downloads – Was ist legal, was illegal?**
Kompetenzen	Die Schülerinnen und Schüler leiten Möglichkeiten für den legalen und gleichzeitig kostenlosen Musik-Download ab.	Die Schülerinnen und Schüler erkennen den Unterschied verschiedener Nutzungsformen von Up- und Downloads urheberrechtlich geschützter Materialien.
Methoden	Internet-Recherche, Tabelle, Unterrichtsgespräch, Einzelarbeit, Partnerarbeit	Internetrecherche, Gruppenarbeit, Kurzreferat, Präsentation als „Verkehrsschild“
Material	Arbeitsblatt	Arbeitsblatt, großes Papier, dicke Stifte.
Zeit (in Minuten)	90	135
Zugang Internet/PC	ja	ja

Hinweise für die Durchführung

AB 1: Musik aus dem Internet?

Verständlicherweise ist es die Regel, dass Musikrechteinhaber Geld verdienen wollen, und die allermeisten kostenlosen Angebote sind illegal. Aber es gibt eben auch Ausnahmen wie die Lizenz „Creative Commons“ oder vereinzelte Angebote. Die „Kindermusikbox“ ist so ein Angebot und soll hier als Beispiel dienen. Die Schülerinnen und Schüler sollen über das Problem reden, das bei kostenloser Musik aus dem Internet entstehen kann. Danach sollen sie in die Rolle des Künstlers/der Künstlerin schlüpfen und ihre Sicht der Dinge (Vor- und Nachteile) mit der eigenen Einstellung vergleichen (ebenfalls Vor- und Nachteile). Zum Schluss sollen sie lernen, genau auf eine Webseite zu schauen und das „Kleingedruckte“ zu lesen. Auf der Seite **www.kindermusikbox.de** unter **www.kindermusikbox.de/Lizenzbedingungen/** zu finden

Die Tabelle könnte so aussehen:

Für den Künstler/die Künstlerin		**Für dich**	
Vorteile	**Nachteile**	**Vorteile**	**Nachteile**
Viele hören die Musik	Sie verdienen kein Geld	Die Musik ist kostenlos	Die Qualität ist vielleicht nicht gut
Es ist billig herzustellen	Sie haben keine Kontrolle, wo die Musik auftaucht	Ich komme schnell an die Musik	Es ist vielleicht verboten
Sie brauchen keinen Plattenvertrag	Sie werden nicht berühmt	Ich kann sie vorher anhören	Ich bekomme keine CD

Außerdem sollen die Schülerinnen und Schüler verschiedene kostenlose (genauer gesagt für Deutschland GEMA-freie) Angebote zum Musik-Download kennenlernen.
Im vierten Arbeitsauftrag sollen die Schülerinnen und Schüler sich darüber informieren, welche legalen Möglichkeiten es gibt, an Musik zu gelangen. Dies sind:
- über Musikportale gegen Bezahlung
- als Download aus freien Quellen, so unter bestimmten Lizenzen und
- als Aufnahmen aus dem Radio (auch dem Internetradio)

Das Problem ist – wie oben beschrieben – dass es nicht immer einfach ist, zu sehen, ob die Quelle legal ist oder nicht. Deshalb ist es sicher von Vorteil, auf bekannten, seriösen Webseiten zu bleiben.

Aus diesem Grunde auch nochmals der ausdrückliche Hinweis auf den Mitschnitt von Musik aus dem Radio, wobei es keine Rolle spielt, ob die Technik zur Übertragung UKW, DAB oder Internet-Streaming heißt.

Hinweise für die Durchführung

AB 2: Up- und Downloads – Was ist legal, was illegal?

Die Schüler recherchieren über die beiden Nutzungsszenarien „zum Download bereitstellen" und „selbst downloaden". Sie können urheberrechtliche Probleme erkennen und denken über den legalen und illegalen Einsatz der unterschiedlichen Dienstleistungen sowie deren technisch-funktionale Unterschiede (Vergleich Tauschbörse – Filehoster) nach.
Mit dem ersten kurzen Austausch soll der Kenntnisstand (und vielleicht die Meinung) in der Lerngruppe ermittelt werden. Oft ist in diesem Bereich das Unrechtsbewusstsein bei Jugendlichen nicht sehr ausgeprägt, es existiert aber eine diffuse Vorstellung davon, dass es z. B. nicht rechtens ist, Musik weiterzugeben. Vielleicht greift an der Stelle schon die bisherige Arbeit zum Urheberrecht. Teilen Sie die Klasse in zwei Gruppen auf, z. B. nach dem Hausnummernprinzip, bei dem die Schüler durchgezählt werden und jeweils diejenigen mit den geraden und die mit den ungeraden Nummern eine Gruppe bilden. Es ist sicher ratsam, dass in jeder Gruppe Schüler sind, die sich bereits gut mit Tauschbörsen auskennen.

Die Internetrecherche ist nicht ganz einfach. Sie sollten den Schülern und Schülerinnen ausreichend Zeit geben, die Fragen zu beantworten.

Lösungen:

Aufgabe 1: Die David Guetta-Kopie – erlaubt oder nicht?
Till hat die CD illegalerweise heruntergeladen und somit auch illegalerweise zum Download zur Verfügung gestellt. Er hätte wissen müssen, dass die aktuelle Platte der Band nicht kostenlos im Internet zur Verfügung steht. Im Auftrag des Musiklabels sprechen Anwaltskanzleien Abmahnungen wegen unerlaubter Verwertung aus. Till kann also auch zu einem Schadensersatz verklagt werden.

Aufgabe 2: Die Antworten befinden sich in den Sachinformationen.

Aufgabe 3: Textvorschlag Vorfahrtsschild
Bleibt man bei Material, für das die Urheberrechte geklärt sind – sei es, weil es eigenes Material ist oder weil die Rechteinhaber eine Verbreitung erlaubt haben – oder nutzt Filehoster / Tauschbörsen zum rein privaten Gebrauch und nur passiv, ist man meist auf der sicheren Seite.

Lust auf mehr?
- Lebensweltbezug: Ist der Mitschnitt von Musik bei Videos auf YouTube legal? Diese Frage können Sie als Zusatz- oder Hausaufgabe geben.
- Ähnlich wie bei Musik verhält es sich mit Filmen, hier könnten Sie die Schülerinnen und Schüler ebenfalls recherchieren lassen.

Musik aus dem Internet?

Deine Freundin Anna hat dir vor kurzem erzählt,
dass sie sich Lieder aus dem Internet heruntergeladen hat.
Bisher hast du immer gedacht, dies sei verboten.
Auch dein Vater hat dir so etwas erzählt und
in den Nachrichten hört man das doch auch immer.

Arbeitsaufträge:

1. Stelle dir vor, du bist ein bekannter Musiker, der auch schon einige CDs gemacht hat. Würdest du wollen, dass man deine Lieder auch umsonst aus dem Internet bekommen kann? Diskutiert dies in der Klasse!

2. Setze dich mit einer Partnerin/einem Partner zusammen und überlege, welche Vorteile und Nachteile es hat, wenn man Musik kostenlos aus dem Internet herunterladen kann. Füllt die Tabelle alleine aus und vergleicht dann:

Für den Künstler/die Künstlerin		Für dich	
Vorteile	**Nachteile**	**Vorteile**	**Nachteile**

Selbstverständlich ist es verboten, Musik kostenlos aus dem Internet herunterzuladen, wenn der Künstler dies nicht erlaubt. Im Laden musst du ja auch für eine CD bezahlen. Auf **www.kindermusikbox.de** *ist das anders, der Künstler hat dort seine Musik „freigegeben" und jeder darf sie sich kostenlos anhören. Aber das ist eigentlich eine Ausnahme, denn normalerweise muss man für die Lieder bezahlen.*

www.kindermusikbox.de
www.jamendo.de
https://archive.org/details/audio

3. Schaue dir die Seiten aus dem Kasten genau an. Wo steht, dass du die Musik kostenlos benutzen darfst? Arbeitet zu zweit und zeige es deiner Partnerin/deinem Partner.

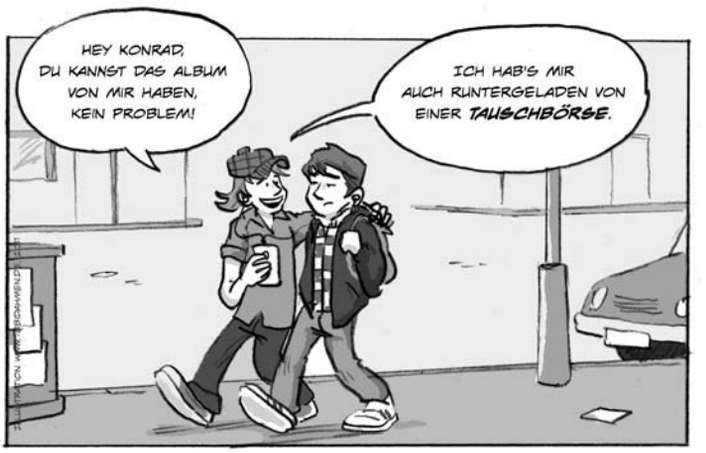
4. Dein Wunschlied läuft den ganzen Tag im Radio rauf und runter. Informiere dich, ob du Lieder aus dem Internetradio aufnehmen darfst oder nicht. Falls ja, wie darfst du das Lied nutzen? Ist die Weitergabe erlaubt? Das Anfertigen einer Kopie? Oder das Kopieren auf einen mp3-Player?

Informiere dich hier, wie du Musik aus dem Internet legal nutzen darfst:

www.irights.info und
www.respectcopyrights.de

Up- und Downloads – Was ist legal, was illegal?

Konrad und sein Freund Till hören auf dem Heimweg von der Schule das neue David-Guetta-Album …



Super Sache, aber kann das wirklich so einfach sein? Und ist das überhaupt legal? Darf man Dateien über solche Angebote herunterladen? Was denkt ihr? Macht eine kurze Umfrage in der Klasse.

Arbeitsaufträge:

1. Teilt euch in zwei Gruppen auf und recherchiert im Internet zu der Frage, ob das legal ist.
2. Teilt euch in Gruppe A und B.
   Bereitet ein Kurzreferat (maximal 10 Minuten) zum eurem Thema vor.
   Nehmt die Fragen und Stichwörter als Hilfen für euer Referat.

Gruppe	A Zum Download öffentlich bereitstellen	B Dateien selbst downloaden
Thema	Darf ich der Öffentlichkeit Dateien zum Download anbieten?	Darf ich Dateien herunterladen?
Fragen	Was ist verboten? Was ist erlaubt? Welche technischen Unterschiede gibt es zwischen Tauschbörsen und Filehostern?	
Stichwörter für die Suche in Suchmaschinen	Privatkopieschranke, Vervielfältigung, öffentlich zugänglich machen, Filehoster, Filesharing, Tauschbörse	
Internetadressen	**http://irights.info/kategorie/themen/filesharing-streaming** **http://www.klicksafe.de/themen/downloaden/tauschboersen/** **http://www.klicksafe.de/themen/downloaden/urheberrecht/** **http://www.klicksafe.de/themen/downloaden/urheberrecht/irights/filehosting/** **http://www.klicksafe.de/themen/rechtsfragen-im-netz/irights/filehosting/s/filehosting/** Artikel: Filehoster – Hehler oder Helfer auf www.spiegel.de („Hehler oder Helfer" in die Suchmaske eingeben)	

3. Erstellt nun Verkehrsschilder für das Bereitstellen und das Herunterladen von Dateien (in Tauschbörsen und über Filehoster) mit folgenden Überschriften:

   Stoppschild: Das ist verboten! Vorfahrtsschild: Das ist erlaubt!