Managing technical vulnerabilities

From report 27: 2019/20 – Information Systems Audit Report 2020 – Local Government Entities

Office of the Auditor General
Serving the Public Interest

Vulnerabilities are flaws in operating systems, devices and applications that attackers could exploit to gain unauthorised access to systems and information. Local government entities should have continuous monitoring processes to understand security weaknesses and gaps in their systems, devices and applications. Vendors generally provide patches to address flaws in applications and systems. Entities should implement appropriate processes and assign responsibilities to identify and treat these flaws.

The following table outlines some guiding principles entities should consider to address vulnerabilities. This is not intended to be an exhaustive list. Further guidance can be obtained from the Australian Cyber Security Centre.[1]

Principle	Our expectation
Stocktake of assets	Entities should have visibility of all their ICT assets on the network including servers, workstations, printers, software applications, IoT and other network devices (switches, routers, firewalls).
Identify vulnerabilities	Regular vulnerability scans must be performed to identify security weaknesses. Where it is not possible to scan all assets at once, entities should prioritise and group assets to scan them in stages. Scans should be regular (e.g. continuous or monthly) as extended time gaps between scans leave the systems exposed for longer periods.
Understand the exposure	Each vulnerability poses a threat but some are more severe than others. Vulnerabilities generally have a severity rating based on impact and how easily they can be exploited. Entities should perform risk assessments to understand the exposure and take appropriate action.
Test and patch vulnerabilities	Entities should test patches before deploying them to live production systems. Ideally vulnerabilities should be patched as soon as possible, in line with their severity and impact levels. Entities should define appropriate timeframes to patch vulnerabilities based on their severity.
Apply mitigating controls if patching is not possible	In some instances, vulnerabilities cannot be addressed as they could affect the operations of a system (usually legacy systems), or a patch may not yet be available. Based on a risk assessment, mitigating controls should be applied with considerations to: • virtual patches • segregating or isolating unpatched systems • upgrading systems that no longer receive security updates.
Don't forget the network devices – and printers	Network devices such as firewalls, routers and switches - and printers - are equally important. Vulnerability management processes must include them as well. Entities should regularly update the firmware and software for these devices.

[1] https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches

Principle	Our expectation
Verify the patches	Entities should establish a process to verify that patches have successfully fixed the vulnerabilities. Some patches may fail to install or could require further configuration to fully address the weakness. Running another scan after applying patches can identify and report such instances.

Source: OAG

Figure 1: Better practice guidance to manage technical vulnerabilities