Protecting Your Organisation from Targeted Cyber Intrusion

How the 35 mitigations against targeted cyber intrusion published by Defence Signals Directorate can be implemented on the Microsoft technology platform.

Microsoft®

Your Organisation is a Target

Sensitive government information, corporate intellectual property, financial information and private personal data is being lost to cyber intrusions targeted at Australian government agencies and private enterprises.

Hacking, defacement and denial-of-service attacks can severely disrupt your organisation's online presence, damage your customers' confidence and even lead to loss of extensive customer information. More persistent threats, incorporating spear phishing and remote access technologies, selectively target individuals to gain a foothold in your network and then proceed to remove sensitive data or intellectual property. And it's not just the largest government and enterprise organisations at risk. Across Australia and globally, small and medium businesses along with state and local governments have suffered losses due to these types of attack.

But there are very effective protections that can be put in place. They need not require new investment in technology or personnel. Defence Signals Directorate and CERT Australia have published guidance on the top 35 strategies to mitigate against targeted cyber intrusion and concluded that at least 85% of the intrusions they responded to in 2010 would have been prevented if only the top 4 of these mitigations had been put in place. Furthermore, CERT Australia recommends these same strategies across critical infrastructure and the private sector. These top 4 mitigations only require you to maintain current, patched applications and operating systems, employ application whitelisting technology and effectively restrict the use of administrative accounts.

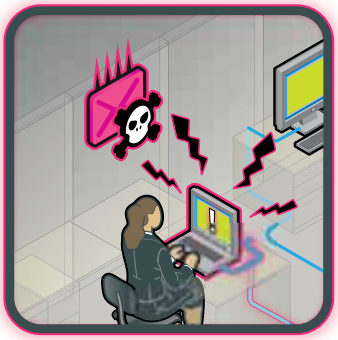
In this paper, we provide a brief overview of how these 35 mitigations can be implemented using Microsoft software. And by implementing the top 4 and then progressively choosing to implement the remaining controls, you will be in a stronger position to prevent and detect targeted cyber intrusions on your network.

Microsoft®

Stages of a Targeted Cyber Intrusion

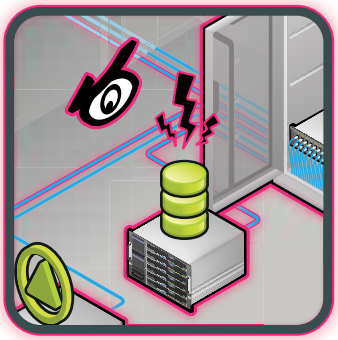
Targeted cyber intrusions can take advantage of a variety of technical and human weaknesses, such as Web servers susceptible to injection of code, unpatched browsers that inadvertently enable malware downloads or users who succumb to opening malware laden email attachments. There is no single pattern of attack, nor is there an entirely predictable sequence of events. An attack might be a single event that lasts for minutes or a sustained progression of intrusions that last for months or even years. However, it is useful to conceptualise a targeted cyber intrusion in terms of three stages: code execution, network propagation and data exfiltration:

1 Code Execution



An adversary performs reconnaissance to select a target user, and sends this user a malicious email containing a malware-laden attachment or link to a Web site. This reconnaissance is easier if the user's email address and additional information is readily available via agency Web sites, social networking Web sites, or if the user uses their email address for purposes unrelated to work. By opening the attachment or visiting the Web site, malicious code is executed on the user's workstation and is typically configured to persist by automatically executing every time the user restarts their computer and/or logs on. The malicious code is remotely controlled by the adversary, enabling them to access any information that is accessible to the user.

2 Network Propagation



The adversary moves through the network to access information on other workstations and servers. Such information typically includes Microsoft® Office files, PDF files as well as information stored in databases. Adversaries also typically access system information including computer and network configuration details, as well as details about users including organisation hierarchy and usernames and passphrases. Although passphrases might be stored as cryptographic hashes to frustrate adversaries, cracking such passphrase hashes to derive the passphrases may be fast, cheap and easy unless all users have selected very strong passphrases that are appropriately hashed. The appropriate use of multi-factor authentication may hinder adversaries.

3 Data Exfiltration

The adversary exfiltrates information from the network using network protocols and ports allowed by the organisation, such as HTTPS, HTTP, or in some cases DNS and email. The adversary typically leaves behind several compromised computers as a backdoor to facilitate further exfiltration of information in the future.

Top 4 Mitigations

1 Patch and deploy current applications

Unpatched applications have become the most common vector for exploitation primarily due to significant vulnerabilities discovered in versions of Microsoft® Office, Adobe® Acrobat® , Oracle Java and all common internet browsers. Frequently, the vulnerabilities exploited by attackers have been public for some time with protective updates already available from vendors but not yet deployed within the targeted organisation. This time delay between availability of an upgrade and its deployment within an enterprise must be minimised, especially for critical updates. Unfortunately, many applications have unique patching methods and requirements that can be challenging to integrate into a single, managed process.

Microsoft provides update tools for the enterprise called Windows Server® Update Services and guidance for the patching process in the Microsoft Security Update Guide. This guide was designed to help IT administrators develop a repeatable, effective deployment mechanism for testing and releasing security updates. Furthermore, Microsoft® System Center Configuration Manager 2012 can provide an integrated update mechanism for all software applications from any vendor.

2 Patch and deploy current operating systems

Effective system hardening begins with the deployment of current, fully updated operating systems, and it is important to recognise that modern operating systems are far more secure than legacy platforms. Against a determined attacker, a fully patched Windows® XP operating system does not provide anywhere near the equivalent security protections of a fully patched Windows® 7 operating system.

This reduction in security risk in Windows 7 is primarily due to features such as user account control, feature lockdown by default and memory protections along with support for security controls like data encryption (Microsoft® BitLocker®) and application whitelisting (Microsoft® AppLocker®). To help with assessing a migration to current operating systems, Microsoft provides a free tool called the Microsoft Assessment and Planning Toolkit. This toolkit can be used for agentless inventory of an IT environment, assessment of hardware and software readiness for migration, and custom reports detailing hardware, device and operating system readiness.

3 Restrict administrative privileges

Administrative privileges need to be tightly controlled and restricted to a small number of known users who must abide by strong authentication policies. Attackers will typically work towards obtaining the credentials of an administrator as this enables them to extend their network access, gain higher levels of access to resources and even cover their tracks. Minimising administrative privileges makes it more difficult for the adversary to extend their intrusion or hide their existence on a system.

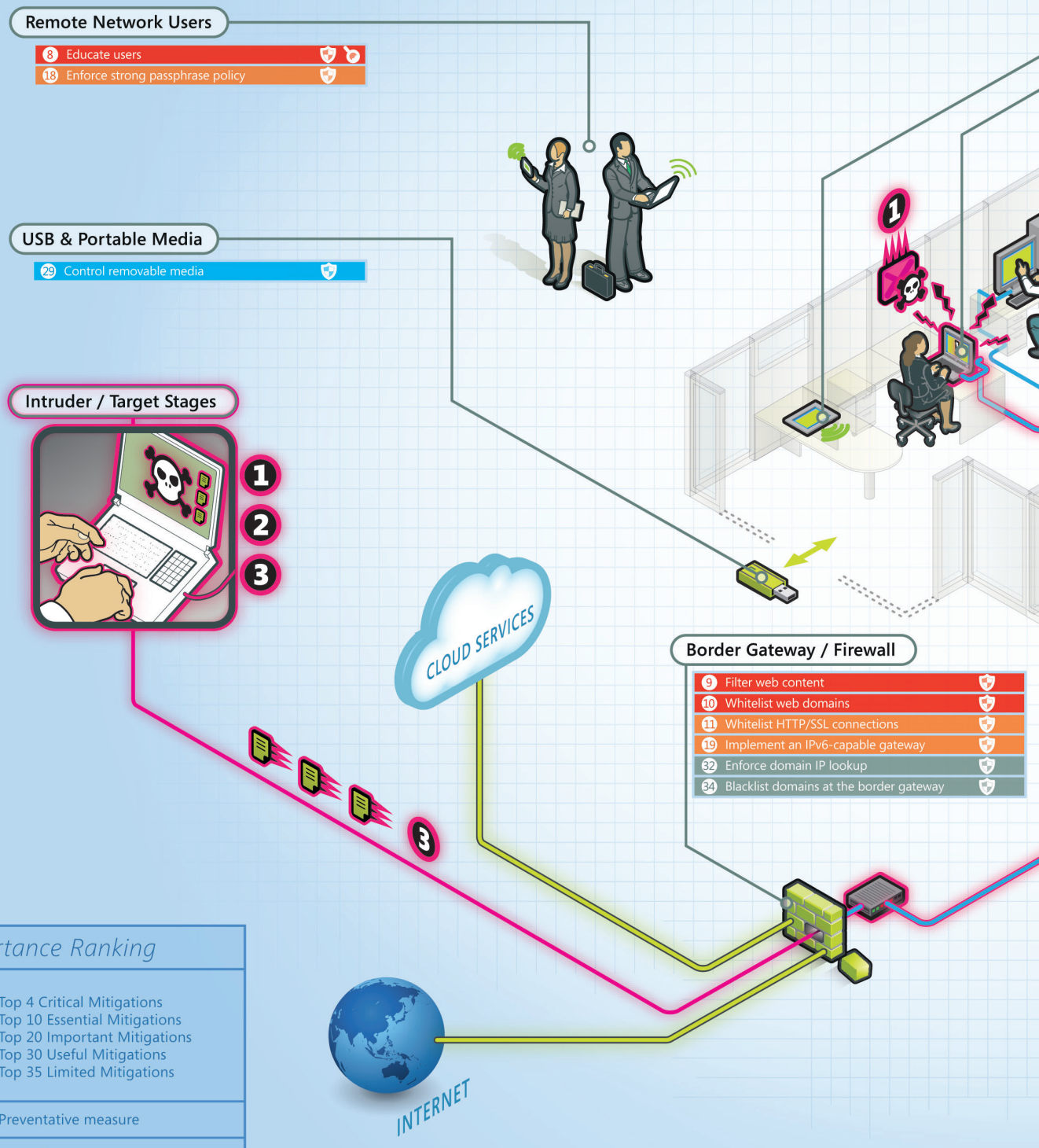
Microsoft® Forefront® Identity Manager 2010 provides a comprehensive solution for managing identities, credentials, and identity-based access policies across heterogeneous environments. It can help with restricting administrative privileges and enabling stronger authentication.

4 Whitelist applications

Application whitelisting is about identifying specific executables and software libraries that should be permitted to execute on a given system, then enforcing a policy so that only those identified components can operate. A system protected by explicit whitelisting of allowed applications will typically block malware such as a remote access tool from executing, providing an effective mitigation against the first stage of a targeted attack.

Microsoft AppLocker is a set of policy settings and software components within Windows® 7 that effectively allows multiple levels of enforcement as well as several methods of recognising whitelisted executables.

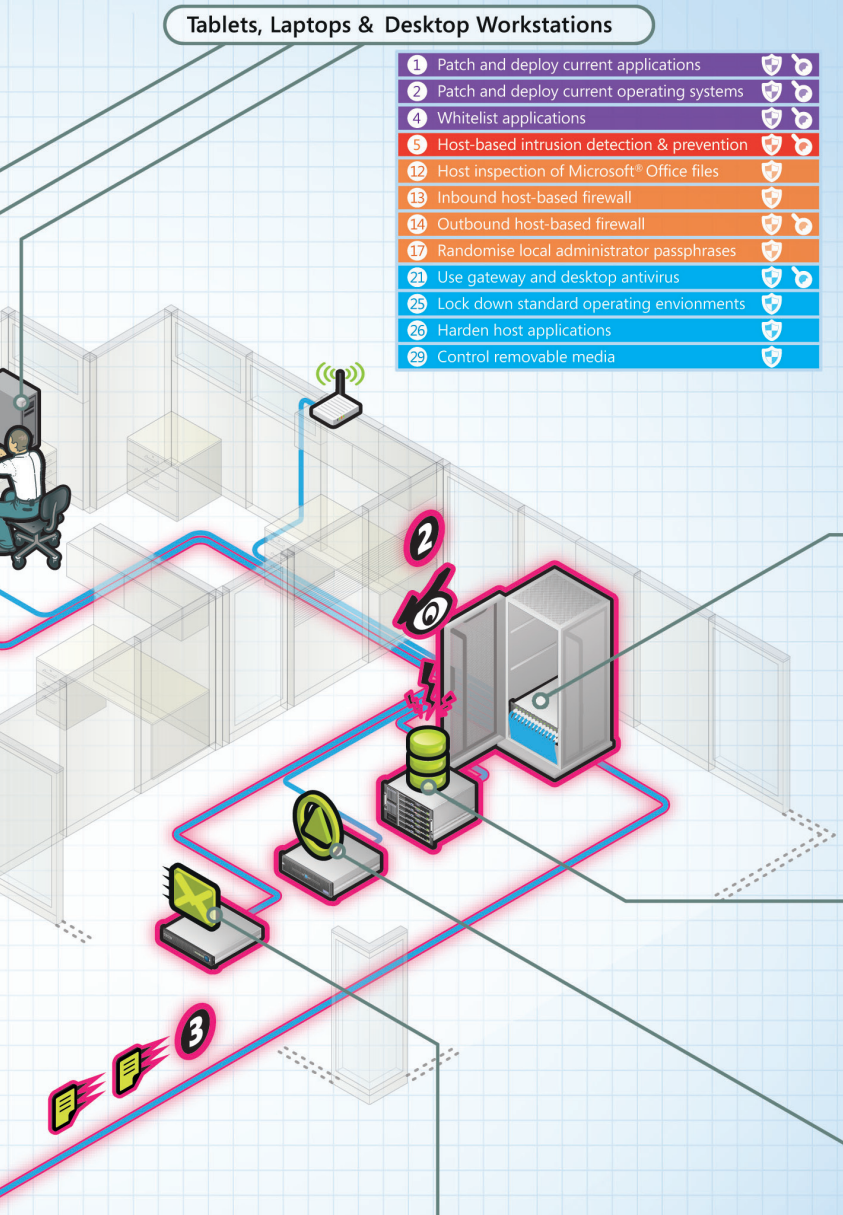
Mitigation Strategies against Targeted Cyber Intrusion



Microsoft® System Center 2012

Microsoft® Forefront® Identity Manager 2010

Windows Server® 2008 R2



Tablets, Laptops & Desktop Workstations

- 1 Patch and deploy current applications
- 2 Patch and deploy current operating systems
- 4 Whitelist applications
- 5 Host-based intrusion detection & prevention
- 12 Host inspection of Microsoft® Office files
- 13 Inbound host-based firewall
- 14 Outbound host-based firewall
- 17 Randomise local administrator passphrases
- 21 Use gateway and desktop antivirus
- 25 Lock down standard operating envionments
- 26 Harden host applications
- 29 Control removable media

Network & Infrastructure Management

- 15 Network segmentation and segregation
- 22 Non-persistent Virtualised Operating System
- 23 Centralise network logging
- 24 Centralise host logging
- 27 Restrict NetBIOS
- 33 Identify anomolous traffic with network IDPS
- 35 Capture all network traffic

Applications & Data Servers

- 20 Implement data execution prevention
- 28 Harden server applications
- 31 Data execution prevention

Directory Servers

- 3 Restrict administrative privileges
- 16 Multi-factor authentication

Email Servers

- 6 Filter email content by whitelist
- 7 Block spoofed emails
- 30 Implement TLS between email servers

Windows 7 | Windows Internet Explorer 9 | Microsoft Office

Defence in Depth

Strengthen workstation defences beyond the top 4 mitigations by deploying antivirus software, firewall restrictions, device encryption, and controls on removable media within a managed operating environment. Microsoft® System Center 2012 along with Windows® 7 provides a complete platform for end-to-end host protection along with guidance in the Microsoft Deployment Toolkit and Microsoft Security Compliance Management solution accelerators.

1 2 4 5 12 13 14 17 21 25 26 29

Harden web and server applications by addressing the most common and easily mitigated web application vulnerabilities such as SQL injection, cross-site scripting and broken session and authentication management. Mitigating these vulnerabilities is best done at design time by leveraging guidance like the OWASP Top 10 along with the extensive tools and guidance available within the Microsoft Security Development Lifecycle Methodology.

20 28 31

Enforce strong user authentication by progressing towards enforcement of strong passphrases and the use of multi-factor authentication such as smart cards. Technologies like Microsoft® Forefront® Identity Manager 2010 provide a broad platform for identity management and strong authentication.

3 16

Protect your email service from spoofed emails, spam, targeted phishing and email interception by whitelisting allowable attachment types so that vulnerable content types or executable files are prohibited, implementing Sender Policy Framework controls and enabling additional authentication between email servers (TLS). These protections can be enabled in Microsoft® Exchange Server 2010 and complemented with online filtering from Microsoft Forefront Online Protection for Exchange server.

6 7 30

Defend the web gateway by filtering the allowable content types and whitelisting allowable domain names for both normal and encrypted traffic. Firewall technology at the gateway should implement application layer protections, stateful inspection and content filtering.

9 10 11 19 32 34

Monitor your system infrastructure by maintaining central configuration and asset management database, automated management processes along with centralised monitoring of server, device and network equipment. Microsoft® System Center Configuration Manager 2012 along with Microsoft System Center Operations Manager 2012 provide these capabilities in an integrated platform.

22 24 27

Monitor your network by centralising logging and using network based intrusion detection to identify and respond to anomalies. Network segmentation is also crucial along with network protections enforced by technologies like Network Access Protection in Windows Server® 2008 R2.

15 23 33 35

Educate users about social engineering including how they can be targeted and how they should respond to suspicious requests, be careful of the information they release and report any incident. In turn, it's important to have a social engineering response process to identify if the threat is real and alert users to prevent an eventual successful breach from a sustained attack.

8 18

Guidance & Tools

Microsoft Technical Security Guidance: **technet.microsoft.com/security**

Microsoft Safety & Security Centre: **microsoft.com/security**

Microsoft Security Update Guide Second Edition: **microsoft.com/security/msrc/whatwedo/securityguide.aspx**

Open Web Application Security Project (OWASP): **owasp.org**

Microsoft Security Development Lifecycle (SDL): **microsoft.com/security/sdl**

Microsoft Solution Accelerators (including Microsoft Deployment Toolkit, Microsoft Assessment & Planning Toolkit and Security Compliance Manager): **technet.microsoft.com/en-us/solutionaccelerators**

Additional information about implementing the 35 mitigation strategies is available from Defence Signals Directorate at **http://www.dsd.gov.au/infosec/top35mitigations.htm**

May we help?

If you need assistance with improving the security of your organisation, talk to your Microsoft account representative or a Microsoft partner. With proven technologies, global experience and local expertise, we can help you select and deploy the most cost-effective solutions to meet your needs.

To speak with your Microsoft account representative or a Microsoft Partner, call 13 20 58.

To locate your nearest Microsoft partner, visit **www.microsoft.com.au/findapartner/solutionfinder**

Microsoft®