

Drotos Engineering: Disaster Recovery and Business Continuity Summary and Plan



Shane Ẽire Byrne

NTC300

**Abstract**

The following material explores the concepts of patch management and the exploration of establishing a patch management system. It will also cover the concept of backing up an organizations data and various methods one can employ to do so. It will also cover disasters that can be addressed and the il-effects as such can be mitigated through proper preparations.

**Patch Management**

The importance of patches in an organization’s computer system is paramount. A patch is a “software update comprised code inserted (or patched) into the code of executable programs” (Techopedia, 2020). Patching allows for errors within software to be corrected after they are discovered. As it is software that controls a computer system (operating systems as well as any other software’s utilized within an organizations systems) it is vital to patch any discovered flaws within a systems software.

The first step in patch management is developing a written patching policy (Cohen, 2008). This should cover all aspects of an organization policies that pertain to the systems affected from a patch as well as all relevant employees needed to implement said patch. This policy should reflect which systems will be patched, how the patches are prioritized, the schedule according to which non-critical patches will be handled, the way critical patches will be handled, and the testing of patches prior to deployment.

Regarding critical patches, it would be beneficial for an organization to establish a hot team (Cohen, 2008). This group responds to all newly identified critical patches and devise a plan for action for the critical patches regarding how they are deployed within the organizations patching policies, and how the oversee the execution of said plan.

Overall the best approach to patch management is to know what you’ve got (Hart, 2018). Logically speaking vulnerabilities cannot be identified if one does not know what they are dealing within a computer system. The system itself should be scanned frequently and an inventory of the systems machines, software, devices (as well as their firmware) should be recorded in order to better identify vulnerabilities within a system. After a system is inventoried it should be assessed for risk.

According to the Australian Cyber Security Centre (ACSC), factors that should be considered when assessing risk management include determining if high value or high exposure aspects are impacted. If no patches are released or simply, they fail to address the security vulnerabilities the patch sought out to alleviate, this could present further vulnerabilities to a system (ACSC, 2020).

**Backup Strategy**

Regarding the recent installed redundant hard drives installed within Drotos’s system these will serve two functions: they will assist in day to day operations and the storage of supplementary data needed for the business that is not utilized on a daily basis but also be utilized as a means to store and provide a back-up in case of unforeseen circumstances pertaining to system failure both partial and total.

It would be advisable to establish a back-up plan prudent to Droto’s needs. Regarding the redundant hard drives prior mentioned, Droto’s systems should be established to preform an initial full back up onto a redundant drive as well as a removable drive. The full backup will be replaced by a bi-weekly differential backup. A differential backup purpose is to back up only the changes that were made during the last backup (Wilson, 2018). The removable back-up drive will instate a differential backup of Droto’s stored data for a daily basis. The policy for this will be the installation of the removable drive towards the end of the business day, the initiation of a backup to the removable drive, and the drive is recommended to be housed in a fire-safe designed to provide safety for storage media; this also pertains to any important organizational documentation (such as governmental forms, financial information, HR information, contracts, and leases) (Lo, 2012). It is also advisable for the removable drive to be encrypted in the event of possible theft or its removal by unauthorized personnel (Beaver, 2008).

With the inclusion of the cloud-based portions of the network, it is also a possibility to set up remote backups (Lo, 2012). The notion if this being key individuals can have backup drives included within their remote terminals that allow for the organizations data to be backed up. All 3 backup systems proposed will give priority to the most critical data. There is also the possibility of remote backup services such as Black Blaze which hosts cloud-based back-up services for both personal and business applications with 99.99% uptime (Black Blaze, 2020); uptime being the time in which a machine is in operation.

If back-up is to exclusively be handled in house there are several tools this organization can utilize in order to initialize automated back-ups. Some of which are opensource such as the Advanced Maryland Automatic Network Disk Archiver (A.M.A.N.D.A.), this in turn uses native utilities and formats which can back up many workstations running both Windows and Linux/UNIX operating systems (Vijayakumar, 2015).

**Types of Disasters**

In the event of a disaster the effect it can have on an organization can be devastating if said organization has not taken precautions to protect itself and its infrastructure. In 2015 alone, cyberattacks, weather events, and equipment failures cost north American firms approximately $700 billion (Matthews, 2018).

Cybersecurity attacks are more prevalent then ever. Instead of going after individuals, hackers can easily go after unprotected or poorly protected organizations. In order to protect an organization, it is best to automate communication with vendors, this would be subscribing to patch alert email lists for all software one’s organization employs (Gregg, 2019). it is also advisable to evaluate and document patch impacts in order to determine how the patch will affect the organizations systems (Gregg, 2019). Network security patches should also be prioritized; document reasoning for holding off on specific patches based on risk and effect to the overall network (Gregg, 2019). Also, it is advisable to have roll back patches in the event of unforeseen issues, with this have a plan in place to remove bad patches (Gregg, 2019).

As weather fronts can grow to be quite extreme it is advisable to have in place a means to protect an organizations data. This can be done through system back-ups. Back-ups can be preformed on site or off site; they can even be configured to be established in cloud-based services such as the Black Blaze. It is also advisable for an organization to invest in means to which to keep its computer system infrastructure operational during poor weather events. In the event of advert weather, it is advisable to backup ones systems and power down (Datasmith, 2018). This protects one’s data and systems from unexpected power surges, however, does hamper an organizations ability to remain operation in the event of a weather phenomenon. The advent of Uninterruptible Power Supplies (UPS) allow an organizations system to be powered by a battery for a finite amount of time (Life Is On, 2019). The integration of generators into an organizations infrastructure can also help in keeping an organizations computer system operational in the event of power failure caused by adverse weather so long as the generators are in operational order (Andress and Winterfield (2013)).

In summation, we have explored what patching is and its necessity within the context of an organizations computer system. This also incudes the establishment of a plan in which to execute or hold off on the execution of patches for critical and non-critical applications. We have explored the options and possibilities of back-up for Drotos Engineering’s computer systems with the possible application of inhouse or cloud-based back-up services. We have also explored various disaster events that could heavily affect an organization and possible means by which to alleviate and mitigate any ill-effects of said disasters.

**References**

Andress, J., & Winterfield, S. (2013). The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber

Warfare in Theory and Practice [PDF edition] . Waltham, MA: Elsevier.

Australian Cyber Security Centre (ACSC). (2020). Assessing Security Vulnerabilities and Applying Patches.

Retrieved from

<https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches>

Beaver, K. (2008). *Ten ways you can make your data backups more secure.*

Retrieved from

<https://searchdatabackup.techtarget.com/tip/Ten-ways-you-can-make-your-data-backups-more-secure>

Black Blaze. (2020). Cloud storage that's astonishingly easy and low-cost.

 Retrieved from <https://www.backblaze.com/index-dd.html>

Cohen, K. (2008). Top tactics for patch management strategy. Retrieved from https://www.computerweekly.com/tip/Top-tactics-for-patch-management-strategy

Datasmith. (2018). Protecting Your Business Data In Bad Weather.

Retrieved from <https://datasmithnetworks.com/tech-tips/protecting-business-data-bad-weather/>

Gregg, C. (2019). How Patch Management Can Prevent Cybersecurity Attacks.

 Retrieved from <http://anderscpa.com/patch-management-prevent-cyber-security-attacks/>

Hart, M. (2018). The best patch management strategy for 2019.

Retrieved from <https://techtalk.gfi.com/creating-your-patch-management-strategy/>

 Life Is On. (2019). Advances in uninterruptible power supply technology deliver cost-effective protection for edge data centers.

Retrieved from <https://www.healthcareitnews.com/news/advances-uninterruptible-power-supply-technology-deliver-cost-effective-protection-edge-data>

Lo, K. (2012). Your Organization's Backup Strategy.

Retrieved from <https://www.techsoup.org/support/articles-and-how-tos/your-organizations-backup-strategy>

Matthews, R. (2018). 4 Tips to Safeguard Your Data from Natural Disasters.

Retrieved from <https://biztechmagazine.com/article/2018/03/4-tips-safeguard-your-data-natural-disasters>

Techopedia. (2020). Patch. Retrieved from <https://www.techopedia.com/definition/24537/patch>

University of Yale . (2020). Why Software Patching is Key to Your Online Security.

Retrieved from <https://cybersecurity.yale.edu/patchyourdevices>

Vijayakumar, G. (2015). Ten Must-Have Open Source Tools for Backup and Recovery.

 Retrieved from

<https://opensourceforu.com/2015/10/ten-must-have-open-source-tools-for-backup-and-recovery/>

Wilson, S. (2018). CompTIA Cloud+ Certification Study Guide, 2nd Edition [VitalSource Bookshelf version].

Retrieved from vbk://1260143503