Universität Konstanz

Programm

Mittwoch, 14.03.2018

Raum: E404, Universität Konstanz

Uhrzeit	
13:30	Begrüßung durch Prof. Dr. Manfred Paul
13:35	**Prof. Dr. Hanno Langweg** (HTWG Hochschule Konstanz)
(30 Min.)	Vortrag: „Erfahrungen mit Capture the Flag in der Lehre von IT-Sicherheit“ Der Vortrag berichtet über die Teilnahme an CTF-Wettbewerben („Capture the Flag“) im Rahmen von Lehrveranstaltungen zur IT-Sicherheit. CTFs erhöhen die Motivation Studierender in IT-Sicherheit und lehren das Finden und Ausnutzen von Schwachstellen in IT-Systemen. Unklar bleibt, ob das Lernziel der Herstellung sicherer Systeme durch CTF-Wettbewerbe gefördert wird. An der HTWG Konstanz wurde in mehreren Projekten systematisch untersucht, wie sich CTF-Wettbewerbe in die Lehre sinnvoll integrieren lassen. Der Referent Dr. Hanno Langweg ist seit 2014 Professor für Datensicherheit in cloudbasierten Systemen und IT-Forensik an der HTWG Konstanz.
14:05	**Florian Fankhauser** (Technische Universität Wien)
(30 Min.)	Vortrag: „Erkenntnisse und Erfahrungen mit unterschiedlichen Arten von CTF-Contests in der (Universitären) Ausbildung“ Der Vortragende stellt kurz unterschiedliche Formen von CTF-Contests vor, präsentiert Beispiele für Anforderungen und Lösungen von Herausforderungen bei der Anwendung von CTF-Contests in der Lehre, gibt Einblick in Lessons Learned aus der langjährigen Durchführung dieser sowie Impulse über den Nutzen von CTF-Contests in der Weiterbildung von IT-Personal. Florian Fankhauser hält mehrere Vorlesungen an der TU Wien und ist dort Leiter der Forschungsgruppe Establishing Security (ESSE). Herr Fankhauser ist anerkannter Spezialist im Bereich von (Cyber-)IT-Attacken und -Defence.
14:35	Gemeinsame Diskussion
(20 Min.)	Prof. Dr. Hanno Langweg, Florian Fankhauser, ggf. Sebastian Klipper

14:55	**Dr. Marco Ghiglieri** (Technische Universität Darmstadt)
(45 Min.)	Vortrag: "Wie Sie sich mit effektiven Maßnahmen gegen Phishing und andere gefährliche Nachrichten schützen können" Angriffe über gefährliche Nachrichten stellen nach wie vor eine große Bedrohung dar, da die automatische Erkennung gerade bei plausibel aussehenden Nachrichten oft Stunden oder Tage hinterher hängt. In dieser Zeitspanne ist der Benutzer gefragt. Bisherige Sensibilisierungsmaßnahmen sind wenig effektiv. Im Rahmen eines vom BMWi geförderten Projektes hat die TU Darmstadt Sensibilisierungsmaßnahmen entwickelt, die nachweislich effektiv sind. Ziel des Vortrages ist es unser Konzept sowie verschiedene Umsetzungsformen vorzustellen. Weiterhin geben wir konkrete Hinweise, wie Nachrichten gestaltet werden sollten, damit Benutzer diese effektiv überprüfen können. Der Referent Dr. Marco Ghiglieri arbeitet seit April 2017 als Postdoc in der Arbeitsgruppe von Prof. Dr. Melanie Volkamer an der TU Darmstadt.
	Pause
16:00	**Sebastian Klipper** (CycleSEC GmbH, Hamburg)
(45 Min.)	Vortrag: "Homo Carens Securitate: Der Mensch, der den Mangel an Sicherheit leidet: Vom Homo Oeconomicus zum Weird Human." In den Wirtschaftswissenschaften kennt man die Figur des Homo Oeconomicus als vorausschauenden, reaktionsschnellen Nutzenmaximierer. In der Informationssicherheit wird das Modell Tag für Tag widerlegt. Hier agiert der Homo Carens Securitate. Er trifft seine Entscheidungen auf Grundlage von hoher Risikobereitschaft bis hin zur Gefährdung eigener Gewinnchancen und mit mangelhafter Voraussicht und Reaktionsfähigkeit. Vom Social Engineer wird er zum Weird Human umprogrammiert. Sebastian Klipper ist der Gründer und Geschäftsführer der CycleSEC GmbH mit Sitz in Hamburg und Lehrbeauftragter an der Wilhelm Büchner Hochschule (Hessen).
16:45	Besprechung des weiteren organisatorischen Vorgehens im AK
(30 Min.)	Vorstellung und kurze Diskussion des Angebots für Schwachstellentests für ZKI Mitglieder (Prof. Dr. Stefan Schwarz)
	Ende des ersten Tages
19:00	Gem. Abendessen **Tamaras Weinstube - Zum Guten Hirten**, Zollernstraße 6 - 8, 78462 Konstanz

Donnerstag, 15.03.2018

Raum: E404, Universität Konstanz

Uhrzeit	
08:30	Kaffee und kalte Getränke
09:00	Begrüßung durch Prof. Dr. Manfred Paul
09:05	**Prof. Dr. Stefan Schwarz** (Universität der Bundeswehr)
(40 Min.)	Vortrag: Awarenessmaßnahmen an der Universität der Bundeswehr München Während die technischen Maßnahmen zur IT-Sicherheit klare Grenzen aufweisen steigt die Gefährdung durch gezielte Angriffe auf die Nutzer der Endgeräte stetig an. Dies liegt vor allem darin, dass ein Großteil der Nutzer durch die üblichen Maßnahmen zur Awareness nicht oder nicht zielführend erreicht werden können. Dies zeigen beispielsweise interne Untersuchungen zum konkreten Verhalten bei Phishing-Angriffen an der Universität der Bundeswehr München. Es gibt dabei auch keinen Zusammenhang zwischen Ausbildung und Position der Opfer, was wiederum zielgerichtete Awarenessmaßnahmen in Form von klassischen Aufklärungen erschwert. Auch eine konkrete Sensibilisierung von Betroffenen zeigt in der Regel nur kurzzeitige Wirkung. In diesem Vortrag wird daher die Möglichkeit vorgestellt, durch wiederholte Simulation von gezielten Angriffen die Awareness der Anwender zu steigern und diese Awareness auch auf einem Mindestlevel zu halten. Der Referent Prof. Dr. Stefan Schwarz ist Leiter des Rechenzentrums der Universität der Bundeswehr München.
09:45	**Oliver Pyka** (Pyka Business, Giebelstadt bei Würzburg)
(40 Min.)	Vortrag: "Compliance und Sensibilität aus der Sicht der IT-Administration" Systemadministratoren sind die Personen, die permanent mit sensiblen Informationen umgehen und Zugriff auf Daten mit sehr hohem Schutzbedarf haben. Es ist eine Herausforderung, damit einhergehende Verantwortung sich jeden Tag erneut ins Bewusstsein zu rufen. Wie es gelingen kann, diese Achtsamkeit dauerhaft auf einem hohen Level zu halten und welche Erfahrungen existieren, wenn dies nicht geschieht oder die passenden Rahmenbedingungen fehlen, erläutert dieser Vortrag. Oliver Pyka ist freiberuflicher IT-Berater mit Sitz in Giebelstadt, stellvertretender Leiter der Datenbank Community der Deutschen Oracle Anwendergruppe (DOAG) und SECUTAIN Botschafter.

10:25 **Andreas Schütz** (Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt)

(40 Min.) Vortrag: "Mobile Security Awareness: Überzeugen Sie Ihre Mitarbeiter, mobile Endgeräte sicher zu nutzen"

Sei es das Sperren des Displays oder das richtige Reagieren beim Verlust eines Gerätes: Mitarbeiter müssen für wichtige Verhaltensweisen im Umgang mit mobilen Endgeräten sensibilisiert werden. Dennoch werden die Gefahren, die von mobilen Endgeräten ausgehen in Unternehmen oft vernachlässigt. Fehlende Richtlinien oder fehlende Prozesse machen es dem Anwender nicht einfach, sich richtig zu verhalten. Andreas Schütz präsentiert in seinem Vortrag aktuelle Forschungsergebnisse hinsichtlich des Ist-Zustandes für mobile Sicherheit. Dabei geht er im ersten Schritt darauf ein, welche Grundlagen geschaffen werden müssen, bevor an sinnvolle Mitarbeitersensibilisierung überhaupt erst zu denken ist. Anschließend erklärt der Vortrag wie Erkenntnisse der Sozialpsychologie in Unternehmen genutzt werden können, um maßgeschneiderte Kampagnen zur Erhöhung der Mobile Security Awareness zu erstellen. Durch die Integration des Prozesses in ein ISMS, können parallel zur Sensibilisierung auch organisatorische und technische Hürden beseitigt werden, die dem sicheren Umgang mit mobilen Endgeräten im Weg stehen.

Andreas Schütz ist wissenschaftlicher Mitarbeiter in der Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt. In seiner Promotion setzt er sich mit Informationssicherheit und Security Awareness auseinander.

Pause

11:25 **Michael Sauer** (Manfred Donike Institut für Dopinganalytik e.V.)

(40 Min.) Vortrag: "Buy-In: Wie sage ich es dem Chef? Die Entscheidungsebene für IT Sicherheit interessieren und sensibilisieren"

In der eigentlich kurzen Frage „Wie sage ich es dem Chef“ verbirgt sich ein extrem komplexes Konstrukt von Technologien, Methoden zur Kommunikation und vor allem Einfühlungsvermögen in die unterschiedlichen Bedürfnisse der beteiligten Akteure. Nicht selten fällt es gestandenen IT Leitern schwer, die für sie offensichtlich einfachen technischen Sachverhalte zur Gewährleistung der IT Sicherheit so an den oder die Chefin zu bringen, dass dort die Einsicht zur Ressourcenfreigabe erzielt wird. Noch weniger wahrscheinlich ist, dass das bloße Benennen von Bedrohungen, Gefahren und Risiken in der Führungsetage Überzeugung für die Sache hervorruft. Der Vortrag schlägt eine Brücke zwischen der Technik zur Gewährleistung von Sicherheit und dem menschlichen Bedürfnis auf Sicherheit, um darauf aufbauend Möglichkeiten und Grenzen zur Sensibilisierung oder sogar Verhaltensänderung darzustellen.

Michael Sauer ist wissenschaftlicher Mitarbeiter am Manfred Donike Institut für Dopinganalytik e.V. Seit 2000 ist er dort und am Institut für Biochemie der Deutschen Sporthochschule Köln Leiter der IT.

12:15 (30 Min.)	Diskussion mit dem Auditorium: Wie können Kollegen und Vorgesetzte effektiv und effizient für Informationssicherheit sensibilisiert werden und was sind die Erfolgsfaktoren für Awareness-Maßnahmen?
12:45 (45 Min.)	Weiteres Vorgehen und Themen im AK für die Herbsttagung Feedbackrunde zum Tagungsformat, Abschluss und Verabschiedung
	Ende der Veranstaltung