

Rotaract Club community services director, Gilbert Carmichael, calls for persons and institutions to work towards solution to indiscipline in the schools.



Hackers, viruses caused great damage in 2003

INTERNET security firm WSI estimates that digital attacks from hackers and viruses have resulted in over US\$100 billion in damages to websites worldwide in 2003.

A record level of attacks - 20 000 in the month of January alone - helped make Internet security one of the leading issues in the online world in 2003. It is predicted that these numbers will continue to increase with the total economic damage from all types of digital attacks worldwide passing the US\$250 billion mark in 2004. This poses a serious threat to online businesses, but it's a threat that can be combated through proper education on the subject. This is the message being relayed internationally by WSI, the world's largest network of Internet consultants.

Once a business has made the decision to go online, there are a number of important considerations beyond the development of the site itself. Concepts such as security - an ongoing and evolving process - is rarely given the attention it deserves.

Through the consulting services offered by WSI, a business can acquire the critical knowledge it needs to protect itself from becoming an Internet security statistic. "Education is the key to a business protecting itself online," explains WSI Internet consultant Rene Garcia. "Every day companies unknowingly make mistakes that leave their systems vulnerable to digital attacks. With the proper

knowledge and software in place these mistakes can be avoided, saving money and increasing productivity and efficiency in the process." Typically, the news media focuses on attacks to large corporations and government agencies, leaving small- to medium-sized businesses with the impression that Internet security isn't an issue that concerns them. Unfortunately, this isn't the case.

Definite threat to all

Any business, no matter what its size or function, faces potential threats from hackers each day for numerous reasons. By teaching companies how to defend their systems, WSI Internet consultants strive to keep their clients informed and safe. As WSI clients know, one of the largest daily threats is the increased reliance on email - one of the most versatile and important tools to any online business. However, email as a communication medium is insecure and opens the door to potential attacks such as virus distribution and unsolicited advertisements or "spam".

The popularity and widespread adoption of e-mail is no accident; it is often more efficient than other means of communication and allows customers to quickly contact a business from anywhere in the world at any time of day. But as inboxes fill up with orders, inquiries and correspondence, they also fill up with spam.

In November 2003, measurements by Brightmail's Probe



Business Monday

Network showed that 56 per cent of all e-mail was spam related. This has caused many industry insiders to predict that by mid-2004 spam will surpass the 60 per cent mark.

And with ever-increasing spam comes larger threats to security.

It also has a negative effect on server and storage space and can slow down connection time. In addition to this, effect on valuable network resources, spam can also contain malicious code, and in some cases has been connected to credit card fraud and software piracy. With thousands of email messages being received and sent by individual companies each day, many businesses are making themselves an easy target to hackers, viruses and spam.

By utilising WSI's industry leading technology such as intrusion detection applications, authentication devices and firewalls, a business can position itself to avoid the costly consequences associated with digital attacks.

Few can forget how fast the Sobig.F virus spread through the online world this past August, crippling entire network systems with the sheer volume of email traffic it produced. In just a few short weeks, this email-based threat caused US\$29.7 billion worth of damage to companies worldwide that were caught unprepared for such an attack.

Businesses can avoid costly security threats by practising safe online behaviour and employing server-based traffic filtering technologies, such as those offered by WSI's hosting environment. As each business is different, WSI Internet consultants can assess which methods will suit a particular company best and then deploy those solutions to protect their clients. As WSI Internet consultant Garcia says, "Knowledge is power and with the right information in hand, most Internet security threats can easily be avoided."

'MyDoom' worm spreads as hunt for author intensifies

LONDON - A cyber dragnet aiming to flush out the author of the MyDoom computer worm intensified on Friday as the outbreak crippled still more e-mail networks.

Investigators and security experts hoped their hunt would get a boost after Microsoft Corp. offered a US\$250 000 reward on Thursday for information leading to the arrest and conviction of the creator of one variant, MyDoom.B.

The offer follows a similar \$250 000 bounty from software firm SCO Group Inc. The "doom" viruses are programmed to unleash digital attacks aimed at overwhelming both firms' Internet sites starting this weekend.

"If there is a break, it will come from the bounties," said Mikko Hypponen, research manager at Finnish anti-virus firm F-Secure.

MyDoom.A, also known as Novarg or Shimgapi, emerged on Monday often masquerading as an e-mail error message from a "Mail Administrator" and other official-looking addresses that contains a file attachment. Hundreds of thousands of computer users have clicked on the seemingly benign attachment, infecting their computers.

The attachment releases a programme capable of taking over the victim's computer, experts warned, before scouring the Internet for more vulnerable machines.

The effect is a massive log-jam of data traffic that bogs down e-mail servers and re-

jects many incoming and outgoing messages.

Computers running any of the latest versions of Microsoft's Windows operating system are at risk of being infected, although the worm does not exploit any flaws in Windows or software.

Patches capable of wiping the virus off a machine are available at anti-virus sites.

On Friday, there was no sign of a let-up.

"It's still spreading voraciously. We've intercepted in excess of eight million viruses since the very first copy started Monday," said Paul Wood, chief information analyst with MessageLabs, an e-mail security firm.

'Nothing personal'

After dissecting the malicious programme, security experts got a little closer to unmasking the perpetrator. The author apparently signed the worm with the name "Andy" and left the message: "I'm just doing my job, nothing personal, sorry."

The first infected e-mails detected appear to have originated in Russia, but, Wood said, it was unclear if they were the engineers behind MyDoom or just early victims.

Nabbing virus writers is a difficult undertaking. Such clues have been used in the past to form a picture of the suspect.

"Most often virus authors are caught when bragging about their exploits somewhere," said Wood.

Given the tight-lipped approach, security experts and

police suspect the authors may be a new breed of virus writers that possibly have a

connection to organised crime groups or spam e-mail peddling syndicates.

Vacancy



MEMBER ANS M.C.E.L. GROUP

SGS Petroleum Inspector

SGS (Societe Generale de Surveillance) Controls Services Inc., a subsidiary of Alstons Shipping Ltd. - Trinidad, is in the process of establishing a SGS Office in Barbados and therefore has a career opportunity for an individual to look after the inspection business in Barbados.

Job Responsibility

Plan and conduct inspection surveys with customers for the purpose of evaluating various products and commodities viz Petroleum products, LPG, Methanol, Anhydrous Ammonia, Caustic Soda, etc.,

Also perform container inspections of dry cargoes, Draft/Bunkers/Off-Hire surveys, etc.

Prepare preliminary and final reports on inspections

Transmit via email or telefax inspection information on a timely basis to the customer

Perform at a high level of efficiency working without supervision and for long hours at a time

on assignment on board vessels or at shore side terminal

Able to relate with all different types of terminal operations

Qualification and Experience

A Technician's Diploma (laboratory science) or Process Plant Operator's Diploma or Natural Gas Technology Certificate

The incumbent must possess a minimum of 5 GCE O' Levels or CXC passes including Mathematics, English and Chemistry. Computer literacy will be an asset. Strong inter-personal skills, good working vehicle and valid driver's permit required.

The successful candidate would be afforded a three-month training period in Trinidad.

All interested persons are to send their resume, no later than February 13th, 2004, to:

The Group Human Resources Manager,

McEamney Alstons (B'dos) Ltd.,

Wildy, St. Michael. FAX: 467-2605 E-Mail: dhamilton@mcalbds.com