Proposal and Evaluation of a Security Incident Response Training Method using Programming

Katsumi Nagai

Faculty of Information Science and
Electrical Engineering
Kyushu University
Fukuoka, Fukuoka, Japan
nagai.katsumi.815@s.kyushu-u.ac.jp

Hiroshi Koide

Research Institute for Information
Technology
Kyushu University
Fukuoka, Fukuoka, Japan
koide@cc.kyushu-u.ac.jp

Kouichi Sakurai

Faculty of Information Science and
Electrical Engineering
Kyushu University
Fukuoka, Fukuoka, Japan
sakurai@inf.kyushu-u.ac.jp

ABSTRACT

Nowadays, there are various cyber-attacks in the world. In terms of dealing with cyber incident, there are many non-technical factors. Table Top Exercises are available for improving it but need some fund, time and trainers who conduct it more smoothly. So, in this work, we propose a security incident response training method using programming. It aims to improve some non-technical skills. Our proposal is actually executed with questionnaires.

CCS CONCEPTS

• Social and professional topics → Adult education

KEYWORDS

Incident handling, table top exercise, security, incident response

ACM Reference format:

Katsumi Nagai, Hiroshi Koide and Kouichi Sakurai. 2019. Proposal and Evaluation of a Security Incident Response Training Method using Programming. In *Proceedings of the 20th Annual SIG Conference on Information Technology Education (SIGITE'20)*, Oct 3-5, Tacoma, WA, USA. 1 page. DOI: <https://doi.org/10.1145/3349266.3351385>

1 INTRODUCTION

Nowadays, there are various cyber-attacks in the world. In terms of dealing with cyber incident, not only technical skills but also non-technical factors are also important. Table Top Exercise is one of the training method to improve it. Actually, Table Top Exercise for cyber-security that aims to understand the situation that change with time and give appropriate instructions are executed [1]. It is effective but hard to execute in terms of fund, time and trainers who execute it more smoothly. So we propose a security incident response training method using programming that aims to improve some non-technical factors.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author.
SIGITE '19, October 3–5, 2019, Tacoma, WA, USA
© 2019 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-6921-3/19/10. <https://doi.org/10.1145/3349266.3351385>

2 PROPOSED METHOD AND EXPERIMENT

Proposed training mainly aims to make the trainees understand the importance of preparing for attacks, understand the situation and deal with it calmly. We create the website for maintaining a program and the situation that participant become the program administrator and deal with the sudden and unpredictable changes of program language specifications with a limited time. We execute proposed training to 21 adults having programming experience. And we ask the participants some questionnaire on a 1 to 10 scale before and after the training. The contents of questionnaire are (Q1) If a cyber-attack has been detected, how important do you think dealing with it calmly is, (Q2) How important do you think preparing the manual for cyber-attacks is and (Q3) How important do you think executing training for cyber-attacks is. Table 1 shows the average of the answer. The result indicates the purpose of proposed training can be achieved but it needs more improvement for better result.

Table 1. The average points of the answer

Questi ons	Before training	After training
Q1	9.00 / 10pt	9.33 / 10pt
Q2	8.38 / 10pt	9.23 / 10pt
Q3	9.09 / 10pt	9.47 / 10pt

3 CONCLUSIONS

We proposed and executed a security incident response training method using programming. In our future work, we will adjust the difficulty of the proposed training and make it more effectively.

ACKNOWLEDGMENTS

This work was supported by JST SICORP Japan partly.

REFERENCES

- [1] JASA 2018, Jan 26. '2017nendo dai1kai saiba-sekyurithikijouenshuuwa-kushoppu repo-to(2017 the 1st workshop report of cyber-security table top exercise)', http://www.jasa.jp/seminar/workshop_exercise_report.html?type=workshop_exercise_report