hochschule mannheim

2021

Simulation provides cybersecurity reality check

kaspersky

BRING ON
THE FUTURE

hs-mannheim.de

Kaspersky Interactive Protection Simulation (KIPS) uses gaming technology to equip students in Mannheim with critical thinking skills needed to anticipate the effects of cybercrime.

Mannheim University of Applied Sciences is one of Germany's most respected academic institutions, specializing in science, technology and engineering.

Higher education
- Germany
- Using Kaspersky Interactive Protection Simulation (KIPS)
- 200 students have been trained using KIPS

"**More than 200 students have been trained using KIPS and I would definitely recommend it to other colleges, universities – and businesses too. It's a great way to create awareness and really emotionally engage people.**"

Professor Dr. Miriam Föller-Nord, Dean of the Department of Computer Science, Mannheim University of Applied Sciences

The university city of Mannheim, located on the Rhine in the German state of Baden-Württemberg, has been a center of engineering excellence since 1898.

Mechanical, chemical and electrical engineering remain an important focus to this day. Now complemented by applied science, technology and social studies faculties, Mannheim University of Applied Sciences is a key research and development center in many domains, including artificial intelligence (AI) and autonomous vehicles. Its goal is to equip its 4,500 students to graduate with a rich mix of skills, ready to contribute to the global economy and wider society.

Challenge

With cybersecurity knowledge, skills and solutions now essential for all industries, businesses and public institutions, the university is committed to high quality, immersive training programs, designed not only to equip its students with essential skills for their future careers but also to ensure that they operate in a cyber secure fashion while studying.

In addition, for many students, investigating the principles widely used in cybersecurity, such as 'defense in depth' and 'need-to-know', provides valuable additional learning opportunities to supplement their core science and technology studies.

Rather than studying security awareness in a one-dimensional textbook style, the university wanted to bring the topic to life. For Professor Dr. Miriam Föller-Nord, Dean of the Department of Computer Science, it was vital to engage with and stimulate students by using a teaching method that enabled them to be hands-on, to experience the real personal danger, jeopardy and fear that cybercriminals cause their victims all over the world every day. In this way, gaining the strategic thinking skills necessary to anticipate and judge how cybercrime could impact business and how to mitigate those negative effects would feel so much more relevant.

In particular, Professor Föller-Nord is a firm believer in the power of gamification as a great way of engaging with students, using the latest technology to simulate real-life cybersecurity scenarios.

The Kaspersky solution

To achieve its goals, the university has developed a close partnership with Kaspersky as part of a pan-European academic cooperation movement to promote innovation, education and training relationships between European universities and business.

"We've been using Kaspersky's board game-style educational simulation KIPS – Kaspersky Interactive Protection Simulation – since 2019 and it has generated a lot of interest in IT security among our students," says Professor Föller-Nord.

"When I first used it, I was stunned – the game is so realistic!"

KIPS, created by a joint team of Kaspersky cybersecurity and computer gaming specialists, features a simulation in which the goal is to protect normal business earnings by minimizing damage from cyberattacks.

During each turn, players pick appropriate actions from the virtual cards they receive. There are ten scenarios across different types of entities that have fallen victim, including a power station and water plant, an oil and gas entity, a bank, LPA, corporation and transport, an airport, the petrochemical industry and a petroleum holding.

Engagement
KIPS' gamification captures the attention of participants

Relevance
The very latest global threat scenarios are recreated

Collaboration
Partners exchange skills and expertise

As each enterprise is exposed to a cyberattack, 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.

"Of course, theoretically you know all these things can happen. But when you then have a very realistic scenario in front of you where, boom, your servers don't work, it feels like real life, it really grabs your attention.

"Suddenly something doesn't work in the company and then you first have to think about what it could be. If a simulation manages to give a user this visceral physical feeling of powerlessness, that means something!

"The game is web-based but it can also be played on-site from the server and comes with a game plan and cards. It is so much more instructive to see events live, including the many possible reactions of the other players, to understand how helpless you are in the face of an attack situation."

Emotional engagement

"In the simulation, different scenarios can be played through in five rounds each," says Professor Föller-Nord.

"It's best to play it in groups, that's when the learning effect is maximized. The game helps players understand that teamwork is one of the key elements of cybersecurity and incident response strategies: quick and coordinated actions help the team be more efficient and at the same time understand that cybersecurity is everyone's responsibility. But you can also play it as a single player. You then have to discover the attack scenarios and find mechanisms to ward them off. Whoever does it best wins and 'earns' the most money.

"We have a cool license that allows us to simulate any number of rounds with an unlimited number of players, to encourage the right attitude towards cybersecurity and influence the right behavior, creating a cybersafety culture. One of the great strengths of KIPS is that Kaspersky's knowledge of the very latest threat scenarios means that the game is a simulation of serious events that are happening right now around the world. Students can see exactly what happens during an attack – that's very powerful.

"So far more than 200 students have been trained using KIPS and I would definitely recommend it to other colleges, universities – and businesses too. It's a great way to create awareness and really emotionally engage people with one of the most important issues we face as a society."

The success of KIPS at the university is also resulting in interest in other Kaspersky training resources.

One of these is Kaspersky ASAP (Automated Security Awareness Platform) which builds an individual's practical cybersafety skills through tailored, interactive and supported activity, with each participant's progress available for monitoring and review.

In the future, the university says that it would like to tap into the pool of experts that Kaspersky can offer to support lectures to its students.

"I think our partnership with Kaspersky through KIPS is excellent and I would like to build on it," concludes Professor Föller-Nord. "It's exciting that there are so many opportunities to collaborate and exchange knowledge and skills."

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security Awareness: kaspersky.com/awareness
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

kaspersky
BRING ON
THE FUTURE