

Assurance for the Intranet

Herbert J. Mattord, CISSP

Michael E. Whitman, Ph.D., CISSP

Kennesaw State University
1000 Chastain Rd. MS #1101
Kennesaw, GA 30144
(770) 499-3568
mwhitman@kennesaw.edu

Abstract

As organizations begin to adopt Internet technology for internal networks, the problems that face the security of the Internet must also be addressed. With the increasing levels of threats to the Internet and TCP/IP based networks, organizations must assess the abilities of their networks to protect against these threats. This paper examines problems inherent in intranets, and provides guidelines for the secure implementation of intranets from a managerial perspective.

Introduction

Internet technology has become so pervasive and popular organizations have adopted it for internal use, thus creating what the industry refers to as an intranet. So popular in fact, that since 1997, more than nine of every ten major corporations have implemented some form of intranet (Baker, 2000). The variations of intranet technology vary greatly, from simple internal web servers providing corporate information, to enterprise-wide networks, replacing traditional LAN technologies and protocols with TCP/IP based components complete with encryption and authentication features. Until recently many organizations have structured intranet defenses by concentrating on securing the perimeter of the network. In theory, this creates a safe place in which they may place and operate the servers making up an Intranet. Unless intranet systems are managed carefully, this approach can create a class of assets that are poorly configured for information security and are susceptible to a variety of risks. If an organization has focused attention on building a secure perimeter to the exclusion of following recommended practices in individual systems, they need to refocus their energies on configuration assurance. Exclusive network protection may create a setting where system administrators are lulled into a false sense of security by the perimeter protection.

Two factors are making reliance on network layer defenses less effective. First, as the number of users on large intranets grows, the security characteristics of that network approach the background risk levels of the public Internet. The exact number of users needed to drive up the risk of an intranet the equal the risk assumed to exist in the broader Internet is unknown. But, it is fairly certain that a mixed-use environment of 100,000 users will reduce intranet information security confidence to a level that is about the same as the public networks. When the user base is large and comprised of employees, contractors, consultants, vendors, trading partners, business partners and associated parties, many assumptions about Intranet security need to reevaluated. More users from more diverse organizations call our internal networks their own. This indicates that network edges are thinning and becoming less defined.

Secondly, at the same time that the network perimeters are thinning, the DMZ (or extranet) pathways to the public networks are becoming less effective. These gateways grow in scope and size to cover ever more organizational assets. The DMZ places many more servers and data assets in the limited security zone offered by that technology. The degree of protection offered by firewalls decreases as more and more exceptions to otherwise tight controls are granted. Intranet servers are only marginally more secure than those in the extranet do. This differentiation will continue to be less and less discernable.

The question is: "What does it take to be ready for the time when intranet services have the same risk profile as the Internet?" When the firewalls are gone in fact as well as in effect, we must be prepared with new tools and new processes to keep them safe.

Making a More Robust Intranet

The first order of business is to bring intranet servers up to the same level of readiness as our extranet servers. As the level of risk in the intranet approaches the level found in public networks, intranet servers require improved systems and methods to keep configurations in line with policies and to insure both the policies of our organization and the resulting configurations are valid for the evolving environment. All systems in the organization must be protected to the same, stringent degree. In order to accomplish this, the organization must first begin with a thorough risk assessment. This is accomplished by:

- 1) Identifying the threats facing the information.
- 2) Identifying the vulnerabilities in the systems containing the information, that could be exploited by each threat.
- 3) Estimating the probability of the threat exploiting the vulnerability (risk).

- 4) Estimating the value of restoring the information should an attack occur.
- 5) Using this value to determine the expenditure levels for the protection of the information and its systems.
- 6) Identifying areas where additional safeguards are needed.

Efforts to improve intranet security should then look to organization information security policy. Using management review and industry comparison techniques, organization information security policy should be periodically verified as complete and correct. This should include insuring that policies are current for the objectives of the organization and the operating environment. The misalignment of Information Security Policy to both industry best practice and organizational goals occurs over time both as the Information Security industry matures and as organizational goals evolve. An ongoing effort to maintain alignment is needed to insure success.

Policies for the organization should consist of three levels. First is the *Program Policy* used to establish the security program, set the tone for the organization's security posture, and provide guidance for subsequent policies and decisions. Next are the *Issue-Specific Policies*, which address specific topics within the organization, such as Internet Use, Classified Document handling and the like. Finally are the *Systems-Specific Policies* addressing particular technologies and systems the organization needs to protect (NIST, 1995).

Before policy can be tested by machine methods, the policy must be translated into discrete measurable items. The discrete, measurable statement of policy makes it possible to implement tools and processes to automatically measure policy compliance. Once policy is available in machine useable forms, we must create processes to evaluate and manage business risk. The maximum desired state security (or reduction in risk) is called the gold-standard benchmark. This gold-standard benchmark serves as a relatively stable comparison for reducing risk. Operating units may find that the enterprise gold-standard benchmark is out of balance with the degree of risk they need to assume for their specific operating environment. More organizations are concerned with *baseline standards of due care*, those security implementations that an organization should implement, as a minimum, to demonstrate, from a liability issue, that they have done what a prudent organization in their industry and size should do to protect their information and systems.

As organizations increase in size, so too do they increase in diversity of purpose and in the need to assume risk for business objectives. Additional processes are needed to develop operating unit benchmarks. The Operating unit benchmark is adapted from the gold-standard benchmark by selective relaxation (or tightening) of the settings based on the assumption of risk by the appropriate business units. In addition to the creation of benchmarks, automated continuous validation of

practices against benchmarks is essential. When possible, real-time notification of departure from benchmark is desired. When not possible, periodic evaluation of current server settings against the gold standard and operating unit benchmarks are needed.

An additional layer of validation, external to policy validation processes, is the ongoing vulnerability analysis. This process of externally verifying the external security posture of your organization serves several important purposes. The most obvious is the ability to detect and remediate high-risk vulnerabilities detected by the process. So long as the testing suite used for the analysis is current and up to the challenge, the process will guarantee strict alignment of policies and practices with the larger reality of the connected world.

Another critical success element can be a warning system for intranet servers. While not every Information Security organization is positioned to get the maximum value from Intrusion Detection Systems (IDS), some groups can find value in them. Not only should all systems be readied for the day when they have to defend themselves, they should be capable of calling for help or running for cover when they cannot prevent a loss. Host Intrusion Detection Systems may offer advanced organizations additional value maintaining a near real-time view of the systems monitored. While expensive to buy, deploy and operate, host-IDS systems may serve some organizations well. There is a down side to IDS systems, however. Most IDS systems require extensive training to implement and configure properly, and require substantial monitoring to ensure that the incidences reported are in fact threats to information security. Even then, organizations are faced with the question of how and even when to act on these notifications.

Translating Policy to Configuration

The translation of policy into benchmarks should consider that some policy elements are objective and can be measured while others are subjective and will require the judgment of a knowledgeable person with the proper skill set and requisite experience. Automated measurements systems cannot measure the subjective elements. However, the objective elements can be measured successfully with the proper automated tools. When working from policy toward automated checks, a key intermediate deliverable is the platform specific checklist. Sometimes these documents, often called 'security cookbooks' are already prepared and in use by systems administrators. The deliverable is the creation of a list of operating system settings that reflect the desired behavior of systems that comply with policy. Development of these lists of desired system settings or, practices, will require platform specific benchmark development by staff with expert technical knowledge. This operating system perspective must be tempered with practical business understanding. This will allow the creation of the gold-

standard benchmark. The gold-standard benchmark determines absolute risk measured against organizational information security policy. Successful measurement using automated means will require a toolkit with adequate flexibility and granularity to provide reliable measurements using multiple benchmarks.

Tempering Policy With Business-Assumed Risk

A single gold-standard benchmark may prove too inflexible for use in a production environment. This shows the need for processes to guide the development of operating unit specific, business-assumed risk benchmarks. Some observations about operating unit benchmarks are that businesses should assume risk so long as the correct organizational level approves. Each operating unit may need its own business-risk assumed benchmark since the realities of the production environment may indicate different levels of acceptable risk. These operating unit benchmarks will allow the operating units to configure their systems as they need to for their own business-related reasons and permit the measurement of relative risk as compared against their own target security practices. Often the inflexible use of gold-standard benchmarks as the only measurement will result in counterproductive strategies as production systems are held to impossible requirements.

Don't give up the gold-standard benchmark. A realistic process of dual measurement can give excellent results. By using the gold-standard benchmark one can measure the absolute risk. By using the operating unit benchmark, one can measure the relative performance of the business unit against the level of risk that has been assumed by management. Each of these outcomes is a part of the overall strategy of risk management over time.

A final note on the benchmarks: do not assume that either the gold-standard or operating unit risk benchmarks are static. In fact, each may have changes triggered by policy changes, or by external factors that cause a re-evaluation of the willingness to assume risk.

Configuration Assurance

Information Protection groups are the consultants to the system administrators in developing and deploying the tools to keep our Intranet assets safe as they move towards the same level of risk as the Internet. One component of a successful Information Security program needs to be the assurance to all levels of management that all systems are configured, operated and maintained to the expected level of security. Two key elements of this process of configuration assurance are:

- Ongoing, periodic review of all systems against both the gold standard benchmarks and applicable business-assumed risk benchmarks, and
- Management processes are required to close the feedback loop and insure configuration shortfalls are remediated.

Intranet Vulnerability Analysis

One truth from recent times is that risks in the connected world change rapidly and continuously. A robust validation program should have a goal of testing configurations against current threats. A validation program for Internet vulnerabilities may be called an ethical hacking unit or a penetration test unit. The commonality of all of these groups is that they bring real-world testing of production systems to the organization on a periodic basis. When configurations in place are found to be lacking, the organization must make changes to insure continued safe operation. This may involve the need to revise policy and then, to drive new configuration requirements to lower risk. Some organizations may choose to assume the risk found in the new threats. One byproduct of a thorough vulnerability analysis program is that it will keep the information security policy and practices in a constant state of review and currency. It becomes quite important to regularly update policy, configuration and vulnerability analysis to meet all new threats.

Host Intrusion Detection

A program to monitor operating systems for possible intrusion may be called a Host Intrusion Detection System (HIDS). HIDS systems pose a risk for immature information security programs. They may become less effective since:

- Pursuing the many false positive attacks strain already limited resources, and
- Occasional success in detecting attackers cannot substitute for consistently valid configurations, which deter attacks all the time. Those information security programs that have achieved some success in developing policy, securing their network and achieving consistency in server configuration can add marginal value by monitoring for intrusion activity with IDS tools. Host Intrusion Detection Systems adds little value to beginning information security programs but can be useful for established programs.

Summary

The following questions summarize the key points of Intranet Security Assurance:

- 1) How effective are your current information security policies?
Regular policy review is key to ensuring effectiveness.

- 2) How effectively do your system configurations reflect your organization's policy?
Aggressive security policy validation is another key element to ensuring program effectiveness
- 3) Are your "shepherds" watching your "sheep"?
Regular Intranet validation scans effectively test the readiness of your technical services team
- 4) Are there "wolves" among your "sheep"?
Proper education and training of employees ensure that accidental and intentional abuse of systems privileges are minimized.

References

- Baker, S. "Getting the Most from your Intranet and Extranet Strategies." *The Journal of Business Strategy*. 21(4). July/August 2000. pp. 40-43.
- NIST. *An Introduction to Computer Security: The NIST Handbook*. NIST Special Publications 800-12. <http://csrc.nist.gov/publications/nistpubs/800-12/> .
- Sholtz, P. "Internal Security: Rules and Risks" *Web Techniques*. 6(7). July 2001. pp. 63-65.
-