Neustar Offers Webinar on DDoS Attack Mitigation to Review Critical Protection Services

Mar 13, 2015

Neustar, Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services and analytics, is hosting a webinar titled “DDoS Attacks: More Dangerous to You, Never Easier to Launch” with a guest speaker from IDC at 2pm EST, on Wednesday, March 17, 2015. The webinar will explore distributed denial of service (DDoS) attacks, and explain how companies can protect their web presence and assets.

Christina Richmond, program director at IDC and Joe Loveless, product marketing at Neustar, headline the hour-long webinar where they will discuss today’s DDoS threat environment, what your organization can do to thwart DDoS threats, and explain why “smokescreening” poses a particular danger.

For more information about the webinar, visit Neustar.biz.

To protect companies’ web presence, Neustar recommends the following eight features in DDoS protection service:

1. Accurate Attack Detection - Investigate provider reputations for accurately detecting threats. Are their customers chasing non-emergencies and misusing time and manpower? Or are they getting reliable data on real attacks as they happen.

2. Deep Expertise and Experience - You want expertise backed by a solid real-life record. Ask for actual examples, even anonymized ones that protect confidentiality.

3. Ability to Handle Numerous Types of Attacks - DDoS attacks come in more than 31 flavors. For instance, volumetric attacks overwhelm sites, while application-layer attacks strike with surgical precision. With hundreds of attack types to defend against, your service must use diverse DDoS blocking technologies combined with the operational knowledge to recognize and mitigate each threat.

4. Hybrid Protection - Top analysts cite hybrid protection, a combination of hardware and cloud mitigation, as a best practice. Make sure your service lets you respond to attacks immediately and that your provider has the bandwidth to handle attacks upwards of 100 Gbps.

5. Massive Traffic Scrubbing Capacity - Attacks measuring as high as 300 Gbps (or higher) have become all too common. Most of the top protection services are cloud-based, but not all are created equal. Choose a provider with enough bandwidth — close to or exceeding a terabyte— to scrub bad traffic in volume while allowing legitimate requests to proceed to your infrastructure.

6. Fast Routing to Scrubbing Centers and Speedy Failover - Although cloud-based protection involves rerouting traffic through a scrubbing center, which can slow traffic, businesses should insist on a solution that routes and cleans traffic quickly, with minimal latency.

7. Ease of Use and Deployment – Simplicity is one reason why DNS redirection is a popular option. Simply point your traffic to a different address and within minutes, you're protected.

8. Complementary DNS Service – With so many DDoS attacks targeting DNS, having protection that compliments your DNS solution is critical – whether it's managed in-house or via a third party. The most seamless approach is to use the same vendor for your DNS and DDoS.

About Neustar

Neustar, Inc. (NYSE:NSR) is the first real-time provider of cloud-based information services and data analytics, enabling marketing and IT security professionals to promote and protect their businesses. With a commitment to privacy and neutrality, Neustar operates complex data registries and uses its expertise to deliver actionable, data-driven insights that help clients make high-value business decisions in real time, one customer interaction at a time. More information is available at https://www.neustar.biz.