DIGITAL STRONGHOLD

The Star - 19/4/2007.

Govt constantly works to keep its online services safe from cyber attacks

By SIM LEOI LEOI

AS MORE of the Government's functions and public delivery system shift into high technology mode, a key concern will be if the computer infrastructure powering these online services is safe from cyber attacks.

After all, world news is replete of the latest attacks from virulent "viruses", "trojan horses" and "worms" by hackers hopping a dig at sensitive and confidential information.

As Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) ICT Security Division Director Wan Mohd Rosdi Wan Dolah put it succinctly:

"One can have loads of services available online, but these have no use if the public doesn't trust your computer networks and security."

Thus, for Malaysia's vision of electronic government to really take off, it first needs to instil public confidence in the public sector's network security.

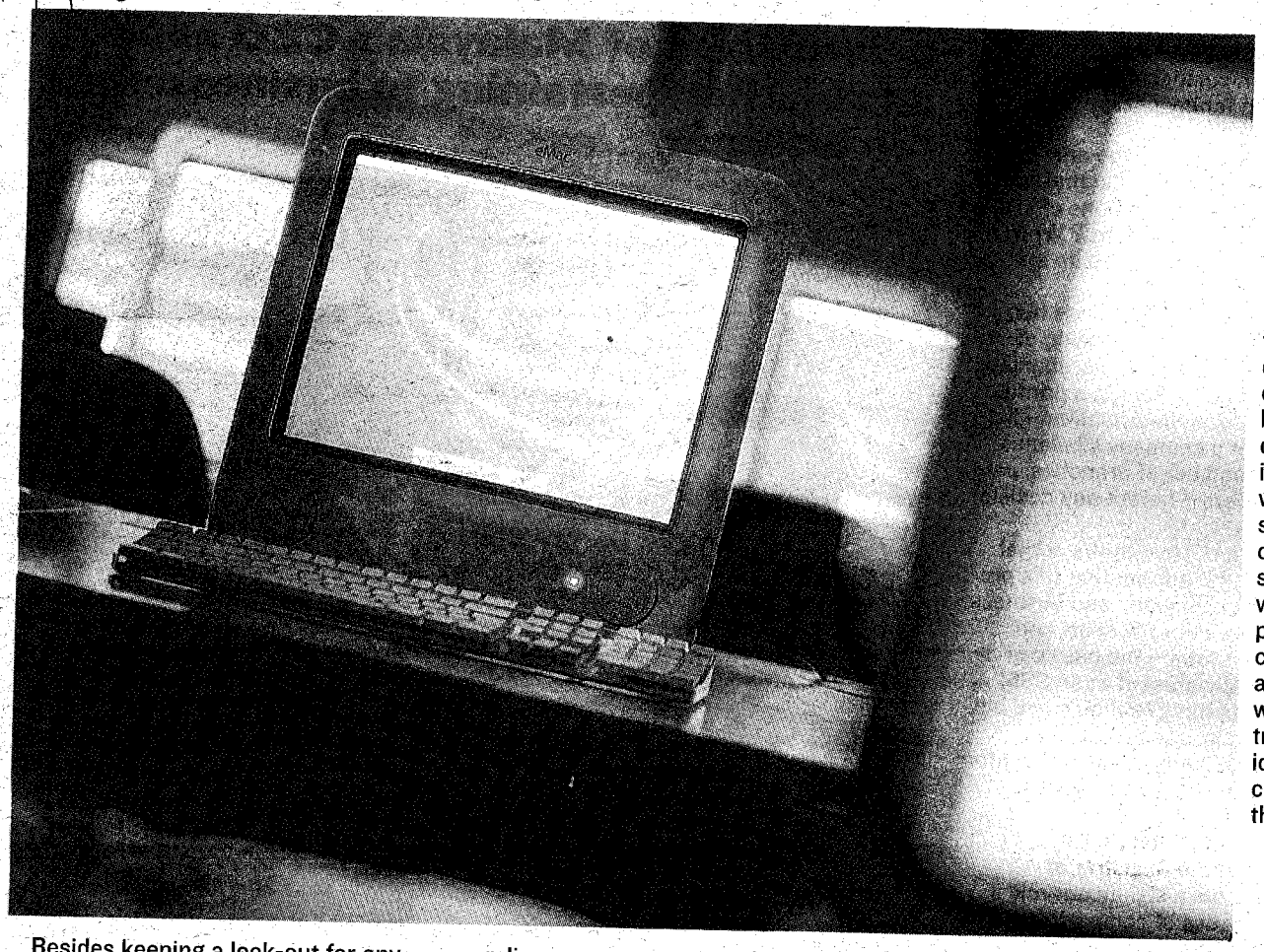
In 2003, the Government ICT Security Command Centre (GISCC) was set up to provide close monitoring, detection and response to online security breaches as well as to reduce the risk for it.

GISCC consists of the Government Computer Emergency Response Team (GCERT) and the Public Sector Network Monitoring System (PRISMA).

While PRISMA'S main role is to detect any attempt at intrusion through alerts from censors installed in the agencies, GCERT receives reports on incidents and is responsible tracing the source of attack and providing technical advice on safeguards and countermeasures to prevent future attempts.

GCERT also makes it compulsory for the Chief Information Officer in charge at every government agency to report to it any untoward "security incident", whether this be an attempt to illegally gain access into its data, denial of service attacks or changes made to software without authorisation.

These incidents are then ranked according to its urgency – priority one for those that may jeopardise lives or the country's security, and priority two for those ranging from break-ins via Internet infrastructure on domain name servers and the defacing of websites.



Data protection: Besides keeping a lookout for any security breach, GCERT is tasked with countering the effects of such break-ins, disseminating information on ways of strengthening computer systems as well as providing consultancy to agencies wanting to track and identify the culprits behind the attacks.

Besides keeping a look-out for any security breach, GCERT is tasked with countering the effects of such break-ins, disseminating information on ways of strengthening computer systems as well as providing consultancy to agencies wanting to track and identify the culprits behind the attacks.

As another frontline defence, the ICT Security Division in MAMPU is also in the process of identifying key agencies within the whole Malaysian administration, where its computer system – and the integrity of the data contained within - is of utmost importance to the country.

"The point of identifying these agencies as Critical National ICT Infrastructures (CNII) is so that we can establish CERT teams to be placed there.

"This will be able to strengthen the management of ICT security incidents at these agencies. This team will act as a first level support to handle our response, to monitor and disseminate information on any matter relating to ICT security," he pointed out.

Among agencies to be considered in the category of CNII are departments like the Immigration, Customs and the National Registration Department, where reliance on computer and data storage is heavy.

"We hope most of the CNII agencies will in the future comply with the standard and best practice in ICT security management.

"Certification is, of course, necessary if the agencies wish for third party endorsement that their ICT security management complies with international best practice standard.

"For the Ninth Malaysia Plan, we hope to have at least 20 CNIIs to be thus certified once these have been identified. Having certification such as ISO will boost our customers' and the public confidence in government service delivery as it continue to introduce more online services in the future," Wan Mohd Rosdi said.

The Government, he said, had also put into place the latest anti-virus and firewall software but all this would have come to naught if the people remained gullible.

This was because ultimately the world's best protection against any hacking or attempt to crack into a computer data system, lies with the very people using this same network.

"Sometimes, the staff may be willing to let his or her password be used by an outsider to access websites on their computers in offices. They may think this is not a serious matter.

"But it can have consequences if the outsider proves to be untrustworthy and takes the opportunity to check out confidential data stored in that computer," he explained.

Another serious matter, added Wan Mohd Rosdi, was the tendency of staff to bow to the "pressure" of giving away confidential information to people claiming to be their superiors.

"For instance, an impostor can call up on the telephone claiming to be representing a minister's office and seeking access into certain confidential domains of the computer network. In this way, passwords can be obtained to gain illegal access into our network.

"To counter this practice, there must be more awareness campaigns carried out to change the way our staff think and act," he said.

The division, added Wan Mohd Rosdi, already had over 1,000 officers exposed to ICT security awareness programmes and issues and hoped every civil servant would be able to handle the most basic of computer security issues.

"After all, everyone works on a computer now," he said.