Interested in learning more about security?

SANS Institute InfoSec Reading Room

Obtaining Better Results from Distributed Environment Security Programs

This paper examines common barriers to achieving desired results from information security programs in mid-to-large-sized corporations. We will consider elements that are often underemphasized when planning security programs and we will expose some of the reasons why those issues tend to be overlooked. Finally, we'll describe the value of, and a methodology for, including those elements in your planning to create a more balanced information security program.

Obtaining Better Results from Distributed Environment Security Programs

Rhonda Cram Manter
March 2, 2002
Version: GSEC ver. 1.2f

Introduction

You've implemented firewalls, intrusion detection (IDS), anti-virus filters and eradication products. Your organization has implemented and communicated a comprehensive set of security policies. You should be set; but security incidents continue. And they frequently materialize in areas where your existing controls should be preventing them! Why aren't your efforts working?

For the mid-to-large-sized organization, the explosion of distributed and interdependent applications present dimensions of security assurance that are difficult to identify, measure and contain.

Abstract

This paper will examine common barriers to achieving desired results from information security programs in mid-to-large-sized corporations. We will consider elements that are often underemphasized when planning security programs and we will expose some of the reasons why those issues tend to be overlooked. Finally, we'll describe the value of, and a methodology for, including those elements in your planning to create a more balanced information security program.

Ultimately, I hope to deepen your perspective of the risk to information assets, the ability to control risk factors, limited budgets and human resources.

This paper will not detail point solutions nor discuss every control mechanism.

The sources of threats

Attacks generally come from one or both of two threat sources: internal and external.

Both internal and external-sourced threat/attacks stem from various motives:

- Access to additional resources
- Competitive advantage
  - Economic
  - Political
- Personal grievance, vengeance
- Curiosity
- Mischief
- Attention[1]

[1] Carpenter, p. 79

The misleading characterization of incidents

The 2001 CSI/FBI Computer Crime and Security Survey cites that "for the fourth year in a row, more respondents "(70%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (31%)."[2] In fact, the survey indicates that the rate of external attacks has been rising, while the rate of internal attacks has been declining. These statistics, while important, shift your focus from the area where you have significant control. Focusing on the source of incidents, especially externally sourced incidents, creates an atmosphere of non-accountability.

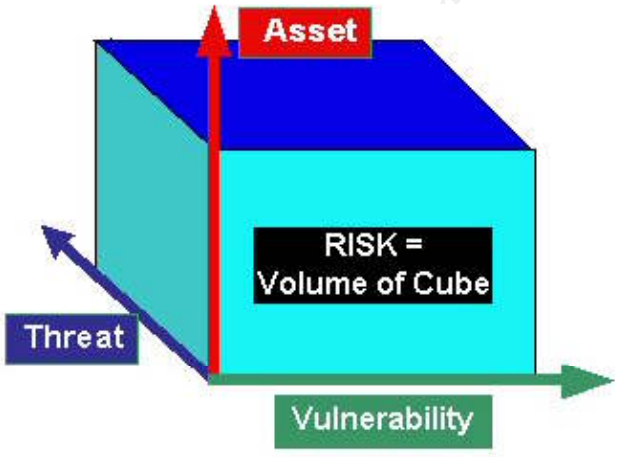
Setting good policies, educating users and enforcing policies reduces some internal threats, but there is very little one can do to eliminate most threats.

However, vulnerabilities are another matter. For a threat to successfully cause a breach of security, a vulnerability must also exist. "Greater than 99% of intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available."[3] Did you catch that? There is a big opportunity for reducing successful attacks by reducing vulnerabilities. Fortunately, vulnerabilities tend to be much more tangible than threats and one can actually look for, find, and eliminate or mitigate them.

Without vulnerabilities, all the threats in the world won't breach your systems.

Therefore, classifying an incident as either external or internal is misleading. The threat may be from an external source, but the vulnerability lies squarely in your court.
L-3 Network Security (recently acquired by Symantec Corporation) defined risk:

Risk = Assets x Threats x Vulnerabilities



Symantec Corporation
Assets, Threats and Vulnerabilities

"Total risk is expressed as the volume of a cube defined by all three of these factors…"[4] This simple approach helps to visualize how reducing of any of these factors lessens overall risk.

- You're not likely to want to reduce valuable assets.
- You have limited ability to reduce threats.
- Vulnerability reduction is the area where you have the greatest amount of control, and should be your focus for reducing risk.

[2] Power, p. 8
[3] Carpenter, p. 84
[4] "Assets, Threats and Vulnerabilities", Symantec Corporation, p. 6

Most vulnerabilities have countermeasures available

Vulnerabilities come in all shapes and sizes. Here I'll list a few loose, but common, classifications of vulnerabilities:

Protocol flaws, operating system and application bugs, social engineering, viruses, worms, trojan horses, weak passwords, physical security, etc.

A very respectable amount of research and analysis has been devoted to identifying existing vulnerabilities and how to mitigate them. There is a plethora of hardening procedures such as Julia Allen's "CERT ® System and Network Security Practices", and even some very good platform-specific security standards. However, I have noticed that most hardening guidelines are very good at telling you what to do, but not how to get it done. The fact is, even though mitigations are usually available, we're not getting them implemented. And the result is that we continue to have incidents.

The complexities of patching vulnerabilities in a distributed environment

Distributed systems are particularly susceptible to improperly managed vulnerabilities. To clearly explain my point I'll first contrast by describing the relative ease of managing in a centralized or smaller environment.

Centralized systems typically have a single or very hierarchical management chain and have related budgeting and business priorities. Often it is a close-knit group that engineers, implements and safeguards the systems. There is a greater personal connection with all aspects of the application or environment. The owners of a system have a better understanding of all interdependencies and of the people involved. While controls and auditing are still appropriate, they can usually be more simplistic.

In a smaller organization, it might only be a matter of handing a set of procedures and specifications to the system administrators and granting them time to comply.

In large, distributed environments, management chains are often disjointed. Budgets are not necessarily in synch. Strict change control and service levels restrict timely patch installation. Administrators have to decide how risky the patch is versus the vulnerability, and how much, if any, testing is required. "Even when administrators know what to do, they often don't have the time to take action; operational day-to-day concerns and the need to keep systems functioning take priority over securing those systems. Unfortunately, managers often fail to understand that securing assets is an ongoing process and not just a one-time fix. As a result, they do not consider this factor when allocating administrator time and resources."[5]

System Administrators, when presented with a vulnerability and a patch or workaround, have a multitude of tasks, decisions and procedures that need to be adhered to prior to getting about the business of applying the patch. This causes what I call 'the credenza

[5] Allen, p. 3

syndrome'. If I can tackle the task in 5-10 minutes from my desk, then it gets done right away. If it takes considerably longer, I set in the pile on my credenza until I have time to tackle the job. Now, some things that get piled on my credenza get done in a reasonable amount of time. But those things are usually the things my boss or a customer is waiting for; not overhead activities – even if I view them as valuable.

The <u>real</u> 'what to do'

We must reduce the time required of information technology (IT) groups to keep their systems managed and maintained in a hardened state. Implementing and complying with security controls must fall within an acceptable level of 'overhead'.

Most administrators and IT managers recognize that some percentage of their time must be spent securing their systems. However, most are surprised at how time-consuming it is. Mark Joseph Edwards of Security Administrator Magazine asserts, "...not enough administrators take immediate action upon learning of new vulnerabilities. This neglect is a huge mistake…"[6]

Over time, IT groups simply cannot sustain the resource drain to comply with every security policy and procedure as business requirements and competitive business demands more service out of fewer resources. More vulnerability/patch alerts are diverted to the credenza. Periodic log reviews are skipped and security configurations slip out of compliance into a weak and vulnerable condition. The systems are perfectly functional, and the administrators scurry off to take care of more pressing requests.

How to fix their (your) problem

Change your perspective from one where your role is solely that of the policymaker/enforcer, to one that is more customer-oriented. After all, the IT groups are your customers.

Define your policies. Then keep going:

1. Information security must research and create specific, secure standard configurations for your top-tier server types. "We strongly recommend that you use the configuration principle "deny first, then allow." That is, turn off as many services and applications as possible and then selectively turn on only those that are absolutely essential. We recommend you install the most minimal operating system configuration image that meets your business requirements."[7] (While it may be your first inclination to require the system administrators to interpret your policy and define which services and ports are required for their particular applications, ambiguity in setting security standards leads to poor compliance. The system administrators I have spoken with tend to prefer a strict set of security standards, with an 'exception' process for adding non-standard services.)

[6] Edwards, p. 1
[7] CERT® Security Improvement Modules

2. List and review all of the activities required of an IT group to keep their systems secure and compliant with policy. Do not just include patch maintenance. There are many other vulnerability types and sources. Include them all. Take special care to include activities that are made more complex in a mid-to-large organization as these items are often underestimated and swept under the rug.
3. Assess the list and 'grade' which activities are farthest from being adhered to.
4. Prioritize the list according to which could have the most positive reduction in vulnerabilities.
5. Interview IT personnel in different areas of the organization and identify for each activity what's preventing them from staying current. Allow them to vent, but make sure you don't conceal the problem by solely blaming business priorities and budget. Again, focus on those things over which you have some control. – Even with limited budget and resources, some other factor is making compliance difficult to obtain.
6. Brainstorm methods with your customers to lessen or eliminate the problems. They are both knowledgeable and willing to share their opinions.
7. Some solutions may come in the form of automation tools. Select tools that integrate well with your processes and other tools. Also use tools where you can delegate and distribute authority and responsibility.
8. Review your user education materials. Make sure you have more than one level of training. IT staff do not want to sit through basic training. They have different depths of security training needs than do the basic user. Do not permit your security training to be endured like the time-share scam, 'Just attend our 90 minute presentation and you will receive a special gift worth $100'. Provide real-life examples they can relate to.
9. Sell your plan to your management and IT management. Your greatest allies will be the IT staff. When I looked at my own organization's situation, each IT group had to figure these solutions on their own, and each individual group couldn't justify buying and implementing slick tools. Nor were they particularly interested in doing so – they had other projects to focus on. Having 20 or so IT groups duplicating work with less to show for it was saving us money in exactly what way? Taking on the responsibility of implementing distributed tools and efficiency processes will cost the overall organization significantly fewer resources. Use a pro-rated charge-back or load your internal service fee.
10. There's no need to do everything at once, but with each 'problem area' corrected, a slice of the risk cube can be removed.

Why haven't we done this yet?

- The field of Information security is still maturing. We had to walk before we could run.
- Statistics tend to show a manifestation, not the root cause.
- It's easier and sexier to work on point solutions such as firewalls (and yes, we did need to work on them) than to unravel enterprise issues.
- It is more convenient and organizationally acceptable to blame external causes over which you have no control.

Problem areas

Following are a number of areas that present vulnerabilities that are more pronounced in mid-to-large organizations. You may wish to review how these add to your risk equation:

1. Account administration problems
    a. User accounts – Ensure your workflow includes account ownership and formal termination. Test for and delete inactive accounts.
    b. System/application accounts – Monitor access to accounts with non-changing passwords and implement procedures to secure accounts to protect from terminated staff. IT groups can have hundreds of accounts with high authority and non-changing passwords.
    c. Keep group membership current. In an enterprise the existence of groups presents a few interesting challenges. If the group is a reflection of the organizational structure, implement a feed from an HR database or hierarchical meta-directory data source to ensure accuracy of its membership. However, if membership is based on some other criteria, maintenance is more difficult over time, since manual review and management of the group membership will be required. Assign ownership and provide tools.
2. Physical security concerns - Ensure your servers are all physically secured. Physical access to any server is a vulnerability that can pose a risk to all of your systems.
3. Varying risk - Vulnerabilities on one system may expose other systems. Coupled with varying degrees of risk tolerance and you have a recipe for trouble. Make sure your compliance exceptions make sense.
4. Put data in front of administrators and management. Periodically run scripts with a tool such as DumpACL (SystemTools Software Inc.) to create detailed access control lists and have the administrators sign off on them.
5. Recognize that not all policies can be reviewed at the same intervals and make your requirements attainable. (If you want logs to be reviewed monthly, then implement event correlating logic-enhanced log consolidation tools.)
6. Implement group policies for users and computers wherever possible.
7. Implement configuration management tools and patch deployment tools such as UpdateEXPERT (St. Bernard Software).

Conclusion

It is not 'too much security' that creates problems for IT administrators and for information security groups. The problem lies with unacceptable levels of overhead. Look past what is not secured and find out why it is not secured. When information security organizations take a more involved role in solving IT problems associated with adhering to security programs, security policy compliance will naturally improve.

References

Carpenter, Jeffrey J. “CERT/CC Overview - Incident and Vulnerability Trends”. Cert Coordination Center. August 17, 2000. http://www.cert.org/present/cert-overview-trends/index.htm

“Assets, Threats, and Vulnerabilities: Discovery and Analysis”. Symantec Corporation. March 30, 2000. http://enterprisesecurity.symantec.com/PDF/AxentPDFs/RiskMgmt.pdf

Power, Richard. “Computer Security Issues and Trends”. 2001 CSI/FBI Computer Crime and Security Survey. Vol. VII No. 1. Computer Security Institute. Spring 2001. http://www.gocsi.com/prelea/000321.html

Allen, Julia. “CERT ® System and Network Security Practices” Networked Systems Survivability Program, CERT Coordination Center. June 11, 2001 http://www.cert.org/archive/pdf/NCISSE_practices.pdf

Edwards, Mark Joseph. “Patching Security Holes: Don't Put It Off”. Security Administrator Magazine. January 31, 2001. http://www.secadministrator.com/Articles/Index.cfm?ArticleID=19816

“Offer only essential network services and operating system services on the server host machine”. CERT® Security Improvement Modules. April 30, 2001. http://www.cert.org/security-improvement/practices/p068.html

Briney, Andy. “2001 Industry Survey”. Information Security Magazine. October 2001. http://www.infosecuritymag.com/articles/october01/images/survey.pdf

Evers, Liesbeth. “Network negligence creates security risk”. Network News Magazine. June 20, 2001. http://www.vnunet.com/News/1123341

“UpdateEXPERT™ White Paper: How UpdateEXPERT Improves System Security and Saves Time for IT Professionals”. St. Bernard Software. http://www.stbernard.com/products/updateexpert/products_updateexpert-whtpaper.asp

Last Updated: July 31st, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Antonio 2014	**San Antonio, TXUS**	**Aug 11, 2014 - Aug 16, 2014**	**Live Event**
Cyber Defense Summit & Training	**Nashville, TNUS**	**Aug 13, 2014 - Aug 20, 2014**	**Live Event**
SANS SEC401 Bootcamp @ Malaysia 2014	**Kuala Lumpur, MY**	**Aug 18, 2014 - Aug 23, 2014**	**Live Event**
SANS Virginia Beach 2014	**Virginia Beach, VAUS**	**Aug 18, 2014 - Aug 29, 2014**	**Live Event**
SANS Chicago 2014	**Chicago, ILUS**	**Aug 24, 2014 - Aug 29, 2014**	**Live Event**
SANS Pen Test Bangkok 2014	**Bangkok, TH**	**Aug 25, 2014 - Aug 30, 2014**	**Live Event**
SANS Delhi 2014	**New Delhi, IN**	**Aug 27, 2014 - Sep 02, 2014**	**Live Event**
SANS Tallinn 2014	**Tallinn, EE**	**Sep 01, 2014 - Sep 06, 2014**	**Live Event**
SANS Brisbane 2014	**Brisbane, AU**	**Sep 01, 2014 - Sep 06, 2014**	**Live Event**
Security Awareness Summit & Training	**Dallas, TXUS**	**Sep 08, 2014 - Sep 17, 2014**	**Live Event**
SANS Crystal City 2014	**Crystal City, VAUS**	**Sep 08, 2014 - Sep 13, 2014**	**Live Event**
SANS Bangalore 2014	**Bangalore, IN**	**Sep 15, 2014 - Sep 27, 2014**	**Live Event**
SANS Albuquerque 2014	**Albuquerque, NMUS**	**Sep 15, 2014 - Sep 20, 2014**	**Live Event**
SANS ICS Amsterdam 2014	**Amsterdam, NL**	**Sep 21, 2014 - Sep 27, 2014**	**Live Event**
SANS Baltimore 2014	**Baltimore, MDUS**	**Sep 22, 2014 - Sep 27, 2014**	**Live Event**
SANS DFIR Prague 2014	**Prague, CZ**	**Sep 29, 2014 - Oct 11, 2014**	**Live Event**
SANS Seattle 2014	**Seattle, WAUS**	**Sep 29, 2014 - Oct 06, 2014**	**Live Event**
SANS Hong Kong 2014	**Hong Kong, HK**	**Oct 06, 2014 - Oct 11, 2014**	**Live Event**
SOS: SANS October Singapore 2014	**Singapore, SG**	**Oct 07, 2014 - Oct 18, 2014**	**Live Event**
SANS Perth	**Perth, AU**	**Oct 13, 2014 - Oct 18, 2014**	**Live Event**
GridSecCon 2014	**San Antonio, TXUS**	**Oct 14, 2014 - Oct 14, 2014**	**Live Event**
SANS Network Security 2014	**Las Vegas, NVUS**	**Oct 19, 2014 - Oct 27, 2014**	**Live Event**
SANS DHS Continuous Diagnostics and Mitigation Workshop with Training	**OnlineDCUS**	**Aug 01, 2014 - Aug 08, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**