baramundi

BARAMUNDI CHECKLISTS provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: www.baramundi.com/checklists

6 best practices to recover quickly from faulty software updates

The unprecedented July 2024 crash of Windows PCs worldwide caused by a faulty CrowdStrike update showed how a seemingly harmless routine update can cause global-scale disruptions. Despite that, it's up to IT teams to identify potential risks and develop plans to limit the scope of damage. This checklist describes 6 best practices for endpoint management that can enable a faster recovery and resumption of normal operations when disruptions occur.

Update Rings

The ring concept calls for staggered distribution of updates. This ensures that problems only affect a limited number of endpoints. Updates are distributed successively to each ring after a specified delay if no problems occurred in the previous ring. Solutions in the baramundi Management Suite (bMS) including baramundi Update Management provide intuitive support for setting up and managing update rings.

Uninstall Option for Microsoft Updates

Successful update management enables IT admins to undo problematic Microsoft and other updates without delay. IT teams can easily create ready-to-deploy jobs with baramundi to remove faulty updates from all affected systems and quickly return them to the previous functional state.

Third-Party Software Updates

Updates for commonly used and specialized third-party software also can lead to widespread system failures. The Managed Software and Deploy modules in the bMS provide straightforward solutions both for automated distribution of tested updates and removing faulty software.

Load Restore Point

A more aggressive solution involves resetting affected Windows systems to a restore point. However, there may be some data loss depending on frequency of the restore points and the consistency of cloud backups. Configuration and triggering can be easily implemented with baramundi Deploy scripts.

Restart in Windows PE

If Windows PCs crash during or immediately after startup and show the blue screen of death or BSOD - as they did during the CrowdStrike incident - the only option is to use the Preboot eXecution Environment (PXE). This requires enabling PXE on client systems, operating DHCP PXE servers, and hardware with network interface cards (NICs). When combined with the baramundi OS Install Module, IT admins can start the Windows PE environment on clients from the network remotely so that faulty updates can be deleted and systems restarted normally. The bMS also enables IT admins to automate much of the process for a rapid recovery. The only other option is a time-intensive manual process in which IT admins must insert a pre-configured USB stick to boot and correct the error on each affected system.

BitLocker Recovery Key Management

IT admins at companies using Microsoft BitLocker disk encryption on client systems must have ready access to the recovery keys for each computer to decrypt drives prior to implementing a fix. The baramundi Defense Control module enables centralized and secure BitLocker management so that needed decryption be done remotely from the bMS admin console. Encryption can be resumed once the fix is implemented on each system. This significantly reduces the time and effort needed for recovery.

In short: experience shows that faulty or problematic updates can affect any system at any time. This checklist and the baramundi Management Suite provide the tools, automation and support that IT teams need to recover from crashes quickly and minimize downtime.