

Abteilung Gymnasium

Arbeitskreis Link-Ebene Wirtschaftsinformatik

Schellingstr. 155 · 80797 München · Tel.: 089 2170-2153 · Fax: -2125

E-Mail: tobias.tyll@isb.bayern.de

**WIn 10.3: Hintergrundinformation zu Schadprogrammen und weiteren Gefahren im Internet**

Hinweis: Diese **Lehrerinformation** umfasst folgende Bereiche:

* typische Funktionsweisen wichtiger Schadprogramme (Diese werden verkürzt beschrieben, nicht aber alle auftretenden Varianten, um die Übersichtlichkeit zu wahren)
* weitere Gefahren im Umgang mit dem Internet
* Verbreitungswege der Schadprogramme
* wichtige Sicherungsmaßnahmen

Hinweis auf Material für die Umsetzung im Unterricht:

* 10\_3 5 Arbeitsblatt zum Film des BSI.docx
* Botnet.wmv
* Botnet.mpg

**1 Wichtige Arten von Schadprogrammen („Malware“)**

* **Virus**: Seine Funktionsweise lässt sich mit der eines Grippevirus vergleichen:

Anstelle bestimmter Körperzellen infiziert er bestimmte Programme, indem er z. B. seinen Code an die exe-Datei des Programms (= „Wirtsdatei“ in Anspielung an die „Wirtszelle“ beim Grippevirus) anhängt und immer dann mit ausgeführt wird, wenn das befallene Programm gestartet wird. Ähnlich wie beim Grippevirus lassen sich drei Funktionen des Computervirus unterscheiden:

* + **Erkennung**: Zunächst stellt der Virus fest, ob die Datei bereits von ihm befallen ist, um nicht unnötig Zeit mit einer Mehrfachinfektion zu vertun. Um sich selbst zu erkennen, hinterlässt der Virus in der infizierten Datei oftmals eine sog. „Signatur“. Damit erleichtert er aber seine Erkennung durch Antivirensoftware.
  + **Reproduktion / Weiterverbreitung**: Befall weiterer Programme auf dem Rechner
  + **Schädigung**: sehr unterschiedlich (von harmlos wie die Ausgabe von Textmeldungen über ihre Existenz bis hin zu gravierenden Folgen wie gelöschte Dateien)

Die Bedeutung der Viren hat aber abgenommen, da Würmer über eine „bessere“ Verbreitungsstrategie verfügen.

* **Wurm**: Im Gegensatz zum Virus handelt es sich beim Wurm um ein **eigenständiges** Programm, das kein Wirtsprogramm benötigt. Er verbreitet sich selbständig, also ohne weiteres Zutun des Benutzers, etwa indem er sich an alle Adressen aus dem Adressbuch des Betroffenen versendet. Da die Empfänger dieser verseuchten E-Mails den Absender kennen, sind sie häufig bereit, dabei mitgeschickte Dateianhänge oder Links, hinter denen sich der Wurm verbirgt, zu öffnen, so dass auch ihr Rechner infiziert wird. In gleicher Weise können auch die Kontakte von Chatprogrammen bzw. von sozialen Netzwerken (wie z. B. Facebook) mit einem Wurm „beglückt“ werden – und zwar ohne dass der Versender dies bemerkt: So öffnet sich z. B. in Facebook plötzlich das Chatfenster mit einer Mitteilung eines Freundes, durch Klick auf den beigefügten Link könne man ein lustiges Bild oder Ähnliches sehen – und dies nur deshalb, weil dieser Freund so unvorsichtig war, selbst auf einen solchen Link zu klicken und sich so diesen Wurm einzufangen.

Für aktuelle Fälle in einer Suchmaschine die Stichwörter „Facebook“ und „Wurm“ eingeben!

Neben ihrer speziellen schädigenden Wirkung verursachen Würmer v. a. durch ihre rasante Verbreitung gravierende Schäden, da Postfächer und Mailserver überlastet werden. Ein Zahlenbeispiel: Nimmt man an, dass ein typischer Nutzer, vorsichtig geschätzt, rund 200 Kontakte hat und etwa die Hälfte der Empfänger durch ihr Verhalten für die Weiterverbreitung sorgt, so ergibt sich:

Runde neu infiziert neu versandte Mails / Nachrichten

1 1 200

2 100 20.000

3 10.000 2.000.000

4 1.000.000 200.000.000

5 100.000.000 20.000.000.000 usw.

* **Trojanisches Pferd / Trojaner[[1]](#footnote-1):** Der Begriff leitet sich aus der griechischen Mythologie ab und spielt auf die bekannte Eroberung Trojas durch eine List der Griechen an: **Ein scheinbar nützliches Programm** (z. B. eine von einer Tauschbörse illegal heruntergeladene Installationsdatei eines eigentlich kostenpflichten Programms oder ein Seriennummerngenerator, um ein solches kommerzielles Programm „kostenlos“ nutzen zu können) **hat ein schädliches Programm** „**im Bauch**“, das unbemerkt vom Benutzer als eigener Prozess abläuft (auch dann, wenn das Tarnprogramm beendet oder gar gelöscht wurde). Dieses Schadprogramm ist häufig **Spionagesoftware**, die z. B. durch Mitprotokollierung von Tastatureingaben („**Key Logger**“) Benutzernamen, Passwörter oder andere persönliche Daten abfängt und an den Angreifer weiterleitet. Außerdem kann es aber auch eine „Hintertür“ (sog. „**Backdoor**“) auf dem betroffenen System öffnen, die dazu dient, weitere Schadsoftware einzuschleusen.

Im Gegensatz zu Virus und Wurm fehlt dem Trojanischen Pferd jedoch die Möglichkeit zur eigenständigen Reproduktion, weshalb oftmals ein Wurm zur Verbreitung des Trojaners genutzt wird.

Eines der bekanntesten trojanischen Pferde ist der sog. „**Staatstrojaner**“, mit dem der Staat auf die Computer von Privatpersonen bei Verdacht auf Straftaten zugreifen kann, um an für die Strafverfolgung als wichtig erachtete Daten zu gelangen.

* **Spyware:** Damit erstellen Softwareproduzenten ohne Wissen des Anwenders ein Benutzerprofil (aufgerufene Internetseiten, Verweildauer auf diesen Seiten, eingegebene Stichwörter in Suchmaschinen, eingesetzte Software auf dessen Computer) und senden dieses, zusammen mit weiteren persönlichen Daten, wie sie z. B. bei der Registrierung der Software erhoben wurden, an den Hersteller oder an Werbefirmen. Die so erhaltenen Informationen werden für zielgerichtete Werbung genutzt, etwa per Mail, Pop-Ups, eine geänderte Startseite des Browsers oder durch Hinzufügen von Internetseiten zum Favoritenordner.

Im Unterschied zu Trojanern weisen die Hersteller auf die Erfassung der persönlichen Daten hin – meist aber schwer versteckt in den seitenlangen Lizenzbedingungen. Fehlt diese Information ganz, kann man wiederum von einem Trojaner sprechen.

Zum Teil dient der Begriff „Spyware“ aber auch als Oberbegriff für jegliche „Spionagesoftware“, also für die hier beschriebene Spyware (im engeren Sinn) und für die zuvor beschriebenen Trojaner.

* **Bot** (von engl. „robot“ = Roboter, Arbeitsknecht):

Programm, mit dem ein Angreifer den PC unbemerkt fernsteuern kann, sobald dieser online ist. Sind mehrere Tausende PCs zu einem **Botnetz** zusammengeschlossen, so kann der „Dirigent“ dieses Netzes sie für

* + den **Spamversand** nutzen (s. u.) oder
  + eine **gemeinsame DoS-Attacke** („Denial of Service“-Attacke) (kurz: DdoS = Distributed DoS) **auf einen Unternehmensrechner** starten. Dabei werden massenhaft Anfragen an den Firmenserver gestellt, so dass dieser schließlich nicht mehr für die Kunden erreichbar ist.

Häufig werden die Botnetze vom ursprünglichen Angreifer auch weitervermietet, damit andere Kriminelle sie für ihre Zwecke (s. o.) ausnutzen können.

Aufgrund der weiten Verbreitung von Breitbandanschlüssen bemerkt der betroffene Nutzer die geringfügige Beeinträchtigung der Verbindungsgeschwindigkeit nicht einmal und ist ständig für neue Kommandos „erreichbar“.

**2 Weitere Gefahren:**

* **Phishing** = „password fishing“ = „nach Passwörtern angeln“: Getarnt als seriöses Unternehmen fordern die Betrüger den Empfänger der E-Mail auf, seine Daten einzugeben, weil z. B. das Sicherheitssystem der Bank verbessert werden soll oder die Kreditkarte ablaufe. Hierzu dient ein Link, der den Benutzer aber nicht auf die tatsächliche Startseite seiner Bank, seines Kreditkartenunternehmens etc. leitet, sondern auf eine täuschend echt aussehende Nachbildung (mit fast identischer Internetadresse). Gibt nur einer von einer Million der massenhaft angeschriebenen Computernutzer dort seine Daten preis, hat sich das Phishing schon gelohnt.

Im Rahmen der ökonomischen Verbraucherbildung bietet es sich an, auch folgende beiden Gefahren zu thematisieren:

* **Hoax** = „schlechter Scherz“: Falschmeldung, die per E-Mail verbreitet wird, verbunden mit der Aufforderung, die Mail allen Freunden zukommen zu lassen, damit auch diese informiert werden über
  + die dringende Suche eines Knochenmarkspenders für erfundene Personen,
  + die Möglichkeit, schnell an Geld zu gelangen (z. B.: „Bill Gates verschenkt sein Vermögen. Für jede Person, an die du diese Mail weiterleitest, spendet er dir … US-Dollar“),
  + skandalöse Zustände beim Unternehmen XY oder
  + die akute Bedrohung durch bestimmte Schadprogramme.

Durch die rasante Verbreitung eines solchen Hoaxes (vgl. Zahlenbeispiel zu Würmern) entstehen unnötiger Datenverkehr im Internet und Zeitaufwand für Millionen Menschen.

* **Spam** = „**S**piced **P**orc and H**am**“ = „Frühstücksfleisch“: Bezeichnet den massenhaften Versand unerwünschter E-Mails. Wie aus dem Frühstücksfleisch ein Synonym für Massen-E-Mails wurde, ist nicht eindeutig belegt.

Dieser dient zu **Werbezwecken** für wertlose oder illegale Produkte (z. B. gefälschte Potenzmittel, Uhren oder illegale Glücksspiele) oder um einen sog. „**Vorschussbetrug**“ zu ermöglichen. Dabei wird dem Empfänger z. B. vorgegaukelt,

* + ein entfernter Verwandter sei gestorben und man habe eine große Erbschaft zu erwarten,
  + man solle bei einer größeren Überweisung aus dem Ausland helfen und dafür sein Konto zur Verfügung stellen, um dafür eine hohe Provision zu kassieren, oder
  + eine (tatsächliche!) Chatbekanntschaft sei im Ausland in Schwierigkeiten geraten und werde sich später revanchieren.

In allen Fällen ist dazu aber erst einmal ein Vorschuss des Empfängers einer solchen Mail nötig (etwa für Anwaltsgebühren). Die versprochene Gegenleistung wird aber nie erbracht.

Um seriöser zu wirken, werden die Empfänger mittlerweile meist sogar persönlich angesprochen und bis zur Nennung der Notwendigkeit eines Vorschusses mehrere E-Mails hin- und hergeschickt.

Die nötigen Adressen erhalten die „Spammer“ einerseits bei professionellen Adresshändlern, die hierzu Homepages, Foren u. Ä. durchkämmen, andererseits aber auch durch schlichtes Ausprobieren. Indem der Nutzer auf die Mail antwortet, bestätigt er die Gültigkeit seiner E-Mail-Adresse und wird daher in Zukunft eher noch häufiger „belästigt“.

Wie beim Phishing gilt: Es reicht, wenn nur ein verschwindend geringer Prozentsatz auf eine bestimmte Masche hereinfällt!

**3 Typische Verbreitungswege:**

* **Drive-by-Infektion** = Schadprogramm nutzt Schwachstellen im Browser aus, um ohne weitere Nutzeraktion schädliche Programme auf dem PC zu installieren
* **E-Mail-Anhänge**
  + von Freunden
  + angebliche Rechnungen von bekannten Unternehmen mit dem Hinweis „nähere Details im Anhang“ (der z. B. den Anschein erweckt, eine normale pdf-Datei zu sein)
  + Warnungen vor auf dem Rechner des Nutzers entdeckter Malware mit beigefügtem Link zum Herunterladen des angeblichen Antivirenprogramms
* **Links** **in E-Mails oder** Facebook- / ICQ –**Chatnachrichten**
* **USB-Sticks** (typischer Trick zur Industriespionage: verseuchten USB-Stick auf Firmenparkplatz legen → ein Mitarbeiter hebt ihn auf, steckt ihn in seinen PC und schon kann die Schadsoftware ihr Unwesen treiben und Daten an die Konkurrenz versenden)
* **Ausnutzen bekannter Sicherheitslücken** von Standardsoftware, die solange ausgenutzt werden können, bis der Hersteller ein Update (oder einen „Patch“) zur Verfügung stellt und der Benutzer dieses auch installiert (!), was häufig unterlassen wird.

**4 Schutzprogramme / -maßnahmen:**

* **Virenschutzprogramme**: Diese überprüfen neue Dateien (z. B. E-Mail-Anhänge, heruntergeladene Dateien), aber auch fortlaufend im Hintergrund die schon auf dem eigenen Computer befindlichen Dateien auf „Fingerabdrücke“ (Signaturen: s. o. bei Virus) bekannter Viren. Dazu ist es aber unbedingt erforderlich, stets (also am besten täglich) die neuesten Signaturen über die Update-Funktion des Anti-Viren-Programms herunterzuladen (hierzu empfiehlt es sich, automatische Updates einzustellen), da sich sonst neuartige Viren, die das Virenschutzprogramm noch nicht kennt, einnisten können. Zwar enthalten moderne Programme Mechanismen, um auch unbekannte Viren evtl. aufspüren zu können, doch diese funktionieren naturgemäß nur in manchen Fällen.
* **(Personal) Firewall („Brandschutzmauer“)**: Eine Software, die den Netzwerkverkehr überwacht und entscheidet, welche Datenpakete hinein bzw. hinaus dürfen. Dies dient dem Schutz vor unerlaubten Zugriffen, etwa durch Spyware. Versucht nun ein Programm von außen auf das eigene Netzwerk zuzugreifen oder umgekehrt Daten über das Internet zu versenden, fragt die Firewall den Benutzer, ob dieser Datenaustausch erwünscht ist (wie dies z. B. beim E-Mail-Programm oder dem Browser der Fall wäre). Somit kann der Benutzer durch vorsichtige Freigaben („Wer / Was darf rein und raus?“ → vgl. Klingel an der Haustür) sein Netzwerk schützen. Dazu gehört es auch, bei der Freigabe von Ports (s. u.) für bestimmte Anwendungen zurückhaltend zu sein.

Hinweis: Bei den meisten Routern ist bereits eine externe Firewall eingebaut, die zumindest ungebetene Zugriffe von außen verhindert, aber noch nicht den unerlaubten Datenversand nach außen (etwa durch einen Trojaner, den man sich über einen verseuchten USB-Stick „eingefangen“ hat); hierzu ist die beschriebene Softwarelösung nötig.

Port („Durchlass“ / „Tor“): vergleichbar mit dem Postfach oder der Zimmernummer einer Abteilung in einem Unternehmen – im Vergleich zur Briefadresse = IP-Adresse.

Möchte man gleichzeitig mehrere Verbindungen zum Internet (zum Surfen, E-Mail-Versenden, Telefonieren usw.) aufbauen, müssen diese einzelnen Verbindungen identifizierbar sein, damit die Weitergabe der Datenpakete reibungslos verläuft (und nicht etwa Datenpakete, die für den Browser bestimmt waren, im E-Mail-Programm landen o. Ä.). Hierzu wird für jede Verbindung eine zusätzliche Nummer aus dem Bereich von 0 bis 65535 (also 216 Nummern) gewählt, die sogenannte Port-Nummer. Für diverse Dienste gibt es international festgelegte Nummern von 0 bis 1023, so dass man sich um diese Ports nicht kümmern muss, z. B.

* + 80: Browser
  + 25 und 110 / 143: E-Mail-Versand bzw. –Empfang
* **Updates / Patches**: Schadprogramme versuchen, Sicherheitslücken (im Betriebssystem oder anderen weit verbreiteten Anwendungen) auszunutzen, um Zugang zum heimischen Computer zu erlangen. Werden neue Sicherheitslücken entdeckt, versuchen die Hersteller dieser Programme, diese schnellstmöglich durch einen Patch („Flicken“) zu schließen. Hierzu muss der Benutzer aber diese Aktualisierungen auch zuverlässig installieren. Zwar kann man diese Aufgabe oftmals „automatisieren“, indem man – wie schon beim Virenschutzprogramm – die Einstellung „automatische Updates“ wählt, jedoch bietet nicht jede Software diese Möglichkeit. Dann bleibt einem nichts anderes übrig, als selbst von Zeit zu Zeit nach Updates für diese Programme zu suchen oder sich in den Hersteller-Newsletter einzutragen.

Achtung: Hinter einer Warnung vor Sicherheitslücken und der dringenden Empfehlung, das entsprechende Update zu installieren, kann sich auch ein Link auf ein Schadprogramm verbergen!

* **Sicherheitseinstellungen im Browser**: Aufgrund der umfangreichen Einstellungsmöglichkeiten, die stets ein Abwägen zwischen Sicherheit und Komfort sind (je strenger man die Sicherheitseinstellungen wählt, umso weniger multimediale Inhalte kann man sich anzeigen lassen), sei auf die detaillierte Anleitung unter

[https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/ SicherheitsCheck/sicherheitscheck\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/WegInsInternet/DerBrowser/%20SicherheitsCheck/sicherheitscheck_node.html)

verwiesen.

1. Streng genommen ist nur der Begriff „Trojanisches Pferd“ korrekt, da die Trojaner (Einwohner der Stadt Troja) ja die Opfer und nicht die Täter waren. Die umgangssprachliche und im EDV-Jargon gebräuchliche Abkürzung „Trojaner“ kehrt die Bedeutung eigentlich um. Da der Begriff aber auch von öffentlicher Seite (z. B. BSI, Medien) verwendet wird, wird auch im Folgenden von Trojanern gesprochen. [↑](#footnote-ref-1)