National Cyber Security Centre

NCSC Security Advisory – NCSC-ADV-201305-0004 **24 May 2013**

Public-Facing Systems

The purpose of this advisory is to highlight the importance of securing government sector public-facing networks and systems. Inadequate security controls, practices and procedures can put classified, sensitive and private information at risk from unauthorised access and disclosure. The implementation of stringent security controls should not be compromised unless the organisation has made a conscious decision to accept the risk. Where this is the case, any residual risk should be addressed by the application of compensatory controls.

The most common public-facing system scenarios in the government sector are as follows:

- provision of internet access to the work-force;
- public access to services and information via the internet;
- public access to services and information from kiosks located on government premises;
- public wireless access to services and information from government premises.

For each of the scenarios listed above the information assets of value and at risk should be appropriately protected. This advisory offers a number of topics for consideration for public-facing systems. The list is by no means exhaustive and the New Zealand Information Security Manual (NZISM) should be referred to for further details of mandatory and discretionary security controls for government systems.

Kiosk Access:
Kiosks providing on-site public access to services and information should be sited in an area where they can be monitored by staff from the host organisation. Staff should be watchful at all times and should promptly investigate what may be anomalous behavior. Kiosk functionality should be minimized to that which is essential for the services on offer. Kiosk sessions should be refreshed once a user logs out or after a period of session inactivity that indicates that a kiosk has been left unattended.

Wireless Access:
If wireless connectivity is made available for network access, WPA2 with EAL-TLS should be used for authentication and encryption purposes. Ensure that wireless keys or pass phrases are changed regularly. Wireless access should not be provisioned out of office hours unless required.

User Authentication:
Authentication methods should be commensurate with the service or information that is being made available for public access. A registered user account with an associated password is the minimum authentication requirement for accessing sensitive, private or classified information.

Network Separation:
ICT resources and information intended for on-site public access should be accessed via an unclassified standalone system. Where this is not feasible, the host system should be

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

connected to an unclassified network that is separated from other networks and systems by a suitable gateway. Access to public network services from corporate systems should also be separated using gateway technology. The gateway should be monitored for any unauthorized activity.

Access to Information:
Access control mechanisms should be applied to all information repositories, folders and files to restrict access in accordance with user rights and privileges.

Activity Monitoring:
Access to information, applications, operating system and workstation features should be restricted in accordance with user privilege levels. All successful and unsuccessful user activity should be logged. Persistent unsuccessful attempts to perform actions should be investigated.

Data Transfer and Media:
Where uploading or downloading of information is permitted, ensure that read and write operations and the use of media types is appropriately restricted. Device disabling, write-blocking devices and device whitelisting can control device usage and data flow in line with usability requirements. Restrict the size and types of files that may be uploaded or downloaded to or from the system and use a reputable security suite to ensure data integrity. Application whitelisting should be used to prevent unauthorised or unwanted execution of files. For sensitive or classified information, consider a 'review and release' process to control inadvertent, inappropriate or unauthorised data transfers.

Internet Access:
Use a web proxy server to control access to external websites and to limit public access to permitted internal web services. A web proxy server can also be configured as a web guard to perform content and malware checking of Internet traffic.

Mail Systems:
Deploy a reputable mail guard to check email content and attachments. Block unapproved file types and sizes and detect and block spam and malware. Enforce mandatory protective marking for all email and restrict the sending of classified or sensitive email to external locations in accordance with policy.

User Awareness:
Ensure that users are aware of the risks surrounding the use of public facing systems and how to mitigate them. Provide training and documentation on how to use systems and services safely and appropriately for each of the usage scenarios described in this advisory. Develop usage policies and ensure that all system users commit to these.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

Top 4 Mitigations:
For organizations outside of the Cyber Security Plan, consider the DSD Top 4 mitigations for all systems. Details can be found here:
http://www.dsd.gov.au/publications/csocprotect/top_4_mitigations.htm

The NZ Information Security Manual (NZISM) provides details of the mandatory and recommended controls for the protection of official information. For further advice or clarification regarding the NZISM or the considerations listed in this advisory, contact the National Cyber Security Centre (NCSC).

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.