SECURITY DAY | 26. Jänner 2016

Gruppe A - GROSSER FESTSAAL

PROGRAMM

08:15 - 09:00 **Registrierung**

09:00 - 09:30 **Begrüßung**
Dipl.-Ing. Gernot Kohl, MSc | Geschäftsführer FH St. Pölten
FH-Prof. Dipl.-Ing. Johann Haag | Studiengangsleiter IT Security
Vorstellung FH St. Pölten
Präsentation Bachelorstudiengang IT Security sowie Masterstudiengang Information Security

09:30 - 10:15 **„Die Macht der Algorithmen“**
Philipp Schaumann | sicherheitskultur.at

10:15 – 11:00 **Interview mit AbsolventInnen zum Thema Berufsbilder und Erfahrungen im Studium**

11:00 - 11:15 Pause

11:15 – 12:00 **„Cheating in Mobile Games – So besiegst du den Drachen schnell und sicher!“**
Dipl.Ing. Manfred Kaiser, BSc | Junior Researcher Josef Ressel-Zentrum für konsolidierte Erkennung gezielter Angriffe FH St. Pölten

12:00 – 12:45 **„upribox (Usable Privacy Box) – Zeroconfig Adblocking“**
Dr. Markus Huber, MSc | FH-Dozent FH St. Pölten

Verlosung einer upribox

12:45- 13:30	**Mittagspause**

13:30 - 15:00 **Workshops und Vortrag**

SECURITY DAY | 26. Jänner 2016

Gruppe B – AUDIMAX

PROGRAMM

08:15 - 09:00 **Registrierung**

LIVE-Stream Audimax

09:00 - 09:30 **Begrüßung**
Dipl.-Ing. Gernot Kohl, MSc | Geschäftsführer FH St. Pölten
FH-Prof. Dipl.-Ing. Johann Haag Studiengangsleiter IT Security
Vorstellung FH St. Pölten
Präsentation Bachelorstudiengang IT Security sowie Masterstudiengang Information Security

09:30 - 10:15 **„Die Macht der Algorithmen“**
Philipp Schaumann | sicherheitskultur.at

10.15 - 10:30 Pause

10:30 - 12:00 **Workshops und Vortrag**

12:00- 12:45	**Mittagspause**

GROSSER FESTSAAL

12:45 - 13:30 **Interview mit AbsolventInnen zum Thema Berufsbilder und Erfahrungen im Studium**

13:30 – 14:15 **„Cheating in Mobile Games – So besiegst du den Drachen schnell und sicher!“**
Dipl.Ing. Manfred Kaiser, BSc | Junior Researcher Josef Ressel-Zentrum für konsolidierte Erkennung gezielter Angriffe FH St. Pölten

14:15 – 15:00 **„upribox (Usable Privacy Box) – Zeroconfig Adblocking“**
Dr. Markus Huber; MSc | Dozent FH St. Pölten

Verlosung einer upribox

WORKSHOPS 1-5: keine Vorkenntnisse notwendig

WS 1: iOS Forensik – Unlocking iPhone Secrets

Dipl.-Ing. Dipl.-Ing. Christoph Lang-Muhr, BSc, BSc |
Researcher Institut für IT Sicherheitsforschung, FH St. Pölten

Auf Smartphones wird eine Vielzahl an Daten gespeichert – sowohl vom Gerät selbst als auch von den installierten Apps wie Facebook oder WhatsApp. Es stellt sich die Frage: Welche privaten Daten befinden sich auf meinem Handy? Was merken sich Apps wie Facebook, Whatsapp und Co. über mich und mein Privatleben? Wer außer mir hat Einblick in meine Privatsphäre? Trotz Sicherheitsfunktionen auf iOS Geräten können Spezialisten sensible Daten mittels Forensik Tools auslesen und analysieren. Die Möglichkeiten, die dazu zur Verfügung stehen, werden im Rahmen dieses Workshops präsentiert und anhand eines praktischen Beispiels veranschaulicht.

WS 2: Physical Security

Studierende IT Security FH St. Pölten

In diesem Workshop wird den SchülerInnen eine kurze Einführung in die Thematik physische Sicherheit gegeben. Dabei wird auch auf die Notwendigkeit für IT- und Informationssicherheit hingewiesen.

Inhaltliche Schwerpunkte der Präsentation:

- Erklärung von Funktionsweisen von Schlössern
- Präsentation von Lockpicking-Werkzeugen und Bumpkeys
- Vorstellung von Methoden um physische Sicherheit zu kompromittieren

Im Anschluss der Präsentation bekommen die SchülerInnen die Möglichkeit die vorgestellten Methoden auszuprobieren.

WS 3: Memory Hacking

Dipl.-Ing. Dr. Sebastian Schrittwieser, Bakk. | Leiter Josef Ressel-Zentrum für konsolidierte Erkennung gezielter Angriffe, Stefan Marschalek, BSc, MSc | Junior Researcher Josef Ressel-Zentrum, FH St. Pölten

Den Arbeitsspeicher eines Computers kann man sich in etwa wie das Kurzzeitgedächtnis eines Menschen vorstellen. Er speichert den Zustand eines Programms (offene Browserfenster, Texteingabe, Punkte in einem Spiel, usw.) solange dieses geöffnet ist. Auf modernen Betriebssystemen hat jedes Programm seinen eigenen Bereich im Speicher, damit sich Programme nicht gegenseitig stören. Es ist jedoch möglich, mit speziellen Programmen auf den Speicherbereich eines anderen Programms zuzugreifen und diesen auch zu verändern. Im Rahmen dieses Workshops wird gezeigt, warum man sich die Zeit sparen sollte zu versuchen, bei Online-Spielen einen Highscore von 9.999.999 Punkten zu überbieten und wie man selbst die Technik der Speichermanipulation in der Praxis anwenden kann, um bei Computerspielen garantiert immer die höchste Punktezahl zu erreichen.

WS 4: Google Hacking

Dipl.-Ing. Robert Luh, BSc | Researcher Josef Ressel-Zentrum für konsolidierte Erkennung gezielter Angriffe | Dipl.-Ing. Matthias Schrattenholzer, BSc | Junior Researcher Information Security (MA), FH St. Pölten

Im Workshop Google Hacking wird auf eine besondere Seite von Internet-suchmaschinen eingegangen: Ihre Bedeutung als Hacking-Werkzeug. In praktischen Übungen wird demonstriert, wie Google & Co als Werkzeuge für Sicherheitsanalysen verwendet werden können, welche Suchmuster dafür erstellt werden müssen und welche Ergebnisse damit erzielt werden können.

WS 5: Internet Privacy

Dipl.-Ing. Gerhard Pötzelsberger, B. Eng., Dipl.-Ing. Gabor Österreicher, BSc | Junior Researcher Institut für IT Sicherheitsforschung

Im Workshop Internet Privacy wird das Thema Privatsphäre im Internet diskutiert und praktische Technologien zum Schutz der Privatsphäre ausprobiert. Dabei werden folgende Themen behandelt: Metadaten, Anonymität und Verschlüsselung. Wir zeigen wie Internetfirmen das Freundesnetzwerk von ihren Nutzern auswerten, wie man ohne Spuren zu hinterlassen im Internet surft und wie man verschlüsselte Nachrichten mit Freunden austauscht.

WORKSHOPS 6-7: Vorkenntnisse notwendig

WS 6: System Exploitation - Wie Hacker Systeme gezielt angreifen

Dipl.-Ing. Daniel Haslinger, BSc | Junior Researcher Institut für IT Sicherheitsforschung, 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.

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

WS 7: WLAN Hacking

André Meindorfer, Assistent IT 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.

Vorkenntnisse: Basiswissen in der Administration von Betriebssystemen (Linux)

Vortrag 1: Steganographie - Versteckspiel mit Nachrichten

FH-Prof. Dipl.-Ing. Dr. Paul Tavolato | Studiengangsleiter Information Security (MA), FH St. Pölten

Um Nachrichten geheim zu übertragen, kann man sie verschlüsseln oder verstecken. Steganographie beschäftigt sich mit dem Verstecken von Nachrichten in Datenströmen. Im Vortrag werden steganographische Methoden und Methoden zum Auffinden versteckter Informationen vorgestellt.