



Australian Government

Attorney-General's Department



AUSTRALIA'S NATIONAL  
COMPUTER EMERGENCY RESPONSE TEAM

# CERT Australia



## Strategies to Mitigate Targeted Cyber Intrusions

### Background information

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.

CERT Australia and the Cyber Security Operations Centre in the Defence Signals Directorate (DSD) have developed a matrix of 35 strategies, ranked by effectiveness, that may assist your organisation better detect and prevent targeted electronic intrusions.

## Mitigation Strategies

A matrix of 35 strategies to mitigate against targeted electronic intrusions has been developed to assist organisations to better detect and prevent 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.

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

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.

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