FIVE QUESTIONS TO ASK WHEN CONSIDERING A DDoS MANAGED SERVICE

When evaluating Distributed Denial of Service (DDoS) protection for your business what are the top questions you should be asking from a managed service provider?

Every business will have some unique technical, organizational or financial requirements. But whether an ecommerce website, customer service portal or internal sales support application, availability is critical to the modern enterprise. DDoS explicitly threatens this availability and it is on the rise. Here are some fundamental questions to ask when evaluating a DDoS protection service.

1. What is the DDoS experience of the service provider, specifically the experience of their Security Operations Center (SOC) operators?

When it comes to a managed service the difference between a good and a great service lies not so much in the technology as the individuals that the customer will be working with during an event. You want to know up front what tier of support you will get when you make the call. And SOC personnel should be highly trained in networking, firewalls, security procedures, traffic protocols and emerging DDoS threat vectors.

2. What processes does the service provider have in place?

Process is the next most critical item in evaluating managed service protection. This means more than identifying and understanding the mitigation process itself (more than what steps will be taken to scrub traffic and deliver a 'clean pipe'). For example, the service provider should have a highly developed, documented escalation procedure. This should include which party is responsible for what decisions, and basics like who communicates to whom, when and how. Superior experience could be born out in documented processes for quickly provisioning additional infrastructure, and on-going training of SOC personnel on different types of application traffic, and recognizing and mitigating new DDoS threats.

3. What technology is the SOC personnel supporting?

It is important to know the number of technologies and services the SOC personnel are expected to support. Ask about their event ticketing and case management system; and what type of reporting you can expect. Beyond that SOC personnel supporting multiple vendor technologies and feature sets may not be as proficient explicitly in DDoS mitigation. When the same SOC is also supporting VPNs, a content delivery network (CDN), managed firewalls, even phone systems, they tend to be generalists and not as focused on DDoS. And when it comes to DDoS attack protection technology, make usre they are using industry leading technology (i.e. stateless, able to stop all types of DDoS attacks) and best practices in deployment (i.e. an intelligently automated combination of in-cloud and on-premise protection backed by continuous threat intelligence).

4. What are the terms of service and Service Level Agreements (SLA's)?

A strong set of SLA's will include clear descriptions for what defines an attack, an incident, incident mitigation, and of course related fees. You want to look for numbers around Mean Time to Detect (MTTD) and Mean Time to Resolve (MTTR). The SLA will also define what you are responsible for, such as what procedures you use to re-route traffic to the service provider.

5. Do you understand the service provider's roadmap? How flexible is the managed service provider?

Look at how the managed service provider can align and support your company's goals. For a dynamic business this means more than simply scaling the size of services.

You may be working on applications now that will need protection soon. Ask about how easy it is and what is involved in adding additional applications during a contract period. Make sure that compatibility exists between the capabilities of the service provider and needs of your future projects.

Managed services can offer distinct benefits in terms of less up front financial commitment, and with the right vendor, rapid scaling as needed. But as with any business relationship, it is important to check the financial stability of your service provider. You do not want to revisit this decision a year from now.

There is more than a financial cost to changing services: DDoS protection is 'sticky'. Even though a managed service, changing vendors means adjusting your firewall infrastructure, making all your subnets point to a new provider, new escalation processes and more. What you are looking for is a stabile platform, a partner you can work. So, ask the right questions!

Learn more on NETSCOUT Arbor's industry-leading portfolio of managed DDoS attack protection and services.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECA_003_EN-1802 08/2018