5-5-2022

Improving the Effectiveness of Security Controls to Prevent APT Attacks

Srinivasulu Vuggumudi
Dakota State University, srvuggumudi@pluto.dsu.edu

Yong Wang
Dakota State University, yong.wang@dsu.edu

Kaushik Ragothaman
Dakota State University, kaushik.muthusamyragothaman@trojans.dsu.edu

Cherie
Dakota State University, cherie.noteboom@dsu.edu

Jun Liu
Dakota State University, jun.liu@dsu.edu

Improving the Effectiveness of Security Controls to Prevent APT Attacks

Srinivasulu Vuggumudi
Dakota State University
srvuggumudi@pluto.dsu.edu

Yong Wang
Dakota State University
yong.wang@dsu.edu

Kaushik Ragothaman
Dakota State University
kaushik.muthusamyragothaman@trojans.dsu.edu

Cherie Noteboom
Dakota State University
cherie.noteboom@dsu.edu

Jun Liu
Dakota State University
jun.liu@dsu.edu

ABSTRACT

An advanced persistent threat (APT) is a prolonged, aimed attack on a specific target. Cyber attackers gain access to a system or network and remain there for an extended period without being detected. The goal of APT attackers is generally stealing data and intellectual property. Despite all the awareness, technological advancements, and massive investment, the fight against APTs is a losing battle. A false sense of security is a belief that the organization is safer than it is. We researched whether organizations have a false sense of security against APT attacks and what contributes to that belief. Our research indicated that employees were not confident about organizations' cybersecurity posture. In this paper, we discuss one of our research contributions, which suggests remediation strategies that organizations can employ to increase the effectiveness of security controls against APT attacks.

Keywords

False sense of security, Advanced Persistent Threats, Effectiveness of Security Controls.

INTRODUCTION

Advanced Persistent Threat (APT) is an organized cyber-attack usually planned and executed by skilled and sophisticated threat actors over a prolonged period (Vukalović & Delija, 2015). Today, organizations rely on advanced information technology to operate their business processes; protecting themselves against APTs is a considerable challenge. There is a 125% increase in cybersecurity incidents, impacting every industry and geography year by year (Accenture, 2021). The involvement of APTs is identified as one of the significant factors in the rise in incidents (Accenture, 2021). Although regulatory agencies require organizations to comply with their respective standards, being compliant alone does not help them evade APT attacks (Grossman, 2008). On the other hand, organizations rely more on sophisticated tools to prevent APT attacks.

A false sense of security is a belief that some situation is safer than it is (Merriam-Webster, 2022). A false sense of security exists when the focus is on implementing a security strategy but not on the effectiveness of the security strategy. We researched whether organizations have a false sense of security regarding their security strategies to prevent APT attacks or not and what contributes to their false sense of security. Our research approach is quantitative using the survey method. Our research model has seven independent variables, one dependent variable, and one moderator variable. The independent variables are Security Awareness and Training (SA), Security Controls (SC), Insider Threat Prevention (IT), Cybersecurity Insurance (CI), Segmentation (SG), Convergent Testing (CT), and Redundant IDS/IPS (RD). Sense of Security (SS) is the dependent variable. Organizational Culture (OC) is the moderator. The sense of security in our research represents the confidence level of employees about their organizations' strategic activities related to security. We used the SurveyMonkey platform to administer the survey. We prepared 45 questions regarding employee perceptions on cybersecurity controls' implementation, monitoring, and effectiveness. All questions were anchored on 5-point Likert scales. The participants are cybersecurity professionals with at least five years of experience working for private (for-profit) organizations. The survey was anonymous and was distributed to 600 qualified participants using email and LinkedIn in spring 2021. We received 253 responses. 207 out of 253 returned questionnaires were useable, i.e., 82% completion rate.

After data collection, we performed confirmatory factor analysis (CFA) to determine the model fit and partial least square structural equation modeling (PLS-SEM) to uncover the cause-and-effect relationships between independent and dependent variables using Warp PLS. Due to high correlations (> 0.85), we dropped two constructs, CT and IT, from the model and performed SEM analysis again. We successfully validated both measurement and structural models.

We tested hypotheses statements using path coefficient and p values. The results indicated that successful implementation of security awareness and training, security controls, redundant IDS/IPS, and purchase of cybersecurity insurance positively impacts the sense of security. However, successful implementation of segmentation does not impact the sense of security. Furthermore, organizational culture moderated the effects of security awareness and training, security controls, and segmentation. The moderating effects of organizational culture on redundant IDS/IPS and cybersecurity insurance were insignificant.

This paper extends our previous research. The main objective of this paper is to suggest remediations that organizations can incorporate to increase the effectiveness of their security strategy, thereby minimizing the false sense of security.

LITERATURE REVIEW

Immensely few academic publications contributed to the remediation strategies exclusively for APT attacks. Bukac et al. proposed a response strategy based on the kill chain concept (Bukac et al., 2014). This strategy aims to collect as much information as possible when an incident occurs and then perform remediation efforts. Messaoud et al. proposed an APT lifecycle model based on attackers' objectives (Messaoud et al., 2017). They suggested four protection technologies. However, they all focus on only technical controls. Brewer et al. suggested an analytics-driven approach to defending against APTs (Brewer, 2014). Mohsin and Anwar discussed an ontology-based approach that uses cyber threat intelligence to evaluate IoT networks against APT attacks (Mohsin & Anwar, 2016). In addition to the remediation strategies, risk management approaches are proposed for the APTs. In (L. X. Yang et al., 2018), Yang et al. developed a risk management approach based on game theory to efficiently allocate resources to fix insecure hosts in an organization. In (X. Yang et al., 2017), the risk assessment is based on state evolution and is modeled as a constrained optimization problem. The risk is measured by the maximum expected loss. In this work, an organization's network is assumed to be fixed; however, in real terms, the network configuration may vary over time. Granadillo et al. proposed a dual approach by evaluating a given security countermeasure's technical and financial impacts by performing a case study on APTs (Daniel Gonzalez Granadillo et al., 2015). Adelaive et al. conducted a systematic review on the mitigation effects of APT attacks (Adelaiye et al., 2018). They identified twelve mitigation techniques, almost all of them being technical controls. Only a limited number of articles in their review discussed security awareness. Their study identifies the low utilization of human intelligence and behavioral patterns in preventing and detecting APT attacks. Further, the level of effectiveness of the mitigation strategies is not obtainable from their study.

REMEDIATION STRATEGY TO PREVENT APTS

Since the effectiveness of the controls plays a significant role in combating the APTs, we suggest the following recommendations for the constructs contributing to the false sense of security.

Security Awareness and Training

Security awareness and training campaigns typically track who underwent training or attended awareness sessions, the number of users who passed the exams, etc. However, they fail to measure the impact of the awareness sessions (Aloul, 2012). Because the effectiveness of security awareness and training campaigns are not measured, employees indicated a low sense of security regarding security awareness and training in our survey. We recommend a cyber security awareness measurement model: Analyze, Predict, Awareness, and Test (APAT) (Khan et al., 2020). APAT model involves a four-step cycle: analyzing the current threats, predicting the impact of threats, providing security awareness and training, and measuring the effectiveness of security awareness and training. The APAT model solves the challenge of delivering an effective security awareness and training program.

Redundant IDS/IPS

Although IDS/IPS systems are constantly improved, evolving evasion techniques can still bypass the systems. We recommend redundancy in setting up IDS/IPS since Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS) are the first lines of defense for organizations. Even if each IDS uses a different detection technique, they analyze each other's alerts and reduce false positives. A reliable intrusion detection solution cannot be achieved without using multiple types of IDS/IPS technologies (Scarfone & Mell, 2007). To improve intrusion detection capabilities, some organizations also use multiple products of the same IDPS technology type (Scarfone & Mell, 2007). Each product uses different detection methodologies and

detects events that another product may miss. So, when multiple products are used to monitor the same activity, it is easier for analysts to validate alerts and identify false positives. It also provides redundancy/reliability should one product fail (Scarfone & Mell, 2007).

Security Controls

Security controls are the countermeasures that organizations implement to detect, prevent, reduce, counteract, or minimize security risks (IBM Cloud Education, 2019). Compliance obligations drive a significant fraction of the overall cybersecurity budget. Security controls based on compliance requirements cannot protect organizations from the ever-changing threat landscape. To address this challenge, we recommend that security controls be built from threat intelligence to complement controls focusing on compliance requirements (Muckin & Fitch, 2019). Cyber Threat Intelligence (CTI) platforms developed by cybersecurity companies such as FireEye, ThreatConnect, McAfee, and many others have an unprecedented ability to prioritize threats, pinpoint key threat actors, understand their tools, techniques, and procedures (TTP), deploy appropriate security controls, and ultimately, improve overall cybersecurity hygiene (Samtani et al., 2019). We recommend considering a CTI platform because of its agility without much human intervention. When selecting a control assessor or team of assessors, we recommend selecting them with deep technical knowledge regarding the systems and their security.

Cybersecurity Insurance

Cybersecurity insurance pays for a company to hire a cybersecurity corporation that conducts a forensic investigation to reveal precisely what happened in an attack (Morris, 2021). It also pays for the legal services required after the attack. Since APT attacks involve data exfiltration and an organization can go bankrupt after a successful cyberattack, we recommend adding cybersecurity insurance to the organization's security program.

Table 1 shows our recommendation for enhancing controls based on NIST 800-53 Security and Privacy Controls (NIST, 2020).

Independent Variable	NIST Control	Action Item
Security Controls	CA-2 Control Assessments	Enhance the security control by ensuring that the assessor or assessment team selected for assessment has deep technical knowledge of the systems and their security.
	ACCESS Control Group: AC-1 to AC-25	Enhance the appropriate controls based on threat intelligence feeds.
	PL-2 SYSTEM SECURITY AND PRIVACY PLANS	Enhance the control based on the threat intelligence feeds.
Redundant IDS/IPS	SI-4 SYSTEM MONITORING	Enhance the control with redundant IDS/IPS systems to monitor the network and systems.
Security Awareness and Training	AT-2 LITERACY TRAINING AND AWARENESS	Enhance the control by applying the APAT (Analyze, Predict, Awareness, and Test) model.
Cybersecurity Insurance	PM-1 INFORMATION SECURITY PROGRAM PLAN	Enhance the control by adding a plan to procure cybersecurity insurance.
	PM-4 PLAN OF ACTION AND MILESTONES PROCESS	Enhance the control by purchasing cybersecurity insurance.
	PM-9 RISK MANAGEMENT STRATEGY	Enhance the control by adding cybersecurity insurance as a risk transfer method.

Table 1. Security and Privacy Controls to Remediate False Sense of Security

DISCUSSION

We selected the NIST 800-53 set of controls to enhance security because it is more complex, more restrictive, and contains more security controls than necessary for any business sector (Slonka, 2020). Any business can pick a list of security controls from NIST 800-53 that are relevant to its sector. Our survey found that organizations do not effectively do segmentation and security assessments as part of their security strategy. The effectiveness of security assessments and segmentation are good candidates to be research constructs in future studies.

CONCLUSION

Our research suggests that organizations need a paradigm shift while setting up defenses against APT attacks; focusing on the effectiveness of the security controls is the key. Our study identified the effectiveness of Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance as essential factors influencing the employees' sense of security. Our recommendations in this paper are to enhance the controls related to Security Awareness and Training, Security Controls, Redundant IDS/IPS, and Cybersecurity Insurance. While organizations focus on setting up security controls to satisfy compliance requirements, our research emphasizes the importance of the effectiveness of security controls.

REFERENCES

1. Accenture. (2021, August 4). *Triple digit increase in cyberattacks: What next?* Accenture Security Blog. https://www.accenture.com/us-en/blogs/security/triple-digit-increase-cyberattacks
2. Adelaiye, O., Ajibola, A., & Faki, S. (2018). Evaluating Advanced Persistent Threats Mitigation Effects : A Review. *International Journal of Information Security Science*, *7*(4), 159–171. https://www.researchgate.net/publication/331210253_Evaluating_Advanced_Persistent_Threats_Mitigation_Effects_A_Review%0Ahttps://www.researchgate.net/publication/331210253_Evaluating_Advanced_Persistent_Threats_Mitigation_Effects_A_Review
3. Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3). https://doi.org/10.4304/jait.3.3.176-183
4. Brewer, R. (2014). Advanced persistent threats: Minimising the damage. *Network Security*, *2014*(4), 5–9. https://doi.org/10.1016/S1353-4858(14)70040-6
5. Bukac, V., Lorenc, V., & Matyas, V. (2014). *Red Queen's Race: APT win-win game*.
6. Daniel Gonzalez Granadillo, G., Garcia-Alfaro, J., Debar, H., Ponchel, C., Rodriguez-Martin, L., Gonzalez Granadillo Joaquin Garcia-Alfaro Hervé Debar, G., & Ponchel Laura Rodriguez Martin, C. (2015). *Considering technical and financial impact in the selection of security countermeasures against Advanced Persistent Threats*. 1–6. https://doi.org/10.1109/NTMS.2015.7266480ï
7. Grossman, W. M. (2008). Complying to a false sense of security. *Infosecurity*, *5*(7), 24–27. https://doi.org/10.1016/S1754-4548(08)70122-0
8. IBM Cloud Education. (2019). *What are Security Controls?* https://www.ibm.com/cloud/learn/security-controls
9. Khan, A. H., Sawhney, P. B., Das, S., & Pandey, D. (2020). Cyber Security Awareness Measurement Model (APAT). *2020 International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control, PARC 2020*, 298–302. https://doi.org/10.1109/PARC49193.2020.236614
10. Merriam-Webster. (2022, February 27). *"False sense of security."* Merriam-Webster.Com Dictionary. https://www.merriam-webster.com/dictionary/false%20sense%20of%20security
11. Messaoud, B. I. D., Guennoun, K., Wahbi, M., & Sadik, M. (2017). Advanced Persistent Threat: New analysis driven by life cycle phases and their challenges. *2016 International Conference on Advanced Communication Systems and Information Security, ACOSIS 2016 - Proceedings*, 1–6. https://doi.org/10.1109/ACOSIS.2016.7843932
12. Mohsin, M., & Anwar, Z. (2016). *Where to Kill the Cyber Kill-Chain: An Ontology-Driven Framework for IoT Security Analytics*. https://doi.org/10.1109/FIT.2016.12
13. Morris, A. (2021). First the attack, then the lawsuits: Why every business should have cybersecurity insurance. *BenefitsPRO; New York*.
14. Muckin, M., & Fitch, S. C. (2019). *A Threat-Driven Approach to Cyber Security Methodologies, Practices and Tools to Enable a Functionally Integrated Cyber Security Organization*.
15. NIST. (2020). *Security and Privacy Controls for Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r5
16. Samtani, S., Abate, M., Benjamin, V., & Li, W. (2019). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 1–20). Springer International Publishing. https://doi.org/10.1007/978-3-319-90307-1_8-1
17. Scarfone, K. A., & Mell, P. M. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. https://doi.org/10.6028/NIST.SP.800-94
18. Slonka, K. J. (2020). MANAGING CYBER SECURITY COMPLIANCE ACROSS BUSINESS SECTORS. *Issues In Information Systems*. https://doi.org/10.48009/1_iis_2020_22-29
19. Vukalović, J., & Delija, D. (2015). Advanced Persistent Threats - Detection and defense. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015 - Proceedings*, 1324–1330. https://doi.org/10.1109/MIPRO.2015.7160480

20. Yang, L. X., Li, P., Yang, X., & Tang, Y. Y. (2018). A risk management approach to defending against the advanced persistent threat. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2018.2858786
21. Yang, X., Zhang, T., Yang, L.-X., Wen, L., & Tang, Y. Y. (2017). *Assessing the risk of advanced persistent threats*. http://arxiv.org/abs/1707.02437