CYBERSECURITY IN INLAND NAVIGATION

PIANC AWARENESS PAPER

RIS WEEK December 2018
Jean-Noël Schilling
Content

Introduction

Our Reliance on Information technology

PIANC Risk Awareness Paper

Next Steps
CCNR’s role

Aiming at further improving and harmonising inland navigation standards and regulations.

The safety of persons and goods in navigation activities is a longstanding concern which, however, requires ongoing adaptation of standards.
Cyber-threats are real

Introduction

Protecting GPS From Spoofers Is Critical to the Future of Navigation

GPS is vulnerable to spoofing attacks. Here’s how we can defend these important navigation signals

By Mark L. Psaki and Todd E. Humphreys

Just hours before U.S. president Barack Obama delivered his final State of the Union speech in January, two U.S. Navy patrol boats wandered into Iranian waters. The Iranian military intercepted the vessels and captured 10 U.S. sailors, making for

Le Monde

Les 10 nuits en enfer de Maersk pour réinstaller 4000 serveurs et 45000 PC

Sécurité : Le transporteur a été frappé de plein fouet en 2017 par le ransomware NotPetya

Outbreak: The First Five Victims of the Stuxnet Worm

The infamous Stuxnet worm was discovered in 2010, but had been active since at least 2006. The attack started by infecting five carefully selected organizations:

- Fordel Technic, International Engineering Co., ICs vendor
- Behrang Co, Elec & Compy Engineering, ICs vendor
- Neda Industrial Group, component supplier
- Control Gostar, Industrial Company, ICs vendor
- Kata Electric, Control & Logic developer

Global Epidemic

Hafen von Antwerpen

Hacker haffen Drogenschmugglern beim Containerklau


Hafen von Antwerpen. Container volles Drogen
MAERSK CASE STUDY

We are sorry but maerskline.com is temporary down.

We confirm that some Maersk IT systems are down. We are investigating the situation. The safety of your business and our people is our top priority. We will provide you with more information.

We apologize for any inconvenience this may cause.

Maersk Line team
Reliance on Information Technology

Our reliance on information technology.
FIRST STEP

Cybersecurity maturity

RISK AWARENESS

Criticality
RISK AWARENESS

1. Systems Currently in Use

2. Future Technologies

3. Recommendations for Follow Up

Report No. PIANC Awareness Paper: Cybersecurity in Inland Navigation
On-board systems
Controls
Navigations

Infrastructure systems
Controls
Lock and bridge management
Traffic planning

Servicing systems
Web portals
Distributed services
RISK AWARENESS

- Automated / autonomous Vessels
- Digital Multimodal Nodes
- E-documents
RISK AWARENESS

- Broaden the risk assessment
- Use all possible levers
- Promote Trainings and continuous learnings

RECOMMENDATIONS FOR FOLLOW UP
Next steps

- Risk Awareness
- Continuity Plan Available
- Recovery Readiness
- Risk Management
- Mitigation
- Competitive Advantage

Cybersecurity maturity vs. Criticity
Question to be answered

What cyber-risks for inland navigation are we (un)aware of?
CESNI 2019-21 work programme

Next steps

TASK OF CESNI/TI

Undertake technical and legal analysis and develop recommendations regarding cyber-risks and other safety risks for IT applications in inland navigation and provide proposals for concrete mitigation measures
2019 Workshop Cybersecurity

- Further Awareness supported by CS experts
- Draw a roadmap for cybersecurity
- Deliver and share good practices
We have created societies in the **physical world** where we feel safe,

We need to make sure that that also happens in the digital World

Jim Hagemann Snabe  
CEO A.P. Møller-Mærsk  
Tallinn Digital Summit keynote speech  
September 2017
THANK YOU FOR YOUR ATTENTION

Jean-Noël Schilling
T +33 (0)3 88 52 45 20
jn.schilling@ccr-zkr.org