Digital security in the post-pandemic business landscape

COVID-19 is changing the digital threat perimeter

According to the global research and advisory firm Gartner, spending on cloud security is predicted to be the fastest riser of all cybersecurity markets, with an expected increase of 33%, driving the market to an expected $585M this year.

In fact, cloud security is the smallest but fastest-growing segment of the cybersecurity market, driven by the small initial market size and companies' opting for cloud-based cybersecurity solutions.

In March, when the global pandemic started, the business VPN solution NordLayer saw a 165% usage spike and an almost 600% increase in sales overall, reflecting the unprecedented need for securing remote access. Since then, the digital threat to bandwidth has increased dramatically.

"In this rush to adapt, many companies have neglected or ignored both their risk and change management processes. Now that many employees have shifted to remote work — in addition to organizations being distracted trying to handle the virus — security and risk management teams need to be more vigilant than ever," says Juta Gurinaviciute, Chief Technology Officer at NordLayer.

Cybersecurity risks posed by remote work can be categorized into three key areas: people, places, and technology. The risks presented by people include employees falling prey to social engineering, phishing, and targeted attacks that aim to capture users' credentials or make them accidentally download malware. Place-related risks include connecting to corporate networks from unsecured homes or public Wi-Fi.

Technological risks have to do with using personal or unauthorized devices that aren't in line with corporate security policies, and patching hardware.

"Despite the speed, we're still at the early stages of the remote work revolution. If you have 5,000 employees, you now have 5,000 remote offices to protect," the NordLayer expert adds.

On the other hand, large, global businesses are continuing to encourage remote work for their employees. Larger companies are better suited to remote work primarily due to their access to innovative collaboration, resources, budgets, and communication services. Alternatively, many SMEs are quicker to adapt, and thus the transition may be easier for them. However, a lack of security education and resources has made SMEs a prime and vulnerable target for attacks.

Gurinaviciute comments: “Cloud computing has proven battle-ready during COVID-19, demonstrating it can support unplanned, unexpected, and dynamic needs.”

COVID-19 has set a new baseline for effective and secure remote work, and we should assume that many organizations will continue to utilize remote and distributed workforces after the pandemic ends. Gartner’s HR survey reveals that 41% of employees are likely to work remotely at least some of the time in the post-pandemic world. In this new normal, cybersecurity leaders will not only have to protect their organizations in remote settings but will also need to make cybersecurity an integral part of their plans to deliver business value.