Infoblox

SOLUTION NOTE

NIS2 and the CAF Framework

NIS2 AND GDPR PENALTIES ARE NOT MUTUALLY EXCLUSIVE

Consider the potential scenario where a regulated entity is subject to penalties under both NIS2 and GDPR.

- NIS2 can bring fines of at least 10 million Euros or up to 2% of the total worldwide turnover (revenue) for an essential entity in the preceding financial year, whichever is greater.
- GDPR can bring fines of up to 20 million Euros or up to 4% of the annual worldwide turnover in the preceding financial year, whichever is greater.

Most sectors of the global economy, including healthcare, finance, energy, and many others, have become extremely dependent on digital technologies. The digital transformation has increased the breadth, depth, and speed of the penetration of digital technologies into everyday life, use in government, and use in business, from the smallest organizations to the very largest global enterprises. Cyberattack activity continues to increase, fueled by organized crime and malevolent nation states.

In the wake of this escalating activity, the European Union had defined and delivered a common cybersecurity strategy in 2013. This was supported by the Directive on Security of Network and Information systems, which was EU wide and known as the European Union cybersecurity Directive 2016/1148) which is also widely referred to as NS1. EU members had adopted NS1 within their respective national legislation by 2020.

NIS2 was conceived to further strengthen security requirements and the associated enforcement. NIS2 will replace the existing NS1 directive and raise the cybersecurity bar even higher for both government and industry. In November of 2022 NIS2 was formally approved by the Council of Ministers. It is expected that NIS2 will be formally adopted (and transposed into national law) by member states over a period of 21 months.

It is important to know that NIS2 expands the sectors and entities beyond those covered by the NIS1 directive. Further, NIS2 exposes “Management bodies” (those individuals that supervise and implement the organization’s functions in support of compliance with the legislation) to potentially onerous fines, personal liability, and more. NIS2 has also added increased notification requirements, specifically within 24 hours of awareness of an event (as opposed to “without undue delay” as in the NIS1 directive).

NIS2 is broad reaching and will impact most organizational digital infrastructure across the EU. Business sectors that are to be subject to NIS2 include sectors such as health, transport, energy, and digital infrastructure. Also impacted under the legislation are chemicals, food, waste management, and manufacturers in the medical device and automotive markets.

NIS2 Impact is Substantial

NIS2 changes are significant and will impact many sectors in new areas.

The implementation of organizational and technical security measures to manage risk remains, with the addition that NIS2 places responsibility on senior management to ensure that the security standards within their organizations are sufficient. This will be judged by the deployment and performance of approved risk management measures. All of this requires careful and complete risk analysis and assessment. If an organization finds vulnerabilities, then necessary and important corrective remediation must happen without delay. DNS security must be addressed within the risk assessment process.

Incident reporting has taken on more sensitivity and the need for more rapid response. Any incident that results in a significant impact to that organization determined by disruption of services, financial loss or other losses must be reported rapidly under NIS2. NIS2 stipulates that the response notification windows will be lowered from 72 to 24 hours; initial notification must also be provided with a final report delivered within one month. Incident reporting must also go to the public in the most serious cases, and include, at least, the consumers of the organization's services. Visibility and well correlated data is essential to understanding potential incidents rapidly and providing accurate and risk-balanced reporting.

Where Does the Cyber Assessment Framework (CAF) Fit In?

The implementation of the EU NIS1 Directive required Competent Authorities to assess the cybersecurity of various parties. In support of this, the UK National Cyber Security Center (NCSC) developed a systematic method of assessing an organization's abilities to manage cybersecurity risks. It remains important to assist organizations to achieve effective and actionable security assessments. This methodology and set of best practices has been assembled and published as the Cyber Assessment Framework (CAF).

The CAF provides a comprehensive framework to assist NIS Competent Authorities to carry out assessments, enable the identification and prioritization of cybersecurity improvement activities, provide a general purpose tool that is industry sector agnostic, and be cost-effective to use and apply. Key objectives of the CAF framework include managing security risk, protecting against cyber-attack, detecting cybersecurity events, and minimizing the impact of cybersecurity incidents.

CAF Objective A. Managing Security Risk

Principle	Guidance and References	Infoblox Capabilities that Address the CAF Guidance
A1. Governance	A1.a Board Direction	
	A1.b Roles and Responsibilities	
	A1.c Decision Making	
A2. Risk Management	A2.a Risk Management Process	• Network automation tools for automated discovery and scanning of all devices on the network to identify misconfigured devices. • Integration with vulnerability management tools which are used when something anomalous is detected.
	A2.b Assurance	

A3. Asset management	A3.a Asset Management	IP Address Management used in the following capacity: • As the single source of truth for network assets. • For automated device discovery. • Integration with vulnerability scanners for scanning when a device joins the network.
A4. Supply chain	A4.a Supply Chain	

CAF Objective B. Defending Systems Against Cyber Attack

Principle	Guidance and References	Infoblox Capabilities that Address the CAF Guidance
B1. Service protection policies and processes	B1.a Policy and Process Development	
	B1.b Policy and Process Implementation	• DNS Firewalling & Malware Detection using aggregated threat intelligence • Detect volumetric DNS attacks • DGA detection, data exfiltration using ML based analytics • Integration with Network Access Control solutions to isolate/quarantine compromised devices and prevent them from joining the network. • DNS Firewalling and automatic incident response via ecosystem integrations using STIX, REST APIs. Rapid mitigation with ecosystem partners (e.g. NAC, Endpoint Detection and Response) • DDI data and threat intel context, automated threat investigation using aggregated search tool
B2. Identify and Access Control	B2.a Identify Verification, Authentication, and Authorization	• Integration with Network Access Control solutions to isolate/quarantine new/rogue/compromised devices and prevent them from joining the network
	B2.b Device Management	
	B2.c Privileged User Management	
	B2.d Identity and Access Management (IdaM)	
B3. Data Security	B3.a Understanding of Data	• Detect DNS tunneling and exfiltration of sensitive data via DNS
	B3.b Data in Transit	
	B3.c Stored Data	
	B3.d Mobile Data	
	B3.3 Media/Equipment Sanitization	

B4. System Security	B4.a Secure by Design	
	B4.b Secure Configuration	
	B4.c Secure Management	
	B4.d Vulnerability Management	• Integration with Vulnerability Management (VM) tools when something anomalous is detected
B5. Resilient Networks and Systems	B5.a Resilience Preparation	
	B5.b Design for Resilience	• On-premises external authoritative DNS with built-in DDoS protection for better resiliency in case of a DNS DDoS attack
	B5.c Backups	
B6. Staffing Awareness and Training	B6.a Cyber Security Culture	
	B6.b Cyber Security Training	

CAF Objective C. Detecting Cyber Security Events

Principle	Guidance and References	Infoblox Capabilities that Address the CAF Guidance
C1. Security Monitoring	C1.a Monitoring Coverage	• DNS Firewalling and Malware Detection using aggregated threat intelligence. • Detects volumetric DNS attacks. • DGA detection, data exfiltration using ML based analytics.
	C1.b Securing Logs	
	C1.c Generating Alerts	• Generate alerts which are passed to the cybersecurity ecosystem including the SIEM and SOAR (example SPLUNK)
	C1.d Identifying Security Incidents	• Insightful reports to quickly identify incidents and associated context for device and user attribution
	C1.e Monitoring Tools and Skills	• Ability to forward DNS requests and DHCP lease logs to 3rd party SIEMs and other SecOps tools for continuous monitoring
C2. Proactive Security Event Discovery	C2.a System Abnormalities for Attack Detection	• Detects DNS tunneling and exfiltration of sensitive data.
	C2.b Proactive Attack Discovery	• Malware Detection using aggregated threat intelligence • Detect volumetric DNS attacks

CAF Objective D. Minimizing the Impact of Cyber Security Incidents

Principle	Guidance and References	Infoblox Capabilities that Address the CAF Guidance
D1. Response and Recovery Planning.	D1.a Response Plan	
	D1.b Response and Recovery Capability	
	D1.c Testing and Exercising	
D2. Lessons Learned	D2.a Incident Root Cause Analysis	IPAM can be used in the following capacity: • As the single source of truth for network assets including contextual data linking the device with the user • Data logged from automated device discovery.
	D2.b Using Incidents to Drive Improvements	

DNS Security is an Essential Part of Your NIS2 Risk Reduction

The UK's prestigious National Cyber Security Centre (NCSC) has issued important recommendations for private companies and government agencies to use Protective DNS (PDNS) to secure and protect information technology assets and networks. During the same time period, The National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA) released a Joint Cybersecurity Information (CSI) brief which contained similar strong guidance on the importance of selecting a protective Domain Name System (PDNS). The NCSC's guidance is in complete alignment with the NSA/CISA CSI technical recommendations, both of which stress the criticality and urgency of implementing a PDNS solution. Protective DNS is part of the growing mix of integrated cybersecurity controls that are now essential to meet the expanding and dangerous threats we all face.

The alternatives are far worse. Potential penalties, loss of reputation, increased risks and harm to your customers due to release of personal and confidential data, and, similarly increased risks and harm to your employees and your organization.

Threat Actors Leverage DNS in the Attack Chain

Threat actors frequently use DNS to support malware infiltration, command and control, and attack execution. DNS is an essential part of the attack chain. Yet DNS has not been within the focus on critical security controls until the past few years. Many organizations have minimal protection in this area.

DNS is continually used to set up and execute attack chains. The attack may involve DNS queries when the victim's system is compromised and infected. DNS is almost always used when an infected system communicates with the command and control (C&C) servers.

The role of core networking services such as DNS in network security are central to network security defense and protection. Advanced, real threat analytics such as those found in BloxOne Threat Defense, focused on DNS services, are critical to identifying and preventing many of these DNS-based attacks.

Threat Intelligence - An Essential Part of the Defensive Mix

Threat intelligence can bring you a very current set of malicious hostnames, domains, IP addresses that you can use such that your DNS servers can then detect and block command and control (C&C) communications to malicious destinations. Advanced techniques such as behavioral analytics and machine learning on real-time DNS queries can rapidly detect and stop a wider variety of attack types (including zero-day DNS tunneling, DGA, data exfiltration, Fast Flux, lookalike domains, and more).

At any point before, during, and after possible attack activity, visibility remains absolutely essential. BloxOne Threat Defense leverages DDI (DNS, DHCP, IPAM database) to provide pervasive asset visibility and awareness. BloxOne Threat Defense does this by using additional contextual information on a compromised system such as location in the network, type of device and an audit trail of all activity from that system. Every IP is linked to a user and related activity. Ask your team members in the SOC. This contextual data can save hours of hunting through log files trying to associate an IP with a user and a particular incident of compromise. This helps administrators quickly identify systems and users that are attempting to reach suspicious and potentially malicious destinations and take quick action to mitigate those threats.

Threat intelligence is also a core component of a Zero Trust (ZT) architecture. ZT is a security concept and framework that assumes that all network traffic is to be untrusted and requires strong authentication and authorization. Threat intelligence can then be used to support the development and implementation of zero trust policies and controls.

Automation is Key

The Security Operations, Network Operations, and Information Technology teams always feel the need for speed. The goal is to get inside of the threat actor's OODA loop before they get inside of yours. The integration of data with SIEM and SOAR infrastructure can provide significant reductions in time for the detection of threats and the automation of incident response. When Infoblox detects something malicious, a new device, or virtual workload on the network, it automatically shares that event information and context with existing security infrastructures like endpoint EDR, SIEM, SOAR, and other solutions. This data can trigger the security tools to prevent access to the network or scan for vulnerabilities until it is deemed compliant with policy.

The June 2021 Gartner report recommends organizations leverage DNS logs for threat detection and forensic purposes with their Security Information and Event Management platforms.

Infoblox

Infoblox is the leader in next generation DNS management and security. More than 12,000 customers, including over 70% of the Fortune 500, rely on Infoblox to scale, simplify and secure their hybrid networks to meet the modern challenges of a cloud-firs world. Learn more at www.infoblox.com.

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

+1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2023 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).