What do you do if a hacker takes over your ship?

March 22 2023

The ship is not behaving as it should. What's up? Captain Odd Sveinung Hareide explains to the others on the bridge what he has done, what he is prioritizing right now and the next move. Credit: Eli Anne Tvergrov, NTNU

You're on the bridge, with the ship's course shown on the digital display. But why is the ship continuing to turn west?

Everything looks normal on the computer screens in the dark wheelhouse—but outside, the land is dangerously close. What's going on?

Down in the engine room, workers report via radio that everything is normal, but they wonder why the bridge has changed course. The engines are revving and the ship is picking up speed. The engine room hasn't done this. What now?

Cybersecurity is a hot topic for the entire maritime industry, as well as in academia. A joint team recently conducted a completely new cyber security course at NTNU in Ålesund.

Probably the first of its kind

The Norwegian University of Science and Technology (NTNU) in Ålesund's program for the maritime industry has just offered a new course entitled "Maritime digital security" (in Norwegian).

Over two months, course participants have looked at digital threats. They have assessed the risk of existing digital threats and realistically practiced a cyber attack on a ship under way. The key focus is on risk management of cyber attacks and building resilience.

"Where information technology and people meet, there is room for digital vulnerability. Security breaches can come in through the ship's systems and through the port system and through the people who operate or supervise them," Marie Haugli-Sandvik and Erlend Erstad said.

Both are Ph.D. candidates at the Department of Ocean Operations and Civil Engineering at NTNU. They are studying how the maritime industry can be better equipped to handle cyber attacks.

The two Ph.D. candidates have developed and now run the maritime digital security course, which appears to be the first of its kind in

Norway.

The course has been included as part of the doctoral theses they are about to complete.

Developed with the industry

"We developed this course in close collaboration with the industry," Erstad said. "We have listened to what they want, looked objectively at their needs, and then tested the best solution we can come up with."

"It's always better to have a broad perspective and different approaches with new projects and methods. Established businesses can also benefit from a fresh look. NTNU is a good place to try out new ideas. As researchers, we can help meet the industry's urgent needs while at the same time discussing solutions with them for the future," Haugli-Sandvik said.

Not enough training in cyber security

Haugli-Sandvik conducted a survey this winter among 293 deck officers from 11 major offshore shipowners in Norway.

- Eighty-three percent said that they had taken part in some form of cyber security training.
- Fifteen percent answered that they had never received training.
- Two percent didn't know if they had had training.

"Eighty-two percent of the deck officers said that they had received the training as e-learning and/or that they had participated in digital safety campaigns sent by their employer," she said.

Employers to a large extent were responsible for this training, in the form of courses. This demonstrates that the industry wants to take responsibility, Haugli-Sandvik believes. But there are many standardized and general IT security courses.

"But most of the training wasn't directly operationally oriented and/or adapted to the maritime industry," Haugli-Sandvik said.

This is illustrated by the fact that 66% of the deck officers surveyed said that they were uncertain or disagreed that they had enough training to handle a cyber incident on board.

Major consequences

Digital IT events can have consequences for ship operations. They can affect administrative systems for ship manifests, passenger lists, digital certificates and sailing licenses and the like. This can delay or impede operations.

Companies that are exposed to these problems can experience significant financial consequences and damage to their reputation.

The Norwegian National Security Authority (NSM) points out that activity in the cyber world can be so advanced that we don't actually notice it, and covert activity can remain hidden for a long time. How should crew on board react to discover hidden threats?

How can the crew on board make the right assessments in advance or make concrete decisions in the brief window of time a few minutes before a ship runs aground?

Knowing what to do, both to prevent this from happening, and to practice what to do if it does, is critical for the industry.

Deck officers and cyber security

Haugli-Sandvik's doctoral dissertation looks at how deck officers experience cyber risk at sea.

"My project is part of the work in one of NTNU's 12 centers for research-driven innovation. This center, SFI MOVE (Marine Operations in Virtual Environments), works with how future maritime operations may look through the use of digital twins, machine learning and control centers on land," she said. "I'm studying how targeted guidelines, training and risk communication can be developed for maritime cyber security. I am also investigating what tools we should develop to handle new cyber risks we may experience at sea."

Erstad, on the other hand, is looking at cyber resilience at sea.

"I'm looking at the best way that navigators can be resistant to, prepare themselves for, and overcome, cyber attacks against the integrated navigation systems on board the ship," he said.

Erstad says the researchers have benefitted from working with researchers at the Cyber SHIP lab at the University of Plymouth in England, which also works with maritime cyber security.

To practice realistic actions and situations in a safe environment, NTNU has opened a Cyber Range, (in Norwegian) especially developed for the maritime sector. The Cyber Range enables practitioners and researchers to uncover vulnerabilities in maritime navigation and control systems for ships.

Simulated event

The larger course exercise relied on ship simulators at NTNU in Ålesund. These simulators are also unique in their design when it comes to realism. The participants took their seats in ship simulators, designed like a bridge on a larger ship underway in the North Sea.

"We make the simulator scenario close to what actually happens on a ship, as well as to what happens in the communication between the ship and the land. But even though the scenario uses full-scale maritime bridge simulators, the focus was mostly on getting a good discussion going," Erstad said.

The exercise also included participants from DNV, the marine underwriters the Norwegian Hull Club, NORMA Cyber, Solstad, public institutions such as the Norwegian Coastal Administration and the Inland Norway University of Applied Science, as well as from the University of Plymout, who were invited in as observers and as resource persons in the simulation.

"We learn the most from the dialogue between the actors in the rehearsal and in the review afterwards, not least because you can then see what was practiced and the event itself from another point of view," says Erstad.

Strengthening the weak link

Professor Kevin Jones heads the Maritime Cyber Threats Research Group and Cyber SHIP lab at the University of Plymouth. He points out that a cyber attack can pose huge problems for the global economy and trade.

"When the large container ship 'Ever Given' ran aground in the Suez Canal, the cause was the weather and wind. Although this was not a cyber attack, the incident illustrates the consequences that can affect a vulnerable global system," Jones said.

Ninety percent of world trade is predicted to be linked to maritime transport, through maritime supply chains. It's entirely believable that a similar incident could occur due to digital vulnerabilities, as a result of unauthorized access to computers and control systems.

"The weak link is the human being, and we have to strengthen this link. Humans are the resource on board that can handle such a situation," Jones said.

Adapt skills development

The exercises and the specific course with the participants, helpers and observers have strengthened the two Ph.D. candidates' view that it is important to adapt skills development to the precise circumstances at hand.

The course offers a clear practical approach to risk management in a digital perspective. This is also included as part of NTNU's master's program in operational maritime management.

"It is important that businesses in the maritime sector familiarize themselves with their values, the digital threats and vulnerabilities they have. Managers need to know their employees will be able to handle the digital threats, and understand the needs they have for skills in working with digital security," Jones said.

The next course in Maritime Digital Security is planned for autumn this year. The offer will then be tailored to an even greater extent for managers, middle managers, operational (sailing) and administrative personnel in the maritime sector, but will also be very useful for other industries.

Related research has been published in the *WMU Journal of Maritime Affairs*.

More information: Erstad, E. et al. A human-centred design approach for the development and conducting of maritime cyber resilience training, *WMU Journal of Maritime Affairs* (2023). DOI: 10.1007/s13437-023-00304-7. link.springer.com/article/10.1 … 7/s13437-023-00304-7

Provided by Norwegian University of Science and Technology

Citation: What do you do if a hacker takes over your ship? (2023, March 22) retrieved 5 May 2024 from https://techxplore.com/news/2023-03-hacker-ship.html