6.7 Chancen und Risiken

Einstieg:

- Die Anbieter der meisten Suchmaschinen verdienen z. B. ihr Geld mit dem Anzeigen von Werbung. Andere Firmen zahlen dann für Werbeflächen, auf denen personalisierte Werbung angezeigt werden soll. Dadurch, dass die Suchmaschine so viele Informationen über die nutzende Person sammelt, kann sie passende Werbung schalten. Die meisten Firmen wären dazu nicht in der Lage, da sie nicht genügend Informationen sammeln können.
  Wenn Ayla für ihr Referat verschiedene Suchbegriffe zum Thema Spanien in eine Suchmaschine eingibt, speichert diese, dass Ayla sich für das Land interessiert. Statistisch wird für sie daher eine Anzeige für Urlaub in Spanien wahrscheinlicher. Viele Webseiten erzielen auch Einnahmen, indem sie Werbung einblenden und Daten zum Surfverhalten weitergeben. Diese Werbungen werden im Hintergrund aber auch wieder von der Suchmaschine ausgeliefert und greifen die Daten ab. Daher erscheinen auch über viele Webseiten hinweg ähnliche Anzeigen.
- Grundsätzlich ist es praktisch, wenn man personalisierte Werbung angezeigt bekommt – für Produkte, für die man sich auch interessiert. Zusätzlich wird man auf Sachen aufmerksam gemacht, die man sonst nicht gesucht hätte, aber benötigen kann.
  Dies kann aber auch dazu verleiten, mehr zu kaufen als man wirklich braucht. Darüber hinaus ist es nicht sicher, ob und wie diese Daten auch gegen die betreffende Person verwendet werden. So könnte das Einkaufsverhaltens eines Nutzers z. B. auch dazu führen, dass dieser für Produkte grundsätzlich höhere Preise angezeigt bekommt als dies bei anderen Personen der Fall ist.

A1

a) Ein Datenpaket (wie z. B. nebenstehend abgebildet),das bei einer HTTP-Antwort durch das Netz geleitet wird, enthält im Datenteil die Daten so, wie sie verschickt wurden. D. h. jeder, der auf dem Weg von Sender zu Empfänger Zugriff auf die Leitung oder ein beteiligtes Netzwerkgerät hat, kann diese Daten mitlesen.

S	T	A	R	T		P	A	K	E	T	
0	8	8	1	2	5	0	4	3	0	0	5
1	7	9	0	6	7	1	0	2	0	9	4
			8	0		5	3	0	6	9	
H	T	T	P		2	0	0				
H	A	L	L	O		D	A	T	E	N	!
E	N	D	E		P	A	K	E	T		

b) Es sind Individuelle Lösungen möglich. Allgemein: Sollen Daten so verschickt werden, dass sie nicht mitgelesen werden können, müssen die Daten in der Anwendungsschicht verschlüsselt werden. Dies geschieht so beim HTTPS. Tippt man im Browser z. B. die Bankzugangsdaten ein, sollte die Online-Banking-Seite auf jeden Fall mit HTTPS aufgerufen werden.

© C.C.Buchner Verlag, Bamberg

A2

a) Es sind individuelle Lösungen möglich.

b) Es sind individuelle Lösungen möglich. Beispiele siehe Einstieg. Weitere Diskussionspunkte sind z. B. der Verkauf der Daten an Versicherer, Banken etc. Hier können für „vorbildliche“ Surfer günstige Konditionen entstehen. Für aus Firmensicht „ungeeignete“ Surfer können Dienstleistungen teurer oder erst gar nicht angeboten werden (Bsp.: Extremsportler und Krankenzusatzversicherung).

A3

a) Es sind individuelle Antworten möglich. Mögliche Beispiele:
positive Aktivitäten:

- Durchsuchen von Bibliotheken
- Ansehen von digitalisierten Werken (Museen, alte Handschriften etc.), die sonst nur für ausgewählte Personen zugänglich wären
- Suchen einer Unterkunft für den Urlaub
- Vergleichen von Artikeln
- Artikelauswahl
- Kommunikation

negative Aktivitäten:

- negative Beeinflussung von Kindern durch Social Media
- Betrug durch Phishing
- Betrug durch Fake-Verkaufsseiten
- Zugang zu illegalen Drogen, Waffen etc.
- anonymes Mobbing
- Beeinflussung von Meinungen durch Streuung oder gezielte (Falsch-)Information

b) Es sind individuelle Diskussionen möglich. Beispiele für Gefahren siehe a). Mögliche Schutzmaßnamen sind:

- Verschlüsselung von Daten
- unbekannten Personen mit Vorsicht begegnen
- bei seltsamen Nachrichten von bekannten Personen: mit direkter/persönlicher Kommunikation klären
- sparsam mit Daten umgehen (z. B. nicht einfach Posten, dass man jetzt im Urlaub ist)
- regelmäßige Updates gegen Sicherheitslücken machen
- Informationen ggf. auf Quellen überprüfen
- sich über Seriosität von Internetseiten erkundigen
- Downloads und Anhänge nicht unbedarft öffnen oder ausführen

© C.C.Buchner Verlag, Bamberg

Aufgabe 1

Wenn die Nachricht über HTTPS verschickt wird, heißt das nur, dass auf dem Weg von Client zum Server keiner die Nachricht lesen kann. Sobald die Daten aber am Server angekommen sind, können die Daten klar gelesen werden. Daher muss die Nachricht selbst vor dem Senden (z. B. mit dem öffentlichen Schlüssel des Empfängers) verschlüsselt werden, so dass nur der Empfänger die Nachricht wieder entschlüsseln kann.

Aufgabe 2

Es sind individuelle Diskussion möglich. Beispielaspekte:
starke Regulierung → Risiken aber auch die Freiheit nimmt ab (Gefahr von Zensur)
wenig Regulierung → Freiheit aber auch Gefahren nehmen zu

© C.C.Buchner Verlag, Bamberg