The top 5 myths of DDoS protection

Buying in to outdated beliefs and pure myth around DDoS protection is a gamble, says Arbor Networks.

By Bryan Hamman, Territory manager of Arbor Networks

Distributed denial of service (DDoS) attacks have evolved to become a lot more sinister than they once were. Yet too many organisations are pinning their defence hopes on outdated and ineffective
solutions, or even gambling by having no defences at all. These risky approaches are based on the top myths in organisations today, around DDoS attacks:

#1 Content Delivery Networks (CDNs) are the panacea

A CDN merely addresses the symptoms of a DDoS attack by absorbing these large volumes of data. But it still allows all the information into and through the network. When relying on CDNs for DDoS protection, it is important to ensure enough bandwidth is available to absorb the high-volume traffic. Also, many organisations will select specific objects and Web pages to utilize the CDN, particularly those with high hit rates. But what if a DDoS attack injected a request for a different page number that is not utilizing the CDN? In these instances, the attack bypasses the CDN and goes directly to the organisation. It is also important to note that DDoS attacks are not always volumetric-based. In many instances, they are part of an advanced threat designed to distract the organization so that a more nefarious and less obvious intrusion can occur. DDoS attacks are also used for application-layer attacks that flood the pipe to an application, thereby blocking access. With application-layer attacks, the volume of attack traffic may be low enough to go unsuspected. Many such applications that can be used for an attack do not utilize a CDN because the cost does not support the average volume of utilization. In these instances, the CDN offers zero protection.

#2 Meet the attack at the security perimeter

Traditional perimeter security solutions such as firewalls and intrusion detection/prevention solutions (IDS/IPS) still have an important role as part of an integrated and multi-layered security posture. These solutions provide stateful inspection and dynamic traffic filtering of network connections, which result in latency. But by increasing latency, IDS/IPS solutions make networks vulnerable to DDoS attacks. Utilizing these solutions to inspect DDoS attack traffic further increases the latency and creates a bigger bottleneck for network traffic. To make it more complex, DDoS attacks can often consume the connection state tables in these perimeter devices, causing them to be bypassed and offer no protection from the DDoS attack. Attackers understand that state tables can be quickly overwhelmed, and often make traditional perimeter security devices the first targets of a DDoS attack.

#3 Risk denial

Just because it hasn't happened yet does not mean it will never happen. Carrying out a DDoS attack is easy and the price for launching such an attack is in the tens of dollars, while the losses for enterprises can be in the tens of millions of dollars. So you have to ask yourself, "Do I feel lucky?"

Organisations need to consider the consequences associated with a DDoS attack, and evaluate a variety of DDoS solutions and establish a plan of action on how to mitigate attacks. Each DDoS attack is unique. It can have many different faces and many different purposes (such as hacktivism or ransom). How each business addresses DDoS in its network environment is also unique. Is a network operations-based solution the way to go? Or is a security operations-based managed solution the answer? Regardless of who owns the solution, availability is the common concern. DDoS means downtime—which can mean lost revenue, angry customers and a tarnished brand.

#4 The service provider will handle it

Most service providers do in fact offer DDoS scrubbing and mitigation services. But how clearly defined are their services in the areas of support and availability? Some providers can deal effectively with DDoS attacks, and many of those have special

programs available to customers. But it is important that companies fully understand the scope and cost of such protection. Other providers simply “black hole” customers who are being attacked as a defence mechanism to protect their other customers. In either case, it is important to understand the contracts you have with all providers, particularly as they relate to DDoS attacks and engage with providers when building a DDoS response plan.

#5 It’s All about big attacks

DDoS attacks were initially about flooding the bandwidth of a network with high-volume traffic. While these large-scale attacks are devastating, some of the newer application-layer based attacks are harder to recover from because they corrupt or seriously damage a critical application and its processes. What’s more, they may go unnoticed because the overall bandwidth they consume is small. Every one of these application-layer attacks is different and potentially crippling. As a result, it is critical that you take a look at the applications you use and develop a plan to not only defend, but also recover them.

DDoS today has morphed from an annoyance to a real threat, and underestimating the possible damage to the organisation can prove to be a costly mistake.