ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

WE ARE EUDRES EUROPEAN UNIVERSITY

Security Day feat. Data Science | 30. Jänner 2024

Programm

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

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

Keynote zum Spannungsfeld „Cloud Security“

Gerald Kortschak, sevian7

Informatik & Security an der FH St. Pölten – das sind wir!

Herfried Geyer | stv. Studiengangsleiter IT Security (BA)
Marlies Temper | Studiengangsleiterin Data Science & Business Analytics (BA)
Thomas Felberbauer | Studiengangsleiter Smart Engineering (BA)

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 „Cloud, Cyber, Cash und Knast“

Herfried Geyer, stv. Studiengangsleiter IT Security

12:40–13:20 Uhr Ein Arbeitstag im Leben unserer Alumni

Absolvent*innen berichten über ihren Arbeitsalltag

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 Vorträge & Workshops

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

Vorträge:

V 1: **Smart World | Basic**

Dieser Vortrag zeigt anhand kleiner Beispiele wie Programme aufgebaut sind und was bei deren Konstruktion und Ausführung schief gehen kann. Jedes unvorhergesehene Verhalten bietet sich als Schwachstelle für Angreifer 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 und erleben anhand der im Studiengang eingesetzten Ausbildungsroboter, 3D-Drucker und Indoor-Navigationssysteme was „vernetzte Produktion“ bedeutet.

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** | **Medium**

PenQuest ist ein digitales Brettspiel für zwei Spieler*innen, bei dem eine Angreifer*in versucht, in ein abstrahiertes IT-Netzwerk einzudringen. Zugleich arbeitet die Verteidiger-Seite daran, die Bedrohung abzuwehren und präventive Maßnahmen zu setzen. Unter der Haube nutzt PenQuest ein komplexes Modell, das eine Vielzahl von

Sicherheitskonzepten umfasst, um so realistisch wie möglich zu sein. So sind die Aktionen der Angreifer*in aus dem MITRE ATT&CK Framework abgeleitet, während Verteidigungsaktionen auf einem gängigen Sicherheitsstandard basieren. Die Effekte von Datenklau, Systemmanipulation und Angriffen auf die Verfügbarkeit werden genauso modelliert wie die verschiedenen Phasen eines Angriffs (von Aufklärung bis „Detonation“) und die Abhängigkeiten der Systeme untereinander.

So lassen sich reale Bedrohungsszenarien zugänglich auf dem Spielbrett nachstellen und zu bewusstseinsfördernden Maßnahmen, Trainings und sogar Risikoanalysen kombinieren. Auf diese Weise soll PenQuest interessierten Personengruppen die Grundlagen von Cyberangriffen und deren Abwehr vermitteln. Dank der freien Konfiguration von Akteuren und Systemen gibt es dabei kaum Einschränkungen: Vom Ransomware-Angriff auf eine isolierte Workstation bis hin zum großangelegten Datendiebstahl ist alles möglich. Weitere Informationen und ein Demo-Video des Spiels finden Sie unter www.pen.quest.

WS 6: **NAO's Coding Adventure** | **Basic**

Gemeinsam mit einem Roboter die Welt des Programmierens entdecken: Hast du dich schon einmal gefragt, ob es möglich ist, die Geheimnisse des Programmierens in kürzester Zeit zu lüften? Wir haben die Antwort: Ja, und zwar mit einem ganz besonderen Begleiter – NAO, der humanoide Roboter! Keine Sorge, wenn du noch nie programmiert hast – wir starten bei Null und führen dich behutsam in die aufregende Welt des Programmierens mit Python ein.

WS 7: **Active Directory | 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. Sie lernen 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 Detection Department' (D5) sind wir die Helden dieser Geschichte! Dein Ziel? Die unbekannte Krankheit verstehen, 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** | **Fortgeschritten**

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.

WS 12: **IT-Security Escape the Room** | **Medium**

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 kennen zu lernen. 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.

WS 13: **Hacking Challenge** | **Fortgeschritten**

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. Versuchen Sie in Teams unsere Aufgaben zu lösen und zeigen Sie, dass Sie 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.