Minimum Baseline Standards

Minimum Baseline Standards (MBS)

Background

Minimum Baseline Standards also referred to as Minimum Security Baseline (MSB) is a minimum information security configuration standard, which can be applied to several layers of an organizations Information Technology Infrastructure. As a best practice, servers, workstations, routers, switches, firewalls, etc. should all have a minimum configuration standard which can include security patch minimums, unnecessary services on a system(s) that should be disabled, and baseline security configuration standards for network appliances.

Additionally, Minimum Baseline Standards will allow organizations to deploy systems in an efficient and standardized manner.

Guidelines

- The scope of the minimum baseline standards will depend on the immediate needs of the organization, and will specify a standard for installing, hardening, and placing into production, new servers and workstations.
- Creating and maintaining your security baseline standards will be an ongoing process, requiring the help and support of a number of departments within the IT organization.
- Setting standards on the organizations IT infrastructure will not only assist with enhancing security, but also make it easier to provide technical support to users by requiring that systems comply to a configuration that has been tested and known to work with the applications used by the organization.
- A common starting point for developing minimum baseline standards is to use a system-hardening guide for the system or component, and then enhancing the standard as necessary to accomplish the security goals of the organization. It is important to ensure that baselines are reasonable, and do not interfere with the organizations ability to operate normally.

Codify

- Once the minimum baseline standards for a particular system or device has been established, it should be appropriately documented and classified according to functional type, such as server type (Web or Application), desktop workstation, router, etc.
- The new standard should be made final and approved by the IT management team, additionally the standard should be published and made available to IT staff and the overall organization.
- The next step is to apply the new baseline configuration against the organizations test machines. This will assist with the identification of issues and insure that your configuration will result in a functioning system or device.
- Once testing is complete and a high level of comfort has been achieved with the minimum baseline standard, documentation should be updated to reflect any changes and final approval by management should be obtained.

Socializing the MBS

- Communication to the organization regarding the minimum baseline standards can sometimes be difficult and without effective communication could easily become a failed IT initiative.
  - Upper management should communicate the importance of MBS to IT and the overall organization via conference calls, and formal meetings.
- Convincing an organization to adopt minimum baseline standards will result in the following:
  - Significant time and cost savings to the organization due to standardization;
  - Risk reductions by eliminating the “low-hanging fruit” vulnerabilities;
  - Ensure that that new systems begin service in a known-state;
  - Assist the support team by giving them standard systems to work with;
  - Help achieve the goals of the security policy;
  - Strengthen the organizations overall security, and help to minimize the damage in the event of a network compromise;
  - Better service level agreements from the help desk

Implementation

- Careful considerations should be made as to the implementation schedule of the Minimum Baseline Standards program. After defining, documenting, testing, and socializing the new standards to the organization, the MBS should be implemented in a phased approach in small host deployments as to eliminate or reduce outages or issues that may arise. If the implementation causes an issue, it can result in future implementation delays or stop the implementation completely. Considerations should be made to implement the following departments or business lines during rollout:
  - Owners of high risk systems – Implementing High Risk Systems in small batches will provide reliance to other system owners that the new standards are not creating issues and allow the organization to operate as normal without system or network interruption. Additionally, implementing these systems will fulfill the organization's regulatory requirements.
  - Businesses with new builds / redesigns - this would create a good opportunity for the organization to begin using the baseline standards on new builds going forward.
  - New solutions hosted on company platform as they can be created as necessary for the organization.
  - Business with low risk - there will most likely be less scrutiny and pushback to the IT organization.

Lessons Learned

- After management has determined the groups or business units that the Minimum Baselines will be deployed to, and implementation is successful; the IT organization should learn from the early adopters of the standards.
- Careful considerations should be made to update documentation and resolve issues that occurred during the initial implementation. The IT organization should work to identify:
  - Specific Minimum Baseline configurations that cause functional and operational issues on network devices and systems.
  - Configurations that will be difficult to implement or create excessive workload on the IT staff. Cost / benefit analysis should be taken into consideration.
- Management should also define a systematic method for managing exceptions. For example, how to customize the standard for systems that require additional enhancements, or for systems that are not capable of running the standard.

Enhancing the Standard

It is the IT Managements responsibility to ensure that the standard is not causing performance issues, or affecting the availability, stability and resiliency of the systems to which it is implemented on. If after implementing the standard it is determined that enhancements should be made, the IT function should immediately remove the minimum baseline standards (if required) communicate to the organization, initiate the changes that should be made, and finally test and re-implement as necessary.

Exceptions Tracking

The IT function should be tracking deviations and exceptions. Additionally, an exception and acceptance program should be implemented. This consideration should be made prior to adopting configuration management.

Creating Visibility & Socializing Program Success

- The IT function should publish Qualitative and Quantitative metrics to management. Examples of the types of data that should be reported include:
  - The amount of systems that are on the standard (Quantitative)
    - *Provide a rational as to why are the others are not (Qualitative)*
  - How many nodes or devices are being monitored (Quantitative)
    - *Provide a rational as to why are the others are not (Qualitative)*
  - How many exceptions have been noted (Quantitative)
  - What is the average number of exceptions (Quantitative)

- Program Managers and Sponsors should be communicating the lessons learned and overall success of the initiative. During these calls / meetings with management and the organization advertisement of the benefits should be reiterated and quantitative metrics on why systems and devices are NOT on the standard should be published and communicated.

Transition to Monitoring

- Once the enhancements have been made and the standard is fully implemented the program will be transitioned to monitoring. The following should be considered
  - The overall maintenance of the the program, which include continued enhancements to the standard as new applications, servers, and network devices are added to the infrastructure.
  - Using metrics to ensuring and measure compliance. All systems and devices within the organization should be utilizing the standard. Outside vendors and remote staff should be aware of the standard and adherence should be made mandatory for all devices added to the network.
  - Issues should be addressed and documented in a timely manner, this includes follow up, resolution, testing and updated documentation
  - Metrics – Metrics should be maintained and communicated to management to ensure the efficiency, and effectiveness of the program; especially where issues are identified or the standard is not being used on specific systems or devices.

Questions