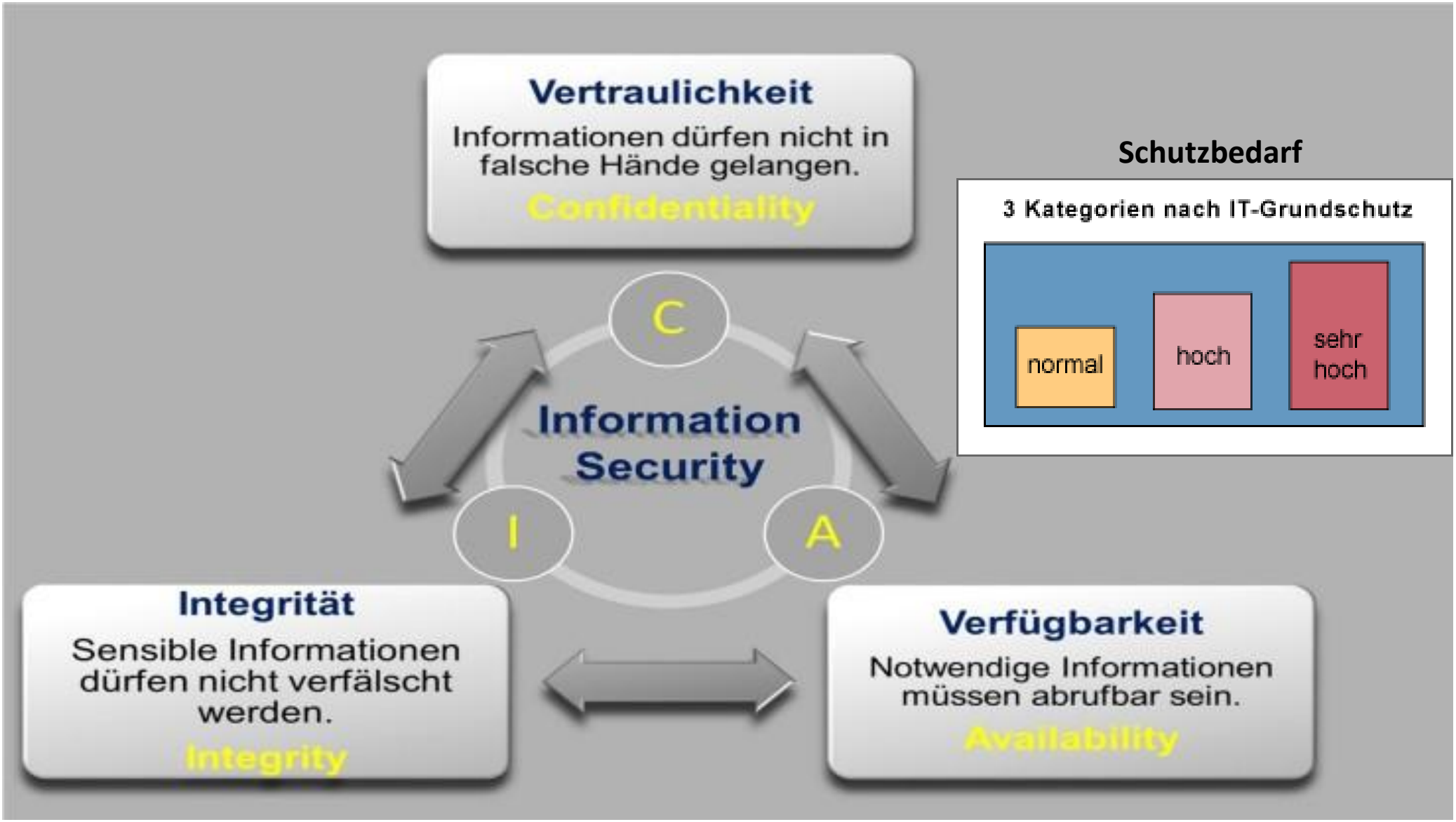
IT-Sicherheit in offenen Netzen

Datenschutz
Welche Schutzziele gibt es?

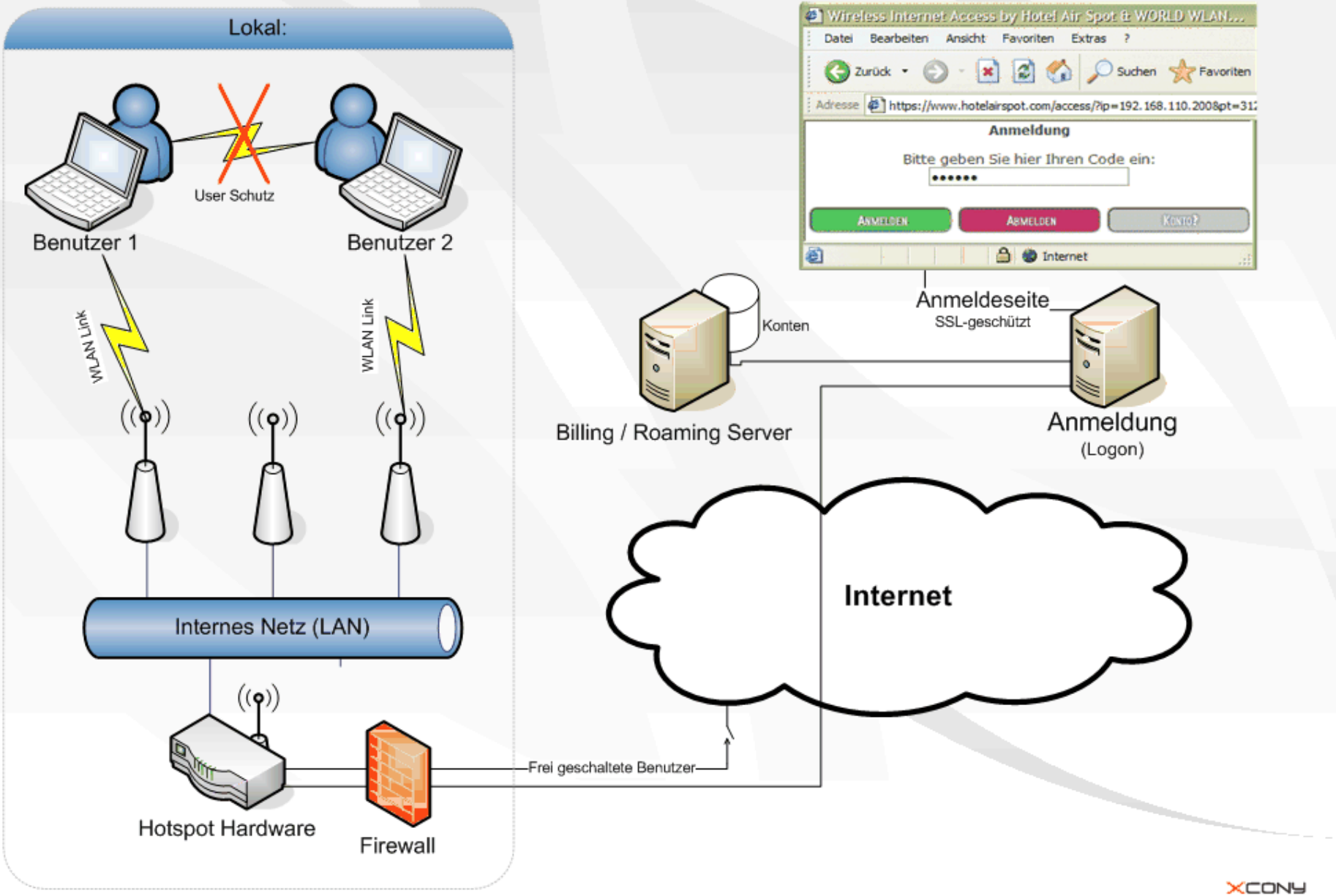


Beispiel für Gefährdungen

Was sind offene Netze?

- Öffentliche drahtlose Internetzugriffspunkte
- Fast ausschließlich wird das WLAN-Protokoll (802.11) verwendet → Unterstützung vieler mobiler Endgeräte

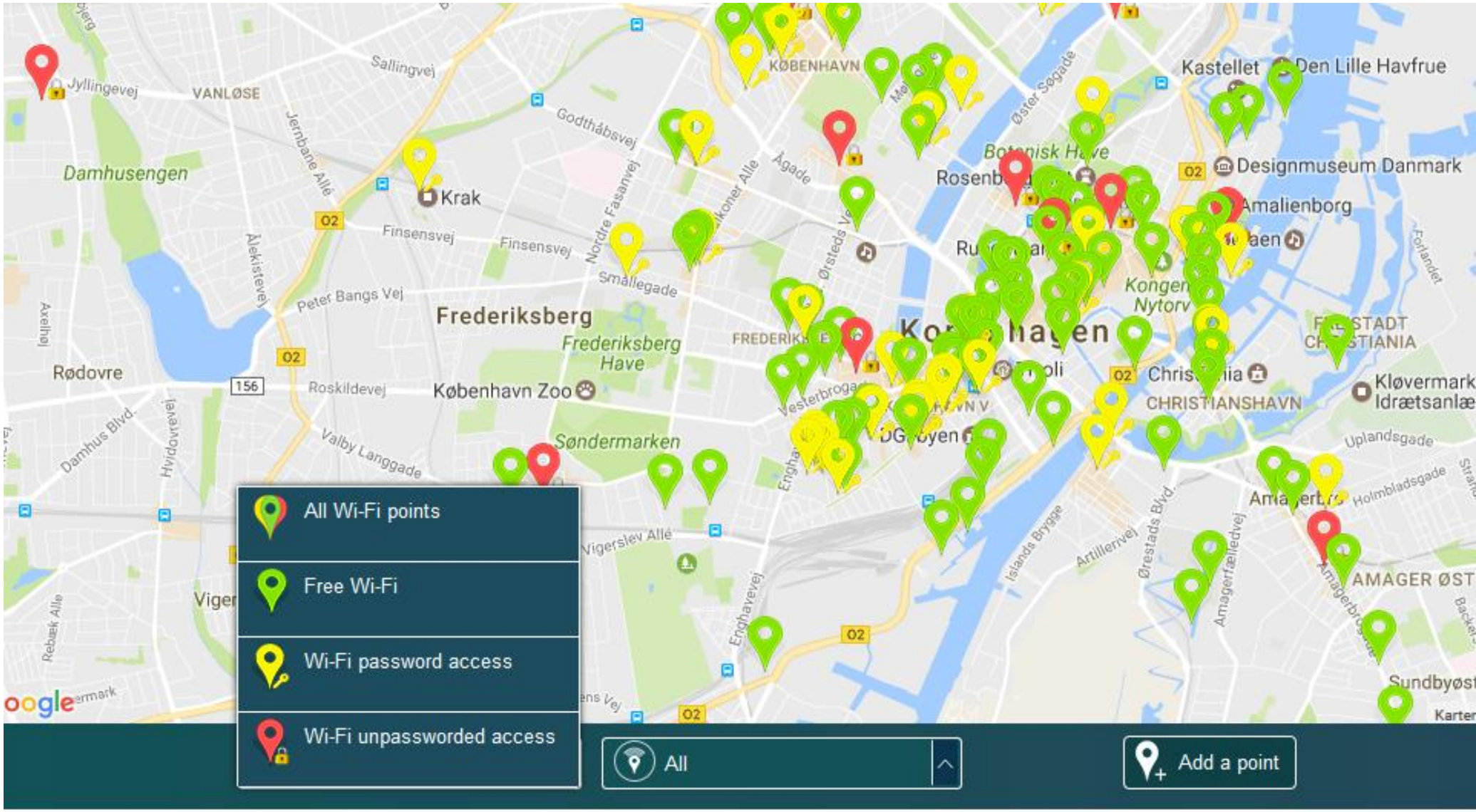
Aufbau von Hotspot Systemen



Unterschiedliche Anbieter

- Kommerziell
- Privat
- Öffentlich
- Freifunk

Freies WLAN



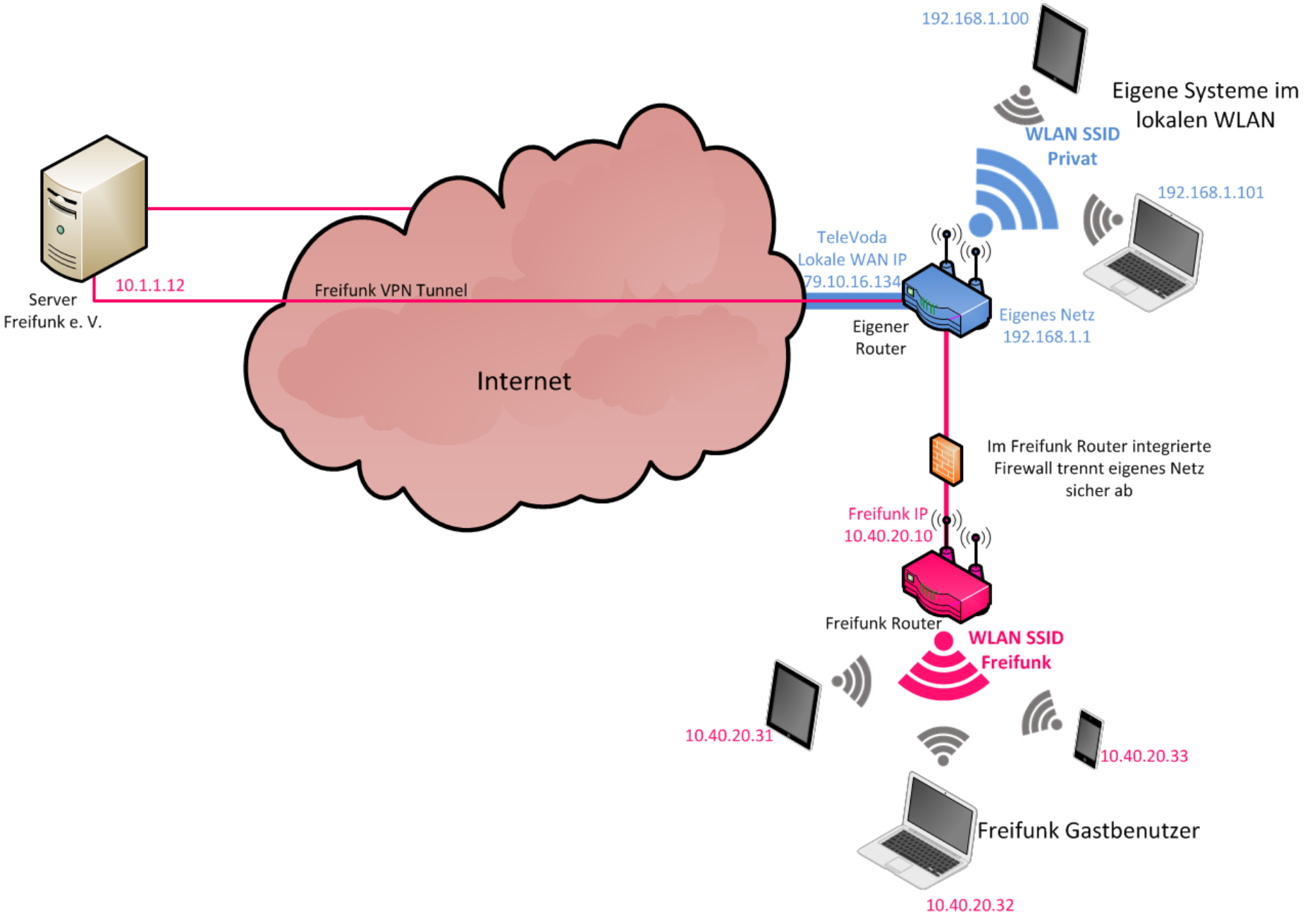
A list of places in Copenhagen with free internet

Kostenloses freies WLAN in evangelischen Kirchen

Freifunk

- WLAN-basierte Funknetze, die von Privatpersonen angeboten werden
- Nutzer sind gleichzeitig Betreiber
- Nutzer stellen Ihren WLAN-Router für alle Beteiligten zur Verfügung → Erstellung eines Intranets
- Über Internet-Provider kann dieses Intranet auch auf das Internet zugreifen

Freifunk-Struktur



Sind die Freifunk-Verbindungen auch wirklich verschlüsselt?

Die Freifunk-Daten sollten über das VPN der jeweiligen Community gehen.

Test

Zugehörigkeit der IP-Adresse, unter der der eigene Rechner im Netz erscheint, überprüfen!

Test-Webseiten wie **utrace.de** zeigen Namen und Ort des jeweiligen eigenen Breitband-Anbieters an.

Was ist Freifunk?

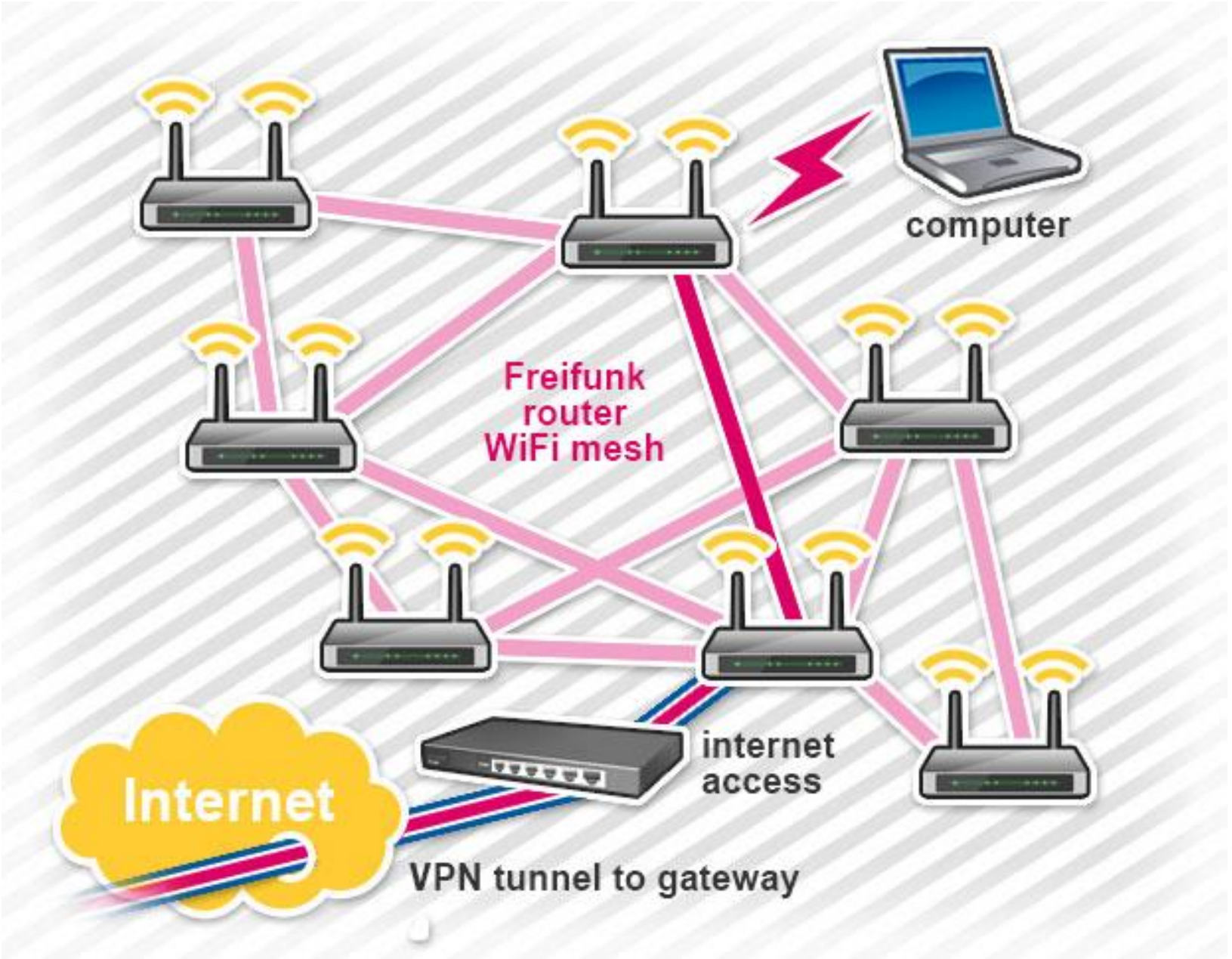
Freifunk ist eine nichtkommerzielle Initiative zum Aufbau freier (Funk-)Netzwerke.

Es geht darum eine stabile und unabhängige Infrastruktur für den **freien Datenverkehr** zu schaffen.

Nutzer stellen Ihren WLAN-Router für alle Beteiligten zur Verfügung

Die Freifunk-Zugangspunkte trennen das Freifunk-Netz vollständig vom privaten WLAN.

Freifunk-Struktur



Lokale Angebote

Freifunk funktioniert wie ein „lokales Internet“.

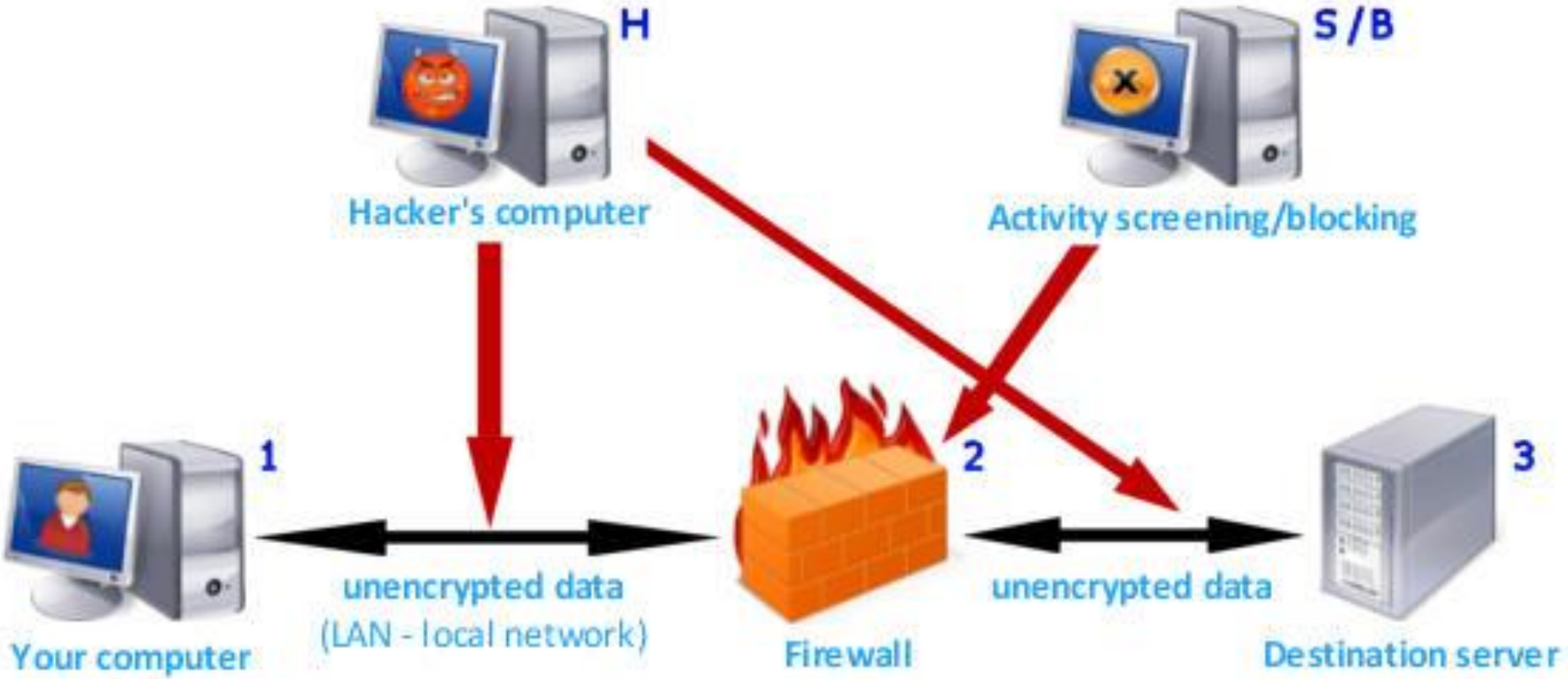
In diesem Netzwerk sind alle Angebote möglich, die wir auch aus dem „normalen“ Internet kennen.

Es können beispielsweise Nachrichtendienste, Soziale Netzwerke, Video- und Musikdatenbank und vieles mehr betrieben werden, ohne auf kommerzielle Anbieter angewiesen zu sein.

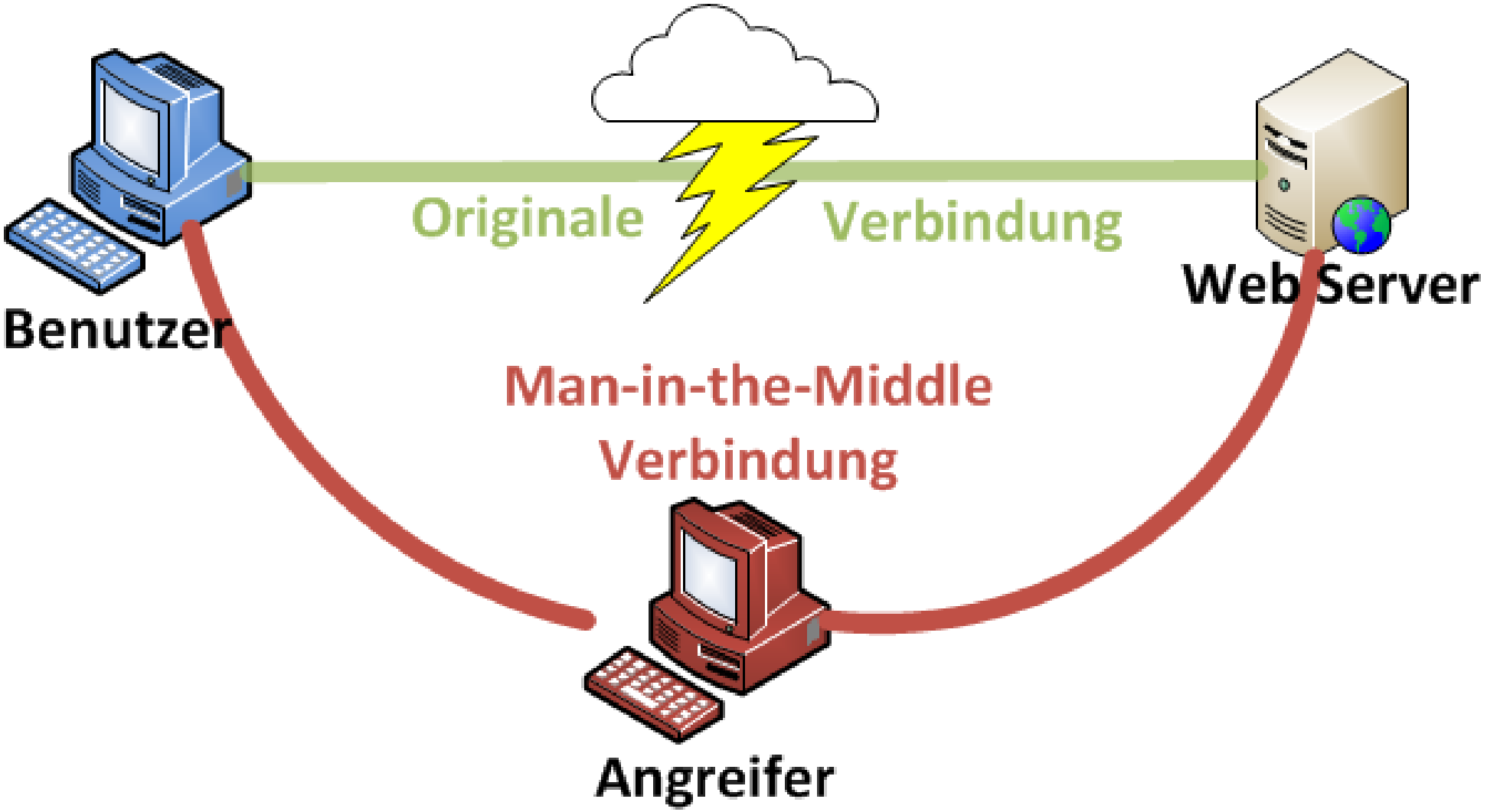
Angriffsmöglichkeiten

- Virusverteilung über das WLAN
- Sniffing
- Man-In-The-Middle-Angriff
- **Snarfing**: Informationsdiebstahl oder Datenmanipulation in kabellosen lokalen Netzwerken wie zum Beispiel in WLANs

Sniffing


H
Hacker's computer
S/B
Activity screening/blocking
1
Your computer
unencrypted data
(LAN - local network)
2
Firewall
unencrypted data
3
Destination server

Man-In-The-Middle-Angriff



Snarfing

In drahtlosen Netzen zunächst drahtlose Geräte aufspüren und dann versuchen, diese anzugreifen.

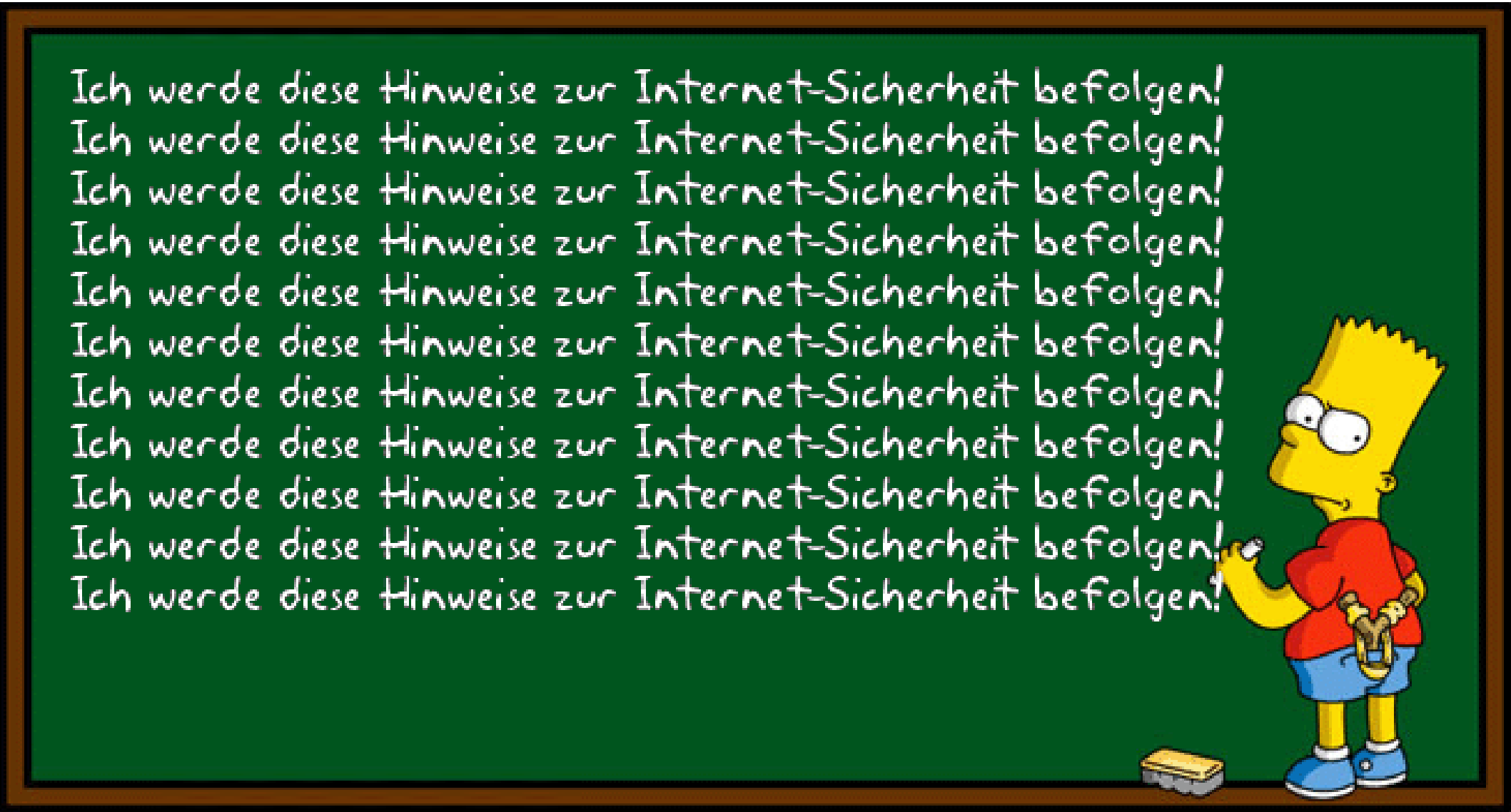
Möglich ist bei öffentlichen WLAN-Hotspots das Vortäuschen eines falschen WLAN-Access-Points.

Der falsche Access-Point leitet die Daten – nach Auswertung und gegebenenfalls Manipulation – zum korrekten Access-Point weiter.

Schutzmaßnahmen - Betreiber

- Firewall
- Grundlegende Netzkonfiguration
- Routerkonfiguration (werksseitige Passwörter, Verschlüsselung
- Schutz der Nutzer untereinander

Schutzmaßnahmen für Benutzer



Sicherheitstipps

Schalten Sie die WLAN-Funktion nur ein, wenn Sie diese benötigen!

Rufen Sie vertrauliche Daten über ein fremdes WLAN-Netz am besten nicht ab. (und wenn, dann HTTPS oder VPN nutzen)

Informieren Sie sich über das Sicherheitsniveau des Hotspots! (Verschlüsselung?)

Deaktivieren Sie die Datei- und Verzeichnisfreigaben.

Verschlüsseltes Surfen

Prüfen Sie vor dem Einloggen, mit welcher Technik das Netz verschlüsselt ist.

Aktueller Standard ist WPA2.

Virtuelles privates Netz (VPN)

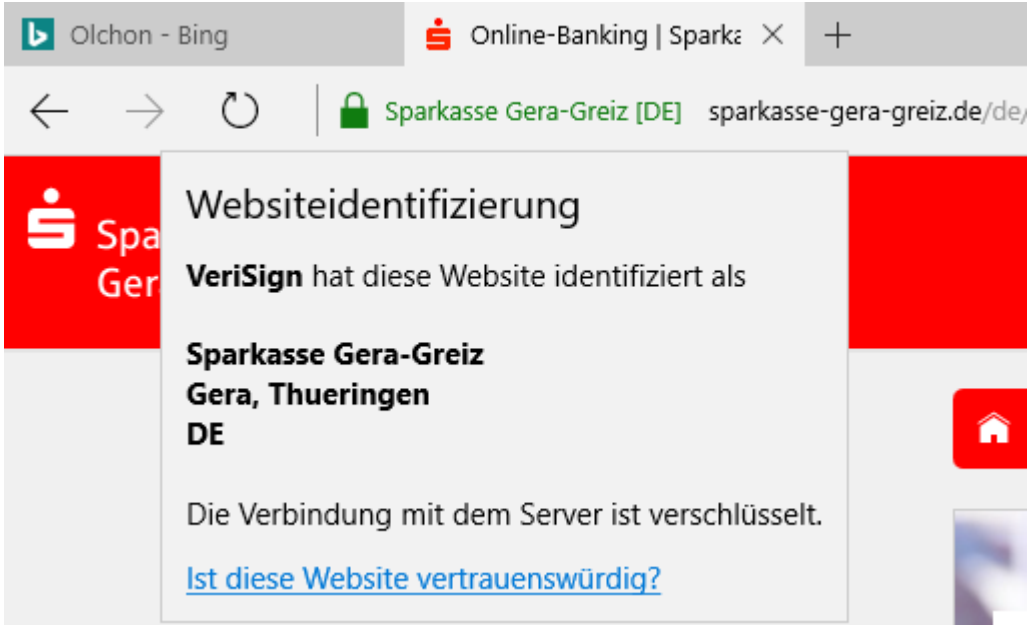
Installieren Sie zusätzlich ein Programm, das um den Computer ein virtuelles privates Netz (VPN) spannt.

Gratis gibt es z.B. ShellfireVPN und Hotspot Shield.

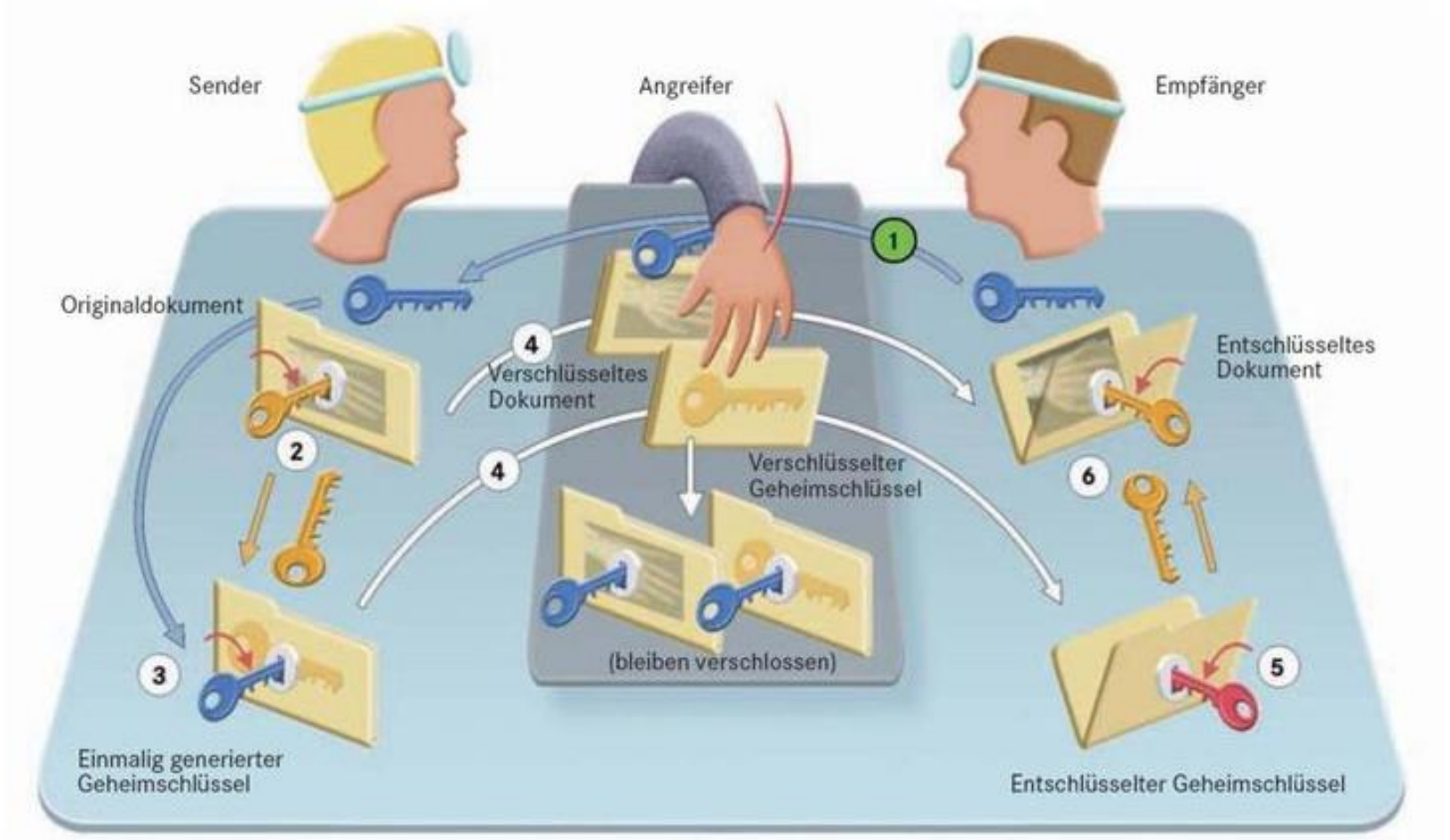
Diese Programme bauen zwischen dem eigenen PC und dem Internet eine geschützte Verbindung auf.

Sichere Websites

Nutzer sollten möglichst nur Seiten besuchen, die mit dem Kürzel „https“ beginnen statt mit dem weniger sicheren „http“.



Verschlüsselung bei https (Protokoll TLS, früher SSL)



Quelle: gematik 2009

Sichere E-Mail

Bei E-Mails gilt es zu beachten, dass die Verschlüsselungsmodi SSL oder TLS dauerhaft aktiviert sind (erkennbar am Vorhängeschloss-Symbol in der Adressleiste).

Regelmäßige Updates

Regelmäßige Sicherheitsupdates des Betriebssystems sind unerlässlich, um den eigenen Rechner oder das Smartphone sicher zu halten.

Kritischer Umgang mit dem Gerät

Die meisten Viren und andere Malware verbreiten sich immer noch über E-Mail, fragwürdige Download-Portale oder Trickbetrügereien z.B. über in Webseiten eingebettete Werbung.

Grundschutzkataloge des BSI

www.bsi.de

Bereich IT-Grundschutz

https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/FremdeWLAN/fremde_WLAN.html

Maßnahmen 4.176 und 5.160, 5.66, 5.177 zum Thema SSL/TLS

Fazit

- Offene Netze sind sehr beliebt, da sie Nutzer auch ohne mobiles Internet verbinden kann.
- Ein Sicherheitsrisiko besteht immer.
- Schutzmaßnahmen der Betreiber sind notwendig.
- Für die Sicherheit sind auch die Benutzerinnen und Benutzer verantwortlich!