8-10-2020

A Survey on Emerging Trends of Cyber Threats to Academic Research

Abhijit Kumar Nag
Texas A&M University-Central Texas, aknag@tamuct.edu

Anitha Chennamaneni
Texas A & M University Central Texas, anitha.chennamaneni@tamuct.edu

Follow this and additional works at: https://aisel.aisnet.org/treos_amcis2020

A Survey on Emerging Trends of Cyber Threats to Academic Research

TREO Talk Paper

Abhijit Kumar Nag
Texas A&M University-Central Texas
aknag@tamuct.edu

Anitha Chennamaneni
Texas A&M University-Central Texas
anitha.chennamaneni@tamuct.edu

Abstract

Recent outbreaks of cyber-attacks made the education sector the most vulnerable out of 17 different industries (SecurityScorecard, 2019). Academia, by nature, supports open network and access concepts to make a welcoming environment to all participants. Moreover, researchers often share their findings and innovation with their collaborators within various universities. In many cases, appropriate steps are not followed while sharing this information among all the parties. The malicious attackers exploit this very concept and launch numerous attacks to compromise the higher education system as a whole. Recent incidents in top rank universities in the US and other countries show that the researchers are, at times, becoming a weapon to start any major data breach events (Bonderud 2019; Campbell 2019; Chapman 2019). Some countries also try to influence faculty to share confidential research-related information with them. Hence, there is a greater need for universities to accurately detect and respond to information security threats to academic research and safeguard their data, intellectual property & sensitive information in research. In practice, finding the right balance in open culture for users and restricting illegitimate access to information is the key to thwarting any security breaches.

Our study analyzes cybersecurity trends and identifies the security challenges and common types of cyber-attacks encountered by universities in research areas in the last five years (2015-2020). We propose a methodology for threat modeling and exemplify a scenario of a phishing attack using attack graph structure depicting a compromise of the university network and stealing sensitive information in research. A black-box based threat model is implemented to categorize and rank emerging cyber-threats to academic research. In this research, the DREAD Average Ranking (Jagannathan, 2016) process is utilized to rank various threat vectors for academic research related to cyber-attacks. Moreover, we propose a PSRV framework with a set of best practices to protect, detect, and respond to information security threats to academic research. These components include people first, strong authentication and authorization procedures, robust network design, and verification of third-party vendors.

As part of future directions, we extend our research to validate the proposed threat model with existing data on varied cyber-attacks. Besides, a user study will be designed to collect information from the administrators about their preparedness and attempted actions to thwart these cyber-attacks. These data will be used to validate any future threat models further.

References

2018 Education Cybersecurity Report. (2018). *SecurityScorecard*. (available at https://securityscorecard.com/resources/2018-education-report)

Bonderud, D. (2019). *Hackers Evolve Attacks Methods in Higher Education Breaches*. Technology Solutions That Drive Education. (available at https://edtechmagazine.com/higher/article/2019/10/hackers-evolve-attacks-methods-higher-education-breaches).

Campbell, S. (2019). *Cybersecurity in Higher Education: Problems and Solutions*. Toptal Insights Blog. (available at https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education).

Chapman, J. (2019). "How safe is your data? Cyber-security in higher education", *Higher Education Policy Institute*.

Jagannathan, V. (2016). *Threat Modeling Architecting & Designing with Security in Mind*, Presentation.