Global Information Assurance Certification Paper

GIAC Training and Certification
Sans Security Essentials – GSEC Practical Assignment – Version 1.2b
John Keuper

Let's Talk People

This paper is being written in accordance with the requirements of the level one security course with the SANS Institute. Being a computer crime investigator in Canada over the past 5 years has helped me gain experience in the area of computer infractions and the legal architecture surrounding this ever-growing area. This paper is being written for the benefit of any company or individual who has been or will be the victim of a computer crime in North America. I will try to emphasize the importance of reporting incidents to your local authorities as well as new and different ways to encourage victims of cyber-attacks to affiliate themselves with groups and organizations that track and report these types of offenses. Reporting incidents is at the heart of controlling computer crime and increasing the number of successful prosecutions; to be able to successfully battle hackers and crackers we have to know what is going on in cyberspace. At the time this paper was written the vast majority of companies and individuals do not report computer crime for fear of the negative publicity that could be associated with a court case and the perception of weak computer security. A good example would be Vladimir Levin's attack on Citibank accounts in 1994-95 in which he successfully transferred over 10 million US to various European accounts. Although later convicted and the majority of the money recovered, the damage was done to Citibank's reputation. I would guess that most major North American banks today would rather absorb a 10 million dollar loss than report it to their local authorities and have it become public, where the damage could be much worse.

Statistics are difficult to come by in the computer crime area; most organizations are still grouping them into "other" federal offences because of the relatively low number being reported. The latest statistics obtained through Intergov show that for 2000 there were approximately 322 million users online, of which over 50% are in North America. There were roughly 282,000 Internet-related complaints filed in the United States in the year 2000 for an average of 773 per day. Of these the vast majority are what we can refer to as traditional crimes being committed through the use of the Internet, i.e. sex crimes, fraud and spamming. Hacking and intrusions comes in near the bottom of the list amongst the "other" category. The reason for these low numbers is directly related to the anonymity problem and complainants fears of the negative impact associated with a security breach. A survey conducted by the FBI/CSI showed that 99% of 247 respondents reported having experienced a cyber-attack and almost half of them indicated that they had suffered financial losses as a result. We know that the attacks are happening but how do we increase the percentage of reporting? I

propose that we give these complainants alternate options that would enable law enforcement to learn of the attack without necessarily identifying the client and compromising the professional image of the institution in question.

Our approach has to change if we want to advance and get the upper hand on hackers and crackers. Legal prosecution isn't always a necessity in computer intrusion cases although when used tends to be very effective. Prosecuting computer criminals and seizing their equipment is an effective method since these individuals tend not to be in the higher income brackets but often have rather sophisticated computer installations, or have put countless hours into configuring lesser equipment to do the job. Thus the loss of this equipment can be a big setback not to mention any fines or prison terms. However there are many instances when just knowing about certain attack trends can give us the upper hand and a better control over these attacks. Therefore we have to establish criteria that will guide us in deciding where we can draw the line and offer anonymity to complainants and when we would have to prosecute. However, before getting that far we have to make sure that our clients are doing several things:

- ✓ Keeping good logs which can be used for possible investigations
- ✓ Protecting those logs (preferably off-site)
- ✓ **Reporting the incident to their local authorities ASAP**

Now let's take a look at what's being reported at the present time. Statistics in this area are difficult to obtain since many private companies refuse to give out security information for fear of being downgraded on the Dow Jones or NASDAQ, government institutions tend to be a little more open in this regard. The Computer Security Institute (CSI) out of San Francisco recently published the "2001 computer crime and Security Survey" in which 85% of all respondents to their survey confirmed a computer security breach during the previous 12-month period. 70% confirmed that it was their Internet connection that was the point of origin for these attacks. 40% confirmed a system intrusion from the outside, 38% indicated that they were the victim of a denial of service attack.

Louis Freeh, director of the FBI, stated for the record before a Senate committee in February of 2000 that the FBI had treated 1154 computer intrusion cases in 1999; of these cases they were able to close 912. That's a pretty good batting average but it's the number of complaints that needs to be addressed. 1154 for a country the size of the United States indicates that we're not getting the collaboration we need in terms of reporting computer incidents, and when you're dealing only with a minority of incidents it's hard to have a good grasp on the latest attacks and threats. M. Freeh identified the need for trained personnel and the importance of building partnerships. The partnership issue has been addressed through an FBI program called "InfraGard" which encourages the exchange of information between government and members of the private sector. It does this through the use of local chapters that report to the local FBI field offices. InfraGard is designed to provide 4 services to members of the local chapters: an intrusion alert network, a secure web site for communicating suspicious activity,

local chapter reunions and activities, and a help desk for questions. The idea I like the best here is the secure web site for reporting incidents, however it has to go one step further. We need to accredit the local chapter members with a token system and them anonymize their transmissions in order to ensure totally confidential submissions, if so desired by the local chapter members. When the member truly wants to address a formal complaint he/she can pass through regular channels that permit identification of the complainant. There are other sites on the web that monitor attacks, an example would doshelp.com, sites such as these are useful but tend not to be well known or well promoted. Once again we must look at ways in which we can promote a better collaboration between law enforcement and the public through new and improved ways to conduct investigations.

There are several things that can be done to improve the way we conduct computer investigations and improve our relationship with the victims of computer crime:

- ✓ Offer the victim anonymity if necessary, in this way we can keep abreast of all relevant attacks and companies can have the peace of mind that their reputation will not be tarnished simply by informing us of an attack.
- ✓ Promote responsible logging activity amongst the computer community so that the majority of attacks can be successfully investigated if the need should arise.
- ✓ Show the victims and the community what computer crime investigators can offer both in terms of technical assistance and criminal prosecution, this could be done through seminars and conferences.
- ✓ When companies and government agencies are granted rights to do business and confirm they will be connected to the Internet in some capacity, they could be directed towards the appropriate resources in terms of security programs.

There's another aspect of this initiative that has to be addressed is the issue of the ISP's or the Web hosting service's responsibility with regards to security. Anytime we don't have a web server directly at our offices then that means we're relying on someone else's services to get us on the Internet. That means that for the most part security issues and logging are not directly in our control. We now have to focus on collaboration with these organizations to ensure that logging and security practices are standardized. In many instances these companies don't like to get into the legal criminal architecture because it costs them money and time and they're forced to furnish logs and supply personnel to testify in court.

Some organizations such as the Internet Engineering Task Force (IETF) are suggesting innovative ways in which we could improve this collaboration. They've set up working groups to work on a protocol for broadcasting alerts of network breaches across proprietary security applications. The Intrusion Detection

Message Exchange Protocol (IDMEP) would let applications - and system managers - quickly share information about attacks, according to IDMEP working group members. The idea is that if a source domain notices an attack, it can notify the destination network automatically. Their protocol would be based on SNMP Version 3 and an alert detailing the type of attack in progress would be automatically sent across the network, along with a reference, such as a URL or a system file, where the network manager can find further information. For law enforcement this could be extremely practical if we could also be notified simultaneously of the attacks, however we have to go back to our initial framework and devise a way that would encourage these groups to collaborate with us, possibly offering anonymity if corporations are wary of the implications.

As noted by Dr. K in his hacker manual, the hacker community likes to downplay the danger they represent and tend to see law enforcement as having a vested interest in promoting them as being the ultimate menace. As we move forward and become ever more dependent on the Internet and it's capabilities, the threat to those services increases proportionately with regard to the damage that can be done. Cyber warfare is being waged through hacking activities and the code being generated through this activity inevitably finds it's way on to the Net where it can fall into the hands of just about anybody. We should be actively attempting to stay one step ahead (or no more than 1 step behind) when it comes to computer intrusions and the potential resulting damage. I feel that an information sharing initiative (anonymous or otherwise) would be a giant step in that direction and hope that this paper will help stimulate further discussion on the matter.

References:

Discovery Channel "The Hacker Hall of Fame" (1997)
URL: http://www.discovery.com/area/technology/hackers/levin.html

Intergov "International Web Police – Latest crime stats" (May 5, 2001)
URL: http://www.intergov.org

Security Wire Digest – "Information Security Magazine" (April 2001)
URL: http://www.infosecuritymag.com

Freeh, Louis J. "FBI – Congressional Statement – 2000 – Cyber crime" (February 16, 2000)
URL: http://www.securitymanagement.com/library/cybercrime0200.html

Computer Security Institute – "2001 Computer crime and security survey" (April 2001)

URL: http://www.gocsi.com/prelea_000321.htm

Anonymizer – Anonymous Web Surfing (May 2001)
URL: http://www.anonymizer.com

DosHelp – Intrusion and attack reporting center (January 2001)
URL: http://www.doshelp.com/internet_report.htm

White, Benjamin; Feinstein, Gregory; "The intrusion detection exchange protocol". Internet Engineering Task Force – IETF
URL: http://www.ietf.org

Dr. K, A Complete Hacker's Handbook. London, England. Carlton Books Ltd. 2000.