Dear Team,

In leu of recent events that have enfolded involving a breach within this organizations database, I was asked to lead an assessment of the network and to delegate my findings. After much research and thought I have constructed the following:

**Who will be assessed ?*:*** Since the scope of this assessment will be the entire network, everyone will be addressed. This includes but is not limited to: The C-Level executives, Managers, DBA’s, HR personnel, Engineers, and even the Janitors. The point of this is to verify that all users and guests only have privileges needed to perform their duties and nothing more. It is essential that permissions be as strict as possible when configuring rights. Because of this, a mandatory password reset should be rolled out company wide. Also, a stronger auditing trail should be implemented for these users.

**What Assets ?:** Below we have proposed the scopes for this epic and have defined the assets of which our company should harden.

*-Hardware:* This includes physical devices that operate this organization like Servers, Routers, Firewalls, Workstations, Wireless Access Points, Biometric Scanners, etc. We will be protecting with concepts like physical security and redundancy.

*-Software:* This includes the applications that this organization uses both in house and hosted in cloud environments. This protection will include concepts of SQL injection on the Data side, as well as architecture and administrative rights in our cloud environments.

*-People:* This includes everyone within the organization. Educating the people about cybersecurity will lead to a greater cyber security posture. This protection will include mandatory trainings and greater ease of reporting suspicious events.

*-Procedures* This includes the actions taken place within the organization. This can include documentation on how to install devices or implement proper development as well as proper procedure for when an employee parts with the company.

***What Threats ?:***

The threats mentioned below will be ordered by their respective Risk Values based on the table below.



|  |  |  |  |
| --- | --- | --- | --- |
| **Threat Level** | **Attack** | **Description** | **Resolution** |
| **5** | **Social Engineering** | The threat of a social engineering attack is high, it can be efficiently executed if crafted correctly. Employees are easily susceptible to phishing attacks and high-risk passwords. | Actively engage team with inhouse phishing emails and other offensive security measures along with quizzed training mandates and strong password policies. |
| **4** | **Privilege Abuse** | Users may have more permission then needed or even the ability for escalation. This can lead to unwanted leaks of information or execution of code on the network. | Implementing a strong audit trail can help alleviate this issue. Along with a strong permission on a need to know basis policy. It is crucial that documentation is followed when off boarding an employee. |
| **3** | **Application Exploits** | The applications within the organization can be susceptible to attacks such as SQL Injection, Cross Site Scripting, and Buffer Overflows. | Applications should actively be penetration tested by a 3rd party to look for holes in the software security posture and to stay up to date with threats. |
| **3** | **Denial of Service** | Services can go down for many reasons both physical and software defined. It is imperative we keep them as safe as possible while still having a contingency plan for redundant operations. | On the application side load balancers and client sides SYN cookies could alleviate threats from floods, while also having backups ready to go on other cloud providers as well as having backup services in house. |

The for mentioned is what we concluded on the security assessment of this organization. The contents of this information should be implemented within the company if this organization is to increase its security posture.

Thank you all!

-ERIC WEBB