Global Information Assurance Certification Paper

The First Trend of Security Initiatives

GIAC GSEC
Practical Assignment
Version 1.1
Option 1

Khoa Nguyen
Garland, TX
2/8/05

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract

Our public and private daily operations depend heavily on a network of systems. The well-being of a single node could effect a city a thousand miles away. For instance, the recent power outage in New York City was caused by the power grid problem in Texas. For years, we have neglected to recognize the interdependencies of these systems and overlooked the security vulnerabilities they might have. After the September 11th terrorist attack, computer security became more recognizable and our government and private sector started taking steps to strengthen our critical infrastructures. This paper will look focus on what has been done within the computer industry to promote computer security awareness through different initiatives. It will also focus on the target audiences of those initiatives and the effectiveness of the various campaigns. In the process, several ethical issues relating to security education will be raised.

Executive Summary

As our technology progresses through the information age, the majority of our critical infrastructures, both private and public sectors, are now operating as online control. The interconnection between the sectors is evident through the network of communication. This emergence provides an incredible amount of opportunities; however, it also brings along a number of vulnerabilities and risks associated with the technology. A system power grid failure in Texas might cause a blackout for half of the New England states [1]. An intruder to Newark airport's main control system might cause air delays for Continental airline around the world. In addition to outsiders, the system is also vulnerable from attacks initiated from insiders, viruses, worms, and other cyber attacks. Since the interconnectivity is so integrated, the magnitude of impact also increases.

Since networks communicate using the Internet, "attacks can originate from anywhere as more and more people have access to the Internet and other public-connected networks" [1]. The tools used to launch cyber attacks are relatively inexpensive or can be easily created by an experienced programmer. The worst part is that there are not enough qualified professionals in the industry to detect and respond immediately to these attacks. Also, there is no established method of spreading alerts to the rest of the country. Finally, many infrastructures have low security measures, and some are not aware of such security holes.

There is no such thing as absolute security. It is a moving target because of the nature of computer technology. One of the essential security practices is the security-in-depth. The security-in-depth concept states that one wooden stick is easy to break; however, if you combined multiple sticks, it is much tougher to

break. The information infrastructure that needs to be protected is like a king in the castle. First, everyone needs to recognize that his security is very important to the well-being of the nation. Secondly, the king is safer if the castle is built properly and has strong walls. Thirdly, the king is safer if there are multiple barriers of guards protecting the castle and protecting him when he travels. Finally, there needs to be a back-up plan in case all of the barriers failed and the king is been captured or killed. This scenario is very similar to the computer security logistic, which includes identification, detection, prevention and recovery.

The understanding of those logistics has a great impact on the level of information security. Most security incidents could be avoided if users recognized that systems are subject to flaws and applied patches whenever possible. This suggests that security awareness has a great impact on the overall security of the system. This paper will look further into what has been done throughout the computer industry to boost computer security awareness. It will also distinguish the different motives, intended audiences, and the success of each program.

Security Initiatives

Black Ice – October 2001

Black Ice was an emergency planning exercise for the 2002 Winter Olympics in Utah. The exercise was conducted by the National Security Agency and the Department of Energy, which collaborated with regional gas, electric and telecommunication companies. The total participants were 225 people and more than 65 organizations.

The simulation was based on an ice storm, which caused a disruption of utility computer systems producing a regional blackout, Internet outage, cellular overload, and telephone failure. It demonstrated how overwhelming the physical and electronic attacks have on the power grid, effecting everything that we depending on for our daily life. The scenario was based on the September 11th attack, and it made a strong case that future terrorist attacks could be worse if they included a major cyber disruption [2]. It helped to build awareness of infrastructure vulnerabilities and interdependencies. It identified the important infrastructures and the challenges they might encounter when trying to restore the entire system.

The result of the Black Ice exercise was an action plan that included an incident prevention plan, a protection critical infrastructures plan, and solutions to communication issues between different entities. The initiative led to Black Ice

phase II that will focus on details of each of the critical entities and propose ways to strengthen the security.

Blue Cascades – June 2002 & September 2004

Blue Cascade I was the first bi-national critical infrastructure protection exercise hosted by the Pacific Northwest Economic Region, along with the US Navy Critical Infrastructure Protection Office, FEMA Region 10, and the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness. It included both private and public sectors. It was necessary to have both nations participate in the exercise because nearly 80 percent of Seattle's natural gas is from Canada [12]. Similar to Black Ice, Blue Cascade's goal was to determine which assets must be protected and to enhance recovery and mitigate the effect of a disruption regardless of whether it was from terrorist or natural causes.

The result from this exercise demonstrated how little the participants knew about how their infrastructures interacted with each other. In most cases, the company was reluctant to consider other's failure as part of their security vulnerability. There were major security awareness fluctuations between major participants as well. The initial response to this issue was to allow the entities with better security programs to share their knowledge and security guidelines to the less mature entities [9]. Another problem between the two nations was the inconsistency with their alert systems and the terminology when referring to incidents. This exercise encouraged the two nations to collaborate their efforts to improve the security of the interdependent systems and also to agree on the common incident terminology. There was also an agreement for a vulnerability assessment to be conducted to help clarify the independencies and determine where the critical nodes for each technology were located and where they overlapped.

Blue Cascade II was created to expand on the findings of the previous exercise. Its goal was determine contingency plans in the event of the loss or damage to electronic systems and was based upon the most important findings of Blue Cascade I. Consequently, Blue Cascades II focused on the Information Technology (IT) dependencies where resources were required to communicate, continue business operations, and execute recovery plans. It also examined specific cyber security vulnerabilities that could impact operational systems, such as the *Supervisory Control and Data Acquisition (*SCADA) system and other electronic processes. This information could then be used to help the public and private sectors better understand the magnitude of disruption an IT shortfall that could cause.

Silent Vector – October 2002

Silent Vector was a two-day national security simulation to challenge government leaders to respond to the pre-attack phase of major terrorist assaults when there is not enough information for effective prevention. The exercise was developed and produced by the CSIS (Center for Strategic and International Studies). The goal for the exercise was to aid the leaders in improving the effectiveness of response during the pre-attack phase, which focuses primarily on the energy sector. The participants of the exercise were presented with a scenario, and they were required to determine whether or not the information provided was from reliable sources, to conduct a break-down analysis on the scenario, to identify vulnerabilities and impacts, and finally develop a security measure to deal with the situation prior to the attack and afterwards, regardless whether or not the attack occurred [4].

The exercise revealed the behavior of government agencies when the information was vague, and it also showed how the public reacts when the government does not have concrete information on such attacks. In most cases, rumors will become fact, and truths will become distorted [10]. It also pointed out that reactions on ambiguous alerts also helped attackers to achieve their goal of causing disruption in the US economy. It is difficult to justify the accuracy of attacks because most of the time, pre-attack information is leaked to the public. The security procedure for the energy sector was not designed to handle terrorist attacks.

Similarly to other exercises, the Silent Vector exercise encouraged the participants to join forces with each other to improve their interdependencies and strengthen security measures for each entity.

TopOff2 –May 2003

TopOff2 was also known as “Top Official” exercise. The Homeland Security’s Office of Domestic Preparedness and the Department of State sponsored it. The exercise was set to demonstrate an attack from multiple locations: Seattle and Chicago. Its purpose was to emphasize how critical it would be if there were a series of attacks from different locations. It gave health workers and agencies a practical in responding to a terrorist attack and was used to assess their readiness, to uncover planning gaps, and to remedy those gaps [11]. For this exercise, the participants from Chicago had to deal with a deadly and highly contagious biochemical attack, while the group in Seattle had to neutralize a dirty bomb attack. The local attack could potentially become a global attack because the virus had the capability to transmit through air using international travelers as its agents. Victim would be dead if they failed to take antibiotic treatment within 18-24 hours of exposure [11]. Conceptually, the

victims would have symptoms similar to common cold or flu. The accurate diagnosis might take a few days to confirm. The first wave of victims would be dead by the time the diagnosis was completed.

This exercise included more than 200 public and many private agencies from the United States and Canada. In Chicago, more than 140 area hospitals participated in the exercise. They were either part of the tabletop exercise or the physical drill. The total number of participants was close to 8,500 people, and it cost nearly $16 million to conduct the exercise. The TopOff2 exercise was the most comprehensive terrorist response exercise to date. The exercise was conducted with a variety of techniques. The most distinctive feature between TopOff2 and other exercises was its computerized capability. The system with artificial intelligence created scenarios and prompted participants for responses. The following phases of the scenarios totally depended on the decision of the participants. The exercise required the participants to make real-time decisions. This dynamic characteristic made the system very realistic. This simulation was part of the ESD Program from Dartmouth University [6]. In addition to the computer simulation exercise, participants also took steps to develop an incident containment response plan to minimize the impact of the attack due to its biochemical nature.

Dark Screen – September 2002

Dark Screen was inspired by the September 11th attacks, and Congressman Ciro Rodriguez (D-TX) used this exercise to challenge the ability of San Antonia and Bexar County to prevent, to detect, and to respond to cyber terrorism.. It was the combined effort of the University of Texas at San Antonio, the City of San Antonio, Air Force's Air Intelligence Agency and Bexar County. The Dark Screen exercise was composed of three phases: tabletop, development and implementation, and live cyber exercise.

During the tabletop phase, the participants were divided into groups (tables) according to their sector. A cyber attack scenario unique to each sector was assigned to each table, and each group received general information about the scenario. The assignment for the participants at each table was to discuss the scenario, request more information if necessary, and discuss its impact on the sector if the incident actually happened. The goal of this phase was to raise the awareness of cyber attacks and its disastrous impact on the sector [7].

The second phase concerned taking what was learned in the tabletop phase and developing a procedure to detect and respond to the incident. Most of the activities involved developing policies and procedures for handling the incident, creating contact lists of appropriate authorities or experts, formulating incident response teams and training for employees to recognize incidents and respond to them.

The last phase involved live operational analysis and simulation of events that would be too disruptive for live analysis. The live analysis tested the security boundary of the sector and its report mechanism if the event happened. The simulation was conducted through the use of "white cards" where each card described the event that occurred and actions taken by officials. The participants then determined whether or not the actions taken by the officials were effective for the incident.

The results from the exercise suggested that the regional public and private sectors needed to have a better information-sharing mechanism. It pointed out that there was a lack of communication between different entities in the region. The exercise proved that communication between local entities was crucial when dealing with cyber attacks. The results also showed that a few entities in the region had a great amount of resources that would be helpful to surrounding entities. There were incidents that individual groups were able to solve by themselves, but the responses were based on an individual's knowledge instead of an established, written policies or procedure. The results from the exercise also suggested that there was a need for establishing a local law enforcement agency to serve as a source for sharing information in the region [7].

Security Initiative Related Issues

As those security initiatives have become more recognizable throughout the country, many IT specialists have started to pay more attention to the quantitative result from federal agencies. For the past fourteen years the amount of security incidents has increased exponentially. In 1990, the Carnegie Mellon Computer Emergency Response Team (CERT) reported 252 incidents. In 1995, the amount of incidents grew to 2,412, and by 2003 the amount of reported incidents increased to 137,529 *[CERT].* The 2001 CSI/FBI Computer Crime and Security Survey gleaned some statistics worth noting. Below is a summary of its findings:

- 91% reported computer security breaches within the previous 12 months
- 70% reported their Internet connection as a frequent point of attack (up from 59% in 2000)
- 64% suffered financial losses due to breaches; 35% could quantify this loss.

There are many factors that have contributed to the dramatic increase in incidents and shock statistics. Some of the factors include an increase in the

number of known vulnerabilities, an increase in organizational awareness of computer security, and organizations implementing policies regarding reporting incidents, along with many other factors. As a result of the above statistics, organizations (public and private) are becoming more concerned with protecting their assets. This has resulted in voluntary, as well as, mandated network vulnerability tests and increased development in security professions. Along with the security awareness improvements, many people have started to doubt whether it is appropriate to expose their internal network to outsiders for testing purposes, and universities have been questioned as to whether teaching students how hackers are able to compromise systems is a good idea.

Ethical hacking/red teaming/penetration testing

Penetration testing is the most intrusive process of security assessment. The activities conducted by penetration testing are not that much different from the actions of an actual attacker. The only difference is that security professionals conducting the tests do not have malicious intents. One of the popular approaches for penetration testing is the use of a "red team." "Red teaming" is an advanced form of information system assessment that can be used to identify weaknesses in a variety of systems" (Wood, 2004). The red teaming concept originated from the military where they have a "red team" and the "blue team" playing the game of attack and prevention (Sinai, 2004). The objective of the red team is to strategize and generate tactics for exploiting the blue team's infrastructure. The red team's approach brings in the following benefits to the assessment:

- Detection of network design vulnerabilities
- Detection of unpatched software vulnerabilities
- Detection of overlooked default accounts

In addition to the above benefits, this approach also provides feedback of the current security state of the system to administrators. Also, if red teaming is conducted during the development phase, then it can be used as security testing.

The new approach in security is to hire "white-hat" hackers as security consultants to tracker down crackers, as well as, to help discover security holes. White-hat hackers are former crackers who have become security consultants in pursuing a more ethical career. "While not a new trend, penetration testing, or testing security from the perspective of a would-be intruder, has gained significant appeal in the wake of recent attacks on high-profile companies like Yahoo and CNN."[1] The case with Kevin Mitnick is the perfect example of why it is necessary to have assessors with hacking knowledge rather than just

[1] http://www.cio.com/archieve/060100_con.html?printversion=yes

academic knowledge without practical experience. "I have real-world experience circumventing security measures, and that might be more attractive than hiring somebody right out of school who has a degree in information security but no practical experience. Companies are more interested in experience than education" said Kevin Mitnick.

Teaching students to break systems (Pro and Cons)

Many people believe that the academic environment should not teach students the art of hacking because they fear that the students will use the knowledge they have learned for malicious purposes. It is similar to the main concern in the Stars Wars trilogy when the Republic asked whether or not they should teach the young Anakin Skywalker to be a Jedi. The whole goal of an educational institution is to raise a student up to benefit society. However, there is no guarantee whether or not he/she will use the knowledge for the benefit or destruction of the community.

The role of the security protector and the hacker is just like the two opposing forces in a war. As Sun Tzu's *The Art of War* suggests, "If you know the enemy and know yourself you need not fear the results of a hundred battles."[2] In other words, it is beneficial for the "good" students to understand the way the hacker operates so that he/she can protect the assets. By "knowing yourself", the student needs to know how the system can be exploited so he/she can recognize when an incident occurs. For instance, the student can use that knowledge of how the system can be exploited in order to set up honey-traps to capture the hacker's behaviors and establish hacker profiles. The protector can use the hacking knowledge to feed the hacker with the information the hacker seeks, and potentially set the hacker up so that a trace can be done to capture the hacker. This is similar to what Cliff Stoll did in the Cuckoo's Egg.

From the student's perspective, it is very beneficial to understand and learn how to break into a system. The only way to help prevent others from breaking into a system is to be able to identify how the system can be exploited and patch it before others try to break it. Despite the pressure for academia to stop teaching hacking techniques, the exposure is unavoidable. "The tricks invented by hackers have become easier for activists to learn and adopt because they are now widely published on how-to Web sites."[3]

[2] http://www.brainyquote.com/quotes/quotes/s/suntzu155752.html
[3] http://www.nyteims.com/library/tech/98/10/biztech/articles/31hack.html

Conclusion

All of the security exercises discussed here were considered successful exercises on the subjective basis. However, these exercises provided little quantitative evidences of whether or not the participants were capable of meeting critical performance levels during real crisis. There was not performance measure over time for improvement. Realistically, regardless of how successful the exercise was, it would be extremely difficult to forecast the outcome of a real crisis because an actual incident has many supplemental factors that the exercises did not take into account. The environmental and human factors, in addition to the evacuation process, are very critical to the success of a terrorist attack containment process.

Despite the fact that there are controversies with network penetration testing, it is still one of the most important processes to deliver an accurate assessment of the current status of a client's network. The client also needs to recognize the nature of network security. The security of the network is very dynamic. Therefore, the result of the assessment does not guarantee the secure level of the network. The one rule of thumb that can be applied to all the ethical controversies is that any action that does not have malicious intent and does not invade other's privacy without consent is considered to be ethical.

After all, there are no boundaries for what is considered a "secured" infrastructure; there is no flawless network. Since our networks are exposed, cyber attacks are unavoidable. For every computer designer, there are million others trying to break the design. Therefore, the ultimate goal is to prevent it from happening through detection processes, along with security measures. If all failed, then it is necessary to contain the incident so it does not cause a disaster. Our government and the private sector are actively preparing for such incidents. Our schools are adding to their curriculum to directly address the security issues of our network infrastructures. Organizations, such as SANS, DISA, and others, are providing courses to network administrator to improve their understanding of how critical it is to protect the network against malicious intentions.

Bibliography

1. Unknown. "Cyber Security – Protecting NYS's Critical Infrastructure." June 2003. The Cyber Security Task Force.
2. Verton, Dan. "Black Ice scenario sheds light on future threat to critical systems". October 2001. Computerworld. http://www.computerworld.com/printthis/2001/0,4814,64877,00.html
3. Verton, Dan. "Exercise Exposes Vulnerabilities". July 2002. Attrition.org http://computerworld.com/printthis/2002/0,4814,72532,00.html
4. Anderson, Phil. "Silent Vector – A Critical Infrastructure Simulation Exercise". October 2002. CSIS.
5. Stannovich, Mark. "Exercise and Scenario Development". 2003. Dartmouth University
6. Patterson, Darby. "Gov. Locke Touts Success of TOPOFF2 Cyber Exercise." May 2003. http://www.govtech.net
7. Unknown. "Dark Screen – A Cyber Security Exercise for San Antonio/Bexar County". September 2003. University of Texas at San Antonio.
8. Scalingi, Paul. "Infrastructure Interdependencies". May 2001. http://www.dtic.mil/ndia/2001wmd/scalingi.pdf
9. Shirhal, Maureen. "Critical Infrastructure operators lack key information". August 2002. http://www.govexec.com/dailyfed/0802/081302td1.htm
10. Unknown. "Silent Vector Briefing". www.csis.org/features/SV/021017briefing.pdf
11. Chase, Marilyn. "Drills to Test Terror Preparedness." May 2003. http://www.ph.ucla.edu/epi/bioter/chicagoseattledrills.html
12. Unknown. "Blue Cascades". http://pnwer.org/pris/bluecascades.htm