East Carolina University

A Layered Approach to Security

A Term Paper Submitted to Faculty Member

Tijjani Mohammed, PhD

For the Partial Fulfillment of the Course Requirements for

Communication Technology 6810

By

Kellen Barrett

A Layered Approach to Security

Kellen R. Barrett

Abstract

The author will discuss how creating a layered approach to Information Security reduced our company's threat risk. Over the past several years we have endured numerous attacks on our network and necessity has required us to continuously rethink are security strategies.

Experience has taught us that no one system is foolproof we've learned it is the layered approach to network security that provides the best coverage. Through the application of new technology and learned experiences based on actual virus attacks on our network, I will prove that the layered approach is the best one for a comprehensive security strategy.

Reviewing this will help many small to midsize company's assess their security strategies as they grow. They can learn from our mistakes and experiences. I believe the results conclusively show that adding additional layers of security significantly decreases the risk of virus attack and network penetration.

Introduction

I work for a mid size insurance company which has, for the past five years, been working on upgrading its information security. Over this time period we have been attacked by many viruses, but only, was able to penetrate through to the core network. However, many viruses are able to infect individual machines and segments of our company. It is nearly impossible to stop this from happening, because the end users do not, or will not follow security protocol and company procedures.

Traditionally companies have employed what I will call single dimension security systems which up until the early 1990's were sufficient. A single layer system is usually your basic Internet firewall, the purpose of which is as Marcus Ranum a firewall expert states "The purpose of an Internet firewall is to provide a single point of defense with controlled and audited services, both from within and without an organization's private network."www.securitystats.com

Now let's look at the layered approach that most companies are employing as a standard currently.

Firewall
Enterprise Level Security Software (Trend Micro, Symantec, Norton).
NAC (Network Admission Control) hardware/software
Email Security (Ironmail)
Active Directory
SSO Single Sign On
Policy Physical Security

Firewalls - Are layered in today's environment as well, you employ a hardware firewall with your router and also an application level firewall such as Windows Firewall.

Enterprise Level Security Software – An enterprise solution should protect a company at multiple levels, messaging, web, network, and endpoint. As the following two quotes from Trend Micro demonstrate "To ensure that spyware and viruses are identified and eliminated as quickly and efficiently as possible, organizations will benefit from multi-layered solutions that are deployed at various levels throughout the enterprise. Your NAC device and security software work together."
http://websecurity.trendmicro.com/pr/tm/en-us/enterprise/ws/document/evaluating_effective_enterprise_white_paper.pdf

NAC – "Secure your enterprise network by screening and remediating infected users before they access your network with Trend Micro Network Security solutions. Trend Micro's flagship network access control (NAC) appliance provides agent less protection that is easy and cost-effective to deploy and manage. Seamless NAC flow integration lowers IT administration and costs."
http://us.trendmicro.com/us/solutions/enterprise/securitysolutions/networksecurity/index.html

Email Security – We employ the Iron Mail messaging security system, described in the following quote. “Iron Mail protects enterprise email systems from inbound threats: spam, viruses; or hackers trying to take down or take over the e-mail system. Iron Mail protects enterprise email systems from outbound threats: regulatory compliance violations, corporate policy violations, or theft (“leakage”) of confidential information or intellectual property.” http://www.ciphertrust.com/products/ironmail/

Active Directory – This is part of your centralized procedures for controlling access to the network. By requiring certified credentials to gain access to the domain, you minimize the possibility of a disgruntled employee purposely opening up the company to attack, because their movements are tracked via the directory. They can also be given various levels of access so that only trusted employees and administrators can download content and executables.

Single Sign On (SSO) – There are many different types of applications that provide this service for companies. The application provides a one stop shop for end-users, they go through a sign up process whereby they enter all of their passwords into SSO and then the application remembers them and deploys them when needed. It will also change all of the passwords at predetermined intervals. Some employ fingerprint technology as well, so as long as your employees have their fingers with them, they will be able to gain access to the network.
http://www.imprivata.com/onesign_platform

Security Policy – Procedures are the first level of defense, it has become a defining part of a company’s corporate culture. From the moment you walk in the door, you are issued a badge, and an ID number. One of the easiest ways for a hacker to gain a foothold into your company is by having someone introduce something to your intranet via a flash drive or CD. By having security measures that control ingress and egress you dramatically cut down on this risk. Another way of monitoring your hardware through good procedural load organization is to set baselines for each load and department, and have your software monitor for changes to this static picture. In this way you can maintain your load integrity, which reduces trouble tickets and helps the engineers troubleshoot when there is a global issue, since all of the platforms are ostensibly the same.

Finally controlling access to the physical network, hardware closets, and data center through additional security doors and password entry privileges provides a final layer of physical protection for your core.

In April of 2002, we had a security vendor come in to evaluate are level of security at the time and show us any inconsistencies and or weaknesses we might have. Of course we thought that our network was fairly secure and that it would be a short presentation. Prior to coming in to see us they had already hacked one of our websites using what is now a fairly common virus attack type known as SQL injection. SQL injection is a dangerous threat to any site that is driven by a SQL database. It is very easy for a hacker to learn how to perpetrate this type of attack, there are how to websites readily available on the internet. So you ask what is SQL injection, quite simply it is using port 80 to send information/commands via the internet through to a unsecured database behind a webpage. Once you have ascertained that you can communicate with the database you can sometimes add login credentials to the database, giving yourself access to the

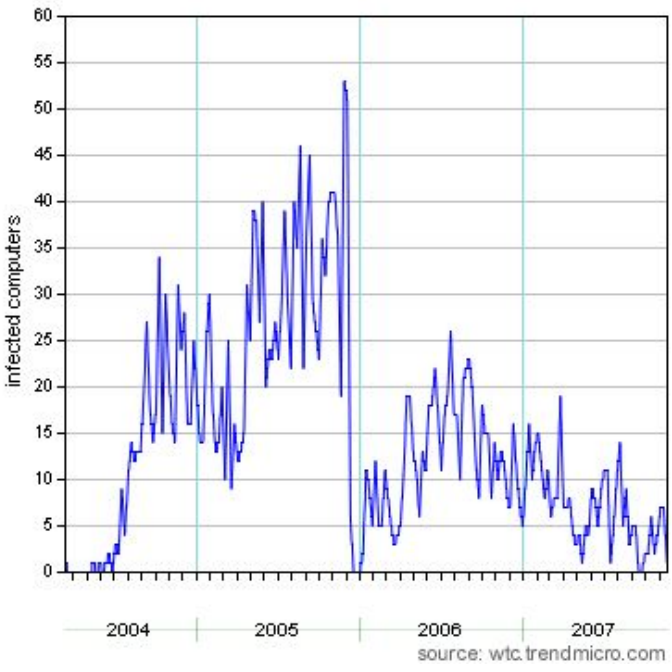
website. Some hackers just choose to add erroneous data to the database.

How do you protect yourself from SQL attacks, multiple layers of protection is the best solution, it is a microcosm of my theory. Here are several ways to avoid attack. You can see that they build on each other to help defend the core network.

1) Use original and difficult to guess table and column names
2) Use aliases
3) Set length limits on any form fields on your site and don't use real column names
4) Keep up to date on patches
5) Audit your code
6) Lockdown your server
   http://www2.giac.org/certifications/security/gsec.php

Okay so we have seen that our network is vulnerable and needs to be defended, let's analyze how the team from SPI Dynamics was able to accomplish their infiltration. They went after one of our websites and asked the backend database supporting it a series of true false questions. After analyzing only four rows of data they were able to extract a series of valid information by sending queries and enumerating one digit at a time. SQL injection can compromise any system that has a connection to the internet. One motivated hacker can compromise your database and use that information to find out your customer base or account numbers the applications of this data is infinite.
http://www.spidynamics.com/assets/documents/Blind_SQLInjection.pdf

Below is a graph of just one SQL injection infection and its life cycle over the past four years.



Computers infected since January 25, 2003	
North America	1,466
Asia	825
Europe	387
South America	52
Australia and New Zealand	43
Africa	2
(unknown)	5
Total	**2,780**

As companies have become more and more security conscious and setup their layers of security this particular virus has become less successful. This holds true for most viruses, their life cycle now is much shorter than in previous years. Security companies have dedicated resources to detect and immediately update their software to repel any new attacks before they can infect users on a large scale. It has become a necessity in the business world to have a top tier virus program as your base Security program.

My company, which I will refer to going forward as company X, had a dual layer system in place in the fall of 2004. We had seen some unusual traffic coming from a workstation; it was trying to access one of the IRC channels. One of our network engineers attempted to take control of this workstation, but was unable to gain access to any of the control systems. We use an application called Big Fix to monitor workstation loads and deploy software. We normally deploy software to a specified location, we realized that an executable had been deployed on the machine, in an erroneous location and we isolated and analyzed it we realized we had a nasty worm virus infection.

Company X realized after recovering from the worm virus attack that additional layers of protection were needed against external threats. We researched and implemented additional security software; I will prove statistically that the new software made a difference by reducing the number of virus hits that successfully penetrated our security. We will look at data before and after and analyze the results.

I have compiled a dataset of three years worth of data for company X including the time period when this virus attack occurred. There are two sets of data, one for viruses which are .exe executables, and one for spyware. The years covered in this dataset are 2003-2006. I have thrown out the outliers and created separate categories for them. The bin count for the datasets will be forty. Dataset A is for the .exe type of virus which was the worm which exploited a weakness in our password security to gain access to our network. Dataset B is for instances of spyware found and removed from company workstations. We have since implemented many different types of safeguards, but I have chosen to focus on two layers one was the installation of an additional virus and spyware prevention software known as Trend Micro, and the other was SSO password

software. On the following page is the dataset table 1.1 for company X. The table shows the number of reported attacks by individuals of executable virus type A and virus type B for each month from 2004 – 2006.

Table 1 Virus Distribution for the Past Three Years

Month	Virus A	A Outliers	Virus B	B Outliers	BIN
Jan-04	11		0		0
Feb-04	21		0		1
Mar-04	17		0		2
Apr-04	7		4		3
May-04	9		0	50	4
Jun-04	0	126	42		5
Jul-04	0	88	17		6
Aug-04	22		9		7
Sep-04	4		15		8
Oct-04	42		10		9
Nov-04	9		9		10
Dec-04	40		12		11
Jan-05	33		19		12
Feb-05	4		7		13
Mar-05	6		19		14
Apr-05	5		14		15
May-05	8		6		16
Jun-05	4		19		17
Jul-05	7		19		18
Aug-05	0	181	15		19
Sep-05	0	84	9		20
Oct-05	6		2		21
Nov-05	4		1		22
Dec-05	6		6		23
Jan-06	26		11		24
Feb-06	2		5		25
Mar-06	1		3		26
Apr-06	1		3		27
May-06	3		4		28
Jun-06	3		4		29
Jul-06	1		2		30
Aug-06	0		3		31
Sep-06	2		0		32
Oct-06	0		3		33
Nov-06	0		1		34

Dec-06	0		1		35
					36
					37

In the graphical depiction in Figure 1, it is easy to see that once the Trend Micro software was implemented in September of 2004, the number of virus's infections has trended down; the software had a statistically definitive affect on the number of infestations we experienced.

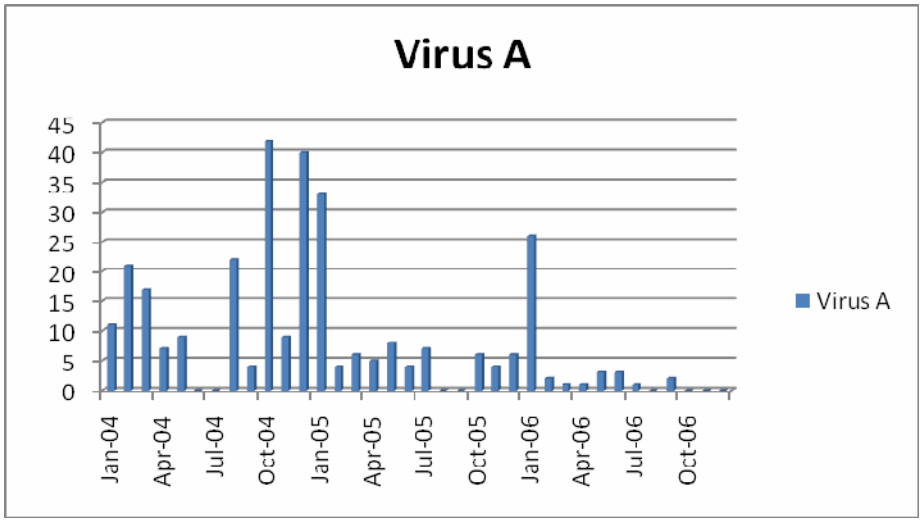


FIGURE 1

The SSO software was implemented in September of 2004, you can see in figure 2 how the number of viruses has trended down, the software had a statistically definitive affect on the number of Spyware instances we experienced.

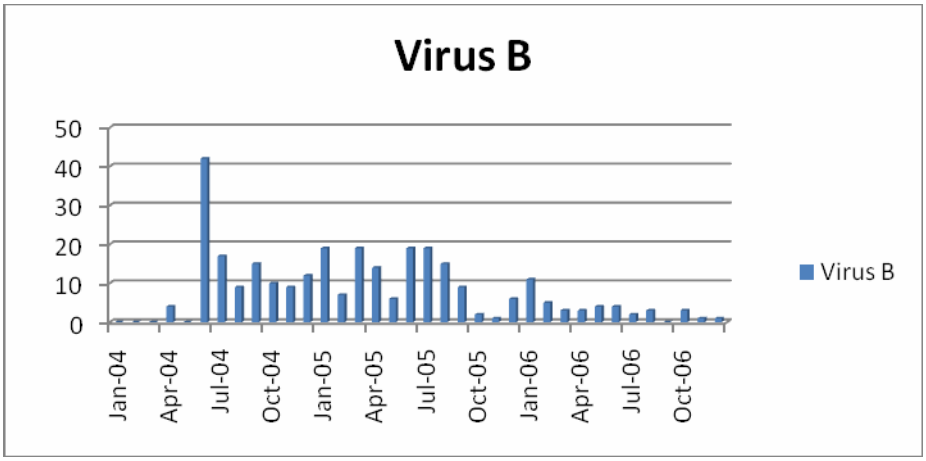


FIGURE 2

By analyzing these two sets of data both before and after we implemented Trend Micro and SSO,

I have statistically shown that as you increase your layers of security protection you significantly reduce your exposure to virus and spyware infection.

As companies have become more and more security conscious and setup their layers of security this particular virus has become less successful. This holds true for most viruses, their life cycle now however is much shorter than in previous years. Security companies have dedicated resources to detect and immediately update their software to repel new attacks before they can infect users on a larger scale. It has become a necessity in the business world to have a top tier virus program as your base Security program.

Conclusion

This analysis of two layers of our network security analysis has shown that the principle of layered or multilevel security systems lowers the number of security breaches a network suffers over time. Over the past five years as we have added each layer of additional security we have become more and more insulated from attacks. It would be interesting to statistically analyze each addition moving forward to see if my hypothesis holds true, or if there is a zero sum barrier that you cross where any additional precautions are unnecessary. Our virus software now defends us from most attacks, and those that do manage to get past the first layer face a maze of other security walls which few are able to surmount. Our network now is like an onion, each time you peel or strip off a piece there is another layer of protection below. Once you have these security pieces in place, it is at this point that you step back as a company evaluate your needs and look for any potential holes in your network security and continue to close them as need dictates and resources allow.

Works Cited

Modes of Attack, Defence, and Why It Matters. Ed. Stuart McDonald. 8 Apr. 2002. Global Information Assurance Certification. <http://www2.giac.org/certifications/security/gsec.php>.

Are Your Web Applications Safe. Ed. LABS SPI. 2007. <http://www.spidynamics.com/assets/documents/Blind_SQLInjection.pdf>.

A Multi-dimensional Approach to Internet Security. Ed. Fredrick M. Avolio. May 1998. ACM Neworker Magazine. <http://www.securitystats.com>.

Trend Micro NAC Description. 2007. Trend Micro. <http://us.trendmicro.com/us/products/enterprise/network-viruswall-enforcer/>.

Evaluating Effective Enterprise-class Anti-spyware. Ed. Trend Micro. May 2005. Trend Micro. <http://www.trendmicro.com>.

CipherTrust Ironmail - The Ideal Solution for Enterprise Level Companies. Ed. CipherTrust. 2006. CipherTrust. <http://www.ciphertrust.com/products/ironmail/>