Why 50,000 ships are so vulnerable to cyberattacks

The world’s shipping industry is vast and spans the globe. But it’s not just a network of vessels. It’s a network of systems that control those vessels. These systems are increasingly connected to the internet, and that makes them vulnerable to cyberattacks.

The problem is that ships are complex systems. They have many different components, and those components need to work together for the ship to function properly. But this complexity also makes it difficult to manage cybersecurity. For example, there are many different classes of vessels, all of which operate in very different environments.

The U.S. Coast Guard (USCG) oversees approximately 800 ports and inlets. They are responsible for regulating maritime security, which includes cybersecurity. But the standards for cybersecurity are not consistent across different sectors. For example, the healthcare industry has strict cybersecurity regulations, but those regulations are not necessarily applicable to the maritime industry.

This is a problem because ships are not just vessels. They are also part of the overall supply chain, and they interact with many other systems. For example, ships transport goods from one place to another, and they must be able to communicate with other systems along the way. If a ship is hacked, the entire supply chain could be disrupted.

The story so far

In 2014, the IMO consulted their membership on what maritime cybersecurity risks were. They identified five key areas:

1. Piracy
2. Piracy
3. Piracy
4. Piracy
5. Piracy

The IMO then worked with member states to develop a set of guidelines for maritime cybersecurity. These guidelines were adopted in 2016, and they include recommendations for how to manage cybersecurity in the maritime industry.

In 2017, the IMO amended two of their general security management codes to explicitly include cybersecurity. These codes are designed to help ship operators manage cybersecurity risks. But the guidelines are not enough. The IMO must also work with member states to ensure that they are implementing these guidelines.

Conclusion

The maritime industry is complex, and its cybersecurity is equally complex. But the IMO and other organizations must work together to ensure that the maritime industry is protected from cyberattacks. This will require a coordinated effort between governments, industries, and organizations.

Alexandersonscc/pixabay, CC BY-SA