Some Thoughts on Computer Defense for Small Business Owners

Ryan M. Ferris

www.rmfnetworksecurity.com

www.rmfnetworks.com

rferris “at” rmfnetworksecurity.com

Preface

There are numerous sites on the internet that offer “self-help” advice on cyber security. Some of my favorite organizations are Microsoft, Cisco, NSA, NIST, CERT, IC3, Carnegie-Mellon, and NCSA. All these organizations offer excellent software, templates, guides and publications on computer security of networks, servers, and clients. I am writing this guide targeted to small business owners, which is a varied group. This is a DIY document of some sort, but the general purpose is to give small business owners an idea of some of the complexity of securing their networks. Parts 2 – 5 represent bare minimum practices for “safe computing” in today's threat environment. They consist of policies and practices that can be implemented by most small business owners.

Today's cyber-threat environment has become increasingly dangerous and complex. Computational infrastructure is now critical to all local and global personal, commercial, governmental and regulatory activity. Yet despite millions of dollars in federal, private and university based research and development, the tragic fact is that entire networks, businesses, communities, nation-states and even countries suffer from damage inflicted from malware or "bad actors". Worse than this, resourced entities that are either state, criminal, or nationalist based (or any combination of the three) have found strong economic and geopolitical motives to sponsor the development of malware and malware based organizations. And these organizations are growing and diversifying in every part of the globe, most especially in impoverished second and third world nations who have turned their keyboards towards more affluent nations.

In this threat environment, small business owners need to have a strategy to secure their assets, their networks, and to make best efforts to bring their resources into some compliance with generally accepted standards of the security industry. The value of such efforts is clearly apparent to every business owner that has suffered data loss due to cyber-theft.

Contents

Basics

Threat Modeling

I feel like such an old-timer when I talk about threat modeling. It was only 14 years ago when I was rolling out the first NT 4.0 Beta to financial services corporation in downtown San Francisco. The word was you could telnet to port 135 to any Windows NT 4.0 build 1234 workstation, type in (10) alpha characters into the console and lock an NT driven CPU at 100%. So one day, I tried this in a lab. Sure enough, reboot required. Much has changed since then.

System software, operating systems and networks "get" the security message in ever stronger doses every year. Solaris, Linux, Apple and BSD based systems bring a level of competitiveness to the race for a secure OS that has helped build a stronger and more secure Microsoft Windows with every release. The world of security engineers, hackers, and state supported spycraft has caused all operating systems to integrate security into all development life cycles. Our government and government sponsored entities (NSA, DOD, NIST, CERT, MITRE, etc.) have gotten heavily involved in cyber-security and cyber-warfare prevention. Security is no longer an afterthought in almost all development life cycles of any product, policy, organization.

Threat Modeling is the art of wondering: "Who will attack me today and why?". Threat Modeling is done with great seriousness and studied attention in the world of computer security now, for very good reason. The interconnectedness of our commerce, governmental, social, research worlds is essentially worldwide. All world-wide decision making is network-centric, all politics are viral, all intelligence is simultaneous. This is a big switch in our world view that has happened very fast. The change in the growth of connectivity make data harder to protect and secrets harder to keep. These days, even a sophisticated assassination team can't seem to get its job done without the world knowing their faces.

So threat modeling is different today than it once was: Your American business can have its payroll stolen by East European hackers. Unbeknownst to you, organized crime can be using your home or work networks as a "Chickens" (bot members) to send anonymous spam by the thousands. Your unprotected server can be used as a C & C (Command and Control) server by Russian nationalists to send DDOS (Distributed Denial of Service) attacks to Lithuania. If you are a member of the DIB (Defense Industrial Base), your systems could be hiding APT (Advanced Persistent Threats): small binaries that lurk in your system undetected by AV (Anti-virus) cracking password hashes and silently sending military secrets and industrial patents to foreign countries. Or if you are an embassy in a foreign country, your system may be used as a surveillance device to remotely turn on your camera and microphone to eavesdrop on your confidences. How do we model threats when attacker

methodologies change so fast?

Use Host and Network Protection

Exterior firewalls are primary defense mechanisms. Running both host and network firewalls assures that many of the numerous attacks are rebuffed and don't gain traction inside your network. Choosing an appropriate hardware firewall is a significant security decision for any level of home or business user. I recommend spending as much as you can afford. Popular business grade router/firewalls are made by Netgear, Sonic Wall, Cisco, and others. They are worth spending some time in configuration, upgrade, maintenance and log analysis.

My hardware firewall routinely rejects hundreds of attacks per week. Many attacks are recognizable, others are targeted to unknown ports that confound analysis. There is no reason to have your network "ride bareback" against the internet. Put a hardware firewall between your network and your hosts. This however, does not mean that you should not protect your hosts with software firewalls available for all desktop/server platforms. Your host firewall determines your relationship to the internet *and* your private network. It functions as both a second line of defense and local policy enforcement. Iptables (Linux), PF (OpenBSD), Pfsense (FreeBSD), and Windows Firewall are native products available for the price of configuration management. Firewall integration and firewall-like application protection are often bundled with your anti-virus software. There may be conflicts between Windows Firewall and anti-virus software.

It should be remembered that software firewalls are the critical defense mechanism in foreign territory; e.g. all wireless networks - 3G, 4G, EVDO, VPN, 802.11a-n. A common exploit in public areas and hotels is the "*hostile hotspot*" with a friendly SSID (Service Set Identifier) . The "*hostile hotspot*" is designed to steal critical information as soon as you connect. This unfortunate reality begs for a remote user security policy; a process which can involve physical theft prevention, data loss prevention, encryption, VPNs (Virtual Private Networks) and user training.

Have a strong Anti-Virus Policy

There are many excellent, industry supported AV (Anti-Virus) vendors, most of them designed for Windows operating systems. This field of software has improved in performance, scope, and updates very recently in response to advanced threats. Comparative anti-virus analysis research is done on a number of sites, Stanford Research Institute's Cyber-TA and Malware Threat Center not the least prestigious among them. These sites will convince you that no AV software covers all threats. Indeed, the some of the most persistant malware incorporates "AV evasion" techniques to avoid detection. However, AV vendors of any worth frequently update

in response to new threats. This enables the user some chance of recovery and protection from "*zero-day*" attacks. Furthermore, some features may detect previously uncategorized (e.g. "new") malware. PC Tools "*Malware Detective Wizard*" will scan your hosts for suspected malware and create a report to help identify and detect new signatures and threats. In addition to AV software, you may want to run specialized utilities that detect and remove spyware, protect your browser from malware, examine your registry and startup folders, and enable you to isolate, audit, and kill rogue processes.

Audit your Networks and PCs

Significant auditing can be done by many users, not just network administrators. Auditing your logs in real time allows the user and administrator to understand computer behavior. If you are an administrator , you need an effective audit policy and framework to make your logging useful and reliable. Third party log collection software can help with this on all platforms, however there is nothing to prevent you from handcrafting firewall, application, system log collection and analysis on your entire network. This is a technical task beyond the scope of this document, but I will create an overview of the logging components:

(1) Intrusion Detection and Prevention Systems
(2) Network Management
(3) Automated Detection and Automated Forensics

Intrusion Detection and Prevention

Many security consulting services deploy Intrusion Detection/Prevention Systems that are either composed of proprietary or open source software. They may well be worth their asking price, especially since many of those service providers can offer consultation, data theft and prevention audits, network management/configuration and training for your firm. Even if you go "in-house" with your security services, you can use outside firms to audit and provide consultation and training on an as needed basis. If you do your own network security or lump network security and network management into one department, you will have to live with the learning curves, risks of infection and data loss. There is nothing wrong with this, provided you accept the risk and *prepare for loss*.

Network Management

Network Management is a critical and important part of network security. Often this point has been obscured by recent developments in network security software. A well managed and monitored network is the first step in assuring security and reliability. Network security is a subset of network management, however network management policies and procedures provide essential system security features such as updates, monitoring of hardware health, traffic flow, capacity monitoring, system alerts, and

file access. Operating system patches are now so critical in the "patch and respond" cycle of system security that Microsoft includes a Malicious Software Removal Tool with each monthly update. Physical management of wired and wireless access points across your network is also an important and critical function of network security often performed by network administrators. Recovery and Rebuilding from any security breach or data loss is another critical security function performed by the network management team. Network management and network security should be closely coordinated in any organization.

Automated Detection, Forensics, Analysis

New hardware and software now bring both automated detection and automated forensics to networks. On large networks in general this will enable faster and more targeted response to threats. Vendors include nCircle, Mandiant, Triumfant, Palantir. These sophisticated appliances and software will benefit businesses with some higher level of resources. The small business owner may not find such choices practical, however some appropriate level of security monitoring can be achieved by using customized toolsets, monitoring of firewalls, and through the use of publicly available tools like Botnet Hunter, MBSA, Powershell, Suricata or Snort. You can tailor your monitoring and reporting needs to the size and asset risk of your respective business. What is appropriate in determining your investment in network security is a thorough understanding of the risk of data loss, network compromise, commercial downtime. Most small businesses operate on thin margins; bankruptcy, business failure, and asset loss are all too often just part of game. However, even a cost-conscious small business can minimize security risk by deploying open source and freely available tool sets.

"Safe" Practices

"Safe" computer use is no joke. No business owner in their right mind would hire a fork lift operator without some level of training and/or drug screening and/or supervision. The risk of accident and destruction is just too great. So it is with computers. "Safe" computing includes training users in avoidance of "spear phishing", malware infected mail, malware infected websites, social engineering, etc. It also involves some level of policy enforcement for computing hours, password length and duration, file and network access, visitor policies, etc. Without policy documents and user training, it is impossible to expect the user to "do the right thing" in a computing environment so infested with malware that the FBI currently recommends home users bank on a computer separate from one on which they surf and mail. For small businesses, security policy documents need to be drawn up not only for user training, but for hiring, network administrators, and building facilities. However, the most basic procedures can be developed and followed by most small business:

(1) automated employee background checks

(2) printed (and signed) “safe” computing documents

(3) appropriate network and file access

(4) managed and audited user accounts

(5) locked computing and server facilities

(6) secure remote access

Note: If you do not have the budget to secure remote access and you do not need it for successful commerce, you probably should avoid traveling laptops and remote access. Physical data theft of traveling laptops has reached epic proportions of late. However, VPN enabled firewalls are reasonable in price now. Many small business will be able to afford remote terminal services for their select employees. Price your need for remote access with respect to the increasing network security risk.

Advanced

Parts 5 – 9 consist of research and network management oriented practices that will challenge non-professionals. These suggestions will strain the resources of smaller businesses, but should be put in place by nearly any mid-sized small business.

Pre-Deployment Testing

Most corporate business cannot afford large scale deployment failures. This means they spend significant resources to test, configure, integrate and construct pilot projects for any application or platform before they purchase or deploy it to the entire corporation. Occasionally, if you work for a niche software firm, Corporation X will ask for your test suite and/or test results before purchase. As a small business, you will not have the type of leverage or buying power to allow you such advantages. However, you may still be able to:

(1) afford a small test lab

(2) test trial versions of software

(3) employ consultants who are certified in specific platforms

(4) create back-up and back-out strategies

Some key questions to ask any consultant (or you) when planning major changes to your network or PC configuration:

- *"What is your experience with the reliability of this product?" "Have you done previous deployments of this product?"*
- *"How will this product integrate with my existing hardware and software? Will any hardware upgrades be required. Do any problematic software upgrades need to be applied?"*
- *"What is your deployment back-out plan?" The "back-out" plan assures that if the deployment goes wrong, your network or PCs can be returned to a "last known good state".*
- *"What is the risk of data loss during either the deployment or implementation of this product?"*

Prepare for Loss

Cyber-warfare and cyber-attacks can mean loss of data, uptime, information, identities, bank account data, among other other niceties. This is *not a question of if...* Identifying your risk and planning for loss are a critical part of any cyber-security strategy. To cover for loss, ask yourself "What if?" questions with regards to assets:

- *"What if those patent pending documents are stolen?"*
- *"What if a hacker or company employee gets my payroll data?"*
- *"What if my payroll account is cashed out by 'money mules' ?*
- *"What if my web-server is defaced?"*

- *"What if my network is used to attack high value targets?"*
- *"What if our company databases or e-mail server is breached?"*

Remember: *not if*, but when. Prevention and recovery strategies are just the most obvious answers. Good security depends on designing a business whose strength can survive the risk of data loss. This could mean range of strategies including:

(1) seeking patent protection early in the business cycle

(2) having adequate insurance to cover cyber-theft

(3) having strong payroll security procedures

(4) employing some form of real-time web-site auditing

(5) advising your employees to be careful with the content confidential e-mails

Security needs to be an integral part of your corporate or small business process in prevention, business strategy, and (if necessary) recovery. The FBI and the NW3C recently have more to say about preventing electronic payroll theft.

Develop Security Policies

Policy development and regular policy review and modification help assure business continuity. They give your business security needs structure that can be maintained and transferred independent of changes in personnel, management, business structure. Policy development, like all other areas of security, requires dedicated time and resources. There are some good arguments for soliciting policy from the bottom up as well as from the top down. Fortunately, there are lots of templates for policy development. The security industry is full of people who write and update documents based on standards: ISO, IEEE, NIST, CERT, CMMI, IAMM. In addition, many technical corporations like Microsoft, Cisco, and others have documentation for practices that apply security through pre-formatted templates. If you are a harried small business person, you may not have time to DIY your own network management or network security policy. But I recommend at least that you keep a detailed binder (in some secure location) of documents, licenses, serial numbers, and contact numbers.

Penetration and Network Vulnerability Testing

No network can be declared secured unless it is regularly tested for weaknesses. Many open source, free and third party products specialize in vulnerability testing. You can request penetration testing from a security consultant in your community. You can also purchase or download and leverage free/open source products include

(1) NMAP Security Scanner

(2) Microsoft's Baseline Security Advisor

(3) NSA SE Linux

(4) Foundstone's Free Tools

(5) The BackTrack-Linux distro

(6) Penetration Tester's Open Source Toolkit

(7) MetaSploit Toolkit

Syngress.com and Amazon.com sell many texts in penetration and security testing. Should a small business owner vulnerability test his own network? I would first recommend learning how to understand logging and auditing for all your platforms: your operating systems, your firewalls, your IDS/IPS. I would then master tool sets for administration of your operating systems. After that point, I would apply security templates to your operating systems as needed. After this point, penetration testing will make more sense. If you choose to hire a penetration/vulnerability consultant, he will have many questions and some recommendations both before and after the tests are performed. Typically, penetration engineers are hired by businesses when:

(1) hardening of an organization's security has been completed or

(2) a vulnerability has resulted in significant loss or

(3) the FBI has alerted your organization to the vulnerabilities in your computer networks because their resources were used in cyber-crime.

Penetration testing in advance of items (2) and (3) above, is recommended.

Conclusion

The problem of computer security will continue to increase in intensity in the coming years. Geo-political conflict, an increasing wealth divide between North and South in an increasingly networked world, and increasingly sophisticated threats will challenge the most well prepared specialists to secure your network. The passage of time has only made the following Unix administrator's adage become more true: "*There are two kinds of computer users: those who have lost data and those who will.*" Which part of that data loss cycle is your destiny?

Some Links

FBI NW3C Internet Crime Complaint Center

CERT Home Network Security

An Introduction to Computer Security: The NIST Handbook

Windows Vista Security Guide

Microsoft's Security Risk Management Guide

Stanford Research Institute's Malware Threat Center