TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

CYBERSECURITY PREPAREDNESS –LESSONS WE LEARNT IN 2020

www.tataadvancedsystems.com

To call 2020 a year filled with unprecedented challenges would not be an overstatement. Right from the eruption of COVID-19 pandemic to a comprehensive list of disruptive cyber-attacks, 2020 has engendered enormous concerns to enterprise cybersecurity teams. While these cyber-attacks have caused terrible damage to many organizations globally, they have also presented several key lessons for cybersecurity and information security professionals moving forward. By taking into consideration these lessons, enterprises can augment and strengthen their security posture against the rising wave of cyber threats.

Now as we move towards a new calendar year, let us have a look at some critical areas that need to be looked after cautiously.

Data Security is Crucial

As per a recent report from Risk Based Security, the number of records exposed through the end of September 2020 has increased to 36 billion. Two breaches in Q3 leaked more than 1 billion records and four breaches exposed over 100 million records, which together accounted for approximately 8 billion exposed records.

Therefore, companies must look to protect their sensitive data in all forms i.e. at rest, in motion and in use throughout its lifespan. They should ensure data integrity, security and consistency by heeding advanced security controls like robust encryption policies that can help in reducing the impact, to some extent, if data is exfiltrated or stolen. They can establish a data governance program to manage the flow of critical information across the organization. This program may include (but not limited to) the below points:

- Assigning roles and responsibilities for managing and monitoring the consistent and effective management of the data assets
- Identifying who can take what actions, with what data, under what circumstances
- Establishing different security levels for different categories of data like highly sensitive, moderately sensitive and publicly available information

Check For Vulnerabilities

Threat actors discover and exploit vulnerabilities in order to penetrate corporate networks and infect critical resources with malware, Trojans and worms. Organizations must seek to identify and address the existing security gaps through vulnerability assessments that should be followed as a continuous practice performed at regular intervals. Such assessments have become more important than ever as employees have started coming back to their offices after a long break of remote working. Safety practices such as patching vulnerabilities and reviewing security settings will play a key role in mitigating cybersecurity incidents.

Cybersecurity Awareness & Training for Employees

As humans are more likely to create errors in comparison with digital assets, threat actors primarily target them using popular techniques like Social Engineering and Phishing. So far, we have witnessed several instances where cybercriminals leveraged human vulnerability to cause damage and gain huge profits.

Did you know that around 22% of breaches in 2019 involved phishing? (Source: Verizon DBIR 2020)

In 2020, the phishing attacks have continued to explode. As per the APWG's Trend Report Q3 2020, around 199,133 unique phishing websites were detected in September. The report revealed that Saas & webmail sites were the most targeted industry sectors in Q3 2020. The most noticeable thing is that 80% of phishing sites were protected by the HTTPS encryption protocol.

Therefore, enterprises must mitigate the probability of human errors through regular training and awareness sessions. Improving awareness will not only enhance cyber hygiene and reduce cyber risks, but also help in cultivating cybersecurity culture within organizations.

Look For Ransomware

Ransomware has been the most prevalent cyber-attack faced by organizations across the world in 2020. As per a recent report by SonicWall, ransomware attacks globally have increased by 40% to reach 199.7 million in the Q3 2020. Enterprises need to remain careful and can follow the below-mentioned practices to ensure their safety:

- Encourage employees to avoid clicking on the unknown URLs
- Create data backup
- Avoid disclosing personal information to unknown calls, texts or emails
- Promote usage of anti-virus/anti-malware software
- Conduct security awareness sessions

Be Ready with Incident Response Plan

Companies should follow a proactive approach while preparing themselves to defend cybersecurity incidents. This approach can help organizations to protect their critical data, brand reputation, customers' trust from getting impacted by malicious activities. An Incident Response plan may include (but not limited to) some key phases including preparing a plan to prevent and respond to events, identify incidents and its severity, containment of the incident before it causes damage, addressing the root cause of the incident and restoration of systems to normal operation.

Towards the End...

Cybersecurity is not an overnight process. It is an ongoing practice that takes time and continuous efforts. This COVID-19 crisis has taught us the reason behind why we are at risk. And that is, we are not enough prepared. We often wait for things to happen and then react accordingly. To stay safe and secure, organizations need to follow a proactive approach and invest in their security infrastructure to prevent themselves from falling short to evolving, complex cyber threats.