TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

FOSTERING CYBER SECURITY IN A HYBRID WORK MODEL

Is Your Organization Ready?

Incontestably, the last 15-18 months have bought a pivotal shift in the lives of people as well as organisations globally. Businesses are brainstorming and coming up with new initiatives to sustain business continuity, preserve employees' well-being and safeguard their reputation, along with critical assets and information against sophisticated cyber-attacks. Accordingly, some companies are planning to adopt or move to a Hybrid Work Environment to resume operations in a post-pandemic atmosphere.

Comprehending The Hybrid Work Model

Hybrid work arrangement is a remarkable shift from the conventional work model. It can have multiple variations. For instance, businesses might provide their employees with the flexibility to work remotely and from the office. Employees have the freedom to choose where they are most productive, and even they can prefer a blend of both.

This model is perceiving a boom in popularity due to several reasons, including an increase in productivity, improved work-life balance and job satisfaction, deep visibility into an employee's performance and reduced costs for businesses. The time in the office can be now utilized for collaborative initiatives and in-person meetings.

Are We Underrating the Risks of the Hybrid Work Model?

The Hybrid Model has undoubtedly gained multiple benefits for organizations. But, concurrently, incorporating this new way of working has opened the doors of new cyber risks to businesses. They are facing different security challenges as the workforce is constantly switching between remote and office locations. While working from outside the office, they often follow sloppy safety measures like using public networks where they may get affected by malware or trojans.

Let's walk through some critical security challenges of a Hybrid Work environment.

- **First Line of Defence – Humans**

  Humans are generally considered the weakest link in the security chain of any organization. Lack of proper cyber security awareness among them may become the major cause of a cyber-attack. Threat actors use techniques like social engineering, phishing, smishing and vishing to trick victims and gain access to their systems. Since the remote workforce is more exposed to these threats, the risk is considerably high.

- **Mounting Reliance on Cloud**

  The growing adoption of cloud technology over the last two years has gained the attention of cybercriminals. Despite having multiple benefits, the cloud has its own set of susceptibilities that could raise concerns about data protection, security and compliance. Business-critical information can be compromised in different ways. It may get damaged, corrupted, inappropriately accessed or simply lost, resulting in a catastrophe for an organization.

- **Shifting Perimeters**
  One of the biggest challenges of this new way of working for organizations is the fact that people will be required to access data beyond the perimeters of the company. In such circumstances, businesses will be required to pay attention to security concerns around how the data is being accessed, transmitted and stored. Investment in the right tool and technology will become a pivotal factor in the race against threat actors.

- **Attacks Targeting Vulnerabilities in VPNs & Windows RDP**
  Cybercriminals always look to target and exploit the vulnerabilities in the unpatched VPNs and misconfigured RDP servers. It will be vital for organizations to ensure that patching is done on time and regularly. They must evaluate their existing authentication systems and implement multi-factor authentication to add an additional layer of security for remote access.

- **Usage of Personal Devices**
  Along with the challenges of the moving perimeter, there are plenty of organizations that are facing issues due to BYOD culture. Since the workforce can use their own personal devices to access corporate assets, companies ended up loosening the security and focus on how the data is moving outside their boundaries. The biggest concern of such policies is to ensure that data is not leaking out of the environment.

How to Protect Your Hybrid Environment?

Businesses moving to the new hybrid model of working must execute security strategies that should safeguard their critical resources (including data, systems, servers, etc.), remote workforce and operational continuity from the rising wave of cyber threats.

An organization must consider the below-mentioned cyber security practices to create a successful hybrid work environment and mitigate the risk of cyber attacks.

- Installation of anti-malware/virus software
- Conducting cyber security awareness sessions
- Implementation of Virtual Private Networks (VPNs)
- Execution of multi-factor authentication
- Patching security loopholes by installing regular updates
- Practising strong passwords
- Maintaining regular data backups
- Implementation of an Advanced Web Application Firewall (WAF)

Towards The End

Establishing a positive and secured hybrid work environment entails the utilization of the right tools and technology to enable the workforce to access all the important resources at the required time to finish their tasks. Enterprises of all sizes can reduce the risk of a hybrid work model by employing a proactive cyber security approach that must involve necessary measures like regular security audits, implementation of Zero Trust, application of anti-malware software, data backups, etc.