CIO INSIGHTS

Bigger Threats, Better Defense

Akamai

Bigger Threats, Better Defense

As the frequency and scale of cyberattacks increase, cloud-based security plays a critical role in protecting enterprises and their customers.

The face of cybersecurity is changing in response to constantly morphing attack methods. Criminals are assaulting organizations with attacks designed to knock websites offline, steal sensitive data, or both. Two particular threats — distributed denial of service (DDoS) and web application attacks — are becoming larger and more frequent, escalating risk for every business with a digital presence, regardless of size or industry.

In this guide, we examine how these attacks increase business risk and explain the core components you need in place to defend against these attacks.

Defining the Threats

DDoS attacks have become more sophisticated, using a variety of methods to flood sites with bogus traffic. Designed to overwhelm a website and render it unavailable to users, DDoS attacks can disrupt a company's digital operations and damage its reputation, productivity, and bottom line.

Web application attacks are designed to compromise data, in the form of personally identifiable information (PII), credentials, or intellectual property. When data is breached, attackers can steal money, information, or identities. Organizations holding the data can be held legally liable for breaches, in addition to the costs required to mitigate the breach. Data breaches can also significantly impact customer loyalty and brand reputation.

> *"DDoS attacks can disrupt a company's digital operations and damage its reputation, productivity, and bottom line."*

Essential Defense

When continuous online availability is business-critical, leadership teams need forward-thinking approaches to cybersecurity to ensure that their digital assets are aggressively defended. On-premises defense systems lack the capacity to ward off DDoS and web application attacks that are becoming larger and more complex; organizations must leverage an advanced cloud platform to stay a step ahead in their battle with cybercriminals.

The Changing Threat Landscape

Organizations are increasingly moving transactions and sensitive data through digital channels, which makes them tempting targets for cybercriminals. Every organization that interacts with customers, suppliers, or employees online is a potential target of malicious actors who have access to powerful tools that can cripple inadequately defended websites and make sensitive data available for exfiltration. The perpetrators can range from lone teenage hackers to state-sponsored organizations.

Massive DDoS Attacks Threaten Availability

In this evolving threat landscape, DDoS attacks are showing a marked increase in scale that raises the threat of business-crippling incidents. The average DDoS attack observed in 2016 was just over 5 Gigabits per second (Gbps), which is large enough to overwhelm most data centers. These incidents, however, pale in comparison to the "mega-attacks" of 100 Gbps or more that have become common. One of the largest DDoS attacks Akamai mitigated on behalf of a single customer in 2016 peaked at 623 Gbps. While unusual, it certainly was not an isolated incident. In Q1 2016 and Q3 2016, Akamai mitigated a record 19 mega-attacks exceeding 100 Gbps.

Moreover, repeat attacks have become the norm. In Q1 2017, attackers targeted the same organization an average of 35 times. The most targeted company was hit with over 350 attacks — averaging nearly four attacks per day.

> ***"The most targeted company was hit with over 350 attacks — averaging nearly four attacks per day."***

Web Application Attacks Cause Costly Breaches

Web applications that store data are targeted by cyberattackers who work to trick the system into a breach. They will target every input, every parameter, and every cookie in search of a viable compromise that allows them to inject malicious payloads that they leverage to find and exfiltrate data.

Attackers are eager to steal PII. With the right combination of personal information, cybercriminals can create new credit accounts, make purchases on those credit accounts, and even craft new identities.

Organizations must apply consistent application controls to minimize vulnerabilities, but attackers work diligently to uncover and exploit those vulnerabilities. That's why organizations need up-to-date cloud-based solutions to shield web applications from malicious traffic.

Deploying an Effective Defense

The potential costs of a cyberattack should give pause to any C-suite. You'll never eliminate every threat to your business. The goal is to minimize business risk — for example, stopping attackers before they get their hands on PII data.

Today's threat landscape is driving scalability requirements, and consequently, adoption of cloud-based security solutions. The best way to protect data and ensure availability is to work with a cloud provider that brings global scale, skills, and a wealth of collective intelligence.

Detection and Mitigation

The ideal platform combines leading-edge threat intelligence and visibility into network traffic with a highly distributed global network of servers supported by data-driven algorithms, automated mitigation strategies, and collective intelligence. These capabilities enable an organization to detect a DDoS assault or an attack on web applications immediately and leverage scale and sophisticated security tools to absorb attack traffic.

Blocking DDoS attacks: By applying controls in the cloud in response to a DDoS attack, such as DDoS scrubbing solutions, a trusted cloud provider keeps your business safe. A robust defense system reduces the attack surface, segregates legitimate traffic from disruptive DDoS packets, and absorbs malicious traffic with capacity far exceeding that of on-premises devices.

Protecting applications: For web application attacks, a scalable, continuously updated web application firewall (WAF) pushes the mitigation of application attacks closer to the source and away from your application. A premier cloud provider can support an end-to-end view of requests and responses that

enables fast, accurate data correlation. This multilayered defense prevents attackers from getting through to your systems and applications and compromising your data.

Staying ahead of attackers: A critical means of protection in the ever-evolving threat landscape is to leverage collective intelligence that keeps the network defense a step ahead of ahead of well-armed cybercriminals. Organizations need access to a big data analysis engine that profiles attackers, exploits, and botnets and continuously monitors their activities. This knowledge base is used to identify the latest attacks as they are first used against one customer, for the benefit of other customers..

“Organizations need access to a big data analysis engine that profiles attackers, exploits, and botnets and continuously monitors their activities.”

Conclusion

Organizations face a steady threat of DDoS and web application attacks that can disrupt key business operations and put sensitive data at risk. Minimizing the impact of these attacks on your business requires world-class cloud-based security with multiple layers of defense. Robust cloud-based security delivers a highly distributed defense network, a constantly updating firewall, rapid attack mitigation, and collective intelligence that will help your organization reduce risk in an increasingly digital environment.

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.
