Practices for financial services sector to protect itself against DDoS attacks

South Africa's financial services sector is widely acknowledged to be both sophisticated and sound, backed by technology as well as a solid regulatory and legal framework. It offers insurance and investment opportunities; commercial, retail and merchant banking; and mortgage lending, while the Johannesburg Stock Exchange is within the top 20 largest exchanges in the world.

Bryan Hamman, territory manager for sub-Saharan Africa at Netscout Arbor

You could say that South Africa's financial services sector remains by and large a feel-good story says Bryan Hamman, territory manager for sub-Saharan Africa at Netscout Arbor, which specialises in advanced distributed denial of service (DDoS) protection solutions.

"However, there is no room for complacency in today's world of growing cybercrime reports. We only have to look at data from the United States to see that in 2017, it saw a 48% increase in general cybersecurity incidents recorded, with 8.5% of these involving the financial services sector, and impacting on organisations such as banks and other organisations offering credit.

"Financial services firms in the US were reportedly hit by cyber attacks 300 times more often than businesses in other sectors. It is clear therefore that the South African financial services sector needs to be on its guard too. It is well-known that the scale and sophistication of DDoS attacks is on the rise, with the aim of taking websites offline by overwhelming the infrastructure with massive traffic flows. Financial institutions must have the appropriate security measures in place to mitigate these attacks, which threaten loss of revenue and damage to a company's reputation and brand."

Practices to protect against DDoS attacks

To assist firms with their DDoS defences, Hamman says that Netscout Arbor proposes three key practices:

Focus on business risk: The arrival of the General Data Protection Regulation (GDPR) in the European Union, and the pending implementation of the Protection of Personal Information Act (POPIA) in South Africa, reminds us that IT security has legal requirements for organisations to be able to prove that they are doing enough to protect their data.

Defend against the most sophisticated threats: DDoS protection is required against both volumetric and application layer attacks. By deploying your own layered defences, traffic can be constantly monitored and threats detected in as little as one second (and blocked inside 41) – all without interrupting normal network services.

Explains Hamman, “DDoS threat capabilities have become more complex, frequently using multi-vector tactics that strike your organisation in different ways. Cyber attackers are banking on the fact that if they use a combination of attack methodologies, this will increase their chances of breaching the targeted organisation’s defences. Therefore, in turn, companies must layer their defences against all types of attack vector.”

Be prepared: NETSCOUT Arbor offers a risk methodology called FAIR (Factor Analysis of Information Risk), which outlines steps that allow your business to take a quantitative, financial approach to analysing the risks of DDoS attacks.

“While no company can expect to be 100% secure all of the time,” says Hamman, “an organisation must focus attention on a response plan that offers different defensive options to different cyberattack scenarios. Using the FAIR processes can help a business to assess its own risk of a modern-day DDoS attack.

“Trust is an intrinsic part of any business, but arguably never more so than when clients’ money and financial assets and protective measures are the crux of the business. Reputation is especially critical to brand health in the financial services sector. The financial services sector is well advised to look beyond compliance and focus on maintaining service availability,” concludes Hamman.