Enterprise IT Security

Workshop, 04.April 2019 (09:00 bis 16:00 Uhr)
Hamburg, Lindner Park-Hotel Hagenbeck

Für eine erfolgreiche Digitalisierung bedarf es einer adäquaten Adressierung der IT-Sicherheit. Die weitgehend automatisierten Geschäfts-, Management- und Fertigungsprozesse müssen während der Entwicklung und der Ausführung die Sicherheitsanforderungen erfüllen. Das allgemeine Bedrohungslage steigt durch die Existenz von KI enorm an, da die Angriffstools durch Maschine Learning an Effektivität und Effizienz gewinnen und dadurch der Faktor KnowHow des Angreifers an Einfluss verliert. Der Verteidigung muss daher ebenfalls KI sinnvoll einsetzen oder zumindest evaluieren. Im Rahmen des Workshops soll auf verfügbare Ansätze und praktische Erfahrungen im Umgang mit Maschine Learning bei IT-Security bei großen, aber auch bei klein- und mittelständischen Unternehmen eingegangen werden. Ebenso sollen Vorraussetzungen diskutiert werden, damit die IT-Security von KI-Technologien, insbesondere Maschine Learning, profitieren können. Die einführende Keynote geht auf Sicherheits- und Compliancefragen ein, die grundsätzlich auch bei der Bereitstellung bzw. bei der Verwendung von KI in Sicherheitsapplicationen zu berücksichtigen sind.

Session 1 - Keynote im Rahmen der ECC-Tagung (09:15 Uhr)

Jens Borchers (BfI Hamburg)

Keynote: Compliance und IT-Security - kommt die Bedrohung immer von außen?"

Eröffnung/Start des Workshops

Session 2 – IT Security (10:30 Uhr):

Sandro Hartenstein (Freelancer)

IT Security und Maschine Learning

- *Basics der IT Security*
- *Maschine Learning für besser IT Security*

Prof. Dr. Ivo Keller (TH Brandenburg)

Intelligente Sicherheit durch gemeinsame Sprache

- *gemeinsame Taxonomie*
- *kooperative IT-Produktion*

12:00 bis 13:30 Mittagspause

Session 3 Anwendung / Nichtanwendung von ML (13:30):

Sandro Hartenstein (Freelancer)

IT Security mit ML im Einsatz

- *Angriffsvektoren durch ML: Maleware*
- *Security Testing mit ML: Deepsploit*

Steven Schmid (DB Station&Service AG)

Port Security mittels Network Access Control –

Herausforderungen und Ansätze

- *Bestandteile und Rahmenbedingungen von IEEE 802.1x*
- *Nutzenpotentiale durch Machine Learning*
- *Proof of Concept mittels Pilotprojekt*

15:00 bis 15:30 Kaffeepause

Session 4 – ML im Sicherheitskontext (15:30):

Holger Könnecke (Uni Potsdam)

Sicherheitsorientierte Digitalisierungsansätze in der operativen Sicherheitswirtschaft

- *Welche Digitalisierungsansätze gibt es zurzeit*
- *Welche Gefahren ergeben sich daraus*
- *Machen wir uns abhängig und verlieren wir die Steuerungselemente*

Die Unterlagen und Ergebnisse der Diskussionsrunden werden zeitnah auf der Webseite der ceCMG (*www.cecmg.de*) publiziert. Änderungen am Programm sind unter Vorbehalt möglich. Für Verpflegung vor Ort wird gesorgt. Für die Teilnahme an der Veranstaltung ist eine Anmeldung zur Enterprise Computing Conference (ECC 2019) erforderlich. Für Mitglieder der ceCMG-, DASMA-, GI- und ASQF gilt eine reduzierte Teilnahmegebühr. Über die Teilnahmegebühr erhalten Sie eine Rechnung der ceCMG e.V. (Central Europe Computer Measurement Group). Eingeschriebene Studenten erhalten einen kostenfreien Zutritt.

Weiteren Informationen und Anmeldung unter: *http://www.cecmg.de*

Kontakt: *Susanne Mund – sekretariat@cecmg.de*

Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Diese Veranstaltung wird durch das Berliner Competence Center Digitalisierung der HWR Berlin am Fachbereich 2 unterstützt!