BIZCOMMUNITY

Understanding cybercrime's true impact is crucial to security in 2021

By Simeon Tassev

3 Feb 2021

During the heaviest lockdowns of the Covid-19 pandemic in 2020, we saw a significant spike in cybercrime. The rapid shift to digital and swift enablement of a remote workforce resulted in an increase in the number of potential targets, as companies had to further open their systems.

Vulnerabilities were exploited to the maximum, and there were a number of highly publicised attacks across the globe. However, while this has led to greater awareness of the risks and an increase in caution, businesses cannot afford to let down their guard in 2021. Cybercrime is an ongoing issue, not a temporary threat due to lockdown, and organisations need to continue to be vigilant and monitor and improve on their security systems.

Understanding the risk is key

Cybercrime is not a new issue, nor is it one that will go away in time. Understanding the specific risks and potential threats in the environment regardless of the size of the business is the first step in formulating an effective security strategy.

Only once the risks and threats are understood, can any gaps in defences be identified and then, through continuous monitoring and improvement, be closed.

One of the considerations many businesses have been forced to take when moving online is the need to be Payment Card Industry Data Security Standard (PCI DSS) compliant.

#BizTrends2021: What the new year holds for cybersecurity

Brian Pinnock 6 Jan 2021

This standard is relevant for any organisation processing payments via payment cards such as debit and credit cards, which means any business that moved to an e-commerce model must comply.

However, this standard is only the minimum requirement, and ensuring effective security, especially when it comes to sensitive information such as customer details and payment data, requires a lot more measures in place. Using PCI DSS as a benchmark is an excellent starting point, but it should not be seen as the ultimate destination.

A tick box approach is not effective

Security is not just about ticking boxes for compliance, it is about protecting your business, by understanding the potential impact on the organisation of cybercrime and the effectiveness of systems in preventing it.

For example, a successful cybercrime attack could result in data held to ransom, costing significant sums to recover and potentially resulting in fines for compliance breaches. The lasting impact of reputational damage can also cause financial strain in the long term.

It is essential for businesses to firstly ensure that their processes are both sustainable and scalable. This is not necessarily relevant only for security, but also for general business operations.

In addition to being sustainable and scalable, processes also need to be defined in a secure manner. Enhancing capacity and performance at the expense of security is a poor strategy that will inevitably lead to problems. All tools need to be fit for purpose and secure.

Lack of awareness is not an excuse

The most critical step to ensuring security in 2021 and beyond is for organisations to understand what the potential risks are. Only once this step is undertaken is it possible to develop a plan of action that is aligned with the specific risk factors and business priorities.

Whether the resulting strategy is to accept the risk or mitigate it, this decision can only be made if the risk is known.

Engaging with a reputable service provider can help businesses to reach the appropriate level of understanding and then make informed decisions around risk, empowering them to deploy the right solutions to ensure adequate and scalable security systems.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa

- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...