White Paper

Patch Management: Security vs Performance – the essential MSP task, by Lindsay Burden, Marketing Manager

What Do We Want? When Do We Want It – Now!

Keeping customer's on track with high availability and minimum downtime whilst remaining secure 24x365 is the ultimate goal of all IT Managed Service Providers.

Notable Flaws

There will always be challenges to achieving this. January 2018's Meltdown flaw spotted by security researchers at Google's Project Zero let hackers bypass hardware barriers between applications and computer memory on Intel chips to steal data. Spectre meanwhile gave wider rogue access to data held on chips from Intel, AMD and ARM due to design flaws in their manufacture. The impact of all this put billions of users at home and at work at risk of having data hacked across numerous devices (including PCs, smart TVs, mobile phones, smart speakers, baby monitors and car systems etc.). The remedy of patch management for Meltdown through updated software for the Operating Systems to address vulnerabilities, may have been effective, but for Spectre the impact goes deeper as it relies ultimately on the very redesign of computer hardware. Added to this, 2017's WannaCry and Petya ransomware, exploited software that hadn't been updated with available patches. But even these came with their own potential for complications.

The Process of Processing Data

The chips that break down data processing, whizz the information around the Operating System trying to use every part of the processor to maximise performance. To free up space however, modern chips try to guess what information will be required. In doing so, some of the data is dumped into the memory (CPU). This can include sensitive information. If not needed, the processor should technically remove all traces of the data, but it doesn't always happen this way and data lodged in the memory can be just what the hungry hacker is after.

Patching Methodology and Risk Evaluation

Patching (updating software with new bits of code), is by its nature, not a straightforward process for organisations. The tradeoff for available patches is often chip performance. So what business wants the prospect of suffering the potential of up to 50% slowdown in performance - and how do MSPs work around this?

Patch management is a blend of understanding the customer's business closely and understanding the security risks, in order to weigh them against business interruption and IT infrastructure malfunction that can arise when patches are applied. Patches can close ports, disable critical pieces of infrastructure, crash systems or cut availability. All scenarios that could leave organisations without the systems they need to operate, or handle transactions – and prove highly frustrating for users if there is lag in the recovery schedule. The system has to be taken down and rebooted to fully implement patches, with potential loss of productivity It is therefore critical to build in time into the activity to test, deploy and document patches. However, patching by its nature can also add new functions, so can bring benefits other than just recovery to steady state.

White Paper

Patch Management – A Very Necessary Fix

Gartner's 2017 white paper* reports that 99% of exploits are based on known vulnerabilities, many of which have patches that fix them. So, for MSPs the key is in defining and executing best practice to manage the process well and deploy patches more quickly to servers, endpoints, databases and applications.

Commenting on this generally unglamorous task, Gartner IT Analyst Terrence Cosgrove shone the light on its true value, "We think that the single most important thing you can do is improve your patching," he says. "It's about doing the basic things well, that's where you can really move the needle on reducing your risk."

At Amicus ITS, our focus is on security and recommended patches. We do not have a test lab inhouse and rely on our gold partner Microsoft to do the testing before release. Applications are much more complicated and can have many different versions, so the manufacturer needs to do any bug fixes in their test environment (and pass on).

Every organisation is different and so we cannot replicate a customer's environment within our own centres as their infrastructure is different. We work around this through best practice, whereby we deploy the patch on a small set of low priority servers selected by the customer. Once these have been observed for a couple of days and seen to be fine, we then roll out the patch to the rest of the customer's estate (and measure/report on this).

Your Patch Management Guideline

1. **Prioritisation** It's important to make patch management a priority. We try to do this with our customers by establishing a strong patch management culture. This creates discipline through a patching schedule and we can then allocate the necessary resources for the task.
2. **Asset Inventory** It's vital to have an accurate inventory of our customer's IT assets to be able to identify which patches are needed when vendors make them available. For large enterprises this may be an impossible objective, but should be the goal. To do this, organisations should seek to standardise on as few platforms as possible. Network mapping and automation can also help create the most accurate inventory possible.
3. **Testing** To manage patching successfully there needs to be a solid testing procedure to test the patch properly to ensure nothing will be broken if you implement the procedure.
4. **Stay committed to the task** So many IT estates are complex and spread over different locations. These can include mobile end points, numerous points of integration, customisation, add-ons, etc. making patching more complicated. It is a necessary evil and arising problems just have to be dealt with head-on and resolved in close collaboration with the customer.
5. **Ownership of the task** Ideally patch management is undertaken by specialists who know and understand the customer's environment and own the task and responsibility. At Amicus ITS we have a team of experts in our NOC on hand to manage this for our customers.
6. **Patch documentation** Record keeping is key for strong patch management. This ensures that in addition to maintaining an updated inventory of a customer's assets, there is a log identifying and documenting patches as they're released and when the work is completed. This is key for Amicus ITS, so we know which vulnerabilities have been addressed, how long systems may go without patching, and where vulnerabilities remain.
7. **Patch management software** There are a range of technologies to help with this, but no single tool to manage every single patch. Amicus ITS uses Desktop Central for patch reporting and our technical talent ensures that the physical installations of patches across varied platforms goes smoothly - and track and manage the process back to the customer through our Service Delivery Management team.
8. **Patch management policy** Having a policy to define this activity and programme methodology will provide you with a solid framework. This needs to be put into context of business risks and each organisation's overall security posture to determine the frequency and programme of patching that needs to occur. You can then use this policy as a review point against other security measures as part of your overall cyber security strategy.

White Paper

Contributing Authors

Amicus ITS **NOC Director, Sudipto Basu** comments, *"Patching is an essential part of a regular IT network defence maintenance programme. It needs to be systematic in approach and planned in execution, with departments working together and keeping the customer informed.*

Amicus ITS **Service Delivery Manager, Simon Coish** notes, *"Risk mitigation is best managed from having a good knowledge of the customer's IT estate. Patch management activities are discussed from a risk viewpoint and this shapes the priorities, actions and timetable for any software updates required. Problems do arise inevitably, but having a cohesive programme, with experts on hand and a positive working relationship with your customer will put you in the best position to face any issues that crop up, or urgent decisions that need to be made to minimise impact.*

Amicus ITS **Director of Technology, Security & Governance, JP Norman** adds, *"If an organisation is forced to become reactive, this is when you are going to become vulnerable to attack from hackers and subject to system failure, with potentially damaging consequences. Being a highly trusted pair of hands and having especially strong relationships with key partners like Microsoft enable us to leverage the best systems, testing and security to keep the lights on for our customers. It's worth noting as a measure or assurance that during the ransomware Wannacry and Petya attacks last year and the Meltdown and Spectre attacks in January, that none of our customers were affected.*

Source: *Technology Insight for Patch Management Tools, Gartner 2017

April 2018