Realtime publishers
"Leading the Conversation"

The Essentials Series: Selecting the Right Network Threat Management Solution

Proper Security Management Enables Operational Efficiency

sponsored by
NOKIA

by Dan Sullivan

Copyright Statement

Proper Security Management Enables Operational Efficiency

It is generally understood that IT departments are expected to do more with less. The benefits of automation that have improved efficiency in other business areas should be applied to IT operations as well—there is a "physician, heal thyself"-type of expectation. An underlying assumption here is that one does not necessarily need to purchase new technology to improve operational efficiency – changes in operations and business practices can help as well. One place you can start to find operational efficiencies is with security operations. There are two broad areas in which security operations can be made more cost effective—proper allocation of staff and by automating key security management tasks.

Optimizing Security Staff

Experienced IT staff are hard to find, difficult to retain, and easy to overwhelm with rudimentary tasks. Take for example, the following hypothetical scenario. Suppose a senior sales executive returns from a business trip with a malware-infected laptop. The laptop is connected to the corporate network infrequently and so has not received recent patches and antivirus updates. He connects his laptop to the corporate network and checks his email. Within minutes, the malware detects the network connection and spreads to other devices, including devices recently re-imaged using a 3-month-old operating system (OS) image. The updated antivirus software on several workstations detects the malware, quarantines it, and notifies users, who call the service desk to report a problem. At that point, the service desk manager decides to escalate the issue and requests assistance from a senior security professional to isolate and eliminate the root cause of the problem.

In some ways, this problem is rather mundane—viruses are commonplace and remediating a minor infection should not require the attention of more senior personnel. The most sophisticated and virulent forms of malware can be difficult to detect and remove, but lesser forms such as the one described here could have been handled more effectively if

- The senior sales executive kept the laptop OS and antivirus software patched and up to date
- A network access control system validated the device configuration and patch level before granting it access to network resources
- A well-defined network access control policy were in place
- Systems administrators methodically re-created device images when patches are released or at least immediately apply patches as soon as an OS image is installed on a device

The problem in this scenario is multifaceted. Yes, the laptop that infected the network should have been better protected, but the bigger issue is that the security management strategy of the organization should have been better focused on preventive measures. Top security talent in an organization is needed to formulate strategies, address critical security issues, and collaborate with other IT staff to maintain the security of systems and data. To allow them to function in these capacities, you need to reduce the burden of rudimentary tasks through more effective automation.

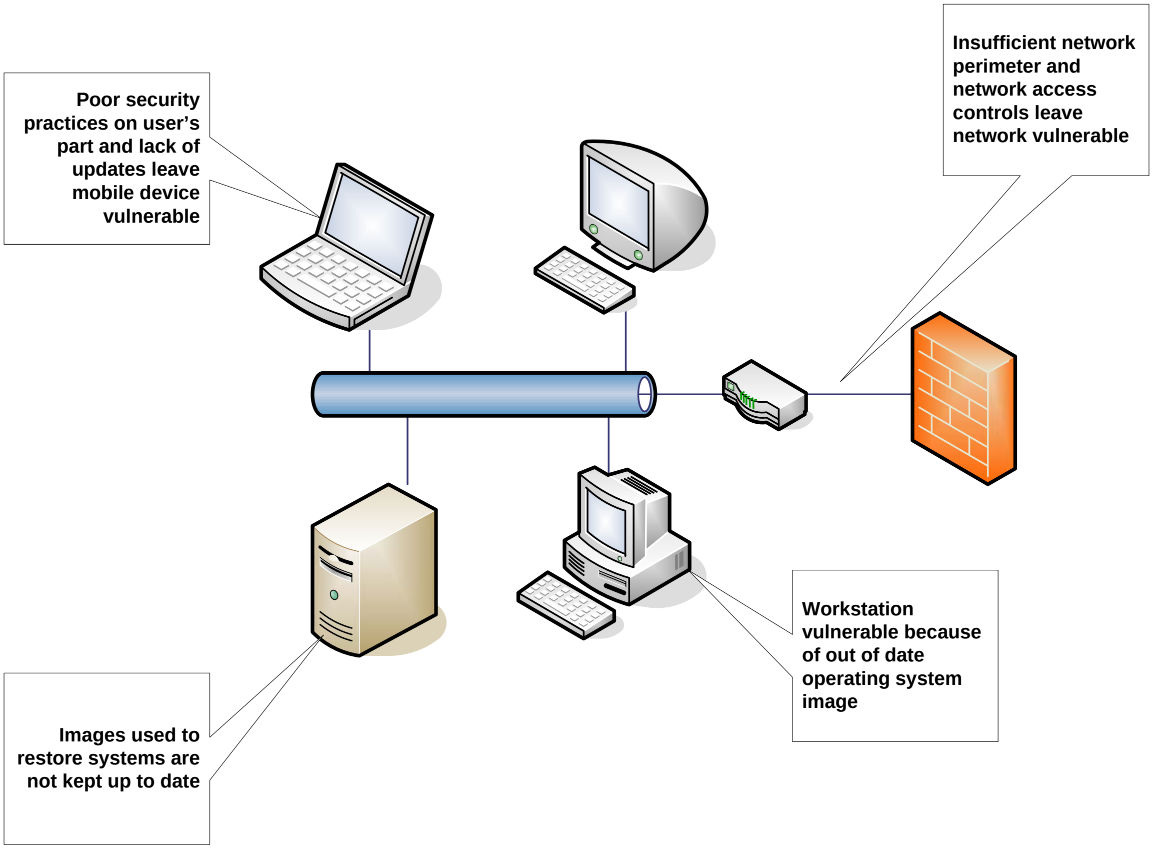
Poor security practices on user's part and lack of updates leave mobile device vulnerable
Insufficient network perimeter and network access controls leave network vulnerable
Workstation vulnerable because of out of date operating system image
Images used to restore systems are not kept up to date

Figure 1: A number of potential threats can be addressed by improving operations management and implementing policy-based controls.

Improving Security Management by Improving Operations

Proper security management can reduce the burden of performing basic but essential tasks. Several areas in particular can help IT and security staff avoid time-consuming tasks:

- Policy administration support
- Granular network monitoring and statistics gathering
- Reporting
- Support for asset and configuration management

Consolidating these tasks, for example, within a single network appliance, can further enhance efficiencies.

Policy Administration

One of the challenges with multiple applications distributed over many servers running a number of different OSs is ensuring proper enforcement of user and application authorizations. Organizations may have a range in the number of users at any point in time, starting with tens of users that grow into hundreds of users and possibly into the thousands. Fortunately, these users can often be clustered into groups with common functional requirements and similar access control rules. This combination of growing numbers of users forcing more efficient access control management and the ability to formulate a smaller number of distinct sets of rules governing their access combine to promote centralized policy administration.

Centralized policy administration uses group-based policies to adapt to the needs of specific types of users while maintaining consistent policies within those groups. This is done with a combination of policy management building blocks:

- Policies or sets of rules that dictate how a device or application will respond to particular requests for services from users or will respond to an event on the network. For example, a Web service providing sales data may be accessible only to members of the "Manager" role.
- Events, such as an access control request, a perceived threat, an unauthorized activity, or the detection of a non-conforming configuration. Typical events include database logon attempts or devices connecting to the network over a wireless access point.
- Tasks, which are actions taken in response to an event; policies define what tasks are preformed in response to an event. Examples include logging event data or terminating a network connection.

Policies, events, and tasks are relatively high-level generic constructs but are sufficiently broad to allow network and systems managers to control processes and respond to changes in dynamic environments.

Granular Network Monitoring and Statistics

Let's face it, network security is installed at mission critical points within the network. However, we make security decisions independent of what is really going on in the network. Fore warned is fore armed. This adage holds for network and security management. With sufficient network monitoring, administrators can collect baseline data on their network operations that helps to understand typical behavior on the network. Detailed information about network performance and load can help with several management tasks:

- Understanding how changes to device configuration and application functionality impact network performance
- Determining the functional impact of changes to security policies, such as implementation of more stringent access controls

- Spotting sudden, unexpected changes in network traffic which can indicate various forms of attack
- Detecting unusual amounts of traffic from certain devices, which can indicate a device has been compromised and is employed as a zombie in a botnet
- Understanding the potential performance impact of new applications on the network like VoIP or streaming video.

Collecting data on network events and traffic must be coupled with effective reporting mechanisms to realize the full potential of this data. Security must be scoped in light of the realities of the network. Not just on what the administrators think is going on. For example, are rogue wireless access points connected to the network? Are unwanted network services running on application servers? Data collection should be generalized enough that data about unanticipated services and network traffic are captured along with expected data. Understanding the different protocols and how the firewall is handling them is also important to ensure proper capacity planning.

Reporting

Reporting on network performance serves at least three distinct purposes:

- Monitoring and alert management, in which data about network traffic and events is used for day-to-day management activities and for making informed security decisions. Alerts are especially important for remediating problems as soon as possible, and this may require drilling down to understand the context and details of an event. Ideally, this information is used to refine policies to prevent such unwanted events from occurring again.
- Compliance reporting, which is a form of security reporting that helps network administrators and IT managers ensure that security policies are enforced. Key performance metrics such as the number of malware-infected emails and volume of spam may prove to be leading indicators for the need for additional security measures. Additionally, these can also help to bridge the information gap between administrators and upper management.
- Capacity planning is the most long-term focused of the reporting purposes. In this area, data collection and reporting can provide information about trends in network performance, traffic volumes, and malicious activity, which can influence future network infrastructure investment decisions. Long-term planning should also take into account policy formulation, improving awareness of network events, and reducing response times to address problematic events.

Support for Asset Management

Asset and configuration management practices can improve security and reduce operation overhead at the same time. The basic principle is that to effectively manage a network, you must understand what devices and applications are on it and keep those devices up to date. Improving security depends on having constant monitoring that will help you identify vulnerable devices.

Operations on devices, such as backups, should be applied consistently across groups of devices as well. This reduces ad hoc management and improves conformance with operations policies. Of course, these principles apply to security devices as well.

Summary

Operations management and security management are closely inter-twined. The better the operational management, the more IT resources can be dedicated for challenging security problems. Several areas of operation management are especially important to improving security, including policy administration support, granular network monitoring and statistics gathering, reporting and support for asset and configuration management. By implementing sound and effective operations management, you can reduce demands on security professionals to assist with mundane tasks and instead leverage their expertise for more challenging demands.