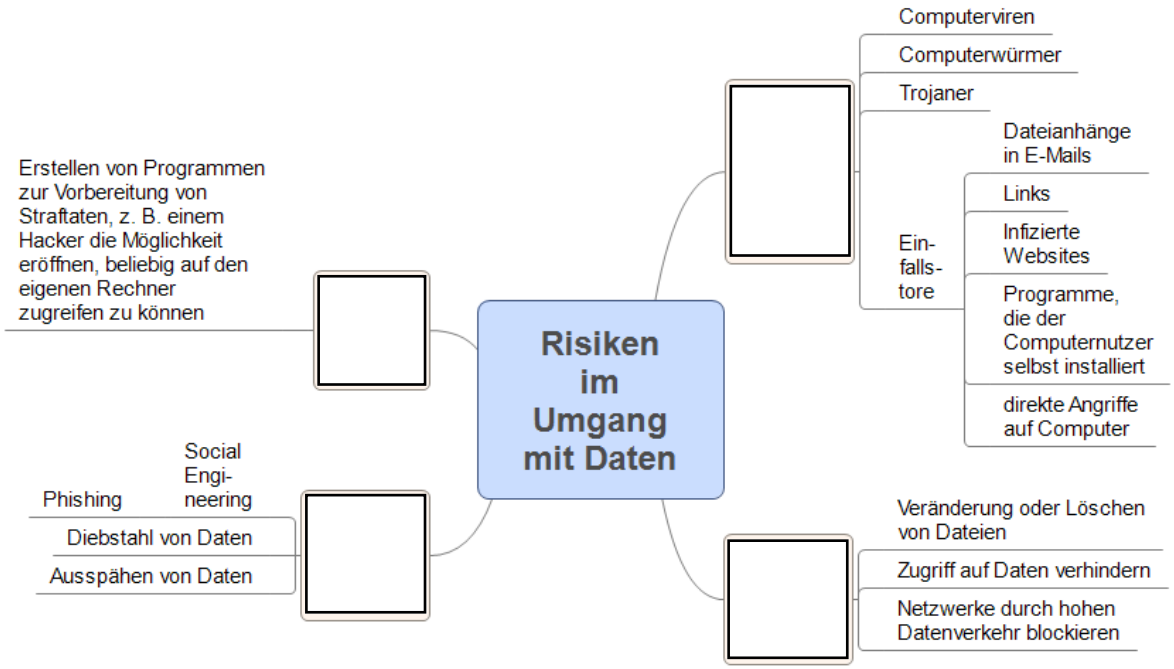
Risiken im Umgang mit Daten

1. Ergänze die Mind Map (vgl. Arbeitsblatt 1.4-17):



2. Ergänze die Begriffserklärungen und Erläuterung der Funktionsweise:
   - **Computerviren** verursachen aktiv Schaden, z. B. _____
     Viren pflanzen sich fort, _____
     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 _____
     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.
     _____

     So kannst du ganz offiziell 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.
   - **Trojaner** verbreiten sich, _____
     Dazu täuschen sie eine sinnvolle Anwendung vor, _____
     _____

     Das kann z. B. der Diebstahl von Zugangsdaten zum Online-Banking sein oder dem Hacker die Möglichkeit eröffnen, von außen beliebig auf den Rechner zugreifen zu können.
   - **Phishing** bedeutet, _____
     _____

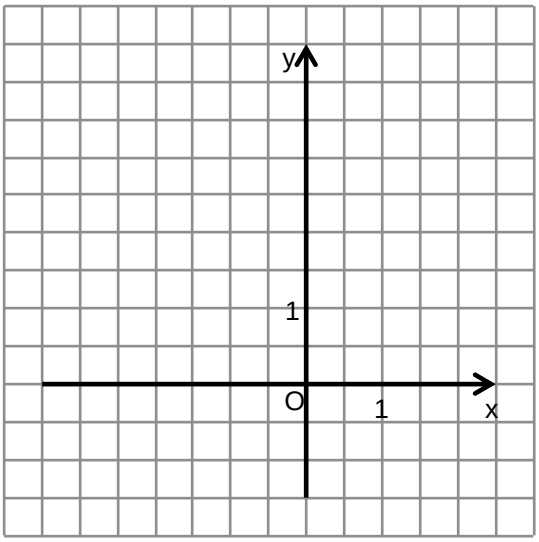
Verschlüsselung von Informationen

Angeblich hat der römische Feldherr Julius Cäsar zur geheimen Übermittlung seiner Nachrichten folgenden **monoalphabetischen Code**, den „Cäsar-Code“, verwendet:
Es werden alle Buchstaben im Alphabet um eine feste Anzahl von Stellen verschoben. Verschiebt man z. B. um sieben Stellen, so wird das A auf den Buchstaben H abgebildet; das Z codiert man zum Buchstaben G:

Alphabet wird mit Zuordnungsschlüssel 7 verschlüsselt (codiert)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G

3. Codiere anhand dieser Tabelle deinen Namen.



➢ Mathematisch vereinbart man damit eine Funktion. Ein Computer kann Daten mit einer mathematischen Funktion einfach verschlüsseln, weil die Daten binär codiert vorliegen, z. B. im ASCII-Code:

Zeichen	A	B	C	…	Z
ASCII-Wert dezimal	065	066	067		090

Auszug aus der ASCII-Tabelle

4. Gegeben ist die Funktion y = x + 2.
   - Zeichne den Funktionsgrafen in ein Koordinatensystem ein.
   - Codiere eine kurze Nachricht mit dem Schlüssel 2, notiere sie auf einem Blatt Papier und sende sie an deinen Banknachbarn. Decodiert dann beide jeweils die Nachricht eures Mitschülers.

     Uncodierte Kurznachricht:

     Codierte Kurznachricht:

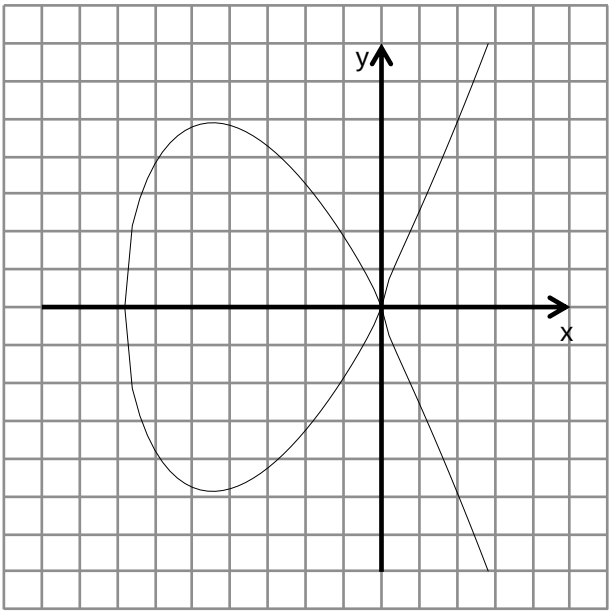
➢ **Kryptographie** ist die Wissenschaft, die sich mit Informationssicherheit befasst, also u. a. mit der *Verschlüsselung* von Informationen. Das *Entschlüsseln* von Informationen bezeichnet man als **knacken**.

5. Knacke die folgende Nachricht:

   GKB NKC CMRGSOBSQ?

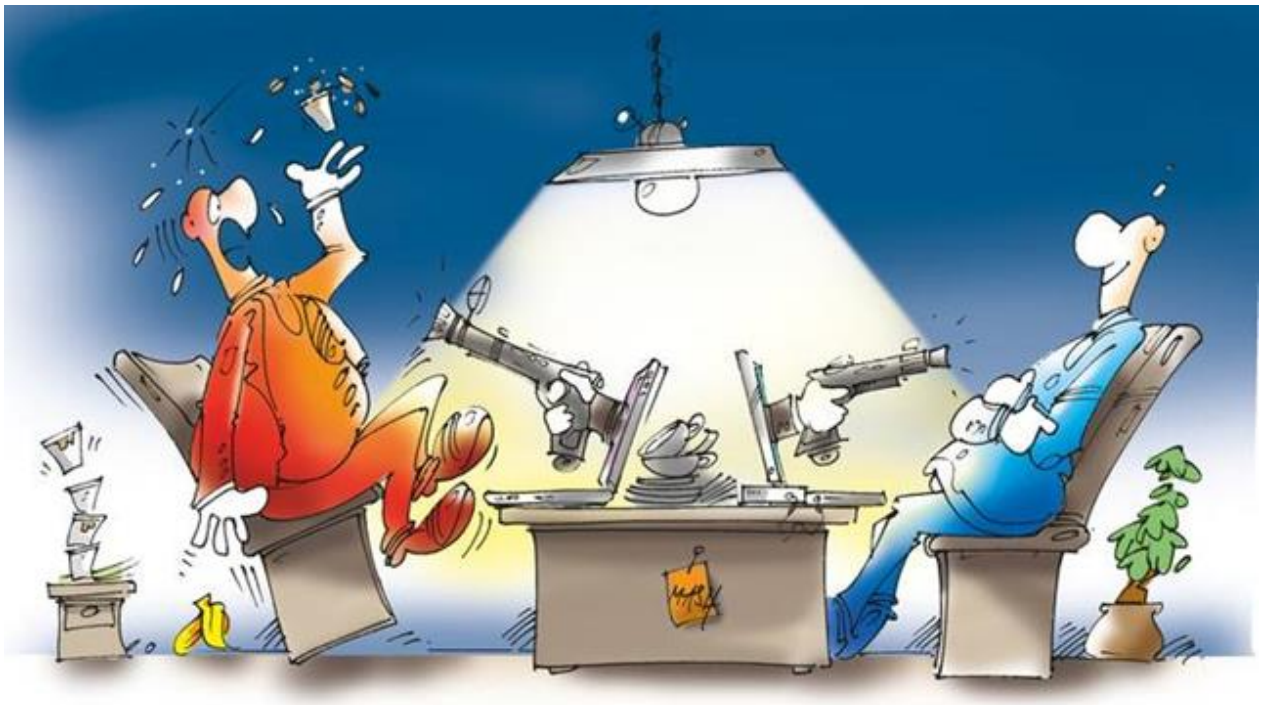
   Der Schlüssel lautet:

   Die entschlüsselte Nachricht lautet:



Den „Cäsar-Code“ kann man recht einfach knacken. Deshalb werden aufwändigere mathematische Verfahren verwendet. Aktueller technischer Stand sind elliptische Kurven, für deren Entschlüsselung man Logarithmen benötigt. (Stand: Dezember 2016)
Ein einfaches Beispiel wäre die Funktion $y^2 = x^3 + 4x^2 + x$, die zu dem rechts abgebildeten Grafen führt.

Editorial: Dies ist keine Übung

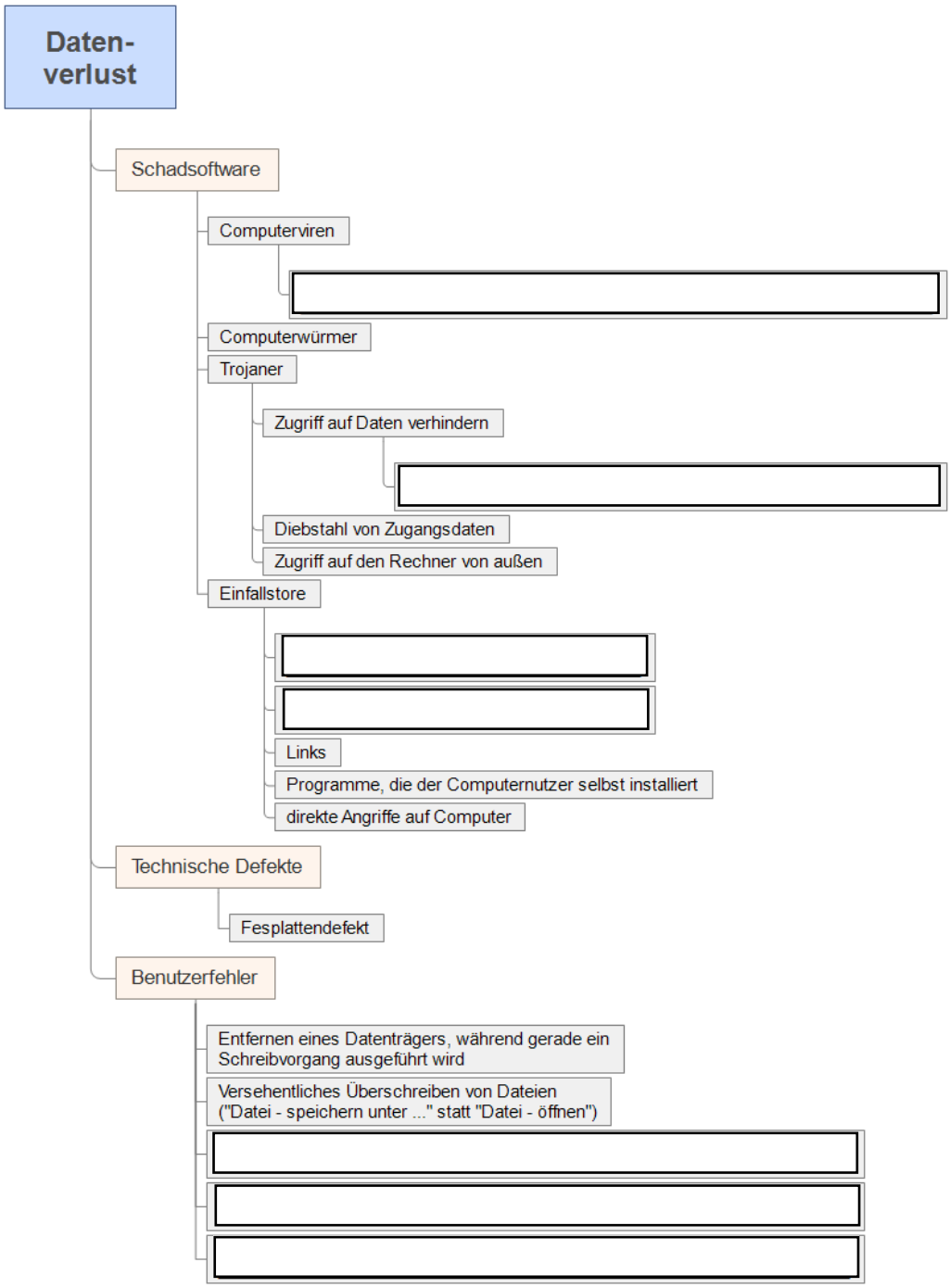


Stellen Sie sich vor, Ihr Rechner sei jetzt, wirklich unmittelbar jetzt, von einem Verschlüsselungs-Trojaner befallen worden. Jetzt. Nicht irgendwann in einer möglichen Zukunft, sondern jetzt.
Ignorieren Sie kurz, dass sich einige Daten eventuell noch retten lassen - selbst wenn das klappt, kostet es viel Glück und Zeit und Schweiß und Flüche. Sie erleben gerade Ihren persönlichen größten anzunehmenden Datenunfall.
Statt Ihrer unersetzlichen privaten und beruflichen Dokumente sehen Sie nur noch die Aufforderung, Geld an einen Unbekannten zu zahlen. Im besten Fall gibt er Ihre Daten wieder frei, womöglich verkrümelt er sich aber mit dem Lösegeld, unverfolgbar. Dann bleiben Ihre Urlaubsfotos, die medizinischen Gutachten, die Seminararbeiten, die fast fertige Steuererklärung auf Dauer verschlüsselt, verloren, futsch.
Wenn Sie ähnlich ticken wie ich, dann haben Sie jetzt kalte Finger und heiße Ohren. Eigentlich bleiben nur zwei Optionen: Entweder betrachten Sie den Trojaner-Befall wie einen fatalen Festplattendefekt, als technisches Versagen ohne Weg zurück. Dann sind die Daten halt hinüber und Sie müssen die Konsequenzen tragen. Oder Sie zahlen den geforderten Betrag und hoffen inständig, dass der anonyme Verbrecher am anderen Ende des Internet sein Wort hält.
Natürlich sollten Sie auf jeden Fall versuchen, lokal zu retten, was zu retten ist. Aber wie gesagt: Glück, Zeit, Schweiß, Flüche. Außerdem gibt es einen viel besseren Weg. Da dies nur ein Gedankenspiel ist, können Sie die Zeit zurückdrehen: vor den GAU. Alle Ihre Daten sind wieder da. Holen Sie jetzt tief Luft und lesen Sie die Artikel ab Seite 76.
Investieren Sie lieber in eine oder mehrere externe Festplatten, statt einem ungewaschenen Erpresser mindestens doppelt so viel Geld in den Rachen werfen zu müssen. Planen Sie eine gangbare Backup-Strategie für sich - und für alle, die Ihnen lieb sind. Nur das kann der Bedrohung den Schrecken nehmen. Nicht aufschieben, sondern sofort erledigen; die Zeit rennt.
Schon bei Ihrem nächsten Besuch einer kompromittierten Webseite, beim unbedarften Klick auf eine verdammt gut gemachte Spam-Mail kann ein Erpressungs-Trojaner zuschlagen - bei Ihnen oder Ihren Lieben. Sie wissen jetzt, wie es sich anfühlt, wenn der Ernstfall eintritt. Stellen Sie also sicher, dass es nicht so weit kommt. Jetzt.
Alles Gute,
Gerald Himmelein

c't 2016, Heft 7, Seite 3 – mit freundl. Genehmigung des Heise Medien GmbH & Co KG

Datenverlust

6. Ergänze die Mind Map mit den Informationen in dem Editorial auf Seite 3.
   Überlege dir weitere mögliche Benutzerfehler.



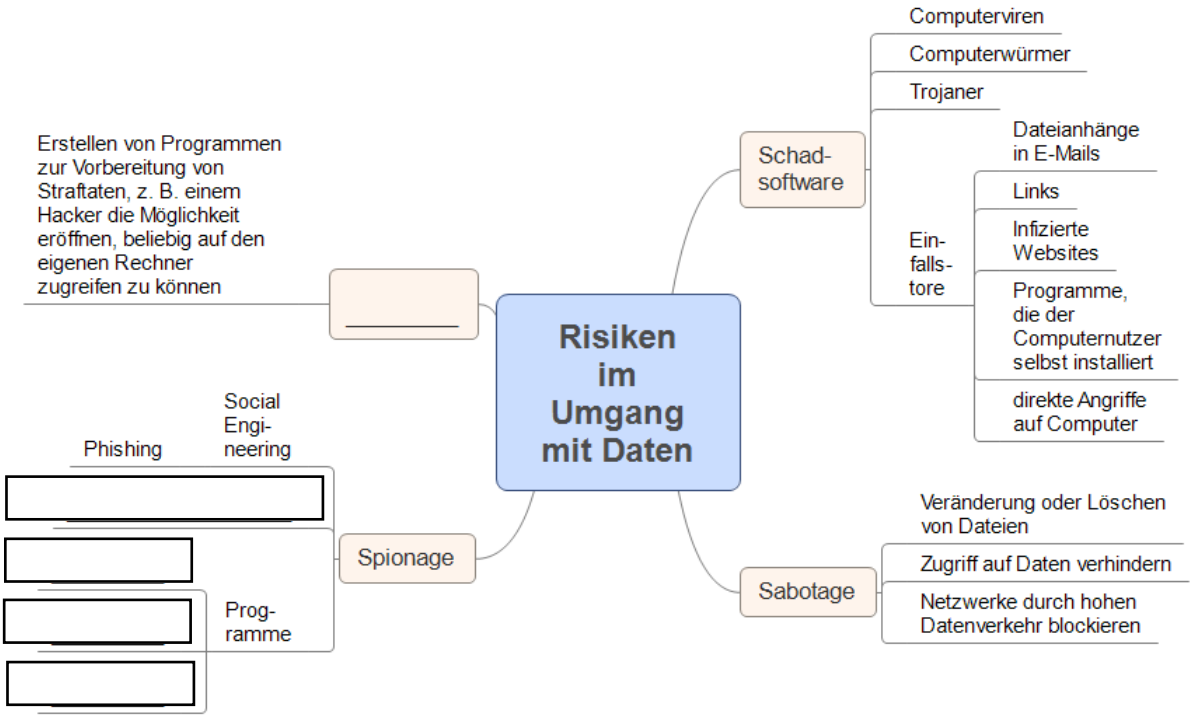
   - Welche Daten sind besonders wichtig und sollten vor Verlust geschützt werden?

     Aus dem Editorial:

     Für dich persönlich, *z. B.:*

Spionage

7. Ergänze die Mind Map:



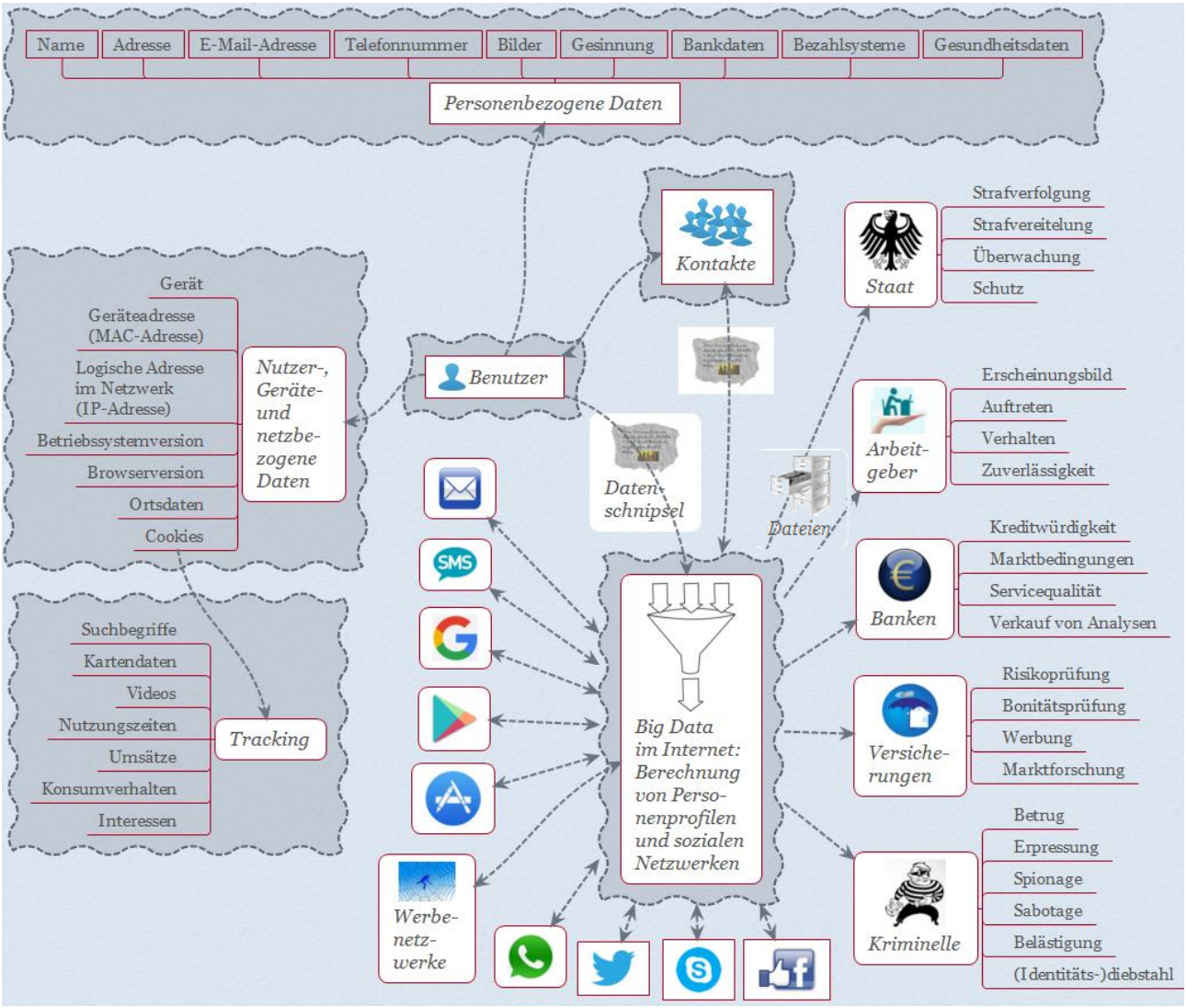
8. Lies die folgenden Pressemitteilungen und gib an, auf welche Geräte der Angriff abzielt.
   Hinweise: *Rooten* bedeutet, sich auf einem Gerät mit Linux-basierten Betriebssystem (z. B. Android) Administratorrechte zu verschaffen.
   Ein *Jailbreak* ist im Prinzip dasselbe bei Geräten mitdem Betriebssystem iOS.

   - Der Android-Schädling *Tordow* ist im Kern ein Banking-Trojaner, der sich Root-Rechte verschaffen kann, um so auf vielfältigen Wegen Informationen abzugreifen... Ist ein Android-Gerät erst einmal gerootet, können Kriminelle im Grunde alles damit anstellen und ihre Opfer vielfältig belauschen. (https://www.heise.de/security/meldung/Android-Schaedling-Tordow-Banking-Trojaner-mutiert-zum-Super-Trojaner-3335146.html; 28.09.2016; 14:00 Uhr; Dennis Schirrmacher)
     Betroffene Geräte: _____
   - Das Spionageprogramm *Pegasus* nistet sich in iPhones ein und kann dort unter anderem E-Mails, Nachrichten, Passwörter abgreifen und Anrufe mitschneiden. (http://www.zeit.de/digital/ mobil/ 2016-08/iphone-sicherheitsluecke-apple-pegasus-schadsoftware; 26. August 2016, 12:18 Uhr; Eike Kühl)
     Betroffene Geräte: _____
   - Bei HbbTV wird konventionelles Fernsehen mit dem Internet kombiniert. Laut einem Bericht aus dem Jahr 2014 wäre es möglich, die eingebaute Kamera zu aktivieren und Videostreams auch bei ausgeschaltetem Fernsehgerät über das Internet zu übertragen. (vgl. c't 2014, Heft 4, S. 78-81)
     Betroffene Geräte: _____
   - Dem ADAC gelang es, mit Hilfe von Hardware im Wert von unter 1000 Euro und einer frei verfügbaren Software, Autos über Mobilfunk zu öffnen (http://www.sueddeutsche.de/digital/it-sicherheitsluecke-adac-knackt-bmws-per-mobilfunk-1.2328051 vom 3. Februar 2015).
     Betroffene „Geräte“: _____

➢ Alle mit dem Internet verbundenen elektronischen Geräte sind potentielle Angriffsziele für Spionage- oder auch Sabotagezwecke.

Missbrauch von Daten

In der Grafik sind einige Möglichkeiten zur Gewinnung und Nutzung von Daten aufgeführt.



9. Wer hat ein Interesse an Daten und was ist das Motiv? Überlege dir, ob ein **Ge**brauch der Daten zum Nutzen Aller vorliegt oder ob das zu **Miss**brauch der Daten führt (vgl. Arbeitsblatt 1.4-18, S. 2).
   - Das Interesse Krimineller ist eindeutig der _____
   - _____ sehen in der Überwachung eine Maßnahme zur Wahrung „besserer Gesellschaftsformen“ und rechtfertigen damit auch Maßnahmen wie Folter und Strafen nur wegen einer anderen (politischen) Gesinnung, Religion oder Sexualität.

     Aber auch für demokratische _____ gibt es Risiken, denn der Übergang zwischen Verteidigung der Freiheit Aller und Überwachung, die die Freiheit des Einzelnen zu sehr einschränkt, hat fließende Grenzen (z. B. Stichwort „Guantanamo“).
   - Arbeitgeber, Banken und Versicherungen können automatisiert erstellte Persönlichkeitsprofile nutzen, um z. B. _____ oder _____ festzustellen, was in Deutschland juristisch nicht zulässig ist und auch gesellschaftlich als nicht Wünschenswert eingestuft wird.

➔ Oft kann man nicht genau festlegen, ob Daten zum rechtmäßigen Gebrauch oder zum Missbrauch erhoben werden. Auch ist es juristisch oft nicht eindeutig, sondern liegt an nationalen Gesetzen.

➢ Eins ist klar: Je weniger Daten öffentlich werden, desto geringer ist die Gefahr des Missbrauchs.