CSC

# Beyond the Firewall:

## *Implementing DNS Defenses to Mitigate Online Vulnerabilities and Threats*

# Beyond the Firewall: Implementing DNS Defenses to Mitigate Online Vulnerabilities and Threats

Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secure, trusted, and controlled internal networks and outside untrusted networks, such as the internet.

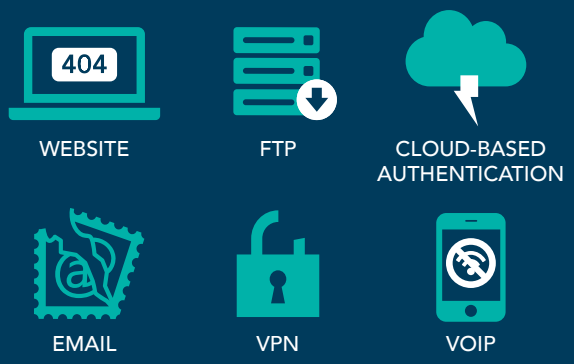
And we need them, because cyber crime is everywhere and growing. Many in the IT security field react by fortifying their defenses within their firewall, and running simulations and penetration tests.

**But a firewall alone is not enough today, when cyber crime is at its highest levels.**

Often overlooked is the security of digital assets that sit outside the firewall—we define these as domain names, the domain name system (DNS), and digital certificates. Well-managed digital assets—DNS in particular—is critical for the smooth operation of business.

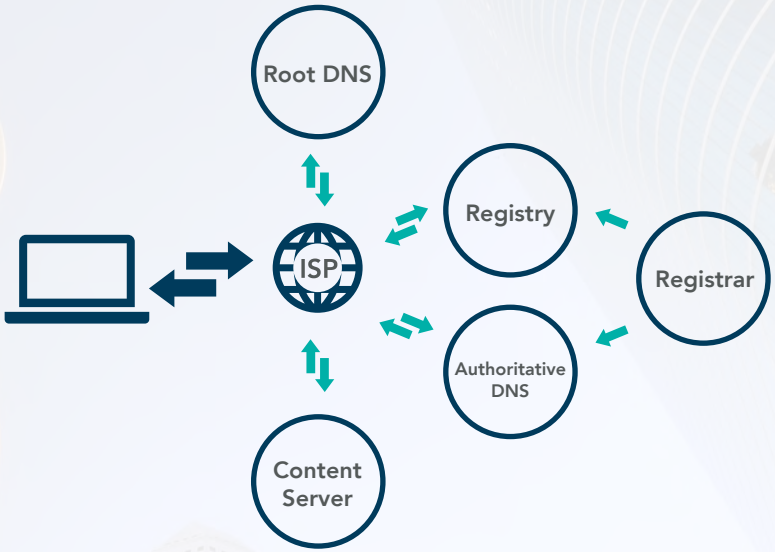
DNS forms the underlying infrastructure for how the internet works, serving as a directory to point users to the right web content. When DNS goes down, websites go down. When that happens, the logical thing is to use phones and email to keep business running. But down DNS means no email, no phones (VoIP), and no remote employee login. It also disallows file transfer protocol for moving large datasets and various multi-factor authentication services (for example email, Google®, and Microsoft®).

Failure of these digital assets leads to a significant impact in terms of lost revenue, data, and brand reputation.




## DNS is fragile; HANDLE WITH CARE!

The simple-looking acronym, DNS, belies the complexity of the system that is made up of a worldwide web of separate entities working in a relay of information exchanges. This complex nature exposes the DNS to multiple potential points of failure, as each point in the system could be vulnerable to attacks, negatively impacting your organization.




## 10 threats and risks associated with DNS vulnerabilities

1. DNS hijacking
2. DNS cache poisoning
3. Domain shadowing
4. DNS outages
5. Malware
6. DNS tunneling
7. Zero-day attacks
8. DDoS attacks
9. Expired, stolen, or lost domains
10. Expired, missing, or poorly installed digital certificates

1

2

3

4

## Four-step defense in depth approach

Defense in depth is the concept of a multi-layered security approach, defending your digital assets outside the firewall.

# STEP 1:

# Employ advanced security features.

For your business-critical domains, those underpinning your business operations, add:

- Registry locks to counter DNS hijacking
- Domain name system security extensions (DNSSEC) to thwart DNS cache poisoning
- Digital certificates to encrypt data
- Domain message authentication reporting and conformance (DMARC) to authenticate your emails and reduce the threat from phishing attacks targeting staff and employees
- Certificate authority authorization (CAA) records to enforce your digital certificate policies

1

2

3

4

## Four-step defense in depth approach

Defense in depth is the concept of a multi-layered security approach, defending your digital assets outside the firewall.

# STEP 2:

# Control user permissions.

Ensure you know who has access to your business critical assets, what permissions they have, and then actively manage those permissions. You should be able to access permissions at the touch of a button, receive notifications, and observe and give permission for any changes within one platform. This will help with unauthorized changes such as DNS hijacking and domain shadowing.

1

2

3

4

## Four-step defense in depth approach

Defense in depth is the concept of a multi-layered security approach, defending your digital assets outside the firewall.

# STEP 3:

# Secure portal access.

You should secure access to all portals you use; each portal should have multi-factor authentication for granting access, including IP validation, two-factor authentication, and federated ID (or single sign on). It also helps to consolidate with fewer providers to manage access and reduce the risk of unauthorized changes to your digital assets.


## Four-step defense in depth approach

Defense in depth is the concept of a multi-layered security approach, defending your digital assets outside the firewall.

# STEP 4:

# Use enterprise-class providers.

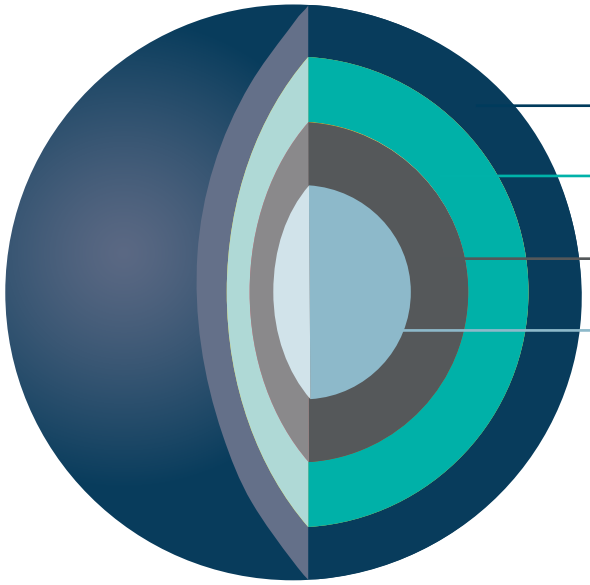
Finally, carefully select your partners. In addition to limiting the number of providers and number of portals you use to control your threat surface, it's important not to compromise on the quality of the domain, DNS, or digital certificate management. The best enterprise providers will enable you to consolidate the management of all these assets, with secure systems, and processes to help mitigate the risks and threats. Enterprise providers have the expertise with in-house analysts, and the knowledge and support from strategic account managers to help you understand the risks involved and choose the right solutions.

## How to gain visibility on security threats outside the firewall

At CSC, we noticed there was nothing on the market to help businesses—in particular the chief information security officer— gauge what is happening with assets outside the firewall. Existing dashboards focus on gaps in internal networks and firewalls, with few tools revealing the serious risks that go beyond the firewall's scope.

CSC Security Center℠ was built to help IT professionals reduce risk from unprotected digital assets. Using our proprietary algorithm, it's able to predict which domain names in a portfolio are vital by examining multiple characteristics relating to the domain and understanding the inter-connected relationships. A further inspection of the domains identifies any instances of risks, and highlights recommendations to mitigate threats.

## Visibility leads to actionable controls and policies



With the development of CSC Security Center, companies can now identify vital domains and security blind spots, including risks from DNS cache poisoning, domain and DNS hijacking, DDoS attacks, and more. We recommend going a step further to put policies in place to set the right framework to strengthen a company's security posture.

### ENTERPRISE CLASS PROVIDER

- ISO 27001 accredited data centers
- SOC 2® compliant
- Third-party penetration, vulnerability testing, security tests
- ICANN and registry accredited
- Best in class partnerships for DNS and digital certificates
- Security first, phishing awareness, and social engineering training
- A mandated clear desk policy
- Mandatory written requests (never via phone)
- Data and GDPR compliant (e.g., WHOIS practices)
- Auto renew policy that is supported by credit on account
- Registry transfer lock policy

### SECURE PORTAL ACCESS

- Mandatory two-factor authentication policy
- Complimentary IP validation
- Complimentary federated ID

### CONTROL USER PERMISSIONS

- Visibility on elevated permissions with notifications
- Authorized contact policy

### ADVANCED SECURITY FEATURES

- Vital domain identification
- Security blind spot detection
- Auto-lock policy

DNS hijacking attacks are taking center stage in cyber security, with daily headlines making 2019 a watershed year.

- CSC Alerts Companies to Increased DNS Hijacking
- DNS Hijacking Abuses Trust in Core Internet Service
- Alert Regarding Published Reports of Attacks on the Domain Name System
- Emergency Directive 19-01 Mitigate DNS Infrastructure Tampering

A global campaign targeting national security organizations, ministries of foreign affairs, and prominent energy organizations was identified to be modifying DNS name records to point users to actor-controlled servers by first targeting third-party entities such as DNS registrars, telecommunication companies, and internet service providers, as well as stealing the organization's legitimate digital certificate for use on actor-controlled servers.

"DNS attacks lead to criminals redirecting web traffic away from a legitimate site to a rogue site, putting customers and companies at great risk," says Mark Flegg, product director for Security Services at CSC. "The recent attacks are complex and vicious, exploiting weaknesses in DNS infrastructure that many companies set up once, then neglect. We strongly advise clients to use the tools and recommendations available to get their digital infrastructure secure."

The severity of the attacks prompted several government and international organizations to react with directives and alerts, something unprecedented in domain security.

"Domain and DNS hijacking are not new security threats, which is why we developed CSC Security Center and are encouraged that hundreds of the world's largest companies are using it to help protect these critical online elements that enable them to operate," says CSC Digital Brand Services General Manager Mark Calandra. "The sophistication and impact of the recent wave of attacks serves as a wakeup call that effectively managing domain names, DNS, and digital certificates needs to be a critical component for enhancing the security posture of any company with an online presence."

To learn more about the risk of DNS hijacking and how best to mitigate the threat, read our blog post ***Confused About Domain Locks? Understand the Intricacies and Security Effectiveness***.

## Four key policies every organization should have for vital domains:

**Mandatory multi-factor authentication to control user access**

**Auto-renew policy to prevent expired and lost domains**

**Auto-lock policy to prevent unauthorized changes on domains**

**Digital certificate policy defining what certificate authority can be used**

Digital asset management is more than managing domain renewals, modification, and replacing digital certificates. We believe in actively helping our clients implement and regulate their policies using innovative technology combined with industry leading service. We're here to help protect our clients business from the threats outside the firewall.

To learn more about the fundamentals of domain security, read our **Digital Asset Security: Back to Basics!** white paper.

cscdigitalbrand.services