Published on *The National Law Review* https://natlawreview.com

Harden Your Organization's Domain Name System (DNS) Security To Protect Against Damaging Data Loss and Insider Threat

Article By:

Brian G. Cesaratto

The importance of the Domain Name System (DNS) to your organization's cybersecurity cannot be understated. Communications between computers on the Internet depend on DNS to get to their intended destination. Network communications begin with a query to DNS to resolve the human readable domain name to a numeric Internet Protocol (IP) address required by computers to route the transmission. A malicious party who is able to exploit a weakness in DNS can re-route sensitive traffic, including Protected Health Information (PHI), Personally Identifiable Information (PII) and other valuable information from the intended recipient to the malicious actor. Indeed, as recent attacks on DNS indicate, even encrypting the communication may not be an effective countermeasure because the transmission can be decrypted after interception. Malicious employees and other insiders may also abuse DNS as a side channel to covertly exfiltrate the organization's most sensitive proprietary information avoiding Data Loss Prevention (DLP) countermeasures that may operate at different layers of the communication process. The recent attacks reported by the Department of Homeland Security reinforce the need to protect DNS functionality as a fundamental component of your organization's overall cybersecurity and compliance strategy.

Although there is no specific mention of DNS in HIPAA, the Gramm Leach Bliley Act, the GDPR or State cybersecurity laws or regulations, including California, Massachusetts or New York, an organization cannot comply with those regulatory frameworks requiring reasonable network security safeguards without considering threats to DNS. The statutory requirements do not generally mandate the particular mix of cybersecurity controls required to protect DNS. Rather, the frameworks require organizations to implement formalized processes to anticipate and assess risks from cyber threats and then adopt reasonable safeguards. [i] Organizations may reference NIST publications and other technical guidance for a catalog of controls to choose from based on the risk assessment. [ii] Consistent with the regulatory imperatives requiring vigilance and appropriate counter-measures to safeguard data when threats evolve, organizations should revisit their defenses given the recent threats to DNS.

Attackers seek to disrupt the normal operations of DNS servers and applications responsible for resolving domain names to properly route network communications between computers. DNS looks up the IP address of the computer to receive the communication based on its domain name and advises the computer requesting a connection of the associated IP address to send the request to.

For example, when a user types “www.anycompany.com” in his or her web browser or sends an email (*e.g.*, “tsmith@anycompany.com”) DNS resolves the domain name (“www.anycompany.com”) to a numerical IP address, such as 172.30.xxx.xxx. DNS advises the requesting computer of the IP address corresponding to the domain name and the requesting computer accordingly directs the traffic.

DNS is under constant attack because of its open and distributed nature. Organizations under persistent threat, particularly healthcare, financial services and technology companies, should be concerned. DHS recently issued its first emergency alert to all its agencies about attacks to hijack DNS resolutions and misdirect the government’s traffic. [iii] Typically, the attacks involved compromise of credentials initially through a phishing attack. DHS reported: “Using compromised credentials, an attacker can modify the location to which an organization’s domain name resources resolve. This enables the attacker to redirect user traffic to attacker-controlled infrastructure and obtain valid encryption certificates for an organization’s domain names, enabling man-in-the-middle attacks.” Further, “because the attacker can set DNS record values, they can also obtain valid encryption certificates for an organization’s domain names. This allows the redirected traffic to be decrypted, exposing any user-submitted data. Since the certificate is valid for the domain, end users receive no error warnings.” DHS emphasizes the criticality of the threat: “This is roughly equivalent to someone lying to the post office about your address, checking your mail, and then hand delivering it to your mailbox.” As DHS also noted, security researchers have identified a wave of other DNS hijacking that affected dozens of government, telecommunications and internet infrastructure entities. [iv]

The risks from DNS exploitation are not exclusively from external hackers. Using DNS to exfiltrate information is also a well-recognized technique for malicious insiders because DNS must permit queries to resolve to perform its functions. Malicious employees and other insiders will try to exploit this functionality for unlawful purposes, including theft of trade secrets and protected data, and to conceal their activities. Hijacking and tunneling attacks to compromise DNS are not new, but the recent attacks highlight how damaging the attacks can be. [v] Moreover, recent caselaw holds that employers may lose statutory protection of their trade secrets if they do not make reasonable efforts to maintain its secrecy and protect it from insider threat. [vi]

Because cybersecurity should be a team effort, here are some steps that IT, HR and Legal should be considering to protect DNS in their particular organization from hijacking and tunneling attacks. Ensure that DNS servers are up to date on all patches and running the latest version of the name server software. Implement complex passwords and multifactor authentication for DNS administrator credentials to prevent unauthorized changes. Implement a formalized system to monitor/proxy DNS traffic to ensure DNS is being used as intended. Implement a formalized system to audit DNS logs to verify that queries are resolving to the intended location. Monitor encryption certificates for your organization’s domain. Consider implementing DNSSEC (which builds trust in the DNS query and resolution process) if technically feasible. [vii] Train your employees in phishing, social engineering and protecting their credentials. Ask basic questions: *e.g.*, What processes are in place to prevent or discover an employee exploiting DNS to exfiltrate sensitive information? What processes are in place to protect administrator credentials? Implement written policies and procedures around protecting DNS, including configuration management, patching, passwords, monitoring and audit. Ultimately, the right mix of DNS safeguards depends on the risks to your particular organization after conducting a risk assessment.

___

[i] See, e.g., 45 C.F.R. §164.306(b); 15 U.S.C. §6801; 23 NYCRR §500.00, 500.02, 500.09; Cal. Civ.

Code 1798.81.5; GDPR Article 32; Massachusetts (M.G.L. c. 93H; 201 CMR 17; Frequently Asked Questions).

[ii] See, e.g., NIST 800-53v4 – Security and Privacy Controls for Federal Information Systems and Organizations, NIST Cybersecurity Framework, HHS Technical Volumes 1 & 2: Cybersecurity Practices for Small, Medium and Large Health Care Organizations.

[iii] DHS Alert (AA19-024A) – DNS Infrastructure Hijacking Campaign; DHS Emergency Directive 19-01 – Mitigate DNS Infrastructure Tampering; CISA Blog – Why CISA issued our first emergency directive.

[iv] Fireeye Threat Research – Global DNS Hijacking Campaign: DNS Manipulation at Scale (https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html); Crowd Strike: Widespread DNS Hijacking Activity Targets Multiple Sectors (https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/).

[v] NIST Special Publication 800-81-2 – Secure Domain Name Systems (DNS) Deployment Guide

[vi] EBG Blog: Even if “Secret” Information Will Not Qualify As A “Trade Secret” Unless Adequate Measures Were Taken To Protect That Secrecy; Abrasic 90 Inc., d/b/a CGW Camel Grinding Wheels, USA v. Weldcote Metals, Inc., Joseph O’Mera and Colleen Cervencik, No. 18 Civ. 05376 (N.D. Ill. March 4, 2019).

[vii] ICANN – DNSSEC – What Is It and Why Is It Important; ICANN Calls For Full DNSSEC Deployment Promotes Community Collaboration To Protect The Internet

National Law Review, Volume IX, Number 93