MedPORTS Forum 2019

Cybersecurity in the maritime sector

Martin de Maupeou
Manager
COSCO Shipping Lines confirms it has been hit by a cyber attack impacting its internet connection within its offices in America.

As such, local email and network telephone were not working properly and the company decided to shut down the connections with other regions for further investigation.

Maersk says global IT breakdown caused by cyber attack

COPENHAGEN (Reuters) - Shipping giant A.P. Moller-Maersk (MAERSKb.CO), which handles one out of seven containers shipped globally, said the Petya cyber attack had caused outages at its computer systems across the world on Tuesday.
Challenges for the smart port

- **Risk exposure** - Low-probability, high-impact incidents
- **Detection** - Complexity of the infrastructure and environment
- **Supply chain** - Increasing number of actors and external providers
- **Complexity** - Ships & ports use the most advanced technology
- **Security culture** - Including cyber in the maritime security culture
Vulnerabilities across the whole value chain
Aggravating factors

• **Human factor** - Reduced crews and lack of skilled profiles
• **Technology** - Use of standard systems with know vulnerabilities
• **Technical factor** - Short life-cycles of IT
• **Operations** - Downsides of uncontrolled openness
Security measures

- **Securing by design** maritime equipment, ICS and architectures
- **Managing access rights** via authentication solutions
- **Adopting a dynamic cybersecurity posture**
- **Training and education** crews and (skilled) staff
Policy driven initiatives

- **International** - Resolution MSC.428(98)

- **European** - Network and Information Security Directive

- **National** - Denmark 2018 maritime cybersecurity strategy