METHODOLOGY

mathias

April 18, 2017

There are quite many techniques or methods that can be employed in calculating the security metrics of a network from being vulnerable to unauthorised attacks. These include:

1 Inventory of Authorized and Unauthorized Devices (both software and hardware)

These assist IT and security departments when changes occur on the network. The goal of this control is to find how many devices are found and based on those devices, which ones are authorized and which are not. It also labels the device owners in the system, and a formular can be applied.

2 Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers:

Here Automated tools to run scans on computers and workstations may be used to find insecure configurations, it can be used to determine how often configurations are being deployed insecurely and on which devices this is occurring and by whom and also using standardized secure images for deployment of machines should be part of initial setup and deployment.

3 Secure Configurations for Network Devices such as Firewalls, Routers, and Switches:

Using percentages to find how many insecure configurations exist overall and of those, how many are firewalls, routers or switches. Quantitative method as well and knowing the quantity of devices that have insecure configurations can assist in knowing the overall vulnerability level of the network are used.

4 Boundary Defence.

Here a boundary shall be established, accessed externally physically, through a firewall, VPN or through a wireless connection. The boundary is defined and, then verifying proper secure implementations be put in place and be analysed. This is where it will be important to find a metric so that boundary defences can be measured and compared against any baseline security practices. Using various metrics is crucial in regards to Boundary Defence. Having a proper logging method in place that alerts and notifies relevant staff when unauthorized packets enter the network is important to test.

5 Maintenance, Monitoring, and Analysis of Security Audit Logs.

S Here logs are checked and how often abnormal traffic with threats or exploits are found beyond normal checks and controls. A procedure for audit logs that are stored will be put in place to check these logs regularly. Having some sort of automation in place so that when log errors or problems occur an email or message is sent to the appropriate department. As these log messages appear they then can be used for later trend analysis and possible reporting to upper management. The metric we will use for will be based on a scoring system that will show the percentage of devices with logging correctly configured.

methods include:

i. Software Security.

ii. Controlled Access Based on the Need to Know

iii. Continuous Vulnerability Assessment and Remediation.

iv. Account Monitoring and Control.

v. Malware Defences.

vi. Limitation and Control of Network Ports, Protocols, and Services.

vii. Wireless Device Control.

viii. Data Loss Prevention.

ix. Penetration Tests and Red Team Exercises.

x. Incident Response Capability.

xi. Data Recovery Capability.

xii. Security Skills Assessment and Appropriate Training to Fill Gaps.

ANTCIPATED OUTCOMES Without the proper security, networks are vulnerable to number of calamities, whether initiated by the technology itself or by the people and processes behind it. Therefore the above methods shall ensure an effective offer to a secure network system which shall give users the confidence in knowing that their most prized assets - their computer systems, networks, and data are safe, secure, and protected against attacks and unauthorized users from inside or outside the network boundary. This shall also help to achieve efficiency, and effectiveness of the network system.