Global Information Assurance Certification Paper

Securing IT Shops

Kenta Watai
October 1, 2004

Abstract

IT Contractors that deal with numerous small businesses have distinctively different security obstacles compared to large organizations with their own IT department. For instance, overhead (such as numerous passwords to memorize) introduces weaknesses in the security infrastructure when dealing with each small business as a separate entity. This paper identifies these unique risks that IT consultants face and discusses how to minimize these threats.

Introduction

The author in this document views the security for IT Shops as an analogy to the following phrase

> The shoemaker's children go barefoot

An IT Shop and its employers service large number of small businesses on a very tight budget. When tasks that require additional equipment, software, and other resources are required to test and develop a system, small to medium businesses do not have the capacity or flexibility to meet these demands. More often than not, the IT Tech and the shop provide their own resources, which can result in a deterioration of the IT shop's security.

Deterioration of IT Shop security can happen because although security may be a prime concern, as time passes, it becomes more and more lenient. During the continuous cycle of testing an application and loosening security, it is not always common for security to be restored to its original settings. Open ports, test accounts, simple passwords, and trust between two systems can become the weakest links in the IT infrastructure if they are not properly controlled. This control can be obtained through the extra efforts of monitoring, auditing, and the use of specialized equipment.

One may question if these additional efforts can be justified. The total value of the data and physical equipment in the network may not validate additional efforts in securing it. However, the client's infrastructure relies indirectly on the integrity of the IT Shop's security. A simple example would be a technician's laptop becoming the carrier agent for a virus or worm that is connected to the client network. Because of the IT shops security problem, the virus or worm could spread even if the client site is equipped with antivirus protection and an external firewall.

In the case of the above, the client trusted the IT Shop's security infrastructure. The spreading of the the viruses could have been prevented if the extra measures were taken on the laptop. The IT Shop can become liable for not taking due diligence with privileges they were provided when performing their work.

This document identifies the following topics unique to IT shops and consultants and discusses methods to mitigate these threats:

Untrustworthy systems in an IT Shop
Untrustworthy client networks and systems
Username / passwords
Virtual Private Networks

Intended Audience

This document is intended for SANS Institute, their GSEC examiners, and IT contractors that serve more than one organization.

Untrustworthy client systems in an IT shop

Client computers are brought into the IT Shop on a regular basis when additional servicing is required. IT shops use specialized hardware and software for troubleshooting that the client cannot afford on its own.

However, IT shops may need to connect client systems to a network to perform one of the following:

Download patches
Download tools for troubleshooting
Test network connectivity

By connecting these client systems to the shop's local network, the client system can become a Trojan horse. It may start spreading viruses and worms, or make contact with an external source, such as a botnet awaiting further instructions. They may even start probing the local network for weaknesses. For example, *The Register* reported the discovery of a network of over 10,000 PCs. These systems were infected by worms such as MyDoom and Bagle, awaiting instructions.

To prevent the above, the system must be placed in an isolated or quarantined network. A quarantined network would need the following features:

- An independent network for each client system. This prevents each system from infecting others.
- Only certain network protocols should be allowed to exit the quarantine network. These could include:
    - HTTP, port 80 (required to test internet connectivity and download tools)
    - FTP, port 20 and 21 (may be required to download tools)

- SSL, port 443 (required to download patches from Microsoft)
- POP3, port 110 (may be required to test email clients)
- IMAP, port 143 (may be required to test email clients)

(All other traffic should be dropped and logged. Ideally, the traffic should be monitored by a transparent proxy server).

Note: SMTP should be blocked in case the client system is infected by a virus that is spreading through SMTP or acting as a spammer. Unfortunately, this will prevent the client from testing outgoing mail. The IT technician will need to punch holes in the firewall to specific IP addresses if e-mail testing is needed.

A simple and cost effective implementation of the above can be created using a Linux operating system acting as a packet based firewall. A transparent proxy server can be loaded as well, such as Squid Web Proxy Cache, available from www.squid-cache.org. Alan Jones provides a sample implementation of a basic firewall in his paper "Netfilter and IPTables – Structural Examination" using IPTables in SUSE.

Note that IPTables are the basic building blocks for building a firewall. It is easy to misconfigure a firewall due to the numerous options. Shorewall, developed by Thomas M. Eastep at www.shorewall.net, provides an abstraction of IPTables. It allows one to develop the firewall based on established firewall policies, without bothering about details such as IP spoofing and invalid packet formats.

Untrustworthy client networks and systems

When an IT Technician services a large number of clients, it is possible that the technician may use the equipment of one of its clients to service another client. To better illustrate, consider a technician on site for client X. The technician then receives an emergency call from client Y, requiring immediate attention. The emergency can be resolved remotely using Terminal services. Luckily, any Windows XP system can log on to a Terminal server using the built-in application "Remote desktop".

Client Y will most likely feel uncomfortable, as it may be against their security policy, allowing an administrator to enter their username and password on equipment that is neither owned by client Y, nor certified by client Y. The possibility of a key logger in the computer that is not under the control of client Y can be considered too dangerous, especially when such a powerful account (in this case the administrative account) is used.

Therefore, logging onto client Y's network using client X's equipment is unacceptable. In conclusion, using client X's equipment for any transaction other

than for client X's interest should be prohibited. If a technician needs to log on to client Y's network, he should be allocated a laptop that meets the security requirements of client Y.

Let us now consider the necessary security precautions for a laptop that is used by a technician. David Friedlander in his article, *Managing and Securing mobile devices*, discusses possible procedures in securing a mobile device.

Among Friedlander's points, the following may in particular strongly apply to IT contractors:

- Antivirus
  - A technician will come in contact with various forms of data in the client's environment. This may include emails, floppies and server shares. It is entirely possible the client site does not have a fully functional antivirus with the latest definitions. The antivirus on the laptop becomes the only protection from a user with infected media (Friedlander).
- Password policy enforced
  - Attempts to tamper with the laptop by guessing the password can be prevented with a strong password policy. Given how the laptop may contain sensitive client information, a good password policy is crucial (Friedlander).
- Encryption
  - Bootable CD's can bypass the operating system's security (Friedlander). A strong encryption scheme, such as Encrypted file systems in Windows XP, or PGP, ensures that it is computationally infeasible to break the encryption (Shinder 1)
- Client firewalls
  - Devices that are connected to a network should be protected against worms, viruses, and direct attacks. Windows XP provides a built-in firewall called *Internet Connection firewall*, which performs basic packet filtering (Friedlander).
- Remote device kills
  - In the unlikely event the laptop is stolen, upon connecting to the internet the laptop can be instructed to call back home for instructions. A self-termination command can even be sent; this ensures the data on the laptop is destroyed (Friedlander).

In addition, any communication between the laptop and a client or IT Shop must be encrypted. This applies to protocols such as HTTP, FTP, POP3, and SMTP.

Similar steps should be taken to PDAs, Black Berries, and other mobile devices.

Please note that the client must agree in writing beforehand if remote support is required through equipment that the client does not certify. Because an IT Shop

must serve many clients, the final policy that is applied to the laptop must satisfy all the clients. In some cases, it may not be an option to even use this laptop for other purposes other than for the one client. An extreme example would be a classified system where a physical separation, known as an air gap, is required between two networks with different security classifications. This would imply that the system cannot be connected to any other network except for a network with the same security designation.

Username/passwords

For small to medium sized businesses, usernames and passwords are the primary defense against unauthorized access to a corporation's resource. This applies to administrative passwords as well. SANS Institute has identified username password authentication in a Microsoft Environment to be one of the top ten problems in computer security. A strong password policy that requires the password to be longer than a certain number of characters and to include special characters is recommended, especially for administrative passwords.

Standard users have a hard time keeping up with this policy. They find ways to circumvent these policies, by writing them down, or by using passwords that should not accepted by the password manager, but are. Ironically, IT shop technicians are no exception, even if they had implemented the policy. Because they are responsible for large numbers of passwords that must be changed every few months, it becomes impossible to store them all in memory, unless one finds ways to circumvent the policy. This is summarized in the following paragraph by Hugh Ranalli,

'The situation is even worse for system administrators, information security officers or IT consultants. People in these positions not only have to deal with many more systems, but typically choose strong (e.g. hard to remember) passwords, and select different ones for each system (Ranalli 1)

In this section, numerous methods are presented, from the simplest and often more risky, to the complicated but safe techniques.

For maximum ease, one could set all system passwords for all the clients to the same value. However, if the password is discovered, cracked, or shared, the user that obtained the password now has access to all the clients that the IT Shop services. Alternatively if the client requests the password for their own systems for their own records, they may unknowingly have access to other clients that the IT Shop serves. Setting all the client systems with the same password is not an option.

This issue can be resolved by making the passwords easy to remember by basing it on the client. For example, if a site specializes in law, then a password

could be forged that is related to law, with a few letters converted to special characters, such as ‘a’ to @ and ‘e’ to 3.

However, as the number of sites that the technician is responsible for grows, the passwords become increasingly simple. A basic algorithm that generates a password might be used. For example, the password may be composed of the client’s name with all the ‘a’ and ‘e’ converted to ‘@’ and ‘3’ respectively. If one discovers the password, he or she may be able to determine the algorithm used to generate the password. With this information, they may be able to deduce other client passwords as well.

Further, because the IT Shop must keep track of the passwords, often by memory, they are not overly complex. The resulting password tends to be one word with only one or two special characters and no longer than 6 letters.

The problem can be countered by storing the passwords. However, if the media that records the password is compromised, the IT Shop can be considered liable. Gaining written permission from the client to record the password is recommended. The client may have a password policy that forbids recording passwords, unless the media and method of storage is approved.

Hugh T. Ranalli in his paper “Options for Secure Personal Password Management” discusses the pros and cons of password storage. For those that feel uneasy with password storage, Ranalli points out the following

‘… as IT professionals, we recognize that security is not about attaining some mythical state of perfection but about risk assessment and mitigation’ (3).

To ensure the password or collection of passwords in a file or database is not compromised, Ranalli points out several criterias when choosing a password manager:

- Strength Encryption (6)
- Overall security (7)
- Configuration (8)

Of course, standard measures should be taken on the server that is hosting the passwords. These include, but are not limited to the following

- Physical Security
- Monitoring of logs for suspicious activity
- Firewall
- Intrusion detection system, and file integrity checker
- Proper ACL
- Auditing of activity

However, as the number of technicians in the IT Shop grows, password management among the technicians becomes a dilemma, unless it is centrally managed. Further, as technicians decide to the leave the IT Shop, all sites that the technician had access to must be changed. Often changing the password is cumbersome as it may need approval from the client, and must be recorded by all technicians. This makes it difficult to frequently change the administrative password.

The issues stated above can be resolved by assigning each technician their own administrative user account. When the technician leaves, one only needs to disable the user account. Unfortunately, this is not possible for devices (such as routers) that only have one administrative account. With remote access technologies (such as VPN, Citrix, and Terminal Server) readily available for small to medium sized businesses, ensuring proper password management becomes extremely important.

RSA key fobs can also solve many of the problems stated above, and even improve security. However, the overhead of implementing and maintaining a RSA server with key fobs are often over the client's IT budget. Ironically, the combined budget of all the clients may be more than sufficient to supply all the technicians and the client staff with RSA key fobs.

Virtual Private Networks

Virtual Private Network's (VPN) functionality can be separated into two tasks. The first creates the illusion that two networks are directly connected to each other, hence the term Virtual. The second encrypts the traffic. This ensures the content of the traffic is confidential, hence the term Private (Tipton 150.) Virtual Private networks (VPN) are becoming more common due to the maturity of the technology and its availability. A VPN server can be built cheaply with Opensource software such as FreeSwan for IPSEC, OpenVPN for TSL and Poptop for PPTP on a Linux Operating system.

From an IT Shop's point of view, VPNs could be one of the greatest inventions for remote administration. VPN allows one to connect to the organization's network from anywhere in the world and provide remote support. Coupled with Terminal Services or Citrix, total network administration is possible except for physical operations.

From a security standpoint, the following two functionalities can be added:

- The first functionality bypasses the physical security of an organization. Any user on the internet with proper authentication can access the organization's main frame with out even entering the building.

- The second functionality is bidirectional traffic. If a user can connect to a device on the network, then devices on the network can connect to the user.

These imply that if a technician were to connect from client X's network to client Y's network to perform remote administration, a technician would be connecting client X and client Y's network. Although routing makes direct communication between the client Y's and client X's network difficult, the technician's system can become the medium for communication.

For example, consider a malicious program on client Y's network searching and probing for weaknesses in the network. When the technician VPNs into the network, the malicious program may discover the technician has not properly patched up the operating system. The malicious program infects the technician's laptop and then starts scanning client Y's network and client X's network. Coincidentally, the technician (on client X's network) authenticates using administrative privileges to the domain. The malicious program piggy-backs onto the authentication and starts infecting administrative shares across the network, such as C$ or admin$ on each workstation. Before you know it, the malicious program could be creating havoc everywhere in client X's network.

Although the above situation requires many conditions to be true, and is preventable by techniques such as antivirus products, IDS, and OS patching, the focus should be placed on the technician that connected the two networks. Should the technician be allowed to VPN from one network to another or should this be prohibited due to the security risks? The final decision is up to the client but steps can be taken to minimize risk.

However, Michael Stines describes in his paper "Remote Access VPN – Security Concerns and Policy Enforcement" the difficulties in maintaining integrity on the client side. From the IT Shop's perspective, the client site can be considered the VPN server. Michael Stines recommends securing the client (in this case the VPN server) by providing company hardware, up-to-date patches, antivirus, and firewalls that comply with corporate policies. However the IT Shop cannot enforce its own policies on these VPN servers. Therefore, the VPN server cannot be trusted and the IT Shop must take precautionary measures.

These precautionary measures are similar to the steps taken to secure a laptop.

Patch the operating system
Install a firewall
    The firewall rules should prohibit any connections made to the laptop. In Microsoft's Internet Connection firewall, rules can be made for each connection, including VPNs.
Install an Antivirus

In addition, the following steps can be taken on the VPN server's side. These steps, which incorporate firewall policies, would benefit all VPN users, not just the technician.

> Restrict traffic from the VPN client only to services that the user requires. For example if the user requires a Remote desktop connection to their workstation, the firewall policy should restrict traffic to port 3389 and IP address ranges that match the workstation address scope.
>
> Restrict traffic from the network to the VPN client only to services that the client requires. There are usually only a few exceptions to this, such as print jobs to the VPN client's office.

Conclusion

Unlike an IT Department that serves one company, an IT Shop must maintain the interest of all their clients. As stated, this involves:

- Developing a quarantine network when servicing client systems
- Providing technicians with dedicated hardware for servicing, accessing and storing confidential information.
- Hardening any mobile devices, such as laptops and PDAs
- Having proper username password management
- Enable protection, such as firewalls between any connections among clients and the IT shop

Unless all the clients trust one another, the IT Shop must consider all their clients untrustworthy. Procedures, hardware and software that are backed up by a security policy are required to maintain the trust that the client places on the IT Shop.

Without these measures, if the IT shop lowers their security posture, it lowers the security posture for all their clients. If the IT shop stores sensitive information on their server, or data is transferred from the shop to the client on a regular basis, the IT shop can become weakest link in the client's security infrastructure. If the security infrastructure is breached due to the lack of security, the IT shop can be liable and incur both a loss of finances and reputation. .

Literature citied

Eastep, Thomas M. Shoreline Firewall 10 July 2004. 27 Sept 2004. <
http://www.shorewall.net/index.htm>

Jones, Alan. “Netfilter and IPTables: A Structural Examination.” The SANS Institute 2 May. 2004. 11 Sep. 2004 <http://www.sans.org/rr/papers/index.php?id=1392>

Friedlander, David. “Managing and Securing Mobile Devices.” Forrester 14 Aug. 2004 12 Sept, 2004 <http://www.csoonline.com/analyst/report2794.html>

Leyden, John. “Telenor takes down 'massive' botnet.” The Register 9 Sept, 2004. 12 Sept, 2004 <http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/>

Ranalli, Hugh. “Options for Secure Personal Password management.” The SANS Institute 14 Dec. 2004. 11 Sep 2004. <http://www.sans.org/rr/papers/index.php?id=1287>

Shinder, Deb Where does EFS fit into your Security Plan 22 Jul, 2004. 27 Sept, 2004 <http://www.windowsecurity.com/articles/Where_Does_EFS_Fit_into_your_Security_Plan.html>

Tipton, Harold F, Micki Krause. Information Security Management Handbook, Volume 3, 4th Edition. Boca Raton: Auerbach Publications

“The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus.” SANS Institute 8 Oct, 2003 18 Sept 2004 <http://www.sans.org/top20/>

Pearson, Oskar. Squid A User’s Guide No date. 22 Sept, 2004 <http://squid-docs.sourceforge.net/latest/book-full.html>

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event