

National Security

BRIEFING NOTES

Advancing domestic and national security practice
July 2007



2007 E-Security National Agenda

The Australian Government has released its significantly revised *E-Security National Agenda* today. It introduces new coordination mechanics to address e-security threats and a number of new initiatives. The agenda has been allocated a budget of \$73.6 million over 4 years.

The new *E-Security National Agenda* updates the former one released in 2001 and reflects three significant changes in the e-security landscape, according to Mike Rothery, Assistant Secretary, Critical Infrastructure Protection, Attorney General's Department.

Firstly, where once IT security in the three areas of critical infrastructure, home and SMEs, and government were all seen as unrelated, today they are seen as highly inter-related. Consequently the agenda brings together all policy and programs in these areas under the control of one government committee.

"The best illustration of the interconnectivity of these three issues is the fact that poor personal computer security has led to significant numbers of Australian household computers being infected with malware which have been used in botnets for massive distributed denial of service attacks (DDoS) on critical infrastructure and government agencies, such as that seen in the Estonian attacks in May 2007", said Mr Rothery.

To ensure effective e-security coordination across the three areas of critical infrastructure, home and SMEs, and government, one whole-of-government committee has been established. Called the E-Security Policy and Coordination (ESPaC) Committee, this committee replaces two former committees – the Electronic Security Co-ordination Group (ESCG) run by DCITA and the Information Infrastructure Protection Group run by the Attorney-General's Branch. The chair of ESPaC is Keith Holland, First Assistant Secretary,

Security Law and Justice Branch, Attorney-General's Department.

The second major departure from the last agenda reflects that there has been a marked increase in the sophistication of e-security attacks. This has required a different response from the past. Historically, the vast majority of attacks, whether phishing attacks, viruses, worms or social engineering, were mass distributed enabling anti-virus and anti-malware companies to identify them. These companies would then quickly incorporate counter-measures into the daily anti-virus update which were automatically downloaded by their subscribers. "However increasingly, the attacks are targeting very small groups, often in conjunction with social engineering, meaning that the anti-malware software companies have difficulties identifying the attacks and protecting their clients", said Mr Rothery. The consequence of this is that the agenda includes initiatives to address the threats that anti-malware companies find more difficult to detect.

Thirdly, the e-security threat is changing so rapidly that the traditional cycle of reviewing government strategies every 4 years is not appropriate. Consequently the new agenda will be reviewed every 2 years for relevance, effectiveness and efficiency.

3 Priorities

The 2007 *E-Security National Agenda* has 3 priorities.

Priority 1: Reducing the e-security risk to Australia's national critical infrastructure

This priority has resulted in additional funding and initiatives for two agencies.

Critical Infrastructure Protection Branch, Attorney-General's Department (CIPB)

CIPB has been funded to significantly expand the operations of GovCERT (Australian Government Computer Emergency Readiness Team). GovCERT

will increase its support to owners and operators of Australia's critical infrastructure, which started in November 2006, to help them reduce the risks from sophisticated electronic attacks and to provide government with information about the electronic risks facing critical infrastructure. Specifically, this will involve identifying those threats not readily detected by commercial anti-malware providers, and working with potential targeted infrastructure. This could include profiling victims of attacks, briefing IT managers on the threat, informing them where to look for evidence and then keeping them updated on emerging threats. An example of a sophisticated new attack that GovCERT could identify and address is a new espionage trojan software. This trojan has been developed to capture passwords for commercial espionage purposes, and gets loaded onto compromised websites. When users visit that website, the trojan automatically gets downloaded onto the user's computer. GovCERT will get 10 additional staff to carry out this work.

The Computer Network Vulnerability Assessment Program run by the CIPB will come under GovCERT. This program is a grants scheme for critical infrastructure owners and operators which helps them check the security of their computer networks, including associated physical and personnel security issues.

CIPB will also initiate a domestic cyber-exercise program. It currently coordinates international

cyber-exercises such as Cyber Storm 1. Planning is underway for Cyber Storm 2 which will be held in early 2008. This exercise will incorporate a number of private infrastructure owners for the first time.

Finally, CIPB will conduct a feasibility study into the development of a Business Centre that allows security information to be shared quickly between government and critical infrastructure organisations so as to minimize the impact of electronic attacks. This feasibility study is due for completion within the next 12 months. It will consider options such as seconding staff to the centre, the need for it to operate 24 hours a day, the benefits of operating it as a virtual centre, and funding options.

Australian Federal Police (AFP)

The AFP will expand its activities in combating online criminal activity including enhancing its ability to detect, deter and investigate criminal threats against critical infrastructure and for technology enabled crime such as online fraud.

Priority 2: Reducing the e-security risk to Australian Government information and communication systems

This priority has resulted in additional funding and initiatives for two agencies.

Defence Signals Directorate (DSD)

DSD will receive increased funding to increase its delivery of e-security services. These include providing technical advice on IT security issues for government agencies, managing e-security breaches for agencies, and analysis of malware to rapidly develop counter-measures. DSD has been unable to meet all requests for assistance and the additional funding will enable it to meet demand. The funding will also enable DSD to better undertake analysis of e-security attacks across government networks and take rapid counter-measures on a network basis.

Australian Government Information Management Office (AGIMO)

AGIMO has been commissioned to establish a single framework for the continued delivery of government services in the event of a disruption and /or failure of government-operated information, communication and technology systems. This will include business continuity measures in existing systems, such as ICON, as well as incorporating robust and reliable



The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues.

About the author

Athol Yates is the Director of the Australian Homeland Security Research Centre which is a non-partisan think-tank on domestic security.

Athol Yates
Australian Homeland Security Research Centre
Tel 02 6161 5143, Fax 02 6161 5144
PO Box 295, Curtin ACT 2605
Australian Institute of International Affairs Building
Level 2, 32 Thesiger Court, Deakin ACT 2600
info@homelandsecurity.org.au
www.homelandsecurity.org.au

Copyright 2007. All rights reserved.

measures during the design phase of new systems. As AGIMO is in the Department of Finance and Administration, which controls expenditure of government, it has powerful means to ensure that IT proposals incorporate the framework's requirements.

Priority 3: Enhancing the protection of home users and SMEs from electronic attacks and fraud

This priority has resulted in additional funding and initiatives for two agencies.

Australian Communications and Media Authority (ACMA)

ACMA will expand its work with Australian internet service providers (ISPs) to help them identify compromised computers of their clients. In particular, ACMA will be identifying home and SME owned computers which are part of botnets involved in spam distribution and DDoS activities. Where likely compromised computers are located, ACMA will inform the ISPs which will then address the issue as appropriate. This may include helping their clients remove the infection. "There is self-interest in ISPs working with their clients to remove infections as their clients will be seen as a value added service and ISPs will see it as way of reducing IT traffic on their network", said Mr Rothery.

Department of Communications, Information Technology and the Arts (DCITA)

DCITA will continue to develop and expand its information to home and SMEs users. It will continue to deliver this information via www.staysmartonline.gov.au.

DCITA is developing information resources to help schools educate students and their families about secure online practices.

Glossary

Botnet

Botnet is a term for a network of compromised computers running worms, trojan horses, or backdoors, under a central command. Botnet networks can be enormous with Dutch police closing a 1.5 million node botnet in 2005. Some analysts claim that up to one quarter of all personal computers connected to the internet are part of a botnet. Once a botnet exists, the group controlling the central command can rent the network out for spamming, denial-of-service attacks, click fraud, and the theft of financial information such as credit card numbers.

Distributed denial of service attack (DDoS)

A distributed denial of service attack (DDoS) occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers.

Estonian DDoS attack

The Estonian attack involved hundreds of thousands of botnet compromised computers sending large packets of information streams to clog government websites, banks and newspapers, causing many to collapse.

ICON

ICON (Intra Government Communications Network) is a communications system providing dedicated point-to-point links for Australian Government agencies in Canberra through use of an underground system of fibre optic cables and conduits with fibre termination panels (FOBOTs) located within user premises. ICON assists agencies with their intra- and inter-communications needs by supplying "dark fibre" connections between their buildings throughout Canberra. Agencies supply and maintain the equipment that "lights" the fibre. Similar to a transportation system, ICON supplies the roads (fibre pathways), the agencies own the vehicles (data services) that travel on it. As ICON is a passive network, it has no monitoring capability and is dependent on the Agencies informing ICON if the fibre connections are disrupted.

Malware

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent, and it includes computer viruses, worms, trojan horses, spyware, dishonest adware, and other malicious and unwanted software.

Phishing

Phishing is a form of social engineering, and is a technique used to gain personal information for the purposes of identity theft by using fraudulent e-mail messages that appear to come from legitimate businesses, commonly financial institutions. Phishers send authentic-looking messages are designed to lure recipients into divulging personal data such as account numbers, passwords and credit card numbers. These emails often copy legitimate logos and message formats and even include links to a website that is a convincing replica of the company's home page.

SME

Small and medium enterprises.

Social engineering attack

A social engineering attack is one which uses human interaction (social skills) to obtain or compromise information about an organisation, a person or a computer. It can be done by someone claiming to be a repair person, new employee or consultant and requesting information. This information can then be used to break into a network, assume an identity or access accounts.