Technische Universität Braunschweig

WLAN - aber sicher!

Tipps zur sicheren Konfiguration von WLAN auf mobilen Endgeräten

Sicherheit im WLAN - Agenda

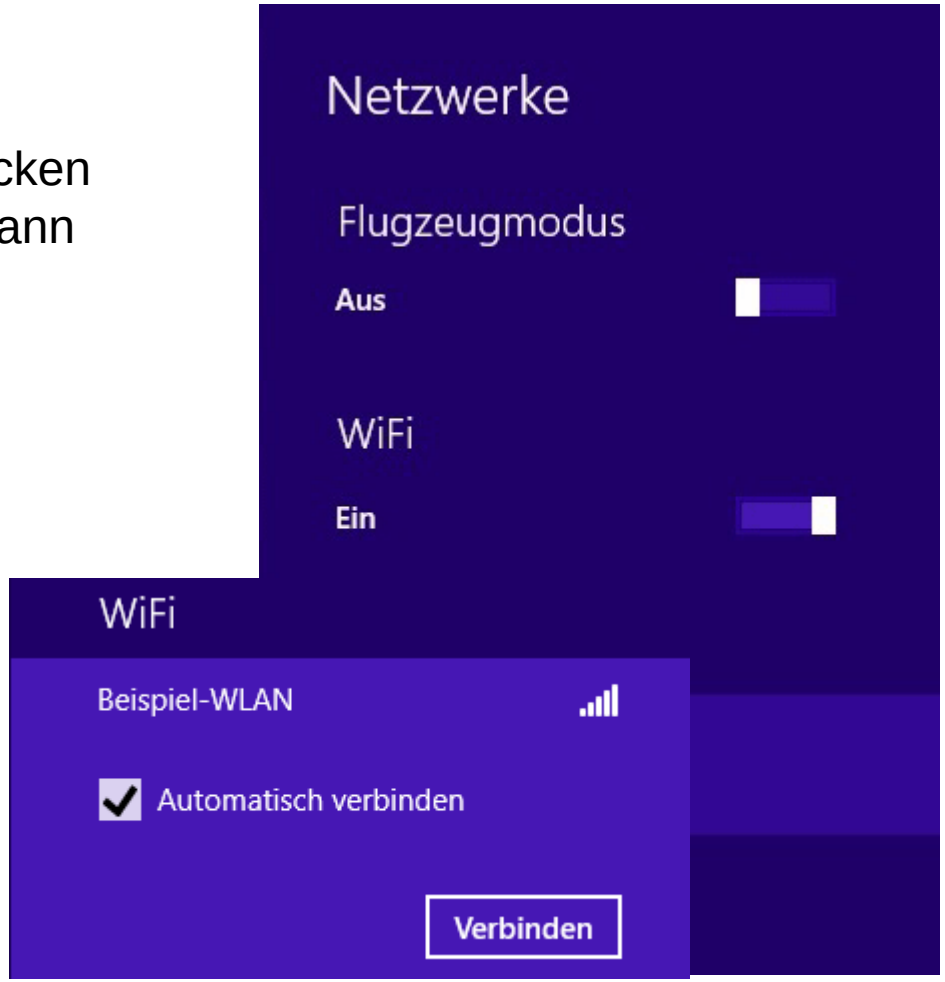
- WLAN automatisch verbinden
- Das „Schloss“
- Fazit, aber…
- Sicherheit im eduroam
- JoinNow – Installer und eduroam
- Ausblick Entwicklung WLAN
- Diskussion, Fragen

WLAN automatisch verbinden

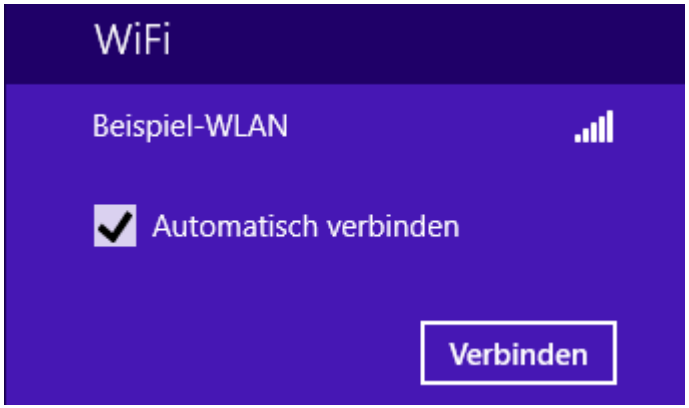
In der Liste der Drahtlosnetzwerke klicken Sie auf das gewünschte WLAN und dann auf „Verbinden“, um eine Verbindung aufzubauen.

Wenn das WLAN verschlüsselt ist, geben Sie den WLAN-Schlüssel ein.

Belassen Sie das Häkchen bei „Automatisch verbinden“.



WLAN automatisch verbinden



Kannste so machen...

WLAN automatisch verbinden ...ist dann aber $#§+^&#

Warum ist **„WLAN automatisch verbinden“** nicht gut?

Ihr Gerät sucht aktiv nach diesem WLAN und versucht sich mit ihm zu verbinden, wenn es erreichbar ist.

Genauer: Wenn ein **WLAN mit dem gleichen Namen** in Reichweite ist.

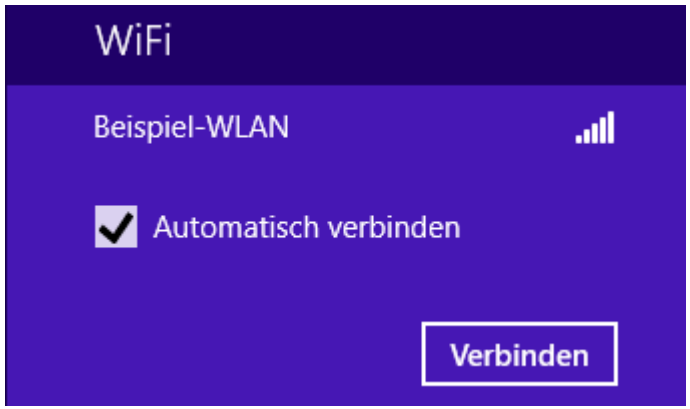
– Dies muss nicht „Ihr“ WLAN sein…

Andere können erfahren, wo Sie (überall) im WLAN waren und diese Information ausnutzen...

...wollen Sie das?

WLAN automatisch verbinden

… ist wie überall den Kopf reinstecken müssen



=

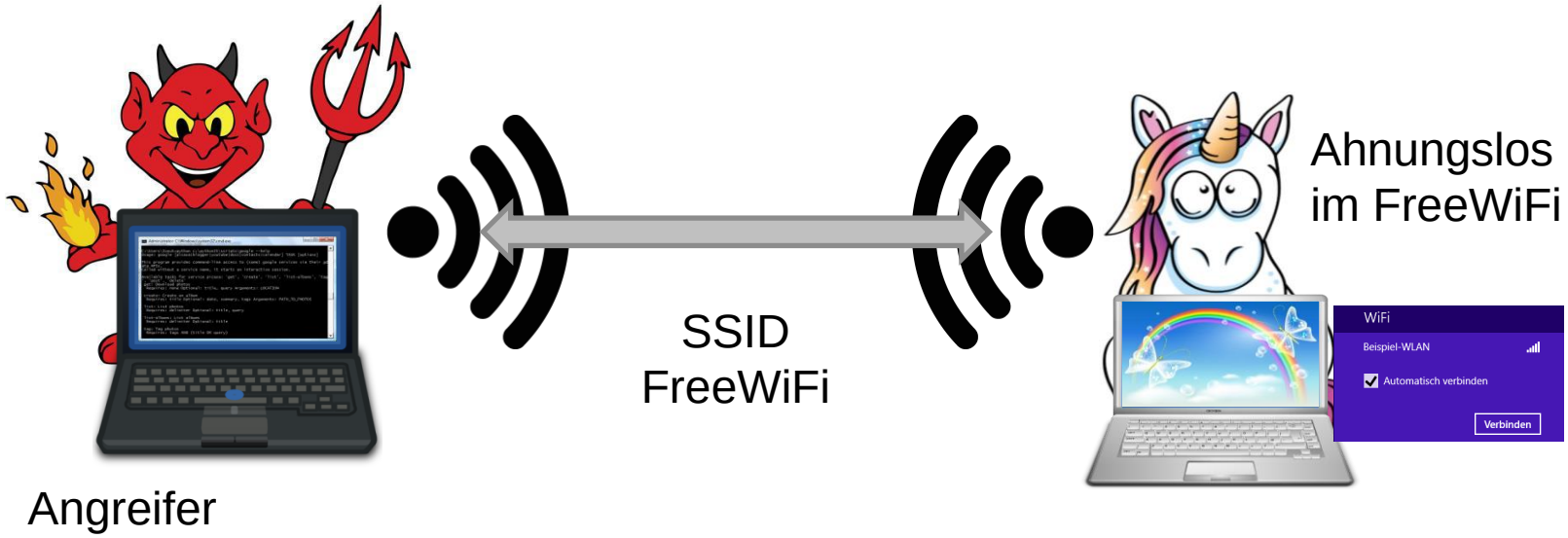
Jetzt zeigen wir Ihnen, was Dritte mit solchen Informationen machen können!

Evil Twin – mit „WLAN FakeAP“ Logins abgreifen

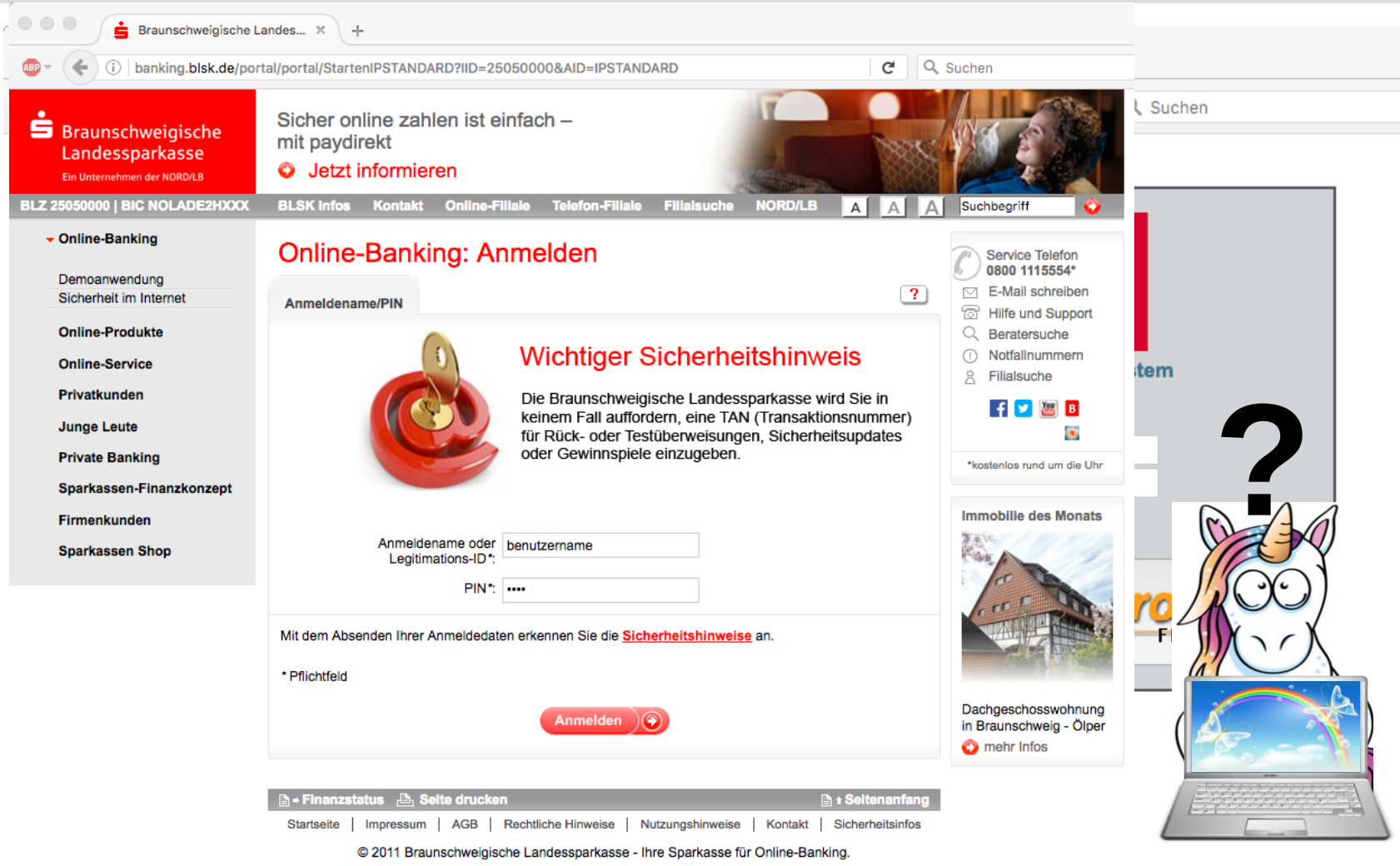
… Wie genau ein solcher Angriff funktioniert,

haben wir beim ECSM 2016 gezeigt …

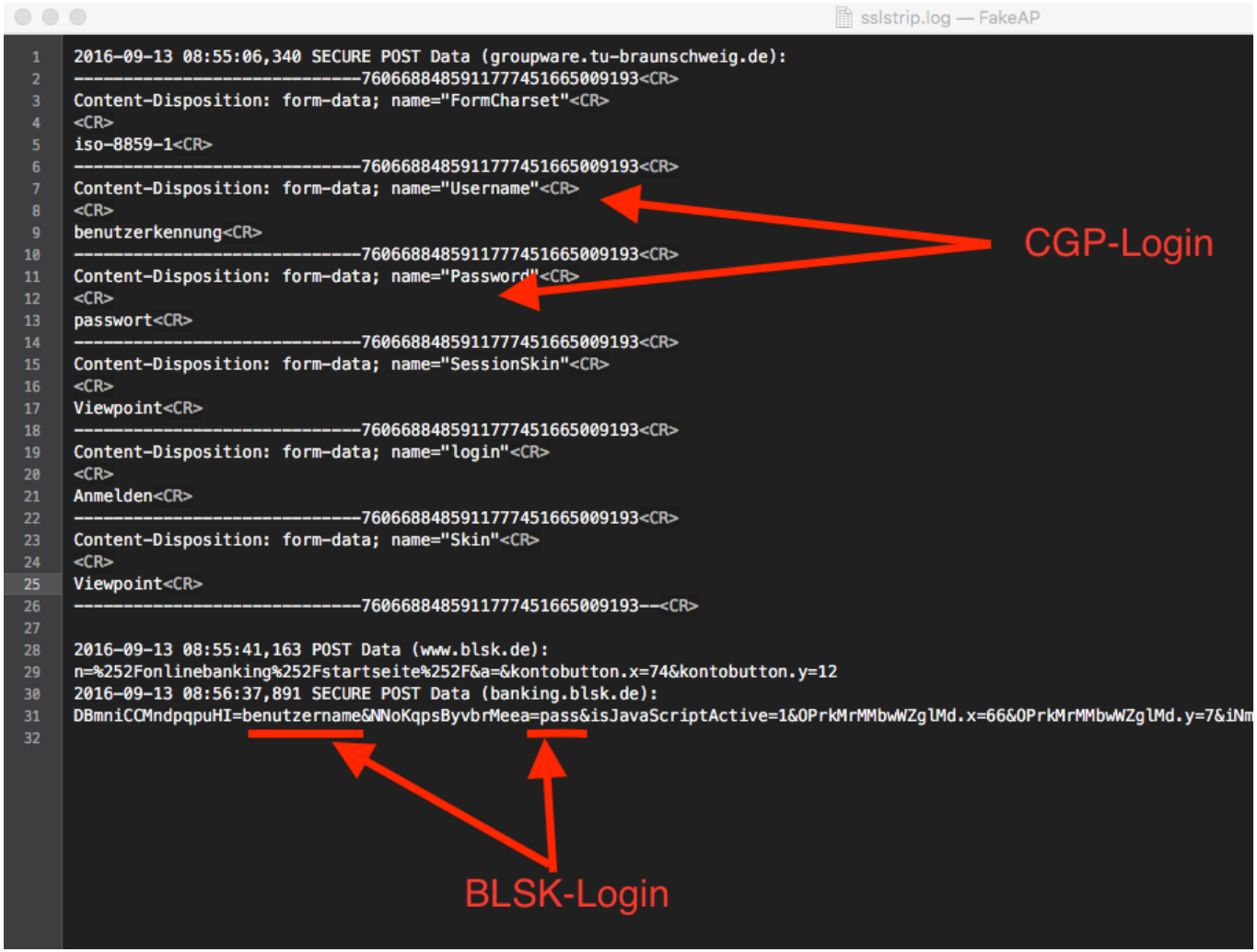
(Material online)



Evil Twin – mit „WLAN FakeAP“ Logins abgreifen



Evil Twin – mit „WLAN FakeAP“ Logins abgreifen



Kann mir nicht passen! Ich achte auf das Schloss!

Sicherheitshinweise für Webseiten und Policies zur IT-Sicherheit beinhalten oft Sätze wie:

„ … das Schloß verrät, dass die Seite sicher ist… „

„… achten Sie auf das Schloß …“

„… die Seite ist sicher, wenn das Schloß angezeigt wird …“

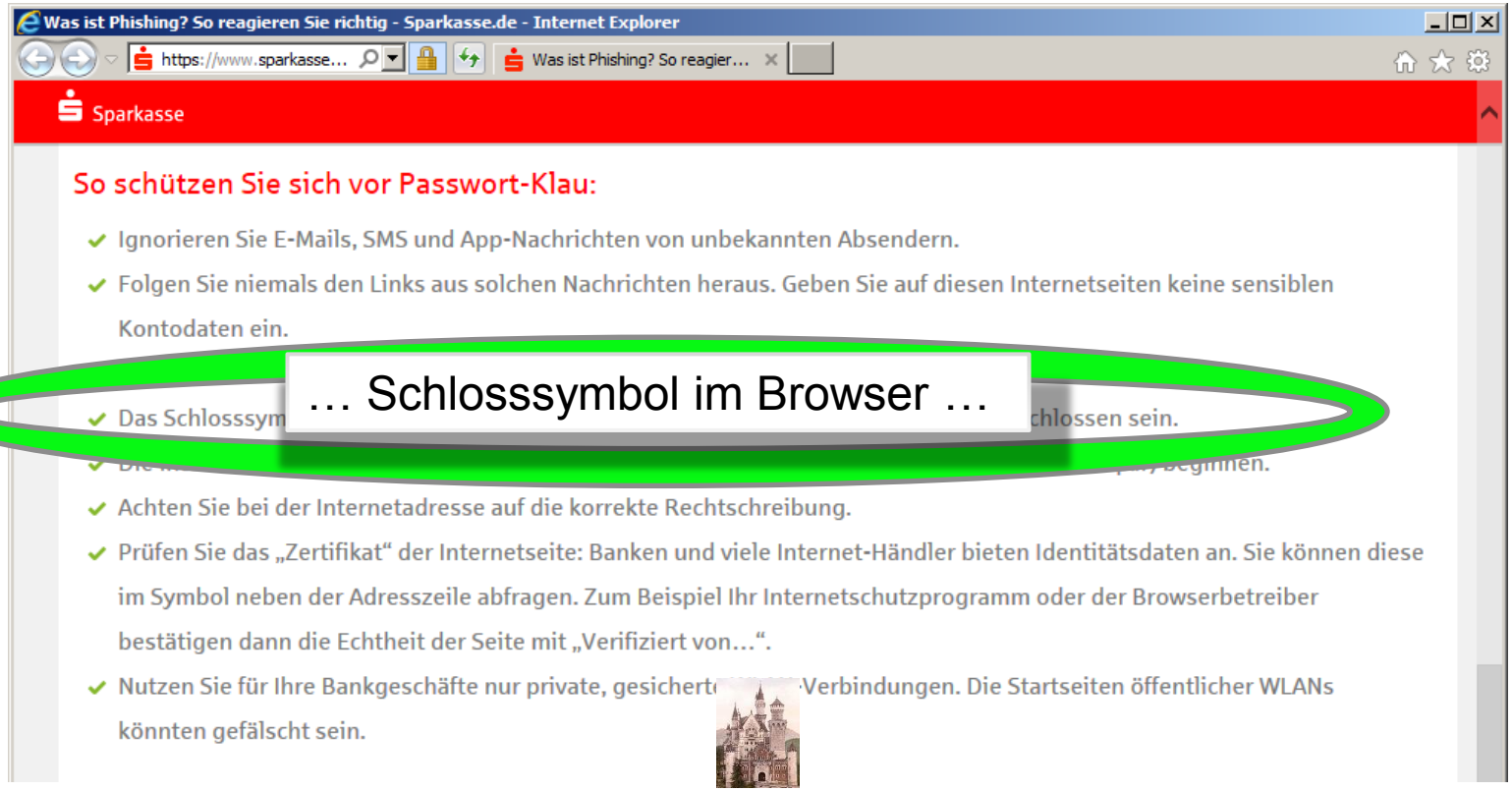
Achten Sie auf das Schloß…

Hätten Sie es bemerkt?

Hier der kleine aber entscheidende Unterschied...

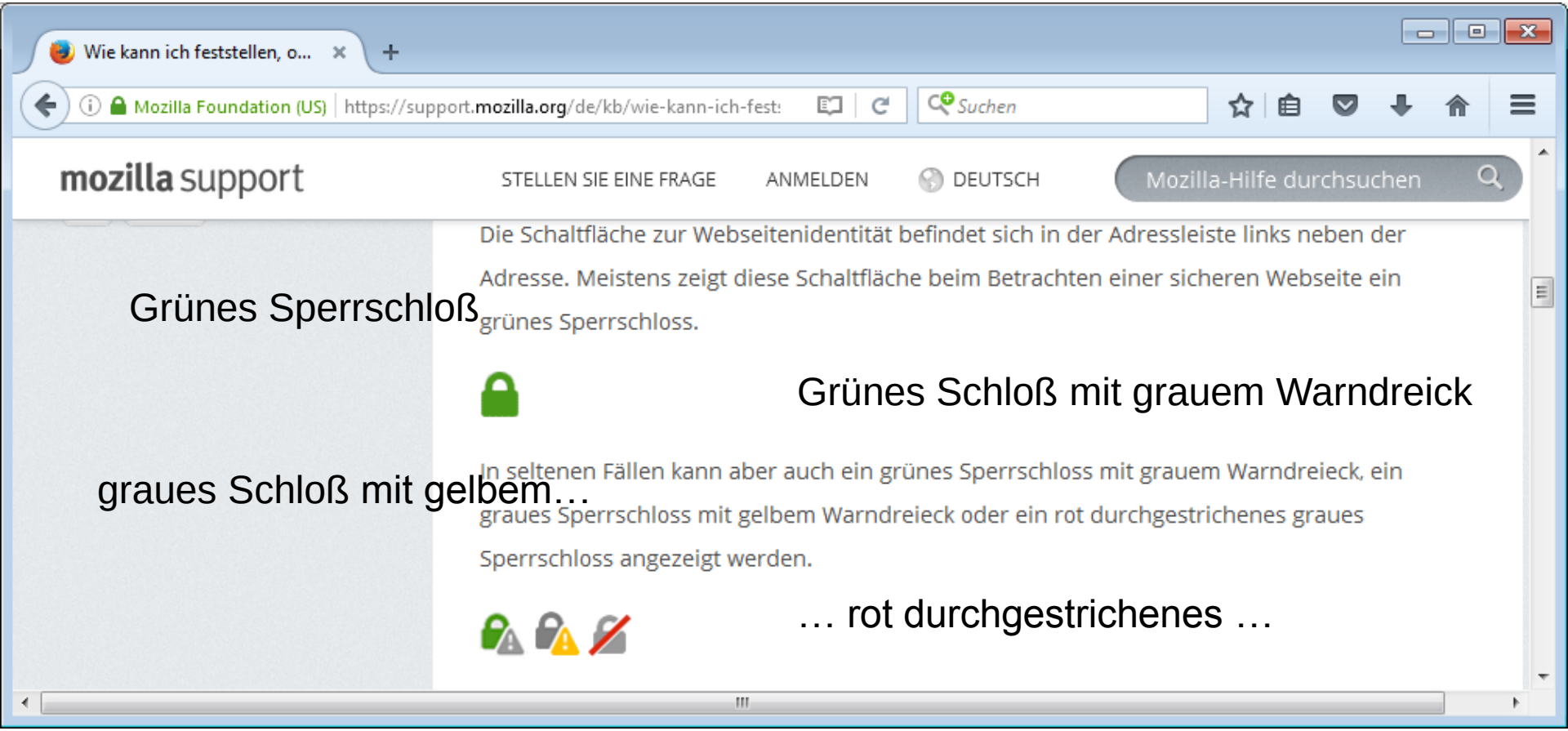
Achten Sie auf das Schloß…

IT-Sicherheitswebseiten der Sparkassen:



Achten Sie auf das Schloß…

Mozilla als Browserhersteller zum Schloß-Symbol:



Grünes Sperrschloß

Grünes Schloß mit grauem Warndreick

graues Schloß mit gelbem…

… rot durchgestrichenes …

Was Sie gelernt haben (sollten):

- „Automatisch Verbinden“
  – keine gute Idee,
  insbesondere bei freien WLANs,
  insbesondere bei „häufigen“ freien WLANs

- Eine verschlüsselte Verbindung im Browser sollten Sie als solche erkennen können

- Profitipp an Rande: WLAN kann man auch ausschalten, wenn man es nicht benötigt. Das schont sogar den Akku…

… eduroam

- **Sicherheit im eduroam?**

Betrifft mich nicht, ich nutze eduroam…

… und eduroam ist sicher:

„(…) Die lokale Zugangsauthentifizierungstechnologie (…) gewährleistet, dass Benutzerdaten und Passwörter auf dem gesamten Weg zur Heimatorganisation verschlüsselt werden (Ende-zu-Ende-Verschlüsselung).“

„(…) Diese Sicherheitsüberprüfung findet am Gerät des Benutzers selbst statt. (…) “

Quelle: Wikipedia & eduroam.org

… eduroam

- **Sicher?**
- **Wirklich?**

Was sagt der DFN-Verein als verantwortlicher Betreiber eduroam in Deutschland zur Sicherheit im eduroam?

Übergabe an Herrn Paffrath, DFN-Verein.

JoinNow – Konfigurationsportal

- **Nutzen Sie unseren JoinNow-Installer (Web-Portal)**
- **Automatisch korrekt gesetzte Einstellungen***
- **Erleichtert die (natürlich unwahrscheinliche ;-)) Fehlersuche**

Anleitung:

https://doku.rz.tu-bs.de/doku.php?id=netz:wlan:wlan_einrichten_plattformunabhaengig

***) betriebssystemabhängig (Android ist M!§#)**

Ausblick – Anstehende Änderungen im WLAN

- **Eduroam setzt korrekte Konfiguration voraus.**

  - Auswertungen (andernorts & hier) zeigen Herausforderung:

    Viele Geräte sind offenkundig von Hand konfiguriert

    (Android ist eine zusätzliche Herausforderung)

    - Anleitungen nutzen: intensiver kommunizieren
    - Konfigurationsparameter enger vorgeben

bedeutet: **Benutzer müssen WLAN neu konfigurieren. (1)**

Ausblick – Anstehende Änderungen im WLAN

- Umbau der Authentifizierungsserver im WLAN steht:

  - Passwortänderungen sind dann sofort gültig
    (via JoinNow konfiguriert: sofort, von Hand konfiguriert: erst z.T. nach einem Tag)
  - Vorbereiten alternativer Authentifizierungsverfahren im WLAN
    (derzeit: EAP-TTLS & PAP, optional MS-CHAPv2)
  - Beginn Einführung IPv6 (im WLAN)
    (stark steigende WLAN-Nutzung, derzeit bis ca. 10.000 gleichzeitige Clients)
  - Langfristig: Erhöhung der Sicherheit z.B. durch automatisierte Quarantäne bei Malware-Bedrohung möglich machen

bedeutet: **Benutzer müssen WLAN neu konfigurieren (2)**

Ausblick – Anstehende Änderungen im WLAN

- **Eduroam setzt Zertifikate zur Absicherung ein, aber:**
  - Wurzelzertifikat „Deutsche Telekom Root CA 2“ **läuft am 09. Juli 2019 ab**, Verlängerung nicht möglich.
  - Genau wie bei Webservern & abgelaufenen Zertifikaten: WLAN-Clients werden Verbindung verweigern.
  - **Tausch des Wurzelzertifikats** „Deutsche Telekom Root CA 2“ gegen Nachfolger „T-Telesec Global Root Class 2” (Gültigkeit bis 2033) **muss bis Juli 2019 umgesetzt sein.**

bedeutet: **Benutzer müssen WLAN neu konfigurieren. (3)**

Ausblick – Anstehende Änderungen im WLAN

- **In zeitlicher Abfolge stehen innerhalb von ca. 1,5 Jahren drei wichtige Maßnahmen im WLAN an:**
  - **Verbindlichere Konfiguration vorgeben**
    (betrifft Sicherheit: „sofort“)
  - **Authentifizierungs-Infrastruktur wird weiterentwickelt**
    („mittelfristig“)
  - **Wurzelzertifikat läuft Juli 2019 ab & Tausch steht an**
    (bis 09. Juli 2019)

Forderung:
Benutzer sollen **WLAN nicht 3x neu konfigurieren** müssen.

Alle 3 Maßnahmen an einem Termin durchführen.

Zielzeit voraussichtlich: Februar/März 2018

Vielen Dank für Ihre Aufmerksamkeit

Fragen, Wünsche, Anregungen

können Sie jetzt mit uns teilen
oder schreiben Sie an:

noc@tu-braunschweig.de