Dahua NIS2 White Paper

Introduction

On December 14 2022, European Union (EU) adopted an updated version of the NIS directive to replace the initial NIS directive that was established in 2016. The new NIS directive ("NIS2") addresses the limitations of the initial NIS directive through establishing with stricter cybersecurity requirements, and expanding the scope of entities and sectors that fall within the scope of the new directive. Overall, the NIS2 Directive focuses on those organizations that are essential and important in the supply chain of critical infrastructure.

As NIS2 is an EU directive, it is not directly applicable in Member States, the Member States is required to transpose it into applicable national laws before October 17, 2024. In addition to this, Member States shall establish a list of essential and important entities that must comply with laws before April 17, 2025.

1.0 The Application Scope of NIS2 Directive

From the perspective of the applicable entities, NIS2 Directive applies to large and medium-sized organizations operating in critical industries such as energy, transportation, banking, finance, digital infrastructure, ICT service management, etc. Depending on the size and the industry, organizations fall that into the "Essential" or "Important" categories must comply with the same security measures. Essential Entities are proactively monitored.

Essential Entities	Important Entities
Annex I Sectors: Large enterprises (>€50M annual turnover; ≥250 employees)	Annex I Sectors: Medium enterprises (>€10M annual turnover; ≥50 employees)
Qualified trust service providers, TLD name registries, DNS service providers	Annex II Sectors: Large & Medium enterprises
Public administration entities, public electronic communications networks providers	Other entities defined by Member States
Operators of essential services	
Other entities defined by Member States as essential entities and critical entities	

Annex I Sectors	Annex II Sectors
Energy	Manufacturing: • Medical devices • Computer, electronic and optical products • Machinery • Electronic equipment • Motor vehicles, trailers and semi-trailers • Other transport equipment
Transport	Digital providers: • Providers of online marketplaces • Providers of online search engines • Providers of social networking services platforms
Banking	Postal and courier services
Financial market infrastructures	Waste management
Health	Manufacture, production and distribution of chemicals
Drinking water & waste water	Production, processing and distribution of food
Digital infrastructure: • Internet Exchange Point providers • DNS service providers • TLD name registries • Cloud computing service providers • Data center service providers • Content delivery network providers • Trust service providers • Providers of public electronic communications networks • Providers of publicly available electronic communications services	Research organizations
ICT service management: • Managed service providers • Managed security service providers	
Public administration	
Space-based services	

2.0 NIS2 Cybersecurity Requirements

As NIS2 outlined certain measures which require relevant organizations to implement. Below is the summary of the main compliance requirements of NIS2 and the measures:

2.1 // Risk Analysis and Information System Security Policies

Establish and maintain an appropriate risk management framework to identify and address the risks faced by network and information system security, clarify the objectives and management methods of network and information system security, and define the responsibilities and authorities of the relevant roles.

2.2 // Incident and Vulnerability Handling

Develop and implement incident and vulnerability handling policies that clearly define the responsibilities, duties, and procedures for detecting, analyzing, containing or responding to, recovering from, documenting, and timely reporting of incidents and vulnerabilities.

2.3 // Business Continuity Measures

Conduct a business impact analysis to assess the potential impact of severe disruptions on business operations. Based on the results of the business impact analysis, establish continuity requirements for networks and information systems. Maintain backup copies of data and provide sufficient available resources, including facilities, networks, information systems, and personnel, to ensure appropriate levels of redundancy.

2.4 // Network and Information System Security (development, maintenance)

Establish security development rules for networks and information systems, and apply these rules during the internal or outsourced development of networks and information systems. These rules should encompass all stages of development, including requirements specification, design, development, implementation, and testing.

2.5 /// Supply Chain Security

Establish, implement, and apply supply chain security policies to manage relationships with direct suppliers and service providers, thereby mitigating identified risks to the cybersecurity and information systems.

2.6 /// Trainings

According to the network and information security policies, policies on specific topics, and other relevant network and information security procedures, establish, implement, and apply a training program. This program should be based on certain standards that specify the training requirements for certain roles and positions.

3.0 Dahua's Compliance Measures

As a supplier, Dahua has adopted comprehensive measures to align with NIS2 requirements:

- Enhancing its Secure Software Development Life Cycle(sSDLC) by regulating and optimizing processes through comprehensive assessments of security activity maturity throughout whole life cycle of product development.
- Attaching great importance to incident and vulnerability management, establishes a complete management process with reference to ISO/IEC 30111, ISO/IEC 29147 and other standards, ensuring that incidents and vulnerabilities can be fixed in time and improving product security in a transparent and open way. Dahua PSIRT monitors global cybersecurity incidents and provides 24/7 emergency response services to global users.
- Conduct business impact analyses to identify critical operations and potential threats and establishes business continuity plans from risk assessment outcomes to minimize system interruptions, shield critical processes from severe disruptions, and ensure swift recovery. This involves regular testing, rehearsals, and updates to these plans.
- Based on cryptographic technology, the whole life cycle of data collection, transmission, storage, usage, sharing, display, copy, deletion and other security protection is built to avoid data leakage, tampering, and destruction, thereby ensuring the security of product data

- Establishing compliance management and control system to promote business compliance in supply chain, delivery and service, marketing, operation and maintenance, human resources and other areas of our business. Dahua ensures supply chain security by implementing robust risk management frameworks that prioritize the security practices of suppliers and service providers when evaluating the competence of suppliers. This involves conducting thorough assessments of suppliers' information security and cybersecurity compliance during the procurement process. It is crucial to select suppliers that demonstrate strong security measures and the ability to sustain operations even during significant disruptions.

- Deliver trainings and updates to employees, and when appropriate, contractors on a regular basis, covering legislation updates, organizational policies, strategies, and procedures to enhance compliance capacities. Security awareness and compliance training is fundamental to effective information and cybersecurity compliance management.

4.0 Dahua's International Standard Conformity

Dahua maintains extremely high standards to protect security and privacy. Dahua continuously evolves product development process, maintaining a security baseline program to enhance security by design. Dahua products are certified with CC (Common Criteria), ETSI EN 303 645, FIPS 140-2 as well as many others. The Dahua information security system and cloud security management have been audited by independent third-party organizations with certifications including:

- ISO 27001 Information Security Management System
- ISO 27701 Privacy Information Management System
- ISO 28000 Supply Chain Security Management System
- ISO 22301 Business Continuity Management System
- ISO 27017 Cloud Security Management System
- ISO 27018 Public Cloud Personal Information Protection Management System
- ISO 20000-1 Information Technology Service Management System

Additionally, Dahua adheres to its core values of openness and constantly seeks cooperation with international authoritative security institutions to jointly build a robust security ecosystem while improving its own security capabilities and solutions.

Dahua has established auditing and certification cooperation with several international security institutions, including British Standards Institution (BSI), Bureau Veritas (BV), TÜV Rheinland, Intertek EWA-Canada as well as many others.

5.0 Dahua's Commitment

As always, Dahua strongly values cybersecurity infrastructure and practices. In compliance with relevant laws and regulations in business operations, Dahua has established a sound cybersecurity management framework. Dahua adheres to industry best practices, conducts stringent risk assessments, implements state-of-the-art security technologies, maintains robust vulnerability management, and conducts security training and audits to safeguard our products and services against emerging threats. Including the measure of maintaining a security baseline program and continuously evolving product development processes to enhance security by design. All these efforts are dedicated to fully assisting customers in improving Dahua cybersecurity defense capabilities. For detailed information, please refer to Dahua Product Cybersecurity White Paper V3.0.

Dahua is committed to handling all cases with transparency and speed in line with industry best practices and international standards.

Thank you for your continued partnership and trust in Dahua.

ENABLING A SMARTER SOCIETY AND BETTER LIVING

Ver. 1, Jan. 2025

DAHUA TECHNOLOGY

Add: No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com

YouTube LinkedIn Partner App Website