infoblox

WHITEPAPER

NIS2 IMPLEMENTING REGULATION AND DNS BEST PRACTICES

Author:
Craig Sanderson,
Principal Cyber Security Strategist
at Infoblox

Register now for the Infoblox Security Workshop

TABLE OF CONTENT

The EU Network and Information Systems Directive ("**NIS2**"), which aims to improve cybersecurity resilience across the EU, is scheduled to be implemented into national EU Member State law on 17 October 2024. For a comprehensive overview of the NIS2 requirements, see our previous blog.

On 17 October 2024, the European Commission adopted the NIS2 Implementing Regulation that sets out, in further detail, some of the technological requirements with which entities subject to NIS2 are expected to comply. The requirements of the Implementing Regulation will form the baseline of compliance across the EU, and we expect them to be supplemented with further technical details and guidance in the coming months.

Of particular relevance to legal, compliance and cybersecurity practitioners working for entities subject to NIS2 are the requirements of the Implementing Regulation on DNS security. The European Commission has long recognized the criticality of DNS as a security control. The NIS2 Directive states that "Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend."

Transitioning from policy recognition to practical application, Article 6(7) of the NIS2 Implementing Regulation requires that "the relevant entities shall . . . apply best practices for the security of the DNS". The European Union Agency for Cybersecurity (ENISA) will help define what constitutes "best practice for the security of the DNS".

In this whitepaper, we recommend regular DNS health and security assessments and highlight a few key elements of DNS security best practices that should be considered, including:

- Implementing DNS as a Cyber Security Control
- Securing the DNS Platform
- Securing the DNS Protocol

1. CONDUCT REGULAR DNS HEALTH AND SECURITY ASSESSMENTS

DNS infrastructure is mission-critical. If it fails, entire networks, along with their applications and users, can be brought down. Thus, DNS is a critical element in an organization's digital resiliency. Unfortunately, in many organizations, DNS infrastructure is not regularly assessed.

Organizations should conduct regular health and security assessments of their DNS infrastructure to ensure security and resiliency. Such assessments should include an evaluation of whether the DNS servers have sufficient capacity to meet the needs of the organization, especially when adopting encrypted DNS protocols. Assessments should also include a review of the health and configuration of the servers to ensure the DNS infrastructure is optimized as part of a highly resilient and redundant architecture.

Infoblox regularly performs DNS health and security assessments for global organizations of all sizes. Please reach out to your local Infoblox account team or register to attend an Infoblox security workshop using the link here.

2. IMPLEMENTING DNS AS A CYBER SECURITY CONTROL

There is a compelling case for implementing controls within the DNS platform to leverage the enormous potential of DNS as a foundational layer of a cyber-security architecture.

The DNS platform is already in use by all types of clients on the network, including on-premises, in the cloud and in all manner of IoT devices. Thus, any protection provided by DNS infrastructure benefits all clients that use that infrastructure for name resolution, regardless of the type of device. It is for this reason that organizations and governments should adopt DNS as a foundational component in their cyber security strategy.

a) Implementing DNS as a Cyber Security Control: Protective DNS Services

Protective DNS ("PDNS") is an umbrella term used to refer to DNS infrastructure that applies policy to DNS resolution. A PDNS implementation can refuse to resolve a set of domain names known to be used for malicious purposes, such as phishing campaigns or malware command-and-control infrastructure. PDNS implementations also log queries for domain names that trigger policy, because those queries may indicate infection by malware or other malicious activity.

As evidenced by the deployment of PDNS platforms by governments around the world and the DNS4EU initiative in the European Union, the use of PDNS has become a DNS best practice. According to U.S. cybersecurity official Anne Neuberger, "using secure DNS would reduce the ability for 92% of malware attacks… from a command-and-control perspective, deploying malware on a given network."[1] Organizations should take advantage of the efficacy, low overhead and ease of configuration of PDNS, whether by configuring Response Policy Zones, forwarding to secure recursive DNS services, or a combination of the two.

When implementing PDNS, organizations need to understand the security capabilities in different PDNS solutions. If using RPZs, organizations should configure RPZs on local recursive name servers directly queried by clients whenever possible. This greatly simplifies attribution, namely the ability to identify which device sent the query. Similarly, if using a secure recursive DNS service, organizations should ensure that it supports some mechanism for attribution.

PDNS platforms should be enriched with threat intelligence that protects against both malicious domains and domains that are suspected with a high degree of confidence that they will be used to launch an attack in the future. State-of-the-art DNS early detection capabilities seek to analyze these domains and categorize them as "suspicious" well before the domains are used for malicious purposes. Doing so with a negligible false positive rate can give organizations the confidence to automatically block suspicious domains without disrupting access to legitimate internet traffic.

b) Implementing DNS as a Cyber Security Control: Maintain DNS Security Logs to Support Incident Response

Organizations should maintain DNS and DHCP log data to support incident response activities. During an incident response, an organization's security operations team will often be required to coordinate with the network services team to research the IP address history, network location, access logs, assigned users, and other necessary metadata to investigate and mitigate the incident. This manual process can take several days and consume the time of incident responders that could otherwise be spent triaging the incident. DNS and DHCP logs can help an organization's SOC team quickly identify who, what and when: which device was compromised, who owned the device, what threat was involved, what activities occurred on the device, what data was stored on or accessed from the device, when the attack reached the compromised device and, last but not least, what remedial actions to prioritize. Automating the allocation of real-time key attributable metadata and making it accessible to both the SOC team and the network services team can expedite research and remediation efforts.

To ensure rapid notification of queries that might indicate infection or malicious or suspicious activity, organizations should integrate DNS security logs from their name servers or their secure recursive DNS service with their SIEM or log analysis platform.

If your organization wants to take advantage of these capabilities, Infoblox Cloud Data Connector provides a simplified means to export the relevant network context and data to security operations platforms such as SIEMs.

[1] https://cyberscoop.com/nsa-secure-dns-service-pilot-defense-industrial-base/

3. SECURING THE DNS PLATFORM: USE SECURE, DEDICATED DNS SERVERS

DNS appliances, like other network appliances, are purpose-built and optimized for ease of management, security, and performance. General-purpose servers cannot match the tuning that these appliances offer and, as such, expose organizations to significant risks given the criticality of DNS as a network service.

However, organizations commonly use Windows servers that host DNS and DHCP alongside Active Directory (AD), another mission-critical identity infrastructure. AD manages user access and permissions and stores critical information, creating a large attack surface that is vulnerable to cyberattacks.

Without this separation of duties, if an attacker follows a common escalation path and targets Active Directory, the DNS service and the network it relies on are at risk. As DNS takes on a more significant role in an organization's cyber security strategy, a dedicated DNS Server will be essential to mitigate these risks.

Similarly, threat actors often seek to take advantage of vulnerabilities discovered in DNS that can impact the integrity of the DNS system or result in denial of service. It is critical that organizations keep their DNS software up to date. Infoblox partners with ISC (Internet Systems Consortium) to provide timely patches to vulnerabilities in BIND. Organizations must have processes in place to ensure their DNS infrastructure mitigates the risk of threat actors exploiting vulnerabilities in the DNS platform and software.

4. SECURING THE DNS PROTOCOL: THE ABUSE OF DNS – DNS DATA EXFILTRATION

The DNS protocol is essential for locating services to enable web browsing, email and other mission-critical applications. As a result, traditional security platforms, such as next generation firewalls, often pass DNS traffic unhindered and uninspected. Threat actors have increasingly turned to DNS as an exfiltration vector. Per the U.S. Cybersecurity and Infrastructure Security Agency (CISA), "DNS infrastructure is a common threat vector for attack campaigns." Threat actors often embed stolen data in DNS packets, relying on the DNS infrastructure to relay the stolen data to the threat actor-controlled DNS servers. DNS platforms are ideally positioned to evaluate recursive DNS requests they receive for attempts to exfiltrate data.

More information on the DNS data exfiltration threat vector is available here – DNS Data Exfiltration Resource Center.

Infoblox has developed threat analytics for both on-premises appliances and the Threat Defense cloud platform to specifically mitigate this threat. More details are available on – Threat Insight.

a) Securing the DNS Protocol: Restrict use of unauthorized public, Internet-based DNS services

Organizations should ensure that users do not deliberately or inadvertently use unauthorized public, Internet-based DNS services. This best practice is specifically called out by CISA, which notes how encrypted public DNS services provide threat actors with an effective way to evade network cyber security defenses. In alignment with its guidance, organizations should:

- Block DNS from the internal network to the Internet, except for name servers authorized to communicate directly with name servers on the Internet, such as forwarders.
- Block DNS over TLS (DoT) from the internal network to the Internet using firewall or router ACLs.
- Block DNS over HTTP-S (DoH) from the internal network to the Internet using RPZs and firewall ACLs.

- Use mobile device management (MDM) or other central management solutions to prevent users from configuring external encrypted DNS servers.

Infoblox Threat Defense has a policy feed that tracks public DoT and DoH servers, which can be applied to network security access control infrastructure platforms such as next generation firewalls.

b) Securing the DNS Protocol: Securing the DNS Namespace

Threat actors have proven that attacks such as phishing are far more likely to succeed if they are linked to domains owned by trusted organizations. As a result, they often register lookalike domains that look similar to but are not owned by the target organization. More concerning, poor authoritative domain hygiene can allow threat actors to take control of domains owned by a trusted organization. As shown by Infoblox's recent research papers, many organizations are exposed to this fundamental risk, yet this can be easily mitigated and should be implemented as a standard best practice.

Organizations should put in place a process to proactively evaluate the configurations and audit the data in zone files of their authoritative DNS domains, ensuring that they have retained control of those domain registrations and accompanying name server delegations. Likewise, proactive monitoring of attempts by threat actors to register similar or "Lookalike" domains is critical to ensure threat actors do not use these to target employees or consumers.

Infoblox Threat Defense has a subscription service that enables organizations to proactively look for lookalikes targeting their external DNS domains, as well as those of important supply-chain partners and other high-profile targets.

As a leading cybersecurity and networking company and the market leader in cloud-managed DNS solutions, Infoblox is well-placed to assist organizations across the EU to assess and meet their NIS2 requirements through the Infoblox DNS Health and Security assessments. If you believe your organization can benefit from this, please reach out to your local Infoblox account team or register to attend an Infoblox security workshop using the link here.

For further information, please contact ga@infoblox.com.

infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20241114v2