How Germany’s third-largest Landesbank is sharpening its employee awareness of information security with Gamification.

As a financial institution, Landesbank Hessen-Thüringen, better known under its abbreviation “Helaba”, is subject to increasing regulatory requirements and supervisory duties. It does not only rely on state-of-the-art technology to protect the bank in the face of growing threats from cyberattacks. This is because Germany’s third-largest Landesbank in terms of total assets is well aware of how important well-trained personnel are today. “In a sense, our employees form the human firewall. If, despite all our precautions, a phishing attack should actually get through, they are the last line of defense,” says Jürgen Vogt from Helaba’s Information Management department. This is why the Bank invests continuously in training courses, lectures and – an “exciting collection of board games”. This is based on a security course developed by T-Systems, which Helaba is now using on its own throughout Germany. And it is amazing that hardly enough game encounters can be organized to meet employee demand.

PLAYING IN A BUSINESS-CRITICAL CONTEXT

In many companies and organizations it is currently “Game on” instead of “Game over”. For good reason. “Playing is an inherent instinct and it makes lots of things easier,” says Peter Kreutter, Director of the Stiftung Wissenschaftliche Hochschule für Unternehmensführung (WHU), located in Vallendar, on the banks of the river Rhine. Kreutter has been working on the topic of gamification in companies for quite some time. So gambling in the office? Not at all, but rather a serious opportunity to sustainably promote sensitivity to information security issues and security awareness at the workplace. Gamification, i.e. the integration of playful elements into a context that is not part of the game, is currently booming. As researchers at the Danube University Krems in Austria have found out, the integration of playful elements makes it easier to motivate employees to solve complex tasks. Through this informal learning, things can be tried out without triggering the danger of real consequences. Motivation is high, because you want to win. The tension increases with a playful approach, and ultimately drier topics can also be conveyed much more easily.

Awareness expert Vogt also confirms this: “Frontal preaching with PowerPoint is not an effective means of achieving awareness for information security”. A playful format, on the
other hand, minimizes the risk of employees’ “switching off” quickly, keeps their attention high and forces interaction. “As moderators from ISM, we act as competent partners in questions of information security. The advantage of this classroom training is the interactivity with the employee. Questions and dangers are discussed in the group and face to face with the participants and, if possible, answered immediately. That works”.

The employee feels taken seriously and is introduced and sensitized to the topics by the moderators. Due to the many constructive discussions and the fun factor when solving the problems during the event, the sustainability of these topics should not be underestimated. Cognitive knowledge and emotional behavior are taught. This kind of “Awareness to touch”, experienced in a Security Parkour as a classroom event is an ideal complement to awareness measures and contributes to the success and creation of Helaba’s security culture.

ANCHORING AWARENESS

The Telekom subsidiary’s security course has been set up very traditionally – as planned by the word creators of the “parcursus” in Old Rome: As an exercise or drill in military and non-military training operations. The only difference is that the obstacles to be crossed on the T-Systems course are based on practically world-famous board game classics. Whether phishing as “fishing for fish”, social engineering as “trivial pursuit” or cyber security as “monopoly” – a moderator, internal or external, serves as the game leader. There is one station for each security topic – for example phishing, social engineering, cyber security or the “Safe on the Move” module; a game usually comprises five stations at which teams of up to ten people compete against each other for around 15 minutes. The game changes from station to station, “and of course we can focus on one or more specific topics as required. This way, the course continues to develop thematically,” says Thomas Schramm, Principal Solution Sales Manager at T-Systems. During the game, the participants have to put aside paper and pencil for notes on the topic. The game is not about passive cramming, but about interactive perception and comprehension in the truest sense of the word.

Helaba has organised such a course eleven times since 2016 with a total of 350 employees. “We achieved an average score of 1.4 on the basis of employee feedback forms. We know of no other training format that is better received by the Group,” says Jürgen Vogt.

Of course, the gamification element is only one element of a very sophisticated training and sensitization concept. Banks are among the country’s critical infrastructures (KRITIS), are subject to countless regulatory and compliance requirements and must report security incidents to the European Central Bank (ECB). As a result, the institutes are having to upgrade their security technology and raise awareness among their staff, particularly in view of the ever-increasing and more complex cyberattacks in the digital age. “Everyone in the chain must know what to do if a security-related incident actually occurs. With the security course, we also want to encourage employees to report such incidents,” says security expert Vogt.

SEAMLESSLY SENSITIVE

This can also be the phishing mail, which has cheated its way through the firewall, but basic security elements are also played through in the course. Basics, of course, routines in which any laissez-faire in the next move of the data thieves can mean “checkmate”. This includes both a clean desk after work, on which no more confidential papers can be found, and the clarification that official e-mail accounts should not be used for private matters. In short, the security course is intended to raise awareness that security must now be a permanent part of professional and private life, 24 hours a day, seven days a week. Just like a safety belt in a car, for example, where the driver does not think for a fraction of a second whether he is going to drive before he has “clicked” in the belt buckle.

And that’s exactly what Helaba has achieved. In cash management, for example, the level of security has “risen extremely” and the rate of phishing suspicions passed on is also much higher than it used to be. The course had encouraged employees to take action and further removed the taboo from the issue of IT security. The virtual “safety belt” is anchored a good deal deeper in the corporate culture, even in departments that have only a few points of contact with potentially risky areas.
Having created this awareness has also made the work of Jürgen Vogt and his colleagues easier. They are now regarded as “buddies” who can be asked for advice at any time when it comes to security. Information Security Management, and with it IT as a whole, now has the reputation of a protector who takes care of his colleagues. “Our employees have understood it: With an awareness of security, you protect yourself, your workplace and colleagues, the company and our customers. The security course was indispensable for creating this awareness,” Vogt sums up. Helaba has understood how to put everything at risk in order not to risk anything.

“In a sense, our employees form the human firewall. If, despite all our precautions, a phishing attack should actually get through, they are the last line of defense.”

JÜRGEN VOGT,
Information Security Management, Helaba

Thomas.Schramm@t-systems.com
www.helaba.com/int
www.t-systems.com/perspectives/security

A suitcase full of challenges – the tasks of the “game collection” are regularly exchanged by the Security Awareness Coaches.