Authentic Web.

ENTERPRISE DOMAIN MANAGEMENT FOR THE NEW TLD ERA

6 DNS PROBLEMS IN THE DIGITAL ENTERPRISE

HOW TO FIND THEM AND FIX THEM

A DISCUSSION BRIEF

"The Domain Name System (DNS) underpins every enterprise digital service. Yet, domain and DNS audits reveal compliance gaps in security policy enforcement. Manual change management processes will not work in the digitally transformed enterprise."

Peter LaMantia, CEO, Authentic Web Inc.

6 DNS PROBLEMS: HOW THEY AFFECT SECURITY COMPLIANCE AND DIGITAL PERFORMANCE

It's human nature; the more ubiquitous something becomes, the less we notice it. Clean drinking water, abundant food supply and ready energy are a given in advanced economies…until things go wrong.

This same phenomenon describes the state of digital complexity growth. As enterprises drive digital transformation, systems we've taken for granted are suddenly rising in priority. The Domain Name System (DNS) is a case in point.

As digital becomes the landscape of everything, the underlying infrastructure of the DNS becomes more strained and weaknesses create exposure. Many a Fortune 1000 C-level team is discovering to its chagrin that it pays to pay attention to this critical network foundation layer of all that is digital. The good news…

A little work on the DNS foundation will ensure your brand house remains intact and "up to code."

WHEN THINGS GO WRONG WITH THE DNS

When domains and the DNS go wrong, consequences range from the inconvenience of break/fix to catastrophic cyber security compromise to your business continuity. Even small DNS errors can open the gates to:

Brand damage

Financial losses

Breach of customer trust

Corporate valuation impact

DOMAINS AND DNS ARE A CORPORATE ASSET

Domains and the Domain Name System (DNS) underpin your brand and customer experience. It's an asset that underlies all digital transformation. Marketing, IT and digital operations need to work in partnership to improve and ensure security, compliance and digital performance.

6 DOMAIN NAME SYSTEM PROBLEMS

Brand stakeholders should understand the risks and pitfalls of an under-managed domain name portfolio and related DNS network. Here are six problems enterprise leaders need to assess.

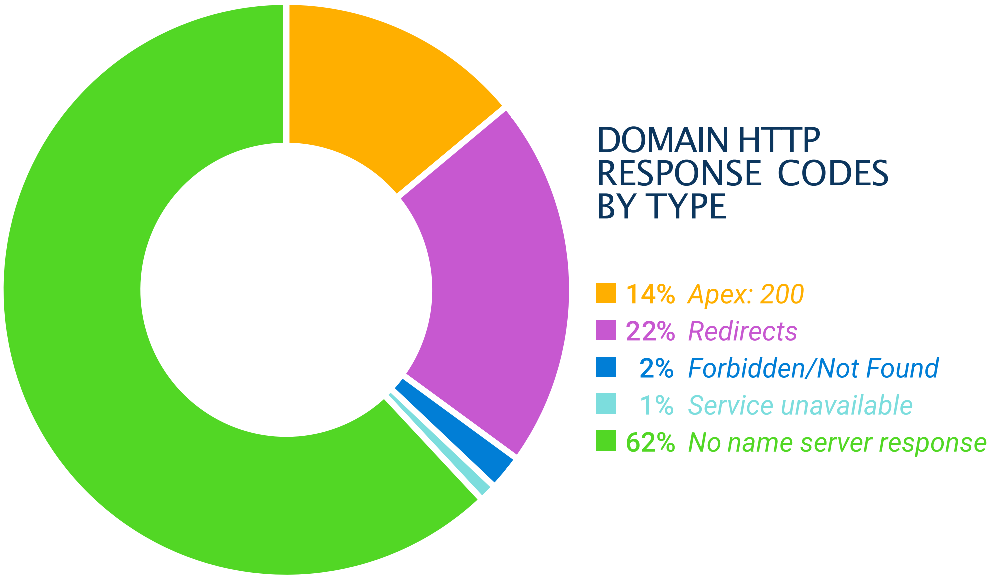
PROBLEM #1:

UNTENDED LEGACY DOMAINS

Marketing folks love domains and order them up like beers at a ballgame. The problem is, many domains are intended for one-time, limited use such as a seasonal campaign, or event landing page. When the campaign or event is over, the DNS settings remain in service, forgotten. This can negatively impact SEO. Worse, unused legacy endpoints can create an entry point for malicious parties to appropriate the domain for nefarious purposes.

PROOF

Our audits of thousands of domains across several verticals including banking, healthcare and technology show huge numbers of domains that fail to resolve, while active DNS settings remain in place.



Source: Authentic Web Inc. Audit of 8 companies; 16,490 domains

SOLUTION

Know the exact HTTP response for each domain and its zone file records at all times. Redirect or expire domains that are no longer required.

PROBLEM #2

MISSING DNS SECURITY SETTINGS

DNS security is critically important and not just an IT security concern. Savvy marketing managers know that DMARC (Domain-Based Message Authentication, Reporting & Conformance) improves outbound email deliverability by 10-15%.

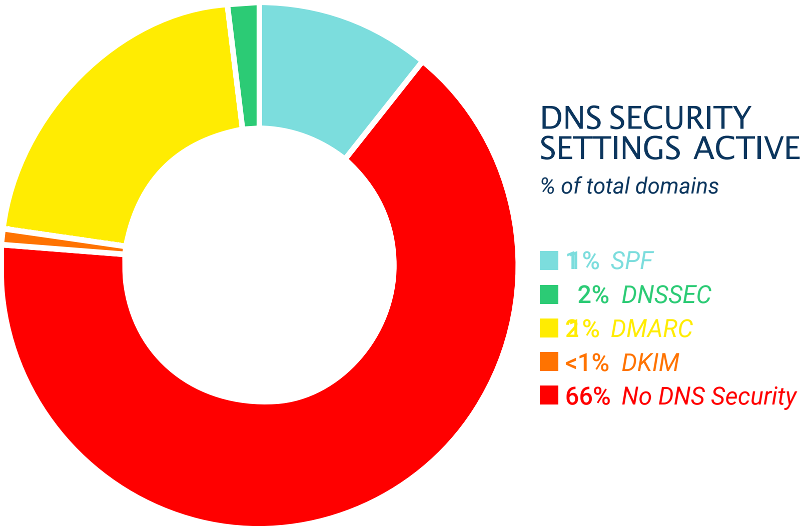
DMARC is one of your most important defenses against email phishing.

SPF (Sender Policy Framework): Authenticates email associated with domains. SFP helps prevent parties from sending phishing emails using your domain.

DNSSEC (Domain Name System Security Extensions): An essential set of DNS protocol extensions that secure the domain name resolving process. DNSSEC helps make the Internet a safer and more secure place for all users, including your customers by reducing the risk of "man-in-the-middle" exploits or cache poisoning.

PROOF

Numerous industry audits show that over most companies fail to activate DNS security settings including DMARC, SPF, and DNSSEC, placing them and their customers at risk. In many cases, DNS settings, especially DNSSEC, are misconfigured.



Source: Authentic Web Inc. Audit of 8 companies; 16,490 domains

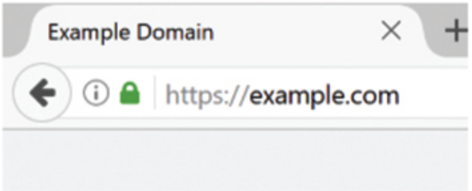
SOLUTION

Every organization should audit its domain and DNS network to identify gaps in DNS security protection that put the enterprise at risk

PROBLEM #3

LACK OF HTTPS ENCRYPTION

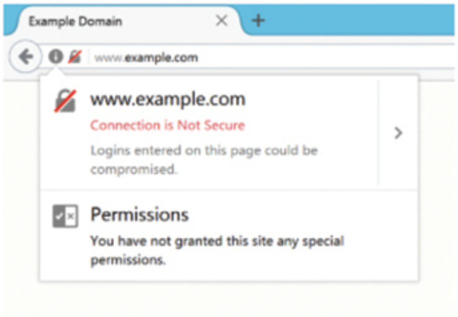
Google Chrome and other major browsers have standardized the requirement that all websites be securely encrypted. This prevents parties from snooping on your customers' browsing sessions, or worse, gaining access to privileged information such as login credentials, or bank account details.



Example Domain

https://example.com

Current secure (HTTPS) connection



Example Domain

www.example.com

www.example.com

Connection is Not Secure

Logins entered on this page could be compromised.

Permissions

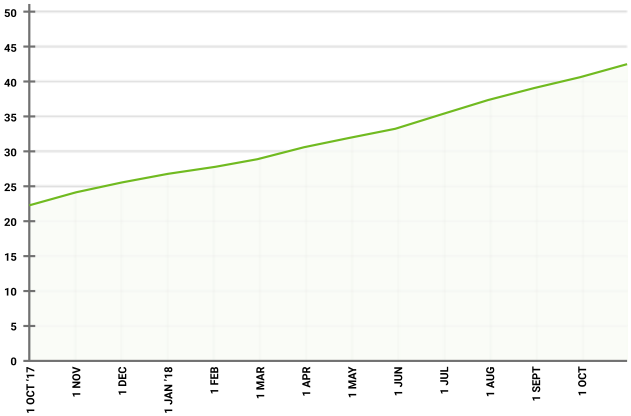
You have not granted this site any special permissions.

HTTPS adoption as a website default has increased from 22.5% to 42.6% on the top 10 million websites (Ranked by Alexa, an Amazon company.) While encouraging, this statistic does not capture HTTPS usage on subdomains or redirects, indicating that there is still a lot of unencrypted content out there, putting companies and users at risk. As companies move to encrypt every web property and redirect, managing all the SSL certificates will become a costly challenge, resource burden and a pain for IT administrators.

PROOF

Google and the large industry certificate authorities have been working for years to encourage universal HTTPS encryption. Failure to protect your web pages can impact your search engine rankings and place your company and customers at risk.

USAGE OF DEFAULTPROTOCOLHTTPS FOR WEBSITES



Source: W³TECH.COM

SOLUTION

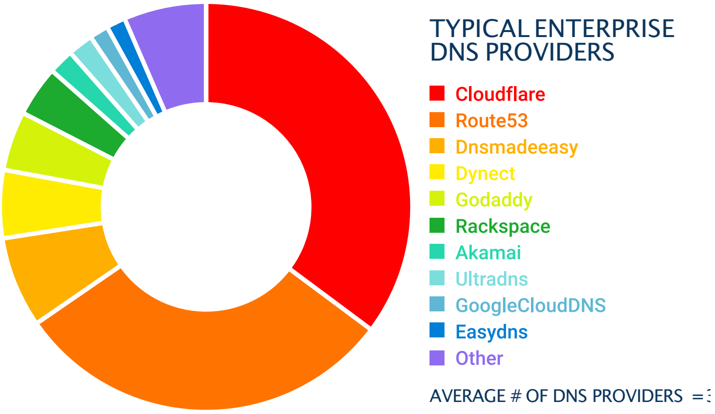
Audit your DNS network to pinpoint pages, domains or redirected domains that are unencrypted. Apply the correct HTTPS certificates with a robust certificate management system.

PROBLEM #4

MULTIPLE DNS PROVIDERS

The most sophisticated enterprise requires two or three Managed DNS services at most:

- *A primary enterprise class AnyCast provider*
- *A secondary service offering automated zone cloning for redundancy*
- *In some instances, specialized services for unique CDN function support*



It's common for organizations to have several – even dozens of active DNS providers with completely unrelated zones under various SLAs and control environments. Having multiple DNS providers (and no secondary DNS) creates problems:

- *Lack of an automated secondary DNS service impacts business continuity*
- *Multiple DNS providers adds control complexity and operational cost*
- *Multiple DNS makes it difficult to get accurate query data*
- *Multiple DNS services proliferates access controls often lacking in change management compliance*
- *This opens attack vector soft spots to nefarious actors*

PROOF

Our DNS audits show that organizations have an average of 39 managed DNS services active. They are typically live due to legacy untended operations set up by past employees who have long since departed.

Number of DNS Providers Audited:

High	71
Low	36
Average	39

Source:
Audit of 8 companies from banking, telecom, manufacturing, and technology.

SOLUTION

Consolidate to a single DNS provider, with secondary DNS redundancy and ensure access, change management and audit controls are in place.

PROBLEM #5

MULTIPLE DOMAIN REGISTRARS

Corporate acquisitions and legacy practices lead many organizations to use multiple domain registrars. Multiple registrars create problems.

- *No single, consolidated view of all domains*
- *Multiple domain system logins and disparate management interfaces*
- *Multiple, disjointed domain administration notices i.e. for domain renewals*
- *Increased cost of maintenance*

PROOF

Our domain audits show that organizations use an average of 12 domain registrars.

Number of Domain Registrars Audited:

High	22
Low	7
Average	12

Source: Audit of 8 companies from banking, telecom, manufacturing, and technology.

SOLUTION

Consolidate to a single corporate domain registrar with a unified, secure access and management system that is more secure, efficient to manage and easier to use.

PROBLEM #6

LACK OF INTEGRATED SYSTEMS

Enterprise operations depend on integration of systems for efficiency and controls. Your finance systems, supplier management – pretty much everything runs best on systems that seamlessly and securely interconnect. Domain and DNS management is rarely integrated in most companies.

- *Task management systems used in the enterprise do not connect to domain and DNS systems*
- *Domain registrar portals rarely connect to DNS (resource record) management controls*
- *DNS security extensions and HTTPS certificates are typically managed separately*
- *Stakeholders rely on emails, spreadsheets and ticketing to get things done*

PROOF

Few organizations have integrated their domain, DNS and ancillary services (such as HTTPS certificates) under a single management system. They rely instead on disparate processes operating in silos.

SOLUTION

Investigate modern, integrated domain/DNS management systems such as DNAM by Authentic Web.

WHERE TO START?

TAKE CONTROL OF YOUR DOMAINS AND DNS NETWORK

Ask yourself three questions. If the answer to any of them is “NO”, take Action!

1. *Do you have a unified, tamper proof system to manage domain and the DNS?*
2. *Can you prove that system enforces security policies and change management?*
3. *Is the system integrated with Registrar and Managed DNS Controls?*

There is no better first step to assessing your digital network security and compliance condition than a third party audit.

Click here to book your domain and DNS audit, at no cost.

DNS AUDIT REPORT

AUDIT VALUE

1. *DNS Visibility*
2. *Security Risk*
3. *Control Gaps*
4. *System Silos*

Cost:
$0.00

Internal Resources Required:
None

Required Info:
A Domain Asset List

Apex Audit Output:

1. *Executive Summary Review and Recommendations*
2. *Domain Inventory by Registrar Service*
3. *Domain Inventory by Managed DNS Service*
4. *Secondary DNS Checkup*
5. *IP/Host Review*
6. *APEX HTTPs Response Inspection/Summary*
7. *DNS Security Review; Pass/Fail; DNSSEC, SPF, DMARC, DKIM*
8. *HTTPS Encryption Report*
9. *Optional: Current Total Cost of Ownership Calculation Session*

NOT READY TO REACH OUT JUST YET?

Click here for an IT checklist
to start a self-assessment.

authenticweb.com

info@authenticweb.com | NA 1.855.436.8853 | INT 1.416.583-3770