ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

Security Day | 2. Februar 2023

Programm

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

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

Vortrag zum Spannungsfeld „Security Blackout“
Gerald Kortschak, sevian7

Informatik & Security an der FH St. Pölten – das sind wir!
Robert Luh | Studiengangsleiter IT Security (BA)
Marlies Temper | Studiengangsleiterin Data Science & Business Analytics (BA)
Thomas Felberbauer | Studiengangsleiter Smart Engineering (BA)

Vortrag „Vereinbarkeit Studium und Bundesheer“
Philipp Leonhardsberger, Österreichisches Bundesheer

Weiterführend stehen folgende **Programmvarianten** zur Auswahl:

Variante A – Workshops/ Vorträge:

10:00–10:10 Uhr Pause

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

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

2. Teil – Programm Großer Festsaal, Gebäude A

12:10–12:40 Uhr Vortrag „Security Blackout“
Tobias Zillner | FH-Lektor

12:40–13:20 Uhr Vortrag „Innovative Forschung und Entwicklung an der FH St. Pölten.
Wie Studierende beim Forschen zum Troubleshooter der Zukunft werden!“
Peter Kieseberg & Sebastian Neumaier | Institut für IT Sicherheitsforschung

13:20–13:40 Uhr	Vortrag „Der Spion in deinem Handy“ Christina Schindlauer, Bundesministerium für Inneres – Direktion Staatsschutz und Nachrichtendienst
13:40–14:00 Uhr	Siegerehrung Workshops „Hacking Challenge” & „Escape the Room” Simon Tjoa | Departmentleiter Informatik & Security
14:00–15:00 Uhr	Live-Hacking Daniel Haslinger und Christoph Lang-Muhr | FH-Dozenten
15:00 Uhr	Veranstaltungsende

Variante B – Hacking Challenge:

10:00–10:15 Uhr	Pause
10:15–13:00 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:

10:00–10:15 Uhr	Pause
10:15–13:00 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: **Information Gathering mit Google Hacking und Shodan | Basic**

In diesem Workshop wird auf eine besondere Seite von Internetsuchmaschinen eingegangen: Ihre Bedeutung als Hacking-Werkzeug. In praktischen Übungen wird demonstriert, wie Google & Shodan 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 befindet sich im Umbruch. Digitale Technologien wie Datenbrille & Co halten Einzug in alle Bereiche. Diese Veränderung wird, wenn es um die Herstellung von Produkten geht, gemeinhin als vierte industrielle Revolution, Industrie 4.0, bezeichnet. Der Workshop des Studiengangs Smart Engineering bietet Schüler*innen einen eindrücklichen und unterhaltsamen Einblick, wie die Produktion der Zukunft aussehen wird, welche technischen Lösungen dafür bereits heute erforscht werden oder auch welche Herausforderungen, z. B. im Bereich der Security, damit einhergehen. Die Teilnehmer*innen erhalten die Möglichkeit, aktuelle Augmented-

Reality-Technologien kennenzulernen, 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: **Deep Fakes | Basic**

Mit Methoden der künstlichen Intelligenz ist es möglich, Personen in Bildern oder Videos durch andere zu ersetzen. Ein sehr bekanntes Beispiel ist das Video vom ehemaligen Präsidenten Barack Obama, der schlecht über Donald Trump redet. In diesem Workshop werden selbst Fake-Videos erstellt, in denen bekannte Persönlichkeiten ausgetauscht werden, etwa Bundespräsident Alexander van der Bellen singt als Reinhard Fendrich „I am from Austria“. Zusätzlich wird die Technologie dahinter leicht verständlich 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 programmieren mit Python** | **Medium**

Ist es möglich, in kürzester Zeit die Grundlagen des Programmierens zu erlernen, ohne auf Hilfsprogramme zurückgreifen zu müssen? – Wenn NAO, der humanoide Roboter, mit im Spiel ist: Auf jeden Fall! In diesem Workshop lernen Sie, was Algorithmen sind und wie diese beim Schreiben von Programmbefehlen eingesetzt werden. Mit diesem Wissen geht es ans Programmieren in Python: Sie werden mit der Syntax vertraut gemacht und üben direkt am Roboter. Die Interaktion mit NAO ist dabei ein essentieller Bestandteil des Konzepts. Der Spaß, den die Arbeit mit dem Roboter mit sich bringt, steigert die Motivation der Teilnehmer*innen enorm. In der Abschlusspräsentation lassen Sie den humanoiden Roboter NAO erfolgreich die selbst erarbeiteten Choreographien in der neu erlernten Programmiersprache Python durchlaufen.

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: **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 10: **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.