Vulnerability Management

By Devarsh Parmar

Vulnerability Management Methodology

Let’s talk about the different phases in Vulnerability Management:

I. Prework
II. Process integration: the methods discussed/shortlisted in the prework have to applied.
III. Continuous Improvement: This consists of many stages, which are based on quick solutions rather than taking time to build a perfect solution.
    A. Identify the issue
    B. Evaluate the cause and severity
    C. Remediate: Patch the issue
    D. Verify i.e. rescan for the same issue if it still persists on the new technology
    E. Summary Report: Finally create a summary report stating the issue and steps taken to resolve it.

In the next few slides we will talk about each of the points in detail.

Prework

First Line of Defense consists of Management control and control of IT.
Second Line of Defense defines policies, frameworks and requirements.
Third Line of Defense consists of audits to test implementations of the previous 2 line of defenses.

Process Integration

1. IT Asset & configuration management
2. Monitoring and event management
3. Incident management

All these stated above are a part of IT service Management process. To achieve a good level of security we will need to have good tools and great tool implementation.

1. Privileged Access Management Tools.
2. Configuration Management database, these can be achieved by storing data in 3 levels of schema.
3. A live scanning tool
4. A live ticketing tool
5. A security orchestration, automation and response (SOAR) tool

Information System Security Baseline

An up-to-date Information System Security Baseline is crucial for several reasons:

1. Any asset not properly configured can become a security vulnerability.
2. Security settings required by an organization are so varied that many of them may be neglected.
3. Updating your data security policy is necessary for compliance.
4. Without updating your security program, your company is more at risk of potential security breaches.
5. Relationships with vendors depend on trust.

Baseline management is fundamental to managing projects of all types and especially important in cybersecurity, where everything is a race against time and against very guileful opponents. Although baseline management seems like time-consuming "record keeping," it is the only way to know where you are, how your assets are operating, what has changed, and what needs to be changed. Baseline Configuration Management requires automated tools to help avoid missteps and oversights. The depth and frequency of baselining becomes a strategic decision that requires the input from cybersecurity and IT, as well as management, and is a vital component of the health of an organization.

Mitigation Planning

Mitigation planning is the process of identifying policies and actions that can be taken over the long term to reduce risk and minimize loss in the event of a disaster occurring. It is a detailed plan that includes the specifics of what should be done, when it should be accomplished, who is responsible, and the funding required to implement the risk mitigation plan. The purpose of risk mitigation procedures is to protect businesses as much as possible from the threat of different risks, such as loss of inventory or machinery malfunctions