MOZTECH

SECURITY

PATCH MANAGEMENT STRATEGIES

www.moztechsecurity.com

MOZTECH
SECURITY

How to develop a strong Patch Management strategy.

Patches are implemented to fix any bugs or security issues within the code of software or programs; therefore, it is imperative that companies have a strong patch management strategy to keep their customers and sensitive data safe from potential cyber-attacks.

Maintain an up-to-date inventory of devices, software and hardware

By maintaining an accurate inventory, it makes the software and hardware much easier to manage in terms of ensuring they have an up-to-date patch. Regularly scanning the networks asset inventory is important for keeping an accurate overview of all devices and applications and what needs to be patched.

Be aware of vendor patch announcements

When it comes to implementing patches, time is always of the essence. It is important to monitor vendor patch announcements to ensure the software and hardware elements are updated and secured in a timely manner, which is crucial as the announcements often include the vulnerability which needs patching, giving cybercriminals time to exploit said vulnerabilities.

Use automation when you can

Typically, with patching, you can use automation to streamline the management process, ensuring that no patches are overlooked or missed leaving your network vulnerable to potential exploitations. Automating the patching process also cuts out the need to manually update each device, which can be time-consuming.

Testing patches before you deploy

As with anything, it is important to test before rolling out live. When it comes to patches, these should be rigorously tested in restricted sandbox settings, ensuring the patch update does not interfere with assets. Once a patch has cleared the restricted environment, it is likely you can then push the patch update live across the rest of the network.

www.moztechsecurity.com