IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4943

SMEs and Knowledge Requirements for Operating Hacker and Security Tools

Murray E. Jennex
San Diego State University, murphjen@aol.com

Aaron Walters
San Diego State University, aaronboy79@mac.com

Theophilus B.A. Addo
San Diego State University, taddo@mail.sdsu.edu

ABSTRACT

SMEs have been singled out as organizations with significant vulnerability to external security threats such as hackers and viruses. This paper explores these issues to determine if SMEs are more vulnerable, and why. It has been postulated that resource issues are the cause for SME vulnerability but the paper finds that there are other contributing issues. Additionally, the paper explores the knowledge requirements required to utilize hacking and security tools and the impacts those knowledge requirements have on SMEs.

INTRODUCTION

The explosion of the Internet as a medium for commerce and exchange has caused information and systems security to be a growing problem. According to a survey performed by the Computer Security Institute (CSI) and the FBI, 90 percent of respondents of small and medium enterprises, SMEs, (34% of all respondents), large corporations, and U.S. Government agencies reported security breaches during 2001, and 80 percent reported financial losses due to these violations, equating to billions of dollars worldwide, (Computer Security Institute, 2002). The losses included not only lost revenue, but also costs relating to cleanup, data loss, liability issues and most importantly, loss of customer trust, Allen, et al. (2002). These figures suggest that there are greater numbers of potential hackers (Allen, et al., 2002) and suggests that despite the overwhelming efforts made on the part of organizations by means of security policies, practices, risk management, technology, security architecture and design, security for information and systems is a serious and growing concern.

Conversely, the explosion of the Internet as a medium for commerce and exchange has also created a world of opportunity for SMEs with 81% of SMEs in Australia (2002) (Brake, 2003), 85% in the United States (by end of 2002) (SBA, 2000), and 85.6% in the United Kingdom (2003) (Ream an Beales, 2003) using the Internet to conduct business. This paper uses Tetteh and Burn's (2002) definition of SMEs as firms with less than 500 employees. This is further broken down into micro companies, those with less than 5 employees, small companies, those with from 5 to 20 employees, and medium companies, and those between 20 and 500 employees.

The problem faced by SMEs is how can they protect themselves against the peril of the Internet exchange medium. During the growth of the Internet the difference between the ease and resulting threat of hacking tools versus the tools used to protect and detect attacks has been perceived to grow wider. Tools for a hacker, a generic term given to all wither script kiddies or uber-hacker, have gone from complicated command line arguments to fully functional GUI applications that wrap many independent functions together. At the same time enterprises wanting to protect themselves have started with no tools but now can select from complex software applications that require complex setup, constant updates, and continual monitoring.

This paper explores the hypotheses that SMEs are more likely to have security issues over larger organizations and that the knowledge requirements to utilize hacker tools are decreasing while the knowledge requirements to utilize security tools is increasing. The implication, should these hypotheses be correct is that SMEs are possibly fighting a losing battle and need to take drastic measures to ensure their cyber security.

Additionally, the difference between the two groups tools should be of great concern to managers and security administrators of SMEs. Administrators should first attempt to know and quantify the ease and risk of attacks. The risk should be measured as a product of total servers, number employees, enterprise goals, and value of the data. Given these factors, the tools to exploit such risks are easy to use by novice and experienced attackers. The more risk an organization has the more time that needs to be spent to qualify the risks. The tools used by the organization should be adjusted for the risk of the organization with a bare minimum for all organization regardless of risk. It is at this moment that one quickly realizes the tools are complex and can create a false sense of security in the organization. Managers need to be aware of the knowledge requirements needed to master security tools so that adequate resources can be allocated for ensuring security.

On the other hand, tools for hacking are increasingly simple to find and utilize. Many published securities flaws such as buffer overflows or exploits are quickly packaged up into script that any person with some skills can figure out. Furthermore, many scripts or command line arguments are bundled into simple graphical programs that anyone with little computer experience can utilize. Should a script or attack not work against the intended target, the hacker can simply utilize any number of other methods to find and exploit vulnerabilities; a distinct luxury an organization does not benefit from. It is clear that hackers have so much at their disposal that SMEs have a true problem.

METHODOLOGY

Practitioner and academic literature was reviewed for studies and data focusing on SMEs and security to determine if there was data to support the hypothesis that SMEs are more susceptible to security issues than larger organizations due to a lack of resources and technical expertise. This data was also looked at to see if this is a problem only for United States SMEs or if it is more global.

Hacking and Security tools were collected from the web and analyzed with respect to the knowledge needed to use them effectively. No attempt was made to collect tools from special hacker sites, only commonly available tools were considered. This was due to the focus on knowledge requirements, special tools and codes posted by hackers for hackers will be effective, to prove the premise that virtually anyone can become a hacker, we looked only at mainstream web tools. Additionally, only tools released since 2000 were looked at. Tools such as

SATAN, released in the mid 1990s are already known to be complex and difficult to use. Hacking tool effective use is being able to use the tool to cause damage. Security tool effective use is being able to use the tool to prevent access from unauthorized sources. Assessment was based on three levels of knowledge requirements:

Low Knowledge:
- Able to use GUIs and wizards
- No special knowledge of programming, operating systems, or networks required

Medium Knowledge:
- Able to modify macros or other code
- Basic knowledge of programming, operating systems, and net works

High Knowledge:
- Able to create custom macros or programs
- Detailed understanding of programming, operating systems, and networks

FINDINGS

Do SMEs Have a Security Problem?

Several studies were found looking at SMEs and security with the consensus being that SMEs are not miniature versions of larger firms, but quite unique in their own right as reported by Barnett and Mackness, 1983 but still true. Some key characteristics of SMEs include:

- Small business tend to rely on one or two persons to make all the critical decisions without the aid of internal employees/special ists and with the owners having knowledge in one or two functional areas of management (Meredith, 1994).
- The small business operating environment includes small man agement teams, strong owner influence, centralized power and control, lack of specialist staff, multi-functional management and informal and inadequate planning and control systems (Reynolds et al., 1994).
- Most SMEs are more concerned with running their businesses than with ensuring that the assets they have now are protected (**Suppiah-Shandre, 2002).**
- Cost is an issue for most SMEs when it comes to IT investment (**Suppiah-Shandre, 2002)**.
- Unlike large companies that have in-house IT personnel to manage their IT solutions and infrastructure, most SMEs depend on their vendors and system integrators for advice or to manage their security. Most SMEs cannot afford to have a full-time IT security officer on their staff (**Suppiah-Shandre, 2002, Bun ker and MacGregor, 2002).**
- Most small firms avoid sophisticated software or applications (Khan and Khan, 1992 and Locket and Brown, 2001). This view is supported by studies carried out in the United Kingdom by Chen (1993) while Cragg & King (1993), Holzinger & Hotch (1993), MacGregor & Bunker (1999 and 2000) and DelVecchio (1994) suggest that small firms often lack the necessary expertise to utilize IT effectively.
- IT/EC adoption inhibitors for SMEs include cost, skepticism about consultants and vendors, web accessibility and unfamiliar ity, lack of knowledge, lack of understanding of vendor advice, security, payments and technical details (Bunker and MacGregor, 2002 and Higgins, 1995).

Characteristics of SMEs with respect to security include:

- A relaxed culture and a lack of formal security policies (Blakely, 2002).
- A small IT staff with no security training (Blakely, 2002).
- Scarce investments in security technologies (Blakely, 2002).
- A lack of either business continuity or disaster plans (Blakely, 2002).
- Time, cost, and resource constraints restricting security efforts (Brake, 2003).
- Overly complex security solutions confusing SME staffs (Brake, 2003).
- Not knowing where to start (Brake, 2003).
- Security simply being put aside for more important things (Brake, 2003).
- Proliferation of 'always-on' connections increasing security risks (**Suppiah-Shandre, 2002 and** Donovan, 2003)**.**
- Believing that they will not be targets of hackers or cyber terrorists and that anti-virus software is sufficient (Jones, 2002).
- Reliance on vendors and consultants for knowledge and expertise (**Suppiah-Shandre, 2002) or on a single systems adminis trator (**Donovan, 2003).

Finally, some general observations on security threats:

- Security threats are growing both in scope and sophistication and forward-thinking organizations of all types and sizes will con tinue to strengthen their defenses against these threats (**Suppiah-Shandre, 2002).**
- Small businesses carry the burden of malicious attacks because they do not have the resources to immediately rectify security breaches, resulting in extended down-time, limited access to company and customer information, and the cost of cleaning up damaged data and hardware (Donovan, 2003).

Security will remain an issue for all businesses, large or small, but has the greatest potential to paralyze small businesses due to the high financial impact of losing commercially sensitive information, loss of productivity and the cost of fixing security breaches (Donovan, 2003).

These studies support the hypothesis that SMEs are more vulnerable to security issues than large organizations. However, the causes for this are more than just resource issues, organizations have cultural issues that increase their vulnerability.

Knowledge Requirements for Hacker and Security Tools

Support was found in the literature to suggest that hacking tools are getting easier to use while security tools are becoming more difficult. Figure 1 summarizes findings from the Electric Power Research Institute in the preparation of their security primer for electric utilities. The figure shows that hacking tools are gaining in sophistication while it is taking less knowledge to use them effectively.

Tables 1 and 2 summarize our findings with respect to hacker and security tools. Table 1 provides the knowledge ratings for the hacking tools we collected and analyzed. Table 2 summarizes the knowledge ratings for the security tools we analyzed.

Figure 1: Hacking Tool Knowledge Versus Security Tool Knowledge (Weiss, 2001)

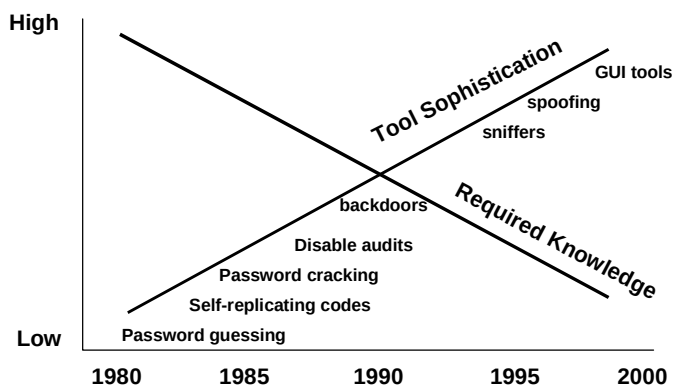

Table 1: Hacking Tool Knowledge Requirements (Jennex and Walters, 2003)

Hacking Tool	OS Knowledge Requirements	Network Architecture Knowledge Requirements	Programming Knowledge Requirements	Total Knowledge Rating
NSLOOKUP	Low	Low	Low	Low
NMAP	Low	Medium	Low	Low
Shed	Low	Low	Low	Low
NeoTrace	Low	Low	Low	Low
Ace Password Sniffer	Low	Low	Low	Low
Nessus	Medium	Low	Medium	Medium
John the Ripper	Low	Low	Low	Low
LOphtCrack	Low	Low	Low	Low
Back Orifice	Medium	Low	Medium	Low
Whois	Low	Medium	Low	Low
Passive Fingerprinter	Low	Medium	Low	Medium

Table 2: Security Tool Knowledge Requirements (Jennex and Walters, 2003)

Hacking Tool	OS Knowledge Requirements	Network Architecture Knowledge Requirements	Programming Knowledge Requirements	Total Knowledge Rating
NTOP	Medium	High	Low	Medium
Snort	Medium	High	High	High
Acid	Medium	High	Low	Medium

CONCLUSION

Most SMEs are more concerned with running their businesses than with ensuring that the assets they have now are protected. However, most SMEs could improve their IT security by about 80 percent with a few inexpensive and not necessarily IT-related actions (Suppiah-Shandre, 2002). However, the conclusion is reached that while the above statement may be true in 2002, it will not be so in the future. It is becoming easier to find and use hacking tools, and while security tools are also becoming easier to use, the dual nature of these tools means that the hackers will maintain their edge given the cultural and resource impediments to improving security that SMEs face. Security tools have a dual nature in that while they are designed to support implementing security, they can also be used to find and exploit vulnerabilities.

The hypotheses of this paper were that SMEs are more likely to have security issues than large organizations and that knowledge requirements for hacking were decreasing while knowledge requirements for hacking were increasing. The data supports that there appears to be a trend in declining knowledge requirements for hacking. However, we also see the trend for declining knowledge requirements for security tools. This implies that there is a gap between the knowledge required to hack versus that required to protect but it doesn't appear to be getting larger. Unfortunately, the data supports the hypothesis that SMEs are more likely to have security problems than large organizations. We observed no trend indicating that this is lessening, and actually conclude it is getting worse as SMEs adopt more sophisticated online applications.

It is also concluded that increased security awareness is not going to solve security issues. SMEs need to perform threat assessments to at least determine if they have at risk assets. It is postulated that a major cause of SMEs being more vulnerable than large organizations is a lack of strategic focus on what enables the SME to compete. Recognizing the value of these assets should induce more SMEs to focus their security expenditures on the correct security measures, this is supported by **Suppiah-Shandre, 2002** who observed that security is an area that many companies are willing to spend on but the type of system installed may not be enough. It is also postulated that large numbers of SMEs will not change their behavior or culture and will continue to be vulnerable until a sufficiently large watershed event occurs that forces them to address their security. Unfortunately, we do not know what the nature of this watershed event will be since it appears that recent events such as the 9/11 terrorist attack and the sobig virus have not caused significant changes in SMEs, Jennex, 2003.

REFERENCES

Allen, J.H., Mikoski Jr., E.F., Nixon, K.M., and Skillman, D.L., (2002). "Common Sense Guide For Senior Managers: Top Ten Recommended Information Security Practices," Internet Security Alliance, 1st Edition.

Barnett, R.R. and Mackness, J.R., (1983). "An Action Research Study of Small Firm Management," Journal of Applied Systems, 1983, 10: pp 63 – 83.

Blakely, B. (2002). "Consultants Can Offer Remedies to Lax SME Security," TechRepublic, February 6, 2002, retrieved from http://techrepublic.com.com/5100-6329-1031090.html October 3, 2003.

Brake, J., (2003). "Small Business Security Needs for the Changing Face of Small Business," Micro and Home Business Association, 14 August 2003, retrieved from http://www.security.iia.net.au/downloads/iia%20-%20launch%20sme.pdf October 3, 2003.

Bunker, D.J. and MacGregor, R.C. (2002). "The Context of Information Technology and Electronic Commerce Adoption in Small/Medium Enterprises: A Global Perspective," 8th Americas Conference on Information Systems, AMCIS, AIS, August 2002.

Chen J.C., (1993). "The impact of microcomputers on small businesses: England 10 years later," Journal of Small Business Management 31:3, 1993: pp 96 – 102.

Computer Security Institute, (2002). "CSI/FBI Computer Crime And Security Survey," Computer Security Issues and Trends, 8(1).

Cragg P.B. & King M., (1993). "Small Firm Computing: Motivators and Inhibitors," MIS Quarterly 17:1, 1993, pp 47 – 60.

Delone W.H., (1988). 'Determinants for Success for Computer Usage in Small Business," MIS Quarterly, 1988: pp 51 – 61.

DelVecchio M., (1994). "Retooling the Staff Along with the System," Bests Review 94:11, 1994: pp 82 – 83.

Donovan, J. (2003). "Small Business Security – Identifying Gaps And Providing Solutions," Symantec Security, February 28, 2003, retrieved from http://www.security.iia.net.au/downloads/small%20business%20security%20article%20-%20revised%2028%20feb_1.pdf October 3, 2003.

Doukidis G.I., Smithson S. and Naoum G., (1992). "Information Systems Management in Greece: Issues and Perceptions," Journal of Strategic Information Systems 1, 1992: pp 139 – 148.

Higgins K.J., (1995). "The Internet Beckons," EDI Information Week October 2, 1995: pp 66 – 70.

Holzinger A.G. and Hotch R., (1993). "Small Firms Usage Patterns," Nations Business 81:8, 1993: pp 39-42.

Jennex, M.E., (2003). "Information Security in the Era of Terrorist Attacks," Information System Security Panel, Information Resource Management Association (IRMA) International Conference Panel, Philadelphia, USA, May 20, 2003

Jennex, M.E. and Walters, A. (2003). "A Comparison of Knowledge Requirements for Operating Hacker and Security Tools," The Security Conference, Las Vegas, Nevada, April 23, 2003

Jones, H. (2002). "Small Firms Warned Over Hackers,' British Broadcasting Company, BBC, News, November 9, 2002, retrieved from http://news.bbc.co.uk/1/hi/technology/2428983.stm October 4, 2003.

Lockett, N.J. and Brown, D.H. (2001). "A Framework for the Engagement of SMEs in E-Business," 7th Americas Conference on Information Systems, AMCIS, AIS, August 2001.

MacGregor R.C. and Bunker D.J., (1995). "Computer Education Requirements for Small Business: A Survey., Information Resource Management Association International Conference Atlanta Georgia, 1995: pp 392 - 394

MacGregor R.C. & Bunker D.J., .The Effect of Priorities Introduced During Computer Acquisition on Continuing Success with It in Small Business Environments., Information Resource Management Association International Conference Washington, 1996: pp 271 - 277

Meredith G.G. (1994). "Small Business Management in Australia," McGraw Hill, 4th Edition, 1994

Ream, M. and Beales, A. (2003). "BCC Broadband Survey," British Chambers of Commerce, September 2003, retrieved from http://www.chamberonline.co.uk/pdf/Broadband_Survey_2003.pdf October 4, 2003.

Reynolds W., Savage W. & Williams A., (1994). "Your Own Business: A Practical Guide to Success," ITP, 1994.

SBA, (2000). "Small Business Expansions in Electronic Commerce," Office of Advocacy US Small Business Administration.

Suppiah-Shandre, H. (2002). "Security - Top Priority For All," SME IT Guide, International Data Group, Singapore, February 2002, retrieved from http://smeit.com.sg/psme.nsf/0/682CECE064DEE44748256B59004D6181?OpenDocument October 3, 2003.

Tetteh, E.O. and J.M. Burn, (2002). "A Framework for the Management of Global e-Business in Small and Medium-Sized Enterprises," Global Information Technology and Electronic Commerce: Issues for the New Millennium, editors: Palvia, P.C., Palvia, S.C.J., and Roche, E.M., Ivy League Publishing, Limited, pp. 215-254, 2002.

Weiss, J. (2001). "EPRI's Enterprise Infrastructure Security (EIS) Program," Electric Power Research Institute, March 12, 2001.