NimbusDDOS

ARTICLE :

How to Gear Up for Cybersecurity in 2020

It's a new year: a time for reflecting on the past and looking forward to the future. An important area for this reflection is in the cybersecurity preparedness of your company — specifically in the area of distributed denial of service (DDoS) attack strategy.

During a DDoS attack, cybercriminals overwhelm your environment with requests so that your customer's legitimate traffic is blocked. Cybercriminals may use the threat of a DDoS attack to extort money from an organization, or launch an attack to conceal a data theft. While these DDoS attacks can be rare, they can happen to companies of any size, and their results are often catastrophic.

Companies may think they are protected from these threats if they have advanced firewalls. Unfortunately, these defenses are unlikely to protect against DDoS attacks. What's required is a comprehensive cybersecurity plan that integrates the specific nuances required to protect against DDoS attacks. The strategy is built upon the three pillars of DDoS protection, People, Process and Technology.

Below, we provide a step-by-step process to help you assess your DDoS attack strategy from the past year, and how to improve upon it in the coming year.

Looking Back

As you think about the past year, which DDoS protection measures did you implement?

- Have you assessed your environment for risk areas?
  This type of assessment scans your environment to identify DDoS risk areas. The process uncovers the attackers viewpoint, determines weaknesses, and identifies corrective actions customized to your environment.

- Have you tested how your environment and IT team will withstand a real-world DDoS attack?
  The only way to truly understand how your environment and teams will respond during a DDoS attack is to perform a controlled real-world test. This helps identify architectural limits, and flaws in incident response processes.

- Have you consulted DDoS experts?
  DDoS attacks are becoming more prevalent and general service cybersecurity firms do not have the expertise necessary to help you craft and maintain a comprehensive DDoS attack strategy.

- Have you implemented a DDoS attack strategy?
  DDoS attacks are aggressive — and proper defense requires a coordinated incident response process. They necessitate a response from IT and cybersecurity teams, but often overlooked are customer support and public relations teams.

NimbusDDOS

Looking Back (cont.)

- Have you trained your team in DDoS attack response?
  Since your team plays such an integral role in a DDoS attack response, they need to be properly educated about DDoS attacks and their roles and responsibilities during an attack.

- Have you pursued or completed a DDoS attack certification?
  Becoming DDoS attack-certified can help you and your company be assured as a team that you are prepared for DDoS attacks.

Reflect

After reviewing the above measures, answer the following questions:

- In which areas were you successful?
- In which areas would you like to improve?
- For which measures do you need help?

Look Forward

Now that you have an image of your prior preparation for DDoS attacks and identified the areas in which you can improve, it's time to make a plan for the future.

The process of preparing for a DDoS attack may seem involved but having DDoS experts from NimbusDDOS can help make the process straightforward and successful.

As experts with more than 20 years of DDoS attack experience, NimbusDDOS has proven methods that can help you work through the above process. With us, you can assess weaknesses, create a response strategy, train your personnel, test your defenses and have a team of DDoS specialists that help you adapt with evolving threats – and your evolving company.

Stay Successful

Since DDoS attacks and your company are constantly changing, NimbusDDOS focuses not just on technology controls, but on the people and processes that will result in a successful DDoS attack response.

If you would like to start the new year off with preparedness and confidence, contact us for a consultation.