BIZCOMMUNITY

The importance of protecting your data

By Lukas van der Merwe

19 Mar 2020

In its recent research, the Ponemon Institute shows that a data breach costs South African companies on average $3.06m - nearly R50m. This is somewhat above the international benchmark, with the study showing that globally the average cost of lost business after a data breach was $1.42m (R22m).

Lukas van der Merwe

For this reason, protecting sensitive data both in transit and at rest has become imperative for modern enterprises, as attackers are finding increasingly innovative ways to breach cybersecurity systems and steal data.

Data protection at rest aims to secure inactive data stored on any device or network, while data protection in transit is the securing of information while it is being transferred from network to network, or from a local storage device to the cloud.

Data on the move more vulnerable

Data in transit is generally more sensitive than data at rest, but attackers often find data at rest to be a more valuable target, as there is a greater quantity of it. Wherever data is being moved to, effective protection measures for in-transit data are critical as information is often considered less secure while in motion.

Legislation, such as the European Union's General Data Protection Regulation (GDPR), has a significant positive impact on improving security controls, as it is designed to maintain the privacy of data of individuals, forcing organisations to adapt technology to meet its requirements.

Essentially, GDPR stipulates that data can only be collected with explicit permission and only for the purposes agreed upon. It also sets out that organisations must have visibility of where data resides, who has access to it and how it is stored, in terms of security and encryption.

The complexity of the legislation and onerous requirements can be problematic to businesses, leading to "compliance fatigue", but the bigger impact on organisations is the business challenge that it creates. It is no longer up to the IT manager to decide who can access data and use it, it is a business-level discussion, involving legal, risk and compliance considerations.

Data regulations to be tightened

Strict data protection legislation is currently lacking in South Africa, which means that organisations are not obliged to report security breaches and these incidents often go unreported, especially when it is deemed that the breach did not affect anyone. However, the imminent Protection of Personal Information (PoPI) Act will tighten up regulations and organisations will be required to post-event reporting and how the incident was dealt with.

The increasing complexity, sophistication and frequency of cyberattacks mean that companies need to think about data protection as a first priority, yet many still see it as an inhibitor. Yet, data protection is not optional, especially in a complex environment where a host of different devices access a network.

Experts in data protection can guide a business from a legal point of view to develop policies, determining what responsibilities the organisation must fulfil, and how systematic processes can be automated to manage and control sensitive data.

Organisation need to keep in mind that no system is impenetrable, and no protection is infallible. Sooner or later, a breach will happen, and companies need to be ready to respond. The response to a cyberattack is very important as it will significantly affect the impact of the breach.

ABOUT THE AUTHOR

Lukas van der Merwe, Specialist Sales Executive: Security at T-Systems South Africa