Datenschutz

Stammdatenspiel

Die TeilnehmerInnen des Workshops sortieren persönliche Daten in verschiedene Privatsphärestufen ein. Am Ende wird diskutiert, wie man sich schützen kann und was die Konsequenzen sind, wenn die Daten in andere Hände fallen.

MEDIEN MONSTER
Medien kreativ begreifen

Lernziel

Schülerinnen und Schüler sollen sensibilisiert werden

- **dass es unterschiedliche Stufen von Privatsphäre gibt**
- **dass diese individuell unterschiedlich ausgelegt werden**
- **welche Funktion die Privatsphäreeinstellungen in sozialen Netzwerken einnehmen**
- **für Konsequenzen, falls ihre persönlichen Daten doch in andere Hände fallen**

Themengebiete

An folgende Unterrichtsfächer kann dieses Spiel angebunden werden:

- **Philosophie**
- **Geschichte**
- **Informatik**

Es sei darauf hingewiesen, dass die Unterrichtsfächer nur Vorschläge sind. Dieses Spiel ist grundsätzlich geeignet für Themen rund um das Thema soziale Netzwerke und Datenschutz.

Bei Facebook und Google ist es möglich, die Daten, die über den Nutzer erhoben werden,

Vorbereitung

Die beiliegenden Karten werden vom Anbieter des Workskshops im Vorfeld ausgedruckt und ausgeschnitten. Für einen mehrmaligen Einsatz empfiehlt sich eine Laminierung der Karten. Um das Spiel ansprechender zu gestalten, können die Karten gerne auf buntem Papier in jeweils unterschiedlichen Farben gedruckt werden.

An der Tafel oder an einer breiten Fläche an der Wand des Klassenraums wird eine große Breite freie Fläche geschaffen. Diese soll ein ein Kontinuum von öffentlich bis privat symbolisieren. Deshalb wird der gesamte Tafelbereich von links nach rechts in die Kategorien „Darf jeder sehen“, „Dürfen meine Eltern sehen“ „Dürfen meine Freunde und ich sehen“ und „Darf nur ich sehen“ eingeteilt.

Durchführung

Am Anfang des Workshops sollte kurz darüber geredet werden, welche sozialen Netzwerke die TeilnehmerInnen im täglichen Leben nutzen. Dabei werden die TeilnehmerInnen auch gebeten, kurz zu erklären, welche privaten Daten sie dabei hinterlassen. Bei einer jüngerern Zielgruppe muss vorher geklärt werden, was eigentlich persönliche Daten sind.

Die Schüler und Schülerinnen werden in Gruppen (bis zu 5 Personen) aufgeteilt. Bei Gruppen bis zu 30 TeilnehmerInnen ist es auch denkbar, dass jede TeilnehmerIn einen eigenen Satz Karten bekommt. Die SpielleiterIn kann die Aufteilung, abhängig von ihrem didaktischen Konzept, frei wählen.

Auf den Karten steht jeweils eine Kategorie persönlicher Daten, beispielsweise „Name“, „Alter“, „Gewicht“, „Partyfotos“ oder „Freunde“. Jede Gruppe bzw. jede SchülerIn hat nun also einen identischen Kartensatz. Die Schüler und Schülerinnen sollen sich zunächst mit den Karten auseinandersetzen und diskutieren, in welche Kategorie sie diese einordnen würden. Nach der gruppeninternernen Diskussion bringen die Schüler und Schülerinnen die Karten mit Klebeband an der Tafel in der jeweiligen Kategorie an. Hierbei entstehen schon die beabsichtigten Diskussionen zwischen den TeilnehmernInnen, da es unterschiedliche Ansichten darüber gibt, welche Karte in welches Feld gehört.

Auswertung

Nachdem die Karten alle eingeordnet wurden, setzen sich die Schüler und Schülerinnen wieder an ihre Plätze und die Lehrkraft übernimmt die Auswertung. Da die jeweiligen Gruppen die gleichen Karten nicht in die gleiche Kategorie eingeordnet haben, kann der Spielleiter nun ausgewählte Karten mit den TeilnehmerInnen diskutieren. In der gemeinsamen Diskussion kann nun erörtet werden, warum Karten in eine Kategorie eingeordnet wurden. Auch Überscheidungen in der Auswahl der Kategorien können Bestandteil des Diskurses sein. Wir möchten betonen, dass es keine eindeutig richtige Zuordnung der Karten gibt. Ziel ist es, dass die TeilnehmerInnen für einen bewussten Umgang mit ihren privaten Daten sensibilisiert werden.

Anschließend werden mit den Schüler und Schülerinnen die Privatsphäreeinstellungen in sozialen Netzwerken durchgenommen. Falls es einen Konsens unter den TeilnehmerInnen gibt, welches das meist genutzteste soziale Netzwerk unter ihnen ist, kann dieses exemplarisch über einen Beamer vorgeführt werden. Nun werden die Privatsphäre Einstellungen des Dienstes (Facebook, Snapchat, Instagram etc.) auf-

Du bist nicht der Kunde der Internetkonzerne, du bist ihr Produkt.

- Jaron Lanier

gerufen. Es folgt eine Diskussion, welche Einstellungen vorgenommen werden müssen, um die Privatsphäre, dem Tafelbild enstprechend, zu gewährleisten bzw. ob dies überhaupt möglich ist.

Sind die Schüler und Schülerinnen jugendlich oder älter sollte auch darüber diskutiert werden, dass alle (privaten) Daten auf teilweise weit entfernten Servern von Privatfirmen liegen und inwiefern Privatsphäreeinstellungen dazu geeignet sind, die persönlichen Daten überhaupt vor dem Zugriff der Firma zu schützen. Des Weiteren sollte darauf hingewiesen werden, dass eingestellte Daten zwar vor anderen Nutzern verborgen werden können, der Dienst selber aber Zugriff auf diese hat.

Hintergrundinformationen

Das im Workshop erarbeitete bezieht sich auf die die Privatsphäreeinstellungen in sozialen Netzwerken. Mit den Einstellungen lassen sich private Informationen vor einfachen Besuchern ein gutes Stück weit schützen - deshalb ist es auch eine gute Idee, die Privatsphäreeinstellungen zu nutzen. Trotzdem sind Privatsphäreeinstellungen keine sichere Lösung des Problems.

Privatsphäreeinstellungen werden genutzt, um festzulegen, welche ausgewählten „Freunde“ bzw. „Follower“ Zugriff auf die eigenen Informationen erhalten. Stellt man beispielsweise sein eigenes Instagram-Profil auf Privat, so können Fremde die eigenen Posts nicht mehr sehen. Nun müssen Fremde eine Anfrage senden, ob diese der eigenen Seite bzw. Profil folgen dürfen. Der Profilbesitzer kann also selbst entscheiden, ob er der anfragenden Person Zugriff auf das eigene Profil gewährt oder nicht. Das Prinzip ist auf anderen Social Media Plattformen sehr ähnlich. In der Regel ist es möglich eigenständig zu bestimmen, wer Zugriff auf die eigenen Inhalte hat.

Ein Grundprinzip des Internets ist, dass jeder Nutzer, der Inhalte lesen kann, diese natürlich auch beliebig kopieren kann (genaugenommen wird schon eine Kopie von dem gespeicherten Posts auf dem Server erstellt, wenn man sich die Inhalte nur auf einem Endgerät wie einem PC, Tablet oder Smartphone anzeigen lässt). Dabei stellt sich natürlich die Frage, ob man jedem seiner >100 Freunde/Follower hier wirklich trauen kann. An dieser Stelle bietet sich eine Diskussion über Online-Freundschaften an.

Stellt man diese mehr oder minder privaten Informationen bei einem sozialen Netzwerk ein, so kopiert man sie auf Server eines Unternehmens, über das man im Regelfall nicht besonders viel weiß und verlässt sich darauf, dass dieses sorgsam mit den eigenen Daten umgeht. Hier wäre denkbar mithilfe einer Online-Recherche die Unternehmstrukturen offenzulegen, um anschließend über den Zwiespalt zwischen Rentabilität und Datenschutz zu diskutieren. Denn es sei darauf hingewiesen, dass einerseits die Nutzer von beispielsweise Facebook kein Geld an dieses Unternehmen entrichten; andererseits die (technische) Infrastruktur, um eine solchen Dienst bereitzustellen, viele Milliarden Euro im Jahr kostet.

Darüber hinaus wird fälschlicherweise häufig behauptet, dass Unternehmen Daten weiterverkaufen. Manche Anbieter von Internetdiensten werben deshalb damit, dass sie ihre Daten nicht an Dritte weitergeben. Das löst aber das Problem nicht. Auch MySpace oder StudiVZ (die zwei in Detuschland populärsten sozialen Netzwerke in den 00er Jahren) warben zeitweise auch damit, dass ihnen Datenschutz wichtig sei und die Daten deshalb besonders schützen. Beide Unternehmen haben keine Daten verkauft, jedoch wurden die Unternehmen als sie wirtschaftlich schwächer gestellt waren, von anderen amerikanischen Firmen aufgekauft, die großes Interesse an den Nutzerdaten hatten. Ein weiterer Punkt sind Hackerangriffe, bei denen in der Vergangenheit bei vielen verschieden großen Firmen persönliche Daten abhandengekommen (LinkedIn 2012, Yahoo 2014) sind. Doch es nicht unbedingt ein Hackerangriff notwendig, dass unbefugte Dritte an persönliche Daten gelangen. Ein Beispiel ist der Fall rund um Cambrige Analytics und Facebook. Seit den Enthüllungen von Edward Snowden wissen wir auch, dass amerikanische Geheimdienste direkten Zugriff auf Server und die darauf gespeicherten Daten, von allen großen amerikansichen IT-Unternehmen (Facebook, Apple, Microsoft etc.), haben können.

Wenn man sagt, die Privatsphäre ist mir egal, ich habe nichts zu verbergen - dann ist das wie wenn man sagt, die Redefreiheit ist mir egal, ich habe nichts zu sagen.

- Edward Snowden

ICH

FREUNDE

MEDIEN MONSTER
Medien kreativ begreifen

ELTERN

MEDIEN MONSTER
Medien kreativ begreifen

ARBEITS-KOLLEGEN

MEDIEN MONSTER
Medien kreativ begreifen

JEDER

MEDIEN MONSTER
Medien kreativ begreifen

Name

Name

Name

Name

Geburtsdatum

Geburtsdatum

Geburtsdatum

Geburtsdatum

Geschlecht

Geschlecht

Geschlecht

Geschlecht

Gewicht

Gewicht

Gewicht

Gewicht

Liebe

Liebe

Liebe

Liebe

Krankheit

Krankheit

Krankheit

Krankheit

Chat-Nachrichten

Chat-Nachrichten

Chat-Nachrichten

Chat-Nachrichten

Partybilder

Partybilder

Partybilder

Partybilder

Wo war ich letztes Wochenende?

Wo war ich letztes Wochenende?

Wo war ich letztes Wochenende?

Wo war ich letztes Wochenende?

Wann ich online bin.

Wann ich online bin.

Wann ich online bin.

Wann ich online bin.

Wo ich mich
gerade aufhalte.

Wo ich mich
gerade aufhalte.

Wo ich mich
gerade aufhalte.

Wo ich mich
gerade aufhalte.

Welche Webseiten ich aufrufe.

Welche Webseiten ich aufrufe.

Welche Webseiten ich aufrufe.

Welche Webseiten ich aufrufe.