Recent Neustar DDoS Report Reveals Implications for CIOs and CMOs

Apr 22, 2015

One-Third of Respondents Attacked Ten-Plus Times a Year; Customer Support, Brand Trust and Loyalty Biggest Casualties in DDoS Attack

Neustar, Inc. (NYSE: NSR), a trusted, neutral provider of real-time information services and analytics, discussed additional findings from its 2015 North American Denial of Service (DDoS) Attacks & Impact Report. The study, which interviewed 510 North American companies with nearly one-third earning more than $1 billion in annual revenue, reveals the widespread brand damage that a successful DDoS attack leaves in its wake.

Key findings:

- 33 percent of companies say customer support is most adversely affected by a DDoS attack
- 30 percent of respondents are attacked more than 10 times per year
- 26 percent report DDoS attacks adversely affect customer trust and brand reputation

“Security is no longer an IT – only issue,” said Lisa Joy Rosner, chief marketing officer at Neustar. “A data breach can immediately and negatively impact a brand; resulting in bad publicity and eroded customer trust and loyalty. CMO’s work for years to build a brand and we have all seen that work undone as a result of attacks.”

According to a Forrester Research report commissioned by Neustar, in 2012, 2.4 billion people used the Internet. In 2017, that number is expected to grow to 3.5 billion – or almost half of the world’s population. As people continue to connect online with brands and share sensitive personal and billing information, it will become a mandate for the CMO and the CIO to collaborate and foster consumer trust.

“When a customer visits a website, they expect an experience that is both responsive and secure,” said Margee Abrams, CISSP, director of security services at Neustar. “A security breach or website that’s inaccessible or sluggish as a result of a DDoS attack can have a devastating effect on consumer trust and equity that the brand spent time and treasure to once establish.”

To combat DDoS attacks, Abrams recommends using hybrid protection in addition to traditional firewalls and routers.

Hybrid protection, a highly recommended approach that allows companies to mitigate DDoS attacks by combining on-site hardware and cloud-based solutions, has increased by 20 percent internationally as companies bolster their defenses against DDoS attacks.

“The increased hybrid adoption reflects the growing need for companies to have immediate, on-premises DDoS defense capabilities along with the capacity to surge defenses in response to larger attacks,” said Abrams. “Companies continue to rely on layered traditional perimeter defenses including firewalls, routers and switches as well as DDoS mitigation services. But when revenues and brand reputation are at risk, deploying a hybrid solution offers the best of both worlds: immediate on-premises protection with the capacity that only cloud providers can offer.” she added.

About Neustar, Inc.

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.