01/20
ITS
NEWS

Das Ende der Kreidezeit

Am 18.12.2019 öffnete das DigiLLab seine Tore. Die neuen Lern- und Lehr- Labore stehen Bayreuther Lehramtsstudierenden ab sofort zur Verfügung. Hier werden medienbezogene Kompetenzen an künftige Lehrkräfte vermittelt. Staatsminister für Wissenschaft und Kunst MdL Bernd Sibler gab sich die Ehre und eröffnete feierlich die Veranstaltung. Das IT-Servicezentrum stand dem DigiLLab bereits während der Vorbereitungen tatkräftig zur Seite.

Eigenes WLAN-Netzwerk

Innerhalb kurzer Zeit wurde im DigiLLab ein eigenes WLAN-Netzwerk installiert. Vier Accesspoints arbeiten in einem vernetzen Modus. Darüber können die VR-Brillen, Tablets und mobilen Tafeln optimal mit großen Datenmengen in dem jeweiligen Unterrichtsszenario versorgt werden.

Imagefilm für die Eröffnung

Ein aufwändiger Imagefilm wurde für die Eröffnungsfeier produziert. Dominik Schramm, Mitarbeiter der Abteilung Zentrale Systeme, drehte dafür in einem flachen Kameraprofil und in einer 4k-Auflösung, um eine sehr hohe Qualität zu erreichen. Außerdem gab es bewegte Kamerafahrten mit Slidern für ein modernes Videodesign. Künftig kann das Video auch auf dem Youtube Kanal des DigiLLab angesehen werden.

Dabei wurde auch ein eigenes Logo für das DigiLLab produziert, welches durch die Druckerei des ITS auf Bodenaufkleber und Rollups gedruckt wurde und der Eröffnungsveranstaltung einen weiteren professionellen Anstrich verlieh.

Technische Betreuung für das DigiLLab

Das ITS unterstützt das DigiLLab technisch. Andreas Brütting kümmert sich unter anderem um das Mobile Device Management. So werden auf den 20 angeschafften Tablets verschiedenste Apps zentral administriert, Lizenzen beschafft und für individuelle Schulpraktika vorbereitet. "Wir können uns leider nicht darauf verlassen, dass an jeder Schule eine WLAN-Anbindung auf uns wartet" so Dr. Matthias Ehmann, Sprecher des Kompetenzzentrums für digitales Lehren und Lernen.

Der Einkauf von kostenpflichtiger Software, sowie die zentrale Installation der Apps, bestenfalls über Nacht und die hohen Anforderungen an den Datenschutz sind wichtige Fragen, bei deren Beantwortung das ITS das DigiLLab auch weiterhin beraten wird.

Neue Ansprechpartner im Forschungsdatenmanagement

Forschungsdaten sammeln, klassifizieren, speichern und die Daten sinnvoll nutzbar zu machen sind im Zeitalter großer Datenfluten ein wichtiger Bestandteil der Wissenschaft. Schon die G8-Wissenschaftsminister machten am 12. Juni 2013 in London deutlich, welch wichtige Rolle, die Forschung bei der Sicherung des gegenwärtigen und künftigen nachhaltigen Wachstums spielen muss [*]. Auch die Universität Bayreuth verfolgt das Ziel, Wissen zu schaffen und zu bewahren, Impulse für kreatives Denken zu geben und neue Erkenntnisse für Wissenschaft und Gesellschaft sowie für nachfolgende Generationen zugänglich und nutzbar zu machen [**].

Welche Anforderungen stellt das Forschungsdatenmanagement (FDM)? Wie sichere ich meine Daten langfristig? Wie mache ich sie verfügbar und behalte dabei die Kontrolle über meine Forschungsergebnisse? Das sind Fragen, mit denen sich Projektleitung, Promovierende oder Studierende zu Beginn eines Forschungsprojekts zwangsläufig auseinandersetzen müssen. Die Arbeitsgruppe Forschungsdatenmanagement berät, schafft Schnittstellen, implementiert Plattformen und kümmert sich um Erfassung und Speicherung Ihrer Daten.

Neue Ansprechpartner

Zu Beginn des Jahres 2020 wurde das Team seitens des ITS neu aufgestellt. Dr. Thomas Martin und seine Kollegen Chettan Kumar und Denys Priadko sind Ihre Ansprechpersonen für den Bereich Datenmanagement und technische Unterstützung. Alle drei haben bereits Erfahrung im Bereich FDM sammeln können und wissen genau, welche Herausforderungen sich den unterschiedlichen Fachbereichen seitens der Wissenschaft stellt. "Mit den Wissenschaftlern für die Wissenschaft" lautet ihr Credo.

Weitere Informationen über das Forschungsdatenmanagement, seine Anforderungen und Möglichkeiten erhalten Sie unter:

www.fdm.uni-bayreuth.de

* https://www.gov.uk/government/news/g8-science-ministers-statement
** https://www.forschungsfoerderung.uni-bayreuth.de/pool/dokumente/20161108_UBT-Leitlinien-Forschungsdaten-Management.pdf

Team Forschungsdatenmanagement des ITS: Chettan Kumar (links) ; Dr. Thomas Martin (mitte), Denys Priadko (rechts)

Wie sicher ist mein Passwort?

HALLO, PASSWORT, hallo123 sind noch immer die Top 3 der meistgehackten Passwörter in Deutschland. Trotz stetiger Hinweise von Behörden, Providern und Bildungseinrichtungen ändert sich seit Jahren nichts an diesen Rankings. Diese bekannten Passwörter sollte man vermeiden, da Hacker auch auf solche Passwortlisten bei ihren Angriffen zurückgreifen. Um Beschäftigte, Forschende und Studierende besser zu schützen und zu unterstützen, trat zur Steigerung der IT-Sicherheit ab dem 1. Februar 2020 eine neue Passwortrichtlinie in Kraft.

Neue Richtlinie für Passwörter

Passwörter, die ab sofort im ITS-Portal neu vergeben werden, müssen bestimmten Anforderungen genügen. Die neue Richtlinie für Passwörter finden Sie unter:

Wissenstransfer > Publikationen > Passwortrichtlinie

Alte Passwörter bleiben weiterhin gültig. Dennoch empfehlen wir Ihnen Ihr Passwort zu überprüfen. Denn ein schlecht gewähltes Passwort ist nach wie vor die größte Sicherheitslücke im Internet. Um ein 6-stelliges Passwort zu knacken benötigt ein Hacker mit einem handelsüblichen PC nur 6,8 Sekunden. Für ein 10-stelliges dagegen 600 Jahre.

Außerdem ist es wichtig, sich für jeden externen Dienst ein eigenens Passwort zuzulegen(z.B. für Turnitin, Office365, Adobe, etc.).

Weitere Hinweise zur IT-Sicherheit und dem Umgang mit Passwörtern erhalten Sie auf der Homepage der IT-Sicherheitsbeauftragten der Universität Bayreuth unter:

www.it-sicherheit.uni-bayreuth.de

Sichere Passwörter

Ein sicheres Passwort besteht aus mindestens 10 Zeichen, besser wären 12, gleichzeitig gilt: je länger umso besser! Dabei verwenden Sie am besten eine Kombination aus Groß- und Kleinbuchstaben und Zahlen sowie Sonderzeichen.

Nehmen Sie sich beispielsweise einen einprägsamen Satz oder die erste Zeile Ihres Lieblingsliedes und nehmen Sie hiervon jeweils die ersten Buchstaben eines jeden Wortes:

Mein Hund Bello isst 4 Dosen Hundefutter mit Pute in 2 Tagen!
MHBi4DHmPi2T!

Sie können Ihr Passwort nun für verschiedene Onlineshops anpassen, sodass Sie niemals das gleiche Passwort für verschiedene Zugänge verwenden, und sich trotzdem Ihre Zugangsdaten merken bzw. herleiten können. Beispielsweise können Sie an der 4. 8. und 12. Stelle Ihres Passworts die ersten 3 Buchstaben der jeweiligen Internetadresse einfügen.

Für einen Adobe-Account (www.adobe.com) würde Ihr Passwort wie folgt aussehen: www.amazon.de
MHBai4DdHmPoi2T!

Übrigens: Auch die Regel, Passwörter alle 90 Tage zu ändern, ist überholt. Wenn das Passwort nach den neuesten Vorgaben als sicher gilt, gibt es keinen Grund, es zu ändern – außer es gibt einen konkreten Anlass wie beispielsweise ein (versuchter) Hacker-Angriff.

Upgrade der Kartenleser

In der Zeit vom 2. März bis 6. März werden auf dem Campus alle Kartenleser an den Kopierstationen getauscht. Leider können die Geräte nicht einzeln ersetzt werden, da die neue Software auf den Geräten nicht parallel mit der alten eingesetzt werden kann.

Wir möchten die Einschränkung möglichst gering halten. Dazu werden erstmal die Hälfte der Geräte umgerüstet und mit dem Umschalten auf den neuen Abrechnungsserver in Betrieb gehen. Erst danach werden die alten Kartenleser getauscht. Die Kopierstationen in der Verwaltung und an den Lehrstühlen sind nicht betroffen.

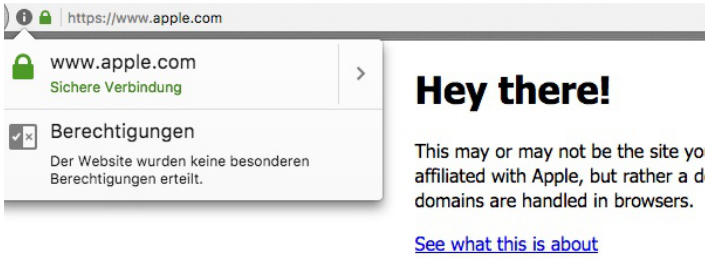
Die Hacker kommen

Am 14. Januar war es wieder soweit. Unter dem Motto: "Die Hacker kommen" fand im Audimax das jährliche Livehacking statt. Das Event zum Thema IT-Sicherheit für Beschäftigte und Studierende der Uni. Die Firma AWARE 7 GmbH zeigte in Zusammenarbeit mit der IT-Sicherheitsbeauftragten Dr. Benda anschaulich, wie leicht Hacker an unsere Passwörter und private Daten kommen.

Immer wieder berichteten wir in letzter Zeit, über die fiesen Tricks, mit denen Hacker sich Zugang zu vertraulichen Daten verschaffen. Beispielsweise wird durch unübersichtliche Links und gefälschte Absenderadressen, vermittelt man würde auf eine Seite der Universität Bayreuth weitergeleitet. Tatsächlich gelangt man auf eine Phising Seite. Eh man sich versieht, hat man seine Zugangsdaten Preis gegeben. Betrüger lassen sich immer wieder neue Tricks einfallen mit denen Sie versuchen uns aufs Glatteis zu führen.

Kyrillische Zeichen in Domains

Kyrillische Zeichen erfreuen sich größter Beliebtheit – zumindest wenn es darum geht das menschliche Auge zu täuschen. Auf den ersten Blick lassen sich die kyrillischen Zeichen nicht von den lateinischen unterscheiden. Doch diese Domains können auf Phishing-Seiten verweisen.



Domain mit kyrillischen Schriftzeichen, die Augenscheinlich auf www.apple.com zeigt

Letztlich schützt nur ein aktueller Browser vor solchen Domains. Denn hier werden die Zeichen in der Regel aufgelöst.

Ein gutes Beispiel für eine gefälschte Domain ist: xn--80ak6aa92e/.com. Hier macht es den Anschein man würde auf www.apple.com weitergeleitet. Tatsächlich handelt es sich um Buchstaben aus dem kyrillischen Alphabet. Es ist also Vorsicht geboten.

Sollten Sie versehentlich über eine Phishing-Mail ihre universitären Zugangsdaten preisgegeben haben, ändern Sie als Erstes Ihr Passwort und informieren Sie unverzüglich die IT-Sicherheitsbeauftragten der Universität Bayreuth. Auch E-Mails, die Ihnen verdächtig vorkommen, können Sie zur Überprüfung an die IT-Sicherheit weiterleiten:

it-sb@uni-bayreuth.de

IMPRESSUM:

Herausgeber:
IT-Servicezentrum
Universität Bayreuth
Universitätsstraße 30
95447 Bayreuth

Leitender Redakteur: Dr. Heiko Schoberth
Autorin: Claudia Willer
Bild: Dominik Schramm
Druck: Eigendruck

TERMINE:

CMS Grundlagenschulung
Di, 03.03.2020, 9 – 11:30 Uhr

CMS Vertiefungskurs
Mo, 09.03.2020, 9 – 11:30 Uhr

PC-Pool FAN A, Raum 0.20

Anmeldung:
oliver.gschwender@uni-bayreuth.de