(UPDATED) DECEMBER 2012

Know and minimise your vulnerabilities before they are used against you

1. In order to protect your network and information you must be aware of your vulnerabilities. If you don't assess, analyse and minimise your vulnerabilities they will be the target for an attacker to gain access to your sensitive, classified or valuable information. This document is intended to assist Information Technology Security Advisers in protecting their networks.

Know and minimise your vulnerabilities

2. A vulnerability is a flaw, bug or misconfiguration that a cyber actor can exploit in order to gain unauthorised access to your network and information.

3. All vulnerabilities are bad, however having vulnerabilities that are publically known, or those for which there is a patch, means that you are leaving yourself open to be easily compromised by an attacker. DSD considers patching operating systems and applications as the number 2 and number 3 strategies for mitigating targeted cyber intrusions.

4. There are many free (or relatively cheap) and easy to use tools on the internet that are constantly updated with new vulnerability signatures by the developers which allow the user to detect or exploit new (and old) vulnerabilities with a few simple clicks or commands.

5. The combination of easily exploitable vulnerabilities present within your network and readily accessible tools able to exploit those vulnerabilities can allow unsophisticated attackers to easily compromise your systems or networks.

6. The best way to protect your agency from attackers exploiting vulnerabilities in your networks or systems is to:

   a. Know what your vulnerabilities are - **Vulnerability Assessment.**

   b. Know the impact of any vulnerability - **Vulnerability Analysis.**

   c. Minimise your vulnerabilities - **Vulnerability Management.**

7. **Vulnerability Assessment** is the review of your network or systems for misconfigurations, bugs or flaws. Vulnerability Assessments should be performed:

   a. On all new systems (or a risk based selection of new systems) before they are deployed.

b. On all systems or networks (or a risk based selection of systems or networks) whenever major changes occur.

c. At regular intervals to determine if new vulnerabilities have been identified since the last assessment.

8. Vulnerability Assessment can be performed using automated assessment tools (either free or paid) or manually by skilled ICT security professionals.

9. There are various types of tools you can use. Some vendors (such as Microsoft) release their own tools to enable you to assess your systems using their software. There are also third party tools that can scan the software of many vendors. Additionally there are tools/services that you can purchase from vendors which scan your systems from the cloud. This enables you to outsource the management, update and configuration of the tool and the vendor simply provides you with the appropriate reports for your systems.

10. Vulnerability Assessment tools can allow the assessor to get broader coverage of systems or vulnerabilities than manual assessment. To get the best results a combination of automated tools and manual testing is usually required. This allows you to get the right balance between breadth and depth of coverage of the vulnerabilities in your environment.

11. **Vulnerability Analysis** is getting a thorough understanding of the impact (what happens if the vulnerability is exploited) and available mitigation techniques (what you can do to protect yourself from being exploited) for vulnerabilities identified during an assessment. Your favourite ICT security website or news group is a great source of information or analysis for known vulnerabilities or paid vulnerability analysis services are available.

12. **Vulnerability Management** is a program to ensure that vulnerabilities in agency systems are identified, analysed and appropriate mitigations are applied in a risk based and timely manner. Mitigations should be prioritised based on risk to your agency and your data. Your vulnerability management strategy is part of your wider security management and monitoring efforts and should be regularly reviewed, audited and accredited by your agency management.

13. No agency can eliminate all vulnerabilities. By performing the three critical tasks above, you can minimise your vulnerabilities and overall risk. By minimising your vulnerabilities you reduce the avenues that a cyber actor can use to intrude into your network and gain access to your sensitive, classified or valuable information.

Contact Details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.