NINE MYTHS ABOUT DDoS PROTECTION

Akamai

The trajectory of DDoS attacks is clear: yearly increases in total DDoS attacks, an ever-growing number of attack vectors, and billions of potentially exploitable devices as the Internet of Things expands the attack surface. Mega attacks keep growing, too. In early 2018, the industry saw a 1.35 Tbps DDoS attack hit an organization – the largest record attack of its kind ever recorded. Organizations are looking for better protection to prevent lost productivity, lost revenue, and damage to their reputations that DDoS-related downtime can cause.

There are a lot of myths about DDoS protection floating around — some of them are even encouraged by security vendors. Any one of them could lead to a vulnerable DDoS defense strategy. Make sure you don't fall for these:

MYTH 1

TOTAL CAPACITY INDICATES AVAILABLE CAPACITY

A simple capacity number leaves out important details. For example, a multi-tenant Content Delivery Network (CDN) may advertise more than 1 Tbps capacity. Yet up to 90% of that capacity may already be consumed by legitimate traffic. With only 100 Gbps left, that CDN is not sufficient to withstand one of the 100+ Gbps mega attacks. What's more, in many cases, a network's capacity is geographically distributed among data centers, so available Gbps is further divided. If, for example, the network has 10 data centers, one center might have 10 Gbps — not enough to absorb even an average DDoS attack. While DDoS scrubbing centers typically have more available capacity, geographic distribution still matters. The number of scrubbing centers in a particular region could have a big impact on latency during an attack.

Dig into the details of capacity when comparing vendors: total capacity, available capacity, geographic distribution of capacity.

MYTH 2

TIME-TO-MITIGATE IS A UNIVERSAL MEASUREMENT

A reasonable definition of time-to-mitigate is the time between the point at which a DDoS attack is identified and the point at which the attack is actually mitigated. However, it turns out that there's a lot of room for interpretation. Be sure to carefully read the fine print for your vendor's service level agreement (SLA). For example, one vendor might not consider a surge in traffic as a DDoS attack until it has lasted five minutes or more. So, the SLA timer may not start until you're already five minutes into the attack. That means an advertised 10-second time-to-mitigate could really be five minutes or more. Another vendor may define time-to-mitigate as the time required to deploy a mitigation control. But security is often an iterative process, and the first attempt may not mitigate the attack. What you care about is how long it takes to get your applications back up and running. If a vendor's SLA doesn't align to what matters to you, then consider alternatives.

Find out all the elements of the time-to-mitigate listed in a service level agreement: recognizing, responding, mitigating.

MYTH 3

BLACKHOLING MITIGATES A DDoS ATTACK

Blackholing is a common response from some DDoS mitigation providers to a DDoS attack. If a site is under attack and putting other customers at risk, the provider may try to prevent collateral damage by dumping that site's traffic in a virtual black hole. Does that really help you? From an attacker's perspective, blackholing means mission accomplished: The target site is effectively offline. Depending on the provider's infrastructure, other customers may end up going offline as well. Instead of mitigation, blackholing could lead to a malicious actor's best-case scenario.

Ask your provider how often they blackhole traffic to a customer site, what steps they take prior to blackholing, and what criteria you'll have to meet to get your service back.

MYTH 4

IT DOESN'T MATTER WHO SHARES THE CLOUD PLATFORM

Every organization needs security. Controversial businesses that attract frequent attacks, such as gambling and porn websites, need security providers, too. Even websites promoting criminal activity and web attacks have purchased cybersecurity from cloud vendors. It's easy to think that it doesn't matter to you. However, if your business shares a cloud security platform with an illegal or frequently attacked enterprise, the potential for collateral damage is high. The vendor's resources may already be tied up or overwhelmed, leaving you exposed.

Read a cloud security vendor's acceptable use policy carefully to confirm that you won't be sharing security with a high-risk target,

MYTH 5

A RUNBOOK WILL KEEP YOUR ORGANIZATION PREPARED FOR ATTACKS

Every organization protecting themselves against DDoS attacks should have a runbook. Essentially a playbook for DDoS response, the runbook can spell out roles and responsibilities, collect important contact information, and specify the escalation path for attacks not quickly mitigated. Even organizations with automatically triggered DDoS protection will need a protocol for zero-day attacks. A runbook can also provide crucial guidance for both internal communications and public relations. However, the book will have little value if only a handful of staff are familiar with its contents. A runbook will not keep an organization prepared unless its specified protocols are practiced, reviewed, and updated regularly.

Build muscle memory by running tabletop drills at least annually to keep the runbook current.

MYTH 6

AN ON-PREMISES SOLUTION GIVES MORE CONTROL

While an on-premises solution allows organizations to turn the knobs and pull the levers themselves, the control can be illusory. The weakest link for any on-premises solution is often the size of the Internet link. As DDoS attacks get bigger and more complex, even a typical attack of less than 4 Gbps can saturate the Internet link and cause denial of service for even those data centers that include the best on-premises hardware. In addition, control requires having the expertise to exercise it properly. In-house IT staff will likely not see as many attacks, or the latest types of attacks, compared to experienced security operations center (SOC) staff for a managed service provider. Without hands-on experience, hard-won DDoS fighting skills can atrophy over time. You can't be in control if your network and staff are overwhelmed.

Consider the increasing size, variety, and complexity of attacks when evaluating defense solutions.

MYTH 7

YOU DON'T NEED MULTIPLE LAYERS OF DEFENSE

Most organizations don't actually believe this, but sometimes they build their defense strategy as if it were true. For example, consider the hybrid approach. An organization looking to bolster its on-premises security solution may upgrade by adding a cloud-based solution from the same vendor. Having one throat to choke may be convenient, but that doesn't necessarily provide defense in depth. If multiple layers of defense are built on the same underlying technology, those layers will have the same gaps and weaknesses, leaving you just as exposed.

Layer best-of-breed technologies with different strengths and weaknesses, so gaps in one layer will be covered by defense in another.

MYTH 8

EVERY 24/7 SOC OFFERS THE SAME LEVEL OF SERVICE

Many vendors advertise a 24/7 security operations center (SOC) on their data sheets. But having a 24/7 SOC isn't what matters. What's important is the level of service you can expect to get when you come under attack. For example, it might sound reasonable for a vendor to have five analysts in its SOC. But if you do that math, 24/7 typically equates to four overlapping shifts. With one person to cover sick days or vacations, that could result in only one person in the SOC at any point in time. This could be a concern if you come under attack at the same time as another customer. Also, consider the level of expertise of the SOC staff, such as how many attacks they mitigate on a daily, weekly, or monthly basis, as well as their processes to institutionalize learning across the organization.

Evaluate the expected quality of service from the SOC based on quantifiable metrics.

MYTH 9

DDoS PROTECTION IS ALL-INCLUSIVE

While a lower price may seem attractive, there could be hidden costs. Some vendors offer a low price but restrict the number or size of attacks that they'll mitigate. If you are targeted with too many attacks, or too large an attack, they will ask you to upgrade to a higher (and more costly) tier of service before stopping the attack — all while you're trying to get your business back online. When comparing vendors and prices, make sure you understand the tradeoffs and their impact on your risk posture.

Understand what's included in the price you're quoted before you sign.

DDoS security is complex, time-consuming, and ever-changing. Staying connected to your clients, customers, and employees is the basis of your business. There's no room for error here — and there's no need to bear the high cost of trying to go it alone. As the largest, most trusted cloud delivery platform for web security, Akamai can help.

Learn more at **www.akamai.com/cloud-security**.