BIZCOMMUNITY

Think cybersecurity is expensive? Just wait until there's a breach...

By Lukas van der Merwe

18 Dec 2020

Medium-sized companies in South Africa are in a precarious position in terms of cybersecurity. While they find themselves firmly in the crosshairs of cybercriminals, they also have limited options to successfully defend themselves against cyberattacks, as the challenges faced by this market segment are multifaceted.

Lukas van der Merwe

South Africa has been near the top of the list for cyberattacks for some time now and has one of the highest risk ratings in the world. Unfortunately, it is becoming increasingly difficult to reduce this, as attacks are continuing to become more sophisticated.

Consequently, companies in the mid-market sector face numerous hurdles with regards to cybersecurity, with affordability topping the list. In most cases, smaller and lower-margin organisations simply cannot afford next-generation technology to improve their cybersecurity posture. At the same time, many still believe that smaller entities are less likely to be targeted than large enterprises.

The affordability aspect is also related to the fact that it requires expert skills to implement and maintain not only next-generation security solutions, but simply what is currently accepted as good practice. Given that the cybersecurity landscape changes on a daily basis, no static implementation would be relevant or offer the kind of protection required. So, if an organisation does not have an extended security team, it is difficult to maintain currency.

Bigger attack surface

The situation is further exacerbated by the current pandemic, as many organisations are adopting remote work practices, cloud and software-as-a-service solutions. While this offers more sustainability under the circumstances, it frequently expands the attack surface of an organisation in terms of cyberattacks.

As a result, the cybersecurity question becomes so overwhelming for many mid-market enterprises that they simply stick to what they know, which is the traditional “castle and moat” approach. This entails putting in place some perimeter defence and endpoint protection, keeping it current and hoping for the best. Yet, this is becoming increasingly inadequate.

It is difficult to quantify a cyberattack in terms of costs for mid-sized companies, as reporting is not mandated in South Africa. However, IBM’s 2019 Cost of a Data Breach Report found that a data breach now costs $3.92 million on average. The report warns that a breach can be particularly acute for small and midsize businesses, with companies with less than 500 employees suffering losses of more than $2.5 million on average.

South African mid-sized businesses come close to the average number quoted in the report, so a cyberattack could potentially be financially devastating. What’s more, enterprises could suffer reputational damage and a resultant loss of business if sensitive customer data is exposed. In addition, depending on the industry, the company and its dependence on IT, a breach could bring operations to a halt, leading to further financial implications.

The bare minimum

As an absolute minimum, all mid-sized enterprises should have perimeter and endpoint protection in place. There is a myriad of solutions that offer multiple layers of protection, depending on the type of information an organisation processes and its specific risk profiling.

From an access protection point of view, beyond basic perimeter protection, companies need to consider network access control to ensure that only authorised users can access its network. With a significant amount of remote workers, companies now need to ensure that they securely connect its network, so VPN technology would be key. The list is almost endless in terms of what solutions can be added on top.

Most mid-size companies can do little of this successfully and this is where managed security service providers can offer significant value. They can leverage shared solutions that are in place for a larger number of customers, whilst maintained by a group of experts with significant experience. This can be implemented at a unit cost, far below what a dedicated investment would be.

They should consider looking at managed security service providers that deliver an end-to-end service, instead of investing in their own technology, which could be prohibitively expensive and difficult to manage and maintain.

It is important that enterprises perform a holistic risk assessment and define the defence cost relevant to their organisation, before dismissing any cybersecurity investment as too expensive. The impact of a breach would be far worse.

ABOUT THE AUTHOR

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