Applied industrial cybersecurity by Kaspersky at the Deggendorf Institute of TechnologyOctober 14 and 15, 2019, Kaspersky ICS CERT experts provided an exclusive two-day training program on applied industrial cybersecurity at the Deggendorf Institute of Technology (DIT) for graduate students specializing in cybersecurity, as well as for 30 students from various DIT courses.



The training included a combination of theoretical sessions and hands-on activities:

* Resolving cybersecurity issues in different industries: manufacturing, energy, oil and gas systems and smart cities;



* In-depth discussions about typical IoT vulnerabilities based on Kaspersky ICS CERT research;



* A special section on how to convince vendors to fix vulnerabilities that they treat as ‘features by design’ – based on Kaspersky ICS CERT research into Gemalto’s Sentinel LDK case.



The trainers provided interactive sessions with real-life exercises around IoT security and YARA rules. The students learned about known attacks on ICSs in the modern world, the work of the IIC and the IoT Security Maturity Model (SMM). The two-day event also included a game session highlighting the main problems solved by SMM in which the participants acted as stakeholders and developers while systematically building a smart city.

 

Another highlight was the Kaspersky Interactive Protection Simulation game that saw students build a cyberdefense strategy at a water processing plant.

In parallel with the training course, a research meeting was held between scientists and researchers from DIT and Kaspersky, where the participants discussed potential areas for cooperative research on different industrial cybersecurity topics, as well as the implementation of an IT security laboratory at the technology campus in Teisnach.



Both students and professors from the Deggendorf Institute of Technology and the Kaspersky ICS CERT team decided to move forward together – conducting joint research, building a new cyberlab and providing expert training for specialists as well as students.

## Participant reviews

The following responses were typical of the feedback we collected online:

*“Very nice to see some ‘real-world’ security-checks/vulnerability testing!”*

*“Very nice and interesting presentations! The second YARA example went a little over our heads! ;) But very nice, that we did some examples!”*

We also received some useful suggestions on how to improve the course. Some participants asked for additional slides during the overall presentation, while others would have liked to spend more time on certain topics.

**Ekaterina Rudina, Head of Security Analysis at Kaspersky ICS CERT**:

*“What impressed me about this audience was that they were equally enthusiastic and receptive to all sorts of information – the ‘geek’ stuff, the ‘legal’ stuff and the ‘fun’ stuff, details on threats specific to the energy and oil and gas sectors, a masterclass on YARA rules, the regulatory and compliance aspects of cybersecurity and a game on protecting a smart city, to name just a few things. It seemed to me that they realized all these things are different facets of the same big issue and were keen to put their newly acquired knowledge into practice.”*

**Professor Andreas Grzemba, Vice President of Applied Research and Technology Transfer at DIT**, thanked Kaspersky for a well-organized training program that was extremely useful for both the participants and the institute in general.

*“We are honored that our students had the opportunity to gain first-hand knowledge about the latest industrial cyberthreats and cybersecurity issues from Kaspersky ICS professionals. With this successful training program, the Deggendorf Institute of Technology and the Kaspersky ICS CERT team have kicked off a series of practical Kaspersky expert workshops, which will now be a regular feature of our study programs,” commented Professor Grzemba.*

*“Moreover, with the implementation of a new ICS Cybersecurity Lab in Teisnach, we will work together with Kaspersky researchers on real research topics and analyze the threats and malware facing a variety of industries. Combining the knowledge of both our organizations and finding ways to prevent cyberattacks together is a huge step towards a secure and safe future.”*