Kaspersky Interactive Protection Simulation

KASPERSKY lab

Protecting Japan's critical industrial infrastructure

鶴岡高専

National Institute of Technology,Tsuruoka College

www.tsuruoka-nct.ac.jp

Japanese vocational training provider arms its students with practical steps to tackle cyber threats, with Kaspersky Interactive Protection Simulation (KIPS).

Education

- Located in Tsuruoka, Yamagata, Japan
- Using Kaspersky Interactive Protection Simulation (KIPS)

“What’s fascinating about this game is that it does not give you example answers. Just like in real situations, it fosters your ability to anticipate attacks and respond accordingly.”

Atsushi Sato
PhD (engineering)
Head Professor
Electricity and Electronics Course
Creative Engineering Dept.
Tsuruoka National College
of Technology

Tsuruoka National College of Technology (TNCT) is a higher education institution specializing in engineering, based in Yamagata, Japan. The organization was founded in 1963, and specializes in IT, electrical and electronics, mechanical engineering, and industrial chemistry.

Professor Atsushi Sato is Head Professor in the college’s Creative Engineering Department. He teaches computer engineering, digital control systems and IoT, while appointing as a Cyber Crime Technical Adviser for the Yamagata Police.

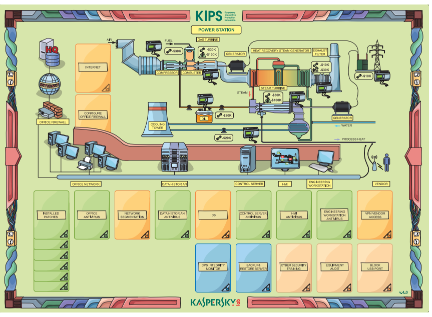
In 2018 Professor Jun Sato carried out a cyber security exercise in collaboration with the Prefectural Police. The objectives of the exercise were to explore attacks on local critical infrastructure providers and small-to-medium businesses.

Challenge

Cyber security is part of the students’ ongoing training at TNCT. It is seen as a basic skill for students; a skill that will become critical for all industrial equipment engineers.

Electric, gas, traffic, communications and production facilities are the perfect target for cyberattacks. As part of its cyber security training, TNCT wants students to identify the potential for cyber attacks early – and be prepared to take appropriate first steps. Increasingly, the college wants these skills to be shared across engineers and management involved in the control systems, not just a limited number of security experts.

“There’s a lack of IT skills education in Japan,” says Professor Sato. “There is a need to create a bottom-up approach to training, including the ability to respond to cyber threats. Cyber security education should be seen as a general IT skill.” However, classroom-based knowledge is not always ideal. TNCT wanted students to explore more practical approaches. “We want to provide students with the skills and confidence to respond rapidly and flexibly to large-scale serious incidents triggered by the latest attack tactics.”



Kaspersky Interactive Protection Simulation: KIPS

Seven enterprise scenarios for all vertical sectors: Oil & Gas, Water Plant, Power Station, Transportation, Bank, Corporation, e-Government

■ The purpose of the game

- Protect your company's assets as part of a plant cyber security team
- Find and analyze all pitfalls in cyber security system and make an appropriate incident response to maximize revenue during five turns. Total revenues determine the winner at the end of the game

Kaspersky Lab Solution

In response, TNCT has introduced Kaspersky Lab's board game-style educational simulation, the Kaspersky Interactive Protection Simulation (KIPS).

KIPS is a simulation in which the goal is to protect normal business earnings by minimizing damage from cyber attacks. During each turn, players pick appropriate actions from the cards they were dealt. There are seven scenarios, including a Power Station and Water Plant, Oil & Gas, Bank e-Government, Corporation and Transportation.

As the enterprise is exposed to a cyber attack the players experience the impact on production and revenues, and learn to adopt different business and IT strategies and solutions in order to minimize the impact of the attack and to earn more money. The purpose of the game is to protect your company's assets as part of a plant cyber security team. In the simulation, students have two production lines running, and have to maximize revenue during five rounds. The winner is determined by total revenue at the end of the game.

Professor Sato believes KIPS is an extremely well-built simulation: "KIPS is the only exercise program I know that allows students to learn specific approaches to cyber security by following realistic scenarios.

"What's fascinating about the game is that the system displays who's ahead by automatically keeping score, but it doesn't give you example answers about how you should've acted. Just like in real situations, it fosters your ability to anticipate attacks yourself and respond accordingly."

Real-life detail adds to authenticity

Professor Sato first used KIPS as part of a cyber security exercise held in conjunction with the Yamagata Police HQ's Cyber Crime Unit. In this exercise, Kaspersky Lab cooperated with important infrastructure providers at one area of the four regions in prefecture.

During the first exercise, around 30 people, including managers from regional public bodies and infrastructure providers were divided into eight teams and played against each other. "Satisfaction with the exercise was high," says Professor Sato, "thanks to the ability to meet local people in cyber security and get some practical learning. You see the results improving every time we switch the team make-up. It might be hard to hold this kind of event with the Prefectural Police very often, but it is definitely something we're considering as an ongoing event."

He says industrial cyber security will inevitably become a greater concern as more industries connect production via IoT.

Aside from the dozen exercises conducted with TNCT students, Professor Sato has observed KIPS exercises carried out elsewhere in Japan. He says the program is applicable for players at all levels, from beginners to advanced.

"It provides invaluable experience, for students and non-students. All the KIPS scenarios are well thought out and produced. People who work with production systems can imagine the work site and picture the steps leading up to situations which should never happen. At the same time, students who have no hands-on experience can get a much clearer image of what kinds of mistakes will lead to those situations than from simple book-learning."

Kaspersky Security Awareness
http://www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness

#truecybersecurity

www.kaspersky.co.jp

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212
info@kaspersky.com
www.kaspersky.com