
WHITEPAPER · COMPLIANCE & SECURITY

Vulnerability and Patch Management

PUBLISHER

Manuel Fernandez

PUBLISHED

16 November 2022

01 Introduction

We are living in an era in which information technology is present in all kinds of business – from small businesses to the most complex organisations such as banks, manufacturers and defence departments, among others.

IT enables the processing, transfer and storage of data in a fast and efficient way (when it is properly implemented and maintained) and helps companies to stay competitive across markets worldwide (as a result of internet commercialisation). Keeping data secure is therefore a key factor for every company, because the loss of information through a cyberattack can cause damage to the company's reputation, financial damage, a weaker competitive position and legal consequences.

Companies from all sectors using IT systems are susceptible to attacks by cyber criminals, but some sectors are known to be targeted most often, because criminals can make the most profit from their activities there:

- Companies with an international presence, which require a complex IT infrastructure for business operations across borders
- Banks and financial institutions
- Governmental institutions or public service institutions
- Small businesses that hold sensitive customer and financial information
- Companies with intellectual property, e.g. the pharmaceutical industry

By implementing vulnerability and patch management processes, companies can mitigate the risk of cyberattacks and keep their data safe in cyberspace.

02 Differentiating vulnerability management and patch management

Before going further into vulnerability and patch management, it is important to understand that they are different. Some might think that vulnerability management is part of patch management, because fixing a vulnerability normally requires installing a patch – but that is not always the case. There can be situations in which no patch is available to mitigate a vulnerability, and the company needs to find another way of dealing with it. For a better understanding, here is the definition of each type of management:

PATCH MANAGEMENT

VULNERABILITY MANAGEMENT

relates to the processes and activities of acquiring, planning, testing and implementing a patch delivered by a specific software vendor. A patch does not necessarily fix a vulnerability; it is often used for bug fixes or software updates (drivers, firmware, service packs).

on the other hand, refers to the processes that identify, assess and mitigate potential vulnerabilities in the IT infrastructure.

Vulnerabilities are not only present in software but also in physical assets that could compromise the security of the software. These are not addressed within the scope of vulnerability management but in other processes – e.g. access policies for server rooms, building access, or data in the intranet, which can be addressed by identity and access management (IAM) processes. For the purpose of this paper, I will focus only on the management of vulnerabilities in software.

03 How to implement vulnerability management

To implement efficient vulnerability management, a company should start with clearly defined policies. Established IT processes, standards and guidelines provide a solid foundation for the further management of vulnerabilities.

With the policies as a baseline for the processes, the IT assets that are meant to be secured should be identified. A vulnerability is defined as a weakness of an IT asset that can be exploited by one or more threats. The IT assets are therefore the main elements of vulnerability management. They can be a server, notebook, database, system software, business application, network component and/or any other related IT component – in short, all information technology resources that IT requires to support business processes.

Then the prioritisation of assets should be defined, to know which elements of the IT infrastructure at risk should be tackled first and whether to eliminate, mitigate or tolerate those vulnerabilities.

01 Assess the criticality profile of the assets.

IT assets run applications that have different relevance for the company. Applications that run core business processes cause a bigger impact when affected by a vulnerability, while supporting applications may not have a big impact. The most important applications should be managed for vulnerabilities first, followed by the other applications in order of relevance. This categorisation also facilitates decision making in exception or risk acceptance processes.

02 Use different methods to identify vulnerabilities or possible threats.

There are different possibilities for keeping the IT infrastructure monitored and secured:

- Publicly available sources on the internet provide information about identified vulnerabilities, so that companies can react immediately if one of them can impact their IT infrastructure (e.g. US-CERT in the USA, CERT-Bund in Germany, the National Vulnerability Database [NVD]). Private companies also track announcements and rate their severity for a fee (e.g. Secunia).
- Software for scanning the IT environment (e.g. Qualys) identifies suspicious activities or possible breaches and gives an immediate alert to take action, analyse and remediate.
- Penetration tests find possible weaknesses or breaches in the IT infrastructure by simulating a cyberattack. Specialised companies run these tests; not every company uses this option because of its cost, but financial institutions are obliged to do so.

03 Prioritise vulnerabilities according to their risk.

The announced severity of a vulnerability, together with the relevance assessment of the IT infrastructure, makes it possible to identify the most vulnerable CIs and decide how to tackle the situation – starting by patching those with the highest risk. Companies with a large IT infrastructure should have a well-defined risk assessment process in place to react quickly to an identified vulnerability and efficiently minimise the possibility of a threat exploiting it.

04 Have a clear change management process.

If a vulnerability is identified, a patch has to be developed and installed on the specific asset to mitigate or eliminate the risk. This means that the asset needs to be modified to put the new patch in place. A standardised process for making changes is therefore required: involve the right stakeholders, keep control during the process, keep all documentation needed and roll back if a problem occurs (e.g. the application is unstable after the patch, or the operating system does not start again). ITIL is the best-known and most widely used practice for IT service management, and change management is one of the processes it defines. Implementing ITIL is recommended because the company will then have a configuration management database (CMDB) as the basis for all important information such as application dependencies, business roles for each application, and hardware and software attributes and components. This information is important not only for vulnerability and patch management but also for other IT operations processes that maintain the IT infrastructure.

05 Keep track of vulnerability management with reports.

Once a cycle of identifying, assessing and mitigating vulnerabilities is complete, the information about the new status of the IT infrastructure must be kept up to date after every patching cycle: which new CIs have been put into production and must be included in the vulnerability management process, which CIs are reaching the end of their support life and

need to be updated, and how many CIs could not be patched. For the latter, a follow-up is required to identify the issue and find a solution so that the CIs do not remain with an open weakness for long – a task to be managed by incident and problem management. Reports also measure particular aspects of the services against the KPIs defined in the agreed service level agreements (SLAs). The information collected gives stakeholders an overview of the actual status of all CIs in the IT infrastructure, gives management an overview of the efficiency of funding and the effectiveness of the cybersecurity protecting the company's assets for decision making, and shows the IT department where to improve processes or take action.

These five steps give a first overview of the elements required for a vulnerability and patch management process. Its implementation, however, involves many aspects that have to be analysed in more detail.

04 Vulnerability management and cloud computing

Cloud computing is a growing trend in today's IT world because of the many advantages it brings to companies: lower costs for maintaining IT infrastructure, the capacity to adapt to economies of scale or to serve small start-ups, the agility to deploy new applications quickly and the capacity to keep information secure – the latter including an efficient process for managing vulnerabilities and patching applications.

Companies such as Amazon with AWS (Amazon Web Services) and Microsoft with Azure provide cloud computing with a variety of services and benefits, so that their clients have an IT infrastructure that is always up to date, eliminating the problem of legacy assets. The infrastructure can be adapted to the best design for the company, and high expertise and best practices are assured for the maintenance and security of the infrastructure assets supporting the cloud – bringing a reduction of complexity and more visibility of managed assets.

The major cloud providers offer out-of-the-box solutions for monitoring all services and resources as well as IAM (identity and access management) that are already optimised for their servers, which are managed on a large scale. This increases the efficiency and reliability of the IT infrastructure and in many cases makes it much better than infrastructure operated by companies on premises. The dynamism of cloud computing also makes it easy to adjust firewalls and security tags on cloud assets to protect the network against newly announced vulnerabilities where patches cannot be deployed for various reasons. Automation is another key solution that is easier to implement in the cloud than on premises, useful for patching activities and for providing status indicators for all assets in the cloud.

Nevertheless, clients still need to take care of their internal assets to keep their complete IT secure. Companies using cloud computing need assets (e.g. computers and internal networks) to connect to the internet and establish a secure connection to the cloud. For these assets, too, vulnerability management must remain a priority to mitigate risks. If this is not well defined and performed internally, the company will be exposed to attacks even with the best cloud solutions.

Another great advantage of cloud solutions is that companies can get guidance on keeping their IT infrastructure secure with vulnerability management processes modelled on best practices that work proficiently with the cloud solutions – making the company's end-to-end processes secure and reliable in the cloud.

05 Conclusions

Vulnerability management is a key element in protecting a company's IT infrastructure from attacks. However, it is a broad topic: implementing it as a solid process requires several aspects to be considered and analysed in detail that are not included in this whitepaper. If a company is not clear about the priorities of its business applications and assets, it will not be able to reach the level of compliance required to manage important data and services reliably.

With the first steps described in this paper, managers can start guiding their company to define, implement and perform an efficient vulnerability management process, and prevent problems that could incur high costs and a loss of client trust.

Cloud computing is also a good option, but companies will have to entrust their most important asset – their data – to a provider. It is therefore important to choose wisely which cloud provider offers the best solutions and security for moving services and data into the cloud.

Let's talk

For further information on this and other exciting topics, we look forward to a personal conversation with you!

COMPANY

DIP Deutsche IT und
Projektberatungsgesellschaft mbH
Rahmannstraße 11 · 65760 Eschborn
info@dip-consulting.de
dip-consulting.de

YOUR CONTACT PERSON

Manuel Fernandez

Management Consultant, Managing Director
info@dip-consulting.de

Mr. Fernandez has been Managing Director of DIP Deutsche IT und Projektberatungsgesellschaft since 2013 and has worked as an IT consultant for 16 years in a wide range of roles on both strategic and implementation-focused projects.

