Cybersecurity & Privatsphäre im Internet

Justus Goltsch und Jannis Manczak

Gliederung

1. Einführung
2. Cybersecurity
3. Privatsphäre im Internet
4. Verbindung der Themen
5. Diskussion

1. Einführung

- Was bedeutet Cybersecurity?
- Was bedeutet Privatsphäre im Internet?

2. Cybersecurity (IT-Sicherheit)

2.1 Grundlagen

- Was sind Daten?
- Was sind Bedrohungen? Viren, Trojaner, Phishing
- Was ist ein Hacker?

2. Cybersecurity (IT-Sicherheit)

2.2 Was sind Cyberangriffe?

- Phishing
- Malware
- DDoS-Angriff
- Brute-Force-Angriff

2. Cybersecurity (IT-Sicherheit)

2.3 Verschlüsselung

- Was ist Verschlüsselung?
- symmetrische Verschlüsselung
- asymmetrische Verschlüsselung
- Beispiel: HTTPS
- Ende-zu-Ende-Verschlüsselung

2. Cybersecurity (IT-Sicherheit)

2.4 Aktuelle Herausforderung

- Cyberkriminalität weltweit
- KI und Cyberangriffe
- Sicherheit vs. Benutzerfreundlichkeit

3. Privatsphäre im Internet

3.1 Grundlagen

- Was sind persönliche Daten?
- Was bedeutet Datenschutz?
- Unterschied: Sicherheit vs. Privatsphäre

3. Privatsphäre im Internet

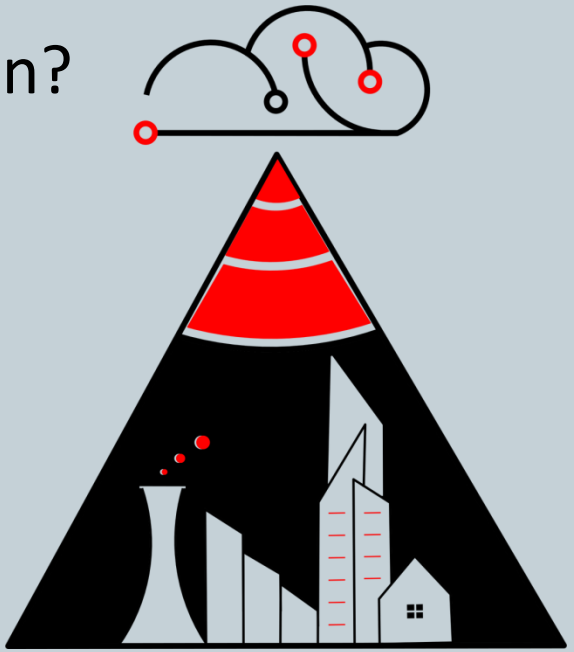
3.2 Datensammlung im Alltag

- Social Media (z.B. Chats, Likes, Standort)
- Cookies und Tracking
- Apps und Berechtigungen

3. Privatsphäre im Internet

3.3 Unternehmen und Daten

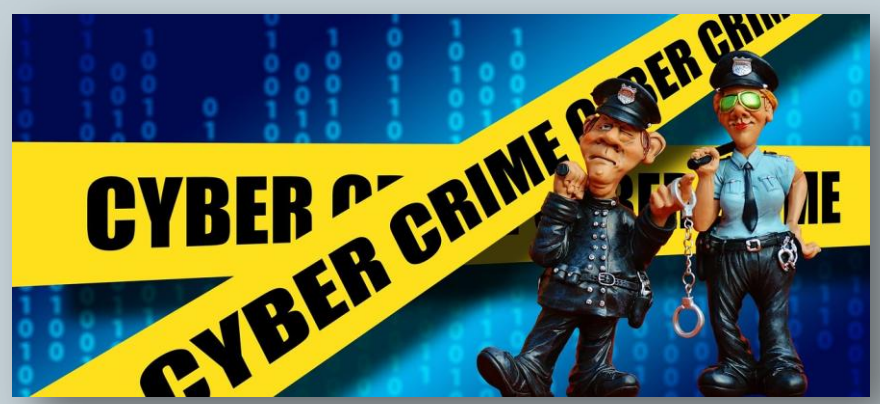
- Wie verdienen Firmen Geld mit Daten?
- personalisierte Werbung
- Datenhandel



3. Privatsphäre im Internet

3.4 Staatliche Überwachung

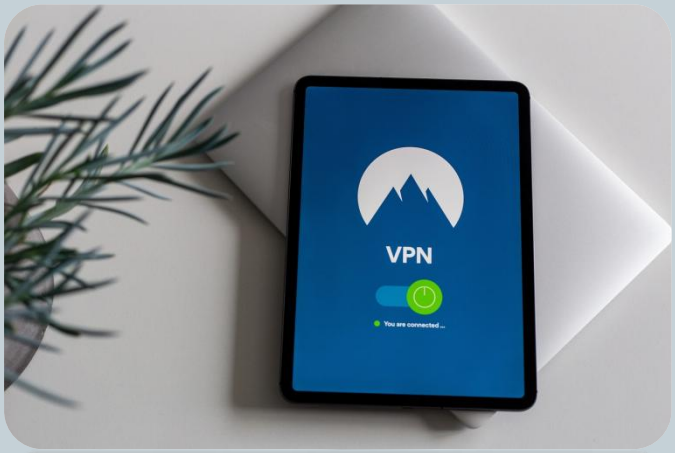
- Warum überwacht der Staat? zur Sicherheit, Terrorabwehr
- Beispiele: Zugriff auf Messenger
  (z.B. WhatsApp - Diskussion)
- Problem: Konflikt zwischen Sicherheit und Freiheit



3. Privatsphäre im Internet

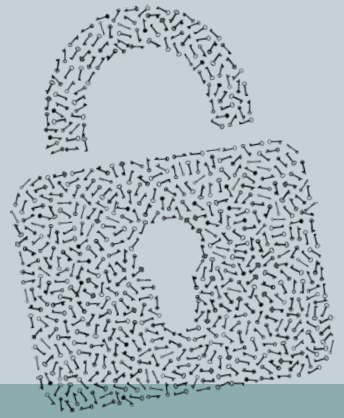
3.5 Mögliche Maßnahmen zum Schutz der Privatsphäre

- Datenschutz-Einstellungen
- VPN
- bewusster Umgang mit Daten
- alternative Dienste



4. Verbindung der Themen

- Wie hängen Cybersecurity und Privatsphäre zusammen?
- Beispiel:
  - gute Sicherheit schützt Privatsphäre
  - aber: Überwachung kann Sicherheit erhöhen und Privatsphäre einschränken



5. Diskussion

DISKUSSION

5.Diskussion

- These 1: „Der Staat sollte Zugriff auf verschlüsselte Nachrichten haben, wenn es der Sicherheit dient.“

→ neutral bis zustimmend

- These 2: „Ich habe nichts zu verbergen, deshalb ist mir Privatsphäre im Internet nicht so wichtig.“

→ dagegen

- These 3: „Unternehmen sollten meine Daten nutzen dürfen, wenn ich dafür kostenlose Dienste bekomme.“

→ neutral bis eher dagegen

5.Diskussion

- These 4: „Starke Passwörter und 2FA sind ausreichend, um sich im Internet zu schützen.“

→ alle relativ neutral

- These 5: „Ende-zu-Ende-Verschlüsselung sollte niemals eingeschränkt werden.“

→ zustimmend (alle)

- These 6: „Die größte Gefahr im Internet sind Hacker.“

→ neutral, dagegen

Quellenverzeichnis

- 10.000+ kostenlose Cyber Security und Cyber-Bilder – Pixabay
- Cybersecurity • Definition | Gabler Wirtschaftslexikon
- So schützt Du Deine Daten im Internet | Verbraucherzentrale.de
- BSI - Bundesamt für Sicherheit in der Informationstechnik – Gefährdungen
- Bundesamt für Verfassungsschutz – Cyberabwehr
- CYBERSICHERHEIT: AUSGLEICH ZWISCHEN SICHERHEIT UND PRIVATSPHÄRE
- Ende-zu-Ende-Verschlüsselung: Was ist das? Einfach erklärt – CHIP
- Hackerangriffe - Aktuelle Nachrichten zu Cyberattacken
- Was ist VPN und wie funktioniert es?
- Cybercrime-Trends 2025 | Report
- DDoS-Angriff - was ist das? | heise online