Security Day | 30. Jänner 2018

Programm

08:15–09:00 Registrierung

09:00–10:00 Heiß diskutiert: IT Sicherheit virtuell vs. real
Diskurs: FH-Prof. Dipl.-Ing. Johann Haag | Studiengangsleiter IT Security sowie Studierende und AbsolventInnen

10:00–11:15 „Die Zukunft der IT Sicherheit und ihr Einfluss auf unser Leben 2.0“
IT Security ist zu einem entscheidenden Faktor in unserem täglichen Leben geworden. Es geht nicht nur um Daten, sondern um unmittelbare Einflüsse bis hin zur Gefahr für Leib und Leben. Wer ist bereit dafür, das aktiv mitzugestalten?
Dr. Wieland Alge | Barracuda Networks

Weiterführend steht folgendes Parallel-Programm zur Auswahl:

Variante A:
11:15 –12:00 Mittagspause

12:00 –13:30 Workshops

13:30 –13:50 Pause

13:50 –15:00 Ethik und Kriminalität: Wie verändert Digitalisierung unser Leben?
SpezialistInnen diskutieren über Cyber Crime, Big Data und Privacy Herausforderungen.

Variante B:
11:15 –15:00 „Hacking Challenge“ inkl. Preisverleihung (Mittagspause ist integriert)

Moderation: Alexander Krenn, MSc | Österreichische Lotterien GmbH

Workshops 1-5 und 8-11: keine Vorkenntnisse notwendig

WS 1: iOS Forensik – Unlocking iPhone Secrets

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 SpezialistInnen 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

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

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

Im Workshop Google Hacking wird auf eine besondere Seite von Internetsuchmaschinen 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

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 NutzerInnen auswerten, wie man ohne Spuren zu hinterlassen im Internet surft und man verschlüsselte Nachrichten mit Freunden austauschen kann.

WS 8: Hands-on Industry 4.0

Die Arbeitswelt befindet sich im Umbruch. Digitale Technologien wie Smartphone, Tablet, 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 SchülerInnen einen eindrücklichen und unterhaltsamen Einblick, wie Produktion der Zukunft aussehen wird, welche technischen Lösungen dafür bereits heute erforscht werden aber auch welche Herausforderungen, z. B. im Bereich der Security, damit einhergehen. Die TeilnehmerInnen erhalten die Möglichkeit Hands-On mit Augmented Reality Technologien wie der Microsoft Hololens zu arbeiten, sie erleben anhand eines Cocktailroboters und eines 3D-Druckers was „individuelle Produktion“ bedeutet und sehen aber auch die Auswirkungen wenn es hier Sicherheitslücken gibt.

WS 9: Data Science Innovations

Produktvorschläge, computergestützte Übersetzung, selbstfahrende Autos oder gezieltes Marketing sind nur einige Anwendungsgebiete in denen AbsolventInnen von Data Science Studiengängen eine entscheidende Rolle spielen.
Interessiert, was noch alles möglich ist und warum Data Scientist zum zweiten Mal in Folge zum besten Job gewählt wurde?
Dann besuchen Sie den Vortrag in dem Sie mehr über Innovationen, welche Data Science Technologien bereits ermöglicht haben, erfahren.

WS 10: Privacy Diskussion: Wie viel sind Sie wert?

Das Thema Datenschutz wurde in letzter Zeit immer prominenter und wichtiger. Speziell durch Leaks von (teils intimen) Fotos und persönlichen Details von Prominenten hat sich auch eine gewisse Sensibilität für das Thema in der Öffentlich breit gemacht. Auf der anderen Seite finanzieren sich viele Gratisdienste wie Facebook und Co. durch das Sammeln von Daten und der zielgerichteten Schaltung von Werbung. Ohne persönliche Daten würden diese Dienste Geld kosten, dennoch sind sie auch heute nicht gratis – denn Sie sind nicht die Kundin/der Kunde, sondern das Produkt, das an Werbende verkauft wird.

In diesem Workshop diskutieren wir, wie viel Ihnen Ihre Daten wert sind, wie Sie sich besser schützen können und wie die zukünftigen Entwicklungen im Bereich des Schutzes persönlicher Daten aussehen.

WS 11: Social Intrusion - Angriffsziel Mensch

Der Mensch ist die Schwachstelle eines jeden Sicherheitssystems. Mit Methoden des Human-Hacking versuchen AngreiferInnen (Social Engineers) Menschen zu manipulieren. Auf diese Art werden nicht komplexe Sicherheitssysteme direkt angegriffen sondern vielmehr umgangen. In diesem Workshop zeigen wir Methoden und Vorgehensweisen von AngreiferInnen, um diese erkennen zu können 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 finden, oder anderweitige Wege zu finden, das Gegenüber für sich zu gewinnen.

Workshops 6-7: Vorkenntnisse notwendig

WS 6: System Exploitation - Wie Hacker Systeme gezielt angreifen

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 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 7: Arbeiten am schlagenden Herzen – Die Heartbleed-Schwachstelle zum selber Testen

Die Heartbleed-Sicherheitslücke wurde im April 2014 bekannt, worauf sehr schnell die notwendigen Patches zur Verfügung gestellt wurden. Allerdings ist diese Schwachstelle durch die große Verbreitung von openSSL auf vielen Geräten Servern aufgetreten. Leider kann es lange dauern bis auf allen Systemen die notwendigen Updates installiert wurden und dadurch kann es vorkommen, dass es anfällige Server gibt, obwohl diese Probleme schon gelöst wurden.
Nun 3,5 Jahre später wird in diesem Workshop vermittelt wie viel bzw. wie wenig Arbeit AngreiferInnen aufwenden müssen um diese Lücke auszunutzen.

Vorkenntnisse: Basiswissen über Webtechnologien (HTTP/HTTPS) und Netzwerktechnik (Netzwerkpakete, Wireshark)

Hacking Challenge

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 TeilnehmerIn ist ein Notebook mitzubringen. Nähere Details folgen gerne nach der Anmeldung.