DDoS: Digital attacks
Understanding the facts

9 myths about DDoS

Myth 1: My industry is not a target

While some industries are more prone to attacks, any industry can be a target. The ease of access and low cost of initiating attacks makes it easy for hackers to launch an attack against any business or individual, in any industry.

Myth 2: My DDoS protection device is good enough

These devices can provide protection; however, they have capacity limits. DDoS attacks are growing significantly in size and can quickly overwhelm a device, leaving your infrastructure exposed.

Myth 3: I can just get more bandwidth

The increasing number of attacks, the exponential growth in the size of attacks and the commoditization of attack tools, mean that attacks can be easily initiated and can overload any system. Provisioning more bandwidth will have very limited impact as new attacks will quickly consume all available resources. According to third-party research, Internet pipe saturation is the point of failure that causes 36% of downtime from DDoS attacks.

Myth 4: I can just get more IP addresses

When a device connects to a network, its new IP address becomes known in minutes. Switching to a new IP address will only provide short term relief until the new IP address is detected. If attacks are aimed at a domain, then changing the IP address will have no effect.

Myth 5: My firewall provides enough protection

Firewalls cannot protect against a DDoS attack as attackers can use methods that leverage messaging or ports designed for legitimate uses. As identified by third-party research, devices such as firewalls and IDS/IPS are the points of failure, causing 31% of downtime from DDoS attacks.

Myth 6: DDoS attacks are only volumetric

While the number of volumetric network layer attacks are higher, the number of application layer attacks are also on the rise. Multi-vector attacks are becoming more common; these combine high volume network layer attacks with sophisticated application layer attacks.

Myth 7: DDoS attacks will only impact my website

Any part of your infrastructure that faces the Internet can be impacted: supply chain, point of sale, transaction processing, patient records and customer service, to name a few. All external facing systems need to be protected no matter where they are managed. Access to your online systems can even be blocked if your domain name servers (DNS) are attacked.

Myth 8: DDoS solutions are not worth the investment

According to a recent study, the average data centre system downtime due to a DDoS attack is 9 hours, with an average cost of $350,000. A Bell-commissioned study showed that 60% of attacks cost between $10,000 and $1,000,000. With the growing number of attacks and the increase in their size, the impacts are set to only get larger.

Myth 9: My organization is too small – we will not get attacked

DDoS attacks can hit any business. One of the largest attacks ever seen was against an individual. With the emergence of DDoS for ransom (RDoS), smaller companies become easier targets as they have limited IT resources to deal with these attacks.

If you require further information about DDoS or to find out more about our security solutions please visit bell.ca/securitysolutions.

Bell