Take a 360 degree approach to a sound cyber security strategy

According to Fortinet, there are over 300 new Zero Day threats and over 140,000 new malware programmes ou there.

By Mayleen Bywater 16 Jul 2019

Mayleen Bywater

According to Fortinet, there are over 300 new Zero Day threats and over 140 000 new malware programmes out there, wh their security products worldwide are helping to resist 545 000 network intrusion attempts and over 300 000 Botnet Comma & Control attempts - every single minute. And, these are statistics from just one security vendor. The numbers are seemin terrifying.

While this growing number and complexity of cybersecurity threats toward business, and the ensuing breaches, continue make headlines around the world, the news coverage of the resulting attacks often tends to focus on larger corporations th are household names. The reality, however, is that all businesses are at risk, regardless of their size, popularity or how mu they make.

As long as a business has confidential customer records or financial information stored on their network, they are a cybercrime target; hackers know how to exploit any and all weaknesses, and organisations need to take a 360-degree approach to security if they are to sufficiently protect themselves.

Policies and procedures

The starting point for any organisation has to be setting the right policies and standards that make security by default a priority. This encompasses conducting a comprehensive risk assessment, the set of guidelines and procedures, who manages security responsibilities, who has access to information, data governance, setting up training and awareness programmes for staff, and ensuring overall regulatory compliance.

Developments in technology have popularised cloud computing, remote working, bring your own device (BYOD) and more meaning that security cannot be seen or addressed in isolation; the organisation has to take a holistic look at their network emails, endpoints, vulnerability, and business continuity.

From a legacy perspective, a company network is the first port of call for any attacker, as this is what breaks out to the internet, and a breach has the potential to compromise your entire organisation. In this case, it is important to have a reputable firewall between your network and the rest of the internet in order to stop hackers 'at the gate'. Having the right products here can further help your organisation better manage available bandwidth, as well as set up proper access cont and user management.

The email threat

But the latest threats don't target networks, but rather emails, which almost every company employee has access to. With improvements in security technology, humans have been left behind as the most vulnerable of gatekeepers.

Statistics show us that 90% of emails being sent have some sort of malicious intent (malware, phishing attacks, and more) with 70% of those leading to a secondary attack on your network. These forms of email attacks are becoming increasingly personalised in order to appear genuine to the end user, and it takes just one compromised email to bring down your entir network.

With a growing number of employees preferring to work from home or remotely, or by using their own devices (laptops, tablets, smartphones and other smart devices), companies need to have a firm grasp of the endpoints that are accessing their network and data. They need to carefully control user management, ensure these devices are secured, as well as ha an understanding of which users have permission to access and modify what data. Your security should be able to detect and take immediate action if an employee tries to connect an infected device to your network.

Backup and business continuity

Despite all these precautions, security as a whole is still not foolproof. If any of these defences mentioned above are compromised, and you don't have a proper backup system in place, you will not be able to restore your business in a timeous manner and risk suffering from further damage to your brand and reputation.

Your business could even end up being held liable if it was found that it did not have the proper systems and procedures i place to store, manage and safeguard customer information and other personal data.

Apart from properly maintaining their security infrastructure and software, businesses need to ensure their security policie are still valid, as these need to be continually updated to match the evolving threat landscape. You cannot comprehensively mitigate today's cybersecurity problems with policies from five years ago.

Skills, education and awareness

To do all of this, however, you need to have the right skills in place if you are to secure your network and data, and this is challenge facing many South African companies. While larger organisations can prioritise security at the C-Suite level an have internal IT staff to maintain network and data security, and ensure that security policies are crafted and adhered to, smaller businesses do not have this luxury - and this is where a managed service provider (MSP) becomes vital.

The right MSP can manage and maintain your security infrastructure, ensure policies are up to date and being adhered to and that best practices are being applied across the organisation. They should be able to alert you to developing situations provide a comprehensive report and review of the attempted/successful breach, and put in place measures to remediate th fault.

Lastly, however, it is important for companies to remember that while they can spend millions on network and data security products and solutions, a human employee that does not understand the security posture or culture of an organisation remains the biggest risk, as all it takes is a click on the wrong link. They need to be continually educated and brought into

fold to be part of your security defence measures.

ABOUT THE AUTHOR

Mayleen Bywater, senior product manager for cloud security solutions at Vox