



Strategies to Mitigate Targeted Cyber Intrusions

Last updated 18 February 2010



CYBER SECURITY OPERATIONS CENTRE

Mitigation Effectiveness Ranking	Mitigation Strategy	Overall Security Effectiveness	User Resistance	Upfront Cost (Staff, Equipment, Technical Complexity)	Maintenance Cost (Mainly Staff)	Designed to Prevent or Detect an Intrusion	Helps Mitigate Intrusion Stage 1: Code Execution	Helps Mitigate Intrusion Stage 2: Network Propagation	Helps Mitigate Intrusion Stage 3: Data Exfiltration
1	Patch the operating system and applications that have a corporately manageable autoupdate feature. Patch or mitigate serious vulnerabilities within two days.	Excellent	Low	Medium	Medium	Prevent	Yes	Conditional	Conditional
2	Patch third party applications e.g. PDF viewer, ActiveX objects and other web browser plugins. Patch or mitigate serious vulnerabilities within two days.	Excellent	Low	High	Medium	Prevent	Yes	No	No
3	Minimise administrative privileges to only users who need them. Such users should use a separate unprivileged account for email and web browsing.	Excellent	Medium	Medium	Low	Prevent	Conditional	Yes	Conditional
4	Application whitelisting to help prevent unapproved programs from running e.g. solutions such as Microsoft Software Restriction Policies or AppLocker.	Excellent	Medium	High	Medium	Both	Yes	Yes	Yes
5	Host-based Intrusion Detection/Prevention System to identify anomalous behaviour such as process injection, keystroke logging, driver loading and call hooking.	Excellent	Low	Medium	Medium	Both	Yes	No	Conditional
6	Workstation conversion/sanitisation of Microsoft Office files e.g. Microsoft Office Isolated Conversion Environment (MOICE).	Excellent	Medium	Medium	Low	Prevent	Yes	No	No
7	Whitelisted email content filtering preferably converting/sanitising PDF and Microsoft Office files.	Excellent	High	High	Medium	Prevent	Yes	No	Conditional
8	Gateway with a split DNS server, an email server, a password authenticated web proxy server and a firewall preventing workstations directly accessing the Internet.	Good	Low	Low	Low	Both	Conditional	No	Yes
9	Data Execution Prevention using hardware and software mechanisms for all compatible software applications.	Good	Low	Low	Low	Prevent	Yes	No	No
10	Antivirus software with up to date signatures and heuristic detection capabilities. Use gateway and desktop antivirus software from different vendors.	Good	Low	Low	Low	Both	Yes	No	No
11	Sender Policy Framework to help block incoming spoofed emails, and to help prevent spoofing of your domain.	Good	Low	Low	Low	Prevent	Yes	No	No
12	Audit reconnaissance tool usage e.g. the system executables ipconfig, net, net1, reg, gpreult and systeminfo.	Good	Low	Medium	Low	Detect	No	Yes	No
13	Restrict access to NetBIOS services running on workstations and on servers where possible.	Good	Low	Medium	Low	Prevent	Yes	Yes	No
14	Application based workstation firewall to protect against malicious or otherwise unauthorised incoming network traffic.	Good	Low	Medium	Medium	Prevent	Yes	Yes	No
15	Network segmentation and segregation into security zones to protect high value assets using routers, switches and firewalls.	Good	Low	High	Medium	Prevent	Conditional	Yes	Conditional
16	Centralised logging using a synchronised time source, combined with regular log analysis .	Good	Low	High	High	Detect	Conditional	Conditional	Conditional
17	Disable unrequired operating system functionality e.g. disable or restrict services such as Remote Desktop, harden configuration of file and registry permissions.	Good	Medium	Medium	Low	Prevent	Yes	Yes	Conditional
18	Application security configuration hardening especially for Microsoft Office applications, PDF viewers and web browsers.	Good	Medium	Medium	Medium	Prevent	Yes	No	No
19	Application based workstation firewall that whitelists applications allowed to generate outgoing network traffic.	Good	Medium	Medium	Medium	Both	No	Yes	Yes
20	Web domain whitelisting (more proactive and thorough than blacklisting) for domains that use HTTPS/SSL encryption.	Good	Medium	Medium	Medium	Prevent	Yes	No	Yes
21	Web content filtering using a combination of signatures, heuristics, and whitelisting allowed content types.	Good	Medium	Medium	Medium	Prevent	Yes	No	Conditional
22	Two factor authentication for access to sensitive information repositories.	Good	Medium	High	Medium	Prevent	No	Conditional	No
23	Removable media control including storage, handling, whitelisting allowed USB devices, encryption and destruction.	Good	High	Medium	Medium	Prevent	Yes	Conditional	Yes
24	Web domain whitelisting (more proactive and thorough than blacklisting) for all domains .	Good	High	High	Medium	Prevent	Yes	No	Yes
25	Disable LanMan password support on workstations and servers.	Average	Low	Low	Low	Prevent	No	Yes	No
26	Block attempts to access web sites by their IP address instead of by their domain name.	Average	Low	Low	Low	Both	Yes	No	Yes
27	TLS encryption between email servers to help prevent legitimate emails being captured over the wire and used for social engineering.	Average	Low	Low	Low	Prevent	Conditional	No	No
28	Randomised local administrator passwords that are unique and complex for all computers.	Average	Low	Medium	Low	Prevent	No	Yes	No
29	Gateway blacklisting to block access to known malicious domains and IP addresses.	Average	Low	Low	High	Both	Yes	No	Yes
30	Network-based Intrusion Detection System using signatures and heuristics to identify internal network traffic such as enumeration of shares and users.	Average	Low	Medium	High	Detect	Conditional	Conditional	Conditional
31	User education about web threats, focusing on identifying spear phishing socially engineered emails.	Average	Medium	High	Medium	Both	Conditional	No	No
32	Network-based Intrusion Prevention System using signatures and heuristics to identify internal network traffic such as enumeration of shares and users.	Average	Medium	High	High	Detect	Conditional	Conditional	Conditional
33	Rolling network capture to perform post-incident analysis of inevitable successful intrusions, to determine the adversary's techniques and assess the extent of damage.	Minimal	Low	High	Low	Detect	No	No	No
34	Network-based Intrusion Detection System using signatures and heuristics to monitor external network traffic (focusing on outgoing traffic).	Minimal	Low	Medium	High	Detect	Conditional	No	Conditional
35	Network-based Intrusion Prevention System using signatures and heuristics to monitor external network traffic (focusing on outgoing traffic).	Minimal	High	High	High	Detect	Conditional	No	Conditional

Further information and contact details to obtain updated copies of this list of mitigations can be found at <http://www.dsd.gov.au/library/infosec/mitigations.html>