Image: Munich Re Oliver Soulas

Cyber Risiken in Transport und Offshore-Energy

VHT Schadenverhütungskonferenz 15.Nov. 2016

Tillmann Kratz, Global Marine Partnership

Munich RE

Agenda

1. Risikobewusstsein
2. Entwicklung der Cyber Risiken
3. Schadenbeispiele und Szenarien
4. Versicherungsaspekte
5. Resumee

Risikobewusstsein
„The risks of a new invention are usually ignored until a catastrophy occurs“

Munich RE

Erfindung	Euphorie	Katastrophe	Reaktion
1871 Beginn industrieller Asbestherstellung	„…ein derart breites Anwendungsspek-trum hat die Welt noch nicht erlebt “	Asbest wird als Krebserreger identifiziert	Nahezu weltweites Verbot
1954 Erstes Atom-Kraftwerk	„ …sichere, billige, effiziente,saubere Energieerzeugung“ Deckt weltweiten Energiebedarf ab	3 Mile Island, Chernobyl, Fukushima	Totaler Atomausstieg bis 2022 in Deutschland
1994 Erster Internetbrowser Netscape Navigator	„…das Internet wird die Welt befreien“	Cyber GAU ???	???

Millenium-Sturm im Wasserglas ?

Der Y2K Virus

Vom Niedergang des Cyber Risiskobewußtseins

Die Fakten

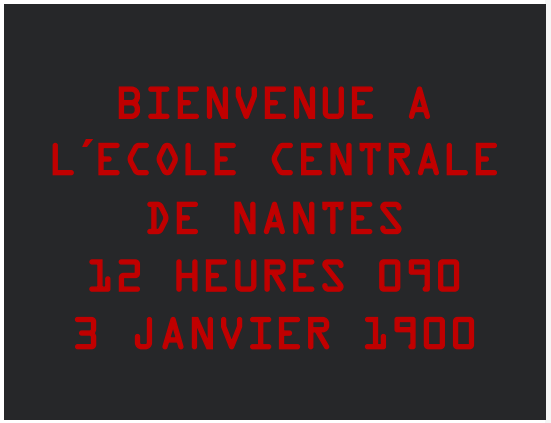
- Um Speicherplatz zu sparen werden bei Datumsangaben die Jahreszahlen nur zweistellig gespeichert („98“ statt „1998“)

Der Medien Hype

- „Weltuntergang“
- „Das Y2K Problem ist das Gegenstück zu El Nino und wir müssen uns weltweit auf böse Überraschungen gefasst machen“

Risiko-Bewußtsein nimmt ab

- Der Respekt vor potentiellen Cyber Risiken nimmt ab, als keine nennenswerten Schäden zur Jahrtausendwende eintreten



Risikobewusstsein in der EU
- Bereich Seetransport -

Munich RE

"Es wurde eindeutig festgestellt dass **das Bewusstsein für Cyber Sicherheit im maritimen Bereich nur sehr gering ausgeprägt bzw. überhaupt nicht vorhanden ist**. Diese Feststellung gilt für alle Bereiche einschließlich staatlicher Stellen, Hafenbehörden und im Seetransport tätiger Firmen."

enisa
European Network and Information Security Agency

Maritimer Sektor ist systemrelevante Infrastruktur für die Weltwirtschaft

90% des EU Aussenhandels beinhalten Seeverkehr

Seetransport und handels bezogene Vorgänge zunehmend IT basiert

Kosten der Cyber-Kriminalität

Munich RE

Annual econ. loss $ 300bn - $ 1tn

McAfee

Annual econ. loss: $ 350bn

EC3 EUROPOL

sueddeutsche.de

Annual econ. Loss $ 400bn

Econ. Cost: $ 114bn

THE Fiscal TIMES

1 Trillion = 1.000.000.000.000

Wie verlässlich sind die Daten zur Cyber-Kriminalität?

Munich RE

Geschätzte Dunkelziffer: 85 %

Vorfälle werden weitgehend unter Verschluss gehalten

Reputations-Risiko!

Datensicherheit könnte aus Kundensicht als gefährdet gelten

Furcht, von Nachahmern als weiches Angriffsziel gewählt zu werden

Cyber Angriff nicht entdeckt

Schaden kann nicht eindeutig auf Cyber Angriff zurückgeführt werden

Gefährdung des Versicherungsschutzes bei Ausschluss von Schäden durch Cyber-Angriffe

Keine rechtliche Verpflichtung derlei Angriffe öffentlich zu machen

Wie alles begann…
Erster Computer Virus, 1982

Munich RE

The Elk Cloner Virus

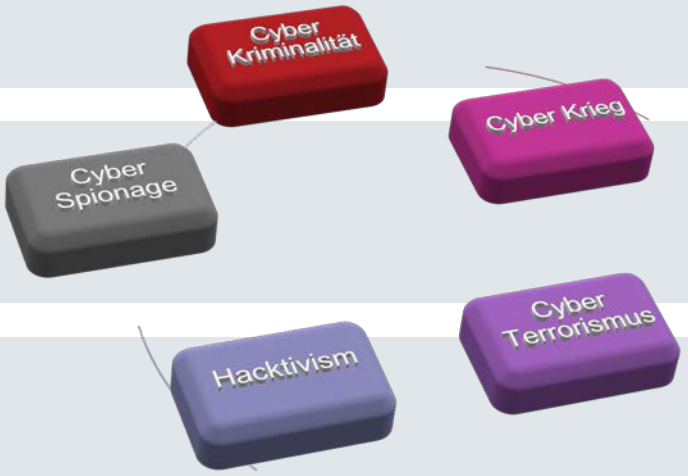
```
Elk Cloner:
The program with a personality

 It will get on all your disks
  It will infiltrate your chips
   Yes it's Cloner!

 It will stick to you like glue
  It will modify ram too
   Send in the Cloner!
```

- Von 15 jährigem Schüler programmiert
- Als Witz gemeint
- Selbsreproduzierender „Boot sector“ Virus

Aus Spaß wird Ernst
Die Entwicklung der Computerviren

Munich RE

Spaß	▪ Elk Cloner
Diebstahl Unterschlagung	▪ Target, 2014, $1bn ▪ eBay, 2014, $145m ▪ MtGox, Bitcoin, 2014, 750.000 customers Bitcoins worth $446m and $500m company bitcoins stolen
Sabotage Erpressung	▪ Baku-Tiflis-Ceyhan Pipeline, Turkey 2008 ▪ Stuxnet, Iran, 2010 ▪ Steel Mill, Germany, 2014 ▪ Et. Al??
Hacktivism Terrorismus	▪ Anonymous, from 2003 ▪ Estonia, 3 weeks in 2007, Russian attack
Cyber-Krieg ?	▪ Sony Entertainment Pictures, 2014 ▪ Ukraine ▪ US Cyber Doctrine, 2011



Hacktivismus, Terrorismus, Kriegsführung „Computerkriminalität aus religiösen sozialen oder politischen Gründen“

Anonymous: dezentralisierted online community, seit 2003

„100 einflussrreichsten Personen in der Welt“

Scientology, Regierungsstellen (US, Israel, Tunisia, Uganda), Visa, PayPal, Copyright Überwachungsinstanzen KKK, Terrorists

In 2007 verärgerte Estland die russ. Regierung mit der Entfernung eines sowj. Kriegerdenkmals

In der Folge wurden Estnische Regierungs-Websites und bilateraler Handel massiv gestört.

Es war einer der größten “DDoS” Angriffe der Geschichte mit dem Estland zeitweilig lahmgelegt wurde

Hacking der TV5Monde IT Infrastruktur, Homepage, Facebook Account und des TV Programms

TV5 Monde ist nach MTV die zweitgrösste TV Gesellschaft der Welt

Die Zukunft - in der Fiktion

Blackout – Marc Elsberg

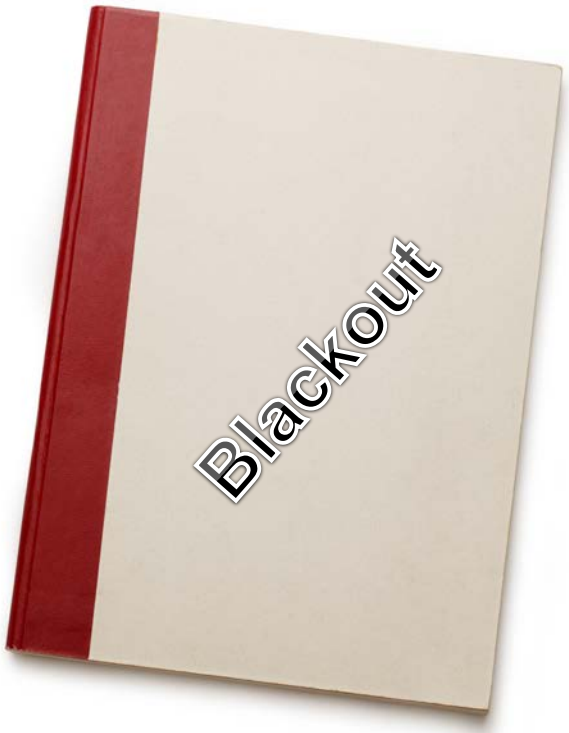


Image: Used under the license of Shutterstock.com

- Terroristen verbreiten einen Computer Virus über IT gesteuerte Energieregler (Smart Meter)
- Durch gefälschte Bedarfssteuerung fahren die Kraftwerke ihre Leistung herab
- Wegen der Stromverteilung über kontinentale Versorgungsnetze kommt es zu regionalen Stromunterbrechungen in Europa
- Die Zivilgesellschaft versagt binnen zwei Wochen und es kommt zu Bürgerkriegen

Die Zukunft - in der Realität

“Hazards and Vulnerabilities in modern societies”
Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB)

„Was geschieht bei einem Blackout?
Über die Folgen eines anhaltenden und weitreichenden Stromausfalles“

(Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, 2011)

1. …es wäre nahezu unmöglich, den Kollaps der gesamten Zivilgesellschaft zu verhindern
2. …trotz des erwarteten Ausmaßes steckt das Risikobewusstsein noch in den Kinderschuhen
3. …nicht beherrschbare Katastrophe
4. …zahlreiche Länder unterhalten „Cyber Armeen“, die bereits in der Lage sind, Versorgungs- und Kommunikationslinien zu beeinträchtigen

Schadenbeispiel “Kreditkarten”

Munich RE

US Target Corporation, January 2014

Image: Used under the license of Shutterstock.com

- Diebstahl von Kreditkartendaten von geschätzt 70 Millionen Kredit- und Debit-Kartenbesitzern während der Weihnachtssaison
- Hinweise deuten darauf, dass der “Einbruch “ aus Russland heraus gesteuert wurde. Ein Glied in der Informationskette öffnete unwissentlich einen mit der Malware versehenen Email Anhang
- Der Schaden könnte über 1 Mrd. USD liegen

Schadenbeispiel “Banken”

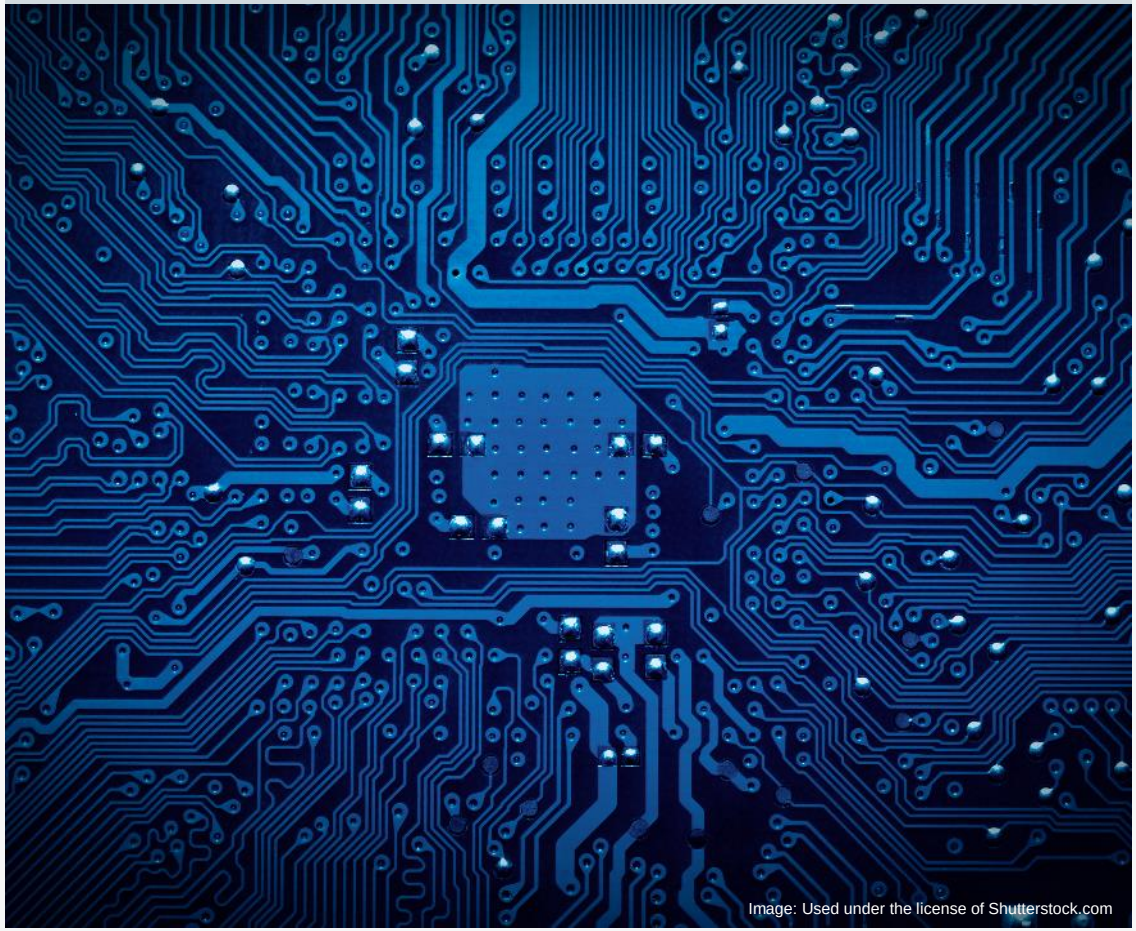
One Billion bank fraud by “Carbanak”, 2014

- Über einen Zeitraum von 2 Jahren stiehlt die Hacker Gang “Carbanak” 1Mrd. USD von 100 Banken in 30 Ländern
- Über einen an die Bankangestellten verschickten Email-Virus werden sämtliche Computer Aktivitäten verfolgt und das Verhalten der Angestellten imitiert.
- Geldausgabeautomaten werden per IT manipuliert

Schadenbeispiel “Unterhaltungsindustrie”

Munich RE

Sony Pictures Entertainment (SPE), 2014



- Unbekannte Hacker Grruppe kopiert 100 Terabyte Daten von den SPE Servern and verbreitet 150 Gigabyte davon im Internet.
- Sie stehlen private Tefonnummern und Email Adressen von sämtlichen prominenten Hollywood Schauspielern, Sozialversicherungsnummern, Kreditkartendaten, unveröffentlichte Filme, Gehaltsdaten aller 34.000 Angestellten sowie den gesamten internen Email Verkehr.
- Retrospektive Schadenanlyse ergibt, dass es nur einen Sicherheitsring gegen Eindringen von aussen gab
- USA machen Nodkorea für den Angriff verantwortlich

Schadenbeispiel “Sabotage”

Stuxnet Virus, first discovered 2010

1. Computerwurm, entdeckt 2010, entwickelt um industrielle Kontrollsysteme anzugreifen

2. Weltweite Verbreitung, 58% aller Computer im Iran befallen

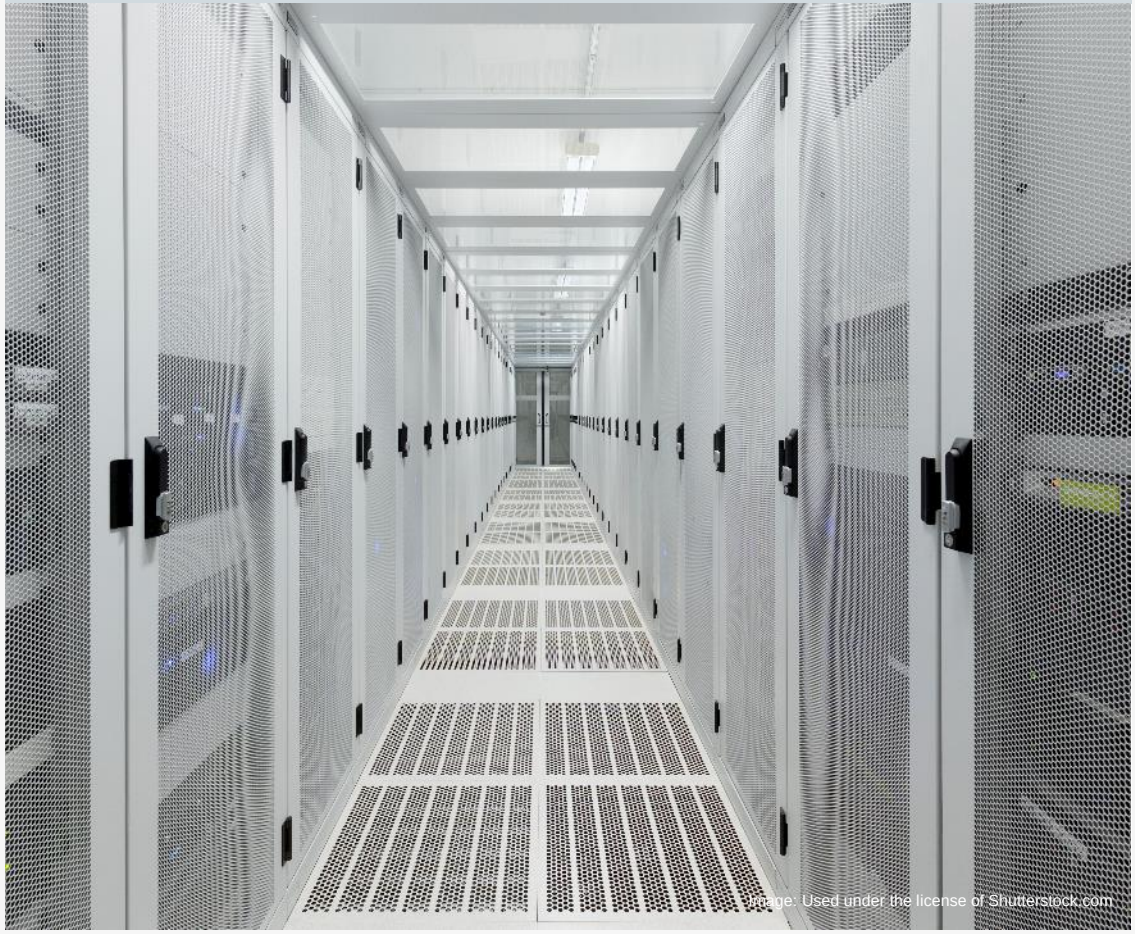
1. „Schläfer“ – Virus, Stuxnet wird erst aktiviert wenn vorgegebene Rahmenbedingungen erfüllt sind

2. Stuxnet hat 20% der Zentrifugen des Iranischen AKW in Natanz zerstört

3. Komplexität und geschätzte Entwicklungskosten lassen auf einen staatlichen Verursacher schließen

Marine Schadenbeispiel “Sabotage”

IRISL data destruction



Iranian Shipping Lines

1. In 2011 wird die IT der Iranian Shipping Line, IRISL, angegriffen. Dabei werden sämtliche Containerverkehrsbezogenen Daten zerstört

2. Erkennbare Motive des Angriffs sind nicht finanzieller Natur. Ziel ist offenbar die reine Zerstörung

Schadenbeispiel “Spionage & Sabotage”

Computer virus “Regin”, first discovered 2011

- Quelle unbekannt, laut Edward Snowden von der NSA mit dem Ziel entwickelt, vollständige Kontrolle über die IT Infrastruktur eines Landes zu gewinnen
- Bis dato komplexeste Malware / Spionageprogramm die viele Millionen USD an Entwicklungs-kosten verschlungen haben muss
- Speziell geeignet,um die nationale mobile Dateninfra-struktur eines Landes zu kontrollieren
- Erstmals 2011 in den IT Systemen der Europäischen Kommission entdeckt
- Bisher bekannt gewordenene Infektion von 27 Zielen in 10 Ländern, hauptsächlich in Russland und in Saudi Arabien

Schadenbeispiel “Energiegewinnung und Verarbeitung”

Sabotage oder Erpressung?

Shamoon & Night Dragon, 2012

1. Aufgrund Computervirus Befalls muss Saudi Aramco am 15th August 2012 ihr gesamtes IT System vom Netz nehmen.

2. 30.000 workstations müssen für 2 Wochen abgeschaltet bleiben und am Ende ausgetauscht werden

3. Aus dem gleichen Grund muss auch die Firma Quatari Liquid & Natural Gas ein paar Wochen später ihr gesamtes IT Netzwerk herunterfahren

Marine Schadenbeispiel “Warenschäden”

Bei 420 Millionen Containern p.a. kann noch viel schiefgehen

Antwerp‘s Port Community, 2013

1. Erfolgreicher Cyber Angriff auf das Container Logistik System des Antwerpener Container Terminals zwischen 2011 und 2013
2. Drogenhändler verdingen Hacker um das Logistiksystem zu manipulieren
3. Container mit Schmuggelware als Beiladung werden an „falsche“ Fahrer ausgeliefert
4. Versicherer erhalten Forderungen rechtmäßiger Empfänger für verloren gegangene Ware in den Schmuggelcontainern
5. Ein Zufallsfund von 2 Tonnen Heroin und ein paar Millionen USD in bar bringt Ermittler auf die Spur

Marine Schadenszenario “Kaskoschäden”

Munich RE

AIS vessel tracking system, 2013

1. AIS - Automatic Identification System installiert auf 400.000 ships

Schaden-Szenario

1. Modifikation von Schiffsdetails wie z.B. Flaggenstaat, Namen, Position, Route, Geschwindig-keit, AToN (Aid to Navigation) Eingaben wie Leuchttürme

2. Falsche Schiffsidentität wird vorgetäuscht

3. Inszenierte Schiffskollisionen, Hafenblockaden etc.

4. Sabotage von AIS, Schiff „verschwindet“

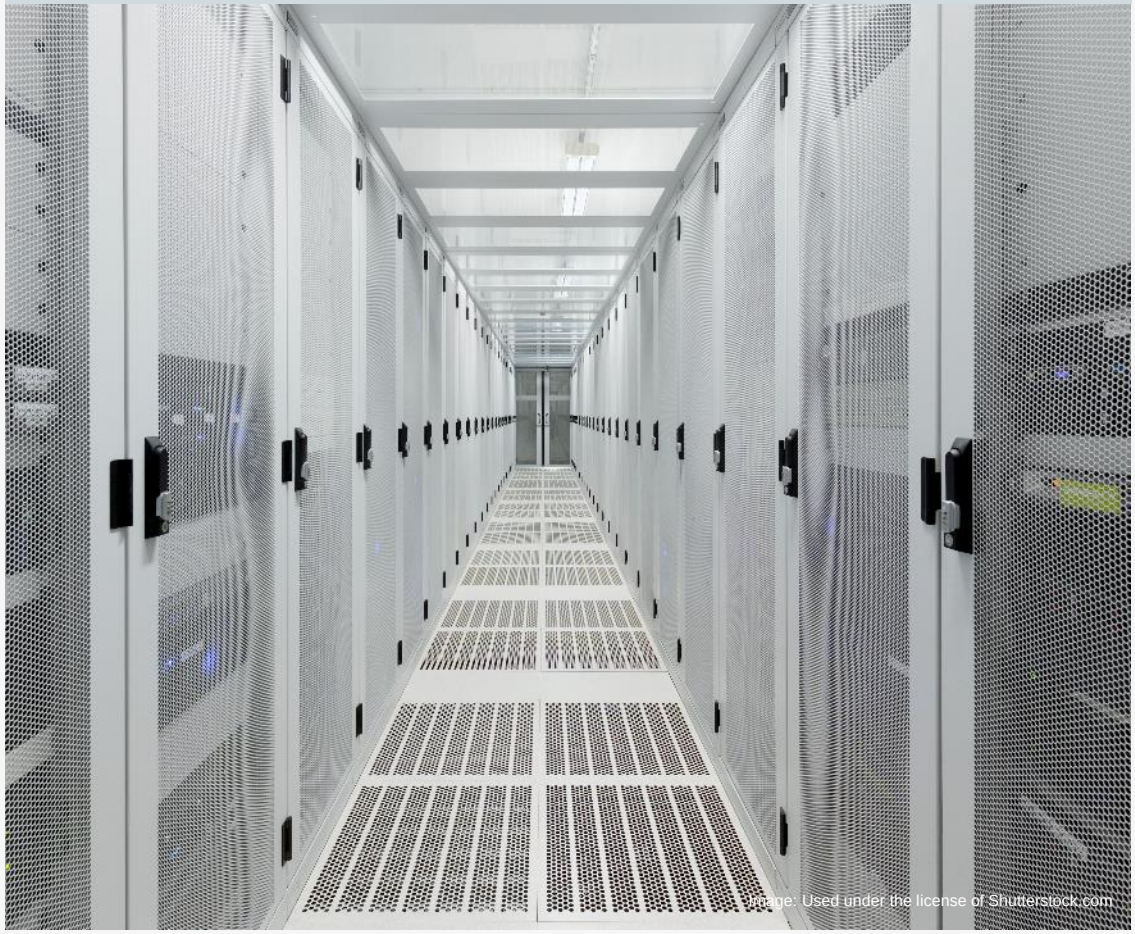
The AIS was designed with seemingly zero security

(Wilhoit & Balduzzi: Vulnerabilities discovered in Global Vessel Tracking systems, 2013)

Marine Schadenbeispiel “Informationsbeschaffung”

Munich RE

Other examples



Pirate Hacker

1. Somalische Piraten verdingen Hacker um in die IT Systeme von Reedereien / Charterern einzudringen
2. Sie erhalten Informationen welche Schiffe wertvolle Ladung fahren oder wie die Sicherungs-vorkehrungen an Bord beschaffen sind

Australischer Zoll

1. Syndikate des organisierten Verbrechens dringen in die Warenerfassungssysteme der Australian Customs and Border Protection ein
2. Sie erfahren ob „ihre“ Container durchsucht werden sollen

Marine Cyber Risikoeinschätzung

- **Höhere Wahrscheinlichkeit**
- Etliche Vorkommnisse
- Zahlreiche Angriffsportale
- Hohes Schadenpotential

- **Mittlere Wahrscheinlicheit**
- Ein paar bekannte Vorfälle
- Zahlreiche Angriffsportale
- Mittleres Schadenpotential
- *Folgen eines Angriffes auf die Logistik?*

- **Geringere Wahrscheinlichkeit**
- Keine bekannte Vorfälle
- Weniger Angriffsportale
- Geringeres bis mittleres Schadenpotential
- *e-Navigation Exposure?*

Images: Used under the license of Shutterstock.com

Gegenmaßnahmen – erste Schritte

Munich RE

IMO INTERNATIONAL MARITIME ORGANIZATION

E

FACILITATION COMMITTEE
39th session
Agenda item 7

FAL 39/7
10 July 2014
Original: ENGLISH

ENSURING SECURITY IN AND FACILITATING INTERNATIONAL TRADE

Measures toward enhancing maritime cybersecurity

Submitted by Canada

SUMMARY

Executive summary:	This document proposes the development of *Guidelines on maritime cybersecurity in light of the dramatic increases in the use of cyber systems across the maritime sector and related risks*
Strategic direction:	6.1
High-level action:	6.1.1
Planned output:	No related provision
Action to be taken:	Paragraph 11
Related document:	FAL 38/7

1. Nutzung und Abhängigkeit von IT Systemen im maritimen Bereich sind stark angestiegen

2. Der maritime Bereich ist nicht immun gegen mögliche Angriffe

3. Praktische Maßnahmen werden von internationalen Verbänden langsam in Angriff genommen

Aktuelle (Rück-)Versicherungspraxis

Munich RE

- Weitgehende Vereinbarung von Auschluss Klauseln wie z.B. Cl. 380 für

INSTITUTE CYBER ATTACK EXCLUSION CLAUSE (CL 380) 10/11/2003

1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any electronic system.

1.2 […*where war is insured, no exclusion for use of IT systems for launch, firing, guidance etc.]*

Aktuelle Themen

1. Wirksamkeit des Cyber-Attack Ausschlusses – Beweisführung
2. Umgang mit Veränderungsrisiko – Gestaltungswille / -möglichkeiten
3. Wie gehen andere Sparten mit dem Risiko um
4. Geschäftsopportunitäten / Neue Produkte
5. Risikoappetit
6. Cyber-Expertise beim Erstversicherer / Rückversicherer
7. Schadenszenarien
8. Quantifizierung national / international
9. Deckungskapazität Erstversicherer / Rückversicherer
10. Kumul-Überwachung Rückversicherer

Resumee

Rückversicherungsschutz ist für spezielle Segmente und auf Einzelrisikobasis möglich

Erstversicherungsmärkte müssen für sich entscheiden, wie sie mit dem veränderten Risiko im Cyber Bereich angehen wollen

Aber auch hohes Schadenpotential in Marine

Momentan größeres Schadenpotential und -häufigkeit in den Non-Marine Sparten

Wenige Beispiele für Schäden in den Marine Sparten erschweren Veränderung

Cyber Risiken haben hohe Geschäftsrelevanz. Sie sind nicht nur ein IT Problem

Cyber Risiken werden weit unterschätzt. Das Risikobewusstsein ist noch zu gering

„There are only two types of companies: those that have been hacked and those that will be.
And that is changing to: those that have been hacked and will be again“
(Robert S. Mueller, FBI Director 2001-2013)

Image: Munich Re Oliver Soulas

Danke für Ihre Aufmerksamkeit!

Tillmann Kratz, Global Marine Partnership

Munich RE