Desktop Security Policy Enforcement - How to secure your corporate mobile devices

Jason S. Meyer

Abstract— **As more and more corporate dollars are being spent on securing the network from outside intruders, the threat from within is being overlooked. The mobile devices and the wireless access to networks open up many new possibilities to expose the corporate network to intrusion and theft. As mobile devices are carried by employees from the safe corporate network to the unsecured wireless networks of coffee shops, bookstores and airports, the need for desktop security is higher than ever. What would you need to protect a mobile device from intrusion while away from the corporate network? Anti-virus software, operating system security patching, firewall software, anti-spyware software, file-encryption software and access-control lists are all items that can make up a comprehensive desktop security package. Each of these items require administration and maintenance that is usually far beyond the ability of the common user to handle on a regular basis. As a layer of the Defense in Depth method, it is the responsibility of the security administrators of a corporate network to secure the mobile devices even when they are not connected to the network to avoid a security risk being brought back into the network. This would be a desktop security policy enforcement that has many different names depending on which vendor is trying to sell it. This paper will discuss the items that make up a secure desktop security policy and explore a few of the available solutions from vendors that meet some or all of the basic requirements.**

Index Terms—Desktop Security Policy, Network Access Policy, Network Admission Control

I.Introduction

DESKTOP security can have many meanings depending on whose definition is being used. Ask a common user what their definition of desktop security is and you may get responses such as anti-virus software is installed or username and password authentication is in place. That user will probably be the same one that turns around and disables the anti-virus software because it slowed down their machine too much and will write their username and password on a post it and put it under their keyboard. Pose the same question to members of management and you may have gotten a response such as the corporation's commitment to information security is of the highest priority and then they will turn around and cut budget proposals for security measures. These cuts will be justified because there have not been any serious breaches or data losses before and the return on investment based on prior history may not justify the costs. With newspaper headlines that uncover sensitive personal information theft due to lax corporate security measures becoming more commonplace, desktop security is coming to the forefront as a necessary aspect of the corporate security policy. Corporate security policies are redefining what is required to secure the desktop that once was a stationary item and all that was needed was anti-virus and a corporate firewall to protect. With higher corporate productivity becoming directly attributed to the degree of mobility afforded through advanced information technology, the need for more in-depth security measures that can handle advanced threats to mobile devices is needed.

II.Desktop security policy

Any Desktop Security Policy is a direct subset of the Corporate Security Policy and must address three general areas; Confidentiality, Integrity and Availability [1]. These areas are not only for the protection of the single desktop but also the network and every desktop that is a member of it. The term Desktop is actually significant of a number of types of devices such as Workstations, Servers, Laptops, Personal Digital Assistants (PDA's), Cell Phones and IP Phones. These devices can be further classified into multiple categories such as;

1. Managed or Unmanaged
2. Wired or Wireless
3. Local or Mobile

Each one of these categories will require adjustments to the Security Policy to accommodate variations of connection times and network access to resources. All of these factors taken into consideration can make the formulation of a Desktop Security Policy quite overwhelming. The key to making the Desktop Security Policy effective is to establish the right combination of security products and procedures to meet the aforementioned requirements [3]. A basic list of the security products would include an anti-virus program, a personal firewall, anti-spyware software, file-encryption software, access-control lists and an operating system patch management solution. Each one of these products will help ensure at least one or more of the three principle areas, Confidentiality, Integrity and Availability are addressed properly. Lets see what each of these products are and how they fit into the overall desktop protection plan.

A. *Anti-Virus Software*

A computer program that attempts to identify, thwart and eliminate computer viruses and other malicious software. Anti-virus software would fit into both the Integrity and the Availability categories. Examples of this would be Symantec Anti-Virus and McAfee VirusScan.

Manuscript received July 17, 2006

Jason S. Meyer is a graduate student at East Carolina University, Greenville, NC, 27858(e-mail: jsm0829@ecu.edu).

B. *Firewall Software*
A computer program that will provide controlled connectivity between zones of differing trust levels as determined by a security policy. Firewall software can be considered a part of the Availability category. Examples of this would be Symantec Client Security Firewall and Sygate Online Scan. Microsoft has added it's own personal firewall software into the Windows operating system starting with XP Service Pack 2 and Server 2003 Service Pack 1.

C. *Anti-spyware Software*
A computer program that attempts to identify and remove spyware from a protected computer. This software can be classified as part of the Confidentiality category. Symantec Anti-Virus now includes this function or there is freeware such as Spybot Search and Destroy. Microsoft is now offering it's own version called Windows Defender.

D. *File-Encryption Software*
A computer program that will take data stored on a media device and apply an encryption algorithm to it in order to render the data unreadable to those without proper access. This software would be part of the Confidentiality category. An example of this software is Credant Technologies Mobile Guardian. Microsoft includes this as an option on it's Active Directory enabled operating systems.

E. *Access-Control Lists*
This does not need to be separate software on the desktop. The operating system most like already accomplishes this through logon username and passwords. Multiple layers of access control may be put in place through other software such as the file-encryption software. This would be classified in the Confidentiality and Integrity categories.

F. *OS Patch Management Software*
There are multiple variations of patch management software available. Some require a managed environment to accomplish patching a desktop where others allow the desktop to update themselves on their own schedule. Either way, it is the means that an operating system receives minor fixes (patches) to fix bugs or security vulnerabilities in the software. This last one may be classified as part of the Integrity and Availability groups. Many different examples are available for this to include Microsoft's Systems Management Server, Computer Associates Software Delivery (ShipIt) and Microsoft's Windows Server Update Services. The last one is a free offering from Microsoft.

There are many software vendors that offer enterprise solutions for each of the above software requirements. They have management consoles and reporting agents that turn in status reports when communications with parent servers are established. Some of them will even "wake" themselves up to report in on a predetermined schedule. Some of the vendors may even be able to supply more that one of the required software that can all be managed by the same management consoles. These solutions have made administration much easier but still do not offer the enforcement mechanism that is needed to ensure that the corporate policy is in place at all times. Having one single desktop that does not maintain an up-to-date security posture is equivalent to a security vulnerability threatening the entire network; therefore it must be required for every desktop in the environment at all times.

III.Network Access Policy

Along with any Desktop Security Policy, we must look at implementing an automatic policy enforcement mechanism that can ensure a high level of endpoint security compliance and at the same time protect the rest of the network [4]. The best time to accomplish this is before the desktop gains unrestricted access to the network. This is to include any access to the network whether it is from an internal wired connection or a wireless connection or a VPN connection. Any viable product that is to be used in this capacity must meet a number of the following criteria;

1. It must be able to recognize all types and variations of the required software that can be available on a desktop
2. It must be able to scan the above software for policy complicity. This will also include signature file age, version control and rule set variations.
3. It must be able to be centrally managed for ease of use by an administrator. Having to manage policy in multiple consoles will allow for duplication error.
4. It must be able to authenticate desktops and users to grant proper network access if authorized.
5. It must be able to deny full network access based on configuration scan results but still offer an avenue for the devices to obtain remediation help.
6. It must have the ability for administrators to easily create custom policies.

These are just a few of the items that a Network Access Control device must be able to accomplish in order to be a complete solution. The first roadblock to this will be the agreement for all vendors to develop and adhere to a common set of standards when it comes to NAC policy. In May 2005, the Trusted Computing Group established and working group named the Trusted Network Connect (TNC) in order to formulate an open set of standards for Access Control. Since its establishment, many software makers have pledged to comply with the standards set forth by the group. Of these groups, two major software vendors come to the forefront whenever NAC is mentioned, Cisco and Microsoft. Lets take a brief look at each of the vendors solutions to review their advantages and disadvantages.

A.Cisco Network Admission Control

1. Host based Agent or Agentless (WebBased)
2. Layer 2 Enforcement
3. Can segment into separate VLAN for remediation
4. Extra layer of authentication
5. Centralized Management Console

6. Centralized Policy Distribution
7. Uses 802.1x Extensible Authentication Protocol L2 Session for compliance scans
8. Can enforce based on User or Computer Role
9. Separate ACL per Role [10]

B.Microsoft Network Access Protection

1. Multiple Host Based Agents (MS Longhorn and Vista Only) and Agentless (WebBased)
2. Layer 2 Enforcement
3. IP Packet Filters or VLAN established until remediation is complete
4. Can use separate layer of authentication, standard is Active Directory
5. Centralized Management Console
6. Centralized Policy Distribution
7. Uses 802.1x Extensible Authentication Protocol L2 Session for compliance scans

So the first problem with Microsoft's version is that it is currently only available in its Longhorn and Vista operating systems. Since these operating systems are in Beta testing, they are not a viable solution for the moment [7]. Microsoft's first attempt at NAC was its Network Access Quarantine Control which is an add on to the Windows Server 2003 operating system and requires that the client be set up in a DHCP based configuration. If a computer owner were to manually insert a good IP address into the computers configuration, it would completely bypass the NAC attempts of scanning and security compliance enforcement. Therefore it would only have been good if the desktop were entering through a remote connection that could be controlled through an RRAS server where it must be DHCP enabled [8].

Cisco is touting its solution as only requiring 5 days implementation time and will require no network upgrades in order to implement. A possible downside to the Cisco solution may be in that anyone can change the registry settings that the Cisco agent checks and make then match the minimum requirements needed to be granted access, thereby bypassing the security check.

On 18 October, 2004, Cisco and Microsoft had announced that they were going to share and integrate their NAC products but have never fully developed this collaboration. Each company ahs continued with its own products with little regard for the other.

IV.Conclusion

In this paper I have reviewed the need for a strong corporate security policy that would include a desktop security policy and a network security policy. I have discussed some of the software items that would be needed to enforce these policies in a LAN environment and reviewed a few of the currently available vendor solutions available.

References

[1] *Sterne, D.F., "On the buzzword `security policy'", Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on, 20-22 May 1991 Page(s):219 – 230

[2] *Varadharajan, V ., "A multilevel security policy model for networks.",

INFOCOM '90. Ninth Annual Joint Conference of the IEEE Computer and Communication Societies. 'The Multiple Facets of Integration'. Proceedings., IEEE 3-7 June 1990 Page(s):710 - 718 vol.2

[3] *Hamed, H.; Al-Shaer, E., "Taxonomy of conflicts in network security policies", Communications Magazine, IEEE, Volume 44, Issue 3, March 2006 Page(s):134 - 141

[4] *Burns, J.; Cheng, A.; Gurung, P.; Rajagopalan, S.; Rao, P.; Rosenbluth, D.; Surendran, A.V.; Martin, D.M., Jr., "Automatic management of network security policy", DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings
Volume 2, 12-14 June 2001 Page(s):12 - 26 vol.2

[5] *Jyh-Cheng Chen; Ming-Chia Jiang; Yi-wen Liu, "Wireless LAN security and IEEE 802.11i", Wireless Communications, IEEE, Volume 12, Issue 1, Feb. 2005 Page(s):27 – 36

[6] *"IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control", IEEE Std 802.1X-2004 (Revision of IEEE Std 802.1X-2001), 2004 Page(s):0_1 – 169

[7] "Network Access Protection Platform Architecture", Microsoft Corporation, May 2006

[8] Wettern, Joern, "Secure Network Access", Redmond Mag.com, June 2005

[9] Conover, Joel, "Produst Analysis: Network Access Control", NetworkComputingReports.Com, 30 Jun, 2006

[10] "Network Admission Control: A Techniacl Overview", Cisco.com, 2005