AKAMAI WHITE PAPER

Making DDoS Mitigation Part of Your Incident Response Plan: Critical Steps and Best Practices

Akamai
FASTER FORWARD

Introduction

Like a new virulent strain of flu, the impact of a distributed denial of service (DDoS) attack is very easy to see – you always know when your applications are down. However, obtaining a firm diagnosis quickly is often difficult and panic usually prevails until experts finally uncover the cause and develop a cure.

Many organizations with Internet-facing networks have experienced this panic during a DDoS attack as IT teams scramble to keep websites and applications available in the face of malicious actors and multiple attack vectors. As the attackers target different network vulnerabilities, IT continues to triage the situation and figure out why network anomalies are occurring. Why are routers passing traffic when load balancers are freezing up? Why is the web server responding, but the database is not? Different people within the organization are placing calls to the Internet Service Provider (ISP) or application vendors for help, but no one really knows whom to call first and what questions to ask. Although a DDoS attack is yet to be confirmed and no obvious fix is apparent, senior managers want a definite answer as to why application services and network operations are being severely impacted and when business as usual will resume. And that's when panic really sets in.

When a DDoS attack cripples or brings down a website or other Internet-facing application, knowing whom to call first and how to marshal the required resources for mitigation can make the difference between organization-wide panic and a calm, orderly response. Most importantly, planning ahead makes the difference between fast and effective DDoS mitigation and extended downtime that can drain thousands of dollars of revenue per hour, not to mention loss of customer, partner and investor confidence.

These days, businesses of all sizes need to be concerned about cyber attacks. As *Akamai's State of the Internet* reports highlight, the attack size and frequency have continued to rise. What's more, the DDoS underground has made it easier for anyone – even without technical skills – to launch a damaging DDoS attack against any website or other Internet-facing application. These attack-for-hire services have commoditized DDoS to the degree that an attacker does not even need to probe or understand the target's vulnerabilities beforehand. Instead, the malicious actor simply goes to the DDoS underworld to leverage DDoS as a Service platforms on booter and stresser sites, which anyone can easily find on the Internet – all for a surprisingly low price. Consequently, Akamai believes that being prepared is the best defense, and that clear, organized communication with all stakeholders in the DDoS mitigation process is the key to fast, successful attack mitigation.

Add DDoS mitigation to your incident response plan

Many companies have incorporated DDoS mitigation as part of their disaster recovery plan. However, disaster implies that something unexpected or accidental threatens business continuity. DDoS attacks are deliberate, targeted events occurring on a daily basis. As such, a preparedness plan is essential. Having developed and tested a viable incident response in advance, it is possible to respond quickly and calmly to any attack and minimize any potential operational and financial damage.

Developing a DDoS mitigation playbook

After you have developed a robust plan for DDoS mitigation, put it down in writing. A DDoS mitigation playbook – similar to a sports playbook that outlines defensive moves based on past winning games – can be essential to a controlled, streamlined response to a DDoS attack.

Organizations work with their DDoS mitigation service provider to create a simulated DDoS attack or "dry run" that makes no actual changes to the network, but will help management see the best way to manage both internal and external communications when confronted with a DDoS attack. The incident response team works through a real-world DDoS attack without doing an actual live test, much like a military training drill in which no live ammunition is used. Depending on the size and complexity of the organization, this type of dress rehearsal exercise can be completed in a little over an hour, or slightly longer if the company's incident response plan has additional requirements. Executive management will understand how long it takes to put the mitigation plan in action. Following this exercise, optimizations may be developed to ensure a rapid, repeatable and predictable action plan.

A DDoS mitigation playbook must include policies and procedures for:

- **Managing communications –** DDoS attacks have an impact not just on IT, but on all users of an organization's services, including non-technical departments. Staff needs to know whom to call and what to do when issues arise during a DDoS attack without disrupting daily business. Akamai advises incident response teams to have a single point of contact for relaying information and short "Twitter-style" updates internally across the organization. These short internal blasts should be confidential and help people understand what is going on during the attack so that they don't panic and create an additional internal crisis.
- **Identifying and contacting key personnel –** The main goal of the playbook is to eliminate organization-wide panic that can delay the mitigation response when a DDoS attack occurs, so it is vitally important that the right people be notified of the attack immediately. Completing a simulation exercise ahead of time ensures everyone in the triage team understands what their role is in the DDoS mitigation process, what changes they need to make to the network, and how they can continue to maintain business-as-usual even when some resources are unavailable.
- **Accessing critical information –** Something as simple as keeping all names and phone numbers of key contacts in a single place can save valuable time. This component of the DDoS mitigation process is all about containment and order – how to turn a DDoS attack from a major disaster into an incident that is routine when handled according to a well-rehearsed play book.

Best practices for building and maintaining a DDoS mitigation plan

Eliminating panic as a result of a DDoS attack is all about what you know – and how well you know – your DDoS mitigation service provider, vendors and mitigation playbook. Akamai recommends these best practices for building and maintaining a DDoS mitigation plan:

Think like a DDoS attacker

Attackers share common behaviors. Typically, they will change attack vectors if they realize that their efforts are beginning to be blocked or they will move on to easier targets if a strong defense is in place. When you think like an attacker, you will start to plan for all possible types of attacks and understand all of the mitigation options at your disposal. Ask yourself: Are all vulnerabilities in the infrastructure protected against attack? If not, make sure any vulnerability is addressed ahead of time.

Don't rely on your ISP

You may have a great relationship with your ISP, but ISPs are generally not known for their flexibility when providing DDoS protection. Ask the tough questions: If your network is hit with 10 Gbps of traffic from a reflection attack, how long will it take for the ISP to block it using an Access Control List (ACL)? More importantly, how large of an attack will the ISP attempt to mitigate before it decides to black hole all traffic to your applications upstream? The bottom line is that if an attack on your site puts all of the ISP's customers at risk, the ISP will black hole your traffic – and your site will be down indefinitely. Again, having a DDoS mitigation solution in place from a proven service provider is always the best defense against cyber threats.

Don't overestimate your infrastructure capabilities

Your current edge network hardware may serve you well during "peacetime," but may easily fail during a DDoS attack because the network edge has been under-resourced. Determine and ensure that infrastructure has sufficient balance with overhead – headroom above and beyond what its peak requirements are – and has robust networking hardware that can handle extra traffic if needed. In addition, stay up-to-date on changing DDoS trends and attack sizes – the average size of a DDoS attack was 7 Gbps in early 2015 – and confirm that your infrastructure can still withstand new vectors and rising attack volumes.

Ensure operational readiness

How robust is your organizational response to a DDoS attack and how fast will you be able to respond? The best way to determine operational readiness is through testing and tabletop exercise. A dry-run rehearsal of a simulated attack is an ideal way to validate your mitigation solution and DDoS defense. Once you confirm that all of the processes and procedures for communicating, decision making, and solution execution are firmly in place, you can bring this validated solution to executive management with confidence.

Deploy a DDoS solution before you need it

An emergency DDoS mitigation solution can usually be deployed within an hour or less in typical cases. However, the best way to avoid site and web application downtime in the first place is to have a *DDoS mitigation solution* in place before any attacks occur. As part of your incident response plan, this solution can help give you peace of mind that your network is always protected by your DDoS mitigation provider, who will be prepared to defend your Internet-facing network and web applications.

Communicate with your DDoS mitigation service provider

Engage a cyber security services provider and keep communications flowing. Ask plenty of questions. A good service provider will have best practices for infrastructure discovery, so you'll know if you have gaps in security, routing leaks, network vulnerabilities you may have missed, and more. Your provider should explain the different approaches to DDoS protection that meet your specific needs – whether network, application, DNS, or IP protection. Establish this dialog before a DDoS emergency hits and you will be well prepared, not panicked, to defend your network. Akamai's managed services customers are always encouraged to call the *Security Operations Center (SOC)* when they suspect they may be receiving a DDoS attack.

Keep the DDoS mitigation playbook up-to-date

Collaborate with your security services provider to keep your DDoS mitigation playbook consistently up-to-date and current with all key information, such as the communications tree contacts and names of authorized contacts with the service provider. Do this on a regular basis, as well as when staff members change departments or new people come on board, or a new vendor is added or replaced. In addition, consistently review and update information related to your network's infrastructure, website, and web applications. Working with current information translates to a faster, more controlled, and calm response to DDoS.

Maintain tight relationships with your vendors

DDoS attacks require a calm, rehearsed response from everyone involved – especially from your security vendor, hosting provider, ISP, and other third-party application providers. Don't wait until there is a DDoS emergency to start a relationship with your service reps. Build tight relationships now – and incorporate them into your incident response plan – so that they will be ready to calmly respond and know what to do when your emergency call comes in.

Validate. Validate. Validate.

Test and validate your DDoS mitigation solution at least once a year, preferably twice a year, to ensure that the solution is continuing to meet the requirements of your incident response plan. Plus, validation enables quality assurance testing to verify that no systems or applications are being adversely affected while traffic routes over the mitigation infrastructure. This process may also reveal any application or networking issues that can be addressed immediately for optimizing routing in particularly large network infrastructures.

DDoS attack readiness in action

A leading travel/hospitality provider and Akamai customer came under a very large and sophisticated DDoS attack one weekend. Fortunately, Akamai and the travel/hospitality firm had planned ahead and worked together to develop a playbook that became a part of the company's incident response plan and fine-tuned the process. Most importantly, this plan identified the key communications channels within the organization and Akamai, so that everyone was on the same page when Akamai activated the on-demand mitigation service that the company had selected.

After receiving a call from the company at 8 a.m. on Monday morning, technicians at Akamai's Security Operations Center (SOC) joined conference calls that the travel/hospitality customer was having with its Internet provider and telco equipment provider. Akamai technicians also began coordinating with their contacts at the company. At 10:00 a.m., according to the customer's playbook and Akamai protocols, Akamai opened up three teleconference bridges while the customer's ISP was still trying to resolve the attack:

- **A Mitigation Bridge –** primarily for engineers to coordinate and monitor mitigation efforts
- **A Troubleshooting Bridge** – primarily for engineers and application owners to investigate any problems arising during the on-ramping
- **A Security Intelligence Response Team (SIRT) –** primarily for security and forensics participants.

These bridges were "always on," enabling participants to periodically check in and monitor the latest developments and communicate news and changes through the playbook channels. At 11:30 AM it was decided that the attack was too big for the ISP to mitigate and traffic would be routed to Akamai. Because of all the upfront planning and testing, this was a relatively simple and almost instant process. Akamai routed traffic from three of the firm's main data centers to its attack mitigation network or "scrubbing centers" and the attack was mitigated.

Because both the travel/hospitality company and Akamai had developed a controlled and streamlined communications plan or playbook upfront, the company was able to deflect the usual panic that can grip an organization during a DDoS attack, and Akamai was able to mitigate the attack even faster and more efficiently.

Conclusion

"Be prepared" is a classic motto that is certainly relevant for any online business today. Akamai advises IT management to talk to their DDoS mitigation services provider before an attack happens. Ask questions and discuss all of the possible DDoS scenarios that the company could experience. The best defense against malicious cyber threats is preparedness and understanding how to use the vendor's DDoS mitigation services to the best advantage.

Any good mitigation service provider should have the expertise and capacity to serve many clients simultaneously – an important factor to consider as the daily occurrences of DDoS attacks escalate. Akamai has been immersed in this cyber war for more than a decade, and our SOC technicians are routinely mitigating dozens of attacks at the same time. In addition, all of our protocols are designed for rapid response to attacks, and we use the same principles demonstrated in the simulations we complete with our customers. Our protocols and procedures are well defined and are tested on an hourly basis during real DDoS events.

In the end, when everyone in an organization – not just IT staff– understands what it is really like to be under a DDoS attack before one actually occurs, they will be able to face the actual event with more confidence, control and calm. As a result, the DDoS mitigation process will go more smoothly for a faster return to business as usual. That is why Akamai advises all of our customers to prepare themselves for the real thing with a simulated DDoS attack and incorporating DDoS into a broader incident response plan.

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit *www.akamai.com* or *blogs.akamai.com*, and follow *@Akamai* on *Twitter*.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.