Rethinking your security posture in the time of Covid-19

By Jared Naude

13 Oct 2020

The global coronavirus pandemic has led to a cataclysmic shift in the way that many organisations do business. With mandatory nationwide lockdowns, organisations have had no choice but to allow workers to work from home. These drastic changes in ways of working have led to several new cybersecurity risks and threats.

Jared Naude, Cloud Architect at Synthesis

Criminals have capitalised on the fear and uncertainty caused by the global pandemic. The use of Covid-19 related screening, contact tracing and conspiracy theories as bait in phishing campaigns to spread malware and disinformation is substantial. Over 154,000 domains have been tied to pandemic related phishing and malware campaigns targeting users all over the world.

A mature security awareness program is critical to tackle these new risks and threats. User education about the dangers of these phishing campaigns and the new risks of working from home is a must.

Security teams need to realise that users are no longer necessarily sitting on secure segmented and monitored corporate networks. If a user were to click on a phishing link or malware sample, a lot of the controls that would typically be relied upon may not be in the picture when a user is working remotely.

Many organisations assumed that they would have user proximity to provide IT support as needed. However, hardware failures and any support requests which need physical interaction pose a challenge. Not all users had laptops and sourcing new laptops was not always possible under nation-wide lockdowns. This led to users using personal devices which present their own set of security issues such as device encryption, anti-virus, data protection and the possible presence of malicious software on the device.

The threat of IOT devices in user's homes should not be underestimated. The rapid adoption of these devices and the vulnerabilities that they have can easily be used to gain unauthorised access to data by a malicious actor.

The challenge

A key challenge that many organisations have faced is keeping devices up to date. In the past, software updates used to take place on the corporate network but with a remote workforce, these updates must be done remotely. This meant that several organisations have had to readjust their access control lists to allow this as it was previously prohibited from the VPN due to bandwidth considerations.

A burning issue with updates done remotely is data usage, not everyone has access to unlimited high-speed internet and with updates being large, users are often required to bear the burden of the data costs.

Not all organisations were able to allow remote working immediately. To enable a remote workforce, many companies spun up cloud-based infrastructure and exposed internal systems to the internet to allow for remote access and management. This has led to a drastic increase in the number of computing systems that have SSH and RDP exposed to the internet.

The traditional model of firewalls and hardware band aid boxes really start showing their weaknesses in times like these. Managing and updating firewalls can be complex in large environments. The series of critical vulnerabilities that have been found in popular firewall products have an additional burden.

To deal with these challenges effectively, organisations should look at the adoption of Zero Trust computing. A Zero Trust model turns the traditional perimeter model on its head, instead of relying on traditional network segmentation, applications are deployed to the public internet and access is strictly controlled through a device and user-centric authorisation workflow.

Combining strong certificate-based authentication with device health and software defined networking can drastically increase the security of environments, not just for remote workers. Google's BeyondCorp framework and Slack's Nebula are great examples are look at.

ABOUT THE AUTHOR

Jared Naude, Cloud Architect at Synthesis