TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

#StayGuarded

VULNERABILITY ASSESSMENT

INCREASINGLY BECOMING TOP PRIORITY OF C-SUITE IN THE NEW NORMAL

contactcs@tataadvancedsystems.com

www.tataadvancedsystems.com

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Conducting an assessment to look out for vulnerabilities existing within the networks, applications or infrastructure has always been an ideal approach to safeguard your organization against evolving and complex cyber threats. And, doing so on a regular basis takes an organization far ahead of the reach of cybercriminals.

But, during these uncertain times when businesses have adapted to a remote working model, the attack surface has exploded to a large scale. After which, Vulnerability Assessment (VA) has now surfaced as the core requirement of the CISOs, CIOs, COOs and other C-level executives. The reason behind the expansion of the attack surface and growing demand for security assessment includes:

- ***Introduction of Personal Devices:*** Most employees were not provided with company-issued laptops or computers to continue work from home. Consequently, they were using their own devices to access corporate resources and data that may have vulnerabilities or already been compromised. Also, they have made a huge dependency on web conferencing & collaboration tools like Zoom, Microsoft Team Meeting, Google Meet, etc. for daily operations. Throughout this global crisis, threat actors have leveraged such platforms to deceive people and compromise their devices.

- ***Migration to Cloud:*** Owing to the current pandemic, organizations have promptly moved to the cloud to accommodate remote workforce requirements. But this swift movement has also opened them to multiple risks including configuration errors, vulnerabilities within the applications, security oversight issues, etc. As per the Cloud Threat Landscape Report 2020, any unauthorized access to cloud assets can result in losses of more than $50000 in less than one hour. Also, over one billion records were stolen in 2019 due to misconfigured cloud servers.

- ***Insecure Home Networks:*** Home networks often lack sufficient security measures that are required for a secured connection with corporate resources. For instance, it does not include intrusion prevention systems, advanced firewalls (say WAFs), etc. This may allow cybercriminals to enter into and get access to critical corporate data and applications. As per a report from BitSight, it was found that home networks are 3.5 times more expected as compared to office networks to be infected by malware. Threats like Mirai malware and Trickbot were observed 20 and 3.75 times, respectively, more frequently on home networks in comparison with corporate networks.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

How Vulnerability Assessment Helps

As the new normal has begun, businesses are recognizing the need for a proactive approach to detect and remediate the security flaws (if any) to prevent threat actors from causing havoc and stealing sensitive business-critical data. The VA provides a clear picture of the effectiveness of the security controls in place. It enables organizations to fill the security gap in their security posture before getting exposed by the cybercriminals. An effective VA can yield several benefits including:

- Find known security vulnerabilities before attackers exploit them
- Discover all the critical assets present on the network, including vulnerabilities associated with each asset
- List of required future upgrades
- Define the level of risk
- Prepare a well-defined response plan

Outsource Vulnerability Assessment Services

Typically, it is often seen that organizations prefer to have their in-house vulnerability assessment team. An in-house team has its business advantages like it has a better understanding of the systems being assessed, and availability as per the company's schedule or requirement. But due to the lack of skilled resources, it is somewhat difficult to find the right talent and create your own VA team. Alternatively, businesses can outsource security teams to conduct VA in their environment. It saves time and efforts that can be further utilized in other business functions. It can also help CISOs and CIOs to reduce dependency on internal resources, improve prioritization of human assets, meet compliance with different industry regulations, etc.

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

How Market is Shaping

As per a report from MarketsandMarkets, the global Security and Vulnerability Management market is predicted to increase from USD 12.5 billion in 2020 to USD 15.5 billion by 2025, with a Compound Annual Growth Rate (CAGR) of 4.5%. The contributing factors include growing cyber awareness among developing economies, soaring mandates for adhering to regulatory compliances across organizations in different verticals, growing volume of cyberattacks such as phishing, ransomware, DDoS and malware. According to an estimate by Cybersecurity Ventures, the global annual cost of cybercrimes will reach USD 6 trillion by 2021.

Conclusion

Rather than a quinquennial review process, Vulnerability Assessment should be viewed as a continuous process performed after regular short intervals. An in-depth understanding of the potential security risks within the security posture of an organization can aid C-level executives and their security teams to effectively manage business operations in the new normal while reducing the risks of being compromised. Conducting assessments, along with the implementation of appropriate security solutions like Zero Trust and Privileged Access Management will expand the security capabilities of businesses and help them to stay on top of the vulnerabilities.

If you are looking to assess and revamp the security posture of your organization, connect with us at

contactcs@tataadvancedsystems.com

or visit at

https://www.tataadvancedsystems.com/cybersecurity.php