International Journal of Gender, Science and Technology
..ISSN: 2040-0748
UGC Care Group I Journal
Vol-11 Issue-02 Dec 2022

Assessing the degree of risk in a distributed and complex system

Tanmaya Kumar Das, Ashok Kumar Panda

College Of Engineering Bhubaneswar,Biju Pattnaik University of Technology,Odisha, India

***Abstract*— The majority of health care systems feature many office sites and a wide area network. Depending on the network topology, each site contains assets that are both distributed and centralized. The network architecture often shows a few complex systems and a large number of distributed systems spread throughout the hospital locations. The security team or other relevant security stakeholder within the firm will develop risk management strategies to mitigate the risk arising from the intricate distribution of assets both inside and outside the network.**

To prevent, detect, and mitigate risks, an approach that assesses the hazards in the organization's systems as well as those provided by outside vendors will be put into place. Complex and distributed systems with access control challenges are set up to perform user credential authentication from any location where the systems will be accessed. When creating the plan, quantitative measures that take into account these systems' risk resilience are crucial [6].

Keywords*— *Defense; cyber-attack; controls; planning; risk assessment.

1. INTRODUCTION

In order to make sure that the developed methodology or framework satisfies the organization's objectives to protect complex and dispersed systems on the network infrastructure, the Risk-Based approach takes the organization's purpose, vision, and goals into account. As illustrated in Figure 1, the methodology consists of five (5) stages: Business Impact Analysis, Risk Assessment, Implement Controls, Testing, and Governance. Three metrics (Activity, Value, and Outcome) assessed every action performed at every stage of the framework [3] at each stage of the technique. Figure 1

2 . FORMULATING RISK APPROACH

The first phase of the approach is Business Impact Analysis (BIA), this is conducted by the security team on the systems to identify the underlying dependencies and relationships with other applications running on the organization network. The relationship between the dependencies and business operations was identified and categorized into technical and non-technical assets. The dependencies associated with the complex and distributed systems evaluated during the categorization process reveal the organization's scope of the risk assessment. The BIA result will reveal somedependencies that would affect business continuity should an incident occur internally or externally. The outcome of the BIA conducted provides a piece of detailed information aboutthe organization environment and how dependencies and their associated systems will be affected. This process comes before conducting a risk assessment.

The risk assessment conducted will cut across the organization locations for all assets owned by the organization and third-party assets. This process is either qualitative or quantitative and the security analyst will identify the vulnerabilities in the assets inventoried and the regulatory standards required for the business process. A comparative analysis of the identified risks can be conducted using machine learning algorithms to detect the trends orpatterns in the analyzed risks data [1], [2]. Each vulnerability is assigned a risk value should the vulnerability leads to an attack. The leadership of the organization will use the risk value to prioritize the risk facing the systems within the organization. During the risk assessment phase, the output of the risk assessment determines the metrics that will be applicable to measure and evaluate the risk level of the systems within the organization. The risk value ranks the systems' vulnerabilities in the organization.

The security team implements needed controls to identify unacceptable risks and assign responsibility to the controls that will mitigate the risks. ISO 27001/27002 and NIST 800- 53 controls are the industry standard adopted during the risk approach formulation for the systems. The controls were customized to meet the organization's mission, vision, threat and vulnerability identification goals. The control process documentation will serve as a decision-making tool for

leadership during the cost-risk analysis. The control implementation provides policies and procedures that communicate the organization's priority and vision for its cybersecurity [4].

The security team administered penetration tests, vulnerability management tests, business continuity tests, internal organization audits, and control assessment compliance. The validation process confirms that the implemented controls are working perfectly and provide the required security for the systems. A new risk value was assigned to the control security and documented in the organization's risk register for prioritization and future analysis. The risk rating of the organization decreases because of the robustness and efficiency of the control security [5].

In the last stage, the formulated risk framework provides a continuous process that monitors and governs the processes stated in the previous phases. The security team documented the risk assessment and appropriate remediation process. Incorporating the process into the organization's risk register provides a general overview of the Risk-Based Approach for the organization. The organization will commit to the framework to ensure that employees and management report mechanism documented check compliance violations within the organization. The Risk-Based approach is summarized based on stakeholder's input as shown in Table 1.

Table 1

Stakeholder Input in Risk-Based Approach

Task	Security Team	Vendors	Employees	Leadership
Conduct Business Impact Analysis	**Yes**	**Yes**		
Perform Risk Assessment	**Yes**	**Yes**		
Identify & Implement Controls	**Yes**	**Yes**		
Test, Validate & Report	**Yes**	**Yes**		**Yes**
Continuous Monitoring & Governance	**Yes**	**Yes**	**Yes**	**Yes**

ATTRIBUTE -BASED CONTROL

The systems owned by third-party connecting to the organization network will expose the organization systems to untraceable risks. Third-party systems or devices added to the organization network must pass their security control test. The access control of these devices needs to communicate with the organization access control technology to ensure andenforce security. The Attribute-Based Control (ABAC) for distributed systems for third-party own devices and systems adoption during the integration process solve the third-party security issues. The systems were integrated into the CHN access control using attributes to define the access control policy rules and enforce the policy among cooperating domains from various vendors. The attributes used for the integration into the organization access control are vendors' characteristics such as the protected resources, location, and time of the vendor and attribute values approved forauthentication by the organization access control policy or permission. The privacy and security controls for patients accessing their My Chart portal from different locations use the Duo Two Factor Authentication method to verify patients' credentials before joining the organization systems. The cyber risk quantification for the organization network applies the Monte Carlo simulations to estimate the value of the risk or expected loss from the risk exposure. The risk value was determined using the time, impact of possible loss should an incident occur, and confidence level. Also, the risk of attackis an important metric that must be considered by the securityteam when quantifying the risk resilience for theorganization. The quantified risk value equals the product of the attack's impact and the probability that the attack will occur.

Monte Carlo Risk Assessment Simulator is known to have some limitations but is very useful and flexible in the analysis of risk associated with distributed and complex systems. The analyst must determine the distributional parameters within the incident data before simulation.

During the simulation, a quantitative risk assessment revealed the patterns in the incident data. The analyst should consider uncertainties related to the organization's environment. During the assessment stage, identified metrics are used in the Monte Carlo Risk Assessment simulator to assess theimpact of the risk to the organization's assets should an incident occur.

CONCLUSION

The procedures used at each stage of the methodology, including business effect analysis, risk assessment, control installation, testing and validation, and monitoring and governance, were detailed in the Risk-Based Approach framework. The relationships and underlying interdependence with the dispersed and complicated systems' operating apps were described. The dependencies and related systems provide insight into the organizational setting in which the risk assessment was implemented. Implementing security controls removes any risk to communication between external systems and the organization's system.

By integrating attribute-based control with the organization's access control system, third-party vulnerability attacks are thwarted against the organization's systems. The danger that could arise from non-employee users gaining access to the organization system is eliminated by the Duo Two Factor Authentication technique used to validate patient credentials. In order to determine the risk impact utilizing certain quantifiable indicators helpful in risk resilience, Monte Carlo simulation was used. To monitor insider activity in real time, operational controls need to be implemented throughout the entire business. in order to stop hostile actors from seizing control of delicate activities. Asset classification, cyber security knowledge, training, and a continuous log file review process from all organization systems and apps are all requirements for the organization. In order to stop the Colonial Pipeline from being attacked again, the security

The organization's stakeholders are required to abide by the topics covered in this report.

REFERENCES

[1] Urenna, N., Abiodun, A., & Yemisi, O. (2021). Application of Instance Learning Algorithms to Analyze Logistics Data, International Journal of Engineering Research & Technology (IJERT) Volume 10, Issue 07 (July 2021)

[2] Urenna, N., Abiodun, A., Isolagbenla, K., & Yusuf A. (2022). Pattern Mining of Hospitalization Data of Covid-19 Patients with Underlying Conditions, International Journal of Engineering Research & Technology (IJERT) Volume 11, Issue 05 (May 2022)

[3] Akinwumi, D. A., Iwasokun, G. B., Alese, B. Oluwadare, S. A. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology*, *36*(4), 1271-1285. https://www.ajol.info/index.php/njt/article/view/164997

[4] Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1),1-10. https://www.inderscience.com/offer.php?id=90580

[5] Gai, K., Qiu, M., & Hassan, H. (2017). Secure cyber incident analytics framework using Monte Carlo simulations for financial cybersecurity insurance in cloud computing. *Concurrency and Computation:* Practice and Experience, 29(7), e3856. hhttps://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.3856

[6] Hu, V. C., Kuhn, D. R., & Ferraiolo, D. F. (2018). "Access Control for Emerging Distributed Systems," in Computer, vol. 51, no. 10, pp. 100-103, October 2018, doi: 10.1109/MC.2018.3971347.