NimbusDDOS

ARTICLE :

3 Pillars of DDoS Protection: Part 1 - People

This article is the first of a three part series on the major pillars that form a comprehensive defense against DDoS attacks. Check our blog (https://www.nimbusddos.com/blog.htm) to read parts two and three on Process and Technology.

The pillars of a comprehensive defense against DDoS attacks are People, Process and Technology. Each of these areas supports the other, and when working properly, the whole is greater than the parts. In this article we will provide a high-level overview of the focus areas necessary to create a team capable of defending against a DDoS attack.

1. Staffing Levels : The defined (or implied) service level agreements (SLAs) for business critical applications should dictate the appropriate staffing level of incident response teams. For instance, if SLAs require 99.9% uptime then relying on escalation by voice or text will be insufficient, and a 24x7 SOC is required. The key is to define SLAs first, then develop the team to support it. Additionally, DDoS attacks create a unique staffing problem due to their long duration. DDoS attacks can run for days or even weeks, which can quickly overwhelm smaller incident response teams.

2. Training : People within the organization must be properly trained in their specific area of DDoS attack preparedness. The training will be specific to the role and can extend beyond technology to other aspects of the business. For instance, it's obvious that incident response personnel should be well versed in mitigation processes and technology, but equally important and less obvious is that PR and social media teams should be prepared to handle any fallout from an event. Since DDoS attacks tend to be infrequent, training is also valuable in maintaining a state of readiness.

3. Detection : Despite technology advances, people are often the first step in identifying a DDoS attack. It's important that people know what to look for, and how to initiate further action. This area is primarily the focus of technical teams, but it can extend beyond to customer support teams or other non-technical teams that may receive first-hand reports from customer or vendors of an issue.

4. Forensics : Often forgotten during an incident response is the postmortem analysis of the attack to guide improvement. This analysis is exclusively the realm of People, and the recommendations and guidance that come from this analysis can improve Process and Technology by identifying what worked/failed during the event.

NimbusDDOS

The People within an organization, when leveraged properly, are the most valuable asset to protect against a DDoS attack. The investment in People allows companies to maximize their investment in DDoS defense technology and mitigation platforms. Ultimately this investment results in quicker DDoS attack mitigtion, less downtime, and a better customer experience.

The DDoS preparedness services offered by NimbusDDOS are designed to help organizations strengthen these three pillars (People, Process, and Technology).

DDoS Testing & Simulation : Real-world, legal DDoS attacks (https://www.nimbusddos.com/ddos-testing.htm)

- Allows confirmation of proper staffing levels through wargames
- Identify gaps in team roles and responsibilities
- Identify training gaps
- Provide experience in DDoS attacks

DDoS Preparedness Training : Formal, and self-paced training in all aspects of DDoS preparedness (https://www.nimbusddos.com/ddos-training.htm)

- Deeper understanding of DDoS attacks
- Knowledge drives better forensic analysis
- Knowledge drives better detection

Please check back for parts two and three to learn how Process and Technology support a comprehensive defense.