BIZCOMMUNITY

Is your network ready for GDPR and PoPI?

By Bryan Hamman

7 Jun 2018

Over recent years, distributed denial of service (DDoS) attacks have become one of the biggest cyber-security headaches for CIOs and CSOs. Each year, these attacks grow in numbers, becoming bigger and more damaging.

Image credit: Jonathan Schöps via 123RF.com.

Previously, the primary DDoS fears were the business disruption and reputational damage that they caused. DDoS attackers harness the power of thousands (sometimes even millions) of devices – each'hijacked' with malicious software – to flood the servers of their targets and bring down their online systems.

But now, the introduction of new legislation is raising the stakes even further, propelling the issue of DDoS attacks to the top of boardroom agendas. The European Union's General Data Protection Regulation (GDPR) came into force on 25 May, likely to be followed soon by the enforcement of South Africa's equivalent to this legislation, the Protection of Personal Information (PoPI) Act.

Both sets of legislation aim to protect consumers' personal information, imposing rigorous laws on how organisations gather and use personal data, increasing levels of transparency, giving individuals greater control over how their data is used, and ensuring mandatory disclosure of any breaches.

Specific reference to DDoS

The new PoPI Act draws heavily on the intent and construct of Europe's GDPR. As our local legislation evolves and formalises, it's instructive for local firms to look at GDPR as the benchmark to achieve international compliance standards. Most legal opinion suggests that if an organisation is in full compliance with GDPR, then it will automatically ensure compliance with PoPI.

Under the new GDPR legislation, organisations that operate in Europe or do any business with European citizens must take stringent measures to protect the availability of their network and secure the data that it carries, among many other compliance considerations.

While most of the GDPR headlines tend to highlight the crippling fines that companies could face (up to 20 million euros or four percent of annual turnover) if they are found in violation, one of the less-understood provisions relates to network availability.

In fact, article 32 of the regulations specifically refers to 'the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services' and the 'ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.'

In recital 49, the regulations go on to specifically refer to denial of service attacks, which I believe shows the importance of organisations protecting themselves from this type of attack, as part of an orchestrated end-to-end security strategy.

Though DDoS attacks have been on the rise, their explicit reference in GDPR illustrates how important they have become to security professionals and regulators alike. The network is the lifeblood of the modern organisation, and any threats are treated extremely seriously by lawmakers.

Here to stay

Staying in-line with new legislation while combating increasingly sophisticated DDoS attacks is a tough ask for security pros. Modern DDoS attacks have evolved a long way from their origins, now often interlacing volumetric, TCP state exhaustion and application layer attack vectors.

This type of complex attack renders standard defences - like firewalls, WAFs, load balancers, and IPS/IDSs – almost completely useless against DDoS onslaughts.

Companies must place a concerted focus specifically on DDoS, with layered, intelligently automated protection strategies that harness the latest technologies to provide instant warning of any new attacks.

I highlighted four key pillars to Arbor's DDoS defence approach:

- Arbor Cloud and 24/7 Security Operations Centre… detects and mitigates volumetric attacks upstream before hitting the organisation.
- Arbor APS… which stops so-called 'low and slow' application layer attacks dead in their tracks.
- Arbor Cloud Signaling… which intelligently routes traffic to secure clouds (preventing on-premise infrastructure protection from being overwhelmed).
- Arbor Atlas Intelligence Feed… which sends continual alerts to security teams to inform them of developing threats and trends.

The reality is that DDoS attacks are here to stay, and there is no 'silver bullet' that can eradicate the industry of this scourge, once and for all. Anyone with an internet connection, some cash to burn, and a grudge to bear, can theoretically launch an attack against your organisation.

In fact, considering the new regulation's emphasis on network protection, hackers may well intensify their DDoS efforts, in

an effort to cause even more chaos and damage to their victims, which are now liable for hefty regulatory fines.

For more information about Arbor in Africa, please contact me at bhamman@arbor.net.

ABOUT BRYAN HAMMAN

Bryan Hamman is a territory manager for sub-Saharan Africa at Arbor Networks.
- Is your network ready for GDPR and PoPI? - 7 Jun 2018

View my profile and articles...