PROTECT

TOP FOUR MITIGATION STRATEGIES TO PROTECT YOUR ICT SYSTEM

1. Targeted cyber intrusions remain the biggest threat to Government ICT systems. Since opening in early 2010, the Cyber Security Operations Centre (CSOC) has detected and responded to thousands of these intrusions.

2. You should never assume that your information is of little or no value. Adversaries are not just looking for classified information. A lot of activity observed by the CSOC has an economic focus, looking for information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions.

3. The threat is real, but there are things every organisation can do to significantly reduce the risk of a cyber intrusion. In 2009, based on our analysis of these intrusions, the Defence Signals Directorate produced 35 Strategies to Mitigate Targeted Cyber Intrusions – a document that lists a variety of ways to protect an organisation's ICT systems. The CSOC estimates that around 85% of targeted cyber intrusions could be prevented by implementing the top four mitigation strategies as a package. This is up from 70% in 2009, due to improvements in ICT security.

4. The top four mitigations are: patching third party applications; patching operating systems; minimising administrative privileges; and application whitelisting. This product is designed to help senior managers in organisations understand the effectiveness of implementing these strategies.

PATCHING SYSTEMS

5. A software patch is a small piece of software designed to fix problems or update a computer program. Patching an organisation's system encompasses both the first and second mitigation strategies. It is important to patch both your operating system and applications within a two day timeframe for serious vulnerabilities. Once a vulnerability in an operating system or application is made public you can expect malware to be developed by adversaries within 48 hours. In some cases, malware has been developed to take advantage of a publicly disclosed vulnerability within eight hours.

6. There is often a perception that by patching a system without rigorous testing, something is likely to break on the system. In the majority of cases patching will not affect the function of an organisation's ICT system. Balancing the risk between taking weeks to test patches and patching serious vulnerabilities within a two day timeframe can be the difference between a compromised and a protected system.

RESTRICTING ADMINISTRATIVE PRIVILEGES

7. When an adversary targets a system, they will primarily look for user accounts with administrative privileges. Administrators are targeted because they have a high level of access to the organisation's ICT system. If an adversary gains access to a user account

with administrative privileges they can access any data the administrator can access – which generally means everything. Minimising administrative privileges makes it more difficult for the adversary to spread or hide their existence on a system.

8. Administrative privileges should be tightly controlled. It is important that only staff and contractors that need administrative privileges have them. In these cases, separate accounts with administrative privileges should be created which do not have access to the internet. This reduces the likelihood of malware infecting the administrator as they should not be web browsing or checking emails while using their privileged account.

APPLICATION WHITELISTING

9. Whitelisting—when implemented correctly—makes it harder for an adversary to gain access to an organisation's ICT system. Application whitelisting is a technical measure which only allows specifically authorised applications to run on a system. This helps prevent malicious software and unauthorised applications running.

CREATING A DEFENCE-IN-DEPTH SYSTEM

10. As a package, the top four mitigation strategies are highly effective in helping achieve a defence-in-depth ICT system. The combination of all four strategies, correctly implemented, will protect an organisation from low to moderately sophisticated intrusion attempts. Put simply, they will make it significantly more difficult for an adversary to get malicious code to run on your ICT system, or continue to run undetected. This is because the top four strategies enable multiple lines of defence against cyber intrusion.

11. Of course, implementing the other strategies will provide additional protection for your ICT system. The top seven strategies have an overall security rating of 'excellent' which means that they are the most effective measures to protect ICT systems. However, an organisation should also conduct a risk assessment and implement other mitigation strategies as required to protect its ICT system. The 35 strategies are designed to be flexible to meet the needs of different organisations, allowing every organisation to assess the risk to its information and act accordingly.

FURTHER READING

12. The full list of strategies and accopmanying documents - *Minimising Administrative Privileges Explained* and *Application Whitelisting Explained* is available at http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm.

CONTACT

Australian government agencies seeking clarification about this document can contact DSD via assist@dsd.gov.au.

Australian businesses and other private sector organisations seeking further information should contact CERT Australia via info@cert.gov.au.