Top 5 Reasons to Turn to the Cloud for Website Availability and Protection

Preventing and overcoming domain name system (DNS) attacks is one of the most important components of a comprehensive security plan for all companies, and particularly for businesses that depend on the Internet for the bulk of their revenue or whose brand and service delivery models are tightly tied into the Internet.

Unfortunately, too many companies still rely on a do-it-yourself approach to DNS, which can leave them exposed. In today's environment, cybercriminals are increasingly targeting DNS vulnerabilities as part of larger, well-coordinated attacks such as denial-of service (DoS) and distributed denial-of-service (DDoS) exploits, exacerbating the security challenges.

DNS attacks are becoming not only more frequent, but also more difficult to detect and defend. According to one survey, DNS attacks increased by 170% in 2012, with nearly 60% of DDoS and DoS attacks characterized as complex—such as those against DNS services—compared with just 23% the year before.[1]

In March 2013, antispam provider Spamhaus suffered one of the largest DDoS attacks ever, which produced more than 300 gigabits per second (Gbps) in traffic by using DNS reflection to amplify the volume of the DDoS attack. Unfortunately, this type of attack is becoming more and more typical.[2] And just as unfortunate, a successful attack can be devastating, resulting in lost sales or advertising revenues, dissatisfied customers and significant damage to the company's brand and reputation.

CONTENTS

Reason No. 1: Your organization is more vulnerable than ever.

Reason No. 2: Do you really want to be in the DNS security business?

Reason No. 3: You can save your company money—while reducing risk.

Reason No. 4: The right cloud-based solution delivers features, functions and levels of protection that are way beyond what you would be able to achieve in-house.

Reason No. 5: Protect your future.

TechTarget Custom Media

[1] "DNS attacks increase by 170%," *Help Net Security*, Jan. 23, 2013
[2] "Spamhaus-style DDoS attacks: All the hackers are doing it," *The Register*, June 3, 2013

For IT and security professionals, this increase in the volume and complexity of attacks against DNS creates significant challenges. The domain name system is one of the most mission-critical elements of a reliable Internet infrastructure. It is the hierarchical naming system for any resource connected to the Internet, enabling email and Web-based applications and other Internet interactions.

DNS is a prime target for DDoS attacks because of its critical nature and the fact that it is based on the User Datagram Protocol (UDP), which by design allows for spoofing of IP packets. Most organizations don't have either the resources or the expertise—or even the inclination—to build the type of DNS infrastructure that will deliver the highest levels of protection. However, companies whose business depends on e-commerce and other Internet activities can't afford to leave themselves open to DNS vulnerabilities.

One of the most efficient and cost-effect ways to bolster DNS protection is to deploy a cloud-based DNS hosting service from a reputable vendor that has a strong history in DNS management. Why turn to the cloud? Here are five top reasons, along with guidance on what to look for in a cloud-based service provider.

REASON NO. 1:
YOUR ORGANIZATION IS MORE VULNERABLE THAN EVER.

Because the domain name system is ubiquitous and a critical element of all Web-based systems, it is a popular target for hackers and cybercriminals. Those who would cause harm for financial, political or other reasons are increasingly coming up with sophisticated ways to attack organizations through DNS. Because of their frequency and the damage they can cause, the following attack methods are of the biggest concern to business leaders, IT departments and security professionals:

- **DDoS attacks:** One of the reasons cybercriminals target DNS is because they realize most organizations are not using the proper resources—such as a cloud-based service. One of the ways to address DNS is to overprovision DNS servers, which is what a reputable cloud service provider can provide. DNS is vulnerable to what is known as DNS amplification attacks, such as the one directed at Spamhaus. In these attacks, hackers use publicly accessible open recursive DNS servers to overwhelm a victim system with DNS response traffic and amplify their DDoS attacks by spoofing requests to open DNS servers from their victims' IP addresses.

- **Attacks against faulty applications:** Organizations that rely on BIND software are at great risk, which is a challenge because BIND is the most widely used DNS software on the Internet. Numerous serious security vulnerabilities have been discovered in various versions of BIND over the years. Because it is still so widely used, however, hackers keep coming up with new ways to exploit it. For example, users were recently warned of yet another new BIND vulnerability whereby hackers can remotely exploit a design error within versions of Internet Systems Consortium's BIND 9 to cause a DoS condition.[3]

[3] BIND 9 Security Vulnerability Matrix, Internet Systems Consortium Knowledge Base, Aug. 12, 2013

- **Man-in-the-middle attacks:** These are also known as cache poisoning attacks. When a recursive server is waiting for a reply back from an authoritative server, a malicious actor masquerades as the authoritative server and sends large amounts of fake authoritatitive server traffic. For example, if the recursive server is tricked, it could cache a bad IP for a legitimate bank domain request. The bad IP address could direct users to a copy of the bank's webpage that's used to steal account credentials.

Other exploits include resource starvation and data modification attacks, and new attack methods are coming up all the time.

REASON NO. 2: DO YOU REALLY WANT TO BE IN THE DNS SECURITY BUSINESS?

There are ways to deal with all of these types of attacks, both preventively and curatively. However, they require levels of infrastructure, expertise and commitment that are typically beyond what most companies are willing to invest in. Understandably, companies that highly depend on the Internet would much rather be spending their time, energy and financial resources on solutions that drive revenues rather than prevent attacks.

For example, there are a variety of standard mitigation techniques companies are likely to utilize to prevent DDoS attacks on their DNS infrastructure. But each one creates a problem that will impact valid traffic. For example, if you block amplification sources, you are likely to block good traffic as well; or if you force DNS queries to TCP rather than UDP, you are going to negatively impact the performance of DNS responses and hinder or divert traffic to your site.

What you really need is a robust and reliable DNS infrastructure with the capacity to handle the largest DDoS attacks, as well as content filtering and other features. To help prevent cache poisoning attacks, you need DNS Security Extensions (DNSSEC) to ensure the authenticity of DNS responses. To mitigate risk of BIND vulnerabilities, an organization may look to a cloud DNS service provider that leverages proven proprietary technology to eliminate risk around BIND open source DNS software.

One other important consideration: These are all things you need to do now to protect your organization. As attackers find new weaknesses to exploit, you have to be vigilant in understanding your vulnerabilities and quick in deploying new solutions.

Here's a question most IT and security professionals have to ask themselves: Are you willing to invest the money, time and staff resources required for DNS security when alternatively you can choose a cloud-based solution that delivers best practices at every level of DNS protection?

REASON NO. 3: YOU CAN SAVE YOUR COMPANY MONEY—WHILE REDUCING RISK.

Working with a cloud-based supplier is typically a far less expensive proposition than building, supporting, maintaining, upgrading and scaling your own infrastructure to protect against today's known and tomorrow's unknown threats. You won't have the upfront capital expenses, and you would spend far less on management over time. Management of the infrastructure is handled by the cloud supplier, and its expertise in adapting to new threats means you won't have to hire your own DNS security experts.

The bigger cost implications, however, are in reducing the risks of downtime. Depending on how much revenue is being driven through the Internet, a single incident could run into millions of dollars. According to one study, the average cost of website downtime was more than $181,000 per hour.[4]

[4] "How the Glitch Stole Christmas," *CFO*, Jan. 4, 2013

REASON NO. 4:
THE RIGHT CLOUD-BASED SOLUTION DELIVERS FEATURES, FUNCTIONS AND LEVELS OF PROTECTION THAT ARE WAY BEYOND WHAT YOU WOULD BE ABLE TO ACHIEVE IN-HOUSE.

So what are the characteristics and features you should expect from a cloud-based service provider? Here are a few:

- **A robust and reliable global DNS infrastructure:** This should include multiple geo-distributed name servers for high availability, as well as multiple Internet service provider connections at each data center. Because of the nature of DNS amplification attacks, the infrastructure should offer overprovisioned services to counter attacks and handle peak loads. If the vendor truly believes in the strength of its infrastructure, it should offer a 100% service-level agreement (SLA) for DNS resolution.

- **A platform for DNS resolution that does not rely entirely on BIND software:** As noted, BIND has a number of documented vulnerabilities. You have to find a reliable and proven alternative.

- **Expert 24/7 support and monitoring:** It should go without saying that today's Internet-based businesses are operating 24 hours a day, seven days a week, 365 days a year. If that is the way your business runs, it should also be the way your DNS management vendor runs.

- **Simplified management:** One of the advantages of using a cloud-based supplier is that it reduces management complexity for your IT and security teams. So you want to make sure your cloud supplier offers simplified DNS management through an intuitive, error-checking console, including a managed DNS reporting service.

- **A full set of features to enhance performance, reliability and availability:** Among the important features to look for: two-factor authentication, DNSSEC compliance, Web forwarding and a Web parking service along with traffic management features of geo-based routing, weighted load balancing and monitoring and failover services. A cloud-based failover solution can automatically detect when your primary site is down and redirect your website visitors to an alternative data center or cloud service, helping to ensure you don't lose their business.

- **DNS expertise and experience:** You want a cloud supplier that lives and breathes DNS, whose very existence is dependent upon ensuring DNS security. This is important as the frequency and complexity of DNS attacks grow. You want a supplier that can not only protect you now, but protect your future as well. Which leads us to . . .

REASON NO. 5:
PROTECT YOUR FUTURE.

Your business depends on the Internet. You can't afford even minutes of downtime. You can't afford the potential bad publicity and ill will that can be engendered by a successful DNS attack. You can't afford to waste precious IT and operational resources. You need to be able to drive efficiencies and free up IT and security practitioners to address more strategic projects. You need a solution that will address today's challenges, and provide you with the infrastructure and expertise to survive future attempted attacks.

As we've discussed here, turning to a cloud solution for DNS management and protection is the most effective and cost-efficient way to protect your current assets and be prepared for future attacks.

But which cloud solution provides the most robust infrastructure, a proprietary secure platform and a full set of features and functions to deliver a best-practices approach to DNS security and protection? Are there any DNS hosting services that offer a 100% SLA for DNS resolution?

As you look into cloud-based alternatives for DNS security and protection, you will find that Verisign® Managed DNS is the solution that offers all of the key features and functions you should be seeking from a cloud services provider. It provides:

- A proprietary platform, called Advanced Transaction Look-up and Signaling (ATLAS®), for secure, consistent and accurate DNS resolution.
- A 100% SLA for DNS resolution.
- The proven expertise and infrastructure of Verisign, including 17 fully redundant, globally distributed DNS resolution supersites that help minimize transactional latency while optimizing availability.
- A network designed and monitored to operate at below 20% of capacity to support traffic bursting.
- A simple-to-use and secure Web-based portal that allows customers to maintain direct and exclusive control over DNS data.
- 24/7, 365-days-a-year expert customer support and performance monitoring.
- A full suite of tools and features to ensure performance and availability, including DNSSEC, Web forwarding, Web parking, two-factor authentication, zone restore, geo-location, failover service and weighted load balancing.

When it comes to protecting the future of your business, having the right solution in place for DNS management and protection is critical—and will likely become even more so as threats continue to multiply in frequency and complexity. You want to drive the availability and reliability of your critical Web systems, and as part of that, you certainly want the highest possible levels of security. Turning to the cloud for DNS is the most efficient and cost-effective way to go.

Ready to take that first step? Get started today!

MVP Network Consulting, LLC

Technology *That Works!*

855-MVPWorks **MVPWorks.com**

*exclusions apply; inquire within for complete offer details.