Hackers/Crackers and Their Effects on E-Commerce

The world seems to have caught on to the idea of shopping in you underwear, so for a business it seems that you cannot be economically effective if you do not give your customers opportunity to shop on the Internet. Thus, this has resulted in a growth in the electronic commerce market that ranges from online auction sites to department store shopping. This growth has come at no small cost to industries that have had hackers and their counterparts infiltrate their systems and cause a great deal of damage. This damage not only causes them to loose money through decreased sales but also through site restoration and heightened security costs. However, these problems could have been avoided by spending more money on security measures during the initial site planning.

E-commerce is defined as the conducting of business communication and transactions over networks and through computers[1]. In 1992, Compuserve pioneered this service by

[1] http://www.dictionary.com/search?q=electronic%20commerce

offering the first retail products online to customers[2]. Since then millions of companies have either started or placed their business online. This has enabled them to reach customers worldwide, but by doing so it also has attracted unwanted visitors as well.

This unwanted and malicious traffic has often been mistranslated by the media as hackers. A more correct term for them would be crackers. According to NISER[3], a hacker is defined as an individual who has strong interest in the workings of any computers and will not to damage the system. There are some hackers who have strayed away from this code and are commonly called black hat hackers. A cracker, however, breaks into systems usually using someone else's code and inflicts damage and defacement to the site.[4] Together these two groups cause a company much grief and cost them a lot of time and money.

A classic example of this is when several international sites belonging to Microsoft.com were hacked. Initially, there did not seem to have been any damage to the

[2] http://newmedia.medill.northwestern.edu/courses/nmpspring01/brown/Revstream/history.htm
[3] National ICT Security and Emergency Response Centre
[4] http://www.niser.org.my/sec_faq.html

sites, but when further research was done it was found that certain source codes were viewed and possibly copied[5]. The source code is the basic building blocks of computer applications and it relates to the computer how the program is to function.

It is also noted that Microsoft not only has a problem with hackers seeing their source code, but also with crackers defacing many of their overseas sites. According to results found on Alldas.org (see Table), Microsoft has been defaced on at least thirty-six separate occasions. Also according to these results, there were twenty-two different attackers. This means that some of the attackers hacked into Microsoft on several different occasions and in several different locations. The dates of these attacks range from January 7, 2001 until March 30, 2002. By these statistics, it seems the hacks are still taking place. This proves that if a giant corporation like Microsoft could be hacked while spending millions of dollars each year on security, it could happen to anyone.

[5] http:www.thesstandard.com/article/display/0,1151,1976700.html

One cannot assume that this was due to lack of preventative maintenance on the part of Microsoft.com. No Internet based company will ever be 100% secure. This is because a hacker or cracker only needs to send an alluring email containing a well-disguised virus to an employee inside the company. Upon opening the email, the virus is automatically placed in the system. Anti-virus software can only find viruses by locating signatures of older viruses. All an attacker has to do is slightly modify the signature to get through.

Microsoft learned the following six lessons, which could be taken by other companies as well in order to prevent such numerous attacks[6]:

1. Offsite computer must be secure have a personal firewall and, up-to date Anti-Virus scanner software
2. External passwords must be kept secure
3. Proactive review of network logs
4. Defense inside the company network by routing all internal modems through firewall as well
5. Once previous steps completed email viruses and web servers become a primary means of network attack
6. Microsoft's own products are the primary target of hackers, so extra precautions need to be taken in the design of their software.

[6] http//www.sans.org

Neglecting any one of these will increase a company's vulnerability of being hacked into.

These and similar attacks caused merchants to wary of online business. Programs created by black hat hackers and crackers duplicate and enter false numbers and identifications. These programs have effected, as shown in a recent study, $700 million of online sales that were lost due to Internet credit fraud in 2001. This is about 1.14% of all online sales compared to only .06% of all real world sales. Because of this credit card companies have fought back by adding passwords and implementing checks for authenticity of online customers[7].

Because of the problems that hackers and crackers have caused, the most productive way a business can prevent these attacks is by implementing preventive maintenance. The first and foremost way to start this is to make sure that all Internet and network connections inside the company go through a firewall. A firewall is computer hardware or software that prevents unauthorized access to private data

[7] http://news.com.com/2100-1017-850258.html

inside a company's network[8]. In other words, a firewall examines all the data trying to enter and exit the network and then determines via user-implemented restrictions whether or not it is allowed to pass through.

A daily review of network log can often detect unusual activity of hackers trying to penetrate internal machines. It is essential to detect these unusual patterns and if a company does this at least once or twice daily it can save them much embarrassment and can intercept the problem before it occurs. This can also be used to track employee's use of the system, which is another major security issue.

The leads us to the next step in preventive maintenance is to keep tight security on each employee's passwords and their restrictions allowed on their computer. This seems to be one of the most neglected areas of security. According to an article in vnunet.com, network managers said they felt that the staff was the weakest link in any security policy[9]. This problem is brought on by ignorance and/or spitefulness of an employee. An unsuspecting employee could open an email titled "Poem about the 9/11 tragedy" or some other

[8] http://www.pcwebopedia.com/term/f/firewall.html
[9] http://www.vnunet.com/News/1114779

tempting subject line and accidentally let in a virus such as the QAZ virus[10], which was used to hack into Microsoft's sites[11]. Allowing the employee access to the Internet through a modem that tunnels around the firewall also provides easy access for hackers and crackers. Also, disgruntled employees with few restrictions as far as what they can access on their computers could purposely try to get into, steal, or deface private company files. Companies need to recognize the symptoms of untrustworthy employees and address them.

With all this knowledge about security and all the software available, there is one major setback to implementing these techniques. Cost. For example, Netcraft offers an e-commerce security analysis with a starting cost of around $7,000. Along with this problem comes a time factor. The minimum extent of time for a full analysis of this type is 5 days[12]. Even thought this seems like a lot of up front costs and downtime, the typical cost of rebuilding a relatively inexpensive site after an attack can meet or

[10] http://rr.sans.org/malicious/QAZ.php
[11] http://networking.earthweb.com/netsecur/article/0,,12084_625631,00.html
[12] http://www.netcraft.com/security/ecommerce.html

exceed $50,000. This would include investigating the vandalism, rebuilding, and testing an upgraded security system[13]. This does not include the revenue a corporation looses due to its downtime.

As earlier mentioned, no site can be 100% secure. There are several things to consider once your site is hacked. First you should consider your two major options. The first one is to disconnect and prosecute. This consists of immediately disconnecting the affected host and analyzing the traces for possible prosecution. The second option is to continue and track the intruder. When using this option, the administrator should be simultaneously backing up all the important data[14]. This is an example of a honeypot, or a network decoy[15]. This allows the network administrator and as well as companies such as MyCert.org[16] to track and study the hacker's actions. This allows them to not only prosecute the hacker, but also to learn how to better secure their own system[17].

---

[13] http://www.netcraft.com/security/whitepaper.html
[14] http://www.niser.org.my/sec_faq.html
[15] http://www.webopedia.com/TERM/h/honeypot.html
[16] http://www.mycert.org/
[17] http://ecommerce.internet.com/news/insights/outlook/article/0,,7761_559431,00.html

As the World Wide Web continues to grow with new E-businesses added every day, more and more opportunities are opening for hackers and crackers with malicious intent to deface them. More capital must be put into security measures to keep up with the never-ending race against the hackers worldwide. Regardless of if it is spent before or after the attack it must be spent to keep the business alive. Hackers and crackers have affected E-commerce in many negative ways but the ending security measures taken has been positive. These final measures reassure the customer that their purchases are secure and they will have access to the site at all times.

Taken from Alldas.org at http://defaced.alldas.org/

Record #	Date(dd/mm/yyyy)	Original Site	Attacker	OS
1	07/01/2000	www.microsoft.com.tw	inferno.br	Unknown
2	03/06/2000	www.microsoft.com.br	InSaNiTy ZiNe c0rp.	Windows
3	11/08/2000	www.fuckmicrosoft.net	DT	Solaris
4	14/12/2000	www.microsoft.si	Furia.BR	Windows
5	18/12/2000	www.microsoft.si	BoLoDoRiO	Windows
6	23/01/2001	www.microsoft.co.nz	Prime Suspectz	Windows
7	27/03/2001	www.microsoft.economy.ru	PNW	Windows
8	27/03/2001	www.microsoft.motivforce.com	PNW	Windows
9	19/04/2001	www.microsoft.be	BLACK-FUUUUUUUU	Windows
10	20/04/2001	www.microsoft.com.gr	Prime Suspectz	SCO
11	20/04/2001	www.emicrosoft.org	IMCB	Windows
12	22/04/2001	www.microsoftofficetips.com	PoizonB0x	Windows
13	26/04/2001	www.microsofttrainingcenter.com	PoizonB0x	Windows
14	27/04/2001	www.microsoft.com.gr	WoH	SCO
15	03/05/2001	www.microsoft.co.uk	Prime Suspectz	Windows
16	04/05/2001	www.microsoft.com.sa	Prime Suspectz	Windows
17	04/05/2001	www.microsoft.com.mx	Prime Suspectz	Windows
18	06/05/2001	www.microsoftofficetips.com	Silver Lords	Windows
19	08/05/2001	streamer.microsoft.com	Prime Suspectz	Windows
20	09/05/2001	pc.microsoft.is	Prime Suspectz	Windows
21	10/05/2001	www.ilmicrosoft.com	Silver Lords	Windows
22	12/05/2001	www.microsoft.motivforce.com	Nukkets	Windows
23	13/05/2001	www.microsoft.nsk.ru	cr1m3 0rg4n1z4d0	Windows
24	15/05/2001	www.microsoft.nsk.ru	Anti Security Hackers	Windows
25	17/05/2001	www.microsoftware.co.jp	PoizonB0x	Windows
26	18/05/2001	www.microsoftware.co.jp	KERNEL	Windows
27	18/05/2001	www.microsoft.ro	pentaguard	Windows
28	18/05/2001	www.ilmicrosoft.com	PoizonB0x	Windows
29	19/06/2001	www.interface.microsoft.co.za	BlackSun	Windows
30	21/06/2001	redsand.rte.microsoft.com	Prime Suspectz	Windows
31	21/06/2001	arulk.rte.microsoft.com	Prime Suspectz	Windows
32	27/07/2001	www.microsoft.com.sa	m0sad	FreeBSD
33	08/03/2002	www.microsoft.economy.ru	Shadow Lords	Windows
34	16/03/2002	officecouncil.rte.microsoft.com	Perfect.br	Windows
35	24/03/2002	cust-supp-chat.one.microsoft.com	Silver Lords	Windows
36	30/03/2002	microsoft.pre-cursor.co.uk	DarkCode	Linux