Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

Evaluating Risk Level for Complex and Distributed System

Folorunsho O. S
Washington University of Science and Technology
Vienna, VA, USA.

Ayinde A.Q
Northcentral University
Scottsdale, AZ, USA.

Yusuf A.S
New York Institute of Technology
Old Westbury, NY, USA

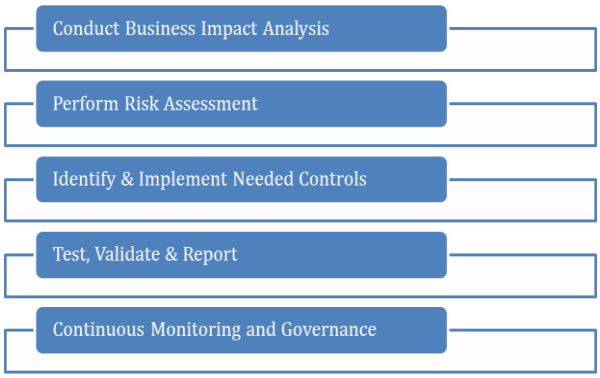
***Abstract*— Most health care system has a wide area network and numerous office locations. Each location has assets that are distributed and centralized depending on the network topology. In most cases, the network architecture indicates a couple of complex systems and numerous distributed systems across the hospital locations. To prevent risk resulting from complexity in the distribution of assets within and outside the network, the security team or security stakeholder of the organization will formulate risk approaches to handle the risk.**
An approach that will evaluate the risks in the systems owned by the organization and those supplied by third-party vendors to prevent, detect, and mitigate risks will be implemented. Access control challenges for complex and distributed systems are configured to conduct user credential authentication from any location the systems will be accessed. Quantitative metrics that will address the risk resilience of these systems are essential [6] when formulating the plan.

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

1. INTRODUCTION

The Risk-Based approach considers the organization's mission, vision, and goals to ensure that the formulated methodology or framework meets the organization's needs to secure complex and distributed systems on the network infrastructure. The approach comprises five (5) phases (Business Impact Analysis, Risk Assessment, Implement Controls, Testing, and Governance), as shown in Figure 1. At each phase of the methodology, three metrics (Activity, Value, and Outcome) evaluated each action taken at each phase of the framework [3].

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 some dependencies that would affect business continuity should an incident occur internally or externally. The outcome of the BIA conducted provides a piece of detailed information about the 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 or patterns 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

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

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**

MONTE CARLO SIMULATION

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 the impact of the risk to the organization's assets should an incident occur.

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 and enforce 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 for authentication by the organization access control policy or permission. The privacy and security controls for patients accessing their MyChart 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 attack is an important metric that must be considered by the security team when quantifying the risk resilience for the organization. The quantified risk value equals the product of the attack's impact and the probability that the attack will occur.

CONCLUSION

The Risk-Based approach framework elaborated the processes applied at each phase of the framework ranging from the business impact analysis, risk assessment, implementation of controls, testing and validation, and monitoring and governance.

Underlying dependencies and relationships with applications running on the complex and distributed systems were specified. The dependencies and associated systems reveal the organization environment where the risk assessment application occurred. Security control implementation allows third-party systems to communicate with the organization system without any risk threat.

The Attribute-Based Control integration into the organization's access control system prevents the organization's systems from third-party vulnerability attacks. The Duo Two Factor Authentication method implemented to verify patient credentials prevents the risk that might occur from non-employee users accessing the organization system. Monte Carlo simulation was adopted to calculate the risk impact using some quantified metrics useful in risk resilience. Operational controls must be deployed across the organization to track real-time insider activities. To prevent threat actors from taking control of sensitive operations. The organization must include asset classification, cybersecurity awareness, training, and constant review of log files from all the organization systems and applications. To prevent a future attack on the Colonial Pipeline, the security

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 01, January-2023

stakeholders in the organization must comply with the points discussed in this paper.

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.