Top 10 Things You Should Know about VAPT

2020, the year of the pandemic, also brought a cyber pandemic. The number of attacks and threats increased significantly and they became more sophisticated. With one attack happening every 39 seconds and, on average, 2,244 times each day, security becomes a major concern for companies big and small.

This is where VAPT comes into play. If you're not familiar with this acronym, we don't blame you – it's a relatively new concept in a world where a new acronym seems to pop up every day. However, the statistics above show that you should get familiar with VAPT before your digital assets get attacked.

Let's dig in!

10 Things You Should Know About VAPT

1. What Is VAPT?

VAPT stands for Vulnerability Assessment and Penetration Testing. VAPT is a term that describes security testing designed to identify and also help address vulnerabilities.

VAPT is an umbrella term that can include several testing techniques like automated vulnerability assessment, penetration testing conducted by skilled human engineers, and even red team operations.

2. VAPT Is a more Comprehensive Testing Solution

Automated vulnerability assessment is a great start. Pen testing is also an important security measure. But VAPT brings both of these techniques and others under the same virtual roof to offer companies a more comprehensive view on their security issues.

With VAPT, it's easier to discover and mitigate critical vulnerabilities across platforms and software types, even third-party ones.

3. VAPT Can Help You Discover Gaps between Various Security Tools

If you're a regular on our blog, you already know that we advocate for a combination of automated and manual testing and assessment. However, even the combination between automated vulnerability assessment and manual pentests leaves you open to some vulnerabilities.

For instance, if you run two different vulnerability assessment tools for the same application, the results can be completely different. How can you know which one to trust?

VAPT adds a new (most often manual) layer to all these. This integrative approach to security testing is designed to bridge the gaps between automated tools and create a unified perspective on security vulnerabilities.

4. VAPT Helps You Prioritize Risks

Even some of the more risk-aware companies forget about this crucial step. They find and collect vulnerabilities but simply forego risk prioritization – the most important step.

In the current cyber security landscape, where threats are increasingly diverse and sophisticated, risk prioritization is an absolute necessity. Otherwise, you may end up spending a lot of time on trivial risks, while the very severe ones are left unattended. In turn, this exposes your organization to serious threats that could have been easily mitigated.

Risk prioritization is an integral part of VAPT. A good VAPT strategy addresses and emphasizes this step by clearly marking which threats and which risks should be tackled first.

5. VAPT Uncovers Misconfigurations and Loopholes in Various Applications

The number one reason for successful cyber-attacks is human error. Web applications, networks, mobile apps – all of these are written by humans and, thus, prone to errors. This is exactly what attackers are looking to exploit.

Most exploitable vulnerabilities are due to misconfigurations or incorrect coding practices. Both of these things can be present in your own applications or in third-party ones.

VAPT run by a third-party company is the easiest way to spot them and address them before they become chronic issues or, worse, before an attacker is successful. Choose your VAPT provider carefully, though. You need to work with a company that cuts no corners when it comes to the skill sets of the engineers they hire.

6. VAPT Improves Your SDLC Process

SDLC (Software Development Life Cycle) is a methodology that IT companies live by. As it happens with all methodologies, SDLC needs to evolve constantly to respond to new market demands and even to new cyber threats.

Regular pen-testing as part of your VAPT process aligned with the SDLC process is the near-perfect way to ensure great security. This way, your code, along with all the changes to it, go through numerous security checks that are able to spot vulnerabilities early on, long before you launch your product.

7. VAPT Has Excellent ROI

Do you know what happens to the money you invest in cyber security? Probably not. In fact, it's one of the fields that's notorious for hard to pinpoint ROI. As long as no attacks happen, you consider it money well invested.

And you're not wrong.

But, thanks to its comprehensive approach, VAPT can tell you exactly how much money you saved by choosing an integrative approach instead of disparate testing methods, for instance. Or how much, on average, a successful attack might have cost you.

8. One Concept, Multiple Applications

VAPT is not only ideal for web applications. It can also be successfully used for mobile apps or for networks. In fact, any internet-facing asset can use VAPT.

Of course, the term is the same, but the approach differs from asset to asset. This is why the human component is essential to the VAPT process. A human-led approach helps with choosing the right tools and the right processes to identify the most frequent vulnerabilities for each type of asset.

9. There Is No One-Size-Fits-All in VAPT

Yes, there are numerous tools that can be used for various applications. And yes, the VAPT process is has a few core components that will stay the same across all the assets to be tested.

But all in all, the VAPT process will be different from company to company. The approach and duration depend on the size of the company, the amount of data, and the amount of devices and assets to be tested and scans.

10. VAPT Helps with Compliance

An increasing number of companies use VAPT as the surest and fastest way to achieve compliance with various standards like GDPR, ISO 27001 and PCI DSS. Even if conducted solely for compliance purposes, VAPT will still spot major vulnerabilities and can help you keep your assets safe.

Final Thoughts

VAPT is, ironically, one of the last things on managers' minds. Until the first attack is successful, that is.

With the average attack costing more than $2 million, do you really want to wait that long? We promise VAPT is less expensive and less painful than a successful attack.

At Bluedog we have a suite of VAPT services, from low-cost monthly automated scans to in-depth manual penetration testing, contact one of our resellers today about VAPT; don't wait until you're attacked.