



Technische
Universität
Braunschweig



WLAN - aber sicher!

Tipps zur sicheren Konfiguration von WLAN auf mobilen Endgeräten

Sicherheit im WLAN - Agenda

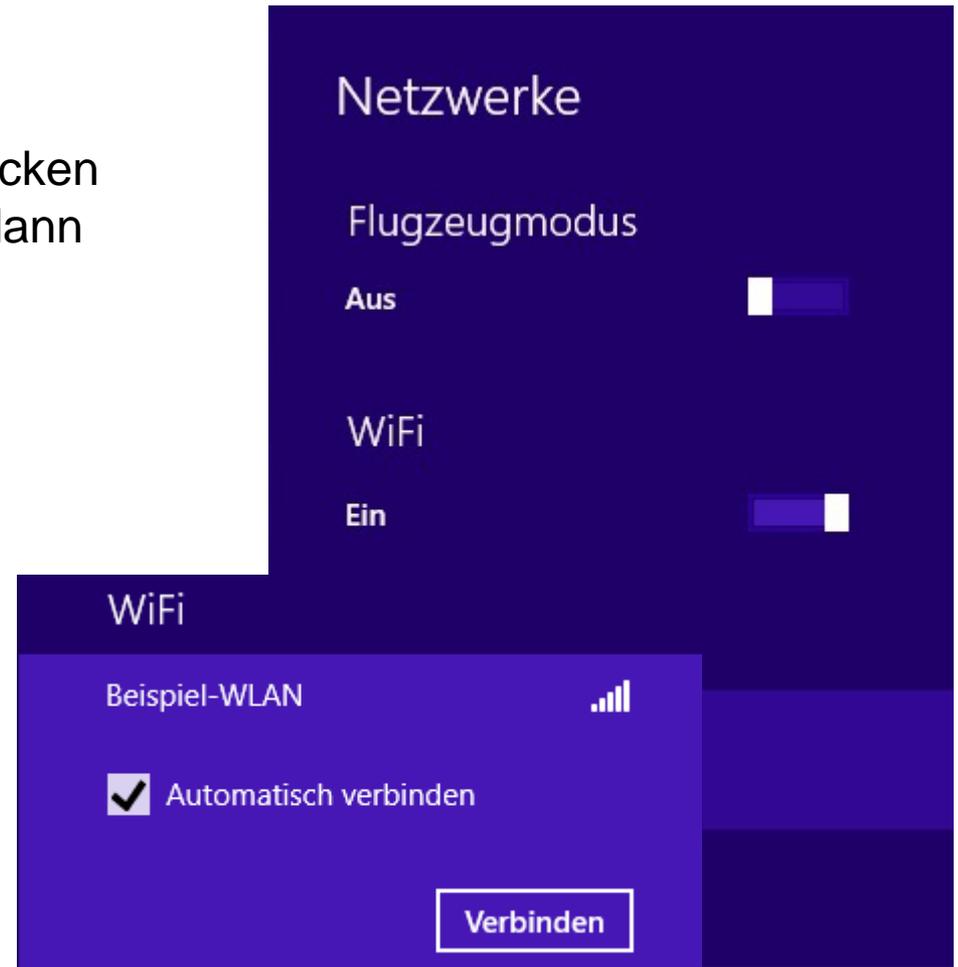
- **WLAN automatisch verbinden**
- **Das „Schloss“**
- **Fazit, aber...**
- **Sicherheit im eduroam**
- **JoinNow – Installer und eduroam**
- **Ausblick Entwicklung WLAN**
- **Diskussion, Fragen**

WLAN automatisch verbinden

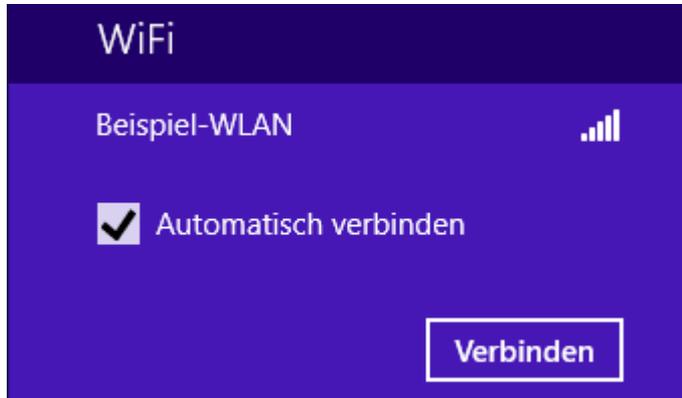
In der Liste der Drahtlosnetzwerke klicken Sie auf das gewünschte WLAN und dann auf „Verbinden“, um eine Verbindung aufzubauen.

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 $\$ \# \S + ^ \& \#$

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.

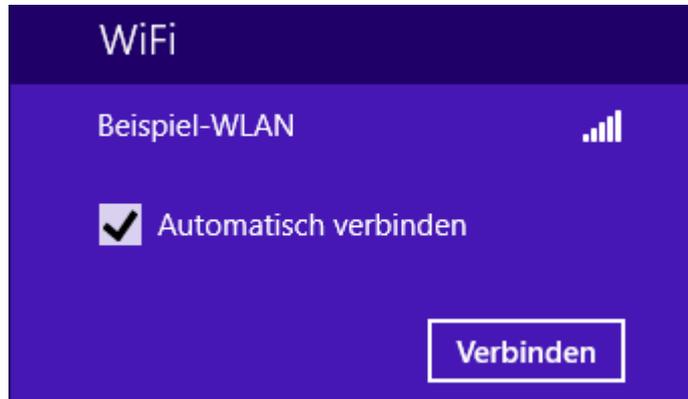
– Dies muss nicht „Ihr“ WLAN sein...

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



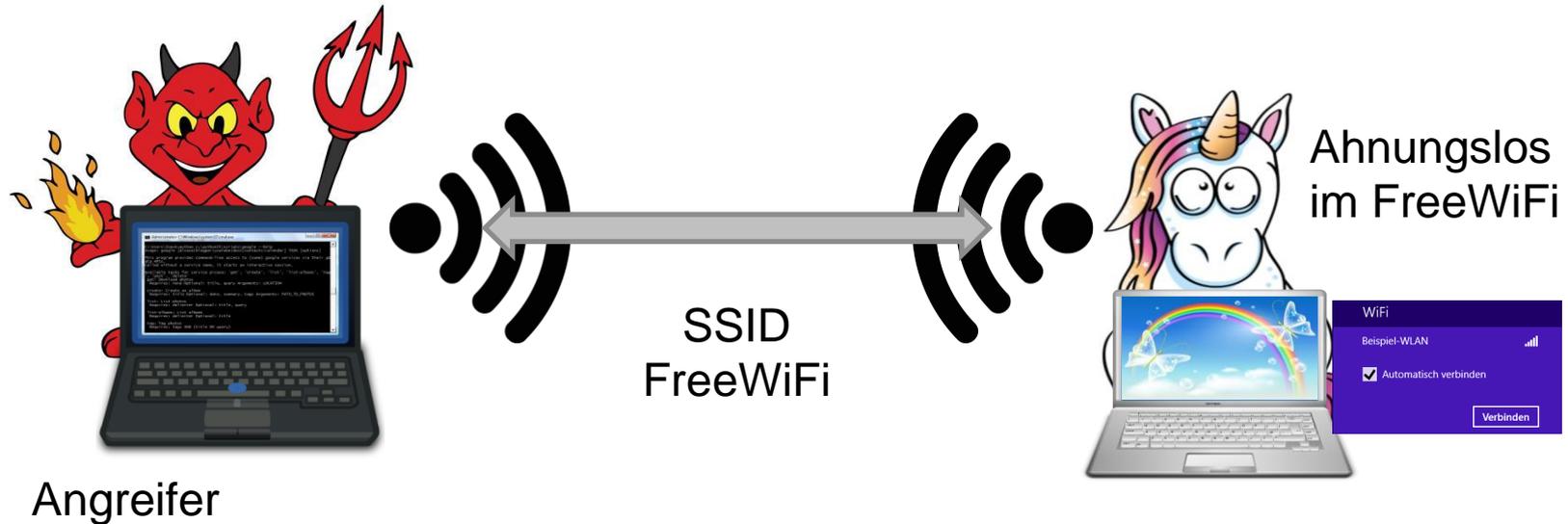
=



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

ABP Braunschweigische Landes... x +

banking.blsk.de/portal/portal/StartenIPSTANDARD?IID=25050000&AID=IPSTANDARD

Suchen

Suchen

BLZ 25050000 | BIC NOLADE2HXXX

BLSK Infos Kontakt Online-Filliale Telefon-Filliale Filialsuche NORD/LB

Suchbegriff

Online-Banking

Demoanwendung Sicherheit im Internet

Online-Produkte

Online-Service

Privatkunden

Junge Leute

Private Banking

Sparkassen-Finanzkonzept

Firmenkunden

Sparkassen Shop

Online-Banking: Anmelden

Anmeldename/PIN

Wichtiger Sicherheitshinweis

Die Braunschweigische Landessparkasse wird Sie in keinem Fall auffordern, eine TAN (Transaktionsnummer) für Rück- oder Testüberweisungen, Sicherheitsupdates oder Gewinnspiele einzugeben.

Anmeldename oder Legitimations-ID*:

PIN*:

Mit dem Absenden Ihrer Anmeldedaten erkennen Sie die **Sicherheitshinweise** an.

* Pflichtfeld

Anmelden

Service Telefon 0800 1115554*

E-Mail schreiben

Hilfe und Support

Beratersuche

Notfallnummern

Filialsuche

*kostenlos rund um die Uhr

Immobilie des Monats

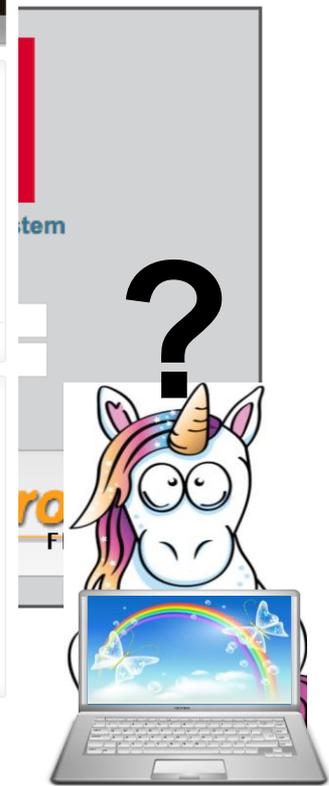
Dachgeschosswohnung in Braunschweig - Ölper

mehr Infos

Finanzstatus Seite drucken Seitenanfang

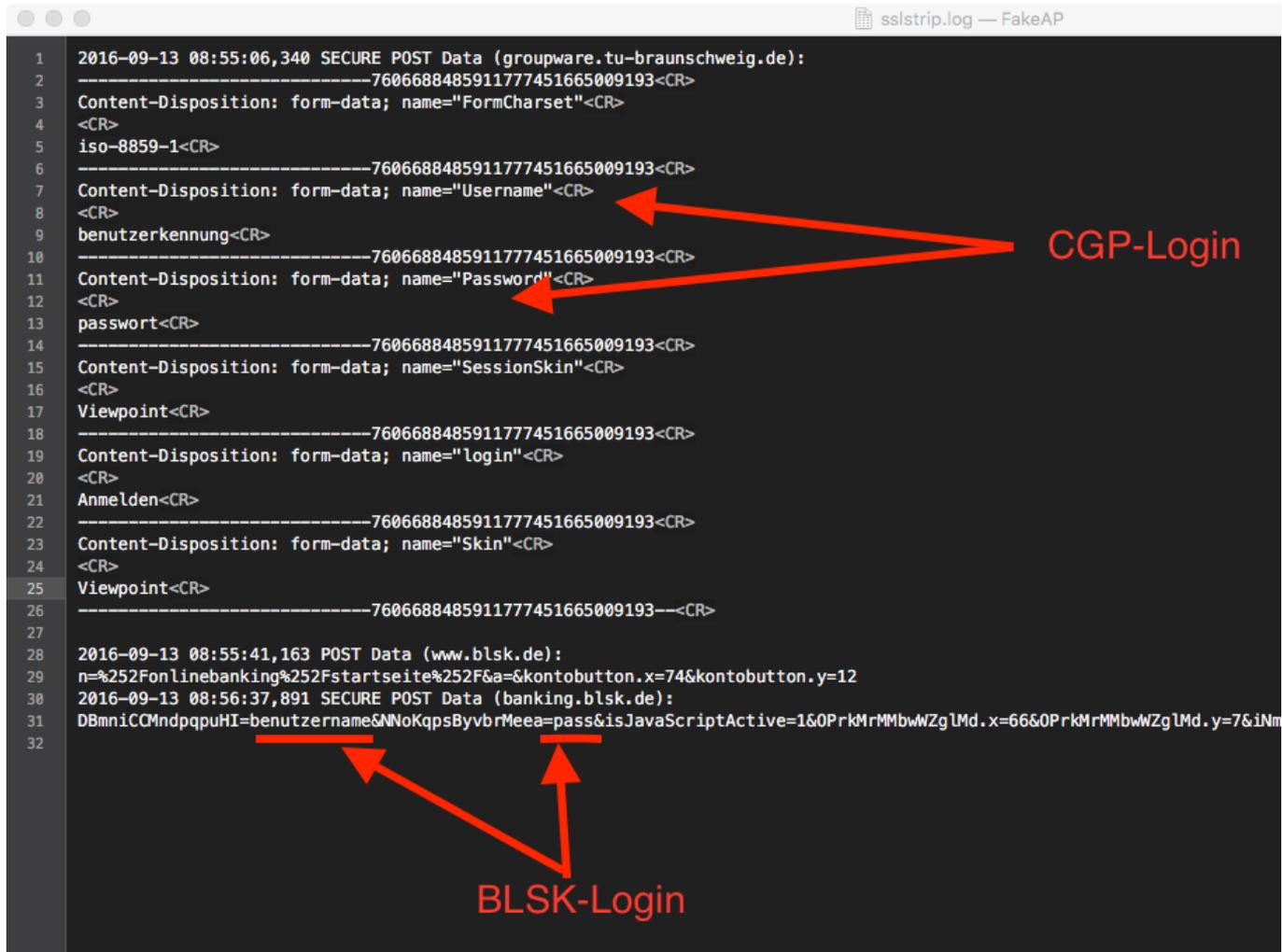
Startseite | Impressum | AGB | Rechtliche Hinweise | Nutzungshinweise | Kontakt | Sicherheitsinfos

© 2011 Braunschweigische Landessparkasse - Ihre Sparkasse für Online-Banking.



Evil Twin – mit „WLAN FakeAP“ Logins abgreifen

```
sslstrip.log — FakeAP
1 2016-09-13 08:55:06,340 SECURE POST Data (groupware.tu-braunschweig.de):
2 -----7606688485911777451665009193<CR>
3 Content-Disposition: form-data; name="FormCharset"<CR>
4 <CR>
5 iso-8859-1<CR>
6 -----7606688485911777451665009193<CR>
7 Content-Disposition: form-data; name="Username"<CR>
8 <CR>
9 benutzerkennung<CR>
10 -----7606688485911777451665009193<CR>
11 Content-Disposition: form-data; name="Password"<CR>
12 <CR>
13 passwort<CR>
14 -----7606688485911777451665009193<CR>
15 Content-Disposition: form-data; name="SessionSkin"<CR>
16 <CR>
17 Viewpoint<CR>
18 -----7606688485911777451665009193<CR>
19 Content-Disposition: form-data; name="login"<CR>
20 <CR>
21 Anmelden<CR>
22 -----7606688485911777451665009193<CR>
23 Content-Disposition: form-data; name="Skin"<CR>
24 <CR>
25 Viewpoint<CR>
26 -----7606688485911777451665009193--<CR>
27
28 2016-09-13 08:55:41,163 POST Data (www.blsk.de):
29 n=%252Fonlinebanking%252Fstartseite%252F&a=&kontobutton.x=74&kontobutton.y=12
30 2016-09-13 08:56:37,891 SECURE POST Data (banking.blsk.de):
31 DBmniCCMndpquHI=benutzername&NNoKqpsByvbrMeea=pass&isJavaScriptActive=1&OPrkMrMMbwZgLMd.x=66&OPrkMrMMbwZgLMd.y=7&iNm
32
```



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?

The screenshot shows a web browser window with the URL `www.blsk.de/online-produkte/oph/index.php?n=%2Fonline-produkte%2Foph%2F`. The page header features the Braunschweigische Landessparkasse logo and navigation links: BLZ 25050000 | BIC NOLADE2HXXX, BLSK Infos, Kontakt, Online-Filiale, Telefon-Filiale, Filialsuche, and a search bar. A sidebar on the left contains a dropdown menu for 'Online-Banking' with options: 'direkt zu: - Bitte auswählen -', 'Anmelden', 'Demoanwendung', 'Sicherheit im Internet', and 'Alle Angebote'. The main content area displays the text: 'Sicher online zahlen ist einfach – mit paydirekt' and 'Jetzt informieren'. Below this, the text 'Sparkassen-Privatkredit' and 'Lächeln ist einfach.' is prominently displayed in red.

Hier der kleine aber entscheidende Unterschied...

Internet-Filiale - Braunschweig x

Norddeutsche Landesbank - Girozentrale - [DE] | <https://www.blsk.de/online-produkte/oph/index.php?n=%2Fonline-produkte%2Foph%2F>

Braunschweigische Landessparkasse
Ein Unternehmen der NORD/LB

Sicher online zahlen ist einfach – mit paydirekt
[Jetzt informieren](#)

BLZ 25050000 | BIC NOLADE2HXXX | BLSK Infos | Kontakt | Online-Filiale | Telefon-Filiale | Filialsuche | NORD/LB | Suchbegriff

▼ Online-Banking
direkt zu:
- Bitte auswählen - ▼

[Anmelden](#)

Demoanwendung
Sicherheit im Internet

► Alle Angebote

Stecken Sie beim Thema Vorsorge nicht den Kopf in den Sand.

Sprechen Sie mit uns!



Achten Sie auf das Schloß...

IT-Sicherheitswebseiten der Sparkassen:

Was ist Phishing? So reagieren Sie richtig - Sparkasse.de - Internet Explorer

https://www.sparkasse... Was ist Phishing? So reagier...

Sparkasse

So schützen Sie sich vor Passwort-Klau:

- ✓ Ignorieren Sie E-Mails, SMS und App-Nachrichten von unbekanntem Absendern.
- ✓ Folgen Sie niemals den Links aus solchen Nachrichten heraus. Geben Sie auf diesen Internetseiten keine sensiblen Kontodaten ein.
- ✓ Das Schlosssymbol ... geschlossen sein.
- ✓ Die ... beginnen.
- ✓ Achten Sie bei der Internetadresse auf die korrekte Rechtschreibung.
- ✓ Prüfen Sie das „Zertifikat“ der Internetseite: Banken und viele Internet-Händler bieten Identitätsdaten an. Sie können diese im Symbol neben der Adresszeile abfragen. Zum Beispiel Ihr Internetschutzprogramm oder der Browserbetreiber bestätigen dann die Echtheit der Seite mit „Verifiziert von...“.
- ✓ Nutzen Sie für Ihre Bankgeschäfte nur private, gesicherte Verbindungen. Die Startseiten öffentlicher WLANs könnten gefälscht sein.

Achten Sie auf das Schloß...

Mozilla als Browserhersteller zum Schloß-Symbol:

The screenshot shows a Mozilla Support page in German. The browser's address bar displays the URL [https://support.mozilla.org/de/kb/wie-kann-ich-feststellen, o...](https://support.mozilla.org/de/kb/wie-kann-ich-feststellen,-o...). The page content includes a search bar and a main article about web page identity. Annotations are overlaid on the page:

- Grünes Sperrschloß**: Points to the green lock icon in the address bar.
- gräues Schloß mit gelbem...**: Points to the grey lock icon with a yellow warning triangle.
- Grünes Schloß mit grauem Warndreieck**: Points to the green lock icon with a grey warning triangle.
- ... rot durchgestrichenes ...**: Points to the red-striking grey lock icon.

The page text explains that the lock icon is located in the address bar and usually shows a green lock for secure sites. It also notes that in rare cases, other lock symbols (grey with yellow or grey warning triangles, or red-striking) may appear.

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

Category	Event Type	Description	First Seen	Last Seen
Exploit Kit	Intrusion Event - exploit-kit	The host may have encountered an exploit kit	2013-09-17 16:46:28	2013-09-20 06:35:31
Security Information System (SIS) detected suspicious activity	Intrusion Event - sis-detected-suspicious-activity	The host may have encountered suspicious activity	2013-09-17 16:46:28	2013-09-20 06:35:31
CnC Connected	Intrusion Event - malware-cnc	The host may be under remote control	2013-09-17 20:09:23	2013-09-19 17:32:49

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