Global Information Assurance Certification Paper

Computer Crime: The Insecurity of Your Network
Steven A. Sandberg
December 14, 2000

Introduction

When the Melissa virus struck, the whole technical community let out a collective gasp. Network managers ran to ensure their own networks had nothing evil lurking about. Then the hacker was caught, and the whole ordeal seemed to strike a nerve with the public.

Everyone waited anxiously to see just what kind of justice the legal system would impose, and then suddenly the story died. Federal and state authorities opted not to pursue the case; the hacker was set free and the media quickly lost interest.

Just because this case didn't result in a prosecution doesn't mean that there is no legal recourse to protect mission-critical data from disgruntled employees and hackers' intent on bringing a business to its knees.

Ask a dozen people about computer crime and you'll get a dozen different answers. The term is as elusive to define as the problem is to stop, and the crime wave is only building. Operating system and application-vulnerability announcements are on the rise. Remote intrusions are on the rise. The FBI continues to struggle under the weight of its caseloads, as CERT reports an overwhelming increase in incidents.

What is computer crime?

When people use the term computer crime, what exactly are they talking about? Web defacements? DoS (denial of service) attacks? Compromised systems? Fraud? Theft? Industrial espionage? It appears that even the phrase computer crime has its fair share of problems. The truth of the matter is that all those examples, or none of them, may be involved when it comes to computer crime.

Computer crime can be initiated using everything from the elegant insertion of some mischievous code to the down-and-dirty instance of copying data onto a floppy and walking out the door. Cutting-edge techniques and technology may or may not have anything to do with it.

For the sake of clarity, however, we will categorize all these examples as computer crime. These crimes generally fall into four areas: fraud, data theft, data manipulation and destruction.

Undeniably, when it comes to raw firepower and anonymity, the wholesale adoption of the Internet has helped the bad guy on the hacking front. Attackers continue to use compromised hosts as launching points for more stealthy attacks and next-generation distributed DoS tools are bringing computer crime to a whole new level.

It's no surprise that the FBI/CSI (Computer Security Institute) report on computer crime trends indicates that organizations this year had 70% of all attacks originating from the Internet. What might come as a surprise is the breakdown of dollar losses. Despite the advances in exploitation trends that the Internet has provided, according to the computer crime report, more than 75% of all dollar losses came from internal intrusions.

That's an interesting statistic. The number of security incidents originating from external attacks is definitely on the rise, but the internal attacks are the real financial killers.

The Problem

Hardened perimeters with mushy inards. It's usually much easier to infiltrate a company from the inside because most organizations place a huge emphasis on defending perimeter but do little to detect, much less protect against, hostile internal activity. While external attacks such as DoS, Web site defacements and data-mining efforts can be humiliating, they're rarely financially devastating, except to Internet start-ups, which can be leveled by DoS related incidents.

While IT managers spent huge amounts of time and resources to thwart the threat of year 2000 problems, information security breaches in the Internet economy are an even bigger threat. And unlike that millenium bug, security is not a one-time, easy to identify issue. It's a process that must be continually refined using audits, new tools, and changes to how data is stored. This may be why so many businesses put security on the back burner until a crisis flares up. It's time to go beyond awareness and take action. Protection from security breaches requires investment in technology, services, and personnel as well as adjustments in corporate culture.

Security also needs to adapt to the new world of broadband remote access, a big source of vulnerability. Small branch offices and telecommuters are replacing intermittent dial-up connections with persistent digital subscriber line (DSL) and cable-modem links that create new security holes. These connections are always on, so the chances that a hacker's ping sweep will find you are very high. These connections have permanent IP addresses, so the hacker can come back again and again and take a ride through your virtual private network right into your company's network.

Security professionals say crooks are targeting remote systems. Some intruders are simply using the hard drives as free offline storage for illicit files. However, others are installing Trojan horse and zombie programs that turn the remote systems into enterprise

back doors and even launch pads for DoS attacks.

Cable systems are even more vulnerable because they basically use the original Ethernet "party-line" architecture and put a neighborhood on a single subnet. Each packet is broadcast to everyone, and only the addressee is supposed to process it. However, neighborhood hackers can use Sniffer technologies to capture everything going across the subnet, and they also have easy access to the other systems on it.
Since broadband is clearly here to stay, enterprises can reduce risks by installing personal firewalls on remote computers and encouraging employees to turn off the machines when they aren't being used.

The unwillingness of companies to go public with security breaches has also frustrated law enforcement officials for years and results in more victims of the same sorts of incidents. Also, incidents that appear to be isolated events may take on considerable significance when aggregated because patterns emerge. As security attacks in general become more complicated and better disguised, the need for cooperation and discussion among potential targets is increasingly important.

Global Integrity Corp., a security consulting firm, has come up with a possible solution: the Information Sharing and Analysis Center (www.wwisac.com), an organization that lets companies share information about security problems anonymously. Global Integrity serves as a trusted broker that collects the information, strips the identity of the source, and puts it in a database that member companies can access. Launched earlier this year, they have members from the banking, energy, manufacturing, pharmaceutical, and securities industries. Security incidents are reported on a daily basis and range from an insider bringing down a critical system to massive attacks on e-commerce servers costing businesses tens of millions of dollars.

The Inside Threat

Senior management would be appalled if desktop and server machines were being stolen, but electronic theft is going on right and left. They just don't see it. Management may be turning a blind-eye for several reasons. One is a trade-off between added security and ease of use. They fear the backlash from both executives and rank-and-file users when measures such as logon time-outs and long alphanumeric passwords are instituted. People forget their passwords and make frequent calls to the help desk, or they write the passwords on Post-its attached to the side their terminals.

Also, make sure that key data is password protected. All employees should have passwords just to get into their own computers. There should be no easy way for someone to sit down at a PC in someone's cubicle and get access to the network. Employees need to change passwords often, and make sure the passwords aren't pets or spouses names. You want letter, number, special character combinations, which are harder to hack.

When it comes to addressing computer crime, the more successful your information security program is, the better equipped you will be to handle the threats. Without proactive security measures, information security practices will continue to be only reactionary and only minimally successful. If organizations want to effectively address the threat of financial losses a security breach can bring, they must first make a strong commitment to deploying a proactive security plan.

However, without upper-management support, information security programs will be moderately successful at best and will fail miserably in most cases. Forming a strategy, educating the organization and working toward covering the basics will go a long way. To prevent computer crime, security must be built into the business process, not around it.

Despite the publicity surrounding denial-of-service and virus attacks, most serious security incidents are never reported because employees perpetrate them. Companies cover them up rather than risk the loss of customer trust.

Numerically, more attacks come from the outside, but they're mostly kids who come in out of curiosity, not really knowing how to attack you with a lot of skill. However, one insider with the right skills can ruin your company. Furthermore, generic attacks such as simple host compromises, require a limited skill set. More complex and often more devastating feats frequently require niche skills or a unique position held by the attacker.

Pulling off such complex attacks remotely is not impossible but is definitely less likely to happen. The skills barrier makes it far easier, and less expensive, to go in as a contractor or employee, get close to the targeted information and gut a company internally. And this is precisely what is happening today.

The need to address employee breaches is often obscured by all the solutions for physical and network security. Firewalls and authentication systems do a good job protecting networks from remote attacks, and heavy doors with biometric locks and video cameras can keep strangers from breaking in at night, but employees are already on the inside.

Legalities

Laws are in place, but most people aren't aware of them and don't know how to gather evidence to ensure prosecution if a hacker strikes. The federal Computer Fraud and Abuse Act, for instance, was updated in 1996 to reflect recent problems, such as viruses that are sent via e-mail. This is the law that's applicable to the Melissa Virus case (for more information, go to www.usdoj.gov/criminal/cybercrime/index.html).

The FBI, in response to an expanding number of instances in which criminals have targeted major components of information and economic infrastructure systems, has established the National Infrastructure Protection Center (NIPC) located at FBI headquarters and the Regional Computer Intrusion Squads located in selected offices throughout the United States.

The NIPC, a joint partnership among federal agencies and private industry, is designed to serve as the government's lead mechanism for preventing and responding to cyber attacks on the nation's infrastructures. (These infrastructures include telecommunications, energy, transportation, banking and finance, emergency services and government operations).

The mission of Regional Computer Intrusion Squads is to investigate violations of Computer Fraud and Abuse Act (Title 8, Section 1030), including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes.

The Computer Fraud and Abuse Act also covers the broader crime of unauthorized access to any computer system, so hacks other than viruses are included. Also, federal obscenity laws have been updated to make it illegal to transmit child pornography images by computer. Most states also have these laws in place.

California, for example, is considered the computer crime and fraud capital of the world. The state has instituted some very defined laws regarding computer cracking. The major body of this law can be found in California Penal Code, Section 502. The statute is comprehensive. It basically identifies a laundry list of activities that come under its purview, including but not limited to any unauthorized action that amounts to intrusion or deletion, alteration, theft, copying, viewing, or other tampering of data. The statute even directly addresses the issue of denial-of-service.

In the state of Texas, it's a bit less stringent and far less defined than California. The Texas Penal Code says merely this:

> A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

Information about computer crime statutes can be obtained from the Electronic Frontier Foundation (EFF). EFF maintains a list of computer crime laws for each state. These laws can be found at EFF's website at:
http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/Legal/comp_crime_us_state.laws

Internet hacking and cracking activity in Europe is quite different from that in the United States. They have different motivations for their activities. Specifically, they tend to be more politically motivated. Europeans are becoming increasingly aware of the problem of hackers and crackers, and there is a strong movement to prevent this type of activity. This can be seen by the Council of Europe's Draft Convention on Cyber-crime, where they are convinced to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cyber-crime, by adopting appropriate legislation and fostering international co-operation.

Aside from computer-specific laws, there are many laws that protect businesses and are used in network-related crimes. Take traditional trespass laws, for instance. Say America Online tells someone to stop sending spam. AOL has the legal protection of existing trespass laws to make sure the spammer stops. Most states also have a trespass law.

Computer Information Officers (CIO) can protect themselves by knowing what kind of electronic paper trails to create so they can present a body of evidence to lawyers following a hacking attack. Federal rules of evidence are key. If you can't make the evidence work, you can't prosecute. What you need are audit logs of all your network activity and password access to all the computers on the network, so you can see who is accessing what and perhaps even head off a problem by scanning the logs for suspicious activity.

Suspicious activity could include accessing a database too often, or making repeated attempts to access something (a server, database, etc.) without getting in. The latter indicates that someone is trying passwords that aren't valid. Suspicious activity also includes someone who isn't part of the network administration staff accessing the network at odd hours. Of course, at some companies, accessing the network in the middle of the night is perfectly acceptable. Look for the unusual, out of the ordinary activity.

Suspicious activity is not always generic. The key is knowing how your network is normally used, having the audit logs on hand and then tuning in to unusual patterns. The lesson here for CIOs is to be meticulous in gathering evidence. And to do that, systems must be in place for that purpose long before an attack ever takes place. It's worthwhile to be prepared, assuming an attack will happen at some point.

Remember that a hacking crime is not unique. People commit crimes, and they leave evidence. In a hacker's case, evidence may be e-mails, stolen passwords, repeated attempts to gain entry into a system, or bitter conversations with other employees in which the hacker complained about the company.

Make sure you have the ability to look at the evidence by setting up your network and security policies carefully. Then if a hacker strikes, you'll have a better chance of having

your claims stand up in court

The role of IT

Ask an administrator of small LAN what needs to be watched and defended, the answer will probably be the servers. Ask the network administrator of a midsize organization where the biggest threats lie and he or she might point toward the firewall. The fact is, many of the defenders of data aren't entirely sure where their most valuable assets reside, or how secure they are.

Computer criminals know this. Many times they play the odds, and they bet that the basics haven't been covered. They bet that administrators don't watch the attempted policy violations on the firewalls. They bet that machines aren't patched. They bet that logs aren't read and that important files aren't audited. They bet that unless they jump up and down, openly trash systems or delete data, they would go unnoticed. And most of the time, they are right on the money.

Some vendors' ship their operating systems with security screws intentionally loosened, and it's up to the administrators to tighten them as needed. For example, the Common Gateway Interfaces in Web server software can supply hackers with root access to the server. Every copy of Apache open-source Web server (widely deployed) comes with these vulnerabilities. You can't just fix the holes in the services you use and leave the rest alone.

Make sure the basics are covered. While some of the more complex incidents, such as extortion attempts, may involve high-tech systems, most crimes are easily tracked using basic logging and accounting techniques. Reading the system and access logs can help identify suspicious behavior. Properly planned and tested disaster recovery procedures can help with cases of sabotage. Staying on top of vulnerability and patch announcements, as well as applying those patches in a timely manner, will limit your chances of a hack.

Restricting access to your network from third parties and Internet users will limit your number of exposure points. Using encryption on laptops will limit the spread of sensitive information if those laptops were stolen. A defined incident response program will help contain breaches and facilitate successful prosecution.

Basic asset identification and data value classification efforts can also work wonders. Many large organizations focus their security efforts on their most valuable assets and work their way out. That is, they first identify, lock down and monitor their most sensitive data, systems and services, and then move toward the less valuable ones. It's a risk management technique, but one that many organizations fail to consider.

IT specialists face a daunting set of challenges when it comes to computer related threats, as they have very few cards to play. The number of intrusions is rapidly rising. DoS tools are evolving and are beginning to employ features such as encrypted channels. New software vendors and programmers continue to prove their ignorance by pushing more and more insecure code into the market, and script kiddies are propagating at a dizzying pace the tools to exploit such pathetic products.

Conclusion

Many organizations don't have many avenues for help. Most companies don't retain an established incident-response team, so external investigations are often at the mercy of internal, ill-equipped and unmotivated personnel to investigate breaches. The bottom line is every organization is on its own, which makes its susceptibility to computer crime highly dependent upon its overall security posture, one that comprises both internal and external defenses.

While detecting and catching high-level, skilled intruders will be difficult for any company; tighter shops will have a greater chance of surviving an onslaught unscathed. Unfortunately, battening down all the hatches is easier said than done. The cards are stacked against organizations trying to defend their digital assets. Intruders come in all forms. A school bus of 15 year old kids, two Russians from Kazakhstan or a 30 year old with two dogs and a Jetta may have backgrounds as varied as their attack methods, but their abilities to damage your organization can be equally alarming.

Computer crime is costing organizations millions of dollars. The fix lies at the heart of good information security practices. Unfortunately, this does not come without its price; security specialists and products are expensive. Doing the things right can take longer and is often more expensive.

In short, the best technologies and wisest policies will take security only so far without extensive user and management buy-in. You have to create a win-win situation, allowing the users to see the benefits themselves; strong security is keeping the wrong people from seeing their salary and personnel records or getting into the bank accounts where their checks are automatically deposited.

Absolute protection may be unattainable, but better levels of security, with equal parts vigilance and honest commitment, will go a long way to protect your company.

Sources

Breidenbach, Susan. "How Secure Are You?" 21 August 00. URL.
http://www.informationweek.com/shared/printArticle?article=infoweek/800/prsecurity.htm&pub=iwk

Swartz, John and McCoy, Kevin. "Corporate networks vulnerable, pros say." 30 October 00. URL:
http://www.usatoday.com/life/cyber/tech/cti734.htm

Sherman, Erik. "Is Your Network Safe?" 27 November 00. URL:
http://www.msnbc.com/news/491830.asp?0nm=-22A

Farell, Greg. "Many victims of hacks clam up." 27 November 00. URL:
http://www.usatoday.com/life/cyber/tech/cti839.htm

Iwata, Edward and Johnson, Kevin. "Computer crime outpacing cybercops." 7 June 00. URL:
http://www.usatoday.com/life/cyber/tech/cth404.htm

Washington AP. "Govt. mulls ways to police Net." 7 Jun 00. URL:
http://www.usatoday.com/life/cyber/tech/cth531.htm

Rapalus, Patrick. "Computer Crime and Security Survey." 22 March 00. URL:
http://www.gocsi.com/prelea_000321.htm

Pond, Weld. "Cybercrime treaty gets it wrong…again." 1 November 00. URL:
http://www.zdnet.com/filters/printerfriendly/0,6061,2647940-2,00.html

This compilation was prepared for the National Institute of Justice (NIJ) by the Institute for Law and Justice, Inc., under contract No. OJP-85-C-006. The Program Monitor for

NIJ was Jonathan Budd. "Computer Crime Statutes." 1 May 00. URL:
http://www.eff.org/pub/Privacy/Security/Hacking_cracking_phreaking/Legal/comp_crime_us_state.laws

"US code: Title 18 - Crimes & Criminal Procedures, part I - Crimes, Chapter 47 - Fraud & False Statements." URL:
http://www4.law.cornell.edu/uscode/18/1030.text.html

"European Committee - Draft Convention on Cyber-crime." November 00. URL:
http://conventions.coe.int/treaty/EN/projets/cybercrime24.htm

"The Texas Penal Code" URL:
http://www.capitol.state.tx.us/statutes/petoc.html

"The California Penal Code" URL:
http://www.leginfo.ca.gov

"The Federal Computer Fraud & Abuse Act" URL:
http://www.usdoj.gov/criminal/cybercrime/index.html

Global Integrity Corp. "The Information Sharing & Analysis Center" URL:
http://www.wwisac.com

Johnson, David R. and Post, David G. "Law and Borders--The Rise of Law in Cyberspace." 1996. URL:
http://www.cli.org/X0025_LBFIN.html

Russel, Deborah and Gangemi, G.T. Sr. O'Reilly & Associates, Inc. "Computer Security Basics" 1991

Anonymous. Sams.Net Publishing. "Maximum Security - The insider's guide to network security." 1997