Global Information Assurance Certification Paper

Desktop Security in the Enterprise: a Real World Evaluation

Introduction

Although it has been said that the only truly secure system is one that is disconnected from a network, encased in concrete and lying at the bottom of the ocean , real world best practices are of necessity somewhat less restrictive than this. The purpose of this paper is to examine and discuss security concerns and configuration for both desktop and mobile systems on an actual production network. Topics covered will include the Operating System (O/S), Antivirus software, client Firewall(s) and remote access. The security of the network Server(s), while certainly of major import in any business, large or small, will not be addressed here.

The subject of this evaluation is a medium sized division (600-700 clients) of a large corporation involved in the Education marketplace. The mindset of mid- and upper- level management is more along the lines of what Mr. Jeffrey Schiller of the Massachusetts Institute of Technology has described as existing in a University setting.* While the parent corporation is a multinational concern, the subject is, for the most part, located in the United States. The computing platform is a mix of Mac O/S 8.x and 9.x on the Macintosh and Microsoft's Windows95(OSR2) (Win95) on the PC clients running on a TCP/IP based network utilizing Services for Macintosh on Microsoft Windows NT4(SP5) servers.

Client Operating Systems (Mac)

All Macintosh clients (all desktop systems, no notebooks) were connecting to our WindowsNT servers via "Services for Macintosh" (SFM) , a built in service of the WinNT operating system. For a variety of reasons, including available hard drive space reporting and system stability, a decision was made to stop using SFM, and implement a product called "DAVE" from Thursby Software. Dave actually implements the NetBIOS protocol stack running over TCP/IP on the Macintosh platform, and in doing so eliminates the ClearText (i.e.: unencrypted) transmission of passwords to the authenticating server, replacing them with a LanMan hash. Although less secure than NTLM or NTLMv2, anything is better than no encryption at all. Another effect of implementing DAVE was the elimination of the ability to "drop" files into another users home share (user folder). This caused a disruption in the workflow of some of our production departments, but it served to increase the security levels on the Macintosh side of the organization.

* Mr. Schiller described the university setting as being more open than the typical corporate network in his tutorial "Network Security: Practical Approaches from the Front Lines" presented at the Networld+Interop conference in Atlanta, Sept., 2000.

Client Operating Systems (PC)

Prior to the current round of desktop system replacements, all PC clients had been standardized on the Windows95 platform. While certainly easier to use than its predecessor (DOS 6.22/Windows for Workgroups 3.11), Win95 did not allow for easy application or administration of security standards. Although the Policy Editor program did indeed allow for some measure of
basic security, implementation on the desktop/mobile environment was not feasible. As the Win95 password security system served only to provide a means of authentication to the local machine, could easily be bypassed by the cancellation of or escape out of the login process and was cached in a relatively easily cracked .pwl file , it became obvious that some other means needed to be found to insure client (and subsequent network server) integrity. The decision was made to migrate to Windows 2000 Professional (Service Pack 1)(Win2k). Easier to configure than the O/S it replaced (Windows NT Workstation), Win2k offers increased stability and security (compared to both Win95 and WinNT) by use of NTLM and/or NTLMv2 password encryption (as opposed to the LanMan Hash used by Win95), while the familiar GUI allows for a relatively simple and seamless transition for the Win95 user. This "ease of use" issue, while not an issue in many platform or major configuration upgrades, is indeed a factor here as the target users are for the most part novice level users (some despite the fact that they have been using computers for years). Any training required must be in text format (hard copy or PDF format), as no time has or will be allocated to hands-on training as of this writing.

The accepted practice when configuring a Win2k client is to allow only those rights and privileges necessary for a user to complete his or her daily tasks. Because only Company approved software is allowed to be added to a client machine (see Appendix 1), this would indicate that the average user be allowed only User level access, with supervisors and managers (perhaps) being given Poweruser status and the subsequent rights to add or remove software (i.e.: limited permissions to modify the user environment).

While this was appropriate for the "in house" clients (desktop PC's, covered in more detail, below), mobile users presented a challenge. As stated by Johanna Ambrosio, some of the main considerations in designing a telecommuting (or mobile) infrastructure are "...simplicity, transparency and security..." . Due to the fact that the bulk of the notebook PC's were true mobile workstations being used by the sales force, and a variety of software products might need to be installed or removed on a regular basis, the decision was made to give mobile users local Administrator status. As a salesperson's permissions were severely limited on the network (for example, few were given access to the User volume on the file server and none had access to the application server), this was felt to be an acceptable tradeoff of security -vs.- ease of use -vs.- Help Desk call volume. In order to streamline the support process, an account was created on all machines with administrator equivalency which contained certain maintenance and administrative items. All users, as local administrator equivalents were given full NTFS permissions (i.e.: Full Control with

Creator-Owner permissions) over their created documents . Because most remote clients would rarely, if ever, be physically be connected to the network, the cached login setting was left at the default value of 10, allowing the remote user to log on to the client before authenticating to the network.

Desktop clients were setup somewhat differently. All in-house users were given Poweruser status, as the Help Desk personnel have easy physical access the client machines and could perform all administrative tasks at the deskside by utilizing the same administrator equivalent account created and used for the mobile clients, above. Permissions for the desktop users were set at "Modify"[]. In order to insure the ability to log in to the local machine in case of network outage or server maintenance, cached logins were also left at the default value of 10. With the desktop users access level set as Poweruser, it was necessary to install several programs (notably those requiring or creating an ODBC data source or connector) as administrator while logged in as the user, easily accomplished using the "Run as" function in setup properties.

AntiVirus Software

All clients, desktop or mobile require some sort of AntiVirus (A/V) protection . The A/V product in use on the Win95 clients (one of three variations of the Symantec's Norton AntiVirus) was deficient in that it only allowed for a one-year period of virus definition updates: additional update subscriptions would have to be purchased separately. This situation lead to many instances where virus definitions were well over a year old, an unacceptable security risk. In addition, the administration of approximately 350 additional update subscriptions would have placed an undue burden on both the Technical and Procurement staff.

Although not necessarily the most appropriate A/V platform for the Macintosh clients (due to the lack of centralized management features), a decision was made at the Corporate level to continue to utilize a Symantec Norton product software across the board. Independent evaluation both in the industry and by this author have shown that NAV is as good or better than it's competitors at protection from known virus/malware infectors (rule based or definition based protection), and above average in protection from unknown threats (heuristic analysis). The specific product chosen allows centralized A/V definition management (the ability to push A/V defs. from a central in house server, as opposed to a scheduled pull of the defs. from Symantec's FTP server(s)). Because the mobile clients are, by definition, not permanently attached to the network, NAV was installed in unmanaged mode, and the A/V defs. are to be pushed out using Mobile Automation 2000, a product which enables the distribution and installation of software fixes, patches updates and executables "behind the scenes" with little or no intervention on the users' part. Network attached clients were set up in managed mode, thereby taking advantage of the central management feature. NAV is set to examine all incoming mail and attachments; exposure to mail-attached malware is reduced by the use of an e-mail platform other than Microsoft's Exchange/Outlook pair (Lotus Notes).

Desktop Firewall and Remote Access

Desktop firewall and remote access will be addressed together for the purposes of this evaluation: prior to the current rollout, there was no security at the desktop except for the anti-virus software discussed above. Remote access was accomplished via dial-up to a nationwide ISP service with hundreds of local points of presence (POP). Although security warnings were used, there was no protection from "hackers", and no way to ensure the integrity of the client O/S or user data.

When planning the Win2K rollout, it was decided to implement a Virtual Private Network (VPN). The single stage login to the network (described above) was replaced by a two stage process: the first connection made is to a local POP, with a second discreet connection made via VPN through an outsourced carrier. This procedure has several advantages: it allows the use of multiple POP's, including high speed connections such as Cable Modem and/or xDSL service as well as standard dial up, it provides the (necessary) added security of a VPN, and it reduces the cost of dialup access by allowing the use of local ISP connections, thereby eliminating excess local or long distance charges.[]

When the VPN software was deployed, a desktop firewall was also deployed. Testing of BlackIce Defender, Zone Alarm (ver 2.6), Zone Alarm Pro (ver 2.6), and Symantec's Desktop Firewall showed all to be about equal in the level of protection offered. Zone Alarm was upgraded during the course of the evaluation,[viii] but the base version "broke" several administrative programs in use by the Help Desk, and so was eliminated from consideration. Cost considerations dictated the use of Symantec Desktop Firewall: site license pricing was half of its' competitors (there is, indeed, something to be said for site licenses...). A rule set was developed (see Appendix 2)and will be applied to the mobile PC's remotely (again via Mobil Automation). There is still some discussion as of this writing as to whether to enable firewall alerts: one group feels that alerts are needed, in the interest of minimizing the impact on our support personnel, while another feels that they should be "off" in the interests of transparency.

Miscellaneous

One other item of change during the rollout and implementation of the new computing platform was the replacement of Netscape Navigator with Microsoft's Internet Explorer. The major reason for the change was the lack of Challenge-Response capability in the Netscape product, necessary for proper function with/on out intranet site, but there is another benefit in that America Online Instant Messenger (AIM) is no longer available. The AIM service is HTTP based, and since our Corporate firewall is configured to allow HTTP traffic, a virus, trojan or worm coded into or piggybacked onto the HTTP source code would have no problem passing the firewall and gaining a foothold on the network. Instant messaging services are provided as a sub-set of functionality of Netopia's Timbuktu Pro, used mainly by the Help Desk as a remote control and observation tool. Also, as many of our users require the ability to respond via e-mail directly from a web page, and MS Outlook/Outlook Express are a notorious source of vulnerabilities, response to a "mail to:" command was set to use Lotus Notes (again, our default e-mail

program).

An issue not addressed during development of the new loadset was that of attachments in general. Although scanned for malware at the desktop, there have been numerous times where an unknown infector has gotten past the A/V software by way of an infected document. There have also been issues with inappropriate material being passed through the e-mail system. While banning attachments is indeed effective, such a draconian measure would hobble the current workflow in the organization under review, as many production and administrative documents are passed both internally and externally as attachments. While there are products (such as MimeSweeper) which will check attachments for appropriateness against a predefined or custom rule set, they have not been implemented as of this writing.

Conclusions

All the procedures implemented and suggested above go a long way towards insuring the security of the desktop and mobile computing platforms. The general consensus is that secure external access, centralized security policy management, basic firewall services and remote control are necessary to successfully safeguard today's computing environment[ix] There must be, however, a happy median between the locked down, concrete encased system powered off at the bottom of the ocean, and a wide open system serving only as an invitation to electronic compromise. While some environments lend themselves either by intent or necessity to a more controlled, more secure model, the environment under consideration tends to be more along the lines an open university type system. The implementation of policies which restrict the "ease of use" of production systems are frowned upon unless absolutely necessary (case in point - many of our users continue to employ their original Help Desk assigned passwords - indeed many do so at the advise of the Help Desk staff). All of the items discussed above represent an increase in security when compared to previously used models, while maintaining, with some exceptions (ie: using "Ctrl+Alt+Delete" to log-in to a workstation). The ease of use and transparency the end users have come to expect.

All the security features in the world will not, however, protect an organization large or small if the end users do not know what to do (or more importantly what NOT to do) to maintain the integrity of the O/S and their data [x]. There is an urgent and immediate need for training; the average end user needs to be educated concerning best computing practices. He or she needs to be made aware of the sometimes serious consequences of a lack of awareness of the implications of their (lack of) action(s) in many day to day and very real situations. Without their cooperation and partnership, little of what we in the security field can do will save our end users from themselves.

APPENDIX 1

Below is an excerpt from the Corporate Handbook:

> **Desktop Computer (PC) Security**
> *Appropriate Use*
> Employees are authorized to use <Company Name> desktop computing resources only for legitimate business purposes….. Multiple installations…Must be approved by your department director and LAN Administrator. No personal software may be used on <Company Name) workstations….

(Please note that originally there were 3 scanned pages of our Security policy here. They were deleted because it was not possible to submit this practical given the size of the resulting zipped archive. PDR)

APPENDIX 2

This a screen shot of part of the custom ruleset created for Symantec Desktop Firewall to allow some of our administrative applications to function. Shown here are the rules for part of the Norton AntiVirus package, one of the Lotus Notes functions, Timbuktu and our Extranet (VPN) client.