Cybersecurity Essentials for 2017

For cybersecurity professionals, 2016 presented a year of distributed denial of service (DDoS) attacks that were unprecedented. Week after week, the public was inundated with news of hacks, attacks, and data leaks. It didn’t take long for everybody to realize the old axiom of cybersecurity still holds true – there are two types of companies: those who are hacked and know about it, and those who are hacked and soon will find out.

As a key player in the war against DDoS attacks, Neustar has been on the front line, detecting, alerting, and mitigating strikes to keep companies and their customers safe.

THREE KEY INSIGHTS TO HELP YOU PREPARE FOR 2017

1. Mirai Was Just the Beginning
   The Mirai code has already morphed from its initial incarnation, producing new strains and code variants that will increase attack size, complexity, and ferocity in 2017. Mirai type of attacks, those that reconnoiter and test credentials as part of an effort to compromise and enroll devices in botnet arsenals, will significantly shape DDoS attack strategies and experiences. As defenses continue to adapt and mitigate Mirai-based attacks, there will be a substantial ebb and flow attackers and defenders work to one-up each other.

2. Conventional DDoS Attacks Continue to Pose a Significant Threat
   Multi-vector strikes will continue to become more prevalent as attackers demonstrate a trend of using botnets and techniques to better test and exercise their arsenals. From January 1 through November of this year, 48% of the identified attacks that Neustar mitigated used multiple vectors. As the world focuses on Mirai, the quiet, targeted attacks will remain constant, steady, and dangerous.

3. New Threats Will Be Realized in 2017
   The ubiquity of the Internet of Things (IoT) devices – and their exploitation – will continue to pose a formidable threat next year. IoT devices, coupled with the effectiveness of ransomware, phishing, and malware will most likely reveal inroads to create lucrative chaos in organizations. As a consequence, 2017 will produce unlimited opportunity and the potential for bad actors to achieve objectives that include theft, disruption, extortion, and impact.

Cyber attackers reaped significant returns on their investment in 2016, and there is no reason to expect them to change next year. The foreseeable road ahead offering a toxic combination of uncertainty, greed, events and technologies to exploit, will compel organizations to take more decisive action.
If Attacked, How Would Your Board Respond?

A strong and well-defended network can be the driving force behind your company’s success. When DDoS attacks and threats abound, the right protection matters. And every second counts.

THREE QUESTIONS YOU MUST ANSWER IN 2017

1. Are we protected across the board?

Your cloud services may not be protecting you. Every device connected to the network puts your digital infrastructure at risk.

What you need to know:
- Cloud services typically don’t include tailored detection and prevention services.
- Many cloud platform providers and ISPs have a “shared security model,” which could make you solely responsible in the event of a DDoS attack.
- To defeat DDoS strikes, you need specialized protection managed by experienced professionals to augment your existing defenses.

2. What’s the plan if we get a DDoS ransom note?

The precedent is set; some companies have already paid hefty ransoms to restore service and “minimize losses.” But, as the saying goes, the only real defense is an active defense.

What you need to know:
- Hope is not a strategy
- Rather than allocate funds for ransom, invest in the proper protection, technologies and expertise that will yield dividends.
- Establish relationships with law enforcement to help identify trends and defeat DDoS attacks.

3. Are we agile enough to block constantly shifting attacks?

With every DDoS assault, attackers are probing and learning about your defenses; and soon they’ll be back with different tactics.

What you need to know – An example from the Neustar Security Operations Center:
- One client incident started as a DNS reflection attack to a certain port, which later expanded to every port.
- Neustar SOC responded with applied filtering to affected ports eventually rate limiting all inbound DNS traffic
- The attacker responded by launching an NTP reflection attack.
- Several moves and counter-moves later the attacker gave up, stymied by professionals who fight DDoS every day.