Australian Government
Department of Defence
Intelligence & Security

CYBER SECURITY OPERATIONS CENTRE

05/2010
17 February 2010

Strategies to Mitigate Targeted Cyber Intrusions

1. Australian computer networks are being targeted by malicious entities seeking access to sensitive data. A commonly used technique is social engineering, in which malicious emails are tailored to entice the reader to open them. Some emails can appear very convincing and unaware users may be tempted to open malicious email attachments or follow embedded links to malicious websites – either action could lead to a compromise of network security.

MITIGATION STRATEGIES

2. The Defence Signals Directorate (DSD) has developed a list of 35 strategies to mitigate against these types of intrusions. At least 70% of the targeted cyber intrusions that DSD responded to in 2009 could have been prevented if organisations had implemented the first four mitigation strategies listed in this paper.

3. The strategies are ranked in order of overall effectiveness. Rankings are based on DSD's analysis of reported security incidents and vulnerabilities detected by DSD in testing the security of Australian Government networks.

4. Organisations should conduct a risk assessment and implement as many of the mitigation strategies as required to manage their level of risk. No single strategy can prevent this type of malicious activity. Organisations should also ensure that the strategies selected address all three stages of a targeted cyber intrusion.

- Stage 1 – Malicious code is executed on the user's workstation, enabling the adversary to access any data accessible to the user.
- Stage 2 – The malicious code propagates through the network, enabling the adversary to access data on other workstations and servers.
- Stage 3 – The adversary exfiltrates data from the network.

5. Information on implementation costs and user acceptance has also been provided to enable organisations to select the best set of strategies for their requirements.

6. The mitigation strategies complement the advice in the *Australian Government Information Security Manual* for the protection of information that is processed, stored and communicated by government systems. A copy of the manual is available at http://www.dsd.gov.au/library/infosec/ism.html

CONTACT DETAILS

7. Additional information on implementing the mitigation strategies is available at http://www.dsd.gov.au/library/infosec/mitigations.html

8. Please contact the DSD advice and assistance line on (02) 6265 0197, for any other queries related to the content of this document.