Balancing Method in Cyber Situational Awareness: Human Psychological Change by Cyber Attack

Minhee Joo, Mookyu Park, Moosung Park, and Kyungho Lee

Abstract— Recently cyber attacks have been increasing in cyberspace as the usage rate of internet has increased. Cyber attacks such as Ransomware, which are attacks that cause damage to the real world for the purpose of monetary profit, are attacked through sites that are easily accessible services that people are heavily used, It is proved that it can give. This study measures the risk that reflects changes in human psychology based on recent Ransomware attacks in Korea. In order to protect the threat of leakage of personal information according to the risk, we suggest ways to balance cyber situation awareness using human psychological change.

Research Keywords— Cyber Situational Awareness, Balancing Method, Cyber Attack

1 INTRODUCTION

In Korea, where the Internet is highly dependent on the population, the rate of Internet banking, which registers official certificates on the Internet, has increased to 2.58 million compared to 2016. Attacks are increasingly tar-geting personal information stored on the Internet[1]. In 2016, staying app that name 'Here In' was hacked and 341 million personal information had leaked. It was an incident that leaked to the cell phone number as well as the user name. Initially, attackers threatened company to pay, but when it was not done, they demanded money from users and leaked 500 personal information to SNS, which made the people feel anxious. Ransomware is infected through a site or e-mail that people use fre-quently[2]. The damage caused by the cyber attack makes the people's psychology anxious and makes impossible about the effective decision making in cyberspace. In this paper, we propose a method to balance the cyber situation awareness by using human psychological change due to cyber attack.

- *Minhee Joo is with the Institute of Cyber Security & Privacy (ICSP), Korea University, Seoul, South Korea. E-mail: mhjoo9321@korea.ac.kr*
- *Mookyu Park is with the Institute of Cyber Security & Privacy (ICSP), Korea University, Seoul, South Korea. E-mail: ctu-pmk@korea.ac.kr*
- *Moosung Park is with Agency for Defense Development, Seoul, South Korea. E-mail: parkms@add.re.kr*
- *Kyungho Lee is with Institute of Cyber Security & Privacy (ICSP), Korea University, Seoul, South Korea. E-mail: kevinlee @korea.ac.kr*

2 RELATED WORKS

Cyber Situational Awareness (CSA) is based on the Endsley's model. It is aware of the security status and the threat environment within an environment of time and space. It is the process of recognizing the elements of the current environment, understanding the present environment and projecting it into the future situation[3]. In this paper, we propose a way to balance this situational awareness.

3 RESULT

3.1 Scenarios of human psychological change by Ransomware

On the way to work, people saw an article on Ransomware that they were attacking. Some people know through SNS, and they found out by using portal site to see infected cases or according to government announcement. People who have known through SNS will be anxious about the posts on SNS. When they see the case of Ransomware using the portal site. People are also worried about that they will not be restored because of vaccine didn't distributed by government 's

homepage. People's psychology creates anxiety in different ways. This study measures the risk of psychological distress by dividing the population into ages.

Data on experience of ransomware, government credibility, and media influence on public psychology were based on a public data portal. The damage experience was selected as the Ransomware infection through the Naver trend. The influencing factors were rated and averaged by age group. In the 10-20 age group, the average is 2, 21-30 is 5.3, 31-40 is 5.7, 41-50 is 3, 51-60 is 2.7, and 61-70 is 2.3. Threats to cyber attacks were determined by the Ransomware countermeasures at the Ransomware center in South Korea. Threat codes have given order and threat score for the threat was given according to how much the threat intensity affects the asset. The frequency occurrence was scored according to how often it occurred, and the final score was evaluated by adding the two scores. The risk of a threat is given by a score that must be balanced by summing the average of the affecting factors and the threat assessment score.

T-01 is threatened by Ransomware infection through spam mail and malware infection, score is 7. T-02 is personal information leakage due to hacking and the score is 3. T-03 is the personal information due to Ransomware infection and the company's secret encryption, the score is 8. Threat score and weight are added. In case of T-01, 10-20 is 9, 21-30 is 12, 31-40 are 13, 41-50 are 10, 51-60 are 10, In the case of 61-70 years old, 9 was born. In the case of T-02, 10-20 is 5, 8-30 for 21-30, 9 for 31-40, 6 for 41-50, 6 for 51-60, 5 for 61-70 . For T-03, 10-20 is 10, 13-30 for 21-30, 14 for 31-40, 11 for 41-50, 11 for 51-60, 10 for 61-70. Calculate the score to give a balance of cyber situational awareness with an average score of the threats.

3.2 Balancing Method in Cyber Situational Awareness

Based on the threat from 3-1, we presented two ways of balancing. The score of the balance method was calculated considering budget, danger and difficulty. The average score was calculated by summing the values for each balance score. The balance method for T-01 is B-01, Introduce software/solution that can detect malicious code, score is 6 and average score is 8.3. B-02 is Educate about using mail score is 2 and the average score is 8.5. The average threat for T-01 is 11, and B-02 is the right balance for each age group. The balance of the T-02 is that B-01, network isolation configuration that is perfectly isolated from the outside and score is 8, average score is 4.2. B-02 is a server management method of server management training with a score of 3 and an average score of 3.5. B-01 was the average of the threats to T-02, which is balanced by age group. B-01 is the Introduced software/solution to detect malware and hacking. The score is 6 and the average score is 7.5. B-02 has a score of 1 and the average score is 10.5. The average age of 12 for the threat against T-03 was B-02, which was balanced by age group. The result is shown in Figure 1

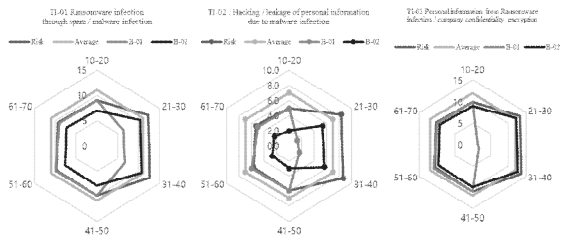

Fig. 1. Graph of B-01, B-02, B-03

4 Conclusion

In this paper, we propose a method of balancing cyber situational awareness by calculatinsg the psychological change and the threat according to the Ransomware. As the number of people storing personal information in cyberspace increases, the damage of personal information leakage due to cyber attacks will increase. Accordingly, if we balance the threats by age group within the cyber situation awareness, it will solve the public anxiety.

Furthermore, if the balance method used in this paper is applied to the actual case and the balance method is implemented by the government, leakage or damage of personal information due to cyber attack will be reduced.

Acknowledgment

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract. (UD060048AD)

References

[1] Shin, Jae Hun, Kim, Yong Hyun. (2016). The plan to strengthen cyber security. Korean Police Studies Review, 15(3), 75-104.

[2] Hyun-sik Yoon, Kyung-hwan Song and Kyung-Ho Lee, 2017, "FAIR-Based BIA for Ransomware Attacks in Financial Industry," Journal of the Korea Institute of Information Security & Cryptology, Vol. 27, No. 4, pp. 873~883.

[3] Bellekens, Xavier, et al. "Pervasive eHealth services a security and privacy risk awareness survey." Cyber Situational Awareness, Data Analytics And Assessment (CyberSA), 2016 International Conference On. IEEE, 2016.

Minhee Joo received the B.S. degrees from University of Seoul in 2017. Currently she is in Master degree student in the Institute of Cyber Security & Privacy (ICSP) of Korea University since 2017. Her research interests include Risk management and Cyber Security.

Mookyu Park received the B.S. degrees from Sejong University in 2014, Currently he is an Ph.D student in the Institute of Cyber Security & Privacy (ICSP) of Korea University since 2014. His research interests include Data minig and Risk management.

Moosung Park received the B.S. degrees from Sogang University of in 1988 , M.S. degrees from Sogang University in 1990, Ph.D degrees from Kwangwoon University in 2004. Currently he work for Agency for Defense Development. His research interests include Cyber defense and Cyber sitautional awareness.

Kyungho Lee received his Ph.D degree from Korea University. He is now a professor in the Institute of Cyber Security & Privacy (ICSP) at Korea University, and has been leading the risk management laboratory in Korea University since 2012. He was a former CISO at NAVER Corporation, and now he is serving as a president of Office of Information Technology & Service Center in Korea University.