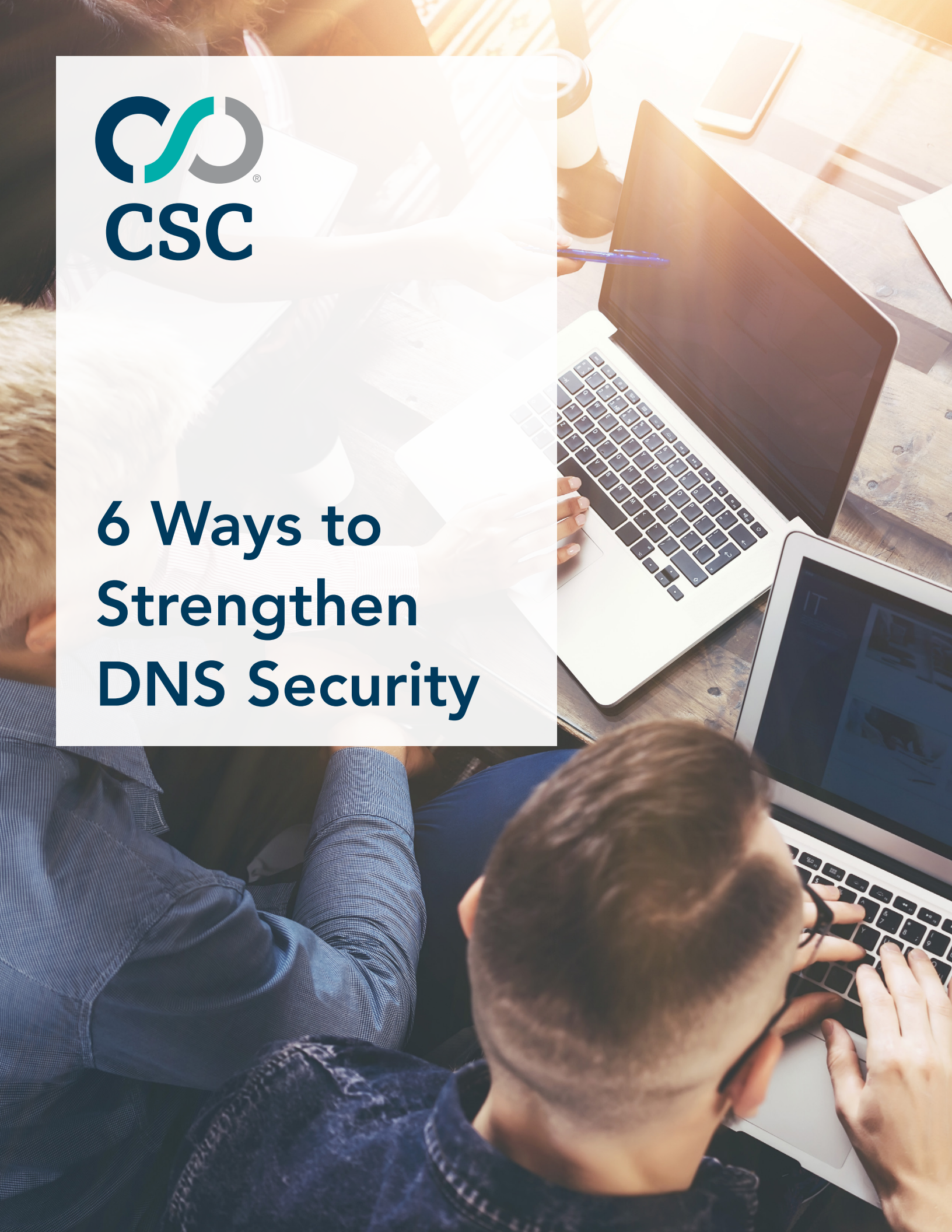

CSC

6 Ways to Strengthen DNS Security

6 Ways to Strengthen DNS Security

The domain name system (DNS) grew to prominence during the initial, innocent days of the internet. During that time, early internet users tended to work for government or education organizations where trust was assumed and security was not even a consideration. Since the online community was small and the internet was sparsely used, the importance of DNS was not widely understood, and as a consequence, left undefended.

Fast-forward to today and you can see the resulting problems. Recent cyber attacks highlight specific techniques bad actors use to intercept and manipulate a company's legitimate web traffic, harvest information like credentials or email addresses, and perform other malicious activities, such as phishing. In some cases, free digital certificates—that require low validation—were used to increase the credibility of the scams, compounding the issue for brands and customers. Consumers are weary of their personal information being accessible to and stolen by criminals, thus breaches hurt the reputation and bottom line of companies around the globe. There's also the exploding problem of distributed denial of service (DDoS) attacks, often aimed at DNS to cripple online business.

For businesses, the stakes are simple: no functioning DNS means no website or internet presence. If DNS fails, customers attempting to visit a website will simply not reach their destination. Nor will employees be able to send or receive company email. If a company relies on VoIP to make and receive phone calls, access is cut off. If DNS goes down, companies will have to resort to using landlines and mobile devices to reach customers. Lastly, the ability for remote employees to access systems via a virtual private network will evaporate, inevitably leaving a company short staffed at the exact time it needs all hands on deck.

Understanding the importance of a robust and secure DNS infrastructure together with domain name and digital certificate management, CSC chose to partner with Neustar®—which has operated one of the world's largest, most trusted DNS networks for over 20 years—and recommends six ways to enhance DNS security.*

**This document is based on "Five Ways Neustar Strengthens DNS Security" by Neustar.*

1 Mitigate DDoS attacks with multi-layered protection

Volumetric DDoS attacks have exploded in size with present day attacks exceeding 1 Terra bit per second (Tbps). Some of the largest attacks on record were aimed at DNS.

There are numerous types of DDoS attacks that target DNS

DNS amplification is one of many attack methods. In this assault, attackers exploit the vast number of open DNS servers on the internet, which can be used to respond to any and all small look-up queries with a spoofed IP of the target. The target then receives much larger DNS responses that quickly overwhelms its capacity. The goal: block legitimate DNS queries by exhausting network capacity.

Another common type of attack is DNS floods, which are directed at the DNS servers hosting specific website(s). These try to drain server-side assets, for instance, memory or central processing unit (CPU), with a barrage of user datagram protocol (UDP) requests, generated by running scripts on compromised botnet machines.

Multiple layers of DDoS protection

To defend against all types of DNS-based attacks, use a solution that comes with multiple layers of DDoS protection.

DNS nodes should be equipped with DDoS mitigation equipment to constantly monitor for malformed traffic as well as traffic from suspicious locations in higher than normal volumes. In many cases, mitigation happens locally.

If an attack is supersized, malicious traffic should automatically re-route to a mitigation network, a completely separate, purpose-built infrastructure. This limits any potential damage to the target nameserver's IPs. With the impact isolated, a 24/7 security operations team is free to be more aggressive in their counter measures.

2 Isolate nameservers through segmentation

Throughout the industry, highly scalable DNS has become a cloud-based service with hundreds or thousands of customers—each with numerous domains—clustered on single networks and sharing a nameserver.

This increases the chances you'll feel someone else's pain. If you use a third-party DNS provider, most attacks on their network won't be aimed at you, but at a domain sharing your provider assigned nameserver.

It's smart to isolate the impact of a DDoS attack

Choose a DNS provider that organizes the DNS network into segments, each with a nameserver announcement shared by only a small group of customers. With fewer customers sharing host names and IP addresses, you face drastically lower odds of feeling a ripple effect.

Here's an analogy. Imagine being in a large hall with 10,000 people and one person jumps up screaming so loudly that nobody can hear the speaker. Now imagine that same scenario, but with just 20 other folks. The impact of the screamer is limited to just the 20. Assuming the screamer is a DDoS attack, when the screamer (attack) starts, the nameserver segmentation and DDoS mitigation strategy instantly moves the entire room to a sound proof area, removes the well-behaved audience members, and works to muffle the screamer before bringing everyone else back in. You can see how with only 20 people, the screaming affected fewer people who were easier to navigate through that attack.

Be protected whether you or someone else is hit

This approach enables individual nameserver announcements to move from the DNS network to the DDoS mitigation network without significantly delaying query resolutions. Your DNS provider should be able to provide effective, immediate mitigation to those under attack, AND prevent any collateral impact for customers still on the DNS network.

When using cloud-provided DNS services, being on a segmented nameserver announcement is an effective way to protect your DNS traffic.

3 Use a non-open source resolver

DNS resolvers—the servers that respond to domain name requests—ensure that users are routed to the correct sites. The most common software application used to manage DNS is Berkeley Internet Name Domain (BIND). Developed at the University of California at Berkeley in 1983, BIND still accounts for the vast majority of global nameserver implementations. Now fully in the public domain, the source code to BIND is open source, and therefore readily available to be explored and exploited by malicious hackers.

Avoid resolver threats

CSC chose to partner with Neustar because they solved that problem years ago. They developed a proprietary code and asked third-party security auditors to look for vulnerabilities. They found none that attackers could exploit remotely, either to steal restricted privileges or hamper directory resolution.

Besides supporting standard DNS specifications and request for comments (RFCs), they have enhanced their resolvers to extend the DNS capabilities while providing extra redundancy and security. Most legacy DNS server implementations never come close.

4 Deploy DNS security extensions (DNSSEC)

As they help internet users find the sites they need, DNS servers query one another. To speed things up, servers cache results for a specified length of time. If there's a query for the same name before the resource record times out, a server will give the cached answer instead of querying another machine.

DNS cache poisoning enables pharming attacks

While this improves efficiency, it also invites cache poisoning. This occurs when a DNS server, usually compromised by criminals, supplies a false answer to a DNS request. Users wind up on phony sites that ask for personal information or simply activate malware.

How can it happen? In many cases, DNS servers don't verify that the responses they receive from other servers relate to the original query. A server will cache bad information and pass it along to others that are DNS clients of the compromised machine.

The key to protection is DNSSEC

DNSSEC is a set of security extensions which authenticate DNS responses. The secret is a series of public and private key combinations to sign information resources. It works by providing a public key that allows the user's resolver to confirm that a DNS answer matches the cryptographic version. All transactions are signed—attackers can't simply spoof the packets.

In more basic terms, DNSSEC secures the DNS process by protecting against cache poisoning, pharming attacks and other serious threats. Ensure you have this turned on.

DNSSEC adoption

From our CSC Cyber Security Reports over the past few years, we have observed alarmingly low DNSSEC adoption rates that vary between 0% to 5% among large global companies across different industries.

5 Increase resilience with a private DNS network

As the old security adage goes, you're only as strong as your weakest link. But what if you could improve your strength posture by eliminating the weak links? By reducing the dependency on public internet connections, the private network has essentially cut out the middle—and most dangerous—part of the DNS transaction where the vast majorities of DDoS attacks and DNS cache poisoning attempts take place. Ask if your provider offers this as an additional service.

A private network offers three key benefits:

Lower latency
In some cases, even if the DNS is working flawlessly, other internet connection issues could cause degradation in DNS performance, thus leading to a poor user experience. The private network provides an online experience that is both fast and efficient because the DNS traffic avoids general internet networking.

Enhanced security
The current Internet of Things-enhanced DDoS attacks that make the internet inaccessible will soon become a thing of the past. A private network for DNS resolution within provider networks minimizes exterior threats like DDoS attacks and cache poisoning attempts.

Better reliability
In the event of a DDoS attack or significant outage, queries will continue to resolve within the private networks where DNS is deployed. This resiliency ensures a superior internet experience for users looking for websites and other vital online assets.

6 Identify security blind spots for your vital digital assets

Companies need to be able to identify their business-critical domains, and monitor them continually to ensure they're secured with the right protections.

We identified that no one was helping companies do this, so we developed CSC Security Center℠, an intelligent platform that understands the threats around vital domains and within the DNS infrastructure on which they sit, and alerts companies to areas of risk.

This unique approach changes the way domains and DNS are secured, and helps companies better identify their security blind spots. Specifically CSC Security Center helps clients:

- Identify which domains are mission critical and require a 100% DNS uptime guarantee
- Identify all current DNS providers and assess any security risks with vendors
- Identify any missing security features increasing the risk of DNS cache poisoning, domain, or DNS hijacking, domain shadowing, DDoS, and phishing.

Request more information on how CSC Security Center and our DNS Management services can help you mitigate cyber threats.

CSC supports companies that are making significant investments in their security posture by exposing blind spots that exist within fundamental internet assets such as domain names, DNS, and digital certificates. By leveraging our proprietary security solutions, CSC secures companies from cyber threats to their digital assets, helping them avoid devastating revenue loss, brand reputation damage, or significant financial penalties as a result of policies like GDPR. Along with internet assets, CSC protects online brands that are being exploited via counterfeit websites, fraud, and IP violations, and helps monitor and mitigate this, providing enforcement and advisory services to protect many of the world's largest brands. Learn more at cscdigitalbrand.services.

cscdigitalbrand.services