Haktivism Presentation

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

The security of any system or network is essential to maintain confidentiality, integrity and availability of the information. With the increase of internet traffic and software development, the related threat to this data is also increasing. Virtualization makes the data handling easy but managing the security of the data is a separate challenge. We will take an overview of 5 recent cybersecurity attacks, their cause, and precautions that are required to mitigate the danger of data theft.

Stuxnet was a worm attack, described as the most advanced cyber attack of that time, was designed to infect secretly into the host network and affect the physical processes controlled by that network. Its target was The HVAC company and the theft of more than 40 million customer’s debit cards was reported. ‘Signature only’ security systems were vulnerable to the attack of this generation. To avoid, zero-day attack technologies emerged which are far from signatures.

A very famous virus that gained popularity all around the globe ILOVEYOU. It would penetrate into hundreds of computers in a very short time. Estonia was under such an attack on April 2017. To avoid such virus eruption in your network, a complete vulnerability scan is required.

Melissa Virus, a malware document which when opened, would email that document to a number of different connections. This virus crushed more than one lac email servers. An open-source firewall is the best option to monitor your network from this attack related to social engineering.

A.P Moller, the shipping company was attacked by a ransomware Petya. Petya had the potential to read encrypted data and then will ask a ransom to return key of decryption and set files free. To avoid such attacks, the security structure is needed to be designed in such a way that they are more integrated and unified.

WannaCry was also a famous ransom based attack that encrypted the data and demanded a ransom (*Preventing-the-next-mega-cyber-attack.pdf*, n.d.). It explored a vulnerability in Windows and also infected the British Health Service profile system and made a lot of money. The attacked could be avoided by installing regular updates of the operating systems because windows cleared those patches after a few days.

References

*Preventing-the-next-mega-cyber-attack.pdf*. (n.d.). Retrieved from https://www.checkpoint.com/downloads/product-related/whitepapers/preventing-the-next-mega-cyber-attack.pdf