What is VAPT?
An introduction for IT Managers

A bluedog Whitepaper

bluedog
SECURITY MONITORING

Contents

Executive Summary 2

Common Cyber Security Challenges for IT Managers 4

Cyber Security Has to Be Built Into Every Product and Solution We Use 4

Widespread Collaboration in Fighting Cyber Attacks Is Paramount 4

A Common Approach in Fighting Cyber Crime 5

When Work Moves to the Cloud, New Threats Appear 5

What Is VAPT? 7

What Is the Difference between VA and PT? 8

Why Is VAPT Required? 9

How Do You Perform a VAPT Test? 10

Gathering the Information 10

Collecting Additional Information 10

Scanning and Discovery 10

Vulnerability Assessment 11

Penetration Testing 11

Final Reporting and Analysis 11

About BlueDog Security Monitoring 12

Executive Summary

A recent survey of IT leaders[1] showed that security is at the top of their concerns. And it's no wonder. 2020 wasn't just the year of the COVID-19 pandemic. It was also the year of the cyber pandemic[2].

We all have brand-new threats to face and we also need to face the "old" attacks that got even stronger. While the vaccine may slow down the COVID-19 pandemic, the cyber pandemic is far from controlled.

This whitepaper analyzes the main cyber security threats IT leaders have to face and offers a solution that fits organizations large and small: VAPT.

The following chapters will shed some light on what VAPT is, why it is important, how VAPT testing is conducted and how it differs from other similar testing solutions.

VAPT helps with the first step of security enhancement: knowing your enemy. It is the solution that helps IT managers assess risks and prioritize them so that they can, afterwards, decide how to tackle them in the short and long run.

Just like any other automated or human-led solution, VAPT is only as good as the way you use it. Thus, this whitepaper also offers practical tips on how to leverage VAPT for your business.

[1] https://cdn2.hubspot.net/hubfs/4265482/Marketing%20Assets/Torii%20IT%20Survey%202019.pdf, retrieved February 2021

[2] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html, retrieved February 2021

Common Cyber Security Challenges for IT Managers

Oftentimes, we think about security as an add-on. It is, perhaps, similar, to the way we tackled operating system security a few years ago: install the operating system, then the anti-virus.

This worked well for a while, especially since not every program on our computer was internet-facing. Today, almost everything is. Even the Office suite demands an active internet connection to check for updates regularly (and to check the license, of course, but that's beside the point).

This is why security can no longer be treated as an add-on or as an after-thought. Which brings us to the first challenge:

Cyber Security Has to Be Built Into Every Product and Solution We Use

This is a perfect example of "easier said than done". Yes, digital solutions creators *generally* make the security of their product a priority. But can you take all of them at their word?

We know that 95% of cyber attacks[3] are the result of human errors. Sometimes, those errors belong to the users and other times to the programmers. Most often, though, it's a combination of the two: the software creators don't account for every real-life scenario and this leaves room for breaches.

Thus, IT leaders must focus on finding solutions that have a strong built-in protection. When that is not possible (or easy to assess), regular security evaluations and scanning can complement the security strategy.

Widespread Collaboration in Fighting Cyber Attacks Is Paramount

The damage caused by hackers, malware, and data breaches is forecast to reach $6 trillion this year[4]. Collaboration between attackers is already the norm.

Unfortunately, privately-held organizations, as well as governmental ones are reluctant to share their data. In a way, it is understandable: no one wants to advertise their vulnerabilities and open themselves to more attacks or worry shareholders and stakeholders.

---

[3] https://www.securitymagazine.com/articles/85601-of-successful-security-attacks-are-the-result-of-human-error, retrieved February 2021

[4] https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/, retrieved February 2021

However, without transparency and collaboration across industries and across continents, the "bad guys" will always have the upper hand. It is senior IT leaders' responsibility and challenge to find the perfect balance between protecting the organization's image and assets and helping fight cyber crime globally.

A Common Approach in Fighting Cyber Crime

The World Economic Forum[5] dubbed this a NATO of sorts for cyber security and the comparison is perfect. Cyber attacks are the second most significant concern of organizations worldwide, right after fiscal crises.

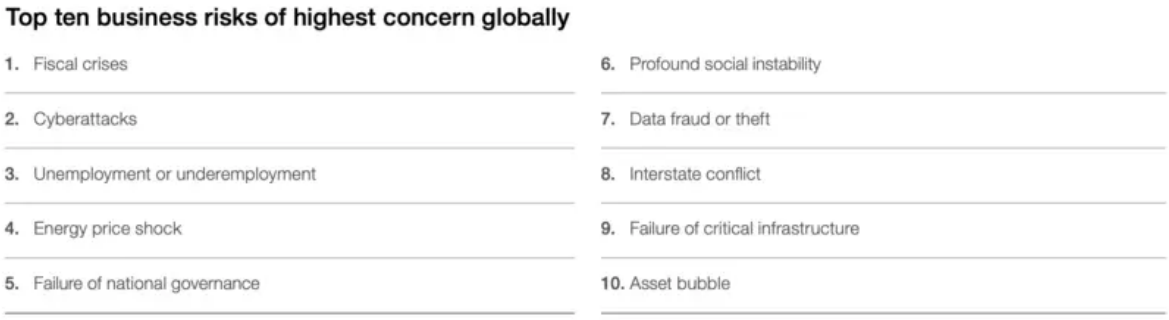

Image source[6]

IT managers are the ones that should lead the race to finding a common approach, starting from educating new generations of cyber security experts[7] and ending with finding new, more effective ways to fight cyber crime.

When Work Moves to the Cloud, New Threats Appear

With 80% of enterprises relying on cloud computing for at least a quarter of their workload[8], the emergence of new types of threats is no surprise. While the adoption of the cloud isn't set to slow down

[5] https://www.weforum.org/agenda/2020/01/four-key-challenges-for-cybersecurity-leaders/, retrieved February 2021.
[6] Ibidem
[7] The skills shortages in cyber security is a serious problem worldwide. We have tackled it comprehensively in this whitepaper that you can download for free.
[8] https://www.globenewswire.com/news-release/2019/01/17/1701128/0/en/Enterprise-IT-Focused-on-Moving-More-Workloads-to-Cloud-in-2019.html, retrieved February 2021

any time soon, it falls to IT managers to find new ways to protect their on-premise assets as well as those that hosted in the cloud.

Again, it all starts with properly assessing the vulnerabilities of both these types of assets. In the following chapters, we will explore vulnerability assessment at length.

What Is VAPT?

VAPT stands for Vulnerability Assessment and Penetration Testing and describes a wide range of tests and scans designed to identify and help address cyber security vulnerabilities.

The power of this solution stems from combining two types of vulnerability testing: vulnerability assessment and penetration testing. These two tests have different strengths, so combining them can offer more comprehensive results within the same area of focus.

As the name implies, vulnerability assessment solutions are designed to discover the vulnerabilities in your assets. Vulnerability scanning works by comparing the findings in your assets with an existent database of known vulnerabilities. The larger the database and the more recently updated, the better your chances at finding the newest vulnerabilities. Using an outdated vulnerability scanning solution can be irrelevant, since it will only identify obsolete threats and leave you blind to the newest ones.

However, irrespective of how good the solution is, the results of the scan can't tell you which of these vulnerabilities can be exploited and which cannot. Some scanning solutions will rank them based on what their database reveals as most threatening, but you still need to conduct your own testing and evaluation.

This is where the second part of VAPT, penetration testing comes into play. PT is an attempt to exploit the vulnerabilities of digital assets in order to determine if any malicious activity is possible.

Pen testing is designed to identify which of the vulnerabilities discovered is most likely to pose a threat to the organization's assets. In other words, penetration testing reveals the severity of each threat. Furthermore, by simulating the attacks, pen testing can show exactly how damaging a successful breach would be.

Together, vulnerability assessment and penetration testing offer a comprehensive picture of the flaws that exist in an application, a network, or any other digital asset and of the risks associated with these flaws.

What Is the Difference between VA and PT?

The section above touches on this topic, but let's make a clearer distinction between VA and PT and to further explain the reason for needing them both.

Briefly put, vulnerability assessment offers a horizontal map of the security status of an organization's network, applications, or software. On the other hand, penetration testing is a vertical dive into the findings of the assessment.

The easiest way to remember the difference between the two is this: VA reveals how **big** a vulnerability is and PT reveals how **bad** that vulnerability is.

Another important difference between the two stems from the way they are conducted. Vulnerability assessment is typically a fully automated process. PT is typically a manual, human-led process.

Of course, there can be human-led actions in VA, too. Ranking the vulnerabilities discovered is usually both automated and manual. Similarly, PT also includes some automated testing, but it's mostly human-led.

The combined approach has an undeniable advantage: it uses the same combination of automated/manual processes that attackers use too, down to the simulated attacks in PT. Hackers too start with automated tools to discover vulnerabilities and then move to manually writing scripts to exploit them.

In a sense, VAPT is beating cyber attackers with some of their own weapons.

Why Is VAPT Required?

As shown above, the increase in cyber threats, as well as the increase in the sophistication of the attacks require modern tools to keep an organization's assets protected. VAPT is a solution that fits the needs of organizations of all sizes, since it can be easily scaled to match various needs and budgets.

Aside from generic recommendations (most safety standards recommend regular VAPT for companies in every industry), there are certain industries where VAPT is mandatory. The regulations specify how often VAPT should be conducted for each of these industries and typically also state that it should be done by an independent company to ensure unbiased results.

Standards like GDPR, ISO 27001 and PCI DSS require regular VAPT testing for compliance. Moreover, there are several industries where regulations also require VAPT testing.

For instance, to become SOC 2 compliant[9], you need to conduct an initial pen test and then repeat it every 180 days.

HIPAA (Health Insurance Portability and Accountability Act of 1996)[10] is the US federal law that governs the privacy, safety, and electronic exchange of medical information. Strictly speaking, HIPAA compliance doesn't require VAPT. At least not explicitly. It does, however, require a risk analysis which, effectively, requires covered organizations to test their security controls.

There are countless other standards and regulations that govern cyber security and most of them require, explicitly or not, for covered entities to conduct regular VAPT. The list of regulations varies from country to country, but it's usually more prevalent in sensitive industries, like the financial and the healthcare ones, where sensitive data is used and stored.

[9] https://www.ssae-16.com/soc-2/, retrieved February 2021
[10] https://www.cdc.gov/phlp/publications/topic/hipaa.html, retrieved February 2021

How Do You Perform a VAPT Test?

There is no one-size-fits-all in VAPT. The way VAPT is run depends on a series of factors. Some of the more prevalent ones are:

- The industry your organization is in
- The type of data it handles (how sensitive and attractive to attackers this data is)
- The number and type of digital assets to be scanned and tested
- The size of the organization.

While the way VAPT differs from organization to organization, there are a few standard phases that apply to most entities:

Gathering the Information

This phase is perhaps the most important one of the entire process. It is a stage where the client works closely with the VAPT provider so that the latter can understand the scope of the entire process.

Gathering the right type of information can help throughout the entire VAPT process and can be extremely useful in the long run since VAPT should be conducted regularly.

Collecting Additional Information

In this stage, the engineers will match the information received from the organization with additional data from public sources. This helps by finding informational gaps (details that the organization didn't know or overlooked).

Furthermore, this stage is designed to put the information gathered in the previous step in a larger context and get a better idea about what the typically threats in an industry are.

Scanning and Discovery

The information from the previous two phases is used to find all the assets that may be vulnerable: ports, various services, subdomains, web applications, and more.

Vulnerability Assessment

Once the basics are identified, the automated vulnerability assessment can begin. This stage identifies all the potential security weaknesses that might allow attackers to gain access to the organization's assets.

The vulnerability assessment will provide a list of threats (usually ranked by severity), but it is up to the cyber security specialists to perform a final check and determine which should be tackled first.

Why can't this be done automatically?

Because vulnerability scans are designed to identify all the potential threats. However, in practice, engineers often find that even though a vulnerability has been listed in the scan results, it has already been mitigated by using another application or service, so it's no longer a priority.

Penetration Testing

This is the human-led phase of the VAPT process and where the magic happens. Security experts will use the results of the scan from the previous step as a starting point. After ranking the threats identified, they will try to manually exploit them, just like a hacker would.

This phase is designed to give you a clearer picture of which vulnerabilities are easiest to exploit and what cost they may incur. It is also where you can better understand which of your assets need better protection.

Final Reporting and Analysis

This is typically the end of the VAPT process, but the beginning of the remedial actions. You will receive a comprehensive report that details the methodologies used and the findings of the VAPT process, along with recommendations for remedial actions and a list of priorities.

The final report is the organization's roadmap for security enhancement. If its recommendations are followed, the next VAPT should reveal fewer vulnerabilities and make remedial actions less and less time- and money-consuming.

About bluedog Security Monitoring

Our goal is to provide businesses with a level of network protection typically only afforded by large corporations. We aim to bring high-quality technology, support, and service to the small to medium business, helping protect their business from cyber threats.

Our company is growing quickly, through our simple and affordable end-to-end network monitoring solution, Microsoft 365 Monitoring, Virtual CISO and low cost VAPT services. Recently voted one of the Top 10 cybersecurity start-ups of 2019 by Enterprise Security Magazine. Whether you are a small business, or an MSP or IT services reseller or distributor, get in touch and have a chat with us.

20-22 Wenlock Road, London, N1 7GU

info@bluedogsec.com

+44 20 8819 6254