C*

*CYBERSECURITY 18
Ratkaisu Magazine Issue Excerpt

CGI

Experience the commitment®

LICENSE TO HACK

LähiTapiola uses white-hat hackers to seek out information security vulnerabilities. **Leo Niemelä,** Director, ICT Risk Management and Security, says that hacker collaboration is beneficial to all parties.

BY ARI RYTSY PHOTOS SHUTTERSTOCK AND SAMPO KORHONEN

LähiTapiola's open award for finding data security vulnerabilities, the Bug Bounty program, sprang from its desire to identify vulnerabilities more efficiently and proac tively. Traditional methods were considered insufficient, despite the fact that LähiTapiola ensures the security of its eServices in a number of ways. Leo Niemelä, Director, ICT Risk Management and Security, points out that even the most careful testing does not reveal every information security vulnerability. The more demanding the code, the more likely it is that some errors will only be found during the production stage.

"All coders are making the occasional error in the current digital upheaval. The Bug Bounty program provides more pairs of eyes when searching for such errors. This is not about blaming coders, but developing the data security of our services," says Niemelä.

LähiTapiola, the first Nordic financial company to begin the Bug Bounty program, did not rush headlong into collaboration with hackers.

Producing the highest quality code is the everyone's goal.

LEO NIEMELÄ
Director, ICT Risk Management and Security, LähiTapiola

QUESTION ABOUT THIS ARTICLE?
Jan Mickos
+358 40 847 8740
jan.mickos@cgi.com

During the half-year design phase, the company conducted thorough risk analysis and threat modelling, since particular attention should be paid to the confidentiality and data protection of personal data in a strictly regulated business area.

The threats have not been realized. On the contrary, results of the Bug Bounty program have been so good that it has been extended, and the individual prize money has been raised from EUR 20,000 to 50,000. In practice, the is bigger the prize, the more significant the vulnerability's business impact would be. Under the new EU data protection regulation, a separate GDPR bonus is paid for detected vulnerabilities.

"EUR 18,000 is the biggest prize we've paid to date. Notification of the vulnerability and its correction was sent to the cybersecurity center of the Finnish Communications Regulatory Authority, FICORA. From there, the information was shared with other companies," says Niemelä.

Hackers make money and gain positive recognition of their skills through the Bug Bounty program. This is more attractive than doing something illegal and having to constantly look over your shoulder in fear of the authorities.

Bug Bounty complements traditional information security

Bug Bounty vulnerability programs are one way of improving the security of corporate online services, which are sure to be targeted by unwanted hacking. The fear that a white hat with permission to hack services would change sides – and sell information on vulnerabilities on the black market – has not been realized.

"Hackers make money and gain positive recognition of their skills through the Bug Bounty program. This is more attractive than doing something illegal and having to constantly look over your shoulder in fear of the authorities," explains Niemelä.

Based on the positive experiences of the Bug Bounty program, LähiTapiola has brought more hackers on board through, for example, its own Hack Day, where the security of the selected target system is probed by teams.

Bug Bounty complements, rather than replaces, traditional information security services. However, its use at LähiTapiola has led to savings in areas such as information security investments. It also plugs information security gaps in operations with various partners.

"LähiTapiola is continually developing new services and applications alongside its partners. Our customers' information security and the confidentiality of information are critical for us in everything we do," emphasises Niemelä.

The publicity attracted by the LähiTapiola Bug Bounty program is due to the company's decision to act as openly as possible. Similar projects are being quietly executed in Finnish companies, so that only they know the hackers who are testing their services. Regardless of the way in which the Bug Bounty program is implemented, Niemelä is convinced of its benefits. In addition to improved service security, such benefits can be seen in the development of the company's security culture and better internal security.

"Producing the highest quality code is everyone's goal. Any vulnerabilities identified are used to help develop the skills of programmers and security testers," he says.

ICT partners are included in the program

That is why a specially designated team, including representatives of the company's ICT partners alongside its own security experts, is in charge of running the Bug Bounty program at LähiTapiola. The involvement of partners has brought a broader understanding of data security and enabled a rapid response to identified recoding needs.

The program has developed its own impetus after a tentative early stage. LähiTapiola's current ICT contracts refer to the fact that the external interfaces of its services are covered by the Bug Bounty program.

No additional recruitment needs have arisen due to integrating the successful vulnerability program with daily operations. Ease of use speed and cost-effectiveness can be added through external partners that are familiar with the applications used in a company.

"The use of programs such as Bug Bounty are sure to increase, particularly for customer interface solutions. In this area, hackers are one more tool in the battle for information security," sums up Niemelä. ✱

4 x Take advantage of hackers

1. Start with planning, and then conduct risk analysis and threat modelling.
2. Pay attention particularly to confidentiality and data privacy.
3. Take advantage of the bounties and use of hackers.
4. Use the findings to train and develop programmers.

Leo Niemelä, Director, ICT Risk Management and Security, says that hacker collaboration is beneficial to all parties.