DATALOCKER®
SIMPLY SECURE

EBOOK

MANAGED SECURE USB DRIVES AND USB PORT CONTROL: ESSENTIAL TOOLS FOR NIS2 DIRECTIVE COMPLIANCE

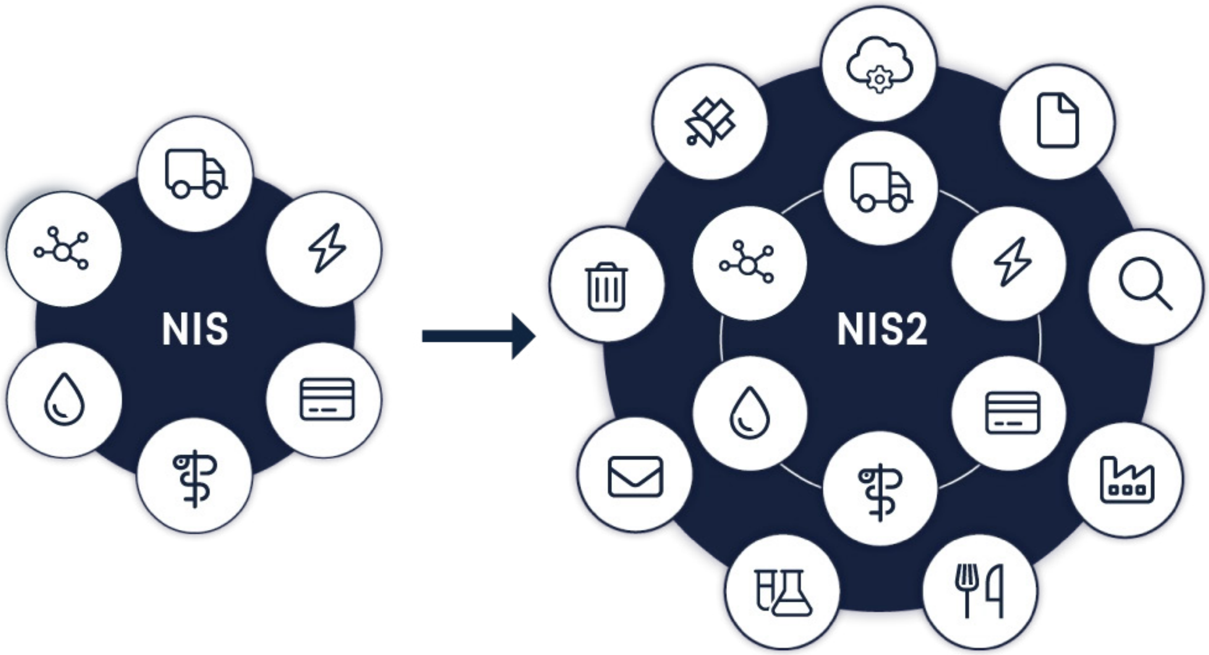


TABLE OF CONTENTS

1 THE NIS2 DIRECTIVE

2 INDUSTRIES AND GEOGRAPHIES AFFECTED BY THE NIS2 DIRECTIVE

3 THE ROLE OF USB DRIVES AND USB PORT CONTROL

4 CONSEQUENCES OF NON-COMPLIANCE WITH THE NIS2 DIRECTIVE

5 NIS2 DIRECTIVE COMPLIANCE AND USB SECURITY: KEY CONSIDERATIONS

6 BEST PRACTICES FOR USB SECURITY IN THE CONTEXT OF NIS2

7 CONCLUSION

SECTION 1
THE NIS2 DIRECTIVE

THE NIS2 DIRECTIVE (DIRECTIVE (EU) 2022 / 2555[1]) IS THE EUROPEAN UNION'S UPDATED FRAMEWORK TO ENSURE A HIGH LEVEL OF NETWORK AND INFORMATION SECURITY ACROSS MEMBER STATES.

As cyber threats become more sophisticated, organizations must implement stricter controls to protect sensitive information and maintain operational resilience. For IT security professionals working in large regulated organizations, ensuring the security of USB drives and USB port control is vitalto safeguarding critical infrastructures and digital service providers.This whitepaper highlights the importance of implementing managed secure USB drives and USB port control solutions in the context of the NIS2 Directive.

THE NIS2 DIRECTIVE

With the NIS2 Directive entered into force on January 16th, 2023, organizations must comply with its requirements or risk substantial financial penalties, reputational damage, and operational disruptions. One critical aspect of complying with the NIS2 Directive is ensuring the security of USB drives and USB port control, as these devices can potentially expose organizations to significant risks, including data leakage, malware infections, and unauthorized access to sensitive information. This whitepaper provides an overview of the industries and geographies affected by the NIS2 Directive, the role of USB drives and USB port control in cybersecurity, and best practices for ensuring USB security in the context of the NIS2 Directive.

[1] https://eur-lex.europa.eu/eli/dir/2022/2555/oj

SECTION 2

INDUSTRIES AND GEOGRAPHIES AFFECTED BY THE NIS2 DIRECTIVE

The NIS2 Directive applies to organizations operating within the European Union. It has a broad scope, encompassing a wide range of sectors, including energy, transport, banking, financial market infrastructures, healthcare, drinking water supply, digital infrastructure, and digital service providers. Organizations operating in the defense, national security, public security, and law enforcement are expressly excluded. Additionally, the Directive covers essential entities, further expanding its reach. IT security professionals working in these sectors and organizations must ensure that their USB security measures align with the requirements of the NIS2 Directive.

SECTION 3

THE ROLE OF USB DRIVES AND USB PORT CONTROL

USB DRIVES AS POTENTIAL THREAT VECTORS

While convenient and portable, USB drives can also serve as potential threat vectors. They can be used to introduce malware, exfiltrate sensitive data, and bypass security measures. The NIS2 Directive emphasizes the need for robust risk management practices and adequate incident response capabilities, making it essential for procurement and IT security professionals to address the risks associated with USB drives.

USB PORT CONTROL AS A SECURITY MEASURE

Controlling access to USB ports is an important security measure to protect against unauthorized data transfers, device connections, and potential malware infections. The NIS2 Directive requires organizations to implement technical and organizational measures to prevent and minimize the impact of incidents, and USB port control plays a critical role in achieving this goal.

SECTION 4

CONSEQUENCES OF NON-COMPLIANCE WITH THE NIS2 DIRECTIVE

Organizations that fail to comply with the NIS2 Directive, when enacted on 17 October 2024, may face severe consequences, including financial penalties, reputational damage, and operational disruptions. National authorities have increased enforcement powers under the NIS2 Directive. They can impose fines of up to 10 million euros or 2% of the worldwide annual turnover for non-compliance (Article 34 of Directive (EU) 2022/2555). Implementing robust USB security measures can help organizations avoid these consequences and ensure compliance with the NIS2 Directive.

IMPLEMENTING ROBUST USB SECURITY MEASURES CAN HELP ORGANIZATIONS AVOID THESE CONSEQUENCES AND ENSURE COMPLIANCE WITH THE NIS2 DIRECTIVE.

SECTION 5

NIS2 DIRECTIVE COMPLIANCE AND USB SECURITY: KEY CONSIDERATIONS

ADDRESSING USB-RELATED RISKS

While convenient and portable, USB drives can also serve as potential threat vectors. They can be used to introduce malware, exfiltrate sensitive data, and bypass security measures. The NIS2 Directive emphasizes the need for robust risk management practices and adequate incident response capabilities, making it essential for procurement and IT security professionals to address the risks associated with USB drives.

INTEGRATING USB SECURITY INTO EXISTING CYBERSECURITY FRAMEWORKS

Controlling access to USB ports is an important security measure to protect against unauthorized data transfers, device connections, and potential malware infections. The NIS2 Directive requires organizations to implement technical and organizational measures to prevent and minimize the impact of incidents, and USB port control plays a critical role in achieving this goal.

SECTION 6

BEST PRACTICES FOR USB SECURITY IN THE CONTEXT OF NIS2

01 IMPLEMENT CENTRALIZED USB DEVICE MANAGEMENT

A centralized USB device management solution, such as DataLocker's SafeConsole, allows organizations to effectively control, monitor, and manage compliant hardware-encrypted USB drives. SafeConsole enables IT security professionals to enforce policies, restrict access, and track device usage, ensuring compliance with the NIS2 Directive's enhanced security requirements.

02 EMPLOY ENCRYPTION AND AUTHENTICATION

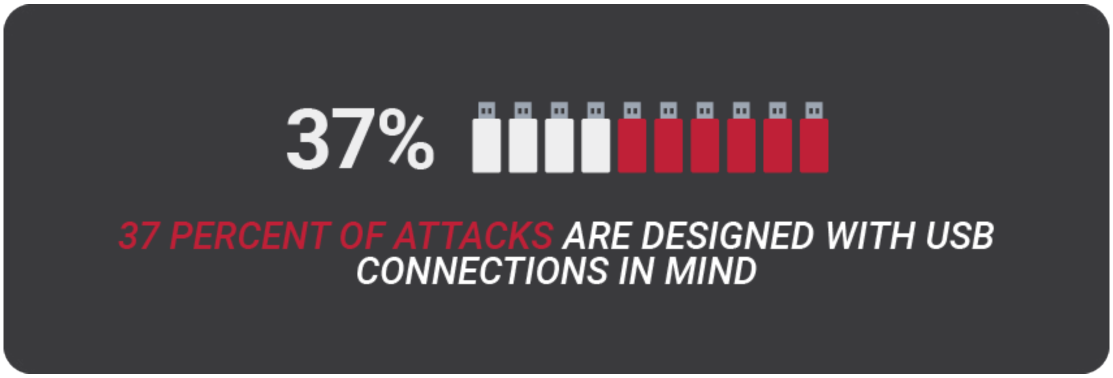
Encrypting data stored on USB drives and implementing robust authentication mechanisms can protect sensitive information and prevent unauthorized access. This aligns with the NIS2 Directive's focus on implementing appropriate technical and organizational measures to ensure a high level of security.

03 CREATE AND ENFORCE USB SECURITY POLICIES

Developing and enforcing comprehensive USB security policies can help organizations manage the risks associated with USB devices. These policies should include guidelines for the acceptable use of USB drives, encryption requirements, and access control measures, ensuring compliance with the NIS2 Directive.

04 SUPPLY CHAIN SECURITY

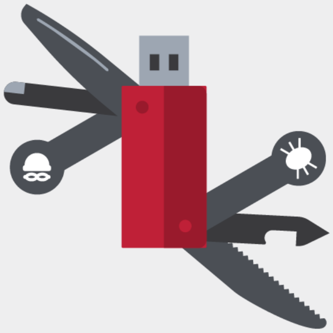
The NIS2 Directive emphasizes the importance of supply chain security, requiring organizations to implement measures to identify, assess, and manage risks related to their supply chain (Article 22 of Directive (EU) 2022/2555). Procurement and IT security professionals should consider USB security a critical component of their supply chain risk management efforts, ensuring that suppliers and partners adhere to the same security standards and practices.



37 PERCENT OF ATTACKS ARE DESIGNED WITH USB CONNECTIONS IN MIND

SECTION 7
CONCLUSION

Managed secure USB drives and USB port control are critical components of an organization’s cybersecurity strategy, particularly for procurement and IT security professionals working in large regulated organizations subject to the NIS2 Directive. By implementing robust USB security measures and leveraging solutions such as DataLocker’s SafeConsole, organizations can minimize the risks associated with USB devices, ensure compliance with the NIS2 Directive, and avoid the severe consequences of non-compliance, including financial penalties, reputational damage, and operational disruptions. Understanding and addressing USB security challenges in the context of the NIS2 Directive is essential for procurement and IT security professionals committed to safeguarding their organizations against ever-evolving cyber threats.



DATALOCKER

DATALOCKER

U.S. Headquarters
+1 913-310-9088

International
+31 467 111 205

sales@datalocker.com
To find your local DataLocker Reseller please visit
datalocker.com