



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Cyber Crime

Whose fight is it?

Dennis L. Lindsey

July 21, 2000

Introduction

Little Johnny can't wait to get home so he can check out the internet for more clues to his PlayStation computer game. When he finally arrives in his room, he throws his books down on his bed and dives for the keyboard. He skillfully double clicks his way to his favorite URL'S and with a few more clicks, he is on his way, losing all track of time. A couple of hours later he begins to shut down and he notices a "new" icon on his desktop. This one says "Hot sex - LIVE!!". How did that get there? Would he get in trouble for clicking it? "Hey...I'll try it just once", he muses. "No one's gonna find out." Just at the moment, Johnny's mom walks in and is shocked to see what is displayed on Johnny's computer screen.....

Carey Bunks recently ordered a digital subscriber line, or DSL. With this high speed Internet connection, Carey figured he could conduct some of his office work from home and also surf the Internet at a higher speed. What he didn't count on was that now he is not the only one who has access to his computer. Within a couple of weeks after the DSL was installed, Carey noticed that a hacker had gained access to his computer and set it up so that it could be controlled by the hacker.....

FBI agent Craig Sorum has just completed his presentation to the SANS training class. This investigation had clearly tested his abilities. Craig's feelings concerning the case was obvious, "It's one thing to go up against the average criminal mind but now I have to match wits with the **cyber**/criminal mind". In this most recent case, a disgruntled employee had quit his job, left the company only to break back into the company's computer to steal company files. Craig was glad that more damage wasn't done. The former employee could have altered the company's web files which dealt with sensitive medical information. This could have led to altering medical dosage for patients and could have affected innocent people's health.....

Wen Ho Lee, laboratory scientist, has been accused of passing classified information from the Los Alamos National Lab to China. Lee has been under suspicion since 1984, but was allowed to continue his job until 1999. This even after Lee attended a technical conference in China without reporting it. Lee was fired and has been charged with illegally copying U.S. nuclear weapons secrets.

Cyber Crime is on the Rise

From frustrating hackers on your home computer to disgruntled employees vowing retaliation to the more serious espionage related crimes, anyone who has a computer can feel threatened by the increasing amount of cyber related crimes that happen in today's

world. According to SC Magazine's Illena Armstrong, "The FBI has reported that cases of computer-related security breaches have risen by almost 250 percent in the past two years. Dollar losses, associated with various computer crimes and theft of intellectual property, were estimated to be in the \$250 billion-range in 1997." The attraction of cyber crime to crooks is easy to comprehend when you account for the fact that many crimes that were once carried out physically, can now be accomplished with a few clicks of the mouse over the Internet. Another attraction to the cyber crooks is not only the ease of performing crime with a computer but also the unlikelihood of being caught. "The Internet is like a city right now where nobody locks their doors, nobody locks their windows," this according to Charles Biggs who is vice-president of product marketing for NetGuard.

Apathy Plays a Part

I think that anyone can plainly see the "writing on the wall" in regards to where we are heading. The "IloveYou" virus which occurred in May of this year and the distributed denial-of-service attacks against Yahoo! eBay, CNN, and Amazon.com are "tips of the iceberg". We should be gearing up for "Cyber War" against cyber criminals, but I'm afraid that many companies are still not convinced that they could be hurt (financially and professionally). Our government, too, should be moving more quickly to (1) pass legislation to convince criminals to think twice and (2) beef up on security in their own systems to prevent breaches. I am convinced that what we have seen so far is only the beginning. We could be witnessing soon a terrorist with a certain agenda, or even an unfriendly nation/state. What better way to wage war against the great USA than to attack its infrastructure? A well placed and well timed trojan could do a lot of damage and cost America trillions.

Is Cyber Crime Different From Other Types of Crime?

I have to wonder why cyber crime is thought of differently than any other type of crime. Shouldn't it be just as unlawful to enter another person's computer than if you were entering the same person's home? Would we allow someone to walk into our home and nail a poster of a nude model to our living room wall? Would we permit a stranger to "drop in " and "borrow our car keys" for a little "test drive"? Would we pursue the prosecution of a former employee who re-enters his former place of employment and begins copying files on the zerox machine? Why does the hacker excuse of "I was just pointing out that systems weaknesses" work? Would the same ploy work if a thief who was caught inside a business claim that he was merely "testing the company's burglar alarm"? Although these crimes are more obvious to us, they are not much different than the crimes being committed with a computer.

Possible Solutions

I really believe that everyone who works, plays, communicates (in other words, lives with) computers must realize and act upon the security measures which will protect his

assets associated with his home or workplace. This is true in the home, at work, in the government, all through society. The home computer should be protected from attack with some sort of personal firewall and the home owner should be aware of the threat. Can the home owner of today go to bed or go on vacation with his door unlocked?

Companies across the world have to have the same mindset and secure its computer resources. The world's most powerful industrial nations (United States, Japan, Britain, Germany, France, Italy, Canada and Russia) recently met to discuss cyber crime in a three day conference. The group of eight nations stated, "Governments and the private sector share a joint interest in the fight against the illegal or prejudicial use of information and communication technologies." "Companies are themselves victims of criminal practice and are especially suited to put forward proposals to counter cyber criminality." According to Lt. Gen. Vladislav Selivanov, who heads the Russian Interior Ministry's high-tech crime division, "If you have a cadaver with two bullets, it can lie there while you hunt for the killer, with cyber criminals, you must act immediately. Otherwise, you lose the possibility of catching them." All of the nations at the conference stressed the necessity of harmonizing laws governing the use of the Internet, speeding up judicial procedures, such as search warrants, and reducing language and cultural barriers between law enforcement agencies in different countries. Faster ways to fight cyber crime should be developed and all governments and industries should work together.

Conclusion

Cyber crime is real and it is growing. Homeowners, businesses, governments, all need to be prepared for the strong possibility that they may be the victim of a computer crime. My hope is that all computer users will join the fight against cyber crime and place the cyber criminal behind bars and away from computers where he belongs.

Resources

Schwartau, Winn. "DDOS: The High Cost of Apathy." March 2000. URL: <http://www.infosecuritymag.com/march2000/news&views.htm> (19 July 2000)

Armstrong, Ilenna. "Computer Crime Spreads." April 2000. URL: http://www.scmagazine.com/scmagazine/2000_04/feature.html (19 July 2000)

Deborah Seward. "Industry urged to join cyber crime war." The Knoxville News-Sentinel. May 18, 2000.

Peter Svensson. "Hacker Risk." The Knoxville News-Sentinel. February 24, 2000

© SANS Institute 2000 - 2005, Author retains full rights.