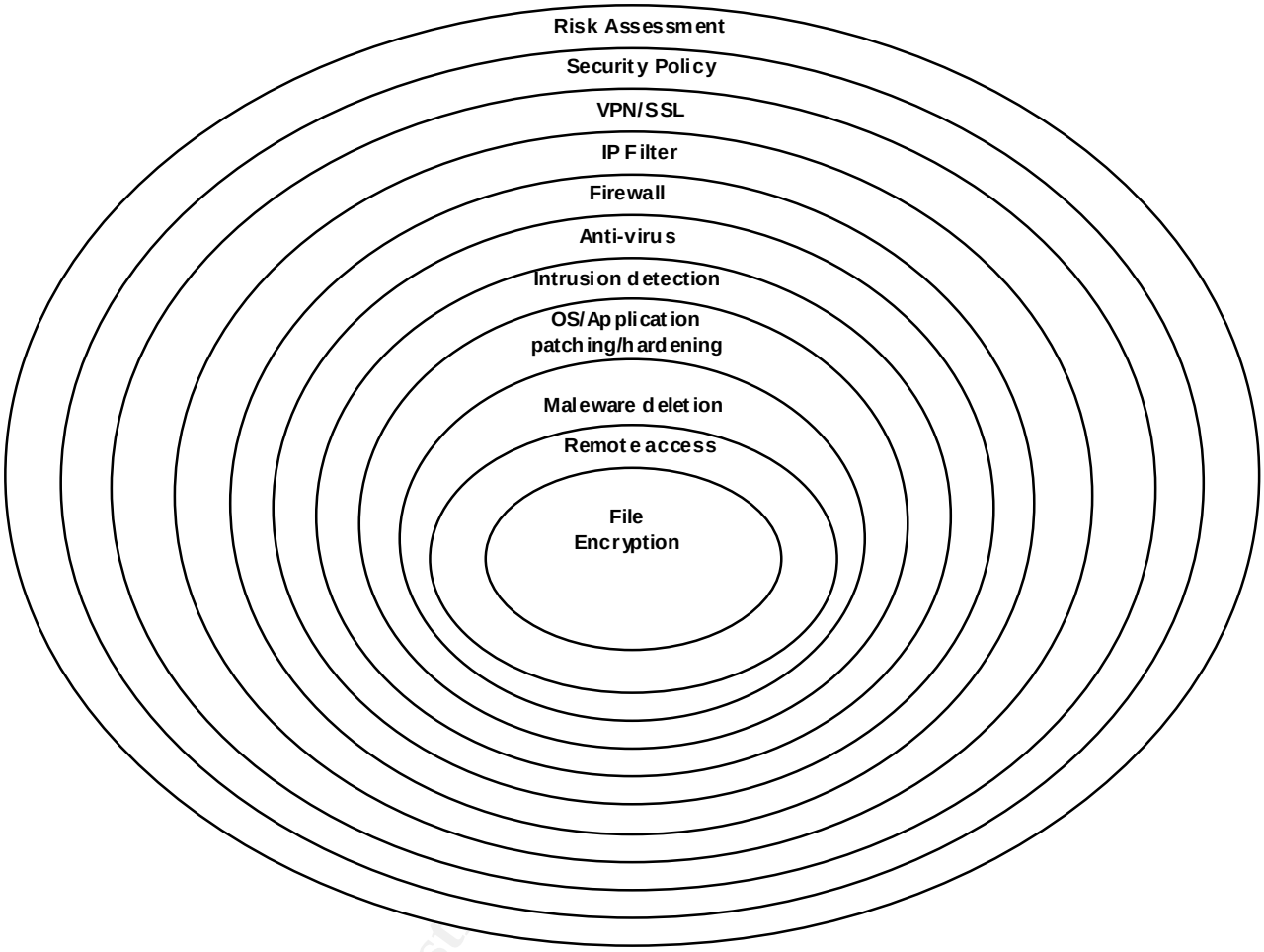
Global Information Assurance Certification Paper

Remote Workstation Security At a Post Secondary Educational Institution



LAYERED SECURITY FOR END POINT WORKSTATIONS

Written by Hugh Burley
Date: April 3, 2003

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b (amended August 29, 2002)

TABLE OF CONTENTS

SUMMARY

Post-secondary educational institutions face most of the security and business concerns of other organizations. Financials, client information, and other confidential business information all need protection from theft and malicious attack. Today's security environment requires that organizations exercise reasonable care not to cause foreseeable injury to others under common negligence law. Educational institutions can no longer argue they were unaware of the potential harm from DDoS attacks. Due diligence is essential to reduce the threat and limit corporate liability for damages.[1]

In the case of the Institution where I am employed, Tutors work entirely at a distance to support our students who also work at a distance. The key security issues surrounding Tutor access; are maintaining the integrity of student grades, securing the confidentially of personal information to prevent identity theft, maintaining the availability and integrity of other corporate data and ensuring that the Institution is protected from liability arising from any misuse of Tutor workstations.

Securing these "End Points" of the corporate network is a relatively new area. When these workstations were purchased in August 2001, senior management was opposed to any security measures being implemented. Even as recently as April 2002, Information Security magazine published an article that recommended only anti-virus software and a VPN for end point security.[2] Although these two components are an important part of the security picture, alone they do not present security in depth. Along with these components there should be a firewall, some form of non-viral malware detection, intrusion detection, perhaps desktop file encryption, patch management for the operating system and other applications. Overlaying these components there should an assessment of risks and vulnerabilities, and a clear security policy.

The ideal product would be centrally administered and incorporate all of the tools and functions required for securing remote workstations. This would greatly reduce the cost and complexity of managing end point security. Unfortunately, at this time no such single tool exists. In this paper the various security components required and some of the products currently available are discussed and consideration is given to how they might function together.

THE PROBLEM

In October 2002, a breach of security on two tutor workstations raised concerns about security on all 100+ tutor workstations.[3] It was discovered that tutor workstations did not use password controls on the Windows 2000 Professional administrative account, and Windows security updates had not been applied since the initial installation in August 2001. These two factors alone would allow an external agent to easily gain control of the tutor workstations from the Internet and thereby gain access to the tutor's local files, and the institutions corporate

[1] Wright, Benjamin J.D. The Legal Risks of Computer Pests and Hacker Tools September 25, 2001 URL:http://www.pestpatrol.com/Whitepapers/LiabilityofPests.asp

[2] Briney, p. 50-51

[3] DameWare is a remote control utility. http://www.dameware.com/

applications. It would also give external agents the ability attack other external systems from these workstations.

Remedial actions were taken to ensure the use of passwords on the tutors Windows 2000 profile. A second administrative profile controlled by IT was created and a malware deletion tool[4] was used to clean the machines. A remote administration tool[5] was installed on each workstation to allow access by IT staff. This was the start of the implementation and support of a full defense-in-depth security suite.

Through this process, it was confirmed that many additional breaches of basic security had occurred. Using this information, a project plan was presented to management for improving the level of ongoing security. This project plan was accepted and funded in March of 2003. The plan provides the framework for the discussion of the issues and components for remote workstation security discussed in this paper. This is therefore a very pragmatic discussion that will weigh an ideal security scenario against costs and the institution's ability to support the solution. The focus of this paper is not to provide definitive answers to all of the issues surrounding remote desktop security or review all of the seventy or so potential security products. The intention is to explore some of the possible alternatives and issues to the extent possible without completing the detailed testing and selection processes that will be required before implementation.

SECURITY COMPONENTS

There are a number of key security components that must be implemented to provide layered security for end point workstations. Although recommendations vary, the following components need consideration; personal firewalls, anti-virus software, VPNs, SSL, authentication, OS and application patching and hardening, intrusion detection, malware detection and deletion, file encryption, and remote access to allow rapid intervention. But all of these components,

> should exhibit several key characteristics. These products must be:
>
> - On-guard full time, 24 x 7 x 365;
> - Transparent to the end user, yet render the end point secure at all times;
> - Highly automated, requiring minimal IT intervention;
> - Flexible enough to represent a wide variety of security policies;
> - Integrated with other related security measures; and
> - Able to strike a healthy balance between security and performance/usability.[6]

Before beginning to select from the nearly overwhelming array of end point security products, risks, threats and vulnerabilities need assessment and security policies need to be developed to address these vulnerabilities.

[4] Spybot http://security.kolla.de/
[5] Radmin http://www.radmin.com/default.html
[6] Phifer, p. 8-9

Risks, Threats and Vulnerabilities

The primary risks driving the need for upgraded security on these workstations are; the possible use of the Tutor Portal for fraudulent manipulation of student marks; the possibility of identity theft using confidential student and tutor information; the threat to the institutions systems from malicious damage or availability attacks; and the possible misuse of these workstations to launch attacks on other internal and external systems.

Primary threat vectors

The tutor workstations connect to the Internet by a combination of ADSL, Cable Modem and dial-up. Those that connect with high speed, either DSL or Cable, are more vulnerable from outside attack since they tend to stay connected to the Internet for extended periods of time and hold their IP addresses longer than those connecting with dial-up. This might allow a hacker to return to the same IP address many times. High-speed access also makes these workstations more vulnerable to a quick attack or file theft, which is less likely to be noticed. Workstations connected with dial-up present the risk of access from War Dialers if the modems are configured to auto-answer. Although the risk of outsider attack is lower for dial-up connected workstations, it remains significant. "The average time it takes "door knob rattlers" to discover a newly-connected system is well under an hour."[7]

For tutors who have connected their institutional workstation to a hub, insider attack from the local network presents a potential problem. This will provide access from workstations that may be used by other family members. These other machines may have inadequate security features and may be allowed to share network drives with the Tutor workstation. It is also possible that some non family member might gain access to these machines and then mount an attack on the tutor workstation.

Since the Tutor workstations reside in the Tutors homes, they are not physically secured from access by other family members or guests and present a high risk of theft or unauthorized access.

All of these factors, increase the probability of attack by malicious code. The greatest security risk however has been the actions of the Tutors. They have installed Instant Messaging, peer-to-peer file sharing applications such as Kazza, downloaded and installed code from a wide variety of locations and run third party email that is not scanned for viruses.

The lack of adherence to standard security practice has left these machines with a wide range of vulnerabilities. No standard IP filter or firewall has been provided; Anti-Virus up-date schedules have not been set; Operating system patches have not been applied; until recently no passwords had been placed on the Windows 2000 profiles; No log files have been kept; and no Security Policy has been defined.

[7] Phifer, p. 4

Not surprisingly, these machines have been found to harbour a significant amount of malicious code and back doors. Undoubtedly, userids and passwords to corporate services have been exposed on some of these machines and they have been used to mount attacks on other systems.

Security Policy

The lack of a clear and comprehensive Security Policy and the lack of adherence to the security guidelines which were in existence, resulted in the installation of these insecure systems. For example, the institution has a clearly written guideline surrounding the use of passwords for desktop systems and servers within corporate headquarters. Managers outside of IT over ruled this guideline at the time these workstations were installed. Other examples of the lack of adherence to IT Security Guidelines are that no schedule was set for anti-virus updates and Tutors have been given administrative accounts on their workstations. This resulted in many machines never receiving new definition files for the anti-virus software and a great many applications being installed.

A lack of policy surrounding OS updates, firewalls, incident handling, web security and the use of personal systems resulted in a computing environment with numerous vulnerabilities. It was not until two systems were found to have DameWare[8] installed, that the extent of the threats to these machines began to be examined. With so many vulnerabilities it was predictable to find that these additional security breaches had occurred.

The positive result of this examination was that it presented management at the Institution with clear evidence of the need for a written security policy and has resulted in approval for striking a Security Policy Committee.

The Security Policy Committee will be responsible for addressing the following issues and defining the following policies in relation to Tutor Workstations:

- Internet access policy
- Firewall policy
- Anti-Virus policy
- Use of VPN and SSL
- Authentication
- Operating System standards
  - Configuration
  - OS hardening details
  - Patching schedule
- Non-viral malware detection
- Desktop intrusion detection
- Desktop file encryption
- Password policy
- Appropriate use policy

[8] DameWare is a remote control utility. http://www.dameware.com/

- Connecting to a private network
- Use of a non-institutional workstation
- Incident handling policy
- Security policy review process

Many of these policies will be formulated based on the processes and procedures that are developed in the course of attempting to secure the Tutor workstations.

Anti Virus

Although Tutors are an academically talented group, on average they have low technical ability. "Even good users circumvent security measures. User education helps, but central enforcement is the only reliable method"; (to ensure that security policy is enforced).[9]

The cost of having Tutors manage their own workstations is also prohibitive as they are paid on the basis of the time they expend working for the Institution. On the Information Technology side the Institution has limited funding for staff to support these workstations. Remote support for Tutor workstations has proven to take two to three times the resources of supporting local workstations. Beyond building the case for adequate staffing, the answer to this dilemma is to automate the processes, centralize management and standardize both policy and technology. Several vendors are now attempting to provide a clear path for achieving these objectives.

The Institution standardized on Symantec™ Norton Anti-Virus software for Windows some time ago and installed this application on all the Tutor workstations. This extremely important utility has been limited in its effectiveness on the Tutor workstations by the lack of an update policy or central management. Many of the workstations have never updated the anti-virus definition files and many more have only updated on an irregular basis.

This process needs to be automated to ensure that updates occur on a regular basis. Workstations that are connected to the Internet with high-speed access should update daily and those connected by dial-up should update at least once per week.

On the head office LAN, a central server logs incidents and allows IT staff to quickly respond to problems and manages anti-virus updates. The Symantec System Center console included with purchase of Norton AntiVirus Corporate Edition Version 7.x and Symantec AntiVirus Solution presents a good method of managing desktops within a Microsoft Windows domain but a rather less impressive method for remote machines.

> Provides easy access to sometimes-connected desktops and laptops, allowing you to keep these hard-to-reach systems up-to-date. Using unique, advanced technology from Symantec, you can send virus definitions as compact email attachments to remote clients. End users download the files and install the updates themselves, keeping them in sync with the rest of the organization-easily and inexpensively.[10]

[9] Phifer, p. 8
[10] http://www.whitehatinc.com/symantec/antivirus/systemcenter.html

This does not present the level of automation that easily allows for the management of over 100 remote workstations. This scenario would require that Tutors adhere to a strict update policy and receive payment for managing their workstations or have IT staff intervene on a regular basis. I talked to Symantec's technical support staff and received the following as an alternative new process.

> In Symantec AntiVirus Corporate Edition 8.x, Roaming Clients access the SAVRoam service to connect to the server on port 1056. RTVScan makes a request to Winsock for port 2967 for IP. This value can be configured by using the following registry key:
>
> HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDesk\VirusProtect6\CurrentVersion\AgentIPPort
>
> If the request for the static port fails, then RTVScan will use a dynamic port. This port will be assigned by Winsock on that server and can be different each time that you request a port.[11]

This would allow IT to distribute updates and track the status of definition files on the remote machines without having to log into each machine and without intervention by the Tutors. A second anti-virus server in a screened corporate segment or DMZ is required with the appropriate ports open. The dynamic IP addresses on the Tutor workstations would result in each workstation having a new multiple listing whenever their IP is changed.

Symantec Enterprise Security Manager™ 5.5 claims to:

> Checks policy compliance and vulnerabilities on servers, workstations, applications, and databases with over 1,500 assessments
> Performs assessments fast and efficiently, with minimal disruption to day-to-day business operations
> Manages enterprise-wide policy compliance from a central console, with easy and secure updating over the Internet via LiveUpdate™
> Provides integrity checks as well as comprehensive reports and compliance management recommendations[12]

[11] From Symantec technical support
[12] http://www.whitehatinc.com/symantec/esm/esm.html

Unfortunately this product is aligned for server management and is cost prohibitive for remote desktops. The Institution is therefore left with three choices. Symantec LiveUpdate™ could be managed on each of the workstations individually. A second instance of the corporate Symantec AntiVirus server could be created with the Tutors defined as a logical group or IT could manually intervene to ensure that emailed updates are applied. Alternatively, another vendor or distribution process could be selected such as Sygate, ZoneLabs, or F-Secure. ZoneLabs is actually capable of managing the Symantec anti-virus update process.[13]

Another type of product that might address the issue is desktop patch management systems such as St. Bernards UpdateEXPERT™.

> Use UpdateEXPERT's exclusive optional client agent to manage machines that are locked down or isolated (e.g., DMZ). You don't need the client agent for any other machines unless you need the best bandwidth management.[14]

Although not specifically designed for anti-virus updates UpdateEXPERT™ is designed to deliver software updates which could include the anti-virus definition files among other software applications. It is unlikely that the cost of this product could be justified for delivering anti-virus definition files only and it is not clear how the anti-virus definition updates are integrated into this product.

Alternatively the Institution could consider purchasing static IP addresses from the ISP(s) to alleviate the problem of tracking remote users. This, as with the other alternatives above, would incur additional costs but might be more cost effective than implementing additional servers or products.

Operating System Patching and Hardening

Since the initial installation of tutor workstations in August 2001 over 200 patches have been issued for Windows 2000 Professional. The majority of these patches have been security patches. Applying Windows patches is not currently mandated by the institution and would require many hundreds of hours of tutor time at $--/hour to complete. On workstations that attach to the Internet via dialup, applying patches through the Microsoft Update site is not feasible. It would require several hours simply to download the 22MB, SP3 for example.

Tutor workstations that are connected with high-speed DSL or Cable service are able to take advantage of the MS Updates for patching. For these workstations OS patching could be managed remotely by IT once the major patches have been applied. Dialup attached workstations will require access to OS patches from CDs supplied by IT. This process will require significant ongoing effort and cost for tutor time, shipping, and IT management. To alleviate this problem, it was recommended that all tutors be supplied with high-speed Internet access where it is available.

---

[13] DeMaria, Mike. Defense Starts Here. Network Computing, February 20, 2003 URL: http://www.networkcomputing.com/shared/printArticle.jhtml?article=/1403/1403f3full.html&pub=nwc

[14] URL: http://www.updateexpert.com

In order to bring tutor workstations up to the latest OS patch levels, it was recommended that machines be returned to the institution where a new image can be loaded on the machines. These images will incorporate all patches and new software.

Ongoing management of OS and application patching should include the use of an automated tool such as UpdateEXPERT™, Microsoft SUS™, Shavlink™ or PatchLink™. The use of any of these products does not resolve the problem of moving large patch files over slow dial-up connections. It will still be necessary to provide high-speed access to the Internet to allow patching to be performed efficiently or for those workstations that cannot get high-speed access; CDs will still have to be issued.[15]

Since these workstations are scheduled to be returned to the Institution for patching, an opportunity for hardening the OS is also presented. One of the first problems to be resolved with these workstations is the removal of administrator privileges for Tutors. They will need the ability to backup files on the system but should not be able to install applications.

Current policy states that all systems should display a Logon Banner warning against misuse of the Institutions systems. These system will have a standard logon banner installed using the Local Security Policy Setting. They will also have lock-outs set for multiple failed login attempts. Strong password rules will be set to ensure that passwords are updated every 90 days and are not repeated. A password protected screen saver will also be applied. In addition the list of installed accessories will be reviewed to determine which accessories might be uninstalled and all network protocols will be disabled other than TCP/IP. IIS will also be disabled.

There are a number of tools that can be used to for hardening a Windows 2000 Professional workstation. Good examples are the Symantec Enterprise Security Manager™ OS Hardening Policies for Windows Platforms[16] and the Center for Internet Security Benchmarks and Scoring Tool for Windows 2000 and Windows NT.[17] These tools can save a great deal of time and effort in identifying baseline hardening requirements.

IP Filtering and Firewalls

A primary component of any secure environment is the ability to block unauthorized access. This is partly achieved through the use of IP filtering and firewalls that can block most ports and remote access attempts. The key question that IT considered in choosing a solution was, "Can tutors be expected to manage their own firewall effectively?" In the opinion of IT staff, tutors in general will not have the level of understanding of firewall issues to manage their own firewall. The most likely scenario is that tutors would open up any port that is requested thereby eliminating all security value. A centrally managed remote firewall system such as Zone Alarms Integrity product or Symantec Enterprise Client Security would allow IT to set

[15] High-speed ADSL funding was approved on April 11, 2003

[16] URL: http://securityresponse.symantec.com/avcenter/security/Content/windows.os.hardening.policies.html (April 22, 2003)

[17] URL: http://www.cisecurity.org/federalcisusers/fed_bench_win2000.html (April 22, 2003)

firewall rules and push those rules out to all workstations. Sygate and F-Secure will also be evaluated.

Zone Labs Integrity Server™ claims to be able to integrate into a variety of authentication processes to ensure that when the Integrity Agent attempts to connect to corporate assets the firewall security rules are forced on them. Zone Labs does not include anti-virus software but supports Symantec as a third party product. Symantec Client Security using the LiveUpdate™ client on the remote system is configured to function with other Symantec products. Many of Symantec's security offerings are the result of recent acquisitions and it is not clear, without extensive testing, how well they have been integrated. Unfortunately the Symantec firewall received very poor ratings in Network Computing's most recent comparison,[18] and does not include centralized reporting of firewall events.

Sygate by comparison claims that they are able to manage a wide variety of third party software in an integrated manner. "The Sygate Enforcers network gateway device communicates with the Sygate Management Server to obtain enforcement policy and authentication information. When Sygate Security Agent connects to the enterprise, Sygate Enforcers initiate a challenge response session that determines the authenticity of the agent, the status of the firewall, intrusion prevention, anti-virus, other security applications, and the adherence of policy, signatures, and virus definitions to corporate policy."[19] Sygate also received the best overall rating from Network Computing.

All of these products are application layer firewalls. Methods of populating and configuring permitted applications vary by product. Some offer a scanning tool that's uploaded to the server; others let a clean client system learn and report back the available applications. All the four products mentioned here compute MD5 hashes, or fingerprints, to protect the network from modified or overwritten applications. All of these products with the exception of Symantec also offer component control; that is, they extend control capabilities to .DLL and other library files with MD5 hashes.[20] This is a significant weakness for Symantec as it allows Trojans to modify .DLL files, however Symantec's product includes anti-virus software that can detect and purge Trojans in a reactive manner.

IT has a good understanding of the application and port requirements for access to the Institutions systems. Currently Tutors connect to the Tutor port with SSL on HTTP port 443, access email using a proprietary client which includes encryption on TCP port 510 or 3004, and access course delivery servers on HTTP port 80 and TCP ports 4445 and 4568 and UDP port 4567 for whiteboard and chat. It has been recommended that the course delivery server access by changed to SSL. The corporate firewall blocks access to all other ports. Many outgoing requests on HTTP port 80 such as ICQ and Instant Messaging are also blocked. A similar configuration is being considered for Tutor workstations.

[18] DeMaria, p. 5
[19] Sygate Secure Enterprise: Making Open Networks Trustworthy. Sygate Technologies, Inc. 2002 URL: http://www.sygate.com/solutions/datasheets/Sygate_Secure_Enterprise_Datasheet.pdf
[20] DeMaria, p. 2

Exceptions to these rules will require a clear business case, an analysis and explanation of risk, and a reasonable level of assurance that security will not be compromised. Application discovery will be important in the initial stages of this implementation, it is therefore important that installation occur on clean systems. The Institutions Security Committee will make these decisions.

The firewall should ideally have an IP packet filtering router in front of it to add an additional layer of security. Obviously this would not apply to workstations connecting by dial-up. Some members of IT have argued that IP packet filtering should be used instead of a personal application-level or stateful inspection firewall. This argument is based on the perception that cost for support of a hardware router with a simple filtering table will be lower than managing a personal firewall with a more elaborate configuration file. This however does not take into account the ability to centrally manage remote firewall rules or the lack of ability to centrally manage routers. It also assumes that the level of security between the two options is equivalent.

Packet filtering routers would require a fairly elaborate rule set to meet equivalent security levels offered by any of the Personal Firewalls. Managing the routers ACL's would be beyond the comprehension of Tutors and most IT staff members. If a change were required, the routers ACL would need to be modified on each router by accessing the console. Console access would need to be secured in order to keep external agents from acquiring access for their own ends.

Given that these changes would most likely be infrequent and that console access security could be maintained, the question still remains whether a packet filtering router provides an equivalent level of security to an Application-level Personal Firewall. In my opinion, although an elaborate packet filter could provide a good level of security, as new applications are introduced and the associated threats change, a centrally managed Application-level Personal Firewall will provide the ability to respond to changes more quickly and provide a higher level of security.

Cost constraints at the Institution make it unlikely that both a packet filtering router and a personal firewall can be funded for these workstations. Although both solutions would be ideal, if a choice must be made, the relative complexity of configuring and managing routers makes it likely that they will be dropped in favour of a centrally managed personal firewall.

Some DSL/Cable routers, D-Link for example, are now packaged with a copy of a personal firewall, Symantec in this case. At this time there does not appear to be a remote workstation solution that combines a router and firewall in a single inexpensive and centrally managed appliance. Current firewall appliances remain too costly to use in a remote workstation environment. Managing 100+ independent routers and firewalls would require additional staffing for the Institutions IT department. Given the current economic environment, it is extremely unlikely that additional staffing can be obtained.

The choice between a stateful-inspection or application layer (proxy) firewall has already been made at the corporate level. The arguments used to make this decision are quite similar to

making a selection for personal firewalls. Although stateful-inspection may give higher performance, this is not a major consideration on a workstation. Generally stateful-inspection firewalls are acknowledged to provide a lower level of security than application-level firewalls and are considered easier to configure improperly. It also appears that at this time there is no centrally controlled, stateful-inspection personal firewall being marketed.

In the final selection process there are several key features that will be used to distinguish between personal firewall vendors. As mentioned previously they will need to incorporate central management in order to accommodate staffing limitations at the Institution. A list of additional features that will be compared is presented below.

Block port scanners
Configurability
Group Level Restrictions
Policy protection, so users can't make changes
Logging options – does it present a central log for all remote systems?
Definable event filters
Automatic policy and software updates
Integration with VPNs and anti-virus programs
Alarm triggers
Leakiness level – as tested by Leak Test
Responsiveness of vendor
Stability of vendor
Recommendations for secure policies and procedures
OS configuration error identification and fix recommendations
Range of threats addressed
Application and protocol level controls
Cost
Ease of use
Frequency of intervention required

Intrusion Detection

Host based intrusion detection is "very expensive in terms of time and resources".[21] Commercial host based intrusion detection products for Windows also have low market penetration. It is for these reasons that centrally managed Anti-Virus and personal firewalls will provide the main intrusion detection information. Logging anti-virus and firewall information to a central location may allow IT staff to identify an attempted attack and adjust settings and configurations to quickly respond.

On top of these centralized logs, Windows 2000 Security event logging will be enabled. This will allow IT staff to review events on the Tutor workstations if a security breach is suspected to have occurred. IT staff may also choose to ask the Tutors to use Netstat and or Fport in the event that there is reasonable suspicion of some problem. The Institution however will be

[21] GIAC Security Essentials – Host-Based Intrusion Detection – page 3 - 43

faced with a high cost if Tutors are asked to use these utilities on a regular basis and are then billed back for the Tutors time.

Unfortunately using a utility such as Tripwire or Windiff on an ongoing basis without some central management console would provide more information than could be managed with current staffing levels. The time to inspect independent logs on 100+ workstations would require an additional FTE for just one of these utilities. These may however be used on an ad hock basis in the event that a security problem arises which cannot be easily identified otherwise.

Malware Detection and Deletion

After having set clear security guidelines, installed Anti-Virus and firewall packages, updated OS/application patches and having turned on the Windows 2000 security logging, IT is still left with the possibility that some unknown threat might allow unauthorized access or install malicious code. Even more likely, a Tutor or one of their family members might install an application on the workstation that could damage the system or compromise security in some unpredictable fashion.

Faronics Technologies Deepfreeze™ would allow IT to ensure that no permanent change could be made to the workstation without authorization from IT. If a tutor installed software or was somehow infected with an unknown virus, a reboot of the machine would delete any changes to the configuration. Tutor files are stored in a specified location that is not affected by the reboot. This would significantly reduce the number of problems introduced to the workstation by tutors but does not prohibit tutors from testing new applications. Deepfreeze would also contribute to identifying an intrusion by logging changes that occurred.

The most significant problem to be overcome when using this utility is to allow necessary Anti-Virus and firewall updates without having to manually intervene on each workstation. This can be achieved by "thawing" the locations where AV definition and firewall configuration files are located. This of course exposes these important files to the very problem that Deepfreeze is attempting to resolve. If there were any Windows registry entries affected by these changes they would be over written on the next reboot. In fact Symantec updates the Windows registry with the last check in date. In a centrally administered scenario the central server would report the last check in date incorrectly. This would not necessarily break the system but would limit the value of these log files. An alternative is to have Deepfreeze turned off at scheduled times to allow the AV and firewall updates. Running these updates on a time-based schedule for Tutor workstations using dial-up would be problematic as they most likely will not be connected to the Internet. At any rate, managing multiple applications to run on a single schedule is bound to be problematic.

Another alternative is that scripting could possibly be used on the central anti-virus and personal firewall server to shut down Deepfreeze during the update process and then restart it on completion. Faronics technical support, were unaware of any organization that is currently using Deepfreeze this way.

Although a useful additional layer of defense, extensive testing will be required to determine if Faronics Technologies Deepfreeze can be used effectively in conjunction with Anti-Virus and Personal Firewall applications. Other products that will be investigated include PestPatrol.

PestPatrol Corporate Edition can be deployed centrally and claims to detect fifty thousand types of pests in memory, on local drives and on network shares, which are not detected by many other remote end point security products. PestPatrol is integrated with Check Point VPN-1. If a pest is detected the SecureClient shuts down any active connection and forwards a failure message containing the name and location of the pest by email. IT would then need to intervene to allow the affected Tutor to regain access to the tutor portal. Although this product may provide some additional layer of security it would once again require significant additional time from IT and might present frustration for Tutors.

Desktop File Encryption

Even with all of the possible security tools employed there will always be some hacker who will gain access to one or more of these workstations either through persistence or because of some error on the part of IT or one of the Tutors. In this event a final layer of security could be applied in the form of file encryption. Entrust, Imecom and SafeIT, all provide desktop file encryption products that could be employed. However, this is not a high-level R & D environment where Tutor files would provide the type of information that a professional hacker would pursue. Any hacker who did go through the trouble of gaining access to these machines would be sorely disappointed by finding at best undergraduate papers in the various fields of Arts an Science.

VPN vs. SSL

Once the Tutor workstations have been secured there still remains the security of the Tutor Portal, where student marks are entered. Currently access to this portal requires 128 bit SSL encryption. SSL provides a high level of session encryption providing message privacy and integrity, but the authentication process remains a userid and password and anyone can hit the login prompt for this server from the Internet.

This Windows 2000 server currently hosts both the Tutor and Student Portals. The first recommendation made was that these portal services be separated and placed on two physically separate servers. This would allow the Tutor Portal to be screen from general Internet access.

The second recommendation for securing the Tutor Portal was to install a VPN to restrict access to this portal to tutors using a VPN client. Ideally these sessions should be mediated by hardware tokens, but funds for SecureID or CryptoCard tokens were not approved. Even without hardware tokens the VPN improves secure access to this server by restricting access to workstations using the VPN client, (software token), and preventing access to all others. A second value of the VPN is that it could provide authentication for Tutor access to central servers which manage the various components of remote end point security.

Three products have been selected for comparison and evaluation; Nortel - Contivity Secure IP Services Gateway, Cisco – VPN 3000 Concentrator Series and Symantec Enterprise Firewall & VPN. The institution currently maintains Nortel local area network technology and a Symantec Enterprise Firewall. Cisco is partnered with Zone Labs to provide authentication for the Integrity Personal Firewall Server. Sygate has partnered with Nortel and Symantec is attempted to provide all the components itself. There is a substantial evaluation process that must be completed before selecting the VPN product. This selection process is beyond the scope of this paper.

Alternatively the Institution could select some other central authentication method for Tutor access. These could include a Windows Domain or LDAP server or an SSL-Based authentication solution such as Rainbow Technologies iKey/iGate. The Rainbow Technologies solution provides a two-factor authentication solution but claims to be simpler and cheaper to implement and maintain than a VPN. In this scenario encryption would continue to be provided by SSL but the Tutor portal would only be accessible directly by authentication through the selected process. This would add only limited additional security value by presenting an additional userid and password. Tutors would also find the additional login frustrating.

The introduction of a VPN, combined with enhanced workstation security and separation of the Portal server, provides better security for student marks, and Tutor and student information, from an external integrity or confidentiality attack.

Review of internal policy and procedure is also required to ensure the internal, head office; attack vector does not present gaps. There is little point in locking the backdoor if the front door is left wide open. The striking of a formal Security Committee will allow the Institution to review internal processes and determine the full extent of the security improvements that may be required within the corporate office.

Remote Access to Workstations

Key to reducing support time for remote workstations is the ability of IT staff to gain access so that they can see what is happening on the workstation and provide quick intervention to identify and resolve problems. Even being able to show a Tutor some simple application tip can save large amounts of support staff time. In the event of a suspected security incident, it is also important to be able to check local log files and run utilities that will generally not be familiar to Tutors.

It was important in identifying a remote control tool to weigh the value of remote control against the risk of opening an additional security hole. The IT department selected Radmin as the remote control tool of choice. This product provides triple DES encryption of the remote control session on a none-standard port and can be assigned a strong password or it can be tied to the Windows Domain authentication process. Opening any additional port on these workstations is cause for concern but a Personal Firewall scan blocker will mitigate this.

EXCEPTIONS AND PROBLEMS

As with any environment there will be exceptions to standard configurations, policies and procedures. Some Tutors will require specialized applications within their area of expertise; others are located in remote areas that cannot currently be connected to high-speed Internet services.

One of the most significant exceptions affecting Tutor workstation security is that some Tutors use they're own personal system or a system provided by another institution. Maintaining security standards on these systems will be difficult to say the least. One simple but expensive solution would be to mandate that all Tutors use only the Institutions workstations. This would entail the purchase of 60 additional systems. Alternatively an attempt can be made to ensure that these systems meet the minimum-security standards of the Institution. A clear and concise Remote Access Security Policy will be required to achieve compliance.

Introducing new applications such as Personal Firewalls and new central administration processes for these applications will create an additional workload for an already stretched IT department. Given current economic conditions within the local post secondary system, it is very difficult to obtain funding for additional staff. However, filling the full time role of Security Analyst is becoming recognized as common practice within the IT community at large. There is hope that this role can be justified and filled for the next fiscal year. In the interim, management of the new central systems and support of remote workstations will need to be absorbed by several staff members. The Security Committee will coordinate these staff members, and some of them will fill seats on the committee.

There is a great deal of hands on testing required to determine how the various components would work individually and together. Ideally one vendor would provide all of the components with a single central management console. At this time no such solution exists although Symantec and others appears to be moving in that direction at least with personal firewall and anti-virus products. Over the next two years, IT will be watching these developments closely.

CONCLUSION

Remote workstations present IT with one of the most difficult array of security problems in any organization. The wide acceptance of high-speed, always on, Internet access and portal technologies that allow access to mission critical information, have made the resolution of this problem extremely urgent. Security vendors have responded with a wide variety of discreet products and have begun to address various parts of the problem, but at this time there is little collaboration even within single vendors to provide coherent management of the whole solution.

Recently vendors such as Symantec, Sygate, F-Secure, and ZoneLabs have begun to address portions of the problem and undoubtedly will do much more to provide fully integrated packages in the next two years. It is too early to determine if these companies will succeed in developing security suites, where companies such as Network Associates and Secure Computing previously failed. While the various security vendors develop these integrated

packages however, IT is still left with an urgent and immediate problem that requires the use of several independent products and processes.

In this paper, risk, threats and vulnerabilities for remote workstations have been examined within the framework of the primary threat vectors and security policy issues have been examined. The current types of security components available for remote workstations have been identified and briefly examined and some of the issues surrounding the use and selection of these components within a post secondary educational institution have been discussed. There is a great deal more work required to identify the details of how these components can work cost effectively together. Detailed policies and procedures still need to be defined to manage Tutor workstations that are owned and managed by the Institution and those that are not. This discussion also included some assessment of the impact on IT department staff that must implement and support these solutions. It is hoped that in the near future, integrated remote workstation security solutions will greatly reduce the complexity and cost associated with these processes. In the mean time the Institution will need to allocate significant funds for additional staff and an array of security components.

References

Avolio, Fred. "Practical Patching." Information Security – March 2003: 46

Briney, Andy. "Internet Security: A Mosaic of Solutions." Information Security April 2002: 48-51

Broday, Jon. Sygate's Personal Firewall Now Combined with Nortel Network Contivity VPN for Advanced Endpoint Security. Sygate Technologies, Inc. August 22, 2002 URL: http://www.sygate.com/news/nortel_spfse_rls.htm (April 22, 2003)

Burley, Hugh. Tutor Workstation and Tutor Portal Security Upgrades. Information Technology Project Scope Document, Open Learning Agency. February 21, 2003

Computer Viruses – from an Annoyance to a Serious Threat. F-Secure Corporation – White paper, September 2001 URL: http://www.f-secure.com/products/white-papers/virus.pdf (April 22, 2003)

Cooper, Russ . "Hardening Windows." Information Security January 2003: 44

Dahahy, Jack. "Down With IDS." Information Security February 2003: 88

Dalton, Curtis E. & Kannengeisser, William. "Instant Headache – The Rapidly Expanding Use of Instant Messaging is Introducing New Security Challenges to Enterprise Networks." . Information Security August 2002: 32-41

Demaria, Michael J. "Buyer's Guide. Desktop Firewalls. The latest breed provides application controls and prohibits policy tinkering." Network Computing September 30, 2002:

DeMaria, Mike. Defense Starts Here. Network Computing, February 20, 2003 URL: http://www.networkcomputing.com/shared/printArticle.jhtml?article=/1403/1403f3full.html&pub=nwc (April 22, 2003)

New Threats, New Solutions: Enterprise Endpoint Security. Zone Labs, Inc. 2002 URL: http://www.zonelabs.com/store/content/company/corpsales/whitepapers.jsp (April 22, 2003)

Phifer, Lisa. Cost-Effective Remote End Point Protection – Against trojans, spyware and other pests. PestPatrol – Technical White Paper. September 1, 2002 URL: http://www.pestpatrol.com/Whitepapers/RemoteProtection0902.asp (April 22, 2003)

Richmond, Robert. Personal Firewall Comparison. November 4, 2000 URL:http://www.sysopt.com/reviews/firewall/ (April 22, 2003)

Saita, Anne. John THOMSPSON. "Symantec's CEO breaks business and cultural barriers in his drive to build a security superpower." Information Security February 2003: 64-68

Security Risks in Telecommuting. F-Secure Corporation – White Paper, April 2000 URL: http://www.f-secure.com/products/white-papers/telecom_risks.pdf (April 22, 2003)

Sevilla, Robert. and Faulkner, Don. To VPN or not to VPN – What Remote Access Solution is Right For You? A comparison of leading remote access solutions. , 2002 Rainbow Technologies, Inc – 11/07/2002 URL: http://www.rainbow.com/Library/8/ToVPNorNottoVPN_whitepaper-Nov20-02b.pdf (April 22, 2003)

Sygate Secure Enterprise: Making Open Networks Trustworthy. Sygate Technologies, Inc. 2002 URL: http://www.sygate.com/solutions/datasheets/Sygate_Secure_Enterprise_Datasheet.pdf (April 22, 2003)

Symantec Client Security. Symantec Corporation. July 2002 URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=154&EID=0 (April 22, 2003)

Taylor, John. "Security For The Virtual Enterprise." Information Security – March 2003: 92

Taylor, Laura. Firewall Shopping 101. Small Business Computing. February 21, 2002 URL: http://www.smallbusinesscomputing.com/buyersguide/article.php/978221 (April 22, 2003)

The Behaviours and Tools of Today's Hackers. Symantec Corporation. Article ID: 1398 September 24, 2002 URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=1398&PID=10112566&EID=0 (April 22, 2003)

The Need for Endpoint Security. The Hurwitz Group white paper written for: Zone Labs, Inc. February 2002 URL: http://www.zonelabs.com/store/content/company/corpsales/whitepapers.jsp (April 22, 2003)

Thorsheim, Per. Comparing Firewall Technologies. Information Security Handbook 4th Edition. 2002 by CRC Press LLC, Auerbach Publications. Editors: Harold F. Tipton, Micki Krause. Chapter 11

Walsh, Lawrence M. "Trustworthy Yet? Microsoft is making significant strides to clean up its security mess, but Trustworthy Computing still has a long way to go." Information Security February 2003: 30-45

Windows 2000 Security. V2.7a January 10, 2002, Security Essentials – The SANS Institute

Wright, Benjamin J.D. The Legal Risks of Computer Pests and Hacker Tools September 25, 2001 URL:http://www.pestpatrol.com/Whitepapers/LiabilityofPests.asp (April 22, 2003)

Zone Labs integrity – Datasheet. Zone Labs, Inc. 2002 URL: http://download.zonelabs.com/bin/media/pdf/integrity_datasheet.pdf (April 22, 2003)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event