Name of Publication: Business Today
Date of Publication: 1/2004
Page(s) in Publication: 85

Electronic Nightmares

Nasty digital bugs can destroy an entire business

They are the most devious and malevolent of creatures. Moving with swift stealth, they can bring airlines, banks, corporations and even governments to their knees. Viruses, bugs and worms and the so-called cyber-terrorists behind them are the scourge of the electronic seas.

While many of the viruses and worms originate as pranks hatched up by adolescent net-nerds gone wrong, these security threats are no joking matter for today's increasingly computerized business world.

Just look at the speed with which Sobig-F, regarded as the biggest virus threat of 2003, spread. Specialists estimate that it infected one out of every 17 e-mails worldwide after its appearance on Aug. 18, 2003.

Other threats are motivated by what specialists call industrial espionage, where paid hackers – as opposed to recreational – infiltrate businesses' IT infrastructure to steal information that can benefit competitors.

Far from being minor nuisances, such cyber attacks cost an average of $500,000 per company in lost business, lost hardware and lost time, according to Amro Elfiky, technical marketing executive at the Giza office of Internet Security Systems (ISS), one of the top five internet security providers in the world, according to IDC. All in all, analysts estimate that more than $2 billion is lost annually due to IT security breaches.

"Lack of awareness is where the roots of almost all security risks can be traced, especially in the MENA region," says Sherif Shaltout, senior X-force analyst at ISS. "The No. 1 rule in IT security is education. If I have a company and I don't understand the impact of security on my business and how it can keep me going, then the minute I have an incident, I am down the drain."

But IT security is often at the bottom of management's to-do list.

"Business managers don't perceive security as a business enabler," Elfiky adds. "They don't see it as an investment on which to expect return, but rather as a luxury they can enjoy when they have enough money to spend."

According to a 2002 report by IDC, spending on IT security in the Gulf region alone is expected to increase by 30 percent from 2002 to 2007, reaching $161 million. Elfiky says that due to the cost of high-end security solutions, large multinationals and state-owned enterprises have been the biggest clients for the security firm, with small and medium businesses lagging far behind.

To raise awareness about security, the Ministry of Communications and Information Technology organized a conference – "Ensuring Security in the IT Infrastructure" – last November where Egyptian and international tech experts highlighted the dangers of cyber-threats. Tossed around were martial-sounding buzz words like demilitarized zone (DMZ), firewalls, proxy servers and intrusion detection – not to mention prevention.

Anas Chbib, managing director of AGT, a German firm providing wall-to-wall IT security solutions to the MENA market, flew in from Berlin to drum up business at the conference.

"There is a problem that stems from deep inside governments, financial and telecommunications sectors," he claims. "They don't appreciate that protecting information is more than just saving into their PCs or installing anti-virus software. IT security needs to be looked at from a more strategic, policy-oriented view."

Elfiky says that although a greater percentage of corporate budgets are earmarked for IT security, the impact has been muted due to a "plug and walk away" attitude.

But in a world where new threats crop up every month, such an attitude is not likely to protect the Middle East against increasingly sophisticated – and common – attacks. According to a global survey by ICSA Labs, a leading IT security product certifier, 105 machines out of every 1000 were the subject of a cyber attack each month in 2003. Less than five years ago, only 32 machines were attacked each month.

The financial and communications sectors have taken the most proactive steps towards preventing cyber attacks, Chbib says, by installing comprehensive security measures.

"Deutsche Bank has a million online transactions per day," Chbib adds. "And if they only make $1 per transaction, that is $1 million lost in one day if their system becomes inoperable."

At the end of the day, however, no business can enjoy complete security. Studies estimate that 80 percent of threats emanate from employees authorized to have access to a company's IT system. bt