Cyber Crime – Enemy Inside

Way back in 1992, a movie called 'Sneakers' with a star-studded cast of Robert Redford, Ben Kingsley, James Earl Jones, River Phoenix and Dan Ankroyd hit the screens depicting the early times of cyber crime.

It showed a new type of criminal infiltration, where brains rather than brawn and traditional defences like 6-inch steel doors, security guards and close-circuit television were as useless and almost comic in its application.

And true to its adage, art imitates life, but this time, we are the actors and the world and your enterprise are the stage; and ripe for the picking.

If you are looking around and wondering what this all means, well, it means governments, multinational corporations (MNCs) and small and medium businesses (SMBs) are looking to have their precious data compromised right before their eyes without any warning.

WHAT IS CYBER CRIME?

The general definition of cyber crime would be the criminal activity where your computer or network is the source, tool, target or place of the crime.

If you are the source then it means the criminal activity is happening from the inside – with crimes like fraud, theft, forgery and embezzlement as some of the traditional crimes using a computer or network.

If you are the target, then you are looking at a few but devastating examples like malware or malicious code, denial-of-services and computing virus.

To prevent "cyber attacks" to happen in your company, it is good to understand how it can happen to an SMB in the first place.

In life, we always tend to think that bad things always happen to the other guy who is more vulnerable and more 'targetable.'

CYBER TERRORISM

Like in 2007, Estonia experienced a series of cyber attacks that swamped its organisation's websites which included parliament, banks, ministries, newspapers and broadcasters.

This involved denial-of-service, spamming using botnets, and website defacement, one of which was the Estonian Reform Party.

This attack known as the Estonian Cyberwar is now a classic case study for many countries and military planners and considered as one of the most sophisticated cyber attack scenario ever attempted.

But like we think, cyber-terrorists are only looking for the big boys, not small guys like SMBs. Wrong.

In 2006, a study by the Federal Bureau Of Investigation or FBI revealed that 9 out of 10 companies have suffered incidents involving cybercrime, with much focus on the business community. It was also reported that one out of five organisations had attempts to steal their data, sabotage their systems and defraud the company in some way.

And why is there an upsurge in cyber crimes? According to the FBI, the revenue earned from cyber crime now exceeds the revenue criminals earn from drugs, prostitution and trafficking. And they do it because it is easy since internet users are unaware of the dangers.

It is basically a low risk, high gain criminal activity.

LET'S GO PHISHING

Let's suppose you receive an email from your various banks asking you to update your details. You click on the link and you reach your bank's website or so you think, since it looks exactly like it.

You enter your account number to verify and Viola! You can update your details without leaving your home! You nod your head and declare the internet is a godsend. While that could be construed as true, it all depends if you were a victim of a phishing scam. If you were, then you can expect your information to be compromised, and your bank account vacuumed dry.

This was what happened recently in the United Kingdom when residents were informed they were due for a tax refund. Those who followed the bogus instructions had their bank accounts cleaned out and their credit cards charged to the limit.

FAST AND FURIOUS

Here's an idea how fast the malevolence can spread. In July 19, 2001, 359,000 computers were infected with the Code-Red (CRv2) worm in less than 14 hours. The worm began to infect hosts running unpatched versions of Microsoft's IIS webserver. The worm spread by probing random IP addresses and infecting all hosts vulnerable to IIS exploit. At its peak over 14,000 hosts were infected every minute.

In a study of this cyberattack, by David Moore and Colleen Shannon from the Cooperative Association for Internet Data Analysis or CAIDA, it was concluded that the speed and geographic extent of the attack showed how so very vulnerable we all are; especially SMBs.

In the report it stated that,

"This assault also demonstrates that machines operated by home users or small businesses (hosts less likely to be maintained by a professional sysadmin) are integral to the robustness of the global Internet. As is the case with biologically active pathogens, vulnerable hosts can and do put everyone at risk, regardless of the significance of their role in the population."

This simply means that SMBs are not only extremely vulnerable but also one on of the best targets to become host and source in the infection process.

SURVIVAL TIPS

Small Business Security Portal.com 1 shares basic guidelines to protect the information infrastructure, to wit:

1. Never open email attachments or download files from unknown sources;
2. Beware of unknown emails with vague subject lines e.g. "document" or "re:document" – they could be a virus. Avoid opening email attachments when the subject line is suspicious even if it appears to come from a friend or someone you know. When downloading files from the Internet, make sure that the source is a legitimate and reputable one;
3. Delete chain emails and junk email. Do not forward or reply to any to them. These types of email are considered spam, unsolicited mail that may contain viruses;
4. Ensure your computer has a firewall intrusion prevention and virus protection software with automatic updates. Companies like Norton, Symantec and McAfee all sell such software packages.
5. Keep your anti-virus updated. There are over 80,000 known viruses and 500 new ones appear every month. Use anti-virus software and services that regularly update current virus information and its scanning engine;
6. Back up your files. A virus can destroy your files. Make sure you backup your files regularly and keep your back up copy in a separate location from your work files, preferably not on your PC hard drive;
7. Ensure your computer's operating system is up to date by visiting the manufacturer's website (e.g. Microsoft);
8. Never enter your credit card or password details unless you are sure the site is real / protected;
9. Seek professional advice from companies whose job is to protect, preserve and upgrade your networking and communication systems no matter how big or small your enterprise.

FIGHTING BACK

In an interview with ZD Netasia late last year, Nato's cyber defense chief Suleyman Anil, said that "computer-based terrorism poses the same threat to national security as a missile attack."

Realistically, the head of Nato Computer Incident Response Capability Co-ordination Centre stresses that a determined cyber attack on a country's online infrastructure would be "practically impossible to stop".

So if it's impossible to stop, what should SMBs do?

In reel life, the good guys always beat the bad guys. And since art imitates life, we can be assured that the good guys will do whatever they can to contain the new evil and win.

But only this time the good guys are not the other guy but you, the SMB. You need to understand and know what you are up against and how to beat the enemy that can worm through your locked gates and into the very heart of your business and lives.

Cyber crime and their players are not just on the news, or the stuff movies are made of. We could be the very victims right now. It could be someone right under your nose, or someone 10,000 miles away. Working anytime and anywhere without your knowing...

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel : 408 526-4000
800 553-NETS (6387)
Fax : 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**