ROBIN LYNN & LEE
In collaboration with DFDL

27 November, 2023

ETHICAL HACKING IN MALAYSIA

Tan Hui Lynn, Michelle Koh

In 2021, Microsoft paid USD13.7 million to researchers who found vulnerabilities in its products. In 2022, Google awarded USD12 million bounty rewards in total. Microsoft and Google are not the only companies with a Bug Bounty program, other companies such as Amazon, Apple, Dropbox, Intel, Meta, Netflix have in place some form of vulnerability rewards programs. Through such programs, organisations crowdsource the task of finding vulnerabilities to external parties and offer rewards (compensation, recognition, or both) to individuals for uncovering and reporting software bugs, particularly if it relates to security exploits and vulnerabilities.

This article explores the concept of ethical hacking in Malaysia, and the contractual considerations companies and service providers should consider when designing a Bug Bounty program or when engaging a service provider to conduct penetration tests.

What does the law say?

Hacking is an offence under the Malaysian Computer Crimes Act 1997 ("**Act**"). A person commits an offence if he, knowing that he does not have authorisation, causes a computer to perform any function with intent to secure access to any program or data held in any computer.

White/Black/Gray hat hackers

What separates the three is whether a hacker has received due authorisation. White hat hackers have permission from the company to help identify vulnerabilities of a company's system. Black hat hackers act without authorisation and hence commits an offence under the Act. Black hat hackers usually hack to steal information and use such information for extortion.

Gray hat hackers usually act without malicious intent of black hat hackers, and sometimes does this to raise public awareness about a certain vulnerability, or sometimes just to prove a point. Notwithstanding, unless they act specifically within the permissible authorisation given by a Bug Bounty program, they would still be committing an offence under the Act.

Bug Bounty Programs and Penetration Tests

Bug Bounty programs are structured initiatives to incentivise independent security researchers, such as ethical hackers and white hat hackers, to discover and report security vulnerabilities in a technology. The objective is to enhance cybersecurity by identifying and addressing potential weaknesses before exploited by malicious hackers.

Companies also pay professional service providers to conduct penetration testing. Such service providers perform simulated attacks on a computer system to evaluate its security. There are many reasons to do this, compliance with laws and regulations and compliance with cybersecurity standards being 2 of them.

Here are a few things to consider when drafting the terms and conditions of a Bug Bounty program, or when entering into an engagement for pen tests.

1. Scope of the Test

Parameters for the test subject should be well defined, and there are various ways to do this:

(a) Referring to the specific domain, application, program, or technology;

(b) Defining the vulnerabilities that qualify for the pay-out;

(c) Defining the priority levels of types of vulnerabilities, and mapping out the ones that are part of the program;

(d) Defining the eligibility criteria of security researchers such as only persons over the age of majority.

For penetration tests, a company may also choose to further limit the:

(a) Testing area, such as creating a sandbox or an artificial environment;

(b) Time, as engagement typically concludes within a timeframe.

Note that design limitations may have an impact on the effectiveness of the test, and we would recommend in house counsels to engage with in house engineers to design the scope.

2. Excluded scope

Equally, you may also want to specifically exclude some examples from the above scope. For instance:

(a) Excluding certain domains such as a newly purchased entity or program which is still undergoing internal testing in which case most vulnerabilities are still being identified and do not warrant a pay-out;

(b) Defining the non-qualifying vulnerabilities such as phishing attempts on employees of the company or use of out-of-date browsers;

(c) Excluding any access to personal data or any other data relating to customers;

(d) Excluding security researchers from countries on sanction lists (which makes pay-outs difficult), or security researchers which are currently in the company's employment.

3. Rules, processes, and procedures

Only a security researcher who has met all prescribed terms and conditions qualify for a reward, and safe harbour from the law. It is therefore imperative for terms and conditions to be clear. A Bug Bounty program may include:

(a) Authorisation for purposes of the Act is only given to security researchers who comply with all terms and conditions of the Bug Bounty program;

(b) Process to submit reports and supporting documents;

(c) Explanation on how are reports handled, investigated, and resolved by the company and the anticipated timeframe before a security researcher will receive a response;

(d) Mechanics on administration of rewards and the quantum of pay-out, typically rewards and recognition is only given to the first person that submits a full report on the specific vulnerability;

(e) Confidentiality provisions and exceptions where companies may choose to publish the reports or share the reports / payout details with third party providers but security researchers would not have this right to disclose vulnerabilities identified;

(f) Actions to take when a researcher inadvertently access customer data;

(g) Guidelines on impact on service levels or no disruption to services provided to customers;

(h) Statement on whether the company will assist to defend security researchers in the event security researchers are prosecuted in a court of law.

Penetration Testing Agreements and Indemnities

In engagement agreements for penetration testing, service providers will typically include indemnities to protect the service provider from lossesd suffered resulting from undertaking the engagement. Such losses may include the cost of defending themselves against a third party proceeding, or even from prosecution. It is important to check:

(a) If a vulnerability affects third parties, will the service provider disclose this vulnerability to a third party;

(b) Are the persons carrying out the assignment contractors or freelancers in which case the confidentiality obligation should also extend to such persons;

(c) What indemnities are given and how much assistance are you required to provide, from appointing counsels for defence, to hiring of expert witnesses, what damages are you expected to indemnify against;

(d) Is the consent waiver / scope of authority given drafted in a clear and concise manner;

(e) If a public prosecutor initiates and investigation against the service provider, what does co-operation look like.

Conclusion

As much as we hate to admit it, terms and conditions and fine prints are essential in setting out the rules of the game. Well-drafted terms and conditions serve to reduce ambiguity and define qualified pay-outs. That said, we are all for drafting in simple language so that any reader who picks up the document will be able to understand the content immediately, something we hope we achieved with this article!

AUTHORS

Hui Lynn Tan
Partner
huilynn.tan@robinlynnlee.com

Michelle Koh
Associate
michelle.koh@robinlynnlee.com