Global Information Assurance Certification Paper

Towards Building Computer Security Into Product Development

Anthony W. Steere, Jr
March 14, 2004

GIAC Security Essentials Certification (GSEC)
Practical Assignment: Version 1.4b – Option 1

Table of Contents

Abstract

This document explores the need for computer vendors to define a Computer Security Product Development policy. Time-to-market focus and a lack of demand from end users have created corporate cultures where security is not a priority. This paper examines several macro influences on vendors that may prompt more companies to incorporate computer security as part of their culture. The paper shifts from the macro influences to examine a recent industry computer model the “appliance” and its specialized offspring the “storage appliance”.

The model is examined to understand if it provides greater security. Assuming sufficient influence, the paper goes on to identify activities organizations must perform to create a computer security culture. These activities provide the framework for a Computer Security Product Development Policy.

Introduction

The literature on computer security often focuses on the user of the computer equipment and not on the vendors of the equipment. This document explores several macro influences on vendors to take a more active role in developing secure products. The macro vectors are legislation, court cases, international standards, customer expectations and industry associations. These vectors individually and collectively influence the business strategies of vendors.

The effectiveness of these strategies to cause vendors to create more secure products is evaluated by looking at the storage appliance model and the vulnerabilities the model contains. Is the storage appliance model inherently more secure?

As can be expected of popular industry jargon, there are a number of claimants to a widely varying term. This paper does not attempt to assess each individual appliance. Instead, the model itself is examined from a security perspective.

Assuming the macro influences have shifted a vendor’s perception, the last section examines what steps can be taken by different parts of the company to increase security.

Influence vectors on vendors

Various influences are increasing the need for companies to address security issues in their products and services. These influences range from mild customer concern to customer refusal to review products not meeting international standards. This section discusses the current state of the vectors that could cause companies to change the way they produce, market, service and support computer products from a computer security perspective.

The following legislation affects the development of computer products:

Legislation	Industry	Impact on security
HIPAA[1]	Medical and Insurance	HIPAA Security Implementation [2]l
Gramm-Leach-Bliley[3]	Securities, Banking, and Insurance.	"Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door"[4]
Sarbanes-Oxley[5]	Publicly traded companies	"Security and Sarbanes-Oxley"[6]

Figure 1: Legislation affecting computer security

A thorough documentation of the legislative impact on computer security is better read via the resources listed in the table and beyond the purpose of this paper. What is important is that these legislative acts increase the importance of products being able to provide the basic issues of computer security.

- Confidentiality
- Authorization
- Authentication
- Integrity
- Non-repudiation[7]

Products that can document and deliver on these issues will sell better to customers affected by these Acts.

ISO/IEC 15408 Common Criteria

Hacking government computer installations was popular before the movie War Games appeared. Defending the thousands of sites across the world from script kiddies to professional agents is extremely difficult.

Principles, guidelines and standards have been created to move these installations to higher levels of computer security.[8, 9, 10] These documents are primarily directed to the Information Technology managers and administrators that use computers and not to the producers of the computers.

The ISO/IEC created the standard, 15408 "Common Criteria", to address building security into products.[11] The latest draft is 15408:1999. The "Common Criteria" establishes a framework for companies to publish the computer security aspects of their products. This allows certified independent testing labs to validate a product meet the level of security or Evaluation Assurance Level (EAL) the vendor claims.

Products without certification can be eliminated from the list of products evaluated. A Request for Proposal (RFP) can simply state the EAL required. It is up to the vendor to provide products that meet the designated EAL.

ISO/IEC 15408:1999 is 632 pages of standards-ease. Translating the standard into a more manageable form could overwhelmingly tax the author and would miss the point of the discussion. The Common Criteria creates a barrier to entry to markets that vendors may be interested in. Vendors must plan for and spend real capital to achieve certification if these markets are important.

News articles on due diligence

Breaches in computer security are news worthy items. The articles often include estimates of the damages these security breaches cost. Last year damages in the UK were four times greater than estimated.[12]

In a litigious society, finding someone to blame is a profitable business. Can the owner of the computer that infected mine be held liable? Opinions vary to what extent an owner can be held liable. Court cases or legislation is needed to establish what is and isn't covered.[13]

> SANS NewsBites Vol. 5 Num. 49 [Editor's Note (Pescatore): for years we've talked about the concepts of downstream liability and attractive nuisance as being existing legal concepts that could be applied to enterprises that leave their computer systems in vulnerable condition. Doesn't seem like we need new legislation until someone figures out how any such legislation could ever be enforced.] [14]

Can the vendor of the computer be held liable? Court cases to date have not created a framework to pursue this avenue. Congress has talked about this issue but no legislation has been passed. Strong interest in defeating such legislation could easily be seen from vendors. Well-funded lobbyists could prevent the liability vector from being an influence to change vendor behavior.

No established criteria for due diligence for computers

The ability of users of defective software to claim losses is governed by the contracts that people quickly click through and often ignore so they can install their software. These contracts often disclaim Merchantability and Serviceability. Additionally, the warranty period is limited and damages capped at the price of the product itself, not the damage that may come through the product via a successful attack. Well-written contracts effectively prevent a lawsuit from influencing vendors to secure their products.

Contracts that cover availability or define a Quality of Service open the door for users to sue. The Maine PUC required Verizon to pay in full rather than their

requested lower settlement due to service downtime from the Slammer worm. Verizon did not patch the equipment that provided a contracted service before the Slammer worm attacked.[15]

What happens if the contract does not provide recourse for inadequate computer security? Can users establish that a vendor did not perform due diligence in producing the product? Can a user show that the vendor so inadequately did their job compared to the rest of the industry that legal recourse is possible?

For example, the need for anti-virus PC software installed only on a company intranet is well-established. It is insufficient to have anti-virus software installed; to adequately protect the PC a user must insure that the latest signature files are also installed.

Let's pretend a PC did not come with anti-virus software and did not allow the user to install anti-virus software. Would the vendor be liable? A user would simply assume that anti-virus software and getting updates would be permitted. They would probably not even think about asking the sales agent.

Imagine their distress when they go to install anti-virus software or their computer gets infected. After long on-hold times to the PC's support center they are told that yes indeed the PC they purchased doesn't have anti-virus software nor can it be installed.

Frustrated, they might check the contract to see what their rights are. Unfortunately, it is not uncommon for the vendor to disclaim Merchantability and Serviceability. They are stuck if the return policy return date has passed.

Can the user in this hypothetical situation sue the vendor for not following due diligence? Unfortunately, there do not appear to be any court cases that establish what due diligence is for computer security.[16] In other words, the user is stuck even though the vendor did not provide even the most basic type of computer security. Due diligence does not provide an influence on changing vendor behavior.

Customer security expectations

What are the expectations of customers on the computers they purchase? Customers' expectations are modulated by their experience. The computer security experience spectrum can range from the novice whose knowledge of computer security is severely limited to the internationally recognized expert representing government intelligence agencies or other interests.

The novice could be managers and administrators of an IT shop seeking to add new technologies they believe will help solve one or more problems they are currently experiencing. Often a novice is unaware of the security implications a

new technology introduces and they accept what the sales people present. This assumes that the sales presentation covers the security capabilities of the product.

At the low-end of the experience level, customers either expect or don't know what to expect from a computer vendor let alone a storage vendor. Assuming a firewall between a storage product and the wild wooly world of the internet, they believe nothing additional is required. Vendors have no need to spend money implementing security requirements to get in the door.

The security expert on the other hand can bewilder the sales people with their security questions sending the sales team packing, wishing they had done their homework. The range of experience creates a complicated range of expectations on vendors.

Somewhere along the spectrum, vendors begin spending time and money on building security into their products and services as well as their sales, marketing, training and support organizations.

Before this point the vendor is not interested in building in computer security. This attitude is matched by a quote taken from a discussion the author participated in:

"If you [the vendor] haven't done due diligence, let the customer know how to protect it [appliance]. Let the customer take the risk."[17]

The discussion group represented a diverse spectrum of companies in terms of size, industry and security requirements. A large portion of the customer spectrum is not significantly influencing vendors to change if the discussion group was indeed representative.

Industry Associations

The final vector influencing vendors to build computer security into their products to be examined are industry associations.

The Storage Networking Industry Association (SNIA), www.snia.org, has a working group Storage Security Industry Forum (SSIF), www.snia.org/ssif/, which is focusing on the security needs in the storage domain. Conferences and papers educate consumers on protecting their environment and what to ask from vendors. Participating vendors are lending their knowledge and skills to identify and improve best-practices and obtain valuable customer feedback.

After reading the papers on the SSIF website, it is unclear if the SSIF has had enough time in one and a half years to assess their impact on vendor products.

Some of the other macro influences, however—particularly, legislative developments and the growing costs associated with virus and worms—are starting to affect vendor products. The next section of this paper discusses a new product development model whose security implications make a case for carefully considering security issues in the product development process.

The Appliance Model

The complexity of computer products has caused various pundits to cry-out for simplicity. Storage Area Networks (SAN) are an example of a complex technology for novice end users. The metaphor of "software wrapped in tin" or "tin wrapped software" is being used by companies seeking to communicate a new level of ease of use.[18]

The term appliance comes from kitchen gadgetry like a toaster or microwave that you can simply plug-in and use. Anybody can use the appliance because it is so simple. Extensive and expensive training on-site or off-site is not required or is limited.

The metaphor has appeal to IS shops because of their efforts to reduce costs. The easier it is to use the lower the Total Cost of Ownership (TCO).

What follows is the author's attempt to list common attributes of an appliance.

- Vendor provided hardware, firmware, OS and applications pre-installed
- Simple customization and the appliance is ready
- Linux or VxWorks
- Open source software
- Web-based GUI
- SNMP Agents that diagnose and let users know of problems via phone, email and pager
- Command-line interface to allow scripting or slow dial-up access
- Interfaces to install additional software may not be available
- Only applications sold by the vendor are allowed on the hardware
- Additional interfaces limited to those required by the installed applications
- Limited set of user ids
- Root or Administrative privileges denied or greatly limited
- No monitor, keyboard and mouse
- Maintenance is provided by the vendor's website or vendor personnel

The command-line interface can be telnet, SSH or application specific. The available command-set may be vendor specified and unchangeable.

On the surface, the appliance metaphor sounds great. The storage industry has also picked up the appliance model and personalized it for storage.

What is a storage appliance?

A storage appliance begins with the appliance attribute list above and solves some type of storage problem.

Domain	Vendor
Data protection	Revivio
Storage security	NeoScale
Eliminates duplicates from backups	Avamar
Backup and recovery	StorageTek

Figure 2: Sample Storage Appliance List[19, 20]

Storage protocols like FICON or iSCSI are also part of the storage appliance and affect security.

Computer Security Benefits of a Storage Appliance

In the author's opinion, certain appliance attributes contribute to making the appliance more secure. These attributes are as follows:

- Reduced interfaces to the appliance make the appliance harder to attack.
- Limited user ids particularly if they are not root, admin etc. make it more difficult for attackers to get both the user id and password.
- Limited or application specific command set prevents authorized users from mistakenly breaking the machine and limiting unauthorized users' abilities to control the appliance and take over other machines.

Computer Security Vulnerabilities of a Storage Appliance

The threat vectors of a storage appliance do not eliminate the common threat vectors of a computer. For a moment, ignoring physical access threats, an appliance that has connections to other machines is vulnerable to attack. This is especially true if the product is using well-known operating systems (Linux), network protocols (TCP/IP) or software packages (Apache/Tomcat).

All interfaces into the storage appliance need to be hardened. The purchaser can ask the vendor to supply written documentation of their efforts. The efforts should include steps to secure the control and data path interfaces as well as the management interfaces. The purchaser should also ask about user training and documentation for securing these interfaces.

The vulnerabilities of a storage appliance are not necessarily present in every appliance. Careful questions by the purchaser will help to identify which vulnerabilities are present and the magnitude of the vulnerabilities. The

purchaser's security policies can increase or ameliorate the impact of the vulnerabilities.

Patch Management

Specialized hardware and limited interfaces force the user to rely on the vendor for patches. These may be available only from the vendor website or vendor personnel. This means that the customer is dependent on the vendor to provide the patches for the appliance that have been downloaded from a third-party vendor, tested by the vendor and made available in a timely manner.

For example, the Linux community announces the availability of a security patch. The IS shop can not download the patch to the appliance and begin testing. They are required to go to the appliance vendor for any patch, even kernel patches. If the appliance vendor is slow to deliver the patch, the customer suffers the consequences.

This leads to a set of questions to ask an appliance vendor:

- Are people dedicated to monitoring the security bulletins by CERT, SANS, vendors and others? The more details you can obtain about their policies and procedures the better.
- What is the process to get notified?
- Who do you call if you don't get notified?
- Is there a commitment to make the security patches available in a timely fashion? Are they willing to put it in writing? If they are, then you may have obtained a Quality of Service obligation on the part of the vendor. Check with your legal department.
- Are the hours of service and response times sufficient given the criticality of the data stored on the appliance? What is the risk to the data if the web was saturated from a virus outbreak and the latest patches could not be downloaded over the internet? Are backup delivery strategies needed?

Audits

What sort of auditing of the appliance is possible? An initial security assessment and regular audits allow an IS shop to detect abnormalities that may indicate an attack has occurred. In the desire to create an easy to use appliance, the vendor may have mistakenly prevented audits.

Are the performance monitors sufficient to indicate an attack? For example, a GUI may only show the performance of a data device and not be able to show that a Trojan horse has been installed and the appliance is being used in an unauthorized manner.

Can the interfaces be hardened if they do not meet a company's policies or procedures? For example, if iSCSI is used to transmit data, can the appliance be configured to use IPsec to carry iSCSI traffic?

Limited user ids and command set

One option in creating an appliance is for the vendor to limit the user ids and passwords on the appliance. What is the magnitude of this vulnerability? The first step is to understand if the vendor has done this. Are these existing ids a problem based on your policies and procedures? Can you change the password expiration policy or is this controlled by the vendor? Does the vendor retain a separate password the customer does not have access to? What is the expiration policy on this user id's password?

The benefit of having limited interfaces and limited command set makes it easier to learn but restricts the ability to conduct security audits. Ask the vendor to provide a list of the hardening they have done to the appliance. If the command set is restricted, there is limited ability to check if the hardening was done correctly. Unfortunately, the limited command set can also shield an attacker from detection because users do not have access to the operating system's command set to detect abnormal usage.

Can the user install their third-party security software? An appliance that has only an application specific GUI and command set may not allow anti-virus software to be installed.

Does the vendor provide an "Unauthorized Access" warning message for all login screens? If inadequate, can the user set the message to their company policy?

Centralized logging is a component in a Defense In-Depth strategy. Hackers will attempt to cover their tracks by looking for the log files setup to create traceability of user activity. What is the mechanism that allows a customer to administer the appliance to use centralized logging and synchronize the system clock?

If the vendor has taken the time to get the appliance certified at a Common Criteria EAL, the purchaser's job is a little easier as some of these questions are already answered.

The Common Criteria and other influence vectors are creating or enhancing the desire of vendors to build computer security into their products and the way the company does business. The next section identifies areas and responsibilities for computer security by different parts of the company.

Creating a computer security focus

The responsibility for creating secure products varies within the functional organizations of a company. It is assumed that the IS organization has already created a secure working environment for the company to conduct their work. Appendix A and B contain additional resources and training for the organization.

Product Development

The burden of computer security falls on product development. The mindset of the product development organization may need to change. One anonymous architect mirrored the mindset in the industry. "We run behind a firewall and use SSL so nothing additional is needed for web security in the first release."[21]

Basic and specialized training will be needed. In-house training for the security technologies used or developed can be expected. Technology evaluation must be expanded to include computer security. Light-weight documented procedures to assist new team members will reduce errors and shorten learning curves.

Code reviews or pair programming are needed to insure that best practices are understood and where to apply them.

People assigned to these tasks should network to avoid replication and share knowledge and skills. Implementing security requirements may require activity (port scanning) that may be viewed as illegal or against corporate policy. Contact IS and make sure they and the appropriate level of management have signed off on the work in writing.[22]

If computer security is recognized as an important product differentiator or simply a "me-to" requirement, the product requirements will reflect this commitment. Product requirements to offset the vulnerabilities of the appliance model are needed.

Product requirements

The operating system, applications, protocols and third-party software need to be hardened. Enough work has been done on these subjects that a team should not reinvent the wheel. Appendix A is an abridged list of resources covering this topic.

The appliance needs to be auditable by the customer. If the only commands a user can run are the commands for the application itself, then the appliance can not be audited. The user needs the ability of determining usage patterns to allow detection of potential attacks.

The GUI or command-line interfaces must be built to allow a user to administer centralized logging which includes synchronizing clocks. This can be done via the OS specific logging facilities, SNMP or appliance specific capabilities.

Additional requirements will be discovered as vendors engage customers in understanding their Defense in-Depth strategies.

Integrating the appliance with customers' Defense in-Depth strategy

Large customers or those affected by the legislative acts mentioned previously have security policies and procedures in place. A coordinated effort between Support, Marketing and Development is needed to understand common strategies and products used by the target customers. This understanding is needed to create an appliance that integrates into the customer's operations easily.

Initial questions are the following:

- Are there Common Criteria requirements?
- What hardening is required and what is optional?
- Are there firewall restrictions?
- Does the appliance need to allow for different mechanisms to secure the application traffic? Is a VPN required for application data and which vendors have been tested? How does the VPN affect performance?
- Does a Host Detection System need to be installed on the appliance? Which vendors have been approved?
- Does anti-virus software need to be installed and updates obtained from a customer local URL rather than the anti-virus vendor?
- What are the centralized logging requirements?
- Does an authorized user need the ability to audit the appliance?
- What are the user id and password management policies?
- What is the need to have third-party security software installed on the appliance? For a company policy may require Tripwire on all servers.

Usability

Usability studies are extremely insightful to understand if the appliance is easy to use. Computer security requirements add to the complexity of the administration of the appliance. Encryption of data in flight requires key administration on both ends of the wire. Is the appliance too difficult for the target user community? Usability studies will help address these questions.

Test

The test organizations have the role of validating that the other organizations have delivered on the requirements. The training for product development can be used to train the test organizations. The test personnel must understand the

customer's security needs, environment and understand the principles behind the security features to be able to determine if the requirements have been properly implemented.

If a "Common Criteria" certification is being pursued, the test organization may want to obtain training to be able to conduct dry-runs of the appliance before submitting to a certified laboratory.

Documentation and Training for customer

The training for the customer must include the computer security features of the appliance. The training will be that much more valuable if the customer can interact with real appliance installation environments. The customer's goal is to understand how to integrate the appliance with their security policies, procedures and products. For example, how can the user administer the appliance to log events to the centralized logging server?

Legal & Contract Administration

The Legal and Contract Administration departments need to make sure they stay current with current case law in computer security. For example, if computer security due diligence was established, the Legal department needs to be monitoring this and notify the appropriate organizations to determine if the products and services are in compliance.

If the appliance includes third party software or open source software, the legal department has the responsibility of keeping current on the restrictions of the licenses used and educating the appropriate parts of the company responsible for fulfilling the licenses.

For example, if the license says that a notice of inclusion must be present in the software, has product development included it in a visible manner? Does the ISV contract make the licensing needs explicit? For example does the vendor want to be liable if the vendor makes the notice visible during startup but the ISV covers it with splash advertising?

The contract administration organization needs to insure that the company is not liable for Merchantability and Quality of Service unless senior management approves. If the company is selling Quality of Service then it needs to make sure there are adequate resources to provide the contracted service levels.

Program Management

Program management serves as the coordination arm of product development. Are the different organizations adequately addressing their responsibilities in the timeframes required?

Training in the basic concepts of security is needed to allow the Program Manager to talk with customers and to work with the different areas of the company who have more specialized knowledge. The program manager also needs to understand the target market and their security needs to justify security requirements to upper management.

Sales and Marketing

There is a direct relationship between the security of an appliance and the cost and time required to develop the product. For the target market segments, what is enough computer security?

Increased security often means increased complexity. One project manager at a Fortune 100 company was responsible for a product affected by this increased complexity. Tensions mounted as the demo failed inexplicably after working great the night before. Five minutes before the start of the demo, someone realized that one of the clients was no longer on the net and that the cryptography key had changed according to company policy.[23]

Understanding customer security needs and what they are willing to pay for is critical and difficult to do. If the target markets are the government intelligence agencies, the requirements are much better defined than if you are selling to a Fortune 1000 company.

The sales and marketing departments need training in the basics of computer security. Specialized training will be needed to address the security features of the products and services being sold. Fundamentally, marketing needs to be able to answer how the product or system can meet the security needs of the target customer set for the price the customer is willing to pay.

Customer Support and Services

Protecting and enhancing a corporate brand can be made or broken by the Customer Support and Services organization. Support and Services must understand the intricacies of the security features being sold. Support has the unenviable task of understanding the relationship between security features in the purchased product and other products onsite while their brain may be fogged at 3am.

Basic training in the security field is the first step. Security certifications are a simple way for an organization to know if people are getting a good foundation. More specialized certification may be needed depending on the products. Support and Services will need additional training in the security features of the products and services being sold. Hands-on time with equivalent customer sites is necessary to understand the nuances of the product and its security. This could be the same training given to Product Development and Test.

Support and Services may be the organization that monitors the news feeds for security issues. They would be responsible for downloading the patches, testing, making the patches available and notifying the customers of new patches.

Computer Security Product Development Policy

Moving the organization to a greater security focus may be easier if the goals are codified in a corporate policy. A corporate policy requires senior management buy-in.

Executive buy-in needed to affect change

Time and money are needed to create a corporate culture where security is not a last-minute patch because script-kiddies have toasted our biggest customers' data. Senior management must agree to fund and not circumvent the time and effort needed to make appliances meet the needs of the target customers.

The change, if not already driven by senior management, will require education of the senior management team to allow them to properly prioritize and fund security requirements identified. Education can occur through various channels including new product presentations, knowledgeable key customers talking with senior managers, training and outside security consultants. A computer security champion may be needed in case significant resistance is encountered within the organization.

Computer Security Policy

A Computer Security Policy may assist the company in creating appliances with consistent security. The time needed to create a policy by leaders across the organizations may not be justified if the hallways are littered with policies that were quickly bypassed at the first excuse or change of management. The reader needs to judge if a policy will significantly assist the ability of producing secure products given the culture of their company. A couple of dedicated individuals on key products may accomplish more than a blue-ribbon board appointed by senior management in a mantra-of-the-month culture.

Grass-roots efforts by individuals on the program team can effect significant change in the security of the appliance. Baby steps that can be achieved over multiple releases can significantly enhance the security of the appliance. The 80/20 rule applies here. The SANS Top Twenty Vulnerabilities list is one place to start.[24]

Summary

The cost of insufficient and ineffective computer security is increasing every year. Corporate computer users are being forced to become more knowledgeable in the security arena because system critical data and processes must be protected. Users are putting pressure on vendors to do a better job. The current Microsoft security focus is said to be a response to the widespread damage done by viruses and worms that propagated via Microsoft products.[25]

The influence of governmental regulation was examined to understand the impact on vendors to supply more secure products. In particular, HIPAA, Sarbanes-Oxley and Gramm-Leach-Bliley are causing IS organizations to change the way they do business. The change in business is providing market opportunities to vendors whose products can address the legislative requirements.

Lawsuits can create incentives for vendors to build in computer security. An overview of current contractual law was explored for its influence on vendors. Well worded contracts effectively prevent users from successfully suing vendors for poor security. Quality of Service clauses can cause a vendor to pay up if the clauses are not honored due to security issues. An appliance vendor is unlikely to agree to a Quality of Service clauses unless they are a service provider. This influence vector is unlikely to cause changes in vendor behavior.

The concept of due diligence was explored as a final legal influence. Could a user win a lawsuit against a vendor because a product did not provide common security features? Currently a definition of computer security due diligence has not been established. Due diligence is not likely to cause increased product security by vendors.

The international standard, ISO/IEC 15408:1999 Common Criteria was examined to understand its influence on vendor behavior. This standard:

- Assists vendors in stating what the security features are.
- Creates the ability for certified independent labs to validate the claims.
- Provides greater confidence to purchasers.

The Common Criteria is a significant influence vector to vendors selling to governmental agencies both here and abroad. What is the additional cost of designing and certifying a product to one of the Evaluation Assurance Levels? Is the cost high enough that acceptance of the Common Criteria outside of governmental agencies and suppliers is not likely to occur? If this is the case, then the standard will not be a large influence upon vendors.

The industry association SNIA SSIF was also discussed. It is difficult to assess the impact on vendors given the short time it has been in existence.

Total Cost of Ownership and pressures to do more with less are helping to make the terms “appliance” and “storage appliance” popular. These terms were examined from a security perspective. The vulnerabilities were explored with questions for a purchaser to understand the risk involved with purchasing a particular appliance.

Assuming that the vectors of influence were sufficient to cause vendors to improve their appliance security, the changes needed inside an organization were identified. Resources and training are included in the Appendices to assist the reader in getting started.

Vendors are caught in an ongoing tension between adding new features in a timely fashion and using the least amount of resources. The vectors discussed are placing various degrees of pressure on vendors to change. As time goes on and more virulent attack vectors arise, vendors that deliver products and services that are more resilient to attack will get the best kind of advertising, word-of-mouth.

Appendix A: Resources

The following is an abridged list of resources to secure an appliance. This information is provided as a starting point.

Linux

“Auditing Linux” by Krishni Naidu, URL: http://www.sans.org/SCORE/checklists/AuditingLinux.doc.[26]

“Linux Kernel Hardening” by Merry Taylor, URL: http://www.sans.org/rr/papers/32/1294.pdf.[27]

“Linux Kernel Hardening” by Anton Chuvakin, Ph.D., 23 January 2002, URL: http://securityfocus.com/infocus/1539.[28]

Linux Security Cookbook by Daniel J. Barrett, et al, June 2003.[29]

Applications

“Developing Secure Applications and Web Services”, URL: http://www.microsoft.com/technet/security/topics/secapps/default.mspx.[30]

IT Security Cookbook, particularly Chapter 13, URL: http://boran.linuxsecurity.com/security/.[31]

"Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense-in-depth approach" by Vilas L. Ankolekar, URL: http://www.giac.org/practical/GSEC/Vilas_Ankolekar_GSEC.pdf.[32]

"A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention" by John Wilander and Miriam Kamkar, URL: http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/10.pdf.[33]

Additional resources may be found from the vendor of the technology. Sun has resources for securing Java.

Web Apps

"Web Application Checklist" by Krishni Naidu, URL: http://www.sans.org/score/checklists/WebApplicationChecklist.pdf.[34]

"Improving Web Application Security: Threats and Countermeasures Roadmap" by J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan, URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp.[35]

"Writing Secure Web Applications", URL: http://www.advosys.ca/papers/web-security.html.[36]

"Web Browser Protection Profile" by George Ryan et al, 4/20/01, URL: http://niap.nist.gov/cc-scheme/PP_WBPP_V0.5.pdf[37]

Protocols

iSCSI: "Storage Basics: Securing iSCSI using IPSec" by Mike Harwood, URL: http://www.enterprisestorageforum.com/ipstorage/features/article.php/3304621.[38]

FICON: The Fibre Channel Security Protocol (FC-HP) is currently in an IETF working group. FC-HP will include FICON when it becomes a standard. URL: www.ietf.org.

Linux TCP/IP: "The official IPsec Howto for Linux", Version 0.9.6, 28 January 2004, URL: http://www.ipsec-howto.org/.[39]

Appendix B: Training

The following is an abridged list of resources for different types of training for a corporation interested in raising their security focus.

Development, Test, Support and Services, Customer Training

The SANS Institute: http://www.sans.org.

CISSP: http://www.cissp.com/Exam/Seminars.html.

Infosec Institute: http://infosecinstitute.com/.

CERT: http://www.cert.org/training/.

Computer Security Institute: http://www.gocsi.com/.

Sun Microsystems: "Developing Secure Web Applications" http://suned.sun.com/US/catalog/courses/WI-3602-90.html

Sales, Marketing and Program Management

The security training classes listed above may be too detailed for sales, marketing and program management. Customized training may be needed to tailor the material to the needs of these organizations. One or two day conferences or seminars may provide the appropriate amount of detail. Talks and tutorials for the IS manager may also provide the correct amount of detail.

The SANS Institute: "SANS Security Leadership Essentials for Managers", http://www.sans.org.

Computer Security Institute: http://www.gocsi.com/.

CERT: "Information Security for Network Managers", http://www.cert.org/training/.

Legal

The SANS Institute: "Business Law and Computer Security", http://www.sans.org.

Computer Security Institute: http://www.gocsi.com/.

Appendix C: References

[1] "Office for Civil Rights – HIPAA". 4 August 2003. URL: http://www.hhs.gov/ocr/hipaa/ (7 March 2004).

[2] Northcutt, Stephen. ed. HIPAA Security Implementation. SANS Press, 2004. URL: https://store.sans.org/store_item.php?item=117

[3] "Financial Privacy: The Gramm-Leach Bliley Act". URL: http://www.ftc.gov/privacy/glbact (7 March 2004).

[4] Langin, Daniel J. "Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door". URL: http://www.securitymanagement.com/library/gramm_tech0902.pdf (7 March 2004).

[5] "Spotlight on Sarbanes-Oxley Rulemaking and Reports". 15 August 2003. URL: http://www.sec.gov/spotlight/sarbanes-oxley.htm (7 March 2004).

[6] Hurley, Edward. "Security and Sarbanes-Oxley". 25 September 2003. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci929451,00.htm (7 March 2004).

[7] "e-Security Defined". URL: http://www.cryptomathic.com/pdf/e-security_defined.pdf (9 March 2004).

[8] Roback, Edward A. "Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products". August 1999. URL: http://csrc.nist.gov/publications/nistpubs/800-23/sp800-23.pdf (27 February 2004).

[9] Swanson, Marianne "Security Self-Assessment Guide for Information technology Systems". November 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf (27 February 2004).

[10] Stoneburner, Gary, Hayden, Clark and Feringa, Alexis. "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)". June 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf, (27 February 2004).

[11] "Common Criteria". August 1999. URL: http://csrc.nist.gov/cc/ (27 February 2004).

[12] Kotadia, Munir. “Virus clean up costs four times higher than predicted”. 2 December 2003. URL: http://www.silicon.com/software/security/print.htm?TYPE=story&AT=39117165-39024655t-40000024c (9 March 2004).

[13] Wylene, Arthur J. “The Curse of Service: Civil Liability for Computer Security Professionals”. URL: http://csrc.nist.gov/nissc/2000/proceedings/papers/028.pdf (7 March 2004).

[14] The SANS Institute. “Sophos Notes Recent Spike in Trojans“. SANS NewsBites Volume 5 Num. 49: Editor’s Note. 10 December 2003. URL: http://archives.neohapsis.com/archives/sans/2003/0175.html (10 December 2003).

[15] Welch, Thomas L. “Inquiry Regarding the Entry of Verizon-Maine Into The InterLATA Telephone Market Pursuant To Section 271 of Telecommunication Act of 1996”. 30 April 2003. URL: http://www.state.ma.us/dpu/telecom/03-38/56attcomne.pdf (9 March 2004).

[16] Woods, Maria V., JD. “Legal Due Diligence”. personal e-mail (27 January 2004).

[17] Denver Mentor Led SANS Security Essentials Course. Group Discussion (4 January 2004).

[18] Tiogo, Jon W. “Invasion of the Tin-Wrapped Software Appliances”. 6 February 2003. URL: http://www.esj.com/news/article.asp?editorialsId=409 (9 March 2004).

[19] Tiogo. page 1.

[20] “EchoView E400 data protection appliance”. URL: http://www.storagetek.com/products/product_page580.html (12 March 2004).

[21] Name withheld by request. personal interview. August 2003.

[22] Young, Beth. “Securing Linux”. URL: http://www.more.net/security/presentations/securelinux.pdf (12 March 2004).

[23] Name withheld by request. personal interview. January 2004.

[24] The SANS Institute. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus”. Version 4.0. 8 October 2003. URL: http://www.sans.org/top20 (13 March 2004).

[25] Rooney, Paula. “Microsoft Launching Major New Security Initiative”. InternetWeek.com. 8 October 2003. URL: http://www.internetweek.com/breakingNews/showArticle.jhtml?articleID=15201798&pgno=2 (12 March 2004).

[26] Naidu, Krishni. “Auditing Linux”. URL: http://www.sans.org/SCORE/checklists/AuditingLinux.doc (7 March 2004).

[27] Taylor, Merry. “Linux Kernel Hardening”. URL: http://www.sans.org/rr/papers/32/1294.pdf (13 March 2004).

[28] Chuvakin, Anton, PhD. “Linux Kernel Hardening”. 23 January 2002. URL: http://securityfocus.com/infocus/1539 (13 March 2004).

[29] Barrett, Daniel J., et al. Linux Security Cookbook. OREILLY. Jun 2003.

[30] “Developing Secure Applications and Web Services”. URL: http://www.microsoft.com/technet/security/topics/secapps/default.mspx (7 March 2004).

[31] IT Security Cookbook. URL: http://boran.linuxsecurity.com/security/ (13 March 2004).

[32] Ankolekar, Vilas L. “Application Development Technology and Tools: Vulnerabilities and threat management with secure programming practices, a defense-in-depth approach”. URL: http://www.giac.org/practical/GSEC/Vilas_Ankolekar_GSEC.pdf (13 March 2004).

[33] Wilander, John and Kamkar, Miriam. “A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention”. URL: http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/10.pdf (27 February 2004).

[34] Naidu, Krishni. “Web Application Checklist”. URL: http://www.sans.org/score/checklists/WebApplicationChecklist.pdf (7 March 2004).

[35] Meier, J.D., Mackman, Alex, Dunner, Michael, Vasireddy, Srinath, Escamilla, Ray and Murukan, Anandha. “Improving Web Application Security: Threats and

Countermeasures Roadmap". URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnnetsec/html/ThreatCounter.asp (27 February 2004).

[36] "Writing Secure Web Applications" URL: http://www.advosys.ca/papers/web-security.html (7 March 2004).

[37] Ryan, George et al. "Web Browser Protection Profile". 20 April 2001. URL: http://niap.nist.gov/cc-scheme/PP_WBPP_V0.5.pdf (27 February 2004).

[38] Harwood, Mike. "Storage Basics: Securing iSCSI using IPSec". URL: http://www.enterprisestorageforum.com/ipstorage/features/article.php/3304621 (13 March 2004).

[39] "The official IPsec Howto for Linux". Version 0.9.6. 28 January 2004. URL: http://www.ipsec-howto.org/ (13 March 2004).