CycleSEC®

Security is a Process, not a Project!

Vorstellung

Aktuelle Tätigkeit:

→ CycleSEC-Gründer und Geschäftsführer
→ Fachbuchautor (Springer/Beuth)
→ Kursautor/Tutor Wilhelm Büchner Hochschule
- „Grundlagen der IT-Sicherheit“
- „Faktor Mensch in der Informationssicherheit“

CycleSEC

Was machen wir heute

CycleSEC®

#1

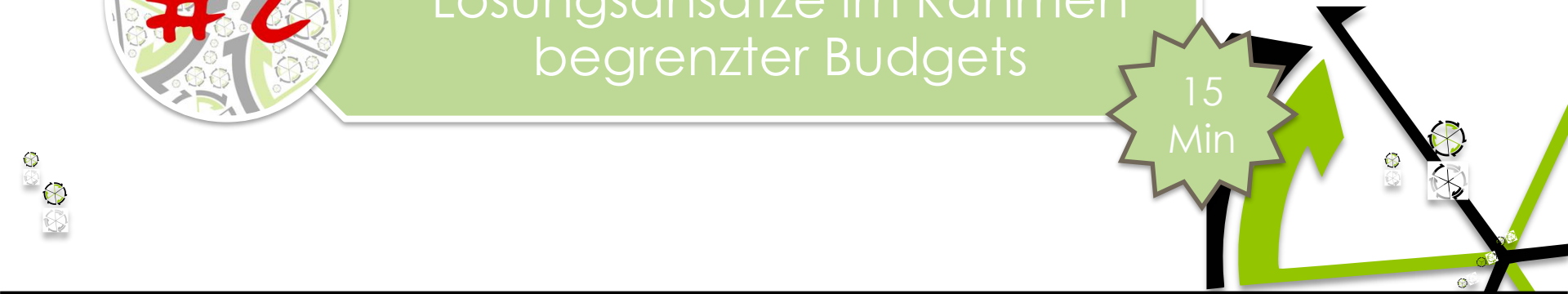
Cyber Security auf Schiffen: Angreifbarkeit von GPS, ECDIS, AIS, INMARSAT und Co.

30 Min

#2

Auf Kurs bleiben: Lösungsansätze im Rahmen begrenzter Budgets

15 Min



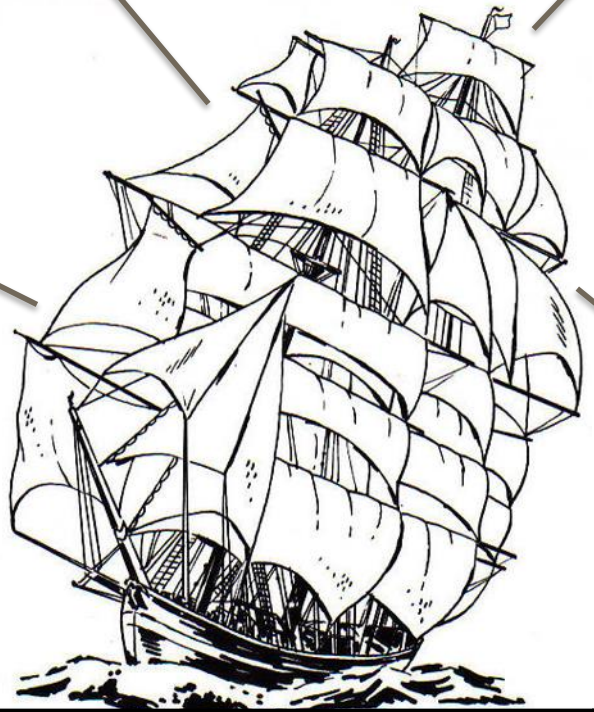
Wandel der Bedrohungslage

CycleSEC®

Cyber-Piraten

Schwindende räumliche Distanz durch Digitalisierung

gehackte Schiffe



Just-in-Time-Logistik

Industrie 4.0 an Land

CycleSEC®

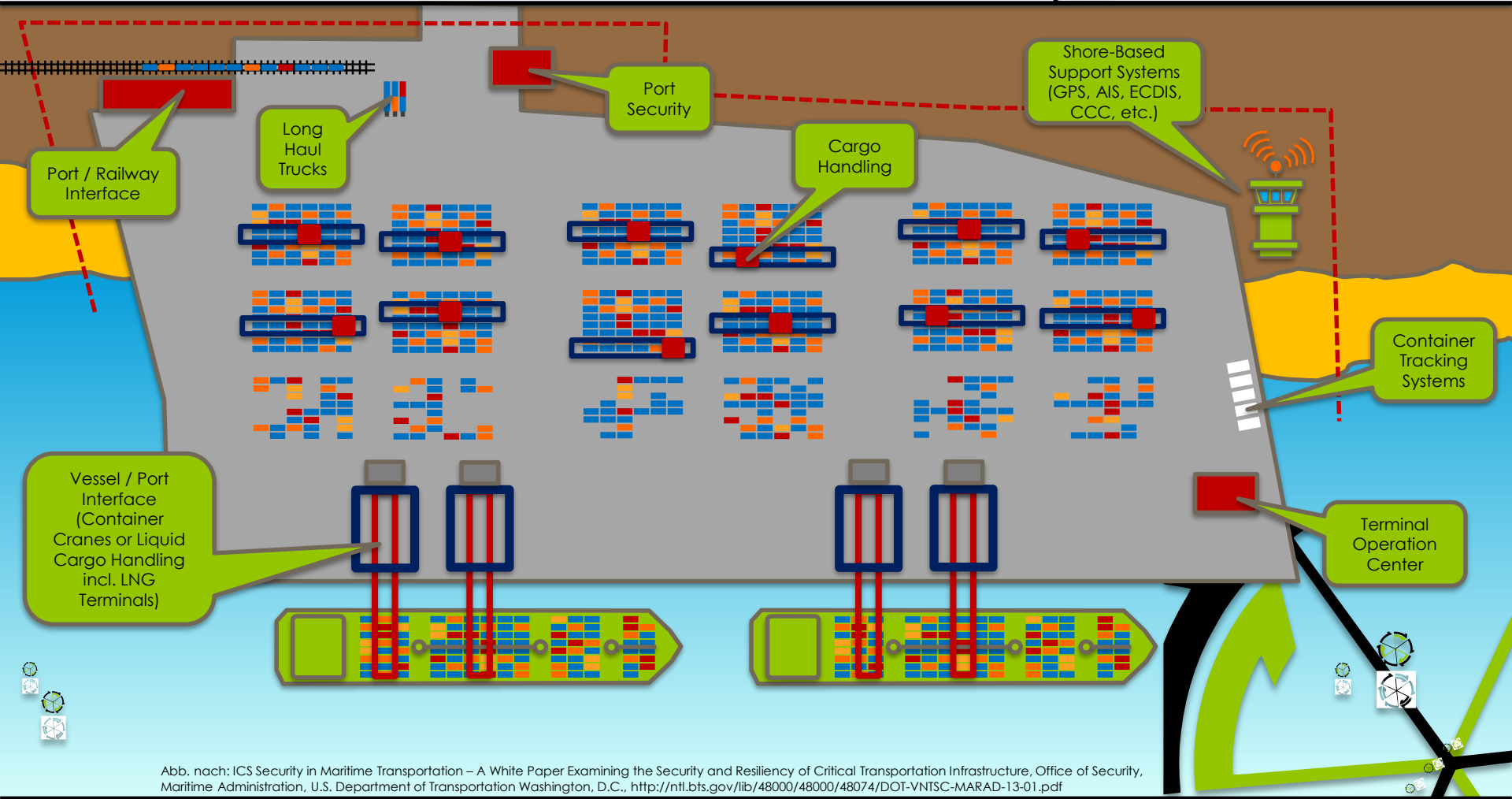


Abb. nach: ICS Security in Maritime Transportation – A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure, Office of Security, Maritime Administration, U.S. Department of Transportation Washington, D.C., http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf

Industrie 4.0 an Bord

CycleSEC®

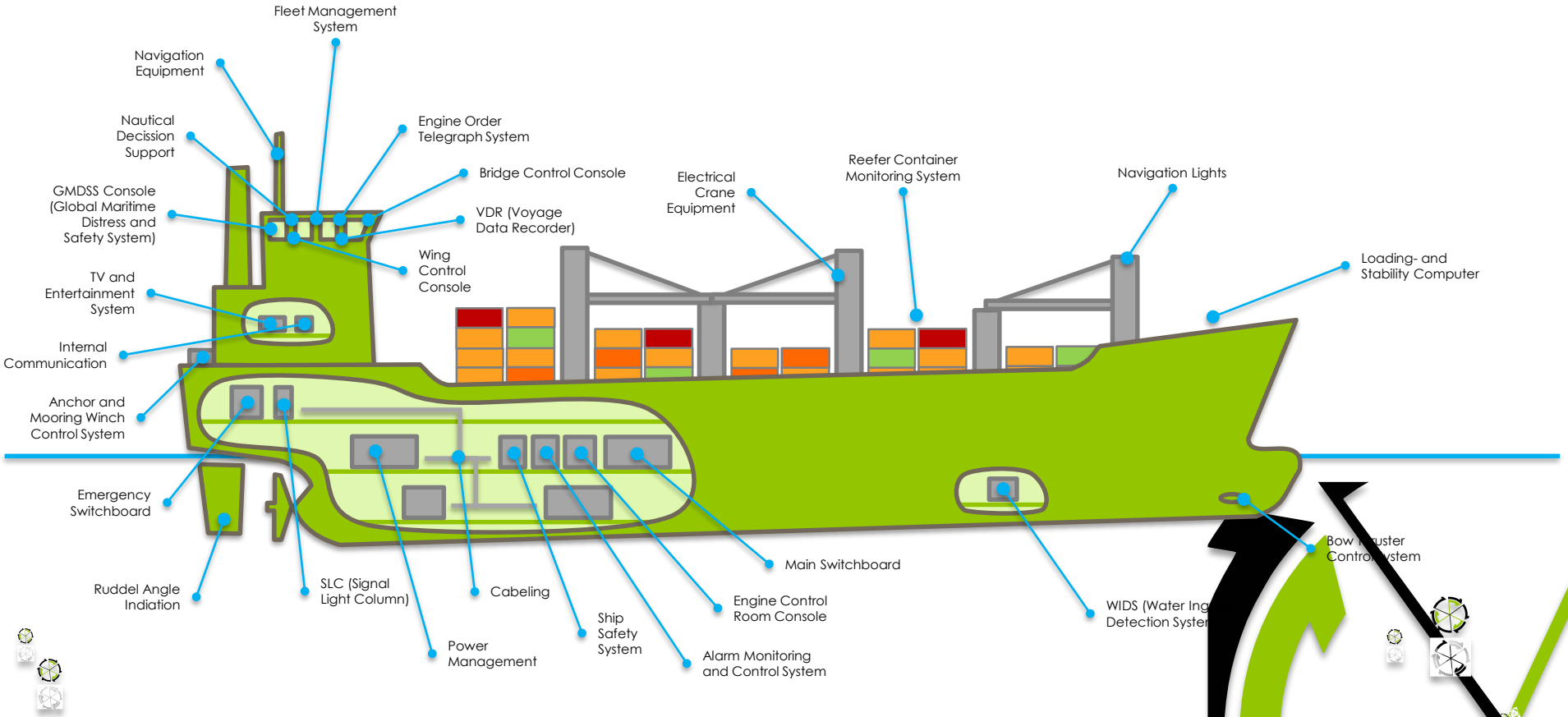
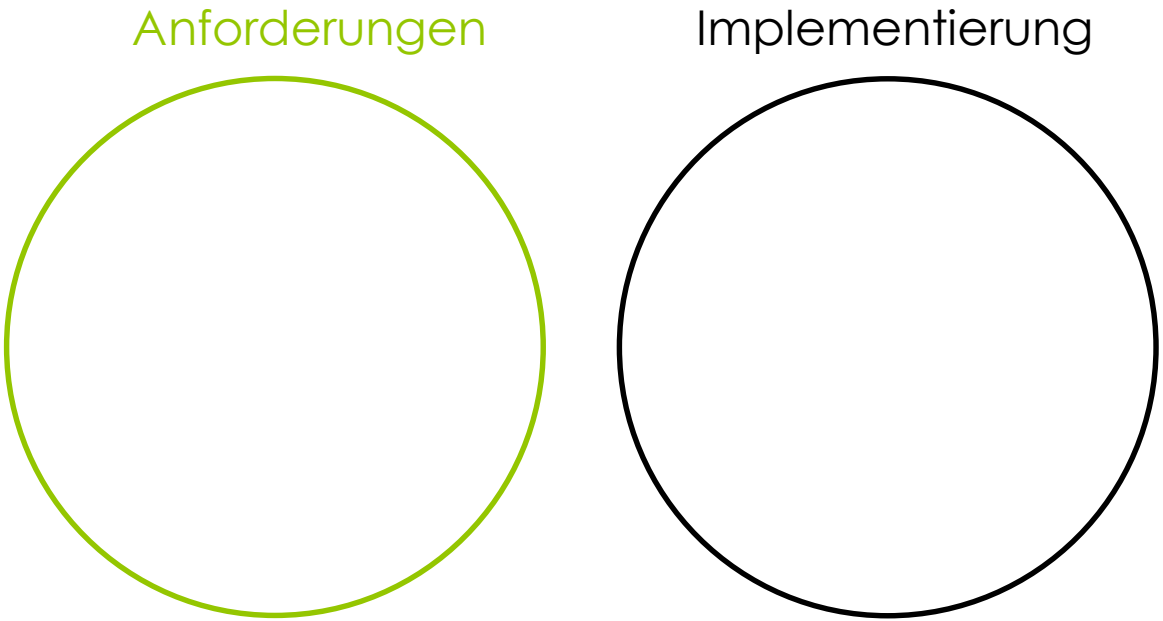
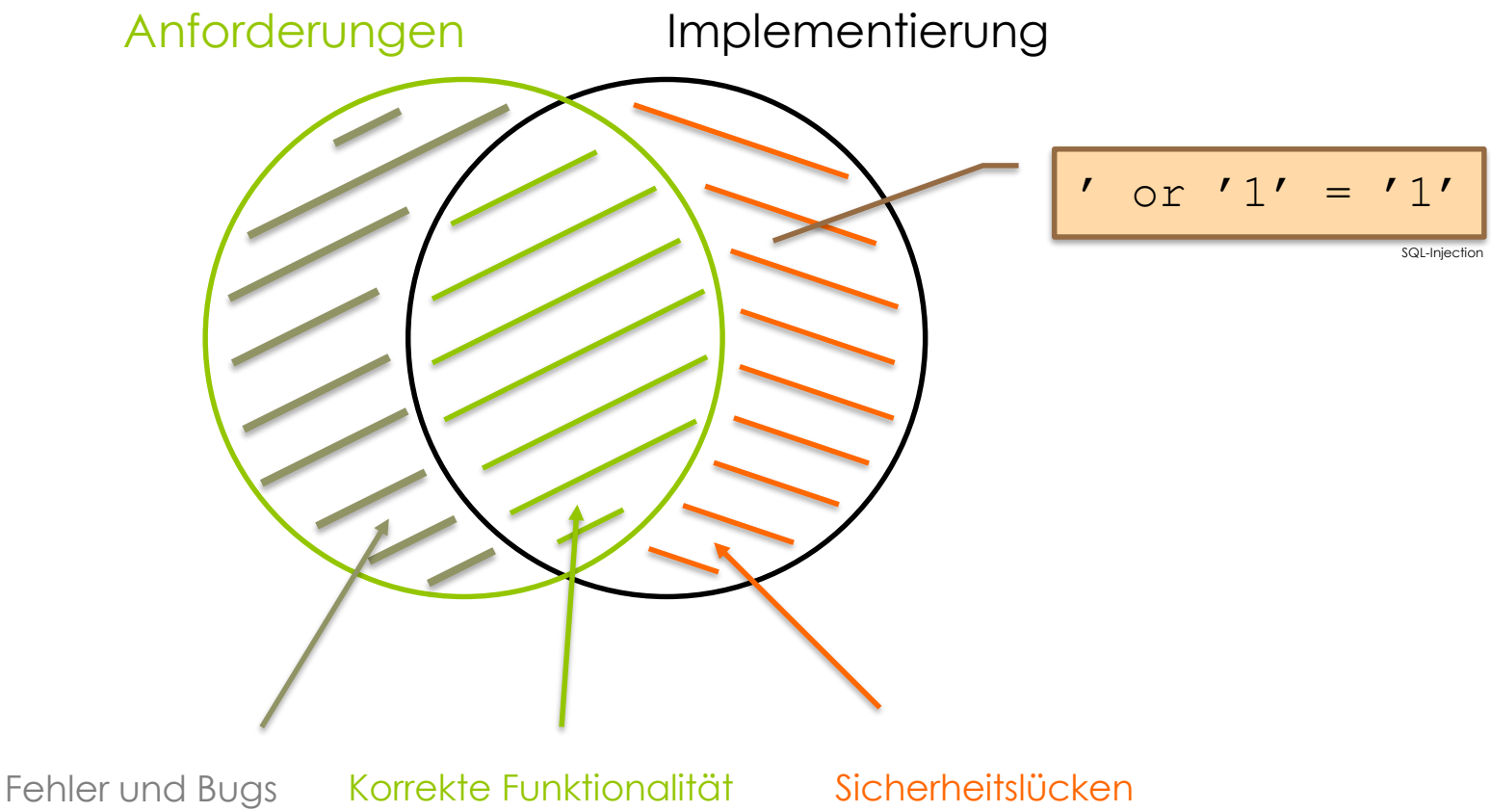


Abb. nach: ICS Security in Maritime Transportation – A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure, Office of Security, Maritime Administration, U.S. Department of Transportation Washington, D.C., http://ntl.bts.gov/lib/48000/48000/48074/DOT-VNTSC-MARAD-13-01.pdf

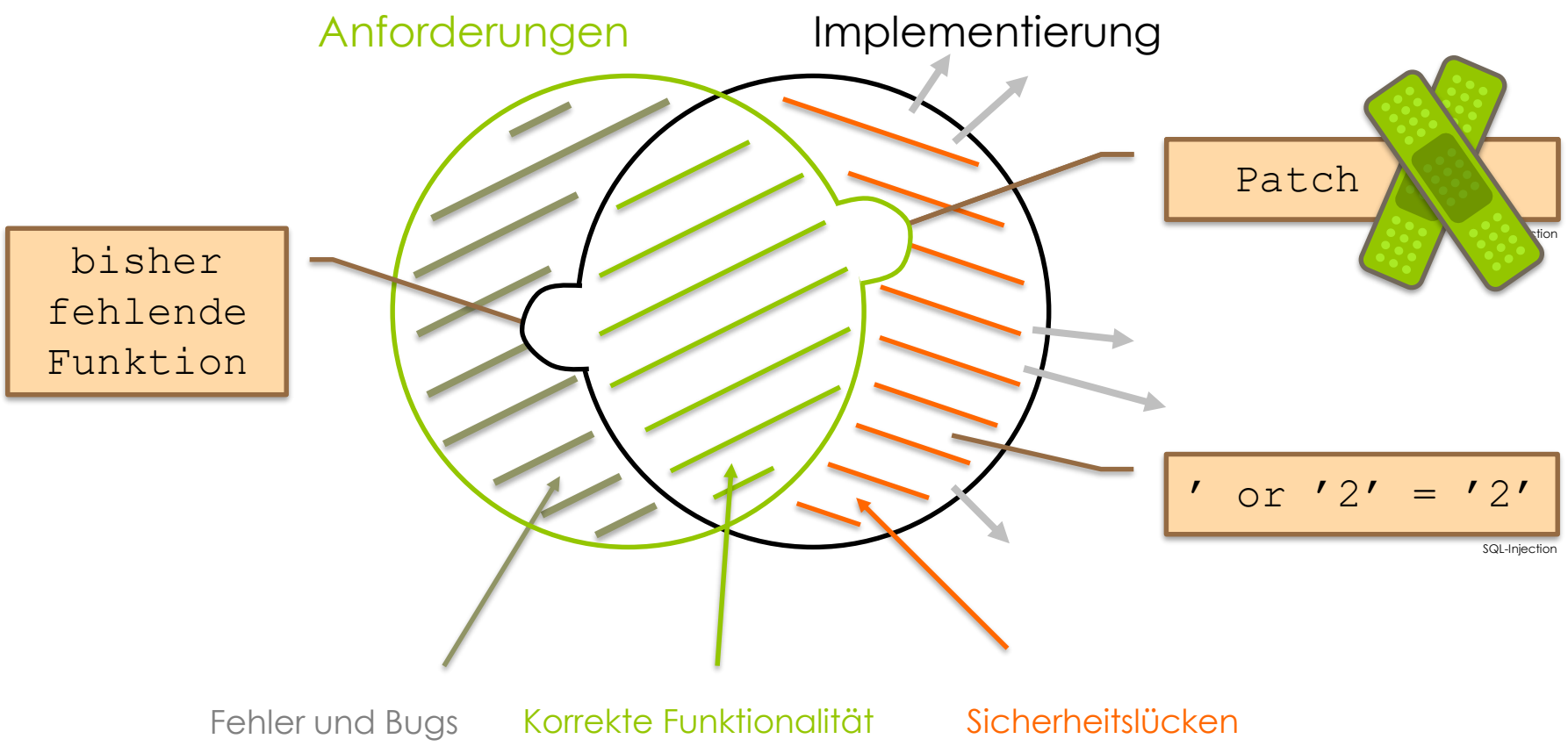
Was ist Software-Sicherheit?



Was ist Software-Sicherheit?



Was ist Software-Sicherheit?



Cyber Security auf Schiffen

MÖGLICHE ANGRIFFE

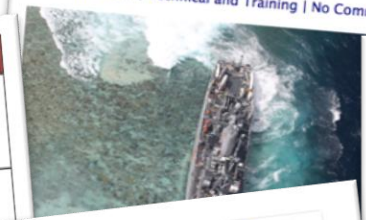
Überblick:

CycleSEC®

Vendor	Product	Vulnerability Class	Service	Severity
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobha		Insecure Protocols		
JRC				

ECDIS Update Kevin Vallance

February 24th, 2013 by JCB
Posted in Articles, Technical and Training | No Comments »



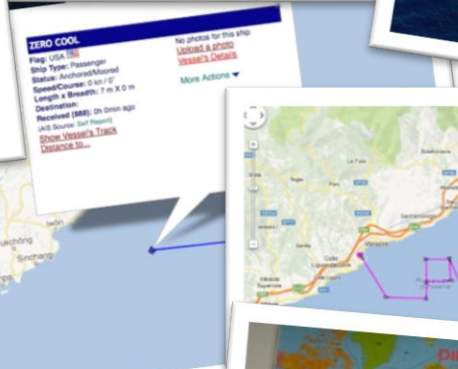
Follow

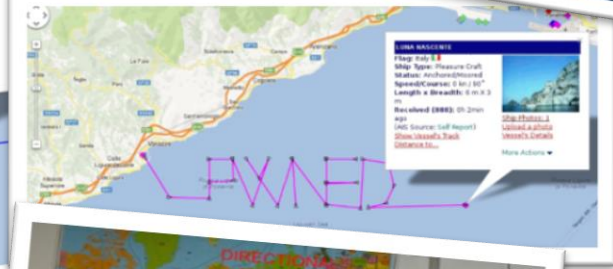
Chris Roberts
@Sidragon1

Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :)

Dan Tentler
@Viss

hey I found that yacht again. Looks like it's a 'demo syste
... and its exploding.





Sea Pirates Hacked Shipping Company to Plan Attacks, Find Valuable Cargo

Sea pirates hire hacker to break into shipping company's CMS

Mar 2, 2016 22:05 GMT · By Catalin Cimpanu

A curious case reported by Verizon's RISK
those lowly sea pirates
Kalashnikovs
up their profits

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

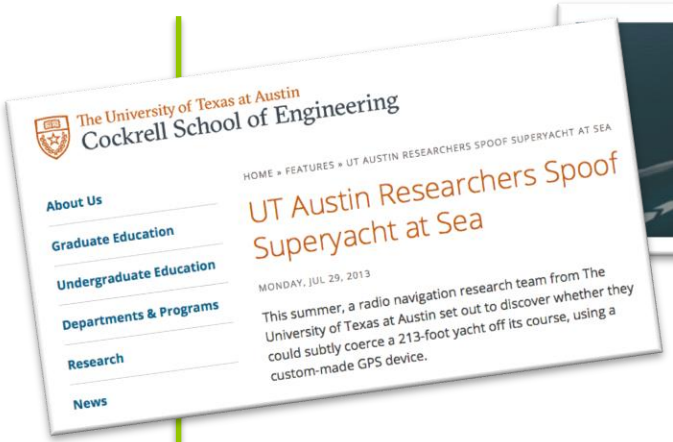
the Tor Browser at "https://www.torproject.org/". If you need
lease google for "access onion page".
e of the following pages with the Tor Browser:

petya37h5tbhyvki.onion/N19fvE
petya5koahtsf7sv.onion/N19fvE

ur personal decryption code there:

If you already purchased your key, please enter it below.

Key:



GPS-Spoofing einer Luxusyacht

80 Mio. $ Schiff, 56m lang

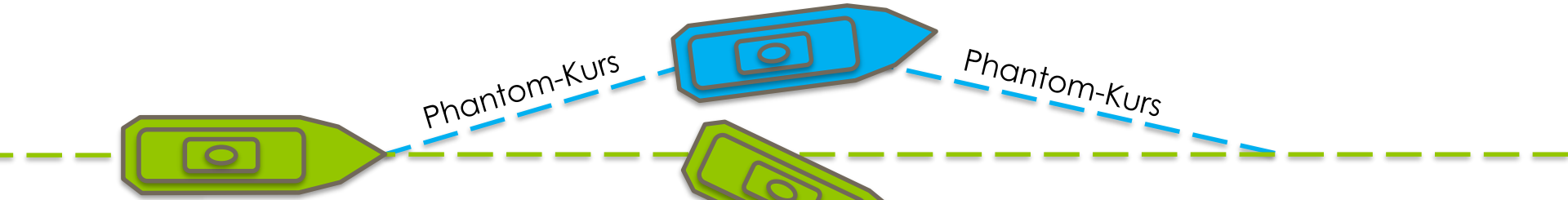
- Forschungsarbeit der University of Texas at Austin
  - Juli 2013
  - Durchgeführt von zwei Studenten
- Kursmanipulation durch gefälschtes GPS-Signal
  - Kursänderung um 3°
  - Angriff durch das Schiff nicht zu detektieren
  - Angreifer müssen in der Nähe des Schiffs sein

Bildquelle: University of Texas at Austin, http://www.engr.utexas.edu/features/superyacht-gps-spoofing

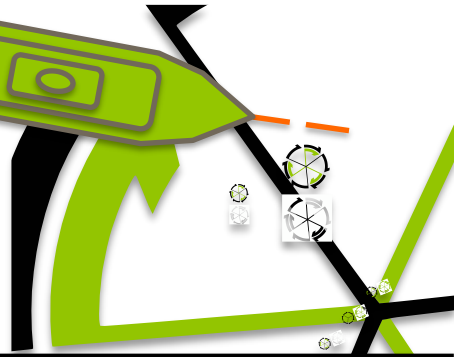
So funktioniert der Angriff

Ziviles GPS-Signal
des Satelliten

Ziviles GPS-Signal
des Satelliten



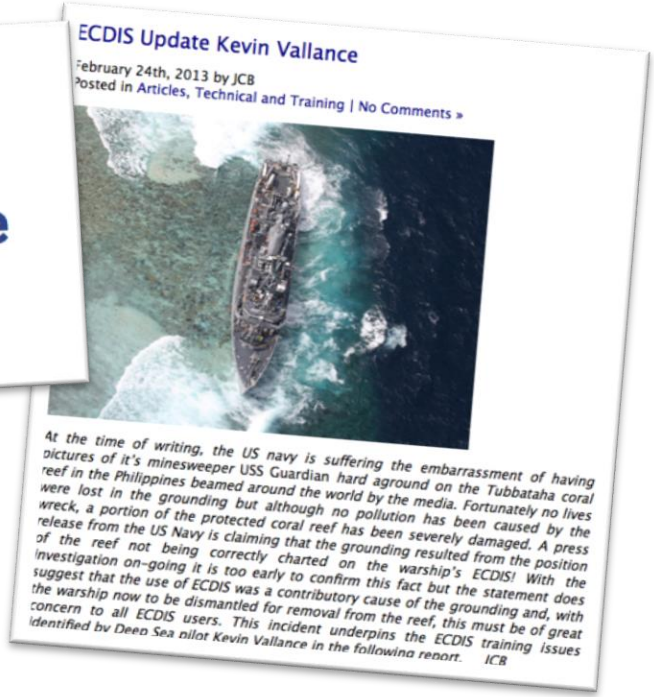
Stärkeres GPS-Signal
des Angreifers



Integrierte Brücken:
Chance oder Risiko?

Schwachstellen im ECDIS

Electronic Chart Display and Information System



- u.A. falsche ECDIS-Daten lassen US Kriegsschiff auf Grund laufen
- Paper zur ECDIS Manipulation von NCC Group

Quellen: http://www.pilotmag.co.uk/2013/02/24/ecdis-update-kevin-vallance/#more-6557
https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf

Piraten setzen „Hacker“ auf Schiffe an

http://cycl.sc/o5lj-

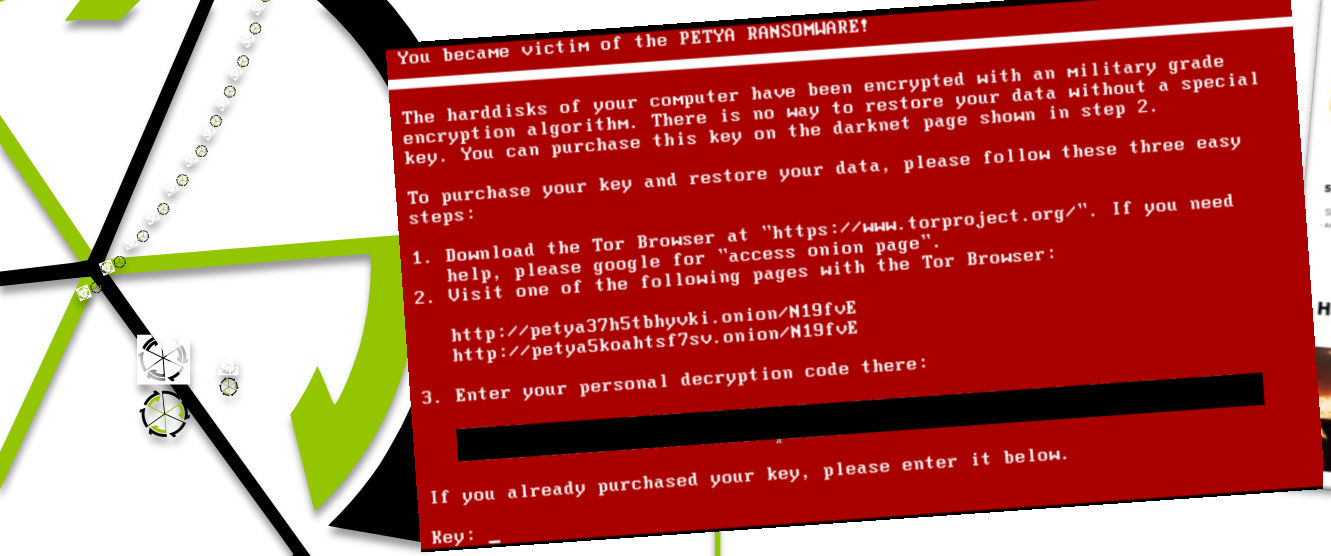
Sea Pirates Hacked Shipping Company to Plan Attacks, Find Valuable Cargo

Sea pirates hire hacker to break into shipping company's CMS

Mar 2, 2016 22:05 GMT · By Catalin Cimpanu

A curious case reported by Verizon's RISK Team shows that even those lowly sea pirates chasing after cargo ships with old Kalashnikovs in worn-out dingies are resorting to hacking to boost up their profits.

- Piraten nutzen Hacker-Know-how
- Einbruch ins CMS des Reeders
- Schiff und Fracht wurden gezielt ausgewählt



Ransomware bei Maersk (Terminals und Reederei)

http://cycl.sc/45g3x

- Ransomware NotPetya
- 17 Terminals von APM
- Container Maersk Line
- 300 Mio. bilanzierter Schaden
- NotPetya war kein gezielter Hackerangriff sondern „leider Pech“

tichwort
Remote Access:
-Systeme
online verfügbar

http://cycl.sc/2iqem

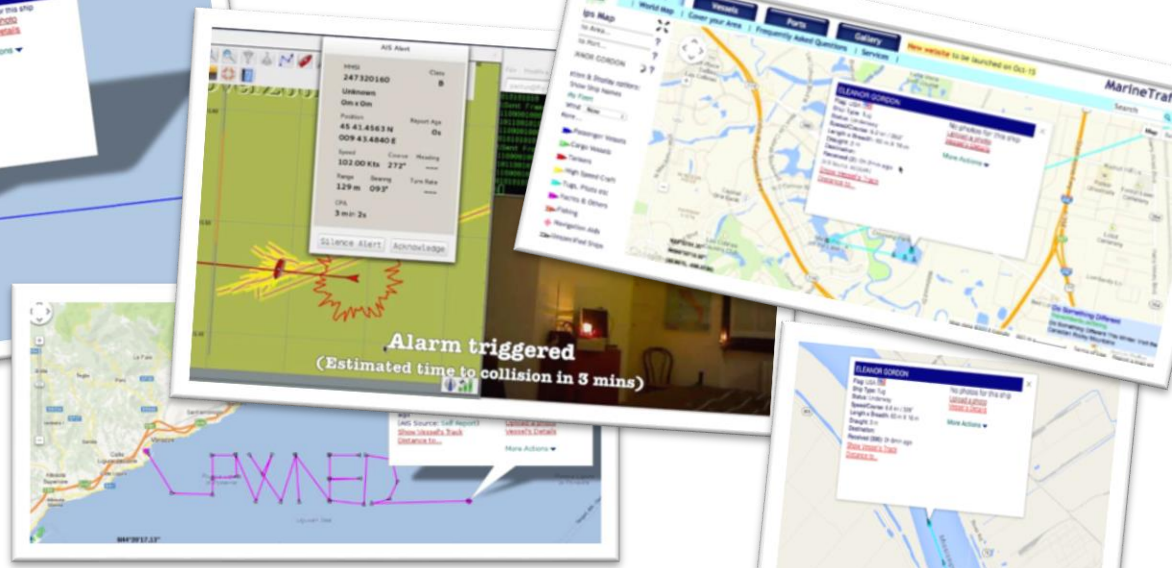
- auch auf Twitter immer häufiger im Gespräch

Bildquelle: Twitter

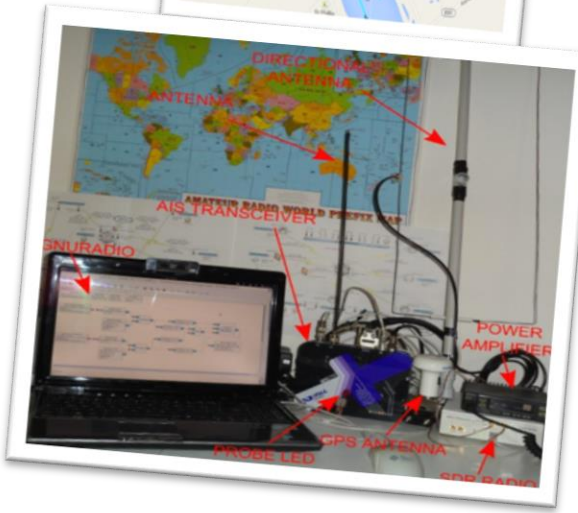
Schwachstellen im AIS System auf der Black Hat 2014

Automatic Identification System

Kosten des Equipments:
wenige 100 $

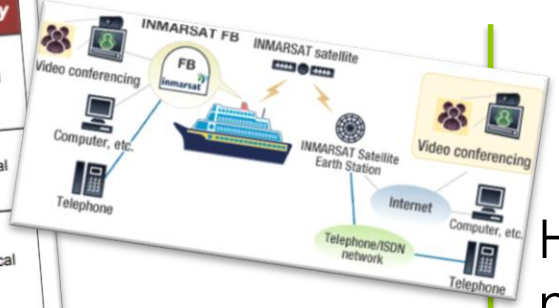


- AIS Online und via Transponder gebrochen!
  - Kollisionsalarme
  - SOS-Signale
  - Wetterberichte
  - Kursdaten



Quelle: https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf

Vendor	Product	Vulnerability Class	Service	Severity
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical



Hacks gegen maritim genutzte Satelliten-Terminals

Vorgestellt auf der
Black Hat 2014

Kompromittierung der Satelliten-Ve[illegible]ung gefährdet all[illegible]nge-schlossenen [illegible]steme

Dienste, die INMARSAT-Verbindungen nutzen:

- Telefon, SMS, VoIP, ViKo, Internet, Email, Daten
- Maritime Informationssysteme wie ECDIS und AIS
- Vessel Routing und Cargo Management
- Fernwartung
- Radio over IP (RoIP) und VHF/UHF Integration
- Crew Welfare und Telemedizin
- Online Training/ Zertifizierung
- Wetterberichte

Quelle: https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf

Cyber Security auf Schiffen

Übertragbare Angriffe auf Entertainment-Systeme

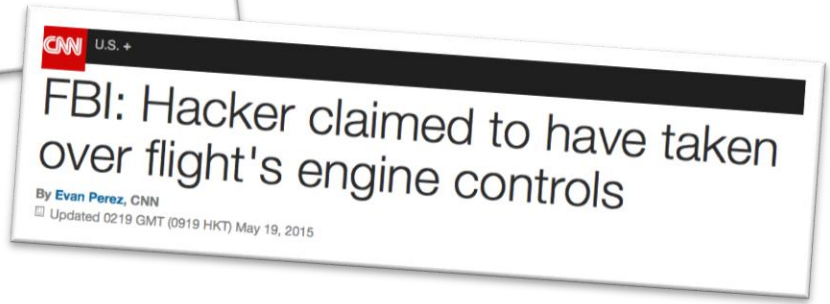
Rückruf von 1,4 Mio. Jeep Grand Cherokee

Totaler Kontrollverlust über das Fahrzeug

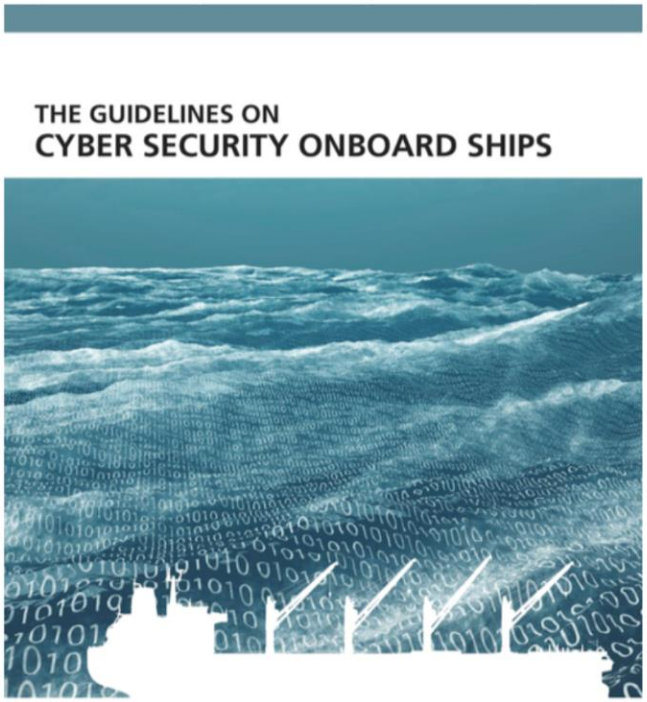
- Angreifer übernehmen die Steuerung
  - Juli 2015
  - Durchgeführt von zwei Hackern
- Angriff über Mobilfunkanbindung und Entertainment-System des Jeeps
  - Fernsteuerung der Hupe
  - Straffen des Gurtes
  - Eingriff in die Steuerung
  - Abgeschaltete Bremsen

„Fernsteuerung“ eines Passagierflugzeugs

Auch Zugriff auf die Triebwerkssteuerung



- Angreifer übernehmen Kontrolle
  - Mai 2015
  - Durchgeführt durch einen Passagier
- Angriff über Entertainment-System von 15 bis 20 Airbus und Boeing Maschinen
  - Erhöhung der Triebswerksdrehzahl
  - Kursänderung via Schubänderung
  - Aktivierung der Sauerstoffmasken
  - Zugriff auf Bordinformationssystem



Problem: Alles richtig

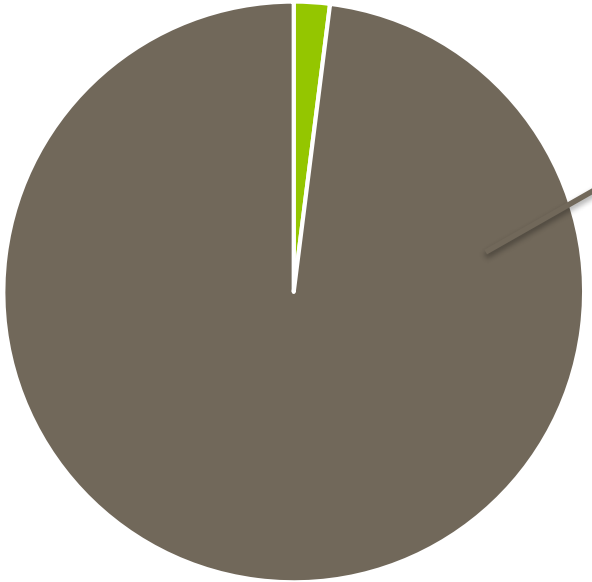
Cyber Security Onboard Ships

Table of Contents

„Maritime Sicherheit“ im Vergleich

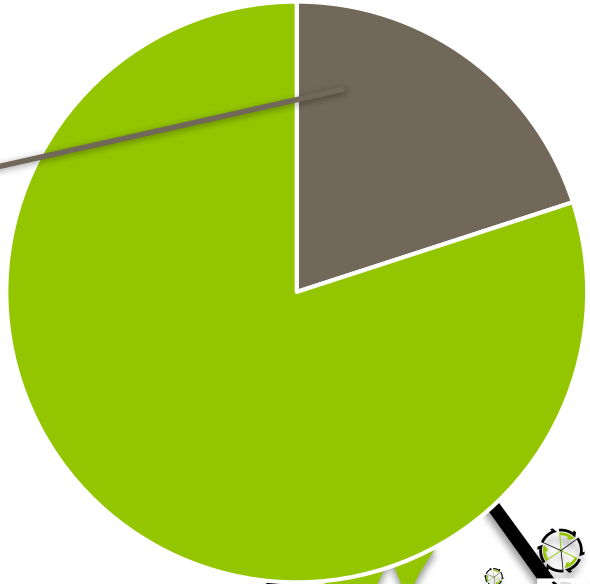
CycleSEC®

Maritime Sicherheit
(Veranstaltung des MCN
am 29.01.2018)



Safety und
physical
Security

Abteilung
Konzernsicherheit
(z.B. in einer Bank)



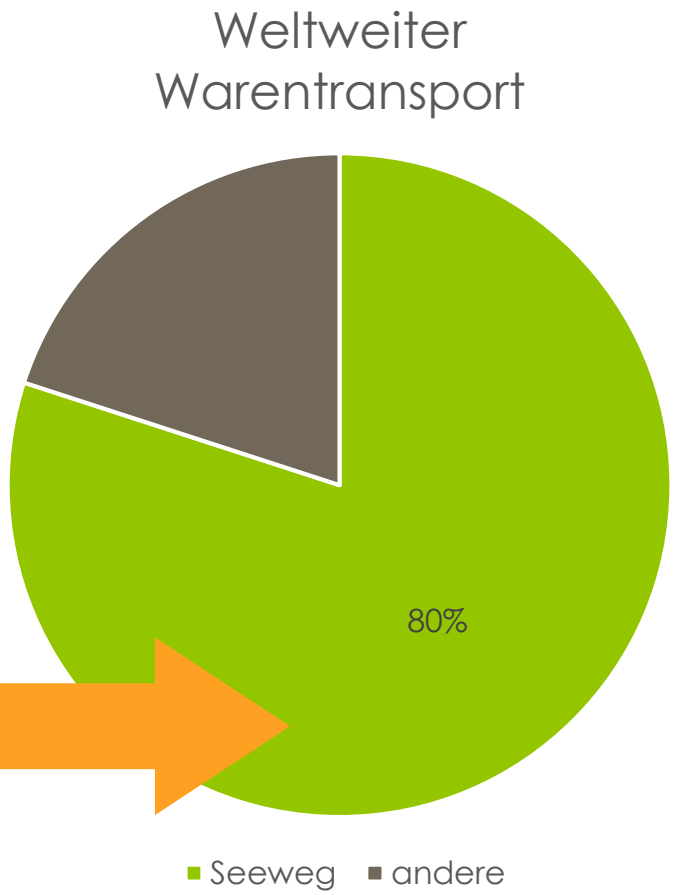
Cyber Security* „alte Security“

* i.S.v. Informationssicherheit, IT-Sicherheit und Cyber Sicherheit

Zeit für ein Ende der Illusionen

CycleSEC®

Wer 80% des weltweiten Warentransports IT-gestützt abwickelt und hochmoderne Schiffe baut, oder bereedert, der darf sich nicht nur auf die „alte Security“ fokussieren!



Zwischenstopp

CycleSEC®

#1

Cyber Security auf Schiffen: Angreifbarkeit von GPS, ECDIS, AIS, INMARSAT und Co.

#2

Auf Kurs bleiben: Lösungsansätze im Rahmen begrenzter Budgets

15 Min

Weiter geht‘s

CycleSEC®

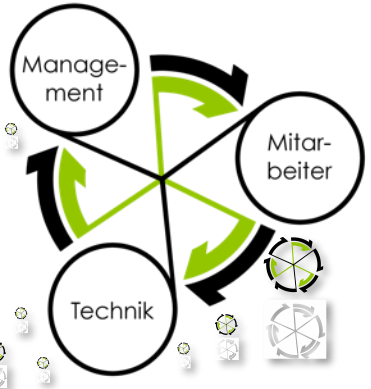
#1

Cyber Security auf Schiffen: Angreifbarkeit von GPS, ECDIS, AIS, INMARSAT und Co.

#2

Auf Kurs bleiben: Lösungsansätze im Rahmen begrenzter Budgets

15 Min



Was ist der Ausweg?

Problem: Alles richtig

- Berücksichtigung von Cyber Security bereits bei Planung und Design
  - z.B. Information Security Management
- Schulung von Besatzungen, Personal und Ingenieuren im Schiffbau
  - z.B. Präsenzschulungen
  - z.B. Awarenesskampagnen
- Gezielte Sicherheitsanalysen bestehender und geplanter Systeme
  - z.B. Simulierte Hackerangriffe (Penetrationstests)
  - z.B. Code- und Systemreviews

Beispiel: Ausbildung

CycleSEC®

Schulung sichere Softwareentwicklung (2 Tage)

Bei einem Schulungsanbieter

Pos.	EUR	Anz.	EUR
Teilnahmegebühr	1.200	×12	14.400
Reisekosten	500	×12	6.000
Summe	**1.700**	**×12**	**20.400**

Beispiel: Incident Management

CycleSEC®

Task-Force Sec-Ops I

10 Tage Forensik und CERT

Pos.	EUR	Anz.	EUR
Tagessatz (3 FTE)	1.600	×30	48.000
Reisekosten	1.000	×6	6.000
Summe			**54.000**

Beispiel: Incident Management

CycleSEC®

Task-Force Sec-Ops II

5 Einsätze Forensik und CERT

Pos.	EUR	Anz.	EUR
Kosten (150 PT)	54.000	×5	270.000
Summe			**270.000**

Situationsanalyse

CycleSEC®

Cyber-“Piraterie“…
…ist eine gemeinsame Existenzbedrohung.

Internationaler Wettbewerb…
…ist die gemeinsame Konkurrenz.

Regionale Zusammenarbeit…
…ist dringend nötig und möglich.

Aus der Geschichte lernen!

Rückblick: „Convoy-Zoll“

CycleSEC®

Hamburger Convoischiffe

Piraterie zu Beginn des 17. Jahrhunderts

1623 Gründung der Admiralität (ohne wirkungsvolle Gegenmaßnahmen)

8 bewaffnete Portugalfahrer + Waren hilflos gegen 2 Barbaresken-Galeeren
Ergebnis ➔ 1,5 Millionen Courantmark Schaden

1665 Gründung der Commerz-Deputation (Bau höchst erfolgreicher Kriegsschiffe)

1867 Umbenennung in "Handelskammer Hamburg"

Ausblick: aus der Vergangenheit lernen

CycleSEC®

Maritime Cyber Deputation

Piraterie zu Beginn des 21. Jahrhunderts

(Gründung einer Admiralität ohne Wirkung bitte auslassen)

(Den nächsten 300 Millionen-Schaden (NotPetya/Maersk) bitte auslassen)

Gründung einer Cyber Deputation (konkurrenzübergreifende Selbsthilfe)

Trägerschaft: Maritimes Cluster, IHKen, Stiftung, eigener Verein…

Vorschlag: „Maritime Cyber Deputation“

Eins ist sicher:
Die Maritime Branche
hat dieses Mal
keine 40 Jahre Zeit!

Convoy-Zoll
für abgehende und eingehende Schiffe
oder etwas zeitgemäßer: auf Umsätze.

Beispiel: Ausbildung

CycleSEC®

Schulung sichere Softwareentwicklung (2 Tage)

Bei einem Schulungsanbieter

Pos.	EUR	Anz.	EUR
Teilnahmegebühr	1.200	×12	14.400
Reisekosten	500	×12	6.000
Summe	**1.700**	**×12**	**20.400**

In-House bei einem der Kunden

Pos.	EUR	Anz.	EUR
Tageshonorar	3.700	×2	7.400
Reisekosten	500	×12	6.000
Summe			**13.400**
Ersparnis			**7.000**

Beispiel: Incident Management

CycleSEC®

Task-Force Sec-Ops I

10 Tage Forensik und CERT

Pos.	EUR	Anz.	EUR
Tagessatz (3 FTE)	1.600	×30	48.000
Reisekosten	1.000	×6	6.000
Summe			**54.000**

Eigenes Personal Cyber-Deputation

Pos.	EUR	Anz.	EUR
Tageskosten (bei 100k)	450	×30	13.500
Reisekosten	1.000	×6	6.000
Summe			**19.500**
Ersparnis			**34.500**

Beispiel: Incident Management

CycleSEC®

Task-Force Sec-Ops II

5 Einsätze Forensik und CERT

Pos.	EUR	Anz.	EUR
Kosten (150 PT)	54.000	×5	270.000
Summe			**270.000**

Eigenes Personal Cyber-Deputation

Pos.	EUR	Anz.	EUR
Mitarbeiter (bei 100k)	90k	×3	270.000
170 PT Rest / Pers.		×3	500 PT
Summe			**270.000**
Ersparnis			**+/- 0**
Rest Verfügbarkeit			**510 PT**

Beispiel: Hochschulzusammenarbeit

CycleSEC®

Gemeinsame Suche nach Forschungsthemen

Abschlussarbeit

Promotion

Förderung

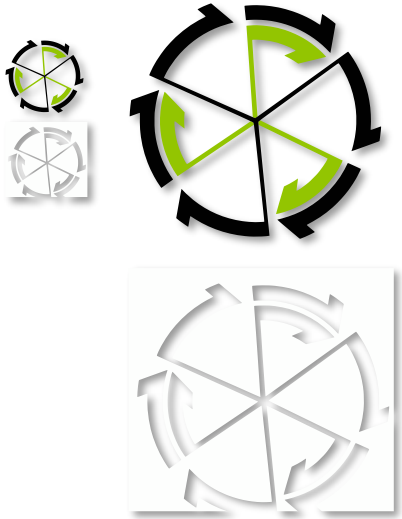
Ergebnisse gemeinsam teilen!

Hinweis

Der Inhalt dieses Dokuments wurde mit Sorgfalt und auf Grundlage der uns bekannten und durch den Kunden übergebenen Informationen erstellt.

Die durch CycleSEC gegebenen Empfehlungen zielen darauf ab, die Risiken für unsere Kunden zu reduzieren. In den meisten Fällen können Risiken jedoch nur reduziert und nicht vollständig vermieden werden.

CycleSEC® GmbH



Sitz:

Rahlstedter Bahnhofstraße 26a
22143 Hamburg
Amtsgericht Hamburg, HRB 146960
USt-ID: DE302369764

Geschäftsführer:

Sebastian Klipper
+49(0)176-62986101
sk@CycleSEC.com