Best Data Security Practices for Businesses in 2019

Data threats are expected to rise rapidly in the near future. Fortunately, the solutions and technologies to prevent and mitigate them are increasing too.

The year 2018 was an excellent one for data security. An increasing number of businesses have already updated their systems and have included orchestration, automation, the cloud and case management into their data security strategies.

However, while businesses are now concerned about the safety of their data and are taking preventive measures, multiple large ransomware attacks and breaches have been observed in the last couple of years.

We present a detailed look at some of the best practices for data security that are expected to rule in 2019.

Tackling IoT ransomware

Traditional ransomware attacks rely on irreversibility where the attacker has the key that can provide you with access to your computer, laptop or smartphone. Contrarily, IoT ransomware depends on timeliness. The attackers strike you at times when you are unable to counter the ransomware effects or reset your device. Paying the ransom seems the obvious solution in such cases.

With the number of connected devices rising significantly with every passing year, businesses would imperatively need to prepare themselves to tackle IoT ransomware in 2019. Implementing robust network security protocols and authentication mechanisms that can prevent spoofing and regularly updating firmware are some of the ways to protect your data from such attacks.

Planning for BYOD

The rising trend of “Bring Your Own Device” (BYOD) also introduces a host of risks concerning data security. To boot, more than 63% of the companies already have remote workers. The number is only expected to rise in the future. Apart from training the employees to protect company data, there is a rising need for additional security measures.

IT security teams need to make sure that they have a multilayer approach with elements like data encryption, device authentication, employee authentication and the ability to wipe the data remotely in the event a device is stolen or lost. As BYOD is known as one of the most significant data blind spots, adequate measures should be put in place to avoid data breaches.

Testing the backups

Most businesses, especially the ones that use cloud computing, now invest in several tools for backing up their data. However, many fail to test them periodically or regularly monitor their functioning.

Do not wait for something like a ransomware attack to know that your data backup tools are not working. If you are planning to invest in such devices in 2019, make sure that they are regularly tested, and the data is safeguarded.
Using advanced data security solutions

It is not just the attackers that are getting smarter. There are now advanced technologies, services and tools that can help businesses keep their data protected. In the coming year, such modern solutions are expected to be used by most large companies. With even small and medium enterprises now concerned about data security, it is only a matter of time that they too start following the trend.

From cloud and SaaS, connectivity and IoT solutions, to mobile device management and protection against DDoS attacks, there are already a host of solutions available to help businesses create effective data protection strategies.

Tata Tele Services offers MPLS-based VPN with Secure Connect, which works as a bridge for providing businesses with a dedicated connection to leading cloud service providers including Microsoft and Amazon.

With multiple options for connectivity, improved security and real-time performance reporting, businesses can improve their performance and place additional layers of protection against data threats of the present and the future.