Global Information Assurance Certification Paper

Security is a 3-Legged Monster
Carl Denowh
December 19, 2000

A hacker might like to picture himself as the romantic figure of a knight in shining armor, charging the corporate monster, and shouting his battle cry, "Information wants to be free!" Well, let's take that picture a little further. That monster is your security. Its job is to protect whatever it is that you consider valuable. Ideally, it will look so scary that the hacker will take one look and decide, "Maybe someone else's information needs rescuing more…." But, no matter how scary it looks, there is no disguising the fact that your monster only has three legs.

The legs are the three types of security you should be worried about: Electronic security, Physical security, and Process security. Electronic security is your defense against most computer-based attacks. Physical security is what you do about the risk of an intruder gaining physical access to your information or the media on which it resides. Process security is the policy and procedures you have in place to maintain the confidentiality, availability, and integrity of your valuable information. If you disable any one of the legs, the monster topples. Circumventing one type of security will often render the other types of security useless.

Security takes money. Your managers see you shoveling money into the monster's mouth, but they don't see anything useful coming out the other end. Your job is to feed your monster enough that it is big and strong enough to do the job, but not so big that you spend all of your money on it. And, while you are striking that delicate balance, you have to keep explaining the need to your management. Is this really the job you signed up for?

All is not lost. You can have an effective monster, make it look scary, and not spend all your money on monster chow. Management, however, is your problem forever. Let's take the monster one leg at a time.

Electronic Security

Electronic security can also be divided into three areas (of course): Networks, Hosts, and Applications.

You protect your networks with firewalls[1], but you also want to make sure your firewalls are current, effective, and operational. Security and computers are changing fast. Those pesky little hackers are a slippery bunch. They keep adapting to the new stuff without abandoning the old. If you don't keep up with the latest patches and updates the bad guys are likely to notice. How do you know what you need? That's where penetration testing comes in. Many companies hire people to attempt to break in and find the vulnerabilities. There are a number of tools to help you do this yourself. Be careful, however. You want to have permission if you are doing this yourself. If you hire someone else, you want to be sure the people you hire are honest. It would be very embarrassing to pay a hacker to find your vulnerabilities and find out that he not only found them, but also used them.[2]

Hosts include network devices such as routers and, yes, the very firewalls you are using to protect your network. Host security includes such things as operating system patches, passwords, permissions, and protocol controls. Essentially, you want to be sure that all accesses to a host be by the proper users, in the proper manner, and limited to the proper areas.

Applications are your nemesis. They exist to make your job complicated. Without them, users would not need access and we could all go home. Unfortunately, management frowns on not allowing applications. We can, however, keep patches up to date, keep access control lists up to date, and separate as much as possible to reduce our exposure when (not if) something goes wrong.

Metrics are your friend. Okay, let me qualify that. *Reasonable* metrics are your friend. Metrics should not be recorded for the sake of having metrics. Every metric should have a purpose. They should tell you when your security is or is not working, assist in resolving a specific problem, or justify your existence. That last is because management is going to want to know that their investment is paying off. Keep the metrics to a minimum.

Logging is also your friend. Make sure you are logging enough information that you can find out what happened, when, how, and how much was compromised. Logging, of course, comes at a price. Servers will experience noticeable performance hits if you turn all logging on. Try to reduce your logging to only what is useful in your production environment.

Physical Security

So, you have a system with BIOS passwords, personal firewall, passworded screen savers set to 15 seconds, and a retina scanner. Are you secure, yet? The janitor doesn't care about all of your electronic security. He simply pops out your hard drive and sells it to your competitor.

Technical people tend to forget about the mundane approach. Imaging the eruption at a certain large company when they learned that a competitor was sending people into their sites in the guise of copier maintenance personnel and taking copies of sensitive documents from the copy centers.

You need physical security. You need multiple perimeters with different levels of security such as your building, your lobby, your server room, and your system cabinet. You need access controls like locks, doors, and walls. You also need a dose of reality. Who can you trust? At least half of all intrusions are from internal personnel.[3] You need to restrict access as much as possible without inhibiting legitimate work.

Process Security

Process security includes the procedures your company follows to insure the security of your information. Procedures rely upon policies, so your process security must also include your policies.

I once discovered a serious flaw in the procedures of a company where I worked. So, in my usual reserved way, I drove the point home by picking up the phone in front of everyone and asking the help desk for a root account on all of the systems that are involved in money. Of course, there were controls. My manager had to be notified of my request and could revoke those accounts whenever he liked, but by the time he read the email notice, it would be far too late.

The point is that policies and procedures must be in place to *effectively* protect everything worth protecting. Policies and processes should address updating security (i.e. passwords, patches, and the procedures themselves), granting access, limiting access, removing access, employee awareness (your main defense against social engineering), disaster recovery, and protecting data (i.e. encrypting email, locking doors, and checking logs).

But, Wait! There's More!

Okay, so now you have a monster with three sturdy legs. Is it effective? Of course not! You have a monster to protect your information, but will he detect the crisis when it gallops past? How will it respond? It needs eyes and big nasty teeth and claws.

For security to be effective, it must have effective mitigation. Mitigation is how you deal with risks. In other words, mitigation is your monster's name. To be effective, mitigation must cover Protection, Detection, and Response. Protection is covered fairly well with the three legs of your monster, but you still need detection and response.

Give your monster eyes by implementing intrusion detection. Imagine a bank with an enormous vault and highly trained police standing by night and day. If there is no alarm system or on-site patrol the bank robbers can count on plenty of uninterrupted time to get through the vault. Intrusion detection systems can include alarm systems, host and/or network based intrusion detection systems, and educated personnel who know to report anything unusual.

The prospect of response is fun, but the reality tends to be tedious. You will need to take the large number of alerts and determine which are real threats, which are false alarms, and which are simply too minor to worry about. Response requires processes in order to be effective.[4]

Response should have the following priorities in the following order: Protect the information, prevent a recurrence, and neutralize the source. Protecting the information is no surprise. Preventing a recurrence is an obvious need, but often overlooked in favor of the last priority. Neutralizing the source should be the last priority, but is generally considered the first by beginners. It requires *correctly* identifying the source, and responding in such a way that the source is unable to repeat the threat. This is where you have the most opportunity to spend money. The cost of intrusion detection systems and the personnel to efficiently respond can be astronomical. You must focus on your first priority of protecting the data and often let the perpetrator get away.

Please remember that response must also be legal. Hackers disguise the true source of attacks so a response will be directed at the wrong target.[5] An unreasonable response could be embarrassing and an illegal response could be a career-ending move. Try to remember you are supposed to be the good guy. An acceptable response will include a legal expert when the source is identified, and will usually be out of the hands of the security person.

So now you have a complete monster. Next comes the hard part: convincing management….

Sources

1. Williams, Jim. "The Threat From Within." 4 May 1998. URL: http://www.netsecurity.about.com/compute/netsecurity/library/weekly/aa050498.htm (4 May 1998).

2. Saunders, John. "Beware of wolf-like hackers in sheep's clothing; An emerging problem is that law-breakers are often the very experts that are being consulted." 9 Mar. 1998. URL: http://www.findarticles.com/m0CGC/n9_v24/20394387/p1/article.jhtml (4 May 1998).

3. Miora, Michael. "Stop Signs, Barricades and Firewalls: Protecting your Systems on the Internet (excerpt)." Dec. 1996. URL: http://www.miora.com/articles/art-protecting.htm (4 May 1998).

4. McGuire, David. "Mitnick On Net Security." 3 Mar. 2000. URL: http://www.computeruser.com/newstoday/00/03/03/news8.html (4 May 1998).

5. Schwartau, Winn. "Cyber-vigilantes hunt down hackers." 12 Jan. 1999. URL: http://www.cnn.com/TECH/computing/9901/12/cybervigilantes.idg/ (4 May 1998).