DAY 2

THE 2016

INCOMPAS SHOW

APRIL 10-13, 2016 | WASHINGTON DC

SHOW DAILY

BEKA Business Media

DDoS Attacks Increase; NTT Com Prevails

Cyber security remains in the headlines with world leaders. They and network engineers are talking about the hazards, the risks and are searching for remedies.

A recent report by provider Akamai found an increase in total distributed denial of service (DDoS) attacks of 149 percent in the fourth quarter of 2015 compared with the same period in 2014. The study also said the average DDoS attack lasted nearly 15 hours.

That means 15 hours during which customers can't shop online, pay their bills or check email.

One of the most common types of online threats, a DDoS attack is an attempt to make a network resource unavailable by interrupting or suspending services of a host connected to the Internet. These attacks can strike at any time, potentially crippling network infrastructure and severely degrading user experience.

Depending on the type and severity of the attack the impact might result in network damages, decreased productivity and irreparable harm to a company's brand.

Any organization with an online presence is a potential target for a DDoS attack, and yet many organizations have inadequate security strategies in place for defending against such a threat.

Early DDoS attacks were focused primarily on flooding network resources with unwanted traffic so that legitimate traffic would be unable to reach the intended target. More recently, application layer attacks designed to compromise a specific service on a host have become more prevalent.

Because application layer attack traffic looks similar to legitimate traffic, traditional security measures, such as filtering, firewalls and IPS/IDS are not sufficient defenses.

In addition, attackers are learning from the defending countermeasures being used and adjusting their attacks towards other targets and vulnerabilities.

The motivations of attackers can range from social and political protests to financial extortion with the intent to disrupt governments, organizations or businesses and cause financial or reputational harm.

In many cases DDoS attacks are the cover for other crimes, such as property, fund or data thefts. Websites dedicated to reporting abuses or censorship often become targets of DDoS attacks as well.

Internet-centric businesses, online retailers and e-commerce websites are especially vulnerable even if they have some DDoS mitigation tools in place. However, insufficient budget resources, shortage of qualified personnel and lack of C-level support are still critical barriers to preventing and mitigating attacks, a report from the Ponemon Institute found.

There is no single defense strategy to defend against today's sophisticated and evolving DDoS threat landscape. Instead, a layered defense approach is recommended that combines traditional security measures, vast availability of bandwidth, intelligent DDoS mitigation systems and sound risk management strategies.

Recognizing the ongoing and increasing threats from DDoS attacks, NTT Com has deployed technologies to help mitigate these threats. Built on industry-leading DDoS protection platforms, NTT Com's global Tier-1 IP network and around-the-clock expert monitoring services, the company's DDoS Protection Service allows for fast and effective actions to minimize the impact of a DDoS attack.

When notified of a possible attack, NTT Com's expert Network Security Team analyzes key network data to confirm whether an attack is in progress, and then rapidly re-directs incoming traffic through the mitigation platform.

The DDoS Protection Service platform is built on best-of-breed technology, which removes attack traffic and passes legitimate "clean" traffic onto a network, allowing businesses to stay online and function during the attack.

NTT Com offers the technology, experience and flexibility that communications service providers, CLECs, ISPs, network operators and Internet-centric businesses need to design and implement a comprehensive and successful DDoS defense strategy. ❑

For more information about NTT Com and its DDoS attack protection, go to www.us.ntt.net.

ANPI Opens UCaaS Solution to VARs and MSPs

ANPI, a provider of unified communications as a service (UCaaS) solutions, announced it will offer its award-winning UCaaS solution to VARs and MSPs for private label.

With the private label solution, ANPI provides all the advanced features, tools and collateral so a provider can market, sell and deliver an innovative, custom-branded UCaaS solution.

The fully-integrated solution includes hosted IP PBX functionality with unified messaging, presence, multimedia collaboration and seamlessly integrated mobility supported by a carrier-grade network and enablement resources that allows partners to be selling in 90 days.

ANPI has enabled more than 100 ILECs to sell their own branded solution.

"The UCaaS market is a multi-billion dollar marketplace with a tremendous growth profile, and with ANPI's unfolding suite of UCaaS solutions, we are well positioned to realize the opportunities in this growing and vibrant marketplace," said Mike Cromwell, ANPI CSO/CMO.

ANPI can enable a partner to be up and running with its own branded offering in less than 90 days.

The most unique aspect of ANPI's offering is its "build-to-bill" order and customer management platform. The software platform, known as Atlas, consolidates order management, fulfillment, provisioning and customer care of the solution into a single platform, giving providers complete control and a personalized process management experience.

ANPI has invested more than $24 million into the UCaaS solution and built it on top of a carrier-grade voice network that transports billions of minutes per year.

The UCaaS solution was purpose-built from the ground up to enable ANPI partners the ability to own the customer experience from proposal through implementation.

ANPI offers a private label hosted unified communications solution for carriers and as direct connections, wholesale long distance, peering, tandem access and SS7 solutions.

Based in Springfield, Ill., ANPI began serving rural telecom companies in 1996, and today serves the voice and data needs of nearly 800 ILECs, CLECs, IXCs and regional wireless carriers, as well as more than a thousand business customers throughout the United States.

ANPI also owns and operates a nationwide IP network with switching and/or PoP facilities in Atlanta, Chicago, Dallas, Los Angeles, Las Vegas, and New York City, and monitors all activity around-the-clock in its own network operations center. ❑

For more information, go to www.anpi.com or call 877-366-2674.