fit's Patching Best Practice

OPERATING SYSTEMS

When planning deployment, research the nodes you're deploying to. Later operating systems have cumulative updates available. Pushing these can be cumbersome on some, Windows Server 2016. However, standalone security updates are available monthly – they're much smaller & straight forward than monthly cumulative updates.

DON'T PATCH ON RELEASE DAY

Do not push patches on Patch Tuesday unless they combat a specific vulnerability which is a priority to resolve. Some patches which are made available are often pulled back and revised due to issues that others face. We recommend planning your test/UAT environment patching at least 1-week post patch Tuesday.

A WATCHED POT NEVER BOILS

There is often no value in sitting & watching the updates download & install. There must be a level of trust with the systems as they are performing this work on your behalf. Start any deployment then do frequent rechecking to ensure things are moving in the right direction.

MAINTENANCE WINDOWS

Agree and maintain maintenance windows, to allow a time to apply patches & perform any maintenance that requires an outage, such as a server reboot. Decide a monthly/weekly time that servers can be briefly unavailable it allows for future planning of maintenance timings.

SAVE YOUR BANDWIDTH

Use a central delivery tool (WSUS/SCCM) to deploy updates. It saves bandwidth letting other bandwidth hefty tasks to perform well (offsite backup copies). SCCM: you download updates once, push them to distribution points then distribute content as required. WSUS: downloads the updates centrally and acts as a distribution source for clients.

COMMUNICATION

Ensure that you regularly warn your end users of patching activities or planned maintenance. Arrange a schedule so that it can be forecasted into the year. However, a lot of activities must be done ad-hoc and therefore keeping your users up to date is key to no disruptions.

KNOW YOUR ESTATE

Identify your estate so that you are aware of your environment and the updates required. A high-risk CVE can affect multiple platforms, also spanning across multiple devices. It's prudent to keep all devices which are supported, as up to date as possible – this goes in conjunction with Windows patching. This also helps with keeping your CMDB up to date.

REPORTING

Reporting can be hard to achieve without a central tool, WSUS/SCCM/RMM tools. Windows nodes shows updates in the WMI database which outputs the installed updates with date & timings. This can be key when reporting on a per node level. A PowerShell script would get this information for a vast number of nodes & output this to a CSV.

AUDITING

SCCM reports compliance based on what's installed, but not say what vulnerabilities exist in your environment. This is identified in a yearly / bi-yearly penetration test. However, tools exist that can do this more regularly and will give you a wider estate view of vulnerabilities that exist.