Focusing on cybersecurity in 2020

By Ralph Berndt

24 Jan 2020

As we welcome in the new year, companies today have unprecedented access to innovative technologies that empower them to drive business opportunities irrespective of industry sector. However, cybersecurity must remain the cornerstone of any organisational strategy to ensure data remains protected.

Ralph Berndt, director of sales at Syrex

Thanks to the arrival of two Azure multinational data centres in the country, it is anticipated that Microsoft will push the security agenda even more as their focus turns to the consumption model of a cloud environment.

This requires a mindset shift from decision-makers as organisations transition from CapEx on-premise setups to OpEx cloud ones. So, instead of worrying about software and hardware maintenance, the business can concentrate on delivering on its mandate while the cloud provider takes care of the rest.

And when it comes to cybersecurity, the biggest question for companies migrating to Azure will revolve around whether they will use the options available from Microsoft or look towards other vendors. Fundamentally, it comes down to protecting both the on-premise and cloud investments while maximising the protection available from the likes of Azure and Office 365.

People management

But in as much as companies need to find technological solutions to provide better data defences, social engineering will remain an increasingly important attack vector to safeguard against. Thanks, in part, to social media, people have become flippant about what information they share online. And this extends to company information as well. More must be done to educate employees about the impact of sharing sensitive information and the typical social engineering tactics used by malicious users.

Even though 2020 will see more focus on corporate attacks, individuals must never rest on their laurels with identity theft, phishing, ransomware, and so on still being significant threats. And given how data drives all our personal and corporate decision-making, the threat landscape will only intensify.

Ongoing attacks

With South African entities (across private and public sectors) hit by numerous Distributed Denial-of-Service (DDoS) attacks last year, this reflects the level of sophistication from attacks. Furthermore, well-orchestrated phishing attacks mean companies cannot ignore investing in cyber protection. Yes, data (whether it is on-premise or in the cloud) can never be considered completely safe, but planning must become an integral aspect in the months ahead.

Overhauling disaster recovery and business continuity strategies are imperative. Also, penetration testing must be regularly done to ensure data is safe and what the steps will be if a compromise should occur. And then, decision-makers must ask themselves how they manage their data and how does it get moved around. It comes down to how data is protected throughout the value chain.

This will result in service providers doing more cloud security readiness profiling for organisations. These assessments will cover not only protection from an external perspective but an internal one as well. How ready are companies to deal with an attack especially prior to migrating their assets to the cloud? The environment must be prepared accordingly with more out-of-the-box thinking needed to protect data in this always-on world.

ABOUT THE AUTHOR

Ralph Berndt, director of sales at Syrex

For more, visit: https://www.bizcommunity.com