Warum Computer krank werden

Die Hintergründe von Schadsoftware

Von Peter Leppelt und Dennis Weber

Jeder weiß es – Computer können Viren bekommen. Die Frage, die sich hingegen kaum einer stellt: Wieso ist das eigentlich so? Man sollte sich diese Frage allerdings ab und an stellen, denn sie kann dazu motivieren, sich zum einen intensiver darum zu kümmern und sich zum anderen auch sehr viel richtiger zu verhalten.

Die Bauart und der Zweck von Computerviren und -würmern haben in den letzten Jahrzehnten (ja, so lange gibt es sie schon) einen radikalen Wechsel durchgemacht. Wurden sie anfangs programmiert, um Fehler in Software aufzuzeigen, entwickelte sich später eine Art Wettbewerb, wer am meisten Rechner infizieren kann.

Diese Zeiten sind – entgegen vieler anderslautender Lehrmaterialien – seit Jahren vorbei. Inzwischen geht es um Geld. Viel Geld. Und wenn man die Systematik dahinter durchschaut, kann man sich sehr viel effektiver schützen – und (vor) seine(n) Schüler(n).

Die wilden Neunziger

Ende des letzten Jahrhunderts war es tatsächlich so: Viren und Würmer wurden zumeist von jungen Leuten geschrieben, die einfach nur angeben wollten. Das Motto war „Hey, ich habe 500 Computer infiziert! Ich bin viel besser als du!“. Diese Schadsoftware hat sich zumeist auf dem Zielrechner bemerkbar gemacht. Beispielsweise waren herunterfallende Buchstaben oder mehr oder weniger lustige Fehlermeldungen sehr beliebt.

Sie wissen, dass es heutzutage mehr Viren als je zuvor gibt – aber wann haben Sie derartige Fehler zum letzten Mal gesehen? Wahrscheinlich ein ganzes Weilchen nicht mehr – woran liegt das?

Die noch viel wilderen Zweitausender

Wenn Sie etwas Ähnliches heutzutage sehen, ist es sehr viel perfider. Es nennt sich „Scareware“. Aber dazu später mehr. Moderne Viren haben zunächst genau vier Eigenschaften:

- Sie wollen möglichst viele Rechner infizieren.
- Sie wollen nicht von Virenscannern gefunden werden.
- Sie wollen unter keinen Umständen vom Benutzer bemerkt werden – und dementsprechend die Stabilität und Funktionalität des Systems nicht beeinflussen.
- Sie wollen der einzige Virus auf dem Computer sein.

Nun könnte man natürlich sagen: „Okay, wenn der Virus meinen Computer nicht zum Absturz bringt oder sonst irgendwie meine Daten beschädigt – was soll's?“ Aber die Schädlinge haben dennoch eine Aufgabe, und das ist das eigentliche Ziel:

- Sie wollen Ihren Computer besitzen.

Im Anschluss an eine Infektion dürfen Sie den Computer zwar noch benutzen, aber er gehört jemand anderem. Immer, wenn der Rechner online ist, wird er benutzt.

Der normale Weg zu einem Virus oder Wurm gestaltet sich heute in der Regel so: Jemand entdeckt eine Sicherheitslücke in einer Software. Diese kann architekturbedingt oder schlicht durch fehlerhafte Programmierung entstanden sein.

Kleiner Einschub für diejenigen, die nun denken mögen „Na gut, das funktioniert ja nur mit Fehlern, und gute Software ist ja schließlich fehlerfrei“: Es ist mathematisch beweisbar, dass es unmöglich ist, eine komplexe Software ohne Fehler zu schreiben.

Die Kenntnis über diese Sicherheitslücke wird nun verkauft. Der Käufer (zumeist das organisierte Verbrechen) erstellt einen Schädling, der diese Sicherheitslücke zur Weiterverbreitung ausnutzen kann, und lässt ihn frei, indem er ihn beispielsweise in Freeware-Programmen, Tauschbörsen oder auf kompromittierten Websites versteckt.

Hat der Virus weltweit hinreichend Privatrechner infiziert – üblicherweise in der Größenordnung zwischen 10.000 und 1.000.000 Windows-PCs – werden sie aktiv und „zusammengeschaltet“. Vereinfacht heißt das: Sie laden weitere, eigene Schadsoftware vom Autor nach, und das komplette Netzwerk reagiert nun wie ein einziger großer Computer, der vollständig unter der Kontrolle des Virenautors steht; ein sogenanntes Botnet ist entstanden.

Mit diesem Botnet könnte der Autor nun so ziemlich alles tun, was er will. Sämtliche optischen Laufwerke aufgehen lassen, auf allen Rechnern gleichzeitig eine beliebige Meldung ausgeben, auf allen Lautsprechern die Melodie von Tetris spielen lassen … Aber so etwas tut niemand. Tatsächlich werden diese Botnets, so wie sie sind, wiederum verkauft.

Der neue Käufer verwendet sein neues Netzwerk üblicherweise für drei große Zwecke:

- Verschicken von Spam: Falls Sie sich schon einmal gewundert haben sollten, woher eigentlich die vielen unerwünschten Werbemails kommen: möglicherweise von Ihrem eigenen Rechner.
- Angreifen von ihm missliebigen Konkurrenten: Mit einem derart großen Netzwerk kann man *gezielte Attacken auf fremde Server* fahren: sog. Distributed Denial of Service Attacks (DDoS-Attacken). Die vielen PCs weltweit fragen alle gleichzeitig einen Dienst eines Servers an (bspw. eine Internetseite eines Konkurrenten) und beschäftigen diesen derartig stark, dass er zu nichts sonst mehr kommt. Er ist praktisch lahmgelegt.
- *Verteilen von illegalem Material:* Sehr heikles illegales Material wird – entgegen anderslautender Aussagen vieler Netzsperrenbefürworter – nur in absoluten Ausnahmefällen über klassische Webserver verteilt. Das liegt im Wesentlichen daran, dass bei einem solchen Vorgehen die Gefahr, erwischt zu werden, extrem hoch ist. Zumeist wird beispielsweise rechtsradikales oder kinderpornografisches Material in geschlossenen Netzen verteilt, die zudem über Botnetze betrieben werden. Das hat für die Urheber den Vorteil, dass das Material nicht von ihnen, sondern ggf. von Ihnen verteilt wird – aus juristischer Sicht kann es durchaus sein, dass der Privatnutzer, über dessen Rechner verteilt wurde, belangt wird. Außerdem ist es so sehr viel einfacher, seine Spuren zu verwischen.

Einige Tricks der halblegalen und illegalen Computerindustrie

Der Kampf einzelner Viren untereinander, mit Sicherheitslücken und mit Virenscannern

Oben wurde es schon erwähnt: Ein Virus möchte gerne der einzige Virus auf einem Computer sein. Das führt zu durchaus interessanten Grabenkämpfen zwischen den einzelnen Viren. Viele Viren (genauer: Würmer) versuchen nach der Infektion eines Rechners als erstes, die Sicherheitslücke, durch die sie eingedrungen sind, zu schließen. Einfach, damit kein anderer Virus die gleiche Lücke ausnutzen kann. Einige, etwas fortschrittlichere Schadprogramme flicken sogar noch weitere, ihnen bekannte Sicherheitslücken, die sie auf dem jeweiligen Computer finden. Ist dies getan, werden ggf. bereits vorhandene Schädlinge gezielt bekämpft; das heißt, sie werden gelöscht oder vom Internet abgetrennt.

Wenn auf dem System ein Virenscanner installiert ist, wird auch dieser nach Möglichkeit unschädlich gemacht. Davon darf der Nutzer natürlich nichts mitbekommen – die Funktion des Virenscanners wird so gut imitiert, dass sich der Rechnerbesitzer in Sicherheit wiegt. Updatemeldungen, Scans, Alarme … alles sieht genauso aus wie immer. Nur ist es eben eine Vorführung, ein Theaterspiel für den Nutzer.

Ist ein Computer bereits infiziert und Sie installieren erst dann einen Virenscanner, gilt in den meisten Fällen: Wer zuerst da ist, gewinnt.

Virenentfernung bei einer verseuchten Maschine gelingt in den allermeisten Fällen ausschließlich von einem nichtkompromittierten System aus. Beispielsweise bieten einige Virenscannerhersteller sog. Live-CDs an, von denen Sie den Rechner starten können. Dadurch wird nicht das installierte Windows, sondern ein Linux von der CD gestartet, wodurch von neutraler Seite nach Schädlingen gesucht werden kann, um diese dann zu entfernen.

Hoaxe und Kettenmails

Leider sieht man es in Lehrmaterialien zum Thema immer und immer wieder: Kettenmails (und die entsprechenden Pendants in sozialen Netzwerken, Instant-Messangern etc.) seien harmlose Scherze. Das stimmt nicht.

Wir haben nun gelernt, dass Spam-Mails über Heimrechner versendet werden. Nun müssen irgendwoher ja auch die E-Mail-Adressen kommen, an die man die unerwünschte Werbung schicken kann.

Das funktioniert neben vielen anderen Methoden auch durch Kettenmails. Die durchschnittliche E-Mail dieser Art besteht aus der Aufforderung, sie an möglichst viele Bekannte weiterzuleiten, gepaart mit einer Drohung („Wenn du sie nicht weiterleitest. dann [Hier bitte beliebiges Unglück einsetzen]“), einem Belohnungsversprechen („Wenn du sie weiterleitest, dann [Hier bitte beliebige, völlig abwegige Belohnung einsetzen]“) oder einem Appell an das Mitleid des Empfängers („Wenn du sie weiterleitest, dann wird [Irgendwer irgendwem irgendwie helfen]“).

Wenn man dann auf „Weiterleiten“ klickt, werden zumeist alle Adressen der vorhergehenden Teilnehmer der Kette in der E-Mail belassen. Nach den Gesetzen der Wahrscheinlichkeit wird eine häufig weitergeleitete E-Mail irgendwann wieder beim ursprünglichen Verfasser – seines Zeichens neben- oder hauptberuflich Spam-Mail-Versender – ankommen. Und zwar mit einem ganzen Stapel von E-Mail-Adressen, die folgende Eigenschaften aufweisen:

- Sie existieren.
- Sie werden gelesen.
- Die Besitzer sind naiv genug, auf so etwas hereinzufallen.

Das macht diese Adressen wertvoll und somit einträchtig für den Spammer.

Scareware

Scareware, vom englischen Verb to scare („jmd. Angst machen“) funktioniert auf besonders einfallsreiche Weise: Sie surfen durchs Netz und irgendwo poppt ein Fenster auf, das wie ein Virenscanner aussieht (bei fortgeschrittener Scareware sogar wie genau der Virenscanner, den Sie installiert haben). In diesem Fenster steht, dass ein Virus bei Ihnen gefunden wurde – natürlich verbunden mit einem Knopf, mit dem man ihn praktischerweise direkt entfernen kann. Und wenn Sie diesen Knopf drücken, haben Sie wirklich einen Virus …

Phishing und Pharming

Weiterhin treten häufig sog. Phishing-Attacken auf: Ein Internetnutzer bekommt beispielsweise eine E-Mail, die vorgeblich von seiner Bank stammt. In dieser E-Mail wird im Namen der Bank darum gebeten, auf einen Link innerhalb der Mail zu klicken und dort seine Zugangsdaten, PINs und mehrere TANs einzugeben. Der Link führt natürlich nicht zu der Original-Bankwebsite sondern zu einer nachgemachten Seite, die der der Bank aber täuschend ähnlich sieht. Im Endeffekt landen die Daten dadurch bei dem Autor der Phishingmail und nicht bei Ihrer Bank.

Pharming ist die etwas weiter entwickelte Variante: Der Rechner ist bereits mit einem Virus infiziert, der dafür

sorgt, dass Internetadressen automatisch zu einem Server des Angreifers umgebogen werden. Das heißt: Der Nutzer gibt z. B. *http://www.deutschebank.de* ein, und der Browser zeigt dies auch korrekt in der Adresszeile an. In Wirklichkeit sind Sie aber auf einer nachgemachten Seite.

Spyware
Abgesehen von der Ausforschung Ihrer Internetnutzung durch Online-Tracking-Systeme, wie sie von der Werbeindustrie angewendet werden, kann natürlich auch Ihr „Offline"-Verhalten oder einfach Ihr Computer für Datenschnüffler interessant sein.
Sogenannte Spyware forscht Ihr allgemeines PC-Verhalten aus und blendet bei (un)passender Gelegenheit auf Sie zugeschnittene Werbung ein – entweder unauffällig im Webbrowser oder ganz direkt als eigenes Fenster.

Aber wie kann man sich schützen?

Es wurde schon erwähnt: Es ist ab seinem gewissen Komplexitätsgrad nicht mehr möglich, fehlerfreie Software zu schreiben. Ein modernes PC-System ist ganz außerordentlich komplex (Bedenken Sie: Ein heutiger grafischer Taschenrechner hat deutlich mehr Rechenleistung als die Bordcomputer der ersten Mondmissionen!) und fällt somit in diese Kategorie.

Anti-Viren-Scanner
Wenn Sie Microsoft Windows verwenden, müssen Sie zwingend eine Anti-Viren-Software installieren. Übrigens müssen Sie diese Software als erstes auf Ihrem Computer nach der Betriebssysteminstallation aufspielen – anderenfalls kann sich ein Virus einschleusen und tarnen.
Sie können sich allerdings nicht darauf verlassen, denn Virenscanner funktionieren mit Virensignaturen. Das heißt, die Dateien auf der Festplatte werden mit Signaturen bekannter Viren verglichen und bei einer Übereinstimmung wird Alarm geschlagen. Die wichtigsten Wörter im letzten Satz sind „bekannter Viren". Kennt der Scanner den Schädling nicht, wird er ihn übersehen, weshalb die neuesten Schädlinge stets weiterhin gefährlich sind.
Zwar arbeiten moderne Scanner auch mit Heuristiken, mit denen man am Verhalten eines Programms zu erkennen versucht, ob es ein Virus sein könnte, aber Tatsache ist: Wenn es jemand speziell auf Sie abgesehen hat und das entsprechende Know-How aufweist, wird er Ihren Rechner unter seine Kontrolle bringen können – Virenscanner hin oder her.

„Firewalls"
„Personal Firewalls" verhindern, dass Ihr Computer unbemerkt von außen attackiert wird oder Daten ohne Ihre Erlaubnis versendet werden. Die integrierten Firewalls von Windows und MacOS sollten als Minimallösung betrachtet werden – sie wehren lediglich Angriffe von außen ab, hindern installierte Programme (wie etwa Viren oder Spyware) aber nicht daran, Daten zu versenden. Auch Firewalls sind prinzipbedingt nicht perfekt. Auch Firewalls werden von Viren bekämpft. Auch Firewalls sind dennoch absolut notwendig.

Und wie kann man sich nun wirklich schützen?!

Freie Software
Nutzen Sie Freie Software (zu unterscheiden von „Freeware", s. u.): Sogenannte Open-Source-Software ist immer gratis, liegt im Programmcode vor und kann so auf „Hintertürchen" kontrolliert werden, was eine riesige Gemeinde von Programmierern auch regelmäßig tut. Die Gefahr, sich Spyware oder Viren zu installieren, die Ihr Verhalten ausforschen, sinkt dadurch stark. Sie erkennen solche Software an der Lizenz; empfehlenswert sind: GPL oder LGPL (GNU General Public License), MIT-Lizenz, Apache-Lizenz, BSD-Lizenz, MPL (Mozilla Public License).
Nutzen Sie nicht nur Standardsoftware: Wie auch in der Biologie fördern Monokulturen den Virenbefall. So ist auf den meisten PCs Microsoft Windows, als Browser der Internet Explorer und als Mailprogramm Microsoft Outlook oder Outlook Express/Windows Mail installiert. Virenautoren schreiben daher in den allermeisten Fällen ihre Schädlinge für genau diese Kombination, um möglichst viele Opfer zu erreichen.
Gute Alternativen, die zudem auch gratis im Internet verfügbar sind, sind beispielsweise: Als Betriebssystem das auf Linux basierende OpenSuSE (*www.opensuse.org/de*), Ubuntu (*www.ubuntu.com*) oder Fedora (*http://fedoraproject.org/de/*) – um nur die drei häufigsten zu benennen –, als Browser Mozilla Firefox (*www.mozilla.com/de*) oder Opera (*www.opera.com*) und als E-Mail-Programm Mozilla Thunderbird (*www.mozilla.com/de*) oder Pegasus Mail (*www.pmail.com/downloads_s3_t.htm*). Firefox und Thunderbird gibt es auch für Microsoft-Windows-Betriebssysteme – wenn Sie also den Systemwechsel scheuen, können und sollten Sie dennoch diese beiden Programme verwenden.
Passen Sie bei Gratisprogrammen („Freeware") im Netz auf: Im Umkehrschluss bedeutet der letzte Tipp, dass Nicht-Freie Software – insbesondere, wenn sie gratis im Internet angeboten wird – mit Vorsicht zu genießen ist. Freeware beherbergt häufig Viren oder Spyware. Wählen Sie Ihre Quellen extrem sorgsam aus!

Windows-Systeme in Schulen
In den allermeisten Schulen werden Microsoftsysteme eingesetzt. Objektiv gesehen gibt es aber keinen Grund dafür. Es existieren gute und einfach zu bedienende Betriebssysteme und Anwendungsprogramme, die zudem gratis (frei) und sehr viel sicherer sind. Ein oft gehörtes Argument für den Einsatz von Windows an Schulen ist: Die Firmen erwarten Kenntnisse in diesem Bereich seitens ihrer zukünftigen Mitarbeiter.
In der Tat ist es aber so, dass sich die Bedienung der Anwendungen zwischen den Betriebssystemen nur sehr marginal unterschiedet. Es ist aus gesellschaftlicher Sicht schwer nachvollziehbar, warum Schülerinnen und Schüler im Informatikunterricht beispielsweise ein Jahr lang Microsoft Excel lernen sollen und dabei auf einen ausländischen Monopolisten geprägt werden. Natürlich ist der Umgang mit Tabellenkalkulationen wichtig – nur existieren eben zahlreiche Freie Software-Produkte, die genau das Gleiche leisten (OpenOffice.org, libreoffice, Koffice …).
Dass Microsoft Schulen verbilligt bis gratis Lizenzen anbietet, ist natürlich vollkommen verständlich. Dass das Bildungssystem dies aber annimmt, ist eher verwundernd.

Gute Passwörter
Passwörter, die aus echten Wörtern oder Eigennamen bestehen oder zusammengesetzt sind, sind prinzipiell extrem unsicher. Gleiches gilt für reine Zahlenketten oder Kombinationen aus beidem. Sogenannte Wörterbuchattacken (engl.: Dictionary- oder Brute-Force-Attacks) mit speziellen Programmen hebeln derlei Passwörter innerhalb weniger Sekunden aus. Dadurch kann zum Beispiel jemand in Ihrem Namen Mails versenden, Ihre Profile bei sozialen

Netzwerken einsehen und verändern oder mit Ihren Daten einkaufen.
Ein gutes Passwort muss aus vollkommen sinnlos zusammengefügten Klein- und Großbuchstaben, Zahlen und Sonderzeichen bestehen, um einen möglichst großen Zeichenraum zu besitzen. Mindestens 8 Zeichen – besser 12 – sollten ebenfalls vorhanden sein. Ein gutes Passwort wäre zum Beispiel: „DG1gPi,egzh."
Nun stellt sich die Frage: Wie, bitteschön, soll man sich so etwas merken? Bilden Sie Merksätze: Nimmt man die Anfangsbuchstaben, Zahlen und korrekte Interpunktion des Satzes „Das Geheimnis 1 guten Passworts ist, es geheim zu halten.", so kommt man auf die obige Zeichenkette und kann sie sich problemlos merken.
Bei einer Zeichenbegrenzung des Passworts durch den Anbieter auf unter 8 Zeichen oder einer Beschränkung auf Buchstaben und Zahlen, versuchen Sie nach Möglichkeit, einen anderen Anbieter zu finden – es sei denn, der Dienst ist völlig unkritisch.
Wenn man aber ehrlich ist, sind diese Tipps zwar nützlich und letztlich Basiswissen – aber dennoch wird man damit nicht alle Gefahren abfangen können.

Und wie schützt man sich so wirklich wirklich?

Der einzig wirkliche Schutz, den es geben kann, ist …

Ihr Großhirn
In der Informationstechnik gibt es eine (relativ gesehen) sehr alte Weisheit, die häufig an Computern in Rechenzentren zu finden ist: „This machine has no brain – please use your own."
Denken Sie nach, seien Sie skeptisch, informieren Sie sich. Die Informationstechnologie steckt voller wundervoller Möglichkeiten, die die Gesellschaft auf bis jetzt noch unabsehbare Weise verändern wird – aber sie ist extrem komplex. Die Einfachheit, mit der uns die Werbeindustrie komplexe Dinge verkaufen möchte, kann prinzipbedingt so nicht existieren.
Denken Sie einfach ab und an nach – und erfreuen Sie sich an den neuen Möglichkeiten!

Dipl.-Ing. Peter Leppelt,
Geschäftsführer.

Dennis Weber,
Softwareentwickler.

praemandatum
Goseriede 4 / Tiedthof, 30159 Hannover
http://www.praemandatum.de

Links

- http://www.praemandantum.de
  Beratung in Sachen Datenschutz, Jugendschutz, PC-Sicherheit u. Ä. für Schulen, Eltern, Privatpersonen und Unternehmen
- http://www.opensuse.org/de
  auf Linux basierendes Betriebssystem OpenSuSE
- http://www.ubuntu.com
  Betriebssystem Ubuntu
- http://fedoraproject.org/de/
  Betriebssystem Fedora
- http://www.mozilla.com/de
  Mozilla Firefox
- http://www.opera.com
  Browser Opera
- http://www.mozilla.com/de
  Mozilla Thunderbird
- http://www.pmail.com/downloads_s3_t.htm
  E-Mail-Programm Pegasus Mail

Praxisbeispiel: KURZVORSTELLUNG

Kursangebote zum Thema Sicherheit

Link: *http://www.praemandatum.de/schulen*

1. UNTERRICHT/SCHULE ▸ **Fächer:** Medienbildung, Gesellschaftskunde ▸ **Klassenstufen:** verschiedene Seminare für Klassenstufe 5–6 („Neue Medien – aber sicher!") und 9–13 („Es sind MEINE DATEN!") ▸ **Schulform:** alle	**3. SCHWERPUNKTE** ▸ **Themen:** Privatsphäre und Sicherheit bei der Nutzung digitaler Medien ▸ **angestrebte Elemente von Medienkompetenz:** u. a. sicherer Umgang mit verschiedenen Diensten des Internets, informationelle Selbstbestimmung
2. RAHMENBEDINGUNGEN ▸ **Zeitumfang:** 2–3 Schulstunden ▸ **technische Ausstattung:** ggf. Beamer und Lautsprecher (kann von den Referenten mitgebracht werden) ▸ **Kosten:** 85 € pro Stunde und Referent	**4. MATERIAL** ▸ Begleit- und Nachschlagmaterial wird zur Verfügung gestellt.

praemandantum bietet u. a. Seminare für jüngere Schülerinnen und Schüler (oder deren Eltern) zu Themen wie:
- Privatsphäre in Zeiten von SchülerVZ, Facebook & Co
- Recht am eigenen Bild
- Umgang mit Bewertungsportalen wie SpickMich
- Richtiges und sicheres Verhalten in Chats und Foren
- Richtiger Umgang mit sogenannten „Killerspielen".

Für ältere Jugendliche gibt es Seminare zu den Themen Datenschutz und Privatsphäre. Hierbei geht es z. B. um:
- Privatsphäre im Informationszeitalter – und: warum?
- Bringt mehr Überwachung mehr Sicherheit?
- Wer hat Interesse an den persönlichen Daten?
- Was wird mit den Daten gemacht?
- Wie behalte ich meine Daten bei mir, wenn ich es will?
- Allmacht und Wissensmonopole digitaler Suchmaschinen.

Angeboten werden darüber hinaus Weiterbildungsseminare für Lehrkräfte (Zeitumfang: 2–6 Stunden).

Praxisbeispiel: KURZVORSTELLUNG

Viren, Würmer, Trojaner als Unterrichtsthema

Link: *http://www.lehrer-online.de/viren-wuermer-trojaner.php*
Autoren: Jürgen Schmitz und Lutz Krone

1. UNTERRICHT/SCHULE ▸ **Fächer:** Informatik, Medienbildung, Politik, Sozialwissenschaften oder fächerübergreifend ▸ **Klassenstufe:** ab 8 ▸ **Schulform:** alle	**3. SCHWERPUNKTE** ▸ **Thema:** Schadsoftware ▸ **angestrebte Elemente von Medienkompetenz:** Sensibilisierung für das Gefahrenpotenzial von Schadsoftware; Schutzmaßnahmen kennen- und anwenden lernen
2. RAHMENBEDINGUNGEN ▸ **Zeitumfang:** 3 – 6 Unterrichtsstunden ▸ **benötigte technische Ausstattung:** Computer zur Internetrecherche; abgesicherte Übungsumgebung mit der Möglichkeit zur Simulation (z. B. Einzelplatzrechner mit Virenscanner und Übungsviren)	**4. MATERIAL** ▸ Unterrichtsvorschlag ▸ Arbeitsmaterialien ▸ weiterführende Links

Mithilfe von Arbeitsblättern und Internetressourcen erschließen sich die Schülerinnen und Schüler im Rahmen dieser – allerdings bereits aus dem Jahre 2005 (!) stammenden Unterrichtseinheit – Grundlagenwissen zu Viren, Würmern und Trojanern und lernen Handlungsmöglichkeiten zum Schutz dagegen kennen. Neben den Arbeitsmaterialien hilft auch ein möglicher Ablaufplan für eine Unterrichtsreihe bei der Umsetzung des Themas.

Quelle: lehrer-online.de

Praxisbeispiel: KURZVORSTELLUNG

Sicherheit im Internet

Link: *https://www.bsi-fuer-buerger.de*
Autor: Bundesamt für Sicherheit in der Informationstechnik

1. UNTERRICHT/SCHULE ▸ **Fächer:** Informatik ▸ **Klassenstufe:** ab Sek. I ▸ **Schulform:** alle	**3. SCHWERPUNKTE** ▸ **Thema:** Sicherheit im Internet ▸ **angestrebte Elemente von Medienkompetenz:** Sicherheitsrisiken im Internet und Sicherheitsmaßnahmen kennenlernen
2. RAHMENBEDINGUNGEN ▸ **Zeitumfang:** variabel ▸ **benötigte technische Ausstattung:** PC mit Internetanschluss	**4. MATERIAL** ▸ aktuelle Informationen zu diversen sicherheitsrelevanten Themen

Die Informationen und Materialien des Bundesamtes für Sicherheit in der Informationstechnik wenden sich zwar nicht direkt an Lehrkräfte bzw. Schulen, bieten jedoch für Laien einen guten Einstieg in die Thematik und lassen sich auch im Unterricht einsetzen. Hier findet man auch Informationen zur Sicherheit von Handys bzw. Smartphones.