Risiken bei der Nutzung digitaler Kommunikationsformen

Fehlinformation

- Bearbeite das Arbeitsblatt 13, Seite 1 und 2: Wahrheitsgehalt von Informationen im Internet

Damals im Wilden Westen war nicht klar, ob eine Information versehentlich oder absichtlich manipuliert wurde. Die Kommunikation im Internet ist ungleich komplexer. Bei Abermillionen von Internetauftritten treten neben Fakes auch bewusste oder unbewusste Manipulations- und Betrugsversuche auf.
Jeder, der sich im Straßenverkehr bewegt, hält die Augen nach Gefährdungen offen. Wenn man sich auf der „Datenautobahn" im weltweiten Netz bewegt, sollte man sich über Risiken genauso im Klaren sein.

Zunächst sollte man die Glaubwürdigkeit und den Wahrheitsgehalt von Informationen prüfen:

- Ein *Hoax* (engl. für Jux, Scherz, Schabernack; auch Schwindel) ist eine Falschmeldung, die im Internet verbreitet werden kann. Viele Menschen halten diese Fehlinformationen für wahr und leiten sie an Freunde weiter.
- Ebenso *Verschwörungstheorien*, bei denen auf Grund einer vereinfachenden Sichtweise Sachverhalte zusammenphantasiert werden, die so nicht existieren.

Ursachen der scheinbaren Glaubwürdigkeit des Internets

- Bearbeite das Arbeitsblatt 13, Seite 3

Natürlich ist der Großteil der Informationen, die im Internet veröffentlicht werden, korrekt. Warum fällt uns die Unterscheidung zwischen wahren Informationen und erfundenen oder verfälschten oft schwer?

- Die meisten Menschen bevorzugen die Informationsaufnahme über das Auge. Die grafisch gestaltete Erscheinungsform des WWW fördert die *Illusion von Zuverlässigkeit und Echtheit*.
- Im WWW lassen sich beliebige Inhalte unabhängig von ihrem Wahrheitsgehalt zu einem komplexen Netz aus Querverweisen miteinander verbinden. Dies erweckt den *Anschein gut belegter Wahrheit*.
- Das Internet ist aufgrund seiner Anonymität eine ideale Brutstätte für die ungeregelte Verbreitung von Klatsch und Gerüchten (Urban Legends), Verleumdungen, Lügen und Verschwörungstheorien.

  - Im Internet besteht die Gefahr einer **Vermischung von Realität und Fiktion**.

Kriterien für die Beurteilung des Wahrheitsgehalts

Dadurch, dass jeder im Netz veröffentlichen kann, müssen Möglichkeiten gesucht werden, Informationen zu überprüfen. Um den Wahrheitsgehalt von elektronischen Publikationen besser beurteilen zu können, solltest du dir folgende Fragen stellen:

- Wer ist der **Verfasser**?
  Hast du von dem Verfasser schon einmal gehört? Ist er Experte? Welchen Ruf genießt er?
  Informationen, die *anonym* verbreitet werden, sollten dich misstrauisch machen.
- Wer ist der verantwortliche **Herausgeber**?
  Handelt es sich um eine anerkannte Organisation oder um eine persönliche Homepage?
  Gibt es einen Auftritt auch außerhalb des Internets, wie etwa bei der Süddeutschen Zeitung oder dem Bayerischen Rundfunk?

- Bemüht sich der Autor um eine **Trennung von Information und Wertung**?
- Handelt es sich um **Werbung**? Dann darfst du keine objektive Information erwarten.
- Sind die Behauptungen im Dokument durch andere, vom Verfasser **unabhängige Quellen** belegbar?
- Wie **aktuell** ist die Information?

- Bearbeite das Arbeitsblatt 13, Seite 4

Spionage und Sabotage

Beim Abrufen von Informationen im Internet sollte man sich also nicht täuschen lassen, sondern auf die *Echtheit* achten. Das wird als **Authentizität** bezeichnet.

A Bearbeite das Arbeitsblatt 14: Phishing

- Eine E-Mail, die unverlangt zugestellt wird und werbenden Inhalt enthält, nennt man **Spam**.
  Der Begriff SPAM stammt von einer Marke für Dosenfleisch. Er setzt sich aus **Sp**iced h**am** zusammen und wurde populär, weil er in einer englischen Comedyserie für einen Sketch verwendet wurde.
- **Phishing** (von engl. „fishing“ für „Angeln“) bedeutet, einem Internetnutzer mit Hilfe einer gefälschten Webseite vertrauliche Daten zu entlocken. Als „Köder“ dienen häufig E-Mails oder Kurznachrichten. Das Phishing ist eine Methode des **Social Engineering** (soziale Manipulation), um Nutzer zu einer Handlung zu beeinflussen. Mit den Daten kann ein Betrüger auf Kosten des Opfers Geld erbeuten.
- Klären der Authentizität einer E-Mail:
  - Abgleich der Absenderadresse mit dem E-Mail-Text.
  - Überprüfen der Grammatik und Rechtschreibung.
  - Klären der Notwendigkeit einer persönlichen Anrede.
  - Internetrecherche mit Hilfe einer Suchmaschine nach einer prägnanten Formulierung, evtl. ergänzt um den Suchbegriff „spam“. Begriffe in Grafiken sind nutzlos.
  - Suche nach Hinweisen auf Spam in dem Internetauftritt des angeblichen Anbieters. Verwende **nicht** den Link in der E-Mail, sondern öffne einen neuen Tab oder ein neues Fenster.

Schadsoftware

A Bearbeite das Arbeitsblatt 15, S. 1: E-Mails mit Dateianhängen

ZIP ist ein wichtiges Dateiformat: In ZIP-Dateien werden Daten ohne Informationsverlust komprimiert, was zu kleineren Dateien führt. Außerdem können mehrere Dateien in einer Datei zusammengefasst werden.

- In solchen Dateianhängen können aber auch Schadprogramme enthalten sein.
  Weitere Dateiformate, die misstrauisch machen sollten, sind z. B. .com, .pif, .ico, .scr oder .exe.
  Solche Dateianhänge sollte man nur öffnen, wenn man sich sicher ist, dass man eine solche Sendung erwartet und sie eindeutig von dem korrekten Absender stammt.

Schadprogramme werden direkt zur *Sabotage* oder indirekt zu *Spionage*zwecken verwendet. Sie werden auch als *Malware* bezeichnet. Man unterscheidet zwischen:

- **Computerviren**, die aktiv Schaden verursachen, z. B. Dateien verändern oder löschen. Viren pflanzen sich fort, indem sie sich selbst in vorhandene Dateien schreiben. Solange sie nicht aktiv sind, bleiben sie oft unbemerkt und werden über Wechseldatenträger oder Dateianhänge von E-Mails verbreitet.
- Im Gegensatz dazu üben **Computerwürmer** nicht unbedingt eine direkte Sabotage aus. Vielmehr ergibt sich schon dadurch eine Schadfunktion, dass sie sich über Netzwerke fortpflanzen, denn das kann für erheblichen Datenverkehr sorgen. Dafür benötigen sie keine Datei als Wirt, sondern nutzen das System des infizierten Computers. Würmer können aber oft weitere Funktionen ausführen, z. B. die E-Mail-Adressen im System auslesen und diese sowie sich selbst an alle Adressen senden.

  So kannst du ganz offizell eine E-Mail von einem guten Freund erhalten, die authentisch zu sein scheint. Sobald du den Dateianhang öffnest, wird das Schadprogramm aktiv.

  Der Wurm kann dann eventuell auch weitere Sabotage- oder Spionagefunktionen ausführen.
- Der Begriff **Trojaner** stammt von dem Trojanischen Pferd ab, mit dessen Hilfe der Trojanische Krieg in Homers Epos *Ilias* beendet wurde. Trojaner verbreiten sich, indem sie aktiv ausgeführt werden. Dazu täuschen sie eine sinnvolle Anwendung vor, enthalten aber zusätzliche Funktionen, mit denen sie Schaden verursachen. Das kann z. B. der Diebstahl von Zugangsdaten zum Online-Banking sein oder dem Hacker die Möglichkeit eröffnen, beliebig auf den Rechner zugreifen zu können.

A Bearbeite das Arbeitsblatt 15, S. 2: Schadsoftware

- Hinweis: Sofern verfügbar, ist hier die Dokumentation „*Tatwaffe Computer*“ aus der Reihe „*Dem Verbrechen auf der Spur*“ empfehlenswert. (Ein Film von Nick Kenton; BBC 2010; Eine Sendung von ZDF Info 2013; Spieldauer 43:22 Minuten; https://www.youtube.com/watch?v=box90MsmLFA); Stand: September 2016)

Ein paar Beispiele zu Schadfunktionen kennst du schon. Zusammengefasst und ergänzt beinhaltet das:

- **Sabotage** soll direkten Schaden verursachen, z. B.:
  - Veränderung oder Löschen von Dateien.
  - Den Zugriff auf Daten verhindern, um Lösegeld erpressen zu können.
  - Netzwerke durch hohen Datenverkehr blockieren.
- **Spionage** dient der Vorbereitung von weiteren Aktionen, mit denen Schaden verursacht wird, z. B.:
  - Diebstahl bzw. Erschleichen von Zugangsdaten, z. B. zum Online-Banking oder E-Mail-Account.
  - Ausspähen personenbezogener Daten, z. B. um E-Mails zum Phishing oder zum Einschleusen von Schadprogrammen zu erstellen.
  - Das Erbeuten von Firmengeheimnissen.
- Erstellen von Programmen zur Vorbereitung von Straftaten, z. B.:
  - Einem **Hacker** die Möglichkeit eröffnen, beliebig auf den eigenen Rechner zugreifen zu können und dann Spionage oder Sabotage zu betreiben.

A Bearbeite das Arbeitsblatt 15, S. 3 – 4: Authentisch oder nicht authentisch?

Einfallstore

A Bearbeite das Arbeitsblatt 16: Weitere Risiken im Zusammenhang mit weltweiten Netzwerken

Oft genutzte Wege, die Kriminellen die Möglichkeit eröffnen, sich zu bereichern bzw. ihren Mitmenschen Schaden zuzufügen, sind:

- Links und Dateianhänge, die unbedarfte Benutzer in E-Mails öffnen.
- Schadsoftware, die über **Programme** eingeschleust wird, welche der Computernutzer installiert.
- Direkte **Angriffe auf Computer**.
- Infizierte Webseiten, die Sicherheitslücken des Browsers ausnutzen (**Drive-by-Download**).
- Nutzung von Filesharing-Netzwerken.

Weitere Risiken

Es gibt nicht nur direkte Risiken durch Software, welche auf dem Rechner installiert wird.
Zusammengefasst sind bedeutende weitere Risiken:

- Unseriöse Angebote und Betrug
  - *Untergeschobene Vertragsabschlüsse* („Abofallen“), z. B. bei Online-Routenplanern.
  - *Betrug bei Einkäufen mit Vorkasse* („Eingehungsbetrug“).
  - *Gefälschte Angebote* z. B. zur Vermietung einer Wohnung oder auch zum Verkauf eines Autos.
- Gefährliche Produkte
  - Die *weltweite Vernetzung* macht es möglich, dass Waren ausgeliefert werden, die europäischen Sicherheitsstandards nicht entsprechen.
    Das betrifft z. B. gefährliche Elektroartikel oder gesundheitsgefährdende Materialien.
- Veröffentlichung von Informationen
  - Ein Aufruf „an alle“ in sozialen Netzwerken kann Probleme nach sich ziehen.
  - Vergehen gegen das **Urheberrecht** (genauere Klärung im Modul 1.7).
- Belästigung
  - Cybermobbing: Fortgesetztes Ausgrenzen, Beleidigen, Bedrohen, Bloßstellen oder Belästigen anderer mit modernen Kommunikationsmitteln.
  - Persönlichkeitsrecht: Werden persönliche Daten, Fotos oder ähnliches ohne Zustimmung des Betroffenen veröffentlicht, verstößt man damit gegen das **Persönlichkeitsrecht**.

A Bearbeite das Arbeitsblatt 17, S. 1: Risiken bei der Nutzung digitaler Kommunikationsformen

Maßnahmen

Die **Prüfung der Authentizität** wurde hier am Beispiel der E-Mail ausführlich besprochen. Das gilt für das Internet grundsätzlich. Du gibst auch nicht jedem Fremden auf der Straße deine Anschrift. Natürlich kannst du nicht für jede Webseite den Rechercheaufwand betreiben, um zu hinterfragen, was angeboten wird. Aber bevor du auf einen Link klickst oder gar einen Download startest, gilt:

- **Erst Hinschauen** und prüfen, **dann** erst **klicken**.
  Es gibt Schadprogramme, die sich durch Angriffe selbsttätig auf fremden Systemen einrichten. Auch gibt es Schadprogramme, die Einstellungen in deinem Computer so verändern, dass du auf gefälschten Websites landest, ohne es überhaupt bemerken zu können.
  Das Risiko ist auf beliebigen Websites natürlich geringer als bei gezielt gesendeten E-Mails, aber:
- **Du bestimmst das Risiko**.
  Wenn sich Inhalte am Rande oder jenseits der Legalität bewegen, steigt das Risiko. So ist z. B. auf der Website eines Filesharing-Netzwerks das Risiko größer als bei einem E-Mail-Provider, dessen Daten auf Servern in Deutschland gespeichert werden. Genau wie das Risiko, von einem Auto angefahren zu werden, auch größer wäre, würdest du bei Rot eine Straße überqueren.
- Wer ohne Virenscanner und Firewall im Internet unterwegs ist, hat sich nach wenigen Minuten einen Computerwurm eingefangen.

Beachte also die folgenden Maßnahmen zur **Verringerung der Risiken**.

- Nutze das Internet nur mit aktivierter **Firewall** und aktuellem **Antivirenprogramm**.
- Achte auf **regelmäßige Updates** der Software – insbesondere des Virenscanners und des Browsers. Aktiviere auch die automatische Aktualisierung, wenn dies möglich ist.
- Für die Nutzung des Computers sollte eine **Benutzerkennung mit eingeschränkten Rechten** angelegt werden. Administratorrechte sind nur für manche Installationaufgaben erforderlich.
- Nutze **Passwörter** nicht für mehrere Portale bzw. Dienste. Achte auf die Vergabe sicherer Passwörter und regelmäßiges Anfertigen von **Sicherungskopien** (Details dazu im Modul 1.8).
- Prüfe die **Glaubwürdigkeit** und **Authentizität** von Inhalten.
  - **Fragwürdige Dateianhänge sollte man auf keinen Fall öffnen.** Es ist gut möglich, dass darin Programme enthalten sind, die schädliche Funktionen ausführen.
  - Bei extrem günstigen oder kostenlosen Angeboten die Produktdaten bzw. Geschäftsbedingungen genau lesen und bei unabhängigen Quellen gegenprüfen. Es könnte sich z. B. um ein gefährliches Produkt oder um eine **Abofalle** handeln.
- Wichtig ist der **Datenschutz**: Sende **personenbezogene Daten** (z. B. Name, Adresse, Bankdaten) nur
  - wenn du dir sicher bist, dass der **Empfänger seriös** ist, die **Daten erforderlich sind** und
  - die Daten nicht veröffentlicht werden.
  - **Veröffentliche** Daten, Bilder, Videos oder jemanden persönlich betreffende Informationen **nie ohne Zustimmung** des Betroffenen bzw. dessen Eltern.
- Solltest du über ein Girokonto verfügen: Regelmäßig die Kontobewegungen überprüfen!
- Darum beachte konsequent:
  In Anwendungen wie dem Textverarbeitungsprogramm oder Offline-Computerspiel sind Aktionen und Inhalte widerruf-, wiederhol-  und löschbar  . **Das gilt für das Internet nicht!**
  Die Kommunikation im Internet ist **nicht** anonym und **virtuell**,
  vielmehr ist sie **real** und du hinterlässt Informationen. Darum beachte die Grundsätze:
  - Bevor du etwas veröffentlichst, bedenke die **Konsequenzen**. Das gilt sowohl für Beleidigungen, Drohungen oder Belästigung als auch für Informationen oder Fotos, die du jetzt vielleicht cool findest. Ob das in 30 Jahren immer noch so ist? **Das Internet vergisst nie!**
  - **Sei misstrauisch!** Manche Nutzer versuchen, andere durch Täuschung zu schädigen.
  - **Schau hin!** Internetbetrüger versuchen, sich auf Kosten anderer zu bereichern.
  - Im Zweifelsfall: **Klick weg!** – Oder besser noch: **Klick gar nicht hin!**

A Bearbeite das Arbeitsblatt 17, Seite 2: Maßnahmen zur Verringerung der Risiken