Global Information Assurance Certification Paper

Iz H4ck1Ng 4ll 8ad?

Author

Mike Miller

Introduction

Much of the information we take in as computing professionals is of a technical nature. We have developed our own techniques of taking in this information in to ensure that we maintain our professionalism in a marketplace that will inevitably be very crowded in the next 10 years. To take in information we commonly use mediums such as magazines, books and newspapers. We also use 'zines, email and IRC amongst other sources to stay on top, but to a large extent the information we buy on paper is a vehicle for advertising and electronically transmitted details is becoming more and more subject to the same "commercial realities" as its paper cousins.

What does this have to do with computer security and more specifically "Is hacking all bad?". Quite a lot. All information carries the view the author and in many instances the views of advertisers and marketers whose interest is more inline with their wallets than the well being of our systems, lives and security. To truly understand the reasons for increased security awareness, it is just as important to understand the mindset of the "hacker" and what motivates a person to illegally gain access to systems that are not there to be tampered with. It is important to look at both sides of the problem to ensure we can act responsibility and in the best interest of the systems we administer. It is important that the issues be put into perspective and that we learn from the hackers as much as they learn from us.

What about these Hackers?

Firstly for the purpose of this paper, the hackers being referred to are the "malicious or inquisitive meddler who tries to discover information by poking around" and not "a person who enjoys learning the details of computer systems and how to stretch them to their limits". These are very similar, except one chooses to learn the details by "attacking" others property.

Do these "hackers" have no conscience, no respect for others privacy, do they snub authority and what it stands for? And importantly how can we as security staff use this information to our advantage. This paper can by no means attempt to answer all the questions and varying opinions that can be raised, but should be seen as a primer and another way to potentially view our situations.

Hackers are people and people are all very different, holding different fears, dreams, ethics and morals. They do however generally fall into a small group of 14 – 25 year

old males who are responsible for the majority of reported activity. This fact alone is interesting as the major reasoning for hacking has been identified as curiosity, prestige/image, thrill and the challenge. These hallmarks of youth are seen in many other non-computer high-risk activities adopted by the young as they "come of age".

Unfortunately the media approach of sensationalism has seen hacking increase dramatically and introduced a much larger group to the idea of hacking as a curiosity, prestige, thrill and challenge of beating the system. This has some very positive aspects to the industry, but it does scare the establishment, as it is very difficult to tell apart the curious teenager who by CERT's admission is seldom responsible for malicious damage and the corporate terrorist.

It is also apparent that in hacking circles, that there are very few "elite" hackers but a vast army of would be hackers. This army rely on the intelligence, and mechanisms identified by these to take advantage of exploits before newer, busy, less conscious administrators (or worse, the accountant with an interest). It has been estimated that these elite may only number in the hundreds throughout the whole USA, but with high profile of security and the apparent ease of access, the army of would be hackers may number in the 10's of thousands.

With the increasing complexity of systems and individual components that build a connected infrastructure hackers work in groups to specialise in areas, transfer knowledge and work together to achieve a common goal. This type of activity, if not directed at unsuspecting organisations, would be applauded as effective utilisation of resources and is not to far removed from normal business methodology. It could be compared loosely to many other groups that are seen by some organisations as socially undesirable like S11 and Greenpeace, but don't have the same lobbying capability as these groups or the computer security professionals in industry.

Unfortunately not all hackers are curious and non-destructive. Systems must be managed to ensure that all unauthorized access is not promoted, it is here that the curious are of assistance to the community at large. This ensures that holes are identified and that attention is raised and that vendors and other keepers of proprietary code are jolted to address areas of weakness. The head in the sand approach of some vocal systems security professionals advocating that without hackers there would be no need to invest so heavily in security is both naive and means that the criminals in cyberspace would have a much easier time both running amok and avoiding prosecution.

Criminals exist in all warps of life, some may consider that inflated damages claims made by some organisations after a breach could be considered fraud. The issue is a what point is curiosity a crime and what resources should be devoted to catching "script kiddies" who are curious and what resources devoted to people engaged in crime. The difference here being a hacker who gains access to a system and does no damage except maybe embarrass the organisation and a hacker who gains access to credit card information and is using the information for profit.

Conclusion

In the business world that we nearly all live in, globalisation and corporate competitiveness knowledge is seen as power, so much of the information we are protecting is seem as an advantage to the "keeper". Globalisation, whether seen as friend or foe, is reality. Trade secrets and information is fundamental to the survival of these companies and the predominantly male youth who spend there free time unpaid to travel the internetworks and identify these weaknesses are actually assisting corporations to ensure the privacy of information.

The morals and ethics of these individuals and groups can be questioned, but as the vast majority are not destructive and do not intentionally make life more difficult for systems owners, it is these people that ensure that our governments invest in the right people and the right tools. It would be an interesting exercise to see how many of these "criminals" would be happy to share their "Adventures" with the corporations they have exploited if fear of prosecution were not inevitable. Would the world be different if an amnesty was put in place and the cracker has 5 days from breach to report the breach? This is assuming of course it didn't involve credit cards, government secrets etc. (Even then, wouldn't it be better to know and to fix than to potentially be subject to repeated abuse without our knowledge?)

Regardless of your standpoint in the debate, it is clear to see that each side of the situation feeds the other, increased security raises the bar and thus the prestige, challenge and thrill in foiling the gatekeepers and beating the systems. Security knowledge for corporate professionals is heightened, so corporate systems are protected and tools developed to ensure the pillars of security, confidentiality, integrity and availability of the information are paramount.

With proper administration and management of information sources to propagate information rapidly to relevant parties, the balance can be maintained in the favour of our systems. These systems require massive investment in infrastructure and marketing to ensure that exploits are minimised. Much of the curiosity can be channeled to environments designed for exploitation, giving computing power and resources normally past the reach of you type young hacker. How better to channel what is primarily negative feelings into a huge security honeypot for all professionals to take advantage of. Who would loose here?

The end result is that hackers will still exercise their curiosity, attempt to increase their personal image amongst their peers, enjoy the challenge and the thrill as well as be prosecuted for intrusion. The security professionals and information systems users will still try and stay one step ahead and learn methods to protect the systems.

References

Reference: Denning Dorothy E "Concerning Hackers Who Break into Computer Systems" http://www.insecure.org/stf/Denning_concerning_hackers.html (Access Date: 17-11-2000)

Reference: Khochaiche, Ahmad "Computers and the Information Age", CC020, 01/08/97, http://minyos.its.rmit.edu.au/~s9715660/intro.htm (Access Date: 17-11-2000)

Reference: Taylor, Paul "Hacker Book" Chapter 6 extract, June 1997 http://rootshell.com/docs/them_and_us.txt (Access Date: 17-11-2000)

Reference: Sterling, Bruce "The Hacker Crackdown" ISBN 0-553-08058-X, January 1, 1994, http://www.insecure.org/stf/hacker_crackdown.txt (Access date: 20-11-2000)