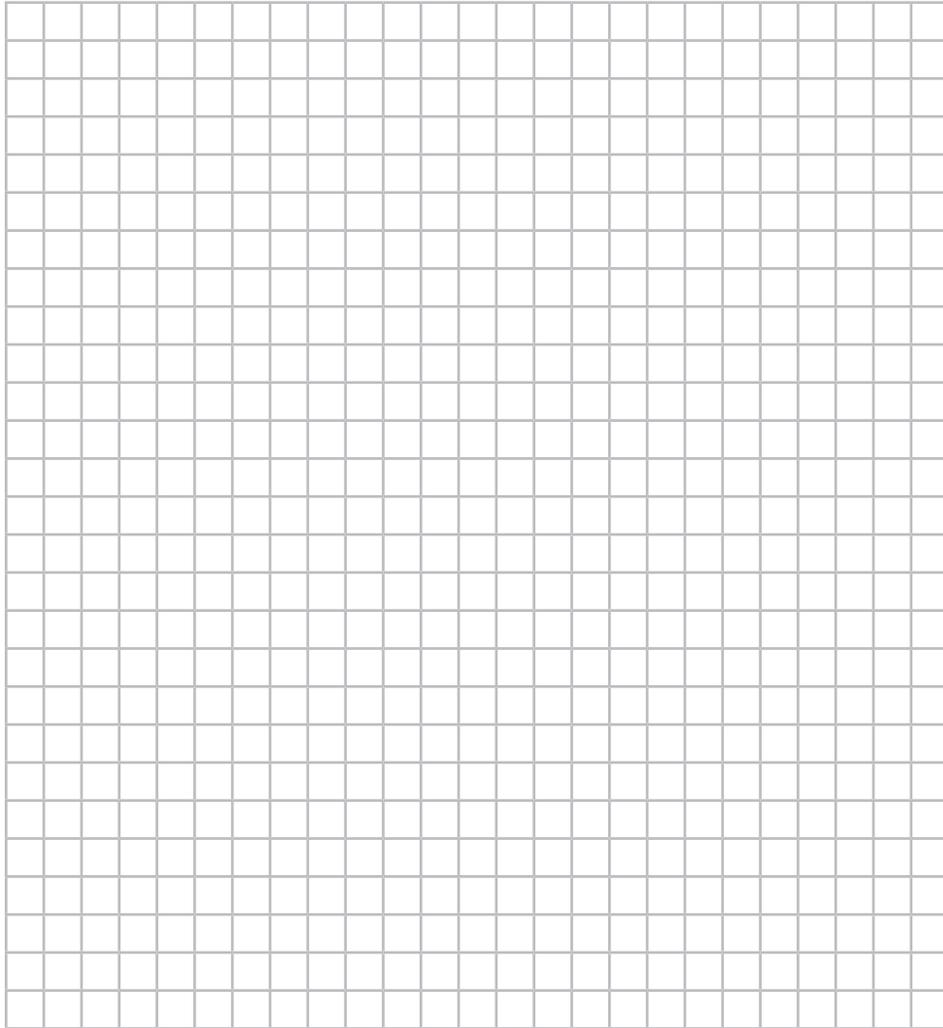


Notizen:



Veranstalter



zkm karlsruhe



ANTI-PRISM-PARTY

4. Staffel



- STATION NR. 6 -

WLAN sicher verwenden

WLAN SICHER VERWENDEN

Welches Problem wird gelöst?

- Wer ein unsicheres WLAN betreibt riskiert, dass seine Daten von Hackern mitgehört werden und der eigene Internetanschluss für illegale Zwecke missbraucht wird. Wer die Empfehlungen für ein sicheres WLAN berücksichtigt, schützt sich effektiv vor Angreifern.
- Fremden WLAN-Netzen darf nicht blind vertraut werden. Wer sie betreibt, kann Informationen ausspähen und missbrauchen. Verwenden Sie nur verschlüsselte öffentliche WLAN-Netze, denen sie vertrauen und denken Sie über die Verwendung einer VPN („virtual private network“) nach.
- Geräte wie Smartphones suchen aktiv nach bekannten Netzen und geben dadurch Informationen preis, die von Hackern genutzt werden können. Deaktivieren Sie diese Funktion und verbinden Sie sich nur mit passwortgesicherten WLAN-Netzen.
- Sicherheit in WLAN-Netzen bedeutet Anonymität, Schutz der eigenen Identität und Verhinderung des Mithörens sensibler Daten wie den Zugangsdaten für's Online-Banking oder persönlichen Informationen.

Wo gibt es gute Anleitungen im Netz?

- Sieben Empfehlungen für ein sicheres WLAN:
<https://aramido.de/s/wlan-sicherheit>
- Schutz vor Dritten – WLAN-Sicherheit:
<https://www.it-sicherheit.de/uploads/media/WLAN-Sicherheit.pdf>
- VPN für Android:
<http://workshop.tecchannel.de/a/vpn-unter-android-einrichten,3277607>
- VPN für iOS:
<https://support.apple.com/de-de/HT201550>



Alle Links finden Sie auch unter:
www.anti-prism-party.de/downloads

Wie heißt die Lösung? Wo kann sie bezogen werden? Welche Alternativen gibt es?

- Aktuelle Firmware des Router-Herstellers, beispielsweise AVM, Linksys, ASUS, etc.
- Informationen zum verschlüsselten WLAN für Karlsruher Bürger:
<https://www.ka-wlan.de/secure.html>
- Freifunk Karlsruhe:
<https://karlsruhe.freifunk.net>
- Tor zur Anonymisierung von Verbindungsdaten:
<https://www.torproject.org>
- VPN-Anbieter:
z.B. <https://zenmate.de>, <https://www.hidemymass.com/de/> (kostenpflichtig),
<https://help.riseup.net/en/vpn>, <http://tinc-vpn.org> (kostenlos)

Was sind die Grenzen der Lösung?

- Aktualisierte Router-Software und zeitgemäße Verschlüsselungsstandards gelten nicht für immer als sicher. Diese sollten regelmäßig auf Aktualisierung hin überprüft werden.
- Setzt man in öffentlichen WLANs VPN ein, verschiebt sich das Anonymitätsverhältnis lediglich vom WLAN-Anbieter zum VPN-Anbieter. Diesem muss deshalb mehr vertraut werden, als dem Anbieter des fremden WLANs.
- VPN-Verbindungen werden von manchen Firewalls geblockt und können dann nicht eingesetzt werden.