Global Information Assurance Certification Paper

SANS GSEC Practical

Dallas Babineaux
GSEC Practical Version 1.4b (1)
05/02/2003

Physical Security & Social Engineering

Table of Contents

Abstract

This paper discusses the security risks presented by imposters and various other attempts at gaining unauthorized access to computing devices such as laptops, PDA's, etc. and the challenges that IT Security personnel face in trying to protect data on such devices. This paper will also discuss some preventative measures that should (if not already practiced) be implemented into your organization as soon as possible.

Introduction

Of all things related to the securing of corporate and personal security, there is one factor that will always be an issue. No matter how sophisticated a computer program or interfacing technology may become we will always be faced with the problem of "people".

When I say, the problem of "people", I am referring to the fact that we are – human... As Kevin Mitnick has so aptly demonstrated (both in life, and in print) People will always make mistakes in trusting those who should not be trusted and/or inadvertently enter incorrect data into computer systems. The issue only gets worse when actual "physical" security coupled with a lack of education concerning Social Engineering is factored into the problem. This paper won't delve into the technical issues… I won't talk about getting past your firewall to gain access to what I want.. I won't need to, if I can get the password, or get your helpdesk to reset my password to my Social Security Number or other "well-known" item I've got all I need…

Who's going to stop an authenticated user?

This paper will deal with two aspects of physical security:

1) The actual physical security of your computing infrastructure
2) The art of Social Engineering.

These two issues will be intertwined throughout this paper because of the very nature of this type of intrusion attempt.

Physical Security

I will begin this paper by addressing the issue of physical security, because even if your staff has been well trained and knows how to handle "out of the ordinary" situations and understands the very critical nature of data security. All

will be for naught if your systems aren't physically secure. Take a moment to think about the security of not only your servers, but also your workstations & PDA's. Even cell phones can be used to glean valuable information from your on-board phonebooks which more than likely contain the names of management and other points of contact.

Many organizations have already realized this problem, and have gone to great lengths to protect their systems by using such things as controlled access, security cameras and roving guards.

There are many companies that have sprung up in recent years in an attempt to address this situation. Companies such as "Stop Theft" which provide tamper proof labels that "tattoo" your computers when removed by using an indelible ink. And other companies such as "Secure Services" which sell products to lock your computer down to the surface of your desk or floor by utilizing a bolted down steel plate.

Although locking down equipment is an excellent start, we all know that this alone will not deter all cases of attempted theft. The foundation of Security starts with the individual employee. Proper training concerning Physical Security and Social Engineering can and will make a difference in your organization. It isn't simply a matter of creating a very secure password, it's more of a mindset - I almost hate to say it, but it's a mindset of "distrust". This training should start as early as the initial hiring orientation session if possible. But, if that's not (or hasn't been) the case, it's better to start the training process sooner than later. In regards to my "distrust" statement above, most businesses are in a particularly awkward position… since the main focus is "customer satisfaction" - being as helpful, courteous and polite as possible. This tends to be a delicate balancing act, as you don't want to appear hostile towards your legitimate customer base. When dealing with customers over the phone, it is simply a matter of training to be able to ask particular questions in a friendly and casual way as to not irritate or harass the person you're dealing with.

Human Nature

The fact of human nature is that we all tend to take the road of least resistance… Especially if a repairman were to come in the door 15 minutes before quitting time on the Friday before Labor Day weekend... How difficult is it for security personnel to locate someone in charge of allowing this person into the building? If it takes the Security personnel more than a few short steps, you might well know that there is a much higher chance that the person will indeed get the access he/she is looking for. Especially if this person has a "quick" errand to take care of, like swapping out a network interface card or "replacing" a workstation or server. Have your security personnel been trained to understand that attempted break-ins will be more focused at these sorts of times? Times

such as Holidays, Friday evenings, and possibly even right after a major company event, (when your security staff is worn down from the constant onslaught of access verification) these would seem to be prime times for unauthorized access attempts.

Human nature dictates that our level of vigilance degrades after constant stimulation. What are you and your company doing to prevent these lapses from "spoiling" your day? Once safely inside the building, Is there any way to control that individual? Or will he/she be allowed to roam the halls with a visitor badge all day? Can your wiring be easily accessed by a "repairman", or do they have to go to greater lengths to gain the needed access. Does your organization have policies on handling outside maintenance vendors? Do your work areas have locking drawers? Has your staff been trained to avoid leaving things such as network diagrams, phone lists, passwords out of sight and locked up?

When's the last time you as your companies Security representative put on your "bad guy" hat and walked through your organization looking for proprietary or confidential information? You don't have to go digging around in people's desks, but on the other hand a network diagram should not be hanging on the wall with server names and roles tagged all over it.
What about your paper waste? Does it get cross-cut shredded? Is there some way to control the access of information via dumpster diving? How adept is your IT department at locating unauthorized equipment? How well do the Security personnel understand the ramifications of unauthorized access? Do you have an EASY to understand policy? As you know, I could go on forever... The important thing is that we all realize how simple it would be to do a lot of the things previously mentioned.

Minimum Effort Required

When you consider how much time and effort goes into learning the Security trade, understanding and configuring Operating Systems and learning and implementing best practices, It can be quite unsettling when you realize how little time a social engineer has to focus on perfecting his/her craft. If their attempt at getting access to your organization fails, they simply "drop" the phone and hang up. Usually there is very little to worry about, if you call back they will probably say you have the wrong number. On the other hand, if the person is indeed able to get a password reset by answering all the questions correctly, then your organization is really in a bind. No matter how secure you make your systems, if I have the password, or can convince the IT helpdesk to reset my password to some known value what are you going to do to stop me? I won't trip any alarms, or any log any unauthorized events… I'm an authorized user, and I have all the time in the world (or at least the rest of the weekend) to glean sensitive information from your systems.

As for actually trying to hack into your computer systems, the “script kiddies” don’t even have to have an in-depth understanding of computers and networks in general. They don’t have to spend time looking through technical manuals and trying out all sorts of different and clever ways to break into a system. They don’t event have to understand system and application architecture. All they have to do is check out the hacker web sites and wait for that next big vulnerability to show up so they can be one of the first ones to attempt a break-in. And if they are really impatient, there are several “Do-It-Yourself” hacking sites out there that will allow you to create your own exploit from easy to manipulate tools and GUI front ends.

Hardware Destruction – An easy fix…

Now lets switch gears for a second here and talk about your hardware… I’m going to pick on something easy… I’m sure you’re familiar with the study by the university students that acquired hard drives from Ebay and electronic swaps. http://zdnet.com.com/2100-1103-980824.html These students acquired 158 disk drives for less than $1000 and were able to glean sensitive information from them like over 5000 credit card numbers, medical records, personal e-mails & etc.

What are you (personally) and your organization (professionally) doing to prevent such an event from occurring? I don’t know about you, but after I heard about the study I made it my personal policy that NO hard drive will be leaving MY house intact… It will be removed and completely destroyed before it leaves my house or gets thrown into the dumpster. How about your systems at work? Is there any REAL reason your old systems have to leave the building with the hard drive still installed? Hard drives are cheap, let the new owner go out and purchase one. Besides, your maintenance/computer staff would probably get a kick out of releasing some pent up stress and irritation on some poor old hard drive !

Your Employees??

What about your employees? What sort of policy do you have to screen system administrators? Have you ever stopped to think that we do a credit and criminal background check for someone wanting to rent a house or apartment, but many times we hire individuals into our organization without much more than reading over a glossy resume’ and giving a quick interview… Especially for jobs such as custodians, clerical & secretarial work. Now consider the fact that these persons (especially secretaries) have more access to sensitive information than normal users do!

On the other hand, Custodians usually have all the keys to the entire building, and the turnover rate is quite high. I’m sure we could come up with a thousand

things that this person could get into if they wanted to. This does tend to be a tough situation, and aside from making sure your information is locked away safely, using cameras throughout the building, performing random searches and securing dumpster access there is little you can do.

Insider Theft

We all know that insider theft is greater than any outside risks. It has been estimated that over 50% of any/all unauthorized attempts at data access are done so by your very own trusted employees. So what are you doing to ensure that your internal employees aren't stealing your secrets? Note that even the FBI & CIA have their share of problems – and you would naturally think that they would be one of the most paranoid people in world with information concerning National Security. If secrets can escape these organizations, it would be foolish to assume that it won't happen in your organization.

Now lets discuss ways to answer some of these questions…It's important however to remember that this battle will rage on forever, it's simply a matter of staying (or attempting to stay) one step ahead of your enemy.

So What Can We Do??

Finally we get to the "action" section of this paper. I will outline several approaches that you should (if you haven't already) employ to help mitigate the risks involved in all forms of Security. It is important to note that these suggestions don't only apply to Computer Systems, they are common sense precautions that can (should) be applied to all forms of Security.

I suggest the following strategies in getting a grasp on these issues:

- Secured Building access with emphasis on prevention of tailgating
- "Need to know" basis of company and personnel information
- Least Privileged Model of Security
- Penetration Testing
- Regular Training of Employees
- Easily Understood and Well Documented Access Requirements
- Organizational Audits

Secured Building access with emphasis on prevention of tailgating

Quite simply your building should be secured, not only by night when everyone has gone home for the evening, but also by day… when I say "by day", I'm talking about the fact that physical access to wiring cabinets, servers, routers &

etc. be placed in locked cabinets - Out of sight. In addition, there should be NO network interfaces active in the public “lobby” area. It is also a good idea to have security camera’s installed at the door to your server room.

“Need to know” basis of company and personnel information

This point goes hand in hand with the next point, in that your organization should have an easy to understand policy concerning what level of security clearance is needed to access certain portions of data. Quite simply, if there isn’t a “need to know” then you should not have access to that data.

Least Privileged Model of Security

It has become standard and approved industry practice to employ the “Least Privileged” model of security. This policy should be approached the correct way, it is easy as a Security Analyst to grow into the attitude of simply rejecting requests because you feel they are asking too much. It is very important that your organization understand that your policy is to provide them with ALL the access they need in order to perform their job duties. The key is that you won’t afford them any MORE privileges than what is absolutely necessary. I can assure you that you will surely get kickback from other units in your organization, but there are plenty of resources on the web that will back up your position and help to make the case.

- All persons with Administrator access should have 2 accounts… One account to perform their normal duties and another account that employs the elevated accesses needed to complete certain tasks.
- Lock down the hours of computer access to groups. This is something that the banking industry has done for years; the bank’s safes won’t open until a certain time in the morning. Microsoft has given us these tools for years, but how many organizations do you know of actually utilize the “allowed to access the system between these hours” settings? Surely certain groups can and should be locked out of the system during off-duty hours.
- Dial-in access should be limited to only a handful of people in the organization actually need this access.
- Registry and File permission should be very closely scrutinized to ensure that only those persons and applications that need Full Access permissions receive it.

When dealing with Auditing & Access permissions, it is important to remember that one group of people should NOT have the authority to both install and administer software. Keeping these tasks separate will go a long way in preventing unauthorized access. The point is that everyone in the enterprise should have “checks and balances” concerning access permissions.

Penetration testing

In my opinion, Penetration testing is one of the most valuable – yet most unused sources of gathering information on the weak spots of your organization. No one (especially the overworked IT personnel) likes to get a report card listing several areas of deficiency. However, there is no better way to truly get an indication of where you stand from a security standpoint and provide a method of tracking your improvements.
Penetration testing should occur at least annually with an official report being sent to senior management and corrective steps implemented throughout the proceeding year.
A good Penetration test will attempt to gain access to your infrastructure in the following ways:

- Social engineering
- Brute force password access attempts
- Modem hacking
- Unauthorized building access

Regular Training of Employees

The results of Penetration tests should (as appropriate) be made available to your organization… This can sometimes be a controversial subject, but it's important to understand that if your organization understands the weaknesses encountered, and how easy it was to break into your systems. It will go a LONG way in getting everyone in the correct mindset. Regular training doesn't have to involve expensive classroom training. It can be as simple as bringing up the topic in weekly team meetings… saying something like "Did you hear about the latest results from the last Penetration Test? -- Someone was able to get access to our systems by doing or saying this or that.. It won't take much time, and will usually stimulate people's thinking along the lines of "I don't want to be embarrassed when I find out that it was me that let someone into our organization by giving out my password to that IT worker…I don't want to be the person that let someone into our organization…" In addition to that, posters around the hallways with Security related reminders will serve to reinforce the message that your company takes this seriously.

Easily understood and well documented access requirements

The documentation for access into your building and how to handle "emergency" situations should be well written and EASILY accessed by your employees. In fact, it should be a part of your initial employee orientation and

training program. Remember, if the documentation is poorly written and a burden to locate and comprehend, it simply won't get followed consistently.

Organizational Audits

Audits are another thing that usually gets put on the back burner… It's hard to justify the time and costs involved. And many departments seem to automatically "push back" on some other unit coming onto "their turf" and snooping around asking a bunch of questions and writing things down on a little notepad. Auditors need to be trained to understand and work to alleviate the fears of other units. To be quite honest, there seems to be a fear of one losing his/her job for doing something wrong during an audit. "We've always done it that way" is something that needs to be re-evaluated on a constant basis. Audits are supposed to uncover overlooked and incorrect processes and provide a checklist of items to be fixed before the next audit. I would suggest that the audit team meet with the area to be audited and explain the purpose of the audit and what will come of the findings. The end result of a good series of audits WILL result in some stress and strain as the organization works to get themselves in a better posture, but in the end, your company will be much more conscience of processes and impacts throughout the corporation.

Something that is often overlooked and should be looked at as a selling point versus a cost issue is the fact that a "secure" company is in a much better position to serve their customers. There will be much less impact with new State and Federal regulation such as HIPAA. And in the very near future, I believe that customers will really begin to focus on the security aspect of a company with whom they are entrusting their data.

Summary

In summary, we as Security professionals must strive to educate those within our organization in order to prevent unauthorized access to our systems. Our employees must be trained to be suspicious of everyone we come into contact with and always follow the rule of "Least Privileged Access". Remember, this rule not only pertains to computer systems, but to Security in general. This is followed closely by taking steps to protect the actual physical access to our systems. If these rules are followed closely, we will have a much better handle on securing our companies most precious asset… it's data.

References

Dacey, Robert F. “Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures”http://www.gao.gov/atext/d03564t.tx (April 2003)

Junnarker, Sandeep “Anatomy of a Hacking” http://news.com.com/2009-1017-893228.html (May 2002)

Chauchan, Abishek.”Do Firewalls and IDS Create a False Sense of Internal Security?” SC Magazine http://www.scmagazine.com/scmagazine/sc-online/2002/article/41/article.html (Sept 2002)

Microsoft TechNet http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/5min/5min-203.asp” (2003)

Mitnick, Kevin The Art of Deception: Controlling the Human Element of Security, John Wiley & Sons, 2002

Website Information

http://www.stoptheft.com/prodset.htm

Information on tamper proof labels to identify stolen systems

http://www.secureservices.com

Information on anchor plates to secure computer systems to your desktop

http://www.dell.com/us/en/bsd/topics/security_001_home.htm

Dell’s method’s and products to physically secure your systems

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor