UNIVERSITÄT BAYREUTH

IT-SERVICEZENTRUM
Wir kümmern uns.

Redaktion: Ariadne Engelbrecht
Stand: Dezember 2016

News 16/04

# BayernWLAN@Uni Bayreuth

## BayernWLAN

Die Uni Bayreuth strahlt ab sofort das öffentliche WLAN-Netzwerk mit der SSID "@BayernWLAN" auf ihren Accesspoints aus. Aber was ist dieses BayernWLAN überhaupt, wie funktioniert es und welche Vorteile hat es gegenüber anderen Internetmöglichkeiten an der Uni Bayreuth – wie etwa unser eduroam?

### Was ist BayernWLAN?

"Der Freistaat Bayern plant bis Ende 2020 BayernWLAN an 20.000 Hotspots zur Verfügung zu stellen. Sie stellen der Öffentlichkeit einen Internetzugang über WLAN zur Verfügung und können völlig kostenlos genutzt werden."[1)]

An der Uni Bayreuth läuft BayernWLAN seit 15.11.2016 auf rund 340 Accesspoints (inkl. Außenstellen) und ist somit überall dort erreichbar, wo auch eduroam zur Verfügung steht.

Wir strahlen BayernWLAN nur aus – der Provider dahinter ist Vodafone im Auftrag der Staatsregierung. Es besteht ein eigener Uplink zu Vodafone, d.h. der generierte Datentraffic geht nicht ins Wissenschaftsnetz wie der Uni-Traffic.

### Eduroam ist doch ganz ok, warum also überhaupt BayernWLAN nutzen?

Zuerst muss gesagt sein, dass eduroam aus Sicherheitsgründen für uns Universitätsangehörige dem BayernWLAN klar zu bevorzugen ist, da eduroam verschlüsselt ist und BayernWLAN nicht.

Eduroam ist für uns eine Möglichkeit ins Internet zu kommen und für diejenigen, deren jeweilige Heimatinstitution eduroam ebenfalls unterstützt. Bekommen wir aber Gäste, wurde es bislang aufwändig – etwa bei Tagungen oder Veranstaltungen.

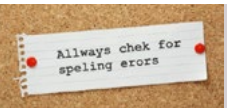
Der Internetzugang auf Tagungen an der Uni Bayreuth wird mit BayernWLAN stark erleichtert. Statt sich wie bisher Kennungen von uns generieren zu lassen, die die externen wlanubtteilnehmenden ohne eduroam-Zugang hier bislang benötigten, kann sich jetzt JEDER und JEDE einfach ins BayernWLAN einloggen.

### Sicherheit?

Bitte bedenken Sie: BayernWLAN ist ein **öffentlicher, unverschlüsselter** Internetzugang über WLAN, d.h. sorgloses Surfen ist nicht möglich.

---

1) BayernWLAN – **FAQs**: https://forum.vodafone.de/t5/Bayern-WLAN/Bayern-WLAN-FAQ/td-p/1296744. (Stand: 24.11.2016)



Aber zumindest sorgen*armes* Surfen ist möglich, sofern Sie dabei die folgenden Stichpunkte, die das Bundesamt für Sicherheit in der Informationstechnik BSI für Bürger zusammengestellt hat, beherzigen:

- √ *Schalten Sie die WLAN-Funktion nur ein, wenn Sie diese benötigen*
- √ *Rufen Sie vertrauliche Daten über ein fremdes WLAN-Netz am besten nie ab (►Dies gilt auch für das bayernWLAN)*
- √ *Informieren Sie sich über das Sicherheitsniveau des jeweiligen Hotspots*
- √ *Deaktivieren Sie die Datei- und Verzeichnisfreigaben Ihres Geräts*
- √ *Deaktivieren Sie nach Möglichkeit die automatische Anmeldung an bekannten Hotspots*

Noch Fragen? Hier finden Sie detaillierte Erklärungen & hilfreiche Tipps für diese Punkte!

**Wie funktioniert der Login?**

1. **Mit dem WLAN-Netz @BayernWLAN verbinden.**
2. Sofern sich die Startseite des BayernWLAN nicht automatisch öffnet: **Eine beliebige http-Webseite im Browser öffnen, nicht https.** z.B. http://www.its.uni-bayreuth.de
3. **Nutzungsbedingungen auf der Startseite des Hotspots durch einen Klick auf „Verbinden" akzeptieren** (vgl. **Abb. 2**).

**Abb. 2: BayernWLAN**

Wichtig: Für Verbindung mit der UBT ist ggf. ein VPN-Tunnel "Outside" notwendig.

Da das IT-Servicezentrum weder juristisch, noch technisch für den Betrieb des BayernWLANs verantwortlich ist, wenden Sie sich bitte bei BayernWLAN-spezifischen Fragen oder Problemen an die von der Landesregierung zur Verfügung gestellte Hotline: **0800 6648386**.

## Rund um BayernWLAN:

» ***BayernWLAN FAQs* von vodafone**
» ***Ein Übersichtsplan der Accesspoints in Bayern***

### Zum Jahreswechsel wird das Netzwerk *wlanubt* abgeschalten

Die somit frei gewordenen IP-Adressen werden dem eduroam-Adressraum zugeordnet, damit sich mehr Teilnehmende als bisher gleichzeitig in eduroam einwählen können. Wenden Sie sich bei Fragen bitte an die ITS-Anlaufstelle/✆3003.

## Das Live-Hacking Event 2016

Am 24.11.2016 waren **Hacker** der Firma *consectra* an der Uni Bayreuth zu Besuch – ohne schwarzem Hoodie, dafür in Hemd und Anzughose; quasi hackende Jedermänner.


**Abb. 1: Hacking Day – Hacker der Firma consectra**

Genau darin läge auch die Gefahr laut *consectra*, nämlich der Einschätzung, dass Hacker vereinzelt seien, obskure, dunkle Typen, die in irgendwelchen Kellern ihrem persönlichen Hacker-Hobby nachgingen. Das ist so aber nicht ganz richtig, denn jedermann und jede Frau kann mit Hilfe von Software hacken und es gibt auch schlipstragende professionelle Hacker. Sie sehen also, die Gruppe an Menschen, vor denen wir uns schützen wollen, ist größer und vielfältiger als stereotyp gedacht. ***Deshalb: Seien Sie digital wachsam!***

Stellen Sie sich ein Haus mit ganz vielen Türen vor – eine für den Pizzamann, eine für den Ehegatten, eine für DHL, eine für die Schwiegerleute, … Wenn Sie die Firewall an Ihrem Rechner ausgeschalten haben, stehen alle Türen gleichzeitig offen. Ihre Firewall muss angeschalten sein, denn Sie müssen die Kontrolle darüber haben, welche Türen (s.g. Ports) Sie für was, öffnen wollen. ***Deshalb: Lassen Sie Ihre Firewall immer an!***

Und was machen Sie, wenn Sie nach dem Urlaub oder ein paar Tagen Absenz wieder "nach Hause kommen"? Nicht die Fenster zum Lüften öffnen, zumindest nicht an Ihrem Rechner! Sie schicken die Putzkolonne vor. Diese ist Ihr aktualisierter Virenscanner, der einen Scan durchführt und ggf. Schädlinge bereinigt. Aktualisieren Ihres Virenscanners ist deshalb so wichtig, da dabei die hinterlegte Virendatenbank des Virenscanners auf Stand gebracht wird. Bereits eine minimale Änderung im Code eines Virus, kann ihn als "neuen" Virus für Ihren Virenscanner (ca. 400 000 pro Tag!) erscheinen lassen, den ein nicht-aktualisierter Virenscanner nicht mehr erkennt. ***Deshalb: aktualisieren Sie Ihren Virenscanner.***

Die zweite Verteidigungslinie nach der Firewall ist ein aktualisiertes Betriebssystem. Updates sind sehr wichtig für das Schließen von Sicherheitslücken. Wenn Sie also das nächste Mal eine Liste von 35 Betriebssystem-Updates sehen, installieren Sie diese Updates, denn es gibt auch Leute, die diese Liste sehen und damit eine Hitliste der aktuellen "Einsteigemöglichkeiten" in Ihren Rechner vor sich haben! ***Deshalb: Aktualisieren Sie Ihr Betriebssystem.***

Wussten Sie eigentlich, dass wir alle im Fokus von Cyberangriffen sind? Selbst die kleinsten Rädchen im Getriebe einer Institution oder Firma sind Angriffsziel. Nicht, weil der Beschäftigte X eine Sicherheitsfreigabe auf sensible Daten besitzt, sondern wegen der resultierenden Schlagzeile wie etwa "Uni Bayreuth/das Pentagon/Yahoo wurde Opfer von Cyberangriffen" – vollkommen egal, was dabei an Daten überhaupt erbeutet wurde oder nicht. ***Deshalb: Schützen Sie bitte sich und uns.***

Was wir noch von den Hackern lernen durften: Auf der Rangliste der gefährlichsten Seiten im Netz kommen Blogs und Web Kommunikation aktuell auf stolze 19,8% – das wiederum kam offenbar für viele im Saal überraschend. Es gibt nämlich nicht nur harmlose Blogs und sichere E-Mails, auch wenn sie vermeintlich von Freunden (Absender-E-Mailadresse beachten!) kommen. Klicken Sie deshalb bitte nur die Links in E-Mails an, die Sie angefordert haben. Falls Ihnen etwas suspekt vorkommt, fragen Sie beim Absender vor dem Klick nach. ***Deshalb: Achten Sie auf Ihr Surf- & Kommunikationsverhalten.***

## Rund um Hacking und Sicherheit:

- *Tipps vom Consectra Live-Hacking-Team*
- *Die Präsentationsfolien zum Download im Intranet der Uni unter "IT-Sicherheit"*
- *Sicher unterwegs mit Smartphone, Tablet & Co vom Bundesamt für Sicherheit in der Informationstechnik BSI für Bürger*
- *IT-Sicherheit, die Seiten der Sicherheitsbeauftragten der Uni Bayreuth*
- *Behörden-IT-Sicherheitstraining BITS*
- *"Wie kann ich mich schützen?" ITS-Flyer zum Thema Sicherheit*

## Termine & Ankündigungen

14.12.16 ab 14 Uhr: Schließung des ITS für Publikumsverkehr wegen interner Veranstaltung

24.12.16–01.01.17: Weihnachtsschließung

Zum Jahreswechsel: Abschaltung des Netzwerks ***wlanubt***

02.01.17–05.01.17: Eingeschränkter Betrieb, Service- und Wartungsarbeiten

16.01.17 ab 9 Uhr: CMS Schulung

19.01.17 ab 14Uhr: Digitalisierung der Lehre: Input und Ideenwerkstatt
(Thema: Anwendungsbeispiele für eine digitale Lehre)