Kontakt

Weststraße 4
57392 Schmallenberg

P : 02972 96396-01

M : 0173 8253824

E : b.richter@cybercomplete.de

w : www.cybercomplete.de

Maritime **Sicherheit**

Unser
Unternehmen

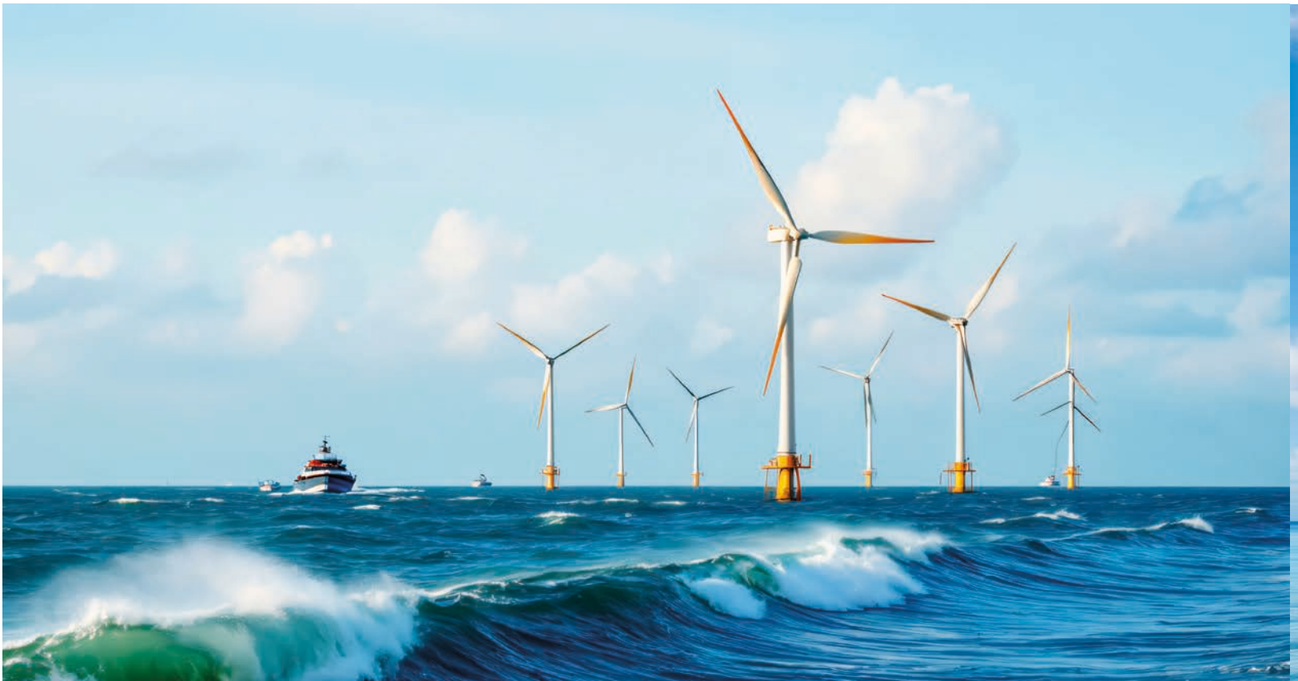
Das Team der Cyber Complete GmbH versteht die Informationssicherheit als ganzheitlichen Ansatz und eine der wichtigsten Säulen in heutigen Unternehmen. In der Industrie- und Wirtschaftswelt des 21. Jahrhunderts ist inzwischen eine Vernetzung und Globalisierung gegeben, die eine Cybersicherheit für Unternehmen, Konzerne und Privatpersonen unabdingbar macht und eine Grundvoraussetzung für ein erfolgreiches Wirken ist. Täglich erfolgen aus allen Winkeln des Globus unzählige Hackerangriffe und Versuche, in die Systeme von Firmen einzudringen – die Tendenz ist weiter steigend. Auch politische Institutionen und ganze Regierungen sind von diesen Entwicklungen betroffen, besonders wenn es dabei um sensible und besonders schützenswerte Inhalte und Daten geht.

Inhaltsverzeichnis

Offshore
fällt unter NIS-2

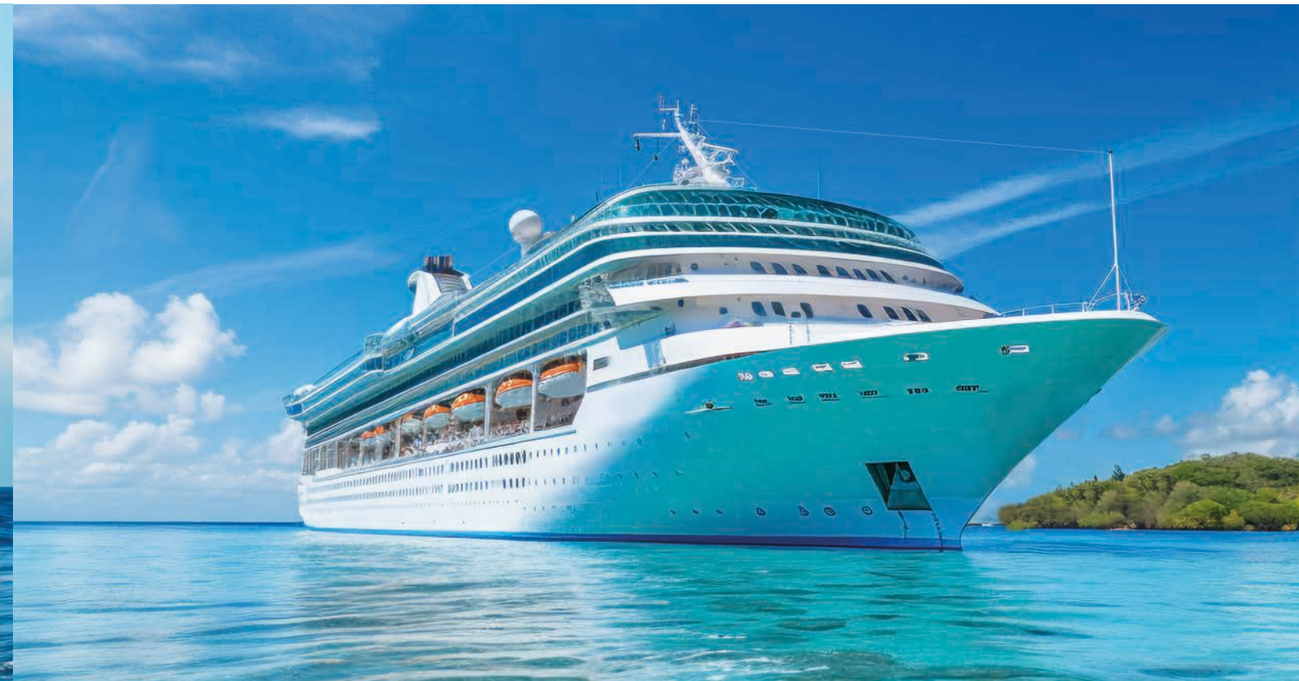
Die NIS-2 (Network and Information Systems Security) ist eine EU-Richtlinie, die die Cybersicherheit in kritischen Infrastrukturen (KRITIS) stärkt. Sie legt verbindliche Sicherheitsanforderungen fest und sorgt für eine bessere Zusammenarbeit zwischen den Mitgliedsstaaten.

Die Regelung reagiert auf die zunehmenden Cyber-Bedrohungen und Angriffe auf kritische Infrastrukturen wie etwa Energie, Verkehr, Ernährung, Gesundheitswesen und Wasser. Sie soll die Resilienz dieser Systeme erhöhen und die Reaktionsfähigkeit bei Sicherheitsvorfällen verbessern.



Maritime Infrastrukturen
- Besondere Herausforderungen

KRITIS-Betriebe sind essenziell für das Funktionieren unserer Gesellschaft. Der Schutz dieser Versorgungsketten sichert nicht nur die eigenen Betriebe, sondern das Aufrechterhalten notwendiger Systeme für eine funktionierende Volkswirtschaft.
Da dieser Bereich von den üblichen Sicherheits- und Versorgungssystemen auf dem Land abweicht, sind die verfügbaren Infrastrukturmöglichkeiten begrenzt. Jedoch muss nichtsdestotrotz ein angemessener Sicherheitsstandard gewährleistet werden, um den Schutz von Daten und Personal zu garantieren und die Resilienz wichtiger Systeme zu stärken.



Satellitenkommunikation & Richtfunkkommunikation

Die Geräte, die für die Kommunikation verantwortlich sind, sollten nicht nur physisch, sondern auch logisch (d.h. innerhalb der IT-Struktur) separat durch eigene Netzwerke von anderen internen Systemen getrennt werden, sodass im Falle einer Kompromittierung der Verbindung kein Einfallstor in andere Systeme der Anlage oder Steuerungen eines Schiffes gegeben ist.

IoT

IoT-Geräte erhalten oft, im Gegensatz zu den meisten anderen Endpunkt-Geräten, nach der Produktion keine Sicherheitsupdates, die potenzielle Schwachstellen in der Software beseitigen. Die Absicherung dieser anfälligen Geräte ist von höchster Wichtigkeit, um Angreifern keine Lücken zu präsentieren, die sie ausnutzen können.

Authentifizierung/ Zutrittskontrolle

Prozesse, die sichere Zugänge auf kritische Infrastruktur und Zugriffe auf sensible Programme und Daten regeln, sind dringend notwendig, um unautorisierte Eingriffe zu verhindern und interne Informationen und Dokumente vor Fremdzugriff, Manipulation oder Entwendung zu schützen.

SCADA Systeme

Meistens wird bei diesen Systemen von den Herstellern bereits eine geeignete graphische Aufbereitungssoftware angeboten. Aber diese bietet in den meisten Fällen keine tiefergehenden Sicherheitsfunktionen an und es muss eine angemessene Lösung implementiert werden, um diesen Bereich abzudecken.

BCM

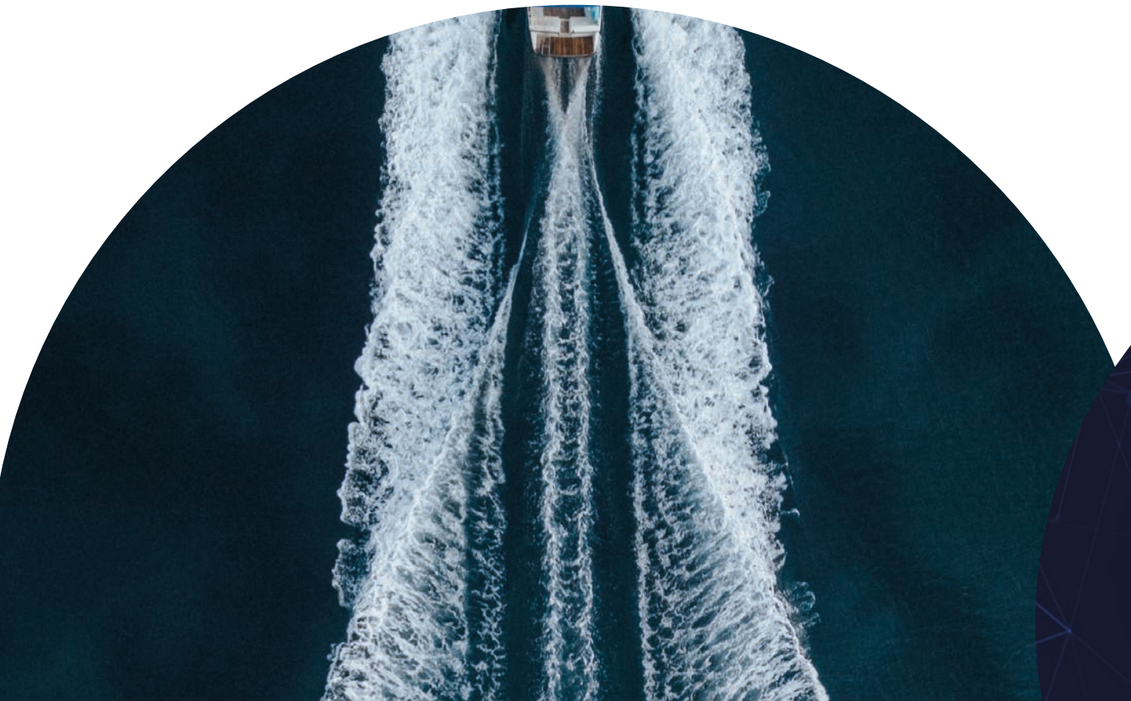
Ein Business Continuity Management stellt sicher, dass trotz Störungen und Zwischenfällen die Funktionalität kritischer Systeme gewährleistet wird und Unterbrechungen des Betriebs so weit wie möglich unterbunden werden.

Verschlüsselung

Durch Verschlüsselung von sowohl Daten in der Speicherung als auch den Datenströmen während Transferprozessen werden Unbefugten der Zugriff auf und das Auslesen der enthaltenen Informationen erschwert

Bitte bedenken Sie, dass dies nur eine Zusammenfassung ist, die einen groben Überblick verleihen soll und nicht den vollen Umfang der notwendigen Maßnahmen darstellt.

Die Implementierung der Maßnahmen sollte mit professioneller Beratung durchgeführt werden.



Blick
in die Zukunft

Die maritime Sicherheit ist ein wichtiger Aspekt der globalen Sicherheit, da der größte Teil des internationalen Handels über den Seeweg abgewickelt wird. Hier sind einige Trends und Entwicklungen, die die maritime Sicherheit in der Zukunft beeinflussen könnten:

Terrorismus

Die Bedrohung durch terroristische Angriffe auf Schiffe und Häfen bleibt bestehen. Der Austausch von Informationen zwischen Ländern und Organisationen kann helfen, Bedrohungen frühzeitig zu erkennen und zu verhindern.

Zunehmende Komplexität

Die zunehmende Komplexität der globalen Lieferketten und die wachsende Abhängigkeit von Technologie eröffnen neue Angriffsmöglichkeiten für Kriminelle und Terroristen.

Die Satelliten-überwachung

Die Satellitenüberwachung kann die maritime Sicherheit verbessern, indem sie eine bessere Überwachung von Schiffsverkehr und Häfen ermöglicht.

Autonome Schiffe

Die Entwicklung autonomer Schiffe kann die maritime Sicherheit verbessern, indem sie die Anzahl der menschlichen Fehler reduziert.

Blockchain Technologie

Die Anwendung von Blockchain-Technologie in der maritimen Sicherheit kann helfen, die Integrität von Lieferketten und die Authentizität von Gütern zu gewährleisten.

Künstliche Intelligenz und maschinelles Lernen

Die Anwendung von künstlicher Intelligenz in der maritimen Sicherheit kann helfen, Bedrohungen frühzeitig zu erkennen und zu verhindern.

Die Zukunft der maritimen Sicherheit wird von technologischen Entwicklungen, internationaler Zusammenarbeit und der Anpassung an neue Bedrohungen geprägt sein.