TAG CYBER

NEXT-GENERATION VULNERABILITY ASSESSMENT AND PATCH MANAGEMENT: AN OVERVIEW OF ACRONIS CYBER PROTECT

EDWARD AMOROSO

Vulnerability assessment and patch management are foundational cyber security tasks that have evolved toward next-generation coverage of multicloud infrastructure, data center virtualization, and zero-trust architectures. The Acronis Cyber Protect Cloud platform is shown to effectively implement these important controls.

INTRODUCTION

Despite the changes that have occurred over the years in cyber security, many traditional protection approaches have remained as important and as effective as ever. Two complementary examples are vulnerability assessment and patch management. As organizations continue to shift toward virtualization, zero trust, and multicloud infrastructure, proper attention to vulnerabilities and patches helps to ensure consistency with cyber risk objectives.

In this report, we review the best current approaches to this combined activity, which we dub VA/PM — and prepend the moniker "next generation" to highlight the evolution of these capabilities to handle multicloud infrastructure, virtualization, zero trust, and many other attributes of modern enterprise networks. The Acronis[1] Cyber Protect Cloud platform is shown to effectively implement this next-generation vulnerability assessment and patch management (NG-VA/PM) approach, especially for service providers.

IMPORTANCE OF VA/PM

Keeping track of vulnerabilities and patches is hardly the most exciting aspect of modern cybersecurity, but it could arguably be viewed as one of the most important tasks in an IT risk program. Security breaches often result from exploitation of vulnerabilities that could have been removed, or from patches that were not applied. So the combined task to address these issues has a clear implication for cyber risk.

As such, every team responsible for security, regardless of size or sector, must have some means of tracking and prioritizing vulnerabilities, and of ensuring the timely application of patches. The ability to ensure high-integrity support with fail-safe operation is also highly desirable. For example, according to one research survey, 88% of companies claim that they would apply patches more quickly if they had the option to un-patch if necessary.[2]

It is worth mentioning that VA/PM is particularly important for managed service providers, because of their scope. That is, as nearly all SMBs rely on service providers to assist in operating and protecting infrastructure, software, and services, their overall cyber risk can be significantly reduced if the service provider handles this task properly. This is one of the great benefits, in fact, of working with a capable service provider.

CHALLENGES OF VA/PM

One major challenge for VA/PM involves the existence of known and unknown vulnerabilities. It is reasonable to assume that a large VA/PM program would have good coverage of known, reported vulnerabilities — but it is not reasonable to expect that this will extend to unknown, zero-day problems. In most cases, teams become aware of zero-day exploits only after they have been used in an actual campaign.

An additional coverage challenge, which is arguably more intense, involves the existence of known and unknown assets in an organization. That is, most nontrivial organizations have an incomplete understanding of their asset inventory. As a result, for any vulnerability, it might be unclear whether it actually applies to the local environment. These two unknowns, vulnerabilities and assets, can be represented in a conceptual matrix (see Figure 1).

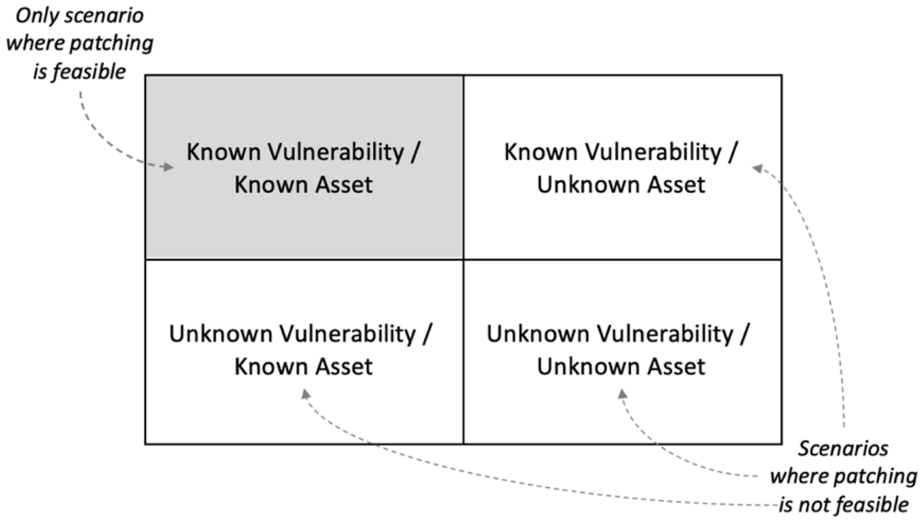

FIGURE 1. Matrix of Vulnerability/Asset Scenarios

The matrix highlights how important it is for vulnerabilities to become well-known quickly, and for assets to also become known accurately and quickly. These next-generation requirements help to explain how NG-VA/PM has come to be — namely, to ensure that organizations wanting to maintain more accurate and complete coverage of vulnerabilities and patches have sufficient means to achieve this critical security objective.

MODERN NG-VA/PM REQUIREMENTS

The cyber security community well understands the vulnerability management challenge and its adjacent tasks of prioritizing and patching (including for non-Windows products). NG-VA/PM is all about making these familiar processes more intelligent, manageable, automated, and complete. The specific types of next-generation continuous security functions that are required in this area include the following:

- *Vulnerability Assessments* – Teams responsible for security must have the ability to collect, catalog, and manage an accurate list of applicable vulnerabilities. This is best done using global threat monitoring and alerting from multiple sources.
- *Prioritized Patching* – Security teams must use analytics and threat intelligence to determine which patches to prioritize. This analysis requires accurate asset management and inventory and good external threat intelligence.
- *Forensic Analysis* – NG-VA/PM programs must support future analysis and investigations by archiving vulnerability-related data and associated patches. This allows for more accurate case analysis.
- *Fail-Safe Patching* – NG-VA/PM programs must support the ability to roll back patches if necessary and to ensure high-integrity patch application.
- *VA/PM Compliance* – As with all aspects of modern cybersecurity, NG-VA/PM includes the obligation to support compliance goals. This often involves the automatic generation of reports for external auditors and regulators.

As suggested above, the progression to next-generation capability for VA/PM includes driving intelligence, automation, and completeness. It also, however, involves extending applicable techniques, tools, and processes to handle the modern transition to new infrastructure such as public cloud, mobile networks, and perimeterless zero-trust environments. In the next section, we use the commercial Acronis platform to illustrate how this can be done in practice.

CASE STUDY: ACRONIS CYBER PROTECT CLOUD PLATFORM SUPPORT FOR NG-VA/PM

The Acronis Cyber Protect Cloud commercial platform is designed specifically to enable MSPs to provide next-generation vulnerability management and patching support for enterprise customers of all sizes around the world. As such, it serves as an excellent use case to demonstrate how NG-VA/PM requirements might be implemented in a live production environment, where a cyberthreat might have significant consequences.

Cyber Protect Cloud includes a range of capabilities that directly address anti-malware, patching, virus scanning, backup, vulnerability assessment, sensitive data protection, and application controls. MSPs can rely on these capabilities to address safety, security, authenticity, privacy, and accessibility requirements among their SMB customers in the context of processes for backup and recovery, security management, and anti-malware (see Figure 2).

FIGURE 2. Acronis Cyber Protect Cloud

The primary advantage of combining these functions into a commercial platform is that it helps to streamline the complexity of many different processes and functions. The many challenges inherent in the coordination, combination, and integration of the various processes shown in Figure 2 should be obvious. Coordinating backups with anti-malware, for example, is one of the great difficulties in dealing with advanced ransomware attacks.

The implication for managed security service provider teams is that an integrated commercial platform such as Acronis Cyber Protect will likely simplify and streamline the overall NG-VA/PM infrastructure and associated processes for enterprise customers. This is an essential task, especially in organizations with considerable size and scope. Attention to simplification will continue to grow as a requirement in emerging compliance environments.

ACTION PLAN

MSPs are advised to take immediate action toward implementing a modern NG-VA/PM program using a suitable commercial platform and associated set of processes — such as with the Acronis solution. This can be achieved by following a simple four-step management plan. Each of the four high-level steps must obviously be decomposed into more granular tasks, but the overall approach should be as follows:

Step 1: Inventory of Existing VA/PM Approaches
The head of security and his/her team should create an accurate inventory of existing approaches to identifying, documenting, assessing, prioritizing, and closing vulnerabilities. In larger firms, this is likely to include many disparate approaches, tools, and processes.

Step 2: Development of NG-VA/PM Requirements
Once the inventory has been established, the security team should create a set of NG-VA/PM requirements along the lines of the functions discussed in this report. The requirements should combine the best elements of approaches identified in the inventory.

Step 3: Commercial Platform Scan and Review
The next step involves scanning and reviewing available platforms such as Acronis Cyber Protect Cloud for suitability in the customers' environments. TAG Cyber analysts can assist with this task, which must take into account nonfunctional considerations such as license terms and cost.

Step 4: Begin Gradual Transition and Integration

The final management step involves transition and integration of the newly selected platform into the local NG-VA/PM ecosystem. The good news is that the types of tasks included in this area are highly conducive to a smooth transition.

ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

[1] Switzerland-based Acronis GmbH (https://www.acronis.com/en-us/) supported and participated in the preparation of this technical report.

[2] 0patch Survey Report, 2018. https://0patch.com/