Global Information Assurance Certification Paper

Jennifer Gruener
SANS Security Essentials
GSEC Practical Assignment Version 1.4b Option 2
December 2, 2003

How do you like your Internal Security? Hard-Boiled or Scrambled?

A Case Study of Hardening Interior Security

Abstract

This is a case study of a company that focused most of its resources on securing the external-facing perimeter. Although this is an important entry point of attack, it is not the *only* point that should be considered. The result of this approach was a lack of defense-in-depth. If you associate this company's security philosophy with the properties of an egg, we hardened the shell. However, the inside was raw and easy to exploit. We needed to move quickly to get it hard-boiled or risk becoming scrambled. To begin to address this risk, first, a new Information Security policy was created and approved. Secondly, security awareness/training was administered to facilitate the policy implementation. Finally, new processes and responsibilities for accessing information resources were implemented.

There were obstacles to overcome, but a broader focus on security was implemented. Company time, people and money are still being allocated to securing the perimeter, but also include an allocation for new policies, user accountability, and an evolving role for the IT Security department. It is our goal to maintain a continual campaign to provide the employees with adequate access, educate them on secure user behavior and hold them accountable for internal security in order to fulfill our security goals of confidentiality and integrity of company information and availability of information resources.

Recognizing the Vulnerability (The Raw Egg)

Background

The company is a provider of residential, commercial and industrial electric, gas, and water utility services. Located in a medium-sized, but rapidly growing, community with a history of loyal long-term employees. Due to the diverse services offered by the utility, a vast array of professions all coexists including five different labor unions. Out of approximately 1000 employees, nearly 900 have access to Information resources. There are a wide variety of applications on an equally wide variety of platforms. The company does have a web presence and does some limited e-commerce including on-line service requests and bill paying. The current trend is to utilize vendors and consultants as contract labor to aid in support and implementation of new systems. Nearly half of them access

systems remotely. Also, approved employees are allowed to access their e-mail remotely and future plans include offering them more remote services.

The IT Security department's main focus has been protecting any external facing systems including firewalls, intrusion detection, routers, current security patches and antivirus solutions. There is little doubt that a great job is being done watching for external security vulnerabilities. Up to this time, no recognizable impact has resulted from a security breach. However, what became obvious, when I attended a SANS Security Essentials course, was that we failed to focus effort on our own internal controls. Further research into this hypothesis was reinforced by a document created by the National Institute of Standards and Technology (NIST). Publication 800-27 titled Engineering Principles for Information Technology Security (A Baseline for Achieving Security). It lays out some generally accepted principles to benchmark sound security practices. It states that although most of the principles center on technical controls, good security design must also take into account policy, operational procedures and user education. By considering all aspects, a layered approach to implementing security measures or "Defense-in-Depth" can be accomplished.

> By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, layered protections enables effective protection of information technology for the purpose of achieving mission objectives. [1]

The importance of implementing a defense-in-depth approach to security is underscored by our voluntary early implementation of the North America Electric Reliability Council (NERC) Security Guidelines for the Electricity Sector. These guidelines identify critical infrastructure in the United States, Mexico and Canada and emphasize the interdependencies of these infrastructures. The guidelines cover nine general categories including: Vulnerability and Risk Assessment, Threat Response Capability, Emergency Management, Continuity of Business Processes, Communications, Physical Security, Employment Screening, Protecting Potentially Sensitive Information, and Information Technology/Cyber Security. For the first time regulatory agencies such as NERC have included protection of Information Resources in the definition of electric system "reliability".

> [Cyber Security] mitigates the threat from inside and outside the organization. Consideration should be given to computer network monitoring and intrusion detection, placing particular attention on EMS, SCADA, or other key operating systems. It is advisable that only authorized persons have access to those critical systems, and only for valid purposes. Consideration also should be given to adequate firewall protection and periodic audits of the network and

existing security protocols. Third-party penetration testing may be useful. [2]

The post 9-11 environment and the continued threat of terrorist acts are to be considered when calculating our risk. This utility holds massive amounts of key infrastructure not included in the NERC guidelines. Natural gas supplies, Water treatment and distribution, and telecommunications could be greatly impacted by malicious attacks from both the inside and the outside. Not only would revenue be lost from downtime, but public safety would also be at stake.

Establishing the Weaknesses

Security Policy and Awareness/Training

A few stray policies for e-mail and Internet addressed the intent of use, right to privacy, and user responsibility, but no broad information security policy existed which first defined an information resource and then second outlined user expectations and enforcement. According to the Generally Accepted System Security Principles (GASSP) as established by the International Information Security Foundation (I^2SF), the Accountability Principle (2.1.1) says that information security accountability and responsibility must be clearly defined and acknowledged.

> Accountability characterizes the ability to audit the actions of all parties and processes, which interact with information. Roles and responsibilities are clearly defined, identified, and authorized at a level commensurate with the sensitivity and criticality of information. The relationship between parties, processes, and information must be clearly defined, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable. [3]

In conjunction with the lack of a broad security policy, we had not conducted Information Security awareness or training. We lacked a plan for educating our users on their responsibilities and recourse for their actions. No curriculum or training plan existed. Management had never been approached on the need for such training. Principle 2.2.2 Education and Awareness of the GASSP states that:

> Management shall communicate information security policy to all personnel and ensure that all are appropriately aware. Education shall include standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply. [3]

It is nearly impossible to hold employees accountable for secure behavior when they don't understand the consequences. They are also at a greater risk of causing others to violate the policy. For instance, a supervisor who requests a subordinate's password to access a system or perhaps a co-worker e-mails a web link to download some unauthorized, unlicensed software. Absence of user training is also a factor in successful Social Engineering attacks by those intending to access restricted information.

Access Control to Information Resources

Another major weakness was in managing access to information resources. There was an inconsistency in the process between organizational areas responsible for access management. Some of the systems were managed by Network Operations and others were by IT Security. There existed no central identity management of a users total access to applications and directories. Therefore, no systematic, periodic audit of a user's access, in respect to their job requirements, existed. It is safe to assume that the principle of least privilege was not being implemented. This principle is based on the understanding that a user should have access to perform only what their job responsibility dictates and nothing more or less. It can also become time focused in that the access granted is maintained only for the duration of the task.

The magnitude and urgency of these weaknesses were continuing to increase due to changes in the local political climate. A shuffle in top management occurred, company owners decided to do a salary and benefits survey to justify cutting benefits, and several rate increases were being planned over the next five years. Community support for the utility was waning. Employee morale, which had historically been extremely high, was in risk of decline. If the company elected to ignore the current state of internal security, we risked compromising all of our security goals.

Implementing the Solution. (Hard-boiling the egg)

Information Security Policy

The first steps in hardening the interior came in the form of an Information Security policy. Both the Director of IT Security and myself set out to draft a policy. We researched several sites to educate ourselves on what this policy should contain. One of the best sites we found was RFC2196 Site Security Handbook [4]. The author, Ed Fraser, points out that the policy will have to balance between "services offered versus security required", "ease of use versus security controls", and "cost of security versus risk of loss". He also goes into detail on the components of a good security policy, which we used as a checklist to ensure we covered all that we should. This policy is only the first of many. It is the cornerstone for the other policies and will be referred to in them.

The first issue our new policy addressed was the expanded meaning of Information Resources. We included paper and printed records, microfilm,

electronic communications, voice mail, e-mail, data, files, software, and the entire contents of any company computer system, corporate network, or personal computing devices. We also wanted to expand the meaning of "user". The company up to this point only considered users to be actual utility employees. Recently, vendors and consultants were doing more with our IT resources so we took this opportunity to expand the policy's audience to include anyone who reads, enters, or updates Information or accesses Information Resources. This includes, but is not limited to, any permanent, temporary, or part time employee; contract employee; or non-employee using the company's Information or Information resources. The users of company information resources have no expectation of privacy because the company declares ownership of it entirely in the policy.

Our policy assigns Information Stewards to approve access. An Information Steward is the person(s) responsible for the business use and results of the information under their control. Once access is approved, the users are compelled to adhere to the password management guidelines, which were already in existence. It is stated that the user's password is considered the same as their written signature and the user is expected to take steps to prevent anyone from gaining knowledge or use of their password. There are also Intent of Use and Disclosure of Information sections in the policy, which covers the risk of unauthorized access.

For the first time, we addressed the issue of copyright law as it pertains to software licensing. Users are to check on available licensing before installing anything onto a company computer. The policy specifically prohibits any personal software be installed on a company computer and/or company software be installed on a user's personal computer. The policy provides for IT personnel to audit the company software installed and also to remove it if no license is obtained. A new process was put in place where the IT Security department would enforce this provision when a violation was reported by the Desktop Support Center. In the past, there was reluctance to enforce this because the Support Center's focus was customer service not policy enforcement.

The policy covers user responsibility for physical security. Users are to secure information resources at all times when left unaccompanied. They are to leave all computer screens locked with a password-protected screen-saver. In the past, common user conduct was to leave the screen-saver to launch when a time-out was met. The time-out can be easily extended with just a simple move of the mouse enabling a browse-attack.

Finally, the policy holds users responsible for information integrity stating that they may not knowingly record any false, inaccurate, or misleading information. It also addressed the company's right to monitor activities without notification and the right to enforce the policy. Enforcement may result in disciplinary action up to and including suspension, termination and/or legal prosecution. When a user

discontinues their relationship with the utility, there is a “no touch” policy for information resources.

The drafted policy followed the normal company approval process. An Executive committee along with the Legal and Human Resources departments reviewed and approved it with very few modifications. Once we received the approved version, we posted it to the company Intranet site for easy access. Because this policy is one that has to be signed and it applies to nearly every employee, we determined that it would be a great mechanism to begin security awareness training.

Security Awareness Training

When I set out to design a security awareness program, there were some obstacles to face. The diverse workforce was not very technical-aware and not much interested in the topic. Furthermore, they are overly trusting of their co-workers and less trusting of the Security department in IT. Common misconceptions about Information vulnerabilities held by most users included:

- Attacks come from the outside and we have firewalls for that.
- People who call for information are who they say they are and I must provide it.
- Employees have all had a background check so I can trust them.
- My password is safe because I have it hidden under my calculator.
- You’d have to have a gun to get in here to my computer. (Said by a user who is located in a locked down facility, but the machine is attached to the corporate network.)

I choose the instructor led style of teaching with a power-point presentation to follow. This helps the group to ask questions and receive instant feedback. If there is an issue raised in class that I cannot adequately answer my research is done quickly and a message is sent back to the participant. I try to make the class entertaining and informative. We review the new policy and I present several scenarios where real exploits have occurred or could occur. Lots of graphics are used in the power-point presentation and I used humor whenever possible. My main objectives in the training were to help users understand that first, the risk is real and the stakes are high. Second, the IT Security department is responsible for protecting the utility, not to be obstructive to the user. And finally, security is everyone’s job responsibility. Although we are still in process, all levels of the company will attend the training including the CEO. For higher level executives, I offer one-on-one courses if they prefer. The curriculum is customized slightly considering the audience.

When the course is completed, a handout containing the presentation is given as reference material. Also an evaluation survey is completed. I find that these

surveys help me to continue refining the presentation and material to better reach the audience. Finally, a security trinket is provided for their attendance. Cyber Mirrors are available from Security Awareness Incorporated [5]. They attach to any surface, preferably the computer monitor. They are a simple oval mirror that reads: "Who's responsible for IT Security?" They are less than $2 a user and hopefully serve as continual awareness.

User Access Control

SANS Security Essentials course acquainted me with the principle of least privilege. Jeff Langford wrote a vary comprehensive paper entitled "Implementing Least Privilege at your Enterprise."[6] He fully defines the principle with some great research. He likens the concept of least privilege with the financial world's "separation of duties" and says that it doesn't always implement smoothly.

> Implementing least privilege will undoubtedly meet with some resistance from both management and staff. In some cases the restrictions associated with least privilege conflicts with the natural desire to be helpful and get the job done in a timely fashion. However in some cases the resistance can be answered by pointing to widely accepted best practices and information technology security standards.

He was absolutely correct when we tried to implement this principle we did meet with resistance. We continually cite best practices and have begun putting probabilities of certain breaches into our justifications for process change.

Network Access

Network Operations department provided all user management for network and remote access accounts. IT Security requested all maintenance through them. In many cases, Networking could not provide documentation as to what a user in a particular group had access to do. To compound matters, the directory services has no central reporting system to give a complete listing of what directories a user can access. This fact alone makes user-access audits difficult to perform adequately.

Due to time constraints on Network personnel, user accounts had not been audited in *years*. Because this is a common avenue for a hacker to access an internal network through an unused account, or for a user to browse in unauthorized directories, I conducted a user account audit where each account was tied back to the Human Resources system. In the process, eighty-three unused accounts were removed.

Application Access

For applications like e-mail and Internet, the IT Security department manages access after obtaining a department manager's approval. For other applications,

approval is received from an Information Steward. Security maintains a log of application accesses by user in an Access database.

Standard procedure is to conduct an annual audit of users and their accesses to identify any pending maintenance. Again due to a lack of IT Security personnel, some of the applications had not been reviewed for many years. First, I reviewed the Information Steward list and revised it to reflect the current organization. Next, I conducted audits on the oldest systems. One audit of a work force management system resulted in one hundred and twenty five unused accounts being removed. Not all of the deleted accounts were terminated employees; some had just changed positions and no longer required access to the system. Apparently these job changes either predated the logging function or the process of Human Resources notifying IT Security of job changes.

After the system-based approach to auditing accesses, I looked at some of the employee's total access based on their job responsibilities. This yielded enough common results to set some standards based on job title. There is a lot more work to be done in this area.

The utility is relying more on vendors and contractors to do system implementations and maintenance so we did some process changes to capture information about their coming and going. We track their access and we apply a time limit to them. A utility employee is assigned to act as a communication liaison and to obtain a signed Information Security Policy agreement from each user employed by the vendor. These user accounts are reviewed monthly.

Current State (Hard-Boiled and Keeping it Fresh)

Security Policy

By implementing the new Information Security Policy, we now have the mechanism in place to hold users accountable for their conduct as well as establishing clear expectations for the handling of company information. We have increased the defense against breaches in confidentiality. Users are locking their computers and stowing or shredding documents. Breaches in integrity are addressed in the Information Integrity section of the policy and now the company has recourse for violations. The security goal of Availability has been reinforced with the recognition of Information Stewards and their role in approving application access and audit of application users.

The definition of Information resources has greatly expanded beyond data in a database and subsequently our role as a Security department now goes well beyond parameter protection. We will continue to develop policies to cover other areas and work to test and revise the current policy as necessary. The utility's management remains supportive of the IT Security department's dynamic needs.

Awareness Training

The simple act of communicating the new policy in a face-to-face exchange has brought about some great new champions of security. Each class taught yields a new fan of protecting our utility and they are infectious to those around them. I now have calls from users "reporting" on security issues. Maybe a co-worker is using someone else's password or a user receives a suspicious inquiry from outside as to what technologies we deploy. One user called to request her own network account because she was using a shared network account also used by others in the same job position. In the future all of the shared accounts will be removed, but it proves users are paying attention when they request it first.

Awareness training has not been all roses, however. There are and continue to be challenges. First challenge is staffing. In order to do awareness training for this utility, over 50 classes must be scheduled and conducted. When only one or two instructors are sharing this load it can be grueling. Second challenge is the few users who have a hard time seeing the value in security. We have not completed rolling out the training, but we will, at some point, be faced with a user who refuses to sign the policy. It will be up to management how far to take the matter.

Implementing this and future policies has its challenges in the details. The lower you go on the company organization chart, the more educating has to be performed to prove that the risk is real and it exceeds the extra administration required to conform with the new policies. Also, it becomes harder not to be portrayed as the bad-guy enforcer, but rather the good-guy protector and enabler. There must be a parallel marketing effort to mitigate this tendency. User buy-in and participation is critical to true layered security.

The final on-going challenge is how to keep the awareness fresh. Designing a continual, informative curriculum that balances adequate information without overloading or creating paranoia. There is a fairly low-priced poster subscription available through Security Awareness Incorporated [5]. They send different posters each month covering topics like: Password Construction, Telephone Fraud, Viruses, PC security, Social Engineering, and Identity Theft. We also plan to do some management by walking around different areas observing user conduct.

Access Control

Great advances were made in centralizing, documenting, auditing and organizing the user accesses. It has been recognized as an IT Security function and not a Network Operations function and the responsibilities continue to transition to our department. IT Security personnel look at each access request with separation of duties and risk management in mind not customer service.

System-based and user-based audits yielded a better defense-in-depth against breaches in confidentiality and implementation of the principle of least privilege.

In the future, more granular data classification and its appropriate handling will be a subsequent challenge in this area. Finally, the future may see the acquisition of an automated identity management tool as opposed to the more manual process that exists today.

Currently a rough debate is ensuing in the IT department on the role of System Administrators. With a finite headcount, it can be difficult to separate duties as much as required to mitigate the risks. We are attempting to redesign the way developers and administrators are organized as well as looking into the job descriptions and role each plays in the system life cycle. Although it is not our primary responsibility, it is encouraging that the IT Security department is now involved in the discussion.

Conclusion

The utility's focus on security has experienced a paradigm shift from emphasis almost exclusively on the external facing systems and parameter to a more global view of protection. It is a migration to a defense-in-depth philosophy. In order to achieve the change in focus, we chose to begin with a security policy followed by awareness training and finally to tighten controls on information resources through implementing the principle of least privilege. Our job is nowhere near complete. We need to continue to look for threats and vulnerabilities both inside and outside.

We have approved budget funds for third-party penetration testing as well as our first ever audit by outside auditors. We are looking forward to prioritizing our largest vulnerabilities as well as proving to our users that we are providing them value. Included in our near term plans are to create an overall business plan for IT Security in hopes that it helps justify our projects and priorities to management.

References

[1] Stoneburner, Gary, Hayden, Clark, and Feringa Alexis. National Institute of Standards and Technology (NIST) Special Publication SP 800-27. "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)". June 2001. URL: http://www.csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf (20 November 2003)

[2] North American Electric Reliability Council. "Security Guidelines for the Electricity Sector". June 14, 2002. URL: http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf (30 November 2003)

[3] International Information Security Foundation. "Generally Accepted System Security Principles". Version 2. June 1999. URL:http://web.mit.edu/security/www/gassp1.html#download (22 November 2003)

[4] Frasier, B. Ed, "Site Security Handbook." September 1997 URL: www.ietf.org/rfc/rfc2196.txt?number=2196. (30 November 2003)

[5] Security Awareness Incorporated. URL:www.securityawareness.com (30 November 20003)

[6] Langford, Jeff. "Implementing Least Privilege at your Enterprise". July 5, 2003. URL: http://www.giac.org/practical/GSEC/Jeff_Langford_GSEC.pdf (30 November 2003)

Other References

SANS Institute. "SANS Security Essentials". SANS Online Training. 2003. URL: http://www.sans.org/onlinetraining/track1.php (25 November 2003)

Wilson, Mark and Hash, Joan. National Institute of Standards and Technology (NIST) Special Publication SP 800-50. "Building an Information Technology Security Awareness and Training Program". April 2003. URL: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf (30 November 2003)

Last Updated: May 28th, 2018

Upcoming Training

SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS Bethesda SEC401 @ USO - Academy	Bethesda, MD	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
SANS Malaysia 2018	Kuala Lumpur, Malaysia	Jul 16, 2018 - Jul 21, 2018	Live Event
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Bethesda SEC401	Bethesda, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Riyadh July 2018	Riyadh, Saudi Arabia	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC401: Security Essentials Bootcamp Style	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive