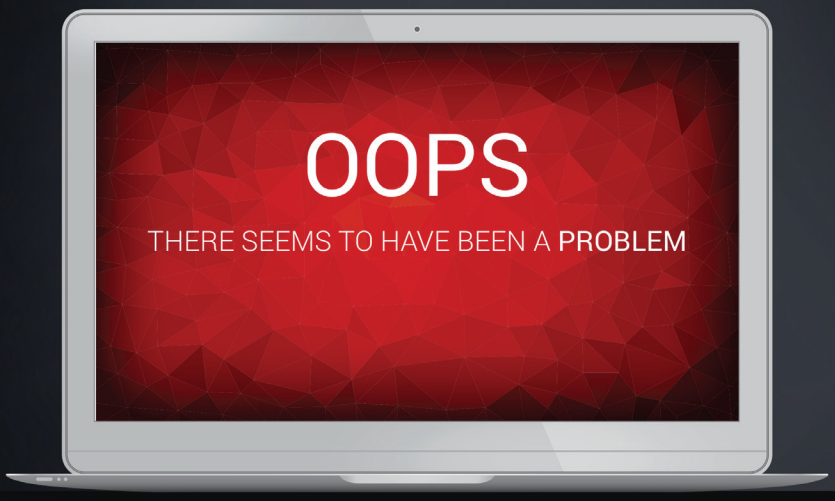
radware



Securing Online Assets: Four Steps to Protect Your Online Business

Businesses of all sizes, across all verticals, generate significant sales online, increasing their risk and exposure from outages and breaches. Unfortunately, malicious actors understand this and target online businesses with this in mind. By and large, their efforts are successful. According to Radware's *2016 Global Network and Application Security Report*, 62% of those attacked suffered downtime or degradation. According to this same report, organizations now see more tangible financial impact from cyber-attacks. Over two-thirds (69%) of organizations say attacks cause revenue, customer, partner, and productivity loss (up from 45% last year).

Attacks aren't just about outages or breaches, performance degradation caused by attacks are a growing problem as well. According to recent studies[1], 40% of customers will now wait 3 seconds or less before moving on to a competitor site, meaning the impact of performance loss is extremely tangible for online businesses.

As cyber threats continue to grow in size, they not only pose security risks but create unnecessary costs that go into processing unwanted data. Processing bad traffic into data centers or cloud hosting environments can result in significant cost, especially to online businesses with largescale networks. Conversely, dropping malicious activity at the border can avoid these unnecessary operational costs and improve overall operational efficiencies. By building strong security controls at all levels of the infrastructure, security teams can provide tools for infrastructure and operations teams to process only legitimate traffic while ensuring that your data center investments are solely for business-related traffic.

Here are four important steps that can help online businesses focus on the threats most commonly targeting these industries.

1 StatCounter Global Browser Stats, February 2015; http://gs.statcounter.com/

Address the Availability Threat

For online businesses, downtime means lost revenue and productivity, making it critical to protect against availability threats, such as DDoS. By and large, there is no longer any debate over the ideal security architecture for providing protection from the wide array of threat vectors related to denial of service attacks. Leading analysts agree that the best solution is hybrid attack protection, a combination of on premise and cloud-based mitigation technology that delivers immediate mitigation of non-volumetric attacks with the availability of additional mitigation resources in the event an attack threatens to saturate the internet pipe of the attack victim.

Guard Against Advanced Bots

Any business that conducts a high volume of online transactions can be a target of bots that exhaust application resources, illegitimately scrape sensitive information from websites and seek vulnerabilities by abusing application logic. To protect applications from advanced bots, operators need more advanced technologies that can track and precisely detect malicious end-user devices regardless of the source IP address. Device fingerprinting generally uses dozens of device characteristics in a unique way to identify and distinguish it from all others. Using this proprietary tracking, a company can generate device reputational profiles that include historical behavioral information to aid in the detection and mitigation of threats.

Protect Customers from Fraud

Protecting online business platforms from fraudulent activity has short-term and long-term benefits in terms of transactions and customer retention. Since many attacks that lead to transactional fraud target application logic vulnerabilities, advanced web application firewall (WAF) technologies should be a critical part of protection strategies. In looking for a WAF that can address more advanced threats, ensure they provide full protection from the OWASP Top 10 threats, use positive and negative security models to keep up with quickly evolving attacks, and minimize manual policy tuning through automation.

Plan for Migration to the Cloud

If your organization hasn't already started to shift its IT and application environment to the cloud, chances are it soon will. According to recent studies[2], over 88% of enterprises are leveraging public cloud resources. While the benefits are obvious, sometimes the security implications are not. Adoption of cloud (both public and private clouds) creates distributed network and application environments that complicate management and orchestration of security policies. Additionally, reliance on a variety of cloud hosting providers creates inconsistency of levels of security being provided to various applications. By leveraging technologies that deliver coordinated policy management across hybrid environments and establish a strong baseline of protection, organizations can progress down the path of cloud migration without compromising their security posture.

Ensure the Availability of Your Online Business

- Reduce the risk of lost revenue, customer churn, and employee productivity by learning about Radware's Online Business Protection Solution.
- Download the eBook *Opportunities, Threats and Security Strategies for Online Business* to learn more about the most common types of attack targeting online businesses

2 http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey