jamk.fi

Summary of Cyber Security Report

Jere Pesonen
TTV18S1

10-19
ICT- Engineering
Technologies field

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Contents

1 Introductory

This document is summary of ‘Bulletproofs annual cyber security report 2019’. The report is 23 pages long PDF file, and contains today’s top targeted industries, evolving threat landscapes, and penetration testing data. Report also writes down some predictions of cyber security field for the upcoming year.

2 The threat landscape

The report claims that attack methods popularity varies. In 2017 the thing was ransomware, a malware that encrypts users files, and demands fees for access of files. At the end of the 2017 ransomwares popularity collapsed, and by the 2018 crypto jacking was highly growing. Crypto mining malware uses victim’s CPU to mine cryptocurrency and its popularity had increased by 629% in the first quarter of 2018. Towards the end of the 2018 card skimming and Magecart became popular. Magecart is a method where malicious JavaScript code is used to capture sensitive information from online payment forms. This method is very unnoticeable because the hacker does not directly attack the company, the JavaScript code just skims the customers information. In the worst case, it can take several months to detect Magecart attack.

3 Penetration testing

Bulletproof has penetration testing unit, which have been scouting for vulnerabilities in infrastructures and applications. The results were inconsistent, as you may assume, excluding the fact that some issuers were found in every single test. Common issues that may cause vulnerabilities was the lack of updates, out of date software, and unsupported software’s. Also, the common use of default credentials is very worrying according to report.

4 Predictions

The possibilities of cyber offenses are almost unlimited and we are going to have a hard time keeping up with the criminals. Potential trending methods or targets might be Sceletonscare, compounding Al and scammer, and IOT devices. Sceletonscare is a sequel for extortion emails where criminal demands payment or he publishes some personal information or something sensitive material of victim. Sceletonscare is a method when email contains some previously gained personal information of target (like old password) to gain authenticity. Al can be used to pull data from breach databases and social media and by then gain access to user accounts. (This Al technology already exits but its not yet the most worthwhile for hackers to adopt.) Lastly since the IOT is growing and households are full of electronics that are connected to internet, there can be loads of vulnerabilities in these devices where hacker can access to your whole smart home hub.

5 Recap

The threats in cyber world are constantly changing. Criminals will always found new ways and methods to break into our systems and cyber employees will have a hard time to keep up. Companies have to put a lot work and money to make sure that their data is safe, although it never is fully secured.

6 References

Security report. N.d. Bulletproof annual cyber security report 2019. Referenced 18.10.2019. https://www.bulletproof.co.uk/industry-reports/Bulletproof%20-%20Annual%20Cyber%20Security%20Report%202019.pdf