Security Day 2013

29. Jänner 2013

Veranstalter:
Studiengang IT Security der FH St. Pölten

/fh///
st. pölten

SPARKASSE NIEDERÖSTERREICH MITTE WEST AKTIENGESELLSCHAFT

RSA The Security Division of EMC

IKARUS security software

SEC Consult ADVISOR FOR YOUR INFORMATION SECURITY

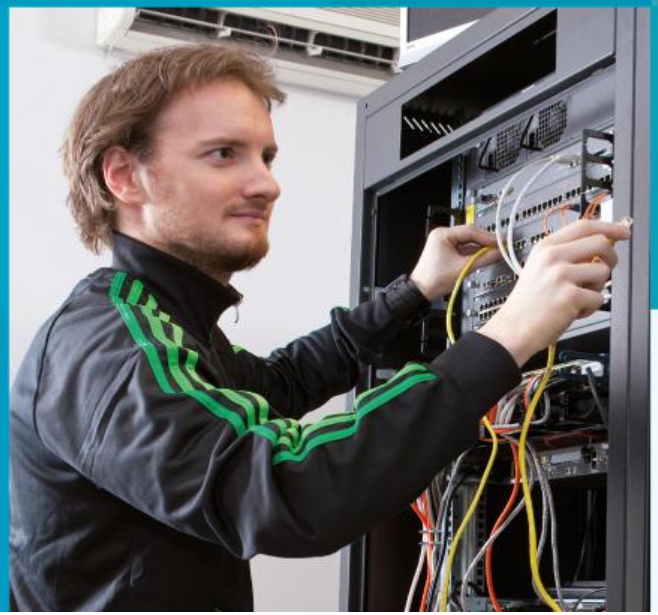
kabelplus WEB . TV . TEL

RADLBERGER

Herzlich Willkommen zum

9. Security Day 2013

IT-Sicherheit hautnah und auf spannende Art und Weise erleben!



29. Jänner 2013

Agenda [1/4]

- Vorstellung FH St. Pölten

- Herausforderungen in der Informations-sicherheit in einem Konzern
  | Mag. Hansjörg Kalcher | OMV AG
- "Cyber threats for grown ups" Dishing the dirt about malware-detection as experienced by the Austrian milCERT
  Praktisches Beispiel, wie Viren durch den Virenscanner durchgeschleust werden können | Mag. DI (FH) Ulrich Pöschl | BMLVS FüUZ / IKT-Sicherheit
- WhatsApp und Co.: Angriffsvektoren bei Smartphone-Messengers | DI Sebastian Schrittwieser | SBA Research

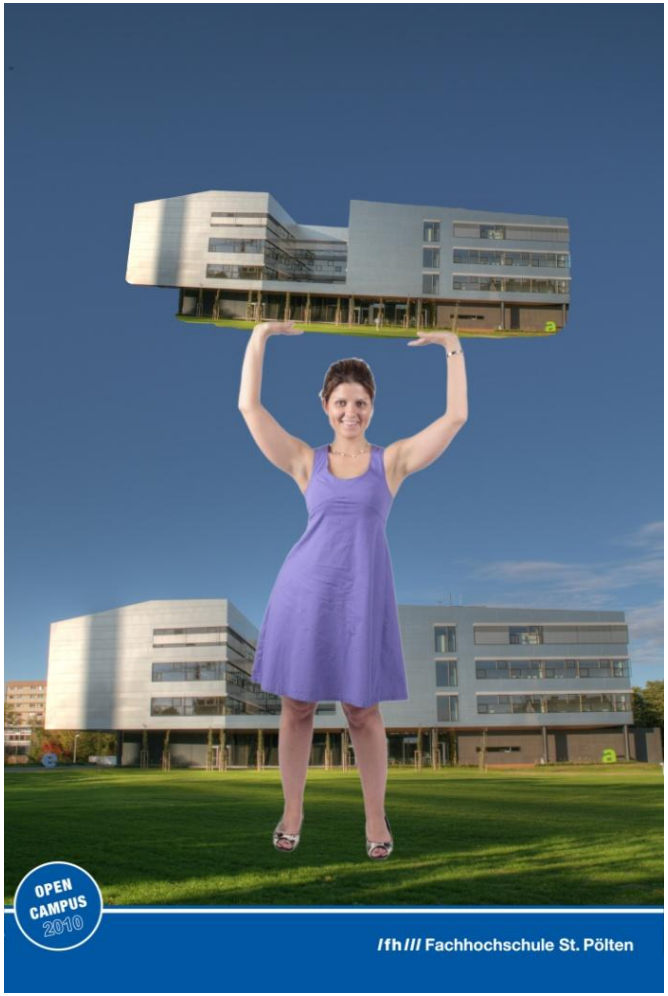
Agenda [2/4]

- 13 Uhr - 14 Uhr MITTAGSPAUSE

Campus & City Radio 94.4

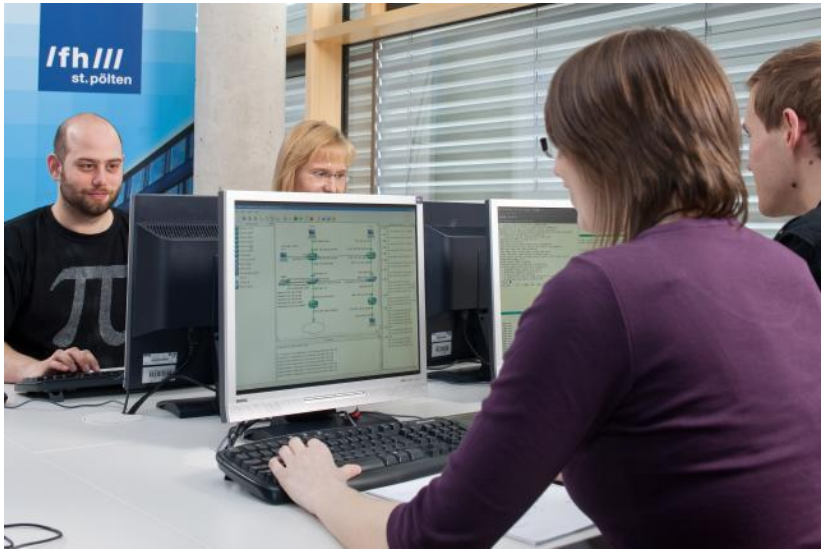
Gruppenfotos im Foyer

Einzelfotos im SR 2.07



Agenda [3/4]

Workshops



WS 1: Forensik

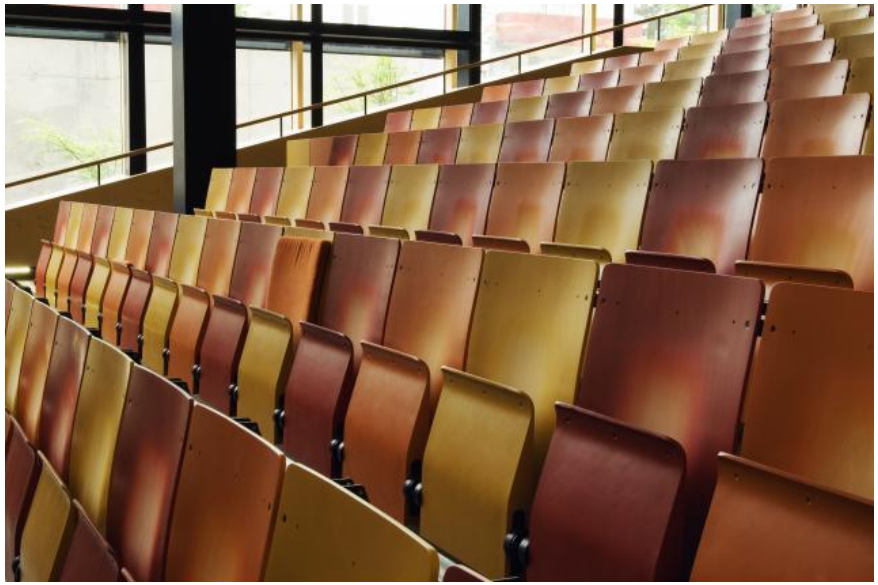
WS 2: Fälschen von Fingerabdrücken

WS 3: Lockpicking in Theorie und Praxis

WS 4: System Exploitation - Wie Hacker Systeme gezielt angreifen

WS5: WLAN-Hacking

Agenda [4/4]



Vorträge

V1: Von Viren, Würmern und trojanischen Pferden

V2: Das Verschlüsseln verstehen

V3: Alltagsspuren im Leben von dir & mir

Ziel dieser Veranstaltung

- IT Security bei SchülerInnen thematisieren/infizieren

- Gefahrenquellen aufzeigen

- Kennenlernen einfacher Schutzmechanismen für zu Hause

Fachhochschulen in Österreich

- Die wesentlichen Ziele einer Fachhochschule sind die Gewährleistung einer praxisbezogenen Ausbildung auf Hochschulniveau (vgl. FHStg §3)
- Anwesenheitspflicht
- Praxisorientierte Ausbildung (in Kleingruppen)

	FH	UNI	Verhältnis FH : UNI
Studierendenzahl	36.085	255.561	1 : 7
StudienanfängerInnen	14.245	42.775	1 : 3
AbsolventInnen	8.774	27.232	1 : 3
AbsolventInnen in der Toleranzzeit	8.774	8.169	!

Stand: 9/2010

Fachhochschule St. Pölten GmbH

- Gegründet 1996:
  „Telekommunikation und Medien“
- 2013: 16 Studiengänge
  11 Weiterbildungslehrgänge
  6 Forschungsinstitute
- Studierende: ca. 2000
- AbsolventInnen: 2100 +
- Insgesamt 460 MitarbeiterInnen

FH Campusgebäude

- Moderne Labors
- Offene CR / Labors
- Bibliothek
- Mensa
- Aufenthaltsräume
- Campusmedien

Ca. 2000 + Studierende in 16 Studiengängen

Medien

- Medientechnik, Bachelor
- Digitale Medientechnologien, Master

Informatik

- IT – Security, Bachelor
- Information Security, Master
- Medientechnik – Interaktive Medien, Bachelor
- Digitale Medientechnologien – Mobile/AMI, Master

Verkehr

- Eisenbahn-Infrastrukturtechnik, Bachelor
- Eisenbahn-Infrastrukturtechnik, Master

Medien

- Medienmanagement, Bachelor und Master
- Media- und Kommunikationsberatung, Bachelor und Master

Gesundheit

- Diätologie, Bachelor
- Physiotherapie, Bachelor

Soziales

- Soziale Arbeit, Bachelor und Master

Studienorganisation FH St. Pölten

	Bachelor-Studiengänge	Master-Studiengänge
Medien / Informatik	**Medientechnik** 6 Semester, Vollzeit 105 Studienplätze pro Jahr Bachelor of Science in Engineering (BSc)	**Digitale Medientechnologien** 4 Semester, Vollzeit 60 Studienplätze pro Jahr Diplom-Ingenieur/in (Dipl.-Ing.)
Informatik	**IT Security** 6 Semester, Vollzeit + Berufsbegleitend 50 Studienplätze pro Jahr Bachelor of Science in Engineering (BSc)	**Information Security** 4 Semester, Vollzeit 20 Studienplätze pro Jahr Diplom-Ingenieur/in (Dipl.-Ing.)
Verkehr	**Eisenbahn-Infrastrukturtechnik** 6 Semester, Vollzeit + Berufsbegleitend 40 Studienplätze pro Jahr Bachelor of Science in Engineering (BSc)	**Eisenbahn-Infrastrukturtechnik** 4 Semester, Berufsbegleitend 25 Studienplätze pro Jahr Diplom-Ingenieur/in (Dipl.-Ing.)

Kompetenzfeld IT Sicherheit

Masterstudium

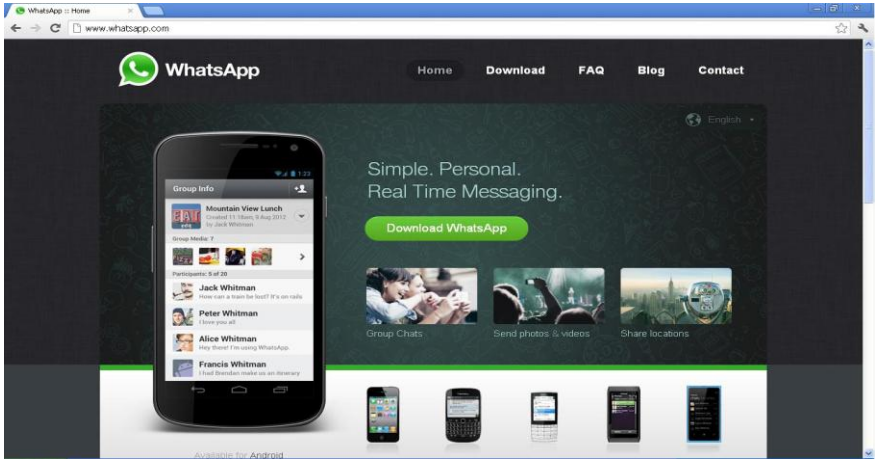
Information Security

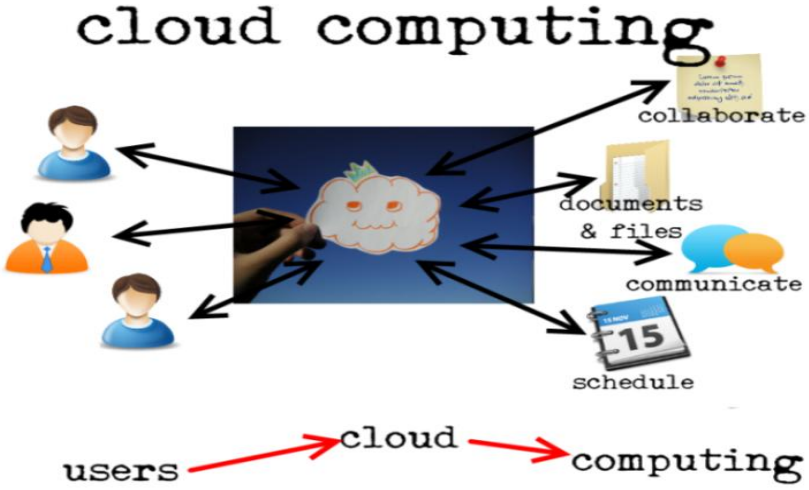
Bachelorstudium

IT Security

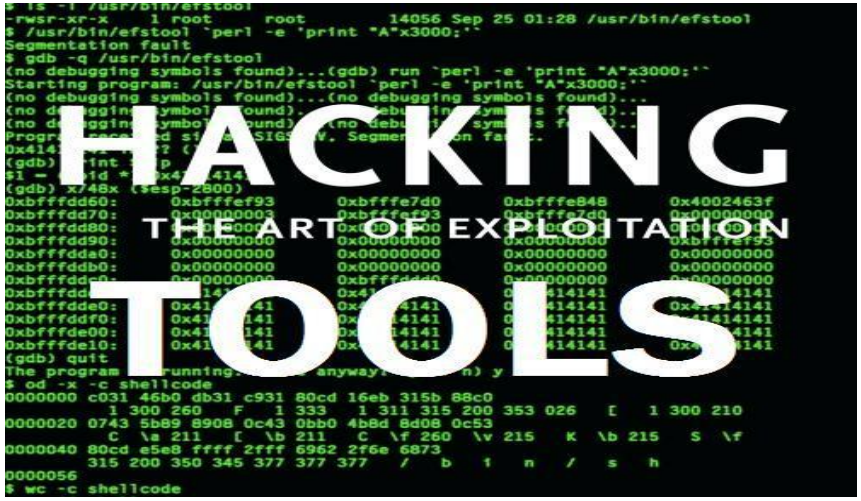
Institut für IT Sicherheitsforschung

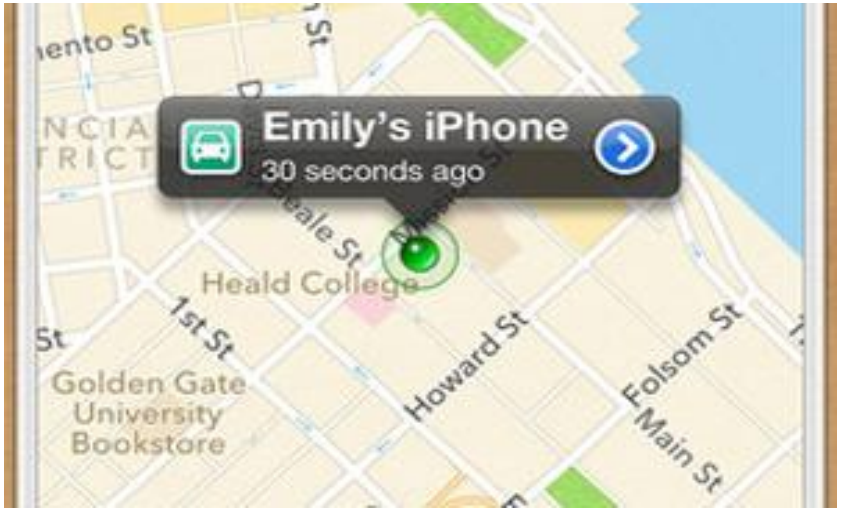
Die Welt der User/innen

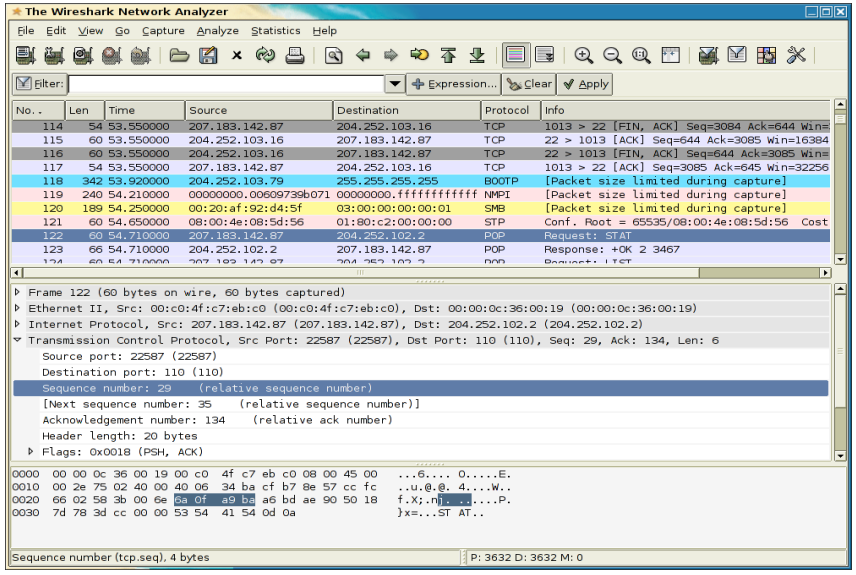


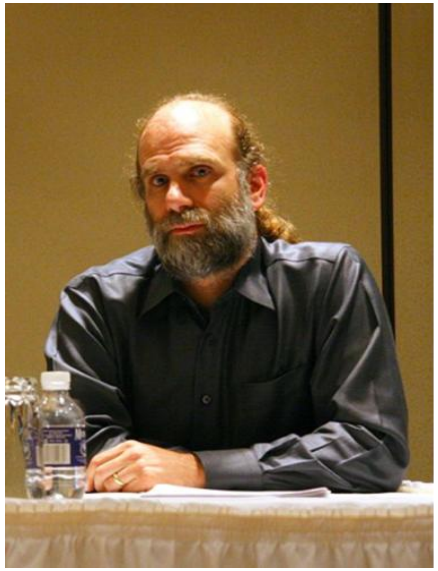


Die Welt der Angreifer/innen







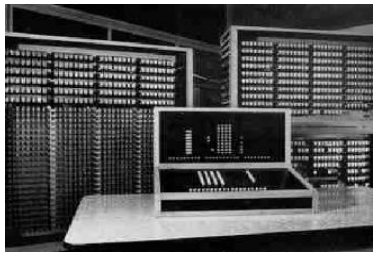


Chancenlos ?

Entwicklung Auto - Computer

1870 1913 1935 2012

142Jahre



71Jahre

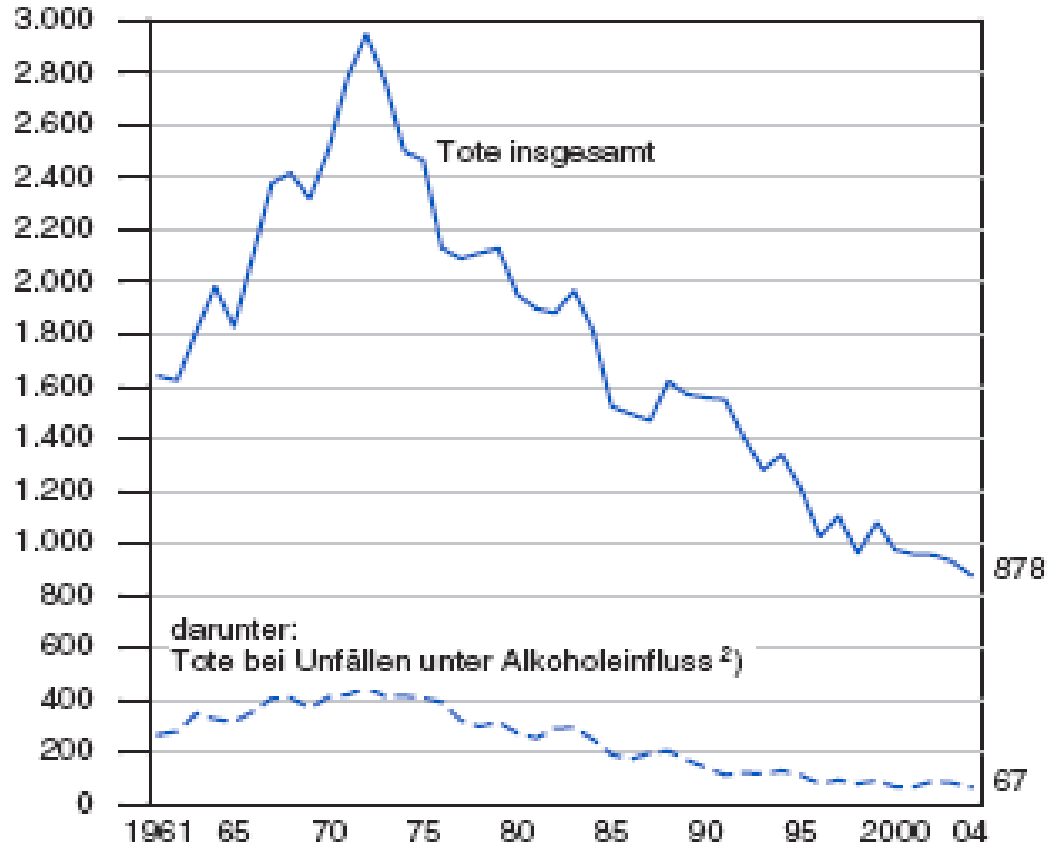
???

1941 1981 2012

Sicherheit im Auto

29.08 Tote [1]) bei Unfällen 1961 bis 2004

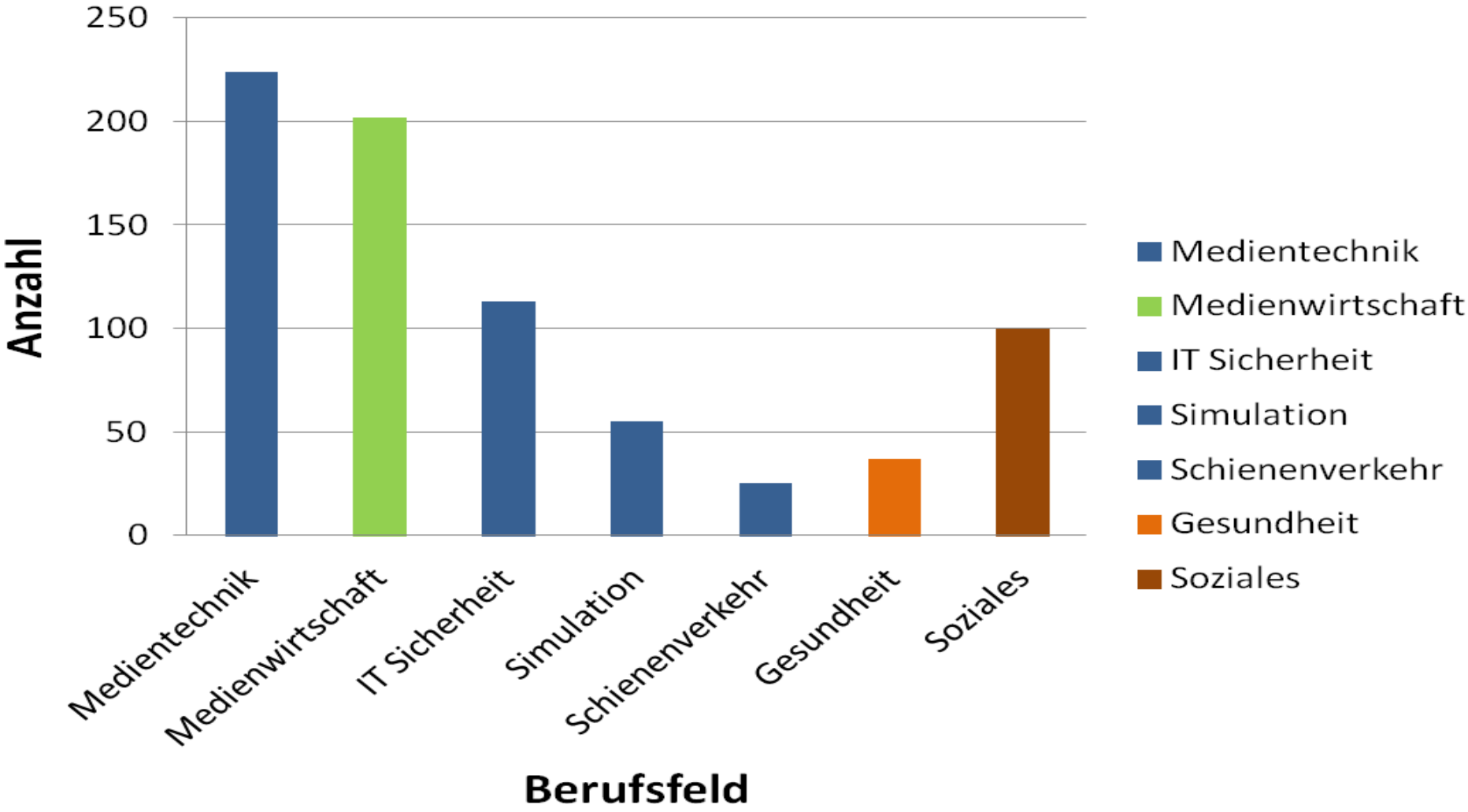
Persons killed by road accidents 1961 to 2004



Q: STATISTIK AUSTRIA. - [1]) Werte von 1966 bis 1991 umgerechnet auf 30-Tage-Frist. - [2]) Ab 1998 Blutalkoholgrenzwert 0,5 Promille.

- **Servolenkung**
- **Scheibenbremsen**
- **Sicherheitsglas**
- **Knautschzone**
- **Sicherheitsgurte**
- **Airbags**
- **Anti-Blockiersystem**
- **Stabile Fahrgastzelle**
- **Elektronisches Stabilitätsprogramm**

Security Experten/innen gesucht



Das Studium IT Security

IT Betrieb

Sicherheitstechnologien

Netzwerktechnik

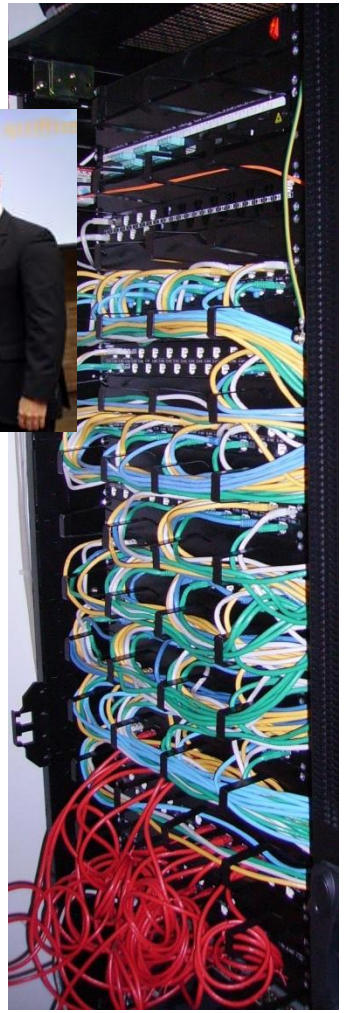
Sicherheitsmangement

NEU: Individueller Schwerpunkt

- IT Infrastruktur
- Malware
- Sicherheitsmanagement

IT Security – das Lernklima

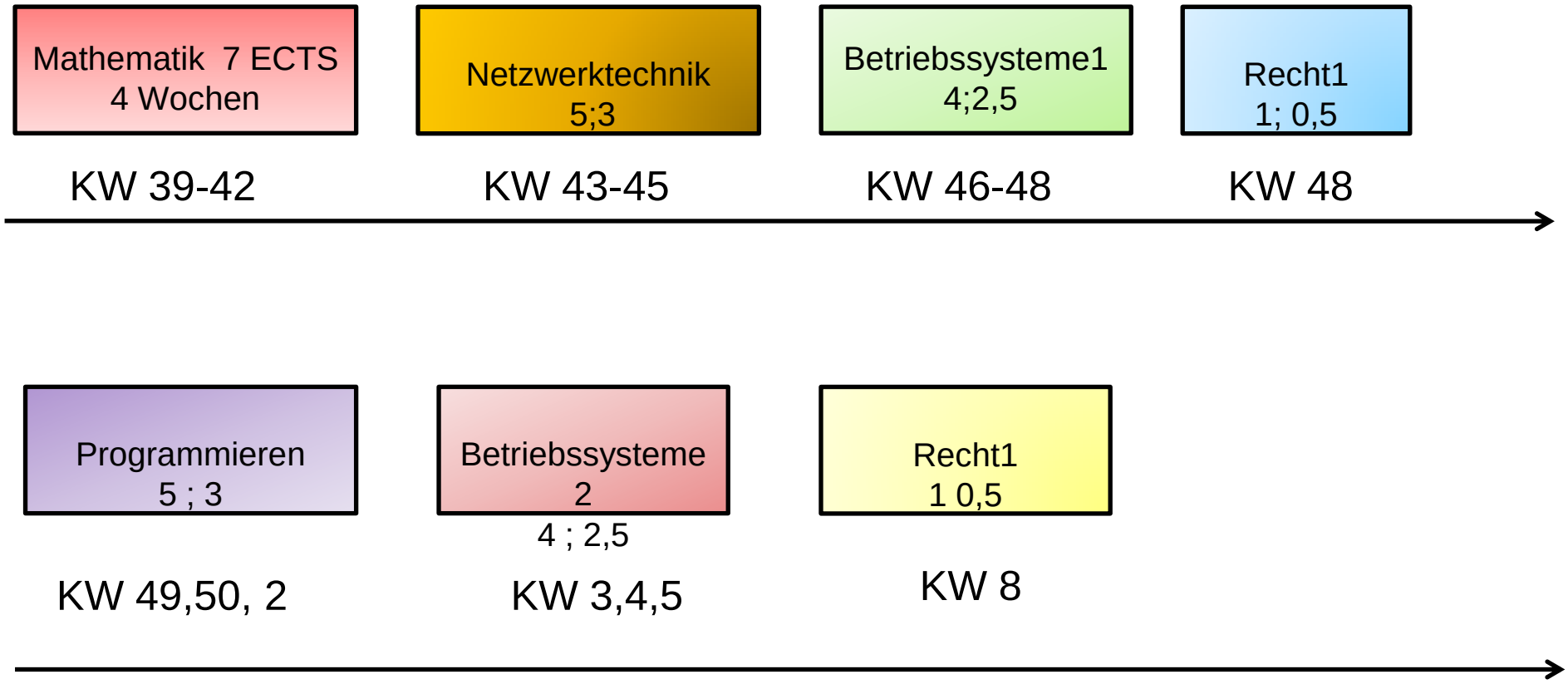
In der Regel merken wir uns beim



- nur Hören: 20%
- nur Sehen: 30%
- Sehen und Hören: 50%
- Sehen, Hören und Diskutieren: 70%
- Sehen, Hören, Diskutieren
  und selber Tun: 90%

→ Sehr viele Praxiselemente im Rahmen des Studiums

Modulunterricht



Modulunterricht: Vorteile

- Sequentielles Lernen bringt besseres Ergebnis als parallele Veranstaltungen
- Mitlernen wird einfacher und kontrollierbarer
- Belastung wird besser verteilt

- Bisher: Notendurchschnitt um 1 Grad besser
- Umstieg auf Hochschule wird „hoffentlich“ einfacher

Studiengangsbeirat

DIGITALES ÖSTERREICH

bwin

CERT.at

Cisco Systems

cryptas

Bundesamt für Sicherheit in der Informationstechnik

ekey

IKARUS security software

ISACA Serving IT Governance Professionals

Ernst & Young Quality In Everything We Do

KiwiSecurity Automating Video Surveillance

Microsoft

kabelsignal

phion

Raiffeisen Informatik

Leiner

Security Research

SEC Consult

SIEMENS

itSV strategie.steuerung.betrieb

VOITH

FH-STP Hacking Challenge

Security Day 2013

Facts - Termine

- Dauer: **15.2. bis 13.3.2013**
- Anmeldeschluss: **13.2.2013**
- Registrierung: **ab 30.1.2013 möglich**
  Registrieren Sie Ihr Team unter supportnwt@fhstp.ac.at.
- Preisverleihung:
  Im Rahmen der Tage der offenen Tür
  16.3.2013, 11 Uhr an der FH
- Ansprechpartner:
  DI Christoph Lang-Muhr, BSc
  Daniel Haslinger, BSc
  Erreichbar unter: supportnwt@fhstp.ac.at

Facts

- Inhalt:
  Challenges in unterschiedlichen Schwierigkeitsstufen

- TeilnehmerInnen:
  - Einzelpersonen oder Teams
  - zwei Kategorien mit unterschiedlichen Schwierigkeitsgraden
    Schulen mit technischem Background (zB HTL) oder
    „andere“ Schulen (zB AHS, HAK)
  - Nur UPGRADE möglich

- Spielregeln: Die Spielregeln werden gemeinsam mit dem Szenario veröffentlicht.

Voraussetzungen

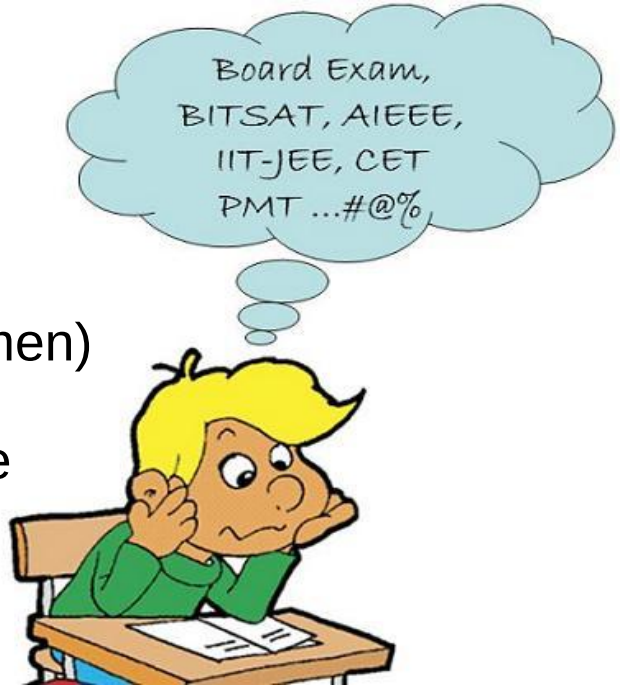
- Zunächst natürlich ein möglichst **motiviertes Team** :-)
  Die Einbettung der Challenge in den Unterricht ist keine Voraussetzung aber erfahrungsgemäß förderlich.
  Es ist möglich, pro Schule auch mehrere Teams zu registrieren.

- Spaß an Technik und Herausforderungen.
  Ob Hacking, investigative Recherche oder logische Kombinationsgabe: geplant ist jedenfalls ein möglichst breites Spektrum an Aufgabenstellungen.

- Zugang zum Internet mit **freiem Port 1194 / udp & tcp**.
  Dies ist notwendig um die Zielsysteme zu erreichen. Bitten Sie Ihren Administrator ggf. um Freischaltung dieses Ports.

Ablauf

- Dauer: 4 Wochen, freie Zeiteinteilung
- Der Zielserver steht rund um die Uhr zur Verfügung
- Technische und theoretische Aufträge werden in einem virtuellen Szenario erledigt
- Punktevergabe erfolgt nach Schwierigkeitsgrad
- Punktestand aller Teams kann während der Challenge auf einem interaktiven Ladder verfolgt werden (genannt werden nur die selbstgewählten Teamnamen)
- Sieger/In: meisten Punkte (pro Institution) und pro Kategorie
- Gewinne: Apple iPads, Sachpreise
- Die ersten 3 Plätze werden am Ende der Challenge inklusive Name der Schule veröffentlicht



Mögliche Themen

Bereits vor Beginn der Challenge erhalten die TeilnehmerInnen eine Liste an Themengebieten, auf welche sie sich vorbereiten können.

Beispiele:

- Forensik
- Steganographie
- Cross Side Scripting (XSS)
- SQL-Injection
- Kryptographie
- Command Injection
- Malwareanalyse
- . . .

Wichtige Termine

- Tage der offenen Tür:
  15. und 16. März
- Aufnahmetag:
  20. Februar – noch rasch anmelden
- Weitere Termine:
  02. April, 25. Mai

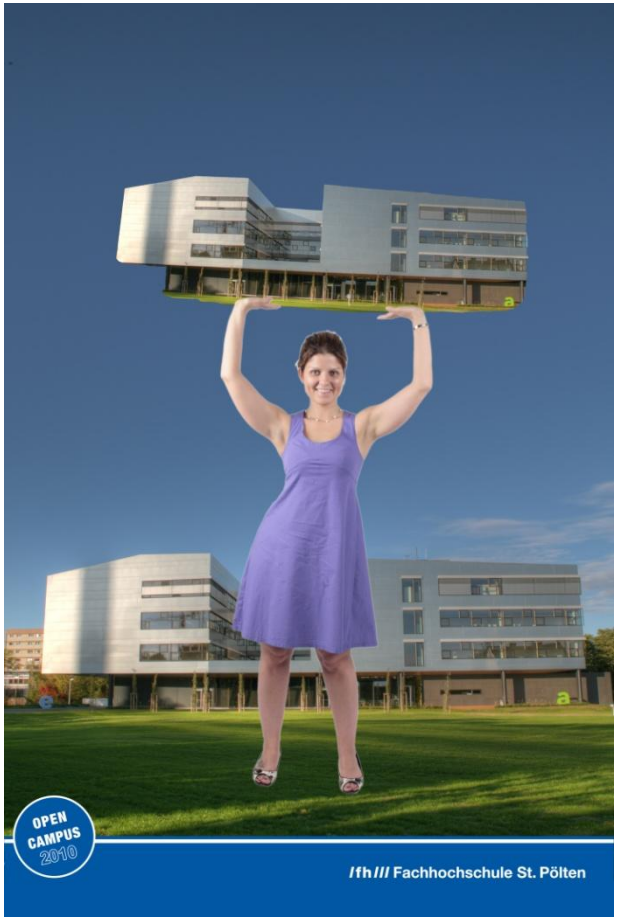
Agenda [1/4]

- Vorstellung FH St. Pölten

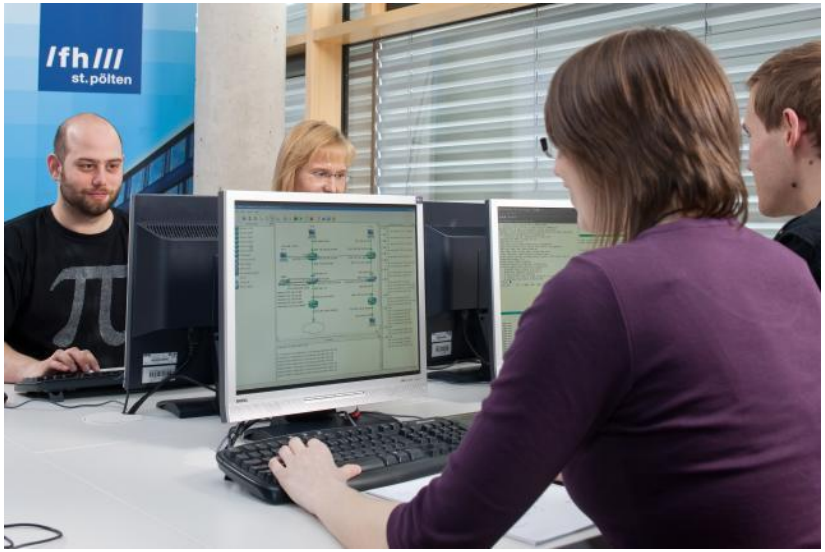
- Herausforderungen in der Informations-sicherheit in einem Konzern
  | Mag. Hansjörg Kalcher | OMV AG
- "Cyber threats for grown ups" Dishing the dirt about malware-detection as experienced by the Austrian milCERT
  Praktisches Beispiel, wie Viren durch den Virenscanner durchgeschleust werden können | Mag. DI (FH) Ulrich Pöschl | BMLVS FüUZ / IKT-Sicherheit
- WhatsApp und Co.: Angriffsvektoren bei Smartphone-Messengers | DI Sebastian Schrittwieser | SBA Research

Agenda [2/4]

- 13 Uhr - 14 Uhr MITTAGSPAUSE
- **Campus & City Radio 94.4**
  Im **Ausbildungsradio** der FH St. Pölten werden alle Aspekte des Radioalltags von Studierenden bewältigt. In der Mittagspause wird eine Live-Radiosendung produziert. LehrerInnen und SchülerInnen werden interviewt . Die Sendung wird auch live im Foyer übertragen.
- **Gruppenfotos im Foyer**
- **Einzelfotos im SR 2.07**



Agenda [3/4]



Workshops

WS 1: Forensik

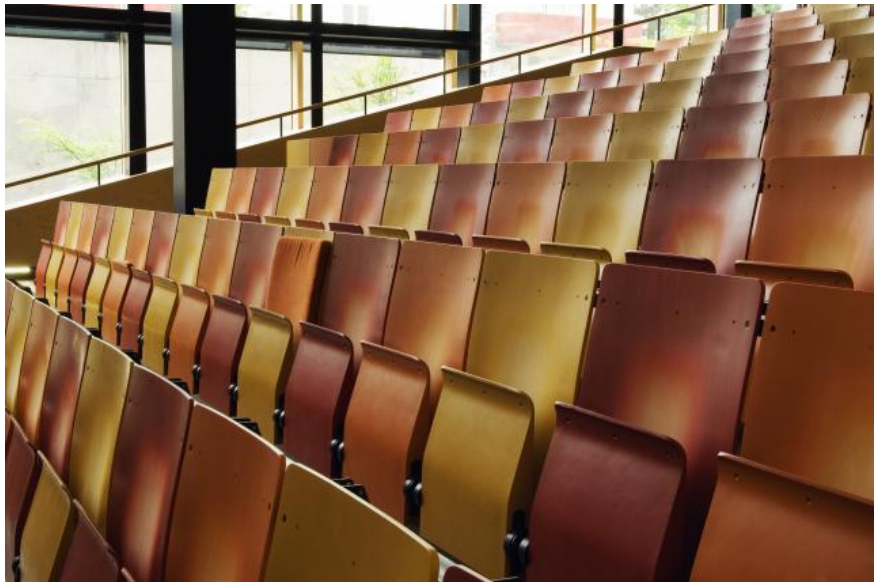
WS 2: Fälschen von Fingerabdrücken

WS 3: Lockpicking in Theorie und Praxis

WS 4: System Exploitation - Wie Hacker Systeme gezielt angreifen

WS5: WLAN-Hacking

Agenda [4/4]



Vorträge

V1: Von Viren, Würmern und trojanischen Pferden

V2: Das Verschlüsseln verstehen

V3: Alltagsspuren im Leben von dir & mir

WORKSHOPS

WS 1: Forensik

DI (FH) Rainer Poisel | wissenschaftlicher Mitarbeiter Institut für IT Sicherheitsforschung FH St. Pölten

Bei der IT-Forensik werden Spuren von verdächtigen Vorfällen erfasst, analysiert und ausgewertet. Typische Beispiele sind Ermittlungen bei "herkömmlichen" Straftaten, aber auch die Unterstützung zur Aufklärung von Fällen illegaler Geldtransfers, von Datendiebstahls und des Kindesmissbrauches.

Im Rahmen dieses Workshops wird gezeigt, wie man forensische Abbilder von Datenträgern erstellt, um anschließend die enthaltenen Beweise und Dateifragmente zu sichern und auszuwerten.

Level: Anfänger

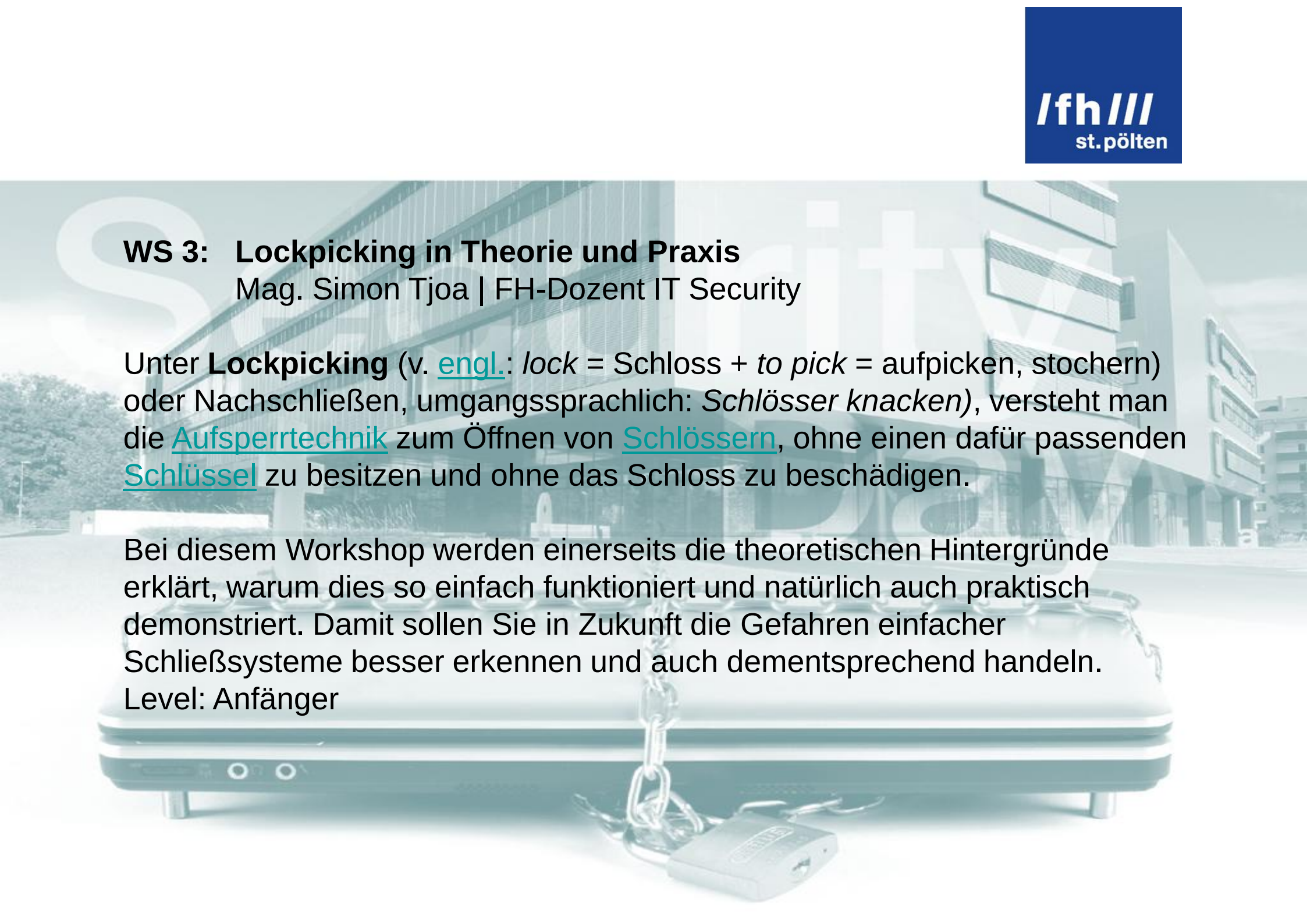
.

WS 2: Fälschen von Fingerabdrücken – Sind Fingerabdrucksensoren wirklich so leicht zu überlisten?

Mag. Dipl.-Ing. Marlies Rybnicek | wissenschaftliche Mitarbeiterin
Institut für IT Sicherheitsforschung FH St. Pölten

Der Mensch benutzt zur Erkennung seiner Mitmenschen charakteristische körperliche Merkmale wie das Gesicht oder den Klang der Stimme. Angelehnt an dieses Verhalten ist die Biometrie die Lehre von der automatisierten Erfassung und Vermessung körperlicher Merkmale wie zum Beispiel dem Fingerabdruck, der Iris, der Retina oder des Gesichts zur Authentifikation von Personen. Biometrische Fingerabdrucksensoren haben den Ruf durch die Herstellung von Fakefingern überlistbar zu sein. Im Rahmen dieses Workshops wird überprüft, ob es wirklich so einfach ist, einen gestohlenen Fingerabdruck zu reproduzieren und damit einen Fingerabdrucksensor zu täuschen.

Level: Anfänger



WS 3: Lockpicking in Theorie und Praxis

Mag. Simon Tjoa | FH-Dozent IT Security

Unter **Lockpicking** (v. engl.: *lock* = Schloss + *to pick* = aufpicken, stochern) oder Nachschließen, umgangssprachlich: *Schlösser knacken)*, versteht man die Aufsperrtechnik zum Öffnen von Schlössern, ohne einen dafür passenden Schlüssel zu besitzen und ohne das Schloss zu beschädigen.

Bei diesem Workshop werden einerseits die theoretischen Hintergründe erklärt, warum dies so einfach funktioniert und natürlich auch praktisch demonstriert. Damit sollen Sie in Zukunft die Gefahren einfacher Schließsysteme besser erkennen und auch dementsprechend handeln.
Level: Anfänger

WS 4: System Exploitation - Wie Hacker Systeme gezielt angreifen

Daniel Haslinger, BSc und
Dipl.-Ing. Christoph Lang-Muhr, BSc | FH St. Pölten

Täglich werden Sicherheitsprobleme und Schwachstellen publiziert und Exploit und andere Angriffswerkzeuge zur Ausnutzung dieser veröffentlicht. Die Beschäftigung mit diesen Werkzeugen, allen voran dem Metasploit Framework, einem Framework zum strukturierten Angriff auf IT-Systeme, kann sowohl für Security Verantwortliche als auch Administratoren und Tester die Möglichkeit bieten, selbst Sicherheitsüberprüfungen durchzuführen und gleichzeitig neue Angriffsmethoden zu evaluieren

.

Voraussetzungen:
Netzwerktechnik & TCP/IP Grundlagen (werden nur ganz kurz gestreift), Basiswissen in der Administration von Betriebssystemen (Windows/Linux)

Level: Fortgeschrittene

WS 5: WLAN Hacking

Thomas Leitner, BSc | Student Information Security FH St. Pölten

In diesem Workshop erhalten die TeilnehmerInnen einen Überblick zum Thema “WLAN-Security“, dabei wird auf das Thema WLAN-Security gezielt eingegangen. Zu Beginn wird ein theoretischer Einblick gegeben, dem folgt die Beschreibung der Verschlüsselungen WEP, WPA und WPA2. Diese Sicherheitstechniken werden sowohl von Seiten des Senders bei der Verschlüsselung als auch aus Sicht des Empfängers beim Entschlüsseln beleuchtet. Es werden mehrere Attacken in Teststellungen vorgestellt und erläutert.

Level: Anfänger