University of Applied Sciences St. Pölten

# Security Day | 27. Jänner 2026

## 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: Industroyer: Blackout auf Knopfdruck
Peter Eder-Neuhauser, Limes Security

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

12:40–13:10 Uhr Informatik & Security an der USTP – das sind wir!

Robert Luh | Studiengangsleiter IT Security (BA)
Marlies Temper | Studiengangsleiterin Data Science & Artificial Intelligence (BA)
Thomas Felberbauer | Studiengangsleiter Smart Engineering (BA)

13:10–13:30 Uhr Siegerehrung „Hacking Challenge” & „Escape the Room”
Herfried Geyer | stv. Studiengangsleiter IT Security

13:30-14:30 Uhr Alltagshacks

Daniel Haslinger | Hochschul-Dozent Department Informatik und Security
Christoph Lang-Muhr | Studiengangsleiter Information Security

14:30 Uhr Veranstaltungsende

### Variante B – Hacking Challenge:

10:10–12:30 Uhr Hacking Challenge (integrierte Mittagspause)

12:30–14:30 Uhr Weiteres Programm & Vorträge im Großen Festsaal, Gebäude A inkl. Siegerehrung

---

## Übersicht Vortrag & Workshops

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

### Vorträge:

**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.

**V 2: Einblick in die Welt des OT- und (I)IoT-Hackings | Advanced**

In diesem Format geben wir, CyberDanube, einen kompakten Einblick in die Welt des OT- und (I)IoT-Hackings. Wir starten mit einer praxisnahen Theorieeinführung: Was unterscheidet OT von IT? Wo liegen typische Schwachstellen? Welche Anforderungen stellen Unternehmen an sichere Industrie-Umgebungen? Dazu werfen wir auch einen Blick auf typische Kundenanforderungen – etwa sichere Fernwartung, robuste Netzwerksegmentierung, Schutz vor Manipulation, Absicherung von Feldgeräten sowie sichere Update- und Firmware-Prozesse. Außerdem zeigen wir, welche Themen wir in realen Industrieprojekten besonders häufig bearbeiten, z. B. Security Assessments von Steuerungen, IoT-Geräten und Gateways, Protokollanalyse, Architektur-Reviews und Absicherung von Produktionsnetzwerken. Wo es passt, verknüpfen wir diese Inhalte mit Forschung

und Lehrthemen der USTP und verweisen auf "unseren" Weg dahin.
Im Anschluss folgt ein kurzer Showcase, der praxisnah demonstriert, wie Hacking an IoT-Geräten konkret aussehen kann. Dafür haben wir eine Firmware-Emulationslösung (MEDUSA) vorbereitet, anhand derer die Teilnehmer live nachvollziehen können, wie ein Industrie-Gerät analysiert und potenzielle Schwachstellen sichtbar gemacht werden.

### V 3: IPv4-Netzwerke mit IPv6 angreifen: Sicherheitsrisiken durch Dual Stack | Advanced

Moderne Betriebssysteme haben IPv6 standardmäßig aktiviert und laufen meist im Dual-Stack-Modus (IPv4 + IPv6 gleichzeitig). Das ist zwar wichtig für die Netzwerk-Kompatibilität, bringt aber auch Sicherheitsrisiken mit sich – besonders in Netzwerken, die sich fast nur auf IPv4 konzentrieren und IPv6-Sicherheit kaum beachten.

In diesem Vortrag geben wir einen Überblick über die wichtigsten Mechanismen zur automatischen IPv6-Konfiguration und zeigen, wie Angreifer diese nutzen können, um IPv4-Netzwerke anzugreifen. Wir demonstrieren, wie IPv6-Funktionen wie SLAAC, Router Advertisements, DHCPv6 oder DNS64/NAT64 in Dual-Stack-Umgebungen missbraucht werden können. Mit Wireshark analysieren wir verschiedene Angriffe und schauen uns an, wie die betroffenen Betriebssysteme auf Paket-Ebene darauf reagieren. Abschließend stellen wir sinnvolle Schutzmaßnahmen vor, um die gezeigten Probleme zu entschärfen.

## 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 Lab | 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: Tauche 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: System Exploitation | Advanced

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 AdministratorInnen und TesterInnen 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 8: 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 9: Hands-on Cloud Computing Lab | Advanced

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 10: 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.

## WS 11: Escape the Room und Lockpicking | Medium

Physical Security und Lockpicking Workshop

Wie realistisch ist es eigentlich, wenn in Spielen, Filmen oder Serien Schlösser im Vorbeigehen geknackt werden? Wie funktionieren Schlösser überhaupt? Was macht ein Schloss sicher? Und lässt sich ein Schloss im echten Leben tatsächlich ohne Schlüssel öffnen? Genau diese Fragen tauchen auf, wenn es um das Thema Lockpicking geht. Lockpicking bedeutet das gewaltfreie Öffnen von Schlössern ohne den passenden Schlüssel. Doch reines Wissen reicht nicht aus – spannend wird es vor allem, wenn man selbst versucht, ein Schloss zu öffnen.

Für alle, die sich für dieses Thema interessieren, bieten wir einen Workshop an, um die Grundlagen von Physical Security und Lockpicking kennenzulernen. Vorkenntnisse sind nicht erforderlich, aber auch alle, die bereits erste Erfahrungen gesammelt haben, sind herzlich eingeladen.

Im Hands-On-Workshop könnt ihr euch an verschiedenen Schlössern ausprobieren – mit Werkzeug, das wir zur Verfügung stellen. Von einfachen bis hin zu komplexen Schlössern, von selbstgebautem bis zu professionellem Equipment ist alles dabei. So habt ihr die Möglichkeit, unterschiedliche Techniken selbst auszuprobieren.

Escape Room

Team Battle 4 vs 4, tank vs bunker, Difficulty: medium, Spieldauer ca. 25 Minuten, Thema: Cyber Security Awareness mit Hauptaugenmerk auf Fake News und Desinformation

## WS 12: Hacking Challenge | Advanced (= 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) 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.