TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

EVOLUTION OF CYBER SECURITY IN THE POST-COVID WORLD

PROACTIVE APPROACH IS A MUST

The concept of a “Proactive Approach to Cyber Security” is not new but seldom applied since most organizations had and still have a reactive cyber security strategy in place. As a result of which a majority of businesses suffered long-term losses, and some got drained. Evolving cybercrime, including new attack techniques and advanced tools, is shifting the momentum from reactive to proactive cyber defence.

While talking about recent times, COVID-19 outbreak has fueled the growing spike of cyber attacks across the globe. It has given cyber criminals a lot of opportunities to break down and evade our efforts to safeguard our critical digital assets. They leveraged the moment when organizations had to switch from the traditional approach to the new normal. As much as we are bringing innovation and automation into the digital ecosystem, it is adding another entry point for the threat actors to get hold of the victims’ systems and sensitive data.

Proactive Approach in Perimeter-less World

These days, businesses of all sizes (across different verticals) are mindful that cyber security matters as the shift to remote work is here to stay for long. As more the workforce will work beyond the perimeters of the enterprises, the attack surface of organizations will continue to increase. It will also become a daunting challenge to manage the security of the remote assets. Additionally, the increased application of IoT devices also made it difficult for organizations to manage security. Since these devices are made keeping user experience in mind, it is slightly easier to shatter their defence and get access to the system.

As attacks are becoming, even more, smarter and persistent than ever, adopting a Proactive Approach can be the key to get back control over what’s happening within your corporate network. It is a holistic approach to security that focuses on prevention rather than repairing.

The Proactive approach helps organizations to understand their security infrastructure and underlying systems, applications, networks, data, etc. It involves recognizing and fixing security risks before attackers exploit them and damage the reputation of the company.

Contents of a Proactive Cyber Security Strategy

Proactive cyber security strategy involves different methods and techniques that helps in preventing cyber attacks from happening. It includes (but not limited to):

- Complete visibility of the security posture
- Red Teaming & Blue Teaming Exercises
- Proactive Monitoring of Networks and Endpoints
- Security Awareness Training
- Advanced Threat Intelligence
- Periodic Vulnerability Assessments
- Build Own Security Operations Center

Reap Benefits of a Proactive Approach

Do not wait for a cyber security incident to happen. Take action before attackers reach you and penetrate your defence. Below are the few advantages of implementing a Proactive Cyber Security Approach:

- Actively prevents cyber attacks and data breaches
- Boosts confidence of the customers, partners and third-party vendors
- Provides time to build effective response strategy for complex threats
- Catch the adversaries by using advanced threat intelligence
- Mitigate the risks from malicious insiders
- Strengthen compliance with industry regulations and data protection laws

Towards The End

Being proactive will offer more control over an environment and provide comprehensive visibility of your organization's IT assets. Adding proactive strategy to cyber defence can really increase the level of protection and resilience against Advanced Persistent Threats (APTs), ransomware, malware, phishing and more related cyber attacks. The ultimate goal of this strategy is to let people –

"Focus on Preparing, Rather than Repairing."