TRAFICOM
Finnish Transport and Communications Agency

Kyberturvallisuus ISM & ISPS

11.9.2020

Kyberturvallisuus merenkulussa pähkinänkuoressa

Aluksien teknisiä järjestelmiä voidaan hakkeroida yhtä lailla kuin järjestelmiä hakkeroidaan maapuolella.

Tämä muodostaa – kyberiskun muodossa – potentiaalisen turvallisuus-/turvariskin alukselle sekä mittavan taloudellisen riskin koko merenkulun elinkeinolle.

Kyberturvallisuus on lyhyesti määriteltävissä toimenpiteiksi, joilla suojaudutaan kyberhyökkäyksiä ja niiden vaikutuksia vastaan sekä toteutetaan tarvittavia vasta-toimenpiteitä varustamon ja aluksen kyberympäristön turvaamiseksi.

Maja Markovčić Kostelac, EMSA's Executive Director:

"In this increasingly digital age, we face borderless cyber-security risks and we must take a borderless response to our cooperation across all transport modes"

Jim Hagemann, Chairman, A.P. Møller-Maersk

"We were basically average when it came to cyber security, like many companies. This was a wake-up call not just to become good, but to have cyber security as a competitive advantage".

Kyberturvallisuus turvallisuusjohtamisjärjestelmässä (SMS/ISM)

- Merenkulun turvallisuuskomitea (MSC) hyväksyi 98. istunnossaan päätöslauselman *MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems*.
- Päätöslauselmalla ohjataan hallintoja, varustamoja ja luokituslaitoksia huomioimaan kyberturvallisuuden yhtenä osana turvallisuusjohtamis-järjestelmää (SMS/ISM)
- Päätöslauselman mukaan varustamon kyberriskien tarkastelu tulee olla tehtynä vuosiauditoinnissa (ISM/DOC), joka suoritetaan 1. tammikuuta 2021 jälkeen

Huomioitava:

- Ei muutosta itse ISM-koodiin
- Turvallisuuskomitea (MSC) toi raportissa esiin, että päätöslauselma on suositus
  - Lainaus MSC 98 loppuraportista: ”The Committee agreed that operative paragraph 2 and the resolution as a whole was recommendatory in nature”.

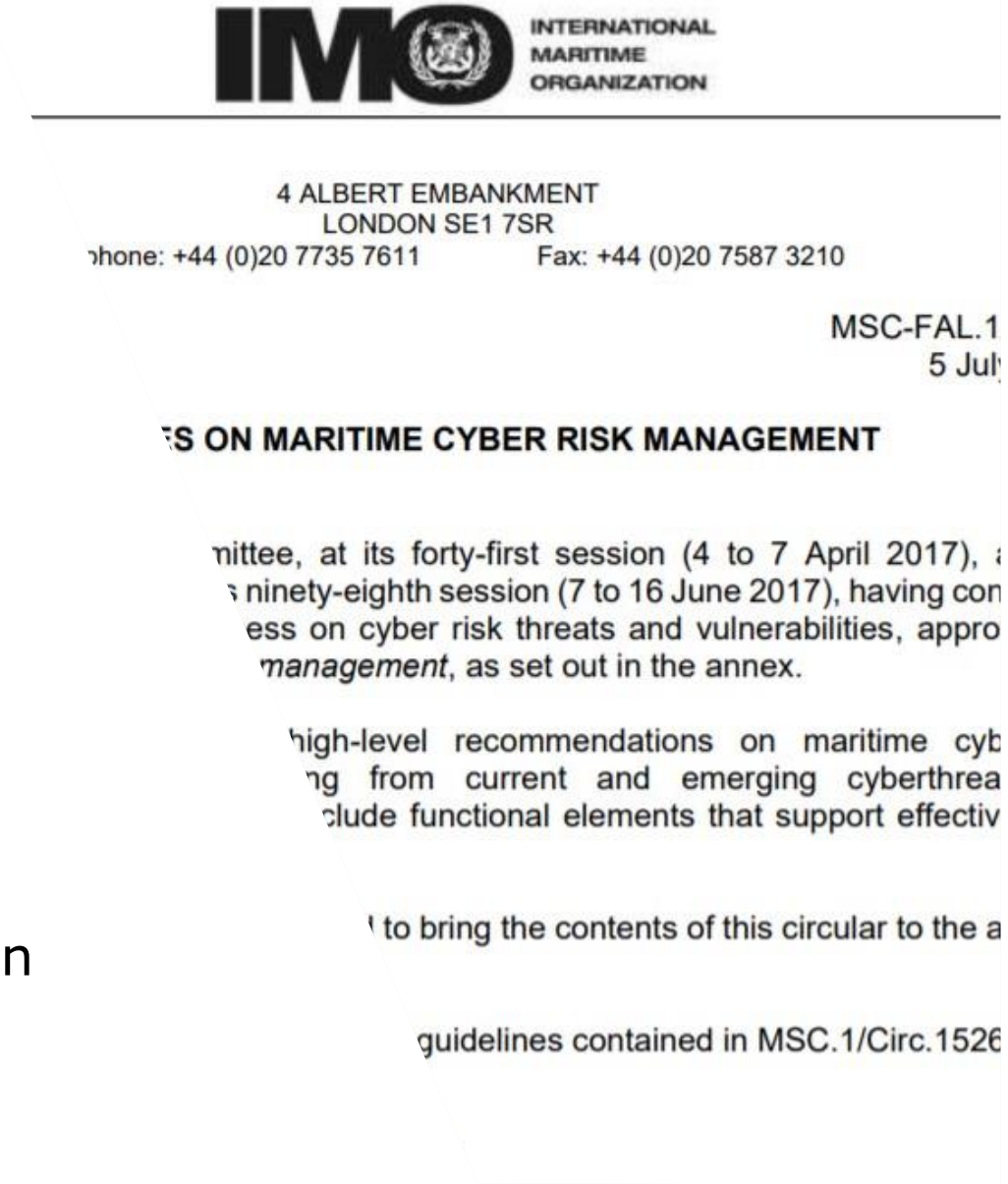
IMO:n ohjeet kyberuhkiin

IMO julkaisi ohjeen kyberturvallisuuden hallintaan kiertokirjeellä MSC-FAL.1/Circ.3 (2017)

- Ohje antaa ylätason suosituksia kyberriskien hallintaan; kyberuhkien ja haavoittuvuuksien tunnistamiseen sekä suojatoimien laatimiseen
- Ohje on suositusluonteinen ja lisätty IMO:n (GISIS) Non-mandatory Instruments -listalle

- Päätöslauselmassa MSC.428(98) ohjataan toimijoita hyödyntämään tätä ohjetta tehdessään oman toiminnan kyberriskien arviointia.

"Tunnista – Suojaa – Havaitse – Reagoi – Palauta"



INTERNATIONAL MARITIME ORGANIZATION

4 ALBERT EMBANKMENT
LONDON SE1 7SR
hone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1
5 Jul

S ON MARITIME CYBER RISK MANAGEMENT

nittee, at its forty-first session (4 to 7 April 2017),
ninety-eighth session (7 to 16 June 2017), having con
ess on cyber risk threats and vulnerabilities, appro
management, as set out in the annex.

high-level recommendations on maritime cyb
ng from current and emerging cyberthrea
clude functional elements that support effectiv

to bring the contents of this circular to the a

guidelines contained in MSC.1/Circ.1526

Kattojärjestöjen kyberturvallisuusohjeet

IMO:n ohjeessa (MSC-FAL.1/Circ.3) mainitaan kattojärjestöjen laatimat ohjeet, joita voi hyödyntää aluksen kyberturvallisuuden edistämiseen aluksilla.

https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

(Ks. ANNEX 2 [s. 42-45])

EU komissio

Kehitteillä interaktiivista ”työkalupakkia” kuljetusyrityksille

- Transport Cybersecurity Toolkit

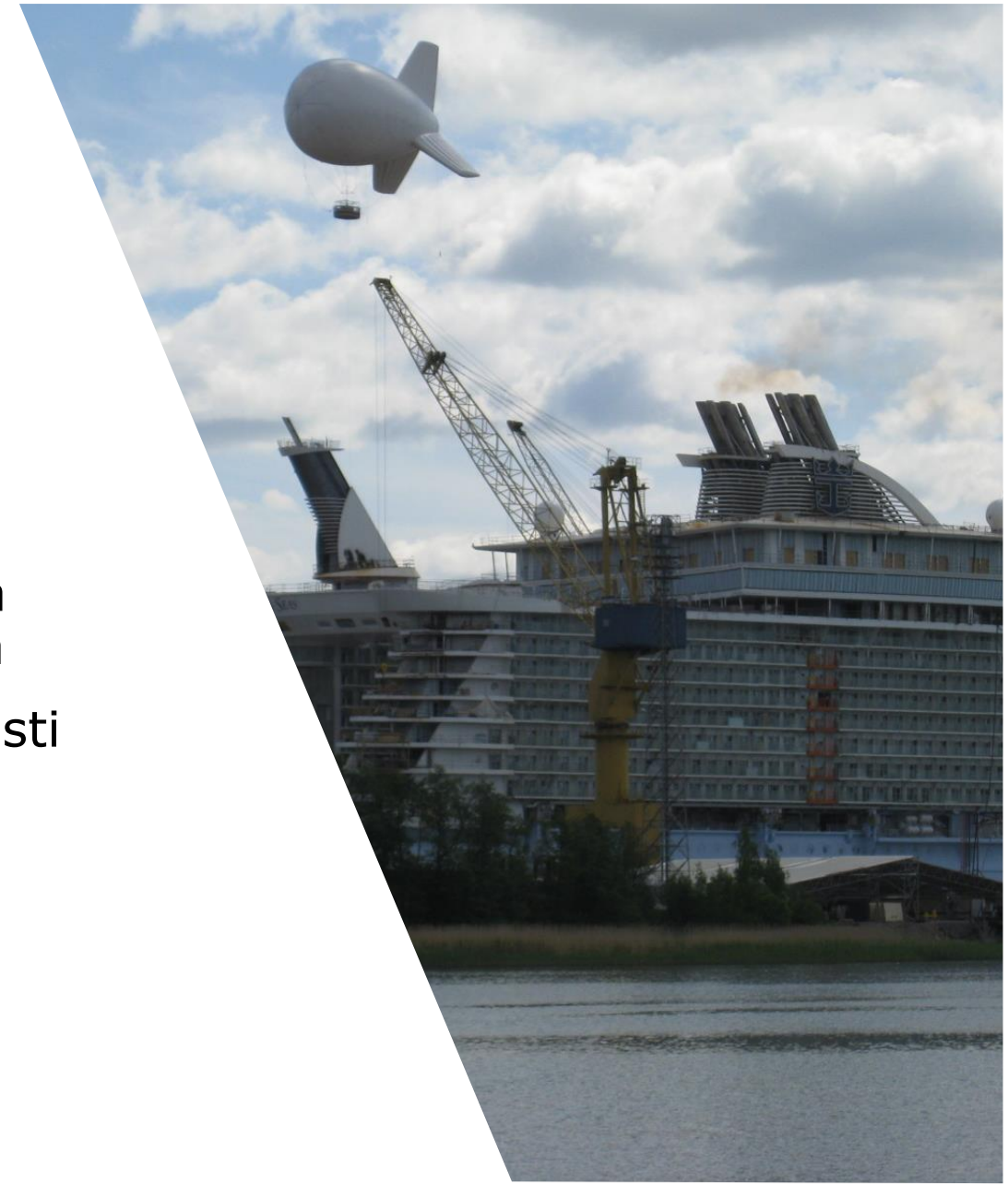
Kuljetussektoreiden (lento-, meri- ja maakuljetukset) tunnistettuja ”Top Five” kyberuhkia:

1. Malware diffusion; The dissemination of a software designed for intentionally damaging computers, networks, clients or networks
2. Denial of service; Flooding the targeted host or network with traffic until it crashes preventing users for accessing, due to the actions of a malicious cyber threat actor
3. Theft;The stealing of financial and/or personal information through the use of computers for making it fraudulent or other illegal use
4. Software manipulation; The process of changing data for making malicious reasons
5. Unauthorised access; The act of directly – or indirectly – accessing information online without authorization.

johtava asiantuntija Juhani Eronen

Kyberturvallisuus aluksella (1/2)

- Alukset ovat riippuvaisia varustamon toimintapolitiikasta. Merenkulkijoiden vaikuttamismahdollisuudet ovat merkittävästi vähäisemmät
- Luokkamerkki kyberturvallisuudelle
  - Perustuu IACS:n sääntöihin, mutta jokaisella luokalla asia on toteutettu hieman eri tavalla
  - Uudet matkustaja-alukset ovat pääsääntöisesti varustettu ”Cyber secure class notation” -merkinnällä
  - Voidaan myöntää vanhoillekin aluksille
  - Kyseinen luokkamerkki on maksullinen lisä
- Uusilla aluksilla (ja uudisrakennuksilla) kyberturvallisuus on helpompi huomioida jo aikaisessa vaiheessa.



Kyberturvallisuus aluksella (2/2)

- Alusten elinkaari saattaa olla hyvin pitkä (25-30 vuotta). Vanhojen alusten riippuvuus laitevalmistajista sekä heidän tarjoamasta huollosta ja päivityksistä aiheuttaa omat haasteensa. Varustamo/alus ei voi asiaan merkittävästi vaikuttaa
- Vanhojen laitteiden kyberuhat ovat pieniä mutta huonosti tunnettuja ja aluksilla on käytössä järjestelmiä, jotka voivat olla 30 vuoden takaa
- Vanhojen laivojen järjestelmät voivat olla monimutkaisia, järjestelmien yhteyksiä ja riippuvaisuuksia ei tarkkaan tunneta
- Kyberturvallisuus on vasta viime vuosina tullut mukaan merenkulkijoiden koulutukseen, näin varustamoiden ja miehistöjen osaaminen kasvaa
- Kyberturvallisuuteen ja kyberuhkiin kiinnitetään nykyään entistä enemmän huomiota
- Turvallisuusjohtamisjärjestelmä (SMS/ISM) on jatkuvasti kehittyvä, ja kyberriskienhallintajärjestelmä on liitettävissä siihen sujuvasti.

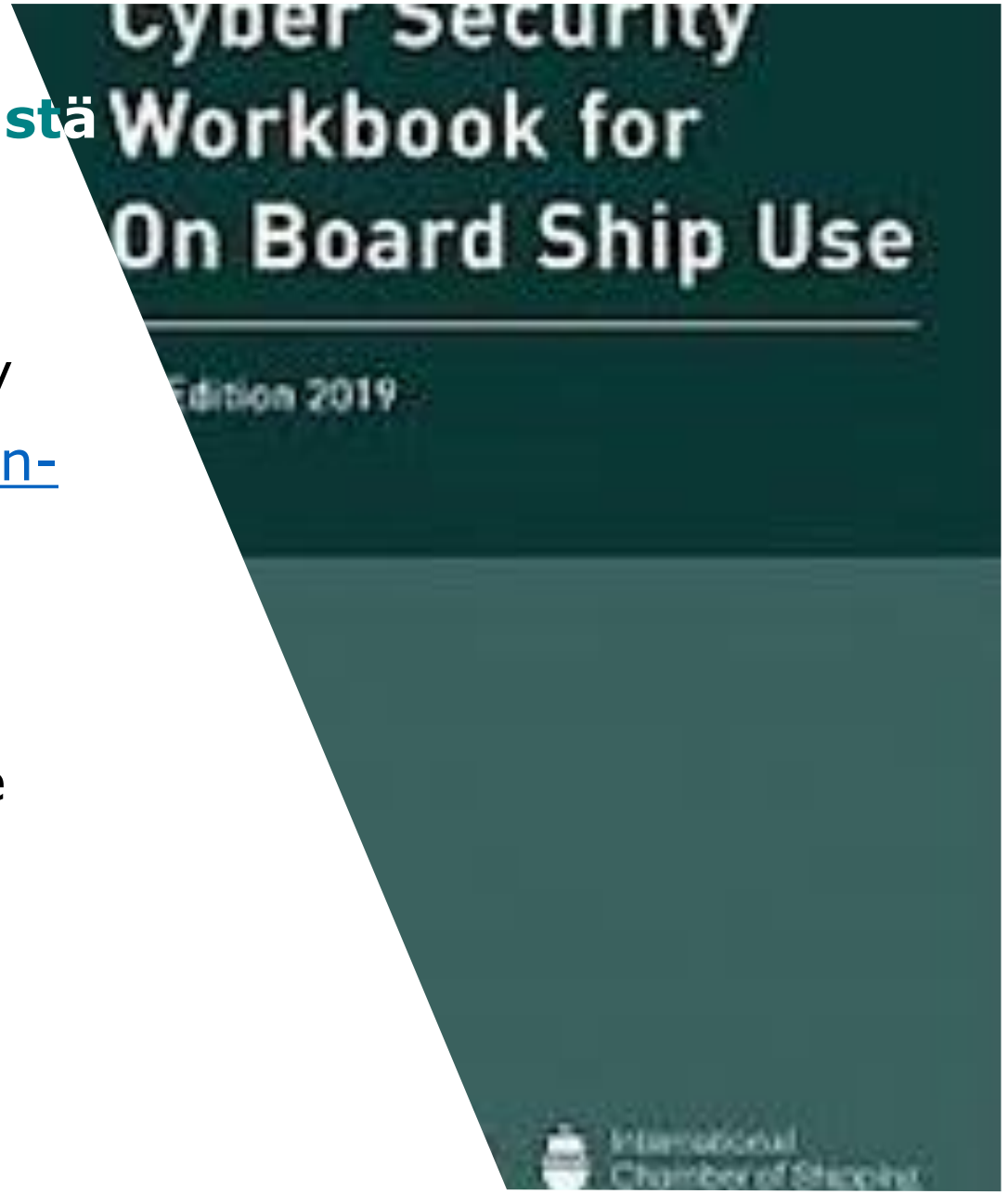
Kyberturvallisuustietoisuuden edistämistä varustamoissa ja aluksilla..

EMSA: Awareness in Maritime Cybersecurity

http://www.emsa.europa.eu/implementation-tasks/maritime-cybersecurity.html

BIMCO:

Cyber Security Workbook for On Board Ship Use



Varustamon mahdollisuudet turvallisuusjohtamis-järjestelmän (SMS/ISM) päivittämiseksi - Traficomin näkemys (1/2)

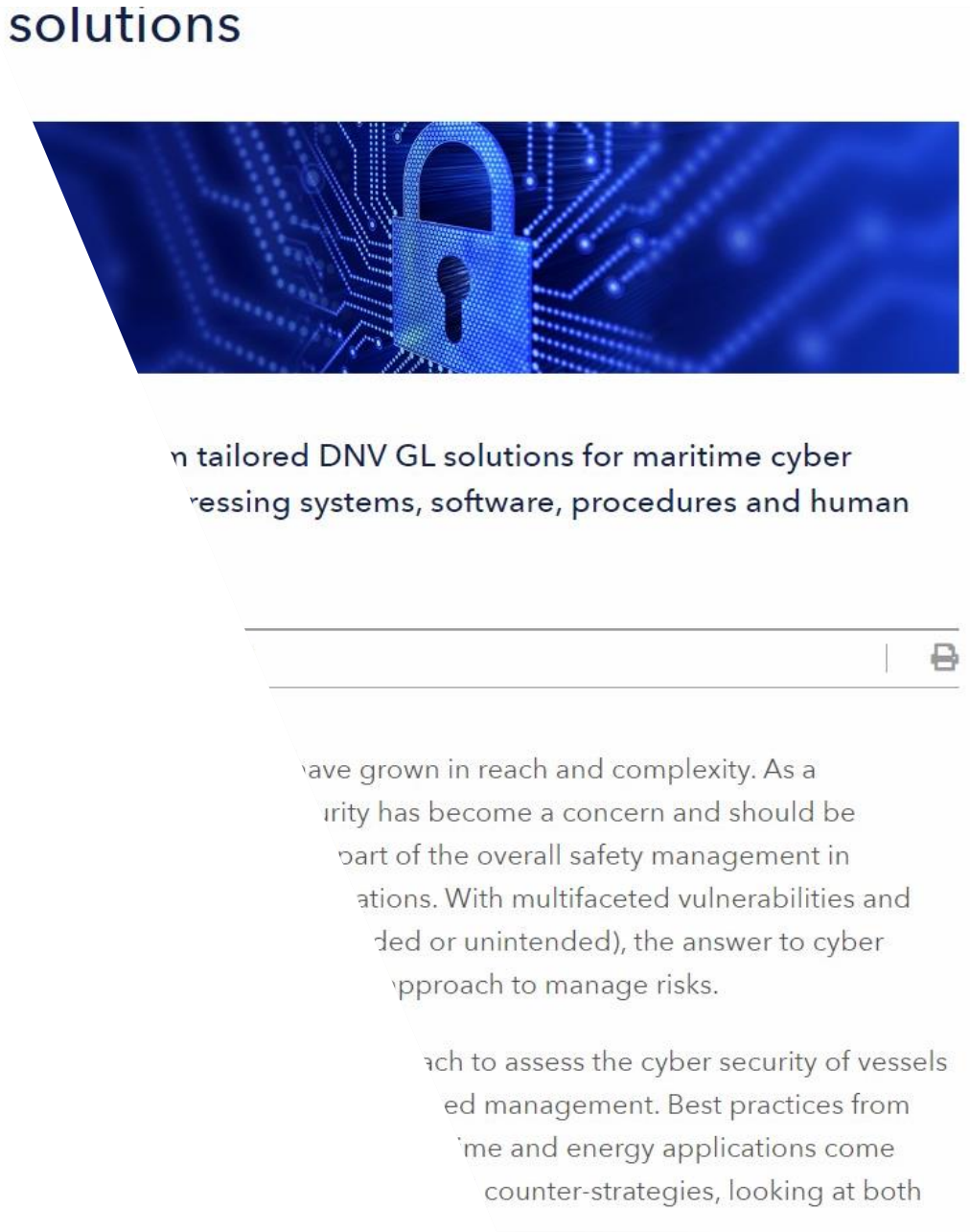
- Varustamo voi itse tunnistaa haavoittavuudet ja analysoida tunnistetut kyberuhat sekä toteuttaa tarvittavat muutokset turvallisuusjohtamis-järjestelmään (SMS/ISM) kyberriskien hallittavuuden suhteen
  - Kyberturvallisuus voi olla haastavaa ja varustamolle voi aluksi olla vaikea tunnistaa kyberriskejä/-uhkia sekä laatia riittäviä suojatoimenpiteitä

- Joillakin varustamoilla on ISO –laatujärjestelmä, jolloin heidän tulee ottaa kyberuhat huomioon ISO –järjestelmässä. Tämä helpottaa asian huomioimista ISM –järjestelmässä
  - ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements.

Varustamon mahdollisuudet turvallisuusjohtamisjärjestelmän (SMS/ISM) päivittämiseksi –Traficomin näkemys (2/2)

- Varustamo voi hyödyntää konsulttia tai tietoturvallisuuden arviointilaitosta
  - Alusympäristö ja merenkulku voi olla vieras toimintakenttä näille toimijoille

- Vaihtoehtoisesti varustamot voivat hyödyntää luokituslaitosten tarjoamia kyberuhkien kartoitus- ja ratkaisupalveluja päivittäessään turvallisuusjohtamisjärjestelmää (SMS/ISM)
  - Luokat myöntävät myös kyberturvallisuuteen liittyviä hyväksyntöjä laitteille.



Kyberturvallisuus ISPS-koodissa (EU 724/2004) – Turvasuunnitelma (SSP)

Kyberturvallisuus on osa alusten ja niihin liittyvien satamarakenteiden turvatoimia laittomien tahallisten tekojen varalta

9.4 Suunnitelmaa laadittaessa on otettava huomioon tämän säännöstön B-osan ohjeet, ja se on laadittava aluksen työkielellä tai -kielillä. Jos aluksella käytetään muuta kieltä kuin englantia, ranskaa tai espanjaa, suunnitelmaan on sisällyttävä käännös jollekin näistä kielistä. Suunnitelmassa on käsiteltävä vähintään seuraavia tekijöitä:

3 toimenpiteet, joilla estetään luvaton pääsy alukselle; (EU komissio on esittänyt tulkinnan, että pääsy alukselle, ei ole ainoastaan fyysinen vaan myös digitaalinen pääsy alukselle (lue 'kyberhyökkäys')).

9.6 Suunnitelman voi säilyttää sähköisessä muodossa. Tällöin sen suojaamiseksi on oltava menettelyjä, joilla estetään sen luvaton poistaminen, hävittäminen tai muuttaminen.

ISPS/B-osa → turva-arviointi (SSA)

8.3 Aluksen turva-arvioinnissa olisi käsiteltävä seuraavia aluksella olevia tai siihen liittyviä osatekijöitä:

5 radio- ja televiestintäjärjestelmät, mukaan luettuina tietokonejärjestelmät ja -verkot; ja

6 muut sellaiset alueet, jotka voivat aiheuttaa vaaraa henkilöille, omaisuudelle tai aluksen tai satamarakenteen toiminnoille, jos niitä vahingoitetaan tai käytetään laittomaan tarkkailuun.

8.9 Aluksen turva-arvioinnissa olisi käsiteltävä kaikkia mahdollisia uhkia, joihin voivat sisältyä muun muassa seuraavat turvavälikohtaukset:

3 lastin, aluksen keskeisten laitteiden tai järjestelmien tai aluksen varastojen luvaton käsittely;

8.10 Aluksen turva-arvioinnissa olisi otettava huomioon kaikki mahdolliset heikkoudet, joihin voivat sisältyä muun muassa seuraavat:

5 turvalaitteet ja -järjestelmät, mukaan luettuina viestintäjärjestelmät.

ISPS/B-osa turva-arviointi (SSA)

9. ALUKSEN TURVASUUNNITELMA

Yleistä

9.1 Yhtiön turvapäällikön vastuulla on varmistaa, että aluksen turvasuunnitelma laaditaan ja jätetään hyväksyttäväksi. Kunkin yksittäisen aluksen turvasuunnitelman sisällön tulisi vaihdella sen mukaan, mitä nimenomaista alusta se koskee. Aluksen turva-arvioinnissa on eritelty aluksen ominaispiirteet sekä mahdolliset uhat ja heikkoudet. Näitä tekijöitä on käsiteltävä yksityiskohtaisesti aluksen turvasuunnitelmaa laadittaessa. Hallinnot voivat antaa ohjeita aluksen turvasuunnitelman laatimisesta ja sisällöstä.

Ilmoita tietoturvaloukkauksesta → https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

Finnish Transport and Communications Agency

Kysymykset keskustelu-osioissa

Kiitos!

jan-christian.welander@traficom.fi
www.traficom.fi
@TraficomFinland