IT Sicherheit

zur digitalen Widerstandsfähigkeit

(Ausfallsicherheit, Zuverlässigkeit)

Morris Becker

Juni 2024

Erfolgreiche Cyberangriffe der Vergangenheit und Gegenwart

WARUM waren/sind Angriffe erfolgreich?

Keine guten Lösungen?
Keine guten Dienstleister?
Zu wenig in Cyber Security investiert?
Hat Cyber Security keine ausreichende Wichtigkeit?

Ist die Cyber Security zu komplex?
Ist die Transparenz der Angriffsfläche und des Risikos zu gering?
Liegt der Fokus zu sehr auf Erkennung und anschließender Abwehr?

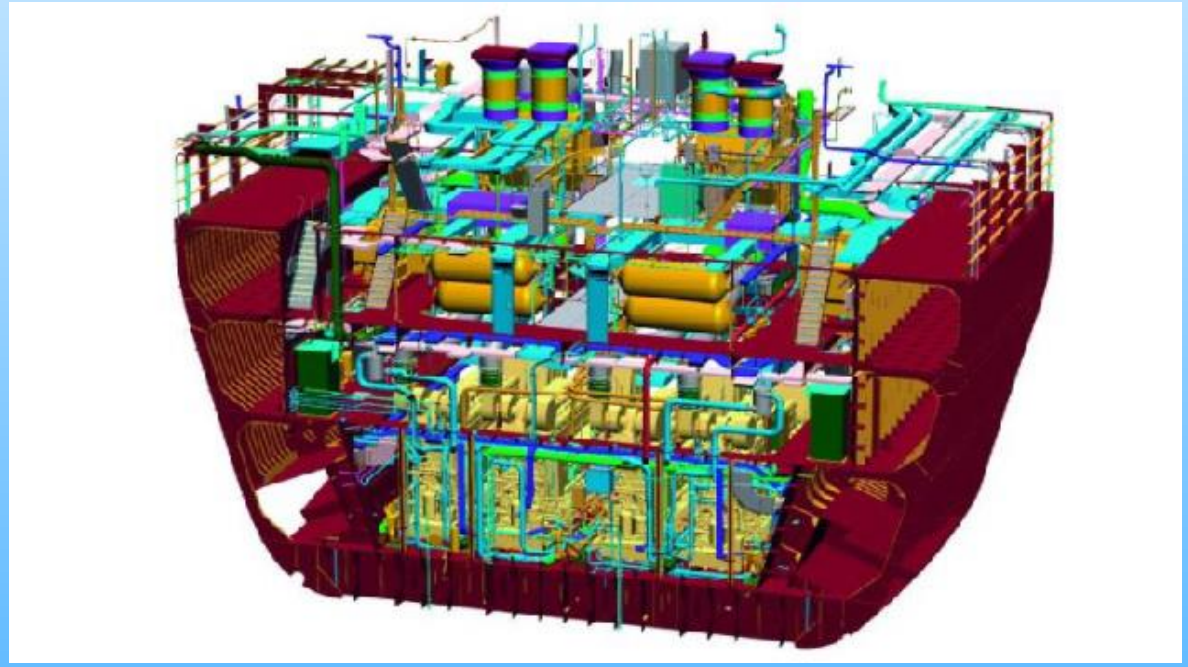
>90% der erfolgreichen Angriffe waren vermeidbar mit vorhandenen Mitteln.

Was war mit der Prävention?

Aktueller Fokus meist zu sehr auf Erkennung

Erkennung (z.B. SIEM – SOC 1.0)

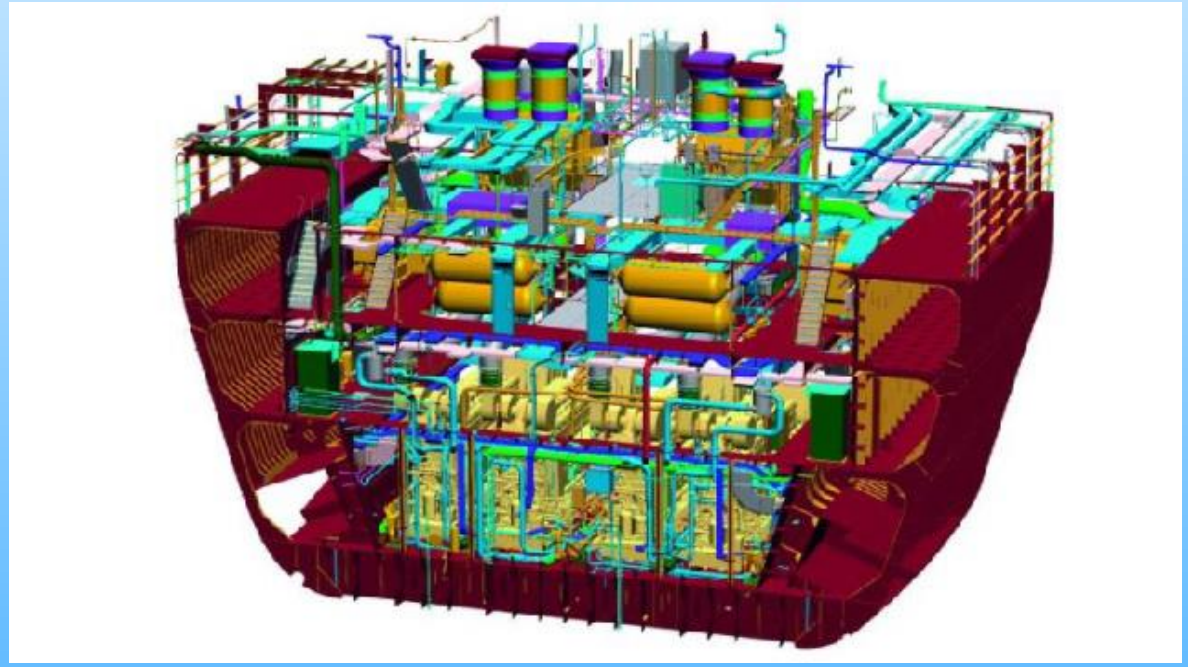
- Wassereinbruch möglichst frühzeitig erkennen.
- Ort des Einbruchs möglichst Präzise melden.
- Methode zur Behebung kennen.
- Behebung möglichst schnell ausführen.
- Schaden abwehren/minimieren.



Aktueller Fokus meist zu sehr auf Erkennung

Erkennung (z.B. SIEM – SOC 1.0)

- Wassereinbruch möglichst frühzeitig erkennen.
- Ort des Einbruchs möglichst Präzise melden.
- Methode zur Behebung kennen.
- Behebung möglichst schnell ausführen.
- Schaden abwehren/minimieren.

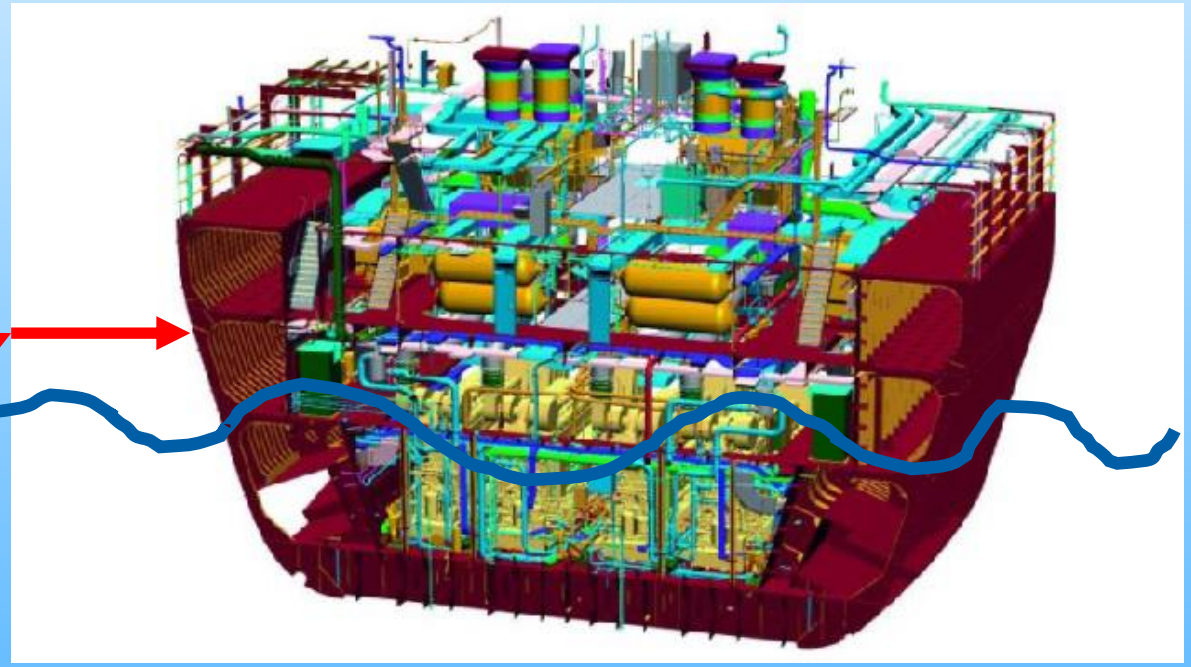


Aber wo liegt der Schwachpunkt?

Aktueller Fokus meist zu sehr auf Erkennung

Erkennung (z.B. SIEM – SOC 1.0)

- Wassereinbruch möglichst frühzeitig erkennen.
- Ort des Einbruchs möglichst Präzise melden.
- Methode zur Behebung kennen.
- Behebung möglichst schnell ausführen.
- Schaden abwehren/minimieren.



Wer erkennt das Leck oberhalb der Wasserlinie, bevor das Schiff beladen wird?

Deshalb: Prävention **VOR** Erkennung und Abwehr

Prävention (SOC 2.0 / SIEM + Continuos Exposure Management)

- Wie dick sind die Bordwände?
- Wie weit ist die Korrosion fortgeschritten?
- Wie ist die Qualität der Schweißnähte?
- In welchem Zustand sind die Nieten?
- Welchen Weg kann das Wasser nach eine Beladung gehen?
- Welche Auswirkung hat die Veränderung des Struktur?

Das Leck vermeiden bevor es erkannt und gestopft werden muss!

Best Practises und Richtlinien – Prävention ist ein Prozess

- Branchen wie Banken und Energieversorger sind Vorreiter
- NIS 2 erweitert die Anforderungen
  - z.B. um Risikomessung und Nachweis von Maßnahmen zur Minimierung

- **Vgl. kontinuierliches und automatisches Abarbeiten von Checklisten, z.B.**
- Tresor steht nicht für jedermann zugänglich an der Straße? ✓
- Raum des Tresors ist mit einem Schloss gesichert? ✓
- Alarmanlage vorhanden + eingeschaltet? ✓
- Code des Tresors komplex und nicht leicht zu erraten? ✓
- Tresor feuerfest? ✓
- Tresor nicht einfach wegzutragen? ✓
- Wird der Weg zum Tresor durch neue Baumaßnahmen nicht verkürzt? ✓
- Ist bekannt, wer Zugang zum Tresorraum hat? ✗
- Boden, Decke, Wände nicht durchbohrbar? ✗