TELEMAR

Ransomware:
When ships go silent

Ransomware is a type of malicious software that encrypts access to computer systems or networks, making data inaccessible until a ransom is paid to the attacker. In the maritime sector, where both shipboard and shoreside operations depend on continuous communication, a ransomware attack poses a serious threat to the safety of navigation.

Why it's dangerous

These attacks can affect everything from route planning systems and communication tools to cargo manifest databases. When systems go down, deliveries are delayed, contracts are disrupted, and trust with clients can be lost.

Real world examples

- A ship stranded in port after ransomware locks access to its navigational data
- An offshore platform's IT system is compromised putting pressure and flow monitoring offline
- A shipping company's shore office loses access to its CRM system, preventing instructions from being sent to crews

How to protect against it

- Regular data backups – both offline and in the cloud
- Early threat detection systems like Marlink Cyber Detection Service
- Limiting user privileges and deploying behaviour-based antivirus protection
- Employ reputable unified threat management and endpoint protection, preferably with a network detection and response solution in place.

Ransomware doesn't just target IT – it halts the entire maritime business chain. Prevention is an investment that pays for itself many times over

Contact us
Email: Sos@telemargroup.com
www.telemargroup.com