Security Day | 28. Jänner 2025

Programm

08:15–09:00 Uhr **Registrierung und Einlass** | Aula, Gebäude A

09:00–10:00 Uhr **Programmbeginn und Begrüßung** | Großer Festsaal, Gebäude A

Keynote: Wozu noch lernen, die KI wird‘s schon richten!
Gerald Kortschak, sevian7

Ein Arbeitstag im Leben unserer Alumni
Absolvent*innen berichten über ihren Arbeitsalltag

10:00–10:10 Uhr Pause

Weiterführend stehen folgende **Programmvarianten** zur Auswahl:

Variante A – Workshops/ Vorträge:

10:10–11:40 Uhr **Workshops** in den jeweiligen Räumen/ Laboren

11:40–12:10 Uhr Mittagspause (Aula Gebäude A)

2. Teil – Programm Großer Festsaal, Gebäude A

12:10–12:40 Uhr Keynote zum Spannungsfeld „Cloud, Cyber, Cash und Knast“
Herfried Geyer, stv. Studiengangsleiter IT Security

12:40–13:20 Uhr Informatik & Security an der FH St. Pölten – das sind wir!
Robert Luh | Studiengangsleiter IT Security (BA)
Marlies Temper | Studiengangsleiterin Data Science & Artificial Intelligence (BA)
Thomas Felberbauer | Studiengangsleiter Smart Engineering (BA)

13:20–13:45 Uhr Siegerehrung Workshops „Hacking Challenge” & „Escape the Room”
Herfried Geyer | stv. Studiengangsleiter IT Security

13:45-14:45 Uhr	Alltagshacks Daniel Haslinger | FH-Dozent Department Informatik und Security Christoph Lang-Muhr | Studiengangsleiter Information Security
15:00 Uhr	Veranstaltungsende

Variante B – Hacking Challenge:

10:10–13:00 Uhr	Hacking Challenge (integrierte Mittagspause)
13:00–15:00 Uhr	Weiteres Programm & Vorträge im Großen Festsaal, Gebäude A inkl. Siegerehrung Hacking Challenge

Variante C – IT-Security Escape the Room:

10:10–13:00 Uhr	IT-Security Escape the Room (integrierte Mittagspause)
13:00–15:00 Uhr	Weiteres Programm & Vorträge im Großen Festsaal, Gebäude A Inkl. Siegerehrung IT-Security Escape the Room

---

Übersicht Vortrag & Workshops

- **Basic:** keine technischen Vorkenntnisse erforderlich
- **Medium:** technisches Interesse aber keine Vorkenntnisse erforderlich
- **Fortgeschritten:** technische Kenntnisse erforderlich

Vortrag:

V 1: **Vertrauen in…Programme | Basic**

Dieser Vortrag zeigt anhand kleiner Beispiele, was bei der Konstruktion und Ausführung von Programmen schief gehen kann. Jedes unvorhergesehene Verhalten bietet sich als Schwachstelle für Angreifer*innen an und gefährdet in weiterer Folge die Sicherheit des Systems.

Workshops:

WS 1: **OSINT: Digitale Aufklärung im Kontext eines Cyberangriffs** | **Basic**

Im Workshop „OSINT: Digitale Aufklärung im Kontext eines Cyberangriffs“ wird auf eine besondere Seite von Internetsuchmaschinen eingegangen: Ihre Bedeutung als Hacking-Werkzeug, um Informationen zu beschaffen. In praktischen Übungen wird demonstriert, wie Google & Shodan & OSINT-Feeds als Werkzeuge für Sicherheitsanalysen verwendet werden können, welche Suchmuster dafür erstellt werden müssen und welche Ergebnisse damit erzielt werden können.

WS 2: **Hands-on Industry 4.0** | **Basic**

Die Arbeitswelt vieler Branchen befindet sich durch den Einsatz aktueller digitaler Technologien im Umbruch. Augmented Reality, Internet of Things, 3D-Druck und Lasercutter – gestalten die Produktion der Zukunft sowohl in großen als auch kleineren Unternehmen oder Manufakturen.

Der Workshop „Hands-On Industry 4.0 Lab“ des Studiengangs Smart Engineering bietet Schülerinnen und Schülern einen unterhaltsamen Einblick in die Labore „Industrie 4.0“ und „Makers‘ Lab“. Dabei können Sie Lerninstallationen zur Produktion der Zukunft haut nah miterleben und live testen. Kritisch werden dabei neben den Möglichkeiten der digitalen Technologien auch die damit einhergehenden Herausforderungen, z.B. im Bereich der Security, diskutiert. Die teilnehmenden Personen erhalten die Möglichkeit, Hands-on mit Augmented-Reality-Technologien zu arbeiten, , sie erleben anhand der im Studiengang eingesetzten Ausbildungsroboter, 3D-Drucker und Indoor-Navigationssysteme was „individuelle Produktion“ bedeutet und sehen aber auch die Auswirkungen, wenn es hier Sicherheitslücken gibt.

WS 3: **Social Intrusion – Angriffsziel Mensch** | **Basic**

Der Mensch ist die Schwachstelle eines jeden Sicherheitssystems. Mit Methoden des Human Hacking versuchen Angreifer*innen (Social Engineers) Menschen zu manipulieren. Auf diese Art werden komplexe Sicherheitssysteme nicht direkt angegriffen, sondern vielmehr umgangen. In diesem Workshop zeigen wir Methoden und Vorgehensweisen von Angreifer*innen, um diese erkennen und Gegenmaßnahmen ergreifen zu können. In jedem von uns steckt ein Social Engineer, sei es beim Versuch eine Beziehung aufzubauen, eine Erklärung für nicht erstellte Hausaufgaben zu erfinden, oder anderweitige Wege zu finden, das Gegenüber für sich zu gewinnen.

WS 4: **Entdecke die Magie der KI | Basic**

Generative AI: Tauchen Sie ein in die faszinierende Welt der Generativen Künstlichen Intelligenz (Generative AI) mit unserem Einsteigerworkshop. Generative AI ermöglicht es Computern, kreative Inhalte wie Bilder, Texte und Musik eigenständig zu erstellen. In diesem Workshop werden die grundlegenden Konzepte und Techniken der Generativen AI auf verständliche Weise erklärt.

WS 5: **PenQuest | Basic**

PenQuest ist ein digitales Brettspiel für zwei Spieler*innen, bei dem Angreifer*innen versuchen, in ein abstrahiertes IT-Netzwerk einzudringen, während die Verteidigerseite die Bedrohung abwehrt und präventive Maßnahmen ergreift. Das Spiel basiert auf einem detaillierten Modell, das verschiedene IT-Sicherheitskonzepte abbildet. Es simuliert alle Phasen eines Cyberangriffs – von der Aufklärung bis zur „Detonation“ – und zeigt die Abhängigkeiten zwischen den Systemen. PenQuest ermöglicht es, reale Bedrohungsszenarien spielerisch nachzustellen und bietet eine Plattform für Training, Bewusstseinsförderung und Risikoanalysen.

In diesem Workshop hast du die Gelegenheit, verschiedene PenQuest-Szenarien selbst auszuprobieren und spielerisch die Hintergründe unterschiedlicher Cyber-Bedrohungen – von Ransomware-Angriffen bis hin zu Datenklau und DDoS-Attacken – zu erkunden.

Weitere Informationen findest du unter https://www.pen.quest/.

WS 6: **Robotic AI | Basic**

Entdecke die Welt der Programmierung und Künstlichen Intelligenz mit einem humanoiden Roboter!

Hast du dich schon einmal gefragt, wie Roboter lernen und wie künstliche Intelligenz funktioniert? In diesem Workshop tauchen wir gemeinsam in die faszinierende Welt der Programmierung ein – und das mit einem besonderen Begleiter: einem humanoiden Roboter! Du wirst nicht nur lernen, wie du diesen Roboter mithilfe von Python programmierst und steuerst, sondern auch Einblicke in die spannende Technologie hinter Künstlicher Intelligenz und großen Sprachmodellen (LLMs) erhalten.

Keine Sorge, du brauchst keinerlei Vorkenntnisse – wir starten bei den Grundlagen und führen dich Schritt für Schritt in diese aufregende Welt ein.

WS 7: **Active Directory Hacking | Fortgeschritten**

Dieser Workshop dreht sich rund um Kerberos - eine Authentifizierungsmethode im Active Directory. Dabei werden die Grundprinzipien vom Einloggen auf einem PC bis hin zum Zugriff auf Ressourcen im Active Directory erläutert. Du lernst zudem über Angriffe, wie z. B. Kerberoasting oder AS-REP-Roasting und wie diese funktionieren bzw. wie man diesen entgegenhalten kann.

WS 8: **System Exploitation | Fortgeschritten**

Täglich werden Sicherheitsprobleme und Schwachstellen publiziert und Exploits 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 Administrator*innen und Tester*innen 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 9: **Die Daten-Detektive | Basic**

Überlebe die Zombie-Apokalypse in Österreich! Willkommen in einer Welt voller Spannung und Gefahr! In unserem Workshop begeben wir uns in eine fiktive Realität, in der eine mysteriöse Krankheit Österreich heimsucht. Als Mitglieder des 'Data Driven Disease Defense Department' (D5) sind wir die Helden dieser Geschichte! Dein Ziel? Die unbekannte Krankheit analysieren, um den Behörden dabei zu helfen, kluge Entscheidungen zu treffen und die Zombie-Apokalypse in den Griff zu bekommen mit Hilfe von Data Science!

WS 10: **Hands-on Cloud Computing Lab | Fortgeschritten**

In diesem Workshop lernen Teilnehmer*innen über Cloud Computing und die dahinter verwendeten Technologien. Gemeinsam erstellen und programmieren wir kleine Anwendungen auf der Cloud-Plattform AWS.

Vorkenntnisse: Netzwerktechnik Grundlagen, Basiswissen in der Administration von Betriebssystemen

WS 11: **Autonomes Fahren mit KI und RC Cars** | **Medium**

In diesem Workshop erarbeiten wir die Grundlagen des autonomen Fahrens mit KI anhand ferngesteuerter Autos. Nach einer kurzen Einführung in die wichtigsten Aspekte der KI wenden wir das Gelernte auf Modellautos (AWS DeepRacer und Donkey Car) an.

Hacking Challenge | **Fortgeschritten** **(= Programmvariante B)**

Hier haben Talente von morgen die Chance, sich in einem Capture-the-Flag (CTF) Game zu beweisen. Interessierte können (ganz ohne Aufwand und Gebühren) erstmals CTF-Luft schnuppern und ganz nach dem Prinzip „Mittendrin statt nur dabei" selbst Systeme unterschiedlichen Schwierigkeitsgrads bezwingen. Die Kategorien umfassen spannende Themen wie Forensik, Kryptographie, Reverse Engineering, Ethical Hacking und Defense. Versucht in Teams unsere Aufgaben zu lösen und zeigt, dass ihr zu den Besten gehören! Das Gewinnerteam erhält einen tollen Preis!

Anforderung: Pro Teilnehmer*in ist ein Notebook mitzubringen. Nähere Details folgen im Anschluss an die Anmeldung.

IT-Security Escape the Room | **Medium** **(= Programmvariante C)**

Dieser Workshop ist eine Schnitzeljagd, bei der es darum geht, Daten aus einem fiktiven Unternehmen zu stehlen. Hierzu wird ein komplexes Passwort benötigt, welches aus mehreren Stationen gewonnen wird. Die einzelnen Stationen bieten eine spannende, lustige Möglichkeit, spielerisch Basiswissen rund um IT Security und Technik kennenzulernen. Unter anderem werden einfache Anwendungen im Bereich Kryptographie, Websicherheit, Forensik, physische Sicherheit und das Bedienen von Technik auftreten. Es handelt sich hierbei um keinen Vortrag, sondern eine Mischung aus Escape-the-Room und Schnitzeljagd. Dieses Abenteuer ist sowohl für Techniker*innen als auch Nicht-Techniker*innen geeignet.