

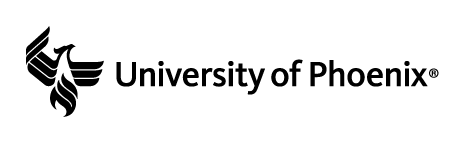
Plan of action and milestones (poa&m)



August 10, 2020

Shane Ẽire Byrne

CYB407



| **Description of Vulnerability** | **Severity Category**  **(Risk Level)**  **-Very Low**  **-Low**  **-Moderate**  **-High**  **-Very High** | **Mitigation** | **Policy** | **Scheduled Completion Date** | **Required Resources** | **Organizational Department** | **Milestones** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Broken access control: access control itself enforces policies as such that users cannot act outside their intended permissions. Consequences of this can be unauthorized information disclosure, modification, or destruction of all data, or preforming business functions outside of the limits of the user. One can either have horizontal privilege escalation (this allows users to preform actions or access data of another user with the same level of permissions) or vertical private escalation (a user can preform an action or access data that requires a level of access beyond their assigned role within the company. (PacketLabs, 2019) | Moderate to Very High: This depends on the permissions that are leaked, if the user is of low access in the system a horizontal access break would potentially give them access to the data of users of similar access; depending on the nature of this data the effect could be minimal however a vertical access break could be detrimental to the whole company potentially. | * Establishment of Access Control Policy and Procedures * Account management as well as access enforcement * Enforcement of information flow. * Separation of duties * Establishment of the concept of least privilege. * Tracking of unsuccessful logon attempts as well as system use notifications, and previous logon access notifications * Concurrent session control as well as session lock and termination * Protections set up for remote access, wireless access, use of external information systems, and information sharing. | Policy in and of itself to ensure the concept of least privilege is established and enacted for user accounts; users should only be granted the rights and abilities within the system that are necessary for their inherit job function; policy should also reflect on the concept of separation of duties so no one user has multitudinous access to the permissions established within the system. | October 1st, 2020 | Enforcement should be rather cost effective if the appropriate tools are in place to do so; cost itself would be the establishment of access controls as well as the resources required to keep the system running and maintained. As the possibility of a data breach from a lack of access control could be several billion dollars in damages depending on the scope of the breach and the nature of the data that is accessed without proper authorization. | IT itself is responsible for the implementation and maintenance of the access controls. Management and supervisory staff are responsible for the enforcement of policies in keeping access control to the appropriate proportions. | Establishment of access control based on the concept of least privilege. Establishment of automated systems to log and test for possible breaches of system assets caused by broken access control. |
| Maintenance: the preservation of an asset through functionality checking, servicing, repairing, or replacement of necessary devices, equipment, machinery, or supporting utilities. Vulnerabilities include physical asset performance and functionality as well as software or application interaction with other assets. | Moderate to Very High; if a system is designed properly with redundancies then a simple failure of a component should not in theory have drastic impact on the rest of the system. Very high would be expected within areas and systems that do not have a redundancy built into them, such is the case of legacy hardware and software that may not have an immediate replacement but are still essential for business operation. | Establishment of system maintenance policy and procedures: this being the development of documentation that indicates the dissemination of roles and establishes system maintenance policies addressing purpose, scope, roles, responsibilities, management commitments, coordination among organizational entities, and compliance. | End of Life (EOL) practices to be established for physical assets. Appropriate redundancies for systems to be put in place to mitigate the failure of a system as to not have it adversely effect the entire system. | October 31st, 2020 | Monetary resources needed being the initial set up of the system as well as acceptable redundancies. Fiscal impact over several years could be several thousand dollars in upgrades as well as replacement of failing equipment. Projected fiscal impact of failure could potentially be millions of dollars depending on the nature of the failure as well as the loss of potential revenue. | IT overall handles the physical and software for the system as it. One could argue the safety of the system is dependent on every single user of it complying with policies underlined (such as anti- phishing countermeasures). | The establishment of control addressed security-related issues that are associated with allotted maintenance tools used specifically for diagnostic and repair actions on organization information systems.  Establishment of inspection of approved storage media. Establishment of the prevention of unauthorized removal of system assets/components. |
| Distributed Denial of Service (DDOS): The flooding of a system and its servers, applications, or other internet-connected resources with unwanted traffic to the extent the system becomes unusable. | Moderate to Very High Risk; as a DDOS is dependent on the system being attacked having an open avenue in which to attach and broadcast the generated traffic towards it is possible for it to be quite detrimental to an organizations system as they are flooded by the activities of said attack. | System and communication protection policies should be put in place. This should also have application partitioning and security function isolation designed into the system itself. Restriction should be placed on internal users as well as the detection and monitoring of the system for a possible influx of traffic from a DDOS attack. Cryptographic keys should be established in allowing computers access to the company’s system. | Policies should be put in place to establish encrypted connections for every access point to the company’s systems. Remote connections through a VPN or any such similar means should be encrypted, an access key should be issued to the remote user. Termination of connection policies should be enacted to disconnect any device connected to the company’s network that remains inactive for an established length of time. | November 14th, 2020 | As a DDOS attack itself could potentially tie up the entire company’s resources it is possible the cost. As a DDOS attack could affect company operations, the monetary value of the attack could be several million dollars if it is not appropriately mitigated. Add onto that possible loss of revenue while the company’s system is down. | Generally, the IT department would bear the brunt of reinforcing the system to mitigate it against a DDOS attack. It would be a requirement of management and supervisory staff to ensure all company personnel are properly trained in how to properly utilize the system as well as the overall enforcement of policies. | Protections should be established to mitigate such an attack. Software can probe and scan the system looking for unusual signs of an attack, the absolute best means by which to deal with an attack is early detection as it is with most things. |

**References**

Cisco Security (2020) Risk Triage for Security Vulnerability Announcements

Retrieved from <https://tools.cisco.com/security/center/resources/vulnerability_risk_triage.html>

Dhanapal, A., & Nithyanandam, P. (2019). The Slow Http DDOS Attacks: Detection, Mitigation and Prevention in the Cloud Environment. *Scalable*

*Computing: Practice & Experience*, *20*(4), 669–685. https://doi.org/10.12694/scpe.v20i4.1569

National Institute of Standards and Technology (NIST) (April 2013) NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal

Information Systems and Organizations Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

PacketLabs (29 Oct 2019) Broken Access Control: Hidden Exposure for Sensitive Data

Retrieved from

<https://www.packetlabs.net/broken-access->

control/#:~:text=Access%20control%20vulnerabilities%20occur%20when,modification%20or%20destruction%20of%20data.