

KR Maritime Cyber Safety News & Report



Vol. 062
June 2024



CONTENTS

Maritime Cyber Safety News

- Key facts about the EU NIS2 Directive regarding cybersecurity
- USCG: Do not click on any links or attachments that may appear suspicious
- Disruption to electronic navigation systems near Saudi Arabia

Advertisement

- KR Cyber Security Training Tool & E-LEARNING

Key facts about the EU NIS2 Directive regarding cybersecurity

Source : *Safety4sea*

The NIS2 Directive is the EU-wide legislation on cybersecurity, providing legal measures to boost the overall level of cybersecurity in the EU.

The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

The Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority,
- cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
- a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Penalties for non-compliance

According to RINA, the NIS2 Directive establishes specific sanctions for companies that fail to meet compliance requirements. These sanctions include:

- Non-monetary remedies: National supervisory authorities can impose compliance orders,

binding instructions, orders to implement security audits, and orders for companies to notify customers of threats.

- Administrative fines: For essential companies, Member States must provide for a maximum fine of at least €10,000,000 or 2% of the total annual global turnover, whichever is higher. For important companies, the maximum fine is at least €7,000,000 or 1.4% of the total annual global turnover.
- Criminal penalties for management: NIS2 introduces measures to hold corporate management members personally accountable in case of serious negligence following a security incident. This can include the order to make compliance breaches public and, in the case of essential entities, a temporary ban on holding managerial positions in case of repeated violations.

These measures are designed to hold corporate management accountable and prevent serious negligence in managing cyber risks.

The cybersecurity risk in the new era of operations

Cyber incidents (36% of overall responses) ranks as the most important risk globally for the third year in a row – for the first time by a clear margin (5% points). It is the top peril in 17 countries, including Australia, France, Germany, India, Japan, the UK, and the USA. A data breach is seen as the most concerning cyber threat for Allianz Risk Barometer respondents (59%) followed by attacks on critical infrastructure and physical assets (53%).

Captain Nitin Chopra, Senior Marine Risk Consultant, Allianz Commercial, highlighted in the Safety and Shipping review 2024 that the use of information systems and data on board vessels is increasing, which presents a new challenge for shipping and makes them more vulnerable to cyber-attacks as they digitize their operations.

Meanwhile, according to DNV's Maritime Cyber Priority 2023, achieving a more cyber-secure supply chain is far from easy. For this to happen, operators need to thoroughly audit their vendors' cybersecurity requirements during procurement, installation and operation of equipment, systems, and software.

USCG: Do not click on any links or attachments that may appear suspicious

Source : *Safety4sea*

The US Coast Guard, in conjunction with the maritime community and the UK Department for Transportation, has been made aware of several phishing attempts by nefarious actors impersonating Coast Guard port state control (PSC) authorities.

These incidents range from unsophisticated attempts asking for vessels to urgently contact PSC teams at a malicious hyperlink, to more sophisticated and targeted “spear phishing” attempts, which include details such as the ship name and IMO number to appear legitimate.

“Phishing is a common form of social engineering that uses email or malicious websites to solicit personal information or to get a victim to download malicious software by posing as a trustworthy entity.”

In that regard, USCG issued a Marine Safety Information Bulletin to highlight that email correspondence from the Coast Guard will always be from the “uscg.mil” domain, will NOT include links requesting information, and will typically copy the vessel’s agent in the port of destination.

“Emails claiming to be from the Coast Guard or PSC teams that do not state the specific purpose of the correspondence and/or are not from the uscg.mil domain should be regarded with suspicion. If you have received correspondence that is suspicious or has left you unsure of its legitimacy, please contact your agent or call the Coast Guard Sector Command Center at your port of destination.”, USCG further explained.

Additionally, the Coast Guard encourages vessel operators to keep the following in mind regarding correspondence that may be phishing attempts:

- Do not click on any links or attachments that may appear suspicious.
- Take time to evaluate a suspicious email or correspondence, as victims of phishing tend to be those who go through emails quickly.

- The Coast Guard will not request personal information via email

The Coast Guard strongly encourages vessel operators to provide regular phishing and cybersecurity awareness training to all employees to identify and report suspicious correspondences. Additionally, the Coast Guard encourages all international partners to pass on information relating to suspicious behavior observed in the Marine Transportation System to their respective regulatory organizations.

Disruption to electronic navigation systems near Saudi Arabia

Source : *Safety4sea*

The United Kingdom Maritime Trade Operations (UKMTO) has issued a warning following a report of a vessel experiencing disruption to its electronic navigation systems.

According to UKMTO, the disruption to electronic navigation incident occurred between 2nd April 2300UTC and 3rd April 0100UTC, approximately 95 nautical miles east of Ras Al Zour, Saudi Arabia. Vessels navigating in the area have been advised to proceed with caution and to report any irregular activity or concerns to UKMTO immediately.

United Kingdom Maritime Trade Operations (UKMTO)
@UK_MTO · Follow

UKMTO INCIDENT 060 ADVISORY - ELECTRONIC INTERFERENCE
ukmto.org/indian-ocean/u...
#MaritimeSecurity #MarSec

UKMTO ADVISORY
INCIDENT 060 – ELECTRONIC INTERFERENCE

Incident Date:
02 APR 2024
Incident Time:
2300UTC

Source: Master
Issued: 03 APR 2024 1620UTC
UKMTO has received a report of a vessel experiencing disruption to electronic navigation systems (GPS/AIS) between 2nd April 2300UTC and 3rd April 0100UTC, 95NM east of Ras Al Zour, Saudi Arabia.
Vessels are advised to transit with caution and report any Irregular Activity to UKMTO.

1:21 AM · Apr 4, 2024

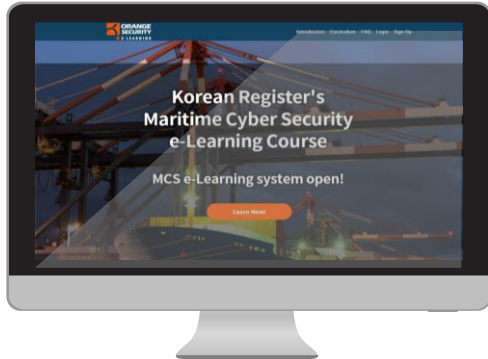
142
Reply
Share

[Read more on X](#)

The disruption specifically affected the vessel's GPS and AIS systems, which are critical for navigation and communication at sea. Authorities are currently investigating the cause of the disruption, and shipping companies are urged to take necessary precautions to ensure the safety of their vessels and crews.

Online Training

KR Maritime Cybersecurity e-Learning Center training course



Q&A : <https://edu.orangecq.com/>

KR reorganized the cyber security e-learning training in cooperation with Orange Security, who is a maritime cyber security specialist. Through this reorganization of e-learning training, KR becomes to provide customized training for each customer.

New curriculum consists of Maritime cyber security Awareness, cyber security Practical Management, cyber security Officers and cyber security Type Approval. Maritime cyber security Awareness is a course to raise awareness of maritime cyber security for employees including crews, which includes two modules - Understanding of Maritime Cyber Security and Practice of Maritime Cyber Security. cyber security Practical Management is a course for ship officers and engineers, which includes KR Remote Cyber Survey as well as Maritime cyber security Awareness course. cyber security Officers is for the person in charge of managing cyber security system and responding classification cyber security survey. This course consists of Administrative Security, Cyber Asset, Threat and Technical Security, Understanding of Maritime Cyber Security Risk Assessment with all modules in cyber security Practical Management. Finally, KR Cyber Security Type Approval is a course for equipment company and provides introduction of international standard related to requirements of cyber security for equipment and materials required for obtaining KR cyber security type approval.

KR CS++

KR Cybersecurity training tool



No.	Titles
1	Understanding of Maritime Cyber Security
2	Practice of Maritime Cyber Security
3	Administrative Security
4	Cyber Asset, Threat and Technical Security
5	KR Cyber Security Type Approval
6	Understanding of Maritime Cyber Security Risk Assessment
7	KR Remote Cyber Survey

KR launched KR CS++, maritime cybersecurity training tool.

KR CS++ was produced in USB type and tablet type for effective cybersecurity training of seafarers in an environment where cybersecurity training is difficult due to the unstable Internet environment on ships. In addition, KR is striving for customer satisfaction by providing various types of services.

Currently, the same service is provided through cybersecurity e-learning education.



Providing the best services, Creating a better world

Cyber Certification Team, Korean Register
(46762) 36, Myeongji ocean city 9-ro, Gangseo-gu, Busan Republic of Korea
Tel +82 70 8799 8595
Fax +82 70 8799 8594
www.krs.co.kr

Copyright © 2023 ALL RIGHTS RESERVED BY KOREAN REGISTER