TRAFICOM
Kyberturvallisuuskeskus

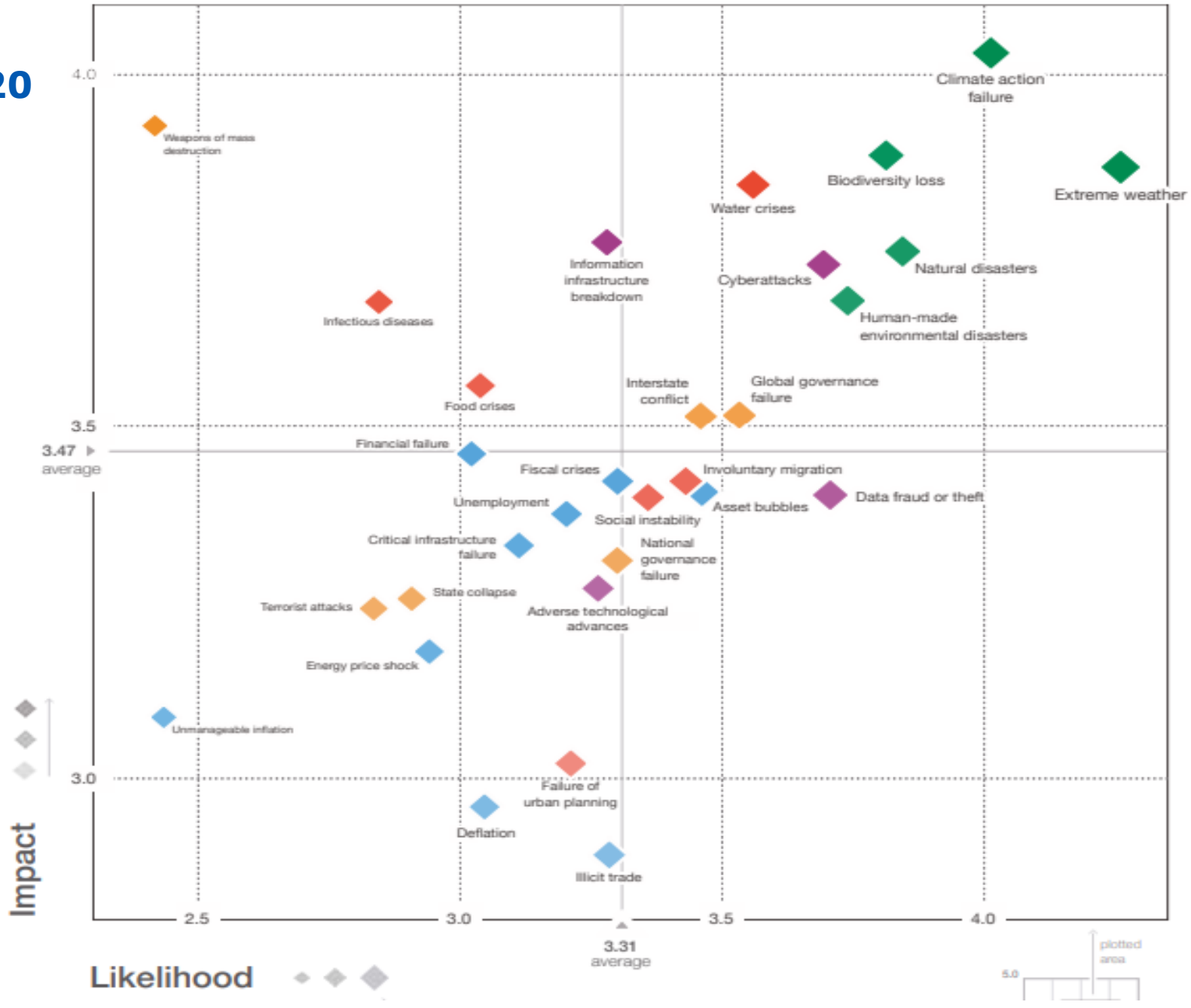
Katsaus merenkulun kyberuhkiin

Kyberturvallisuuden infopäivä 11.9.2020

Virpi Tuulaniemi
Erityisasiantuntija
Liikenteen kyberturvallisuuden koordinaattori

World Economic Forum: The Global Risks Report 2020

Figure II: The Global Risks Landscape 2020



TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kyberturvallisuutta uhkaavat toimijat

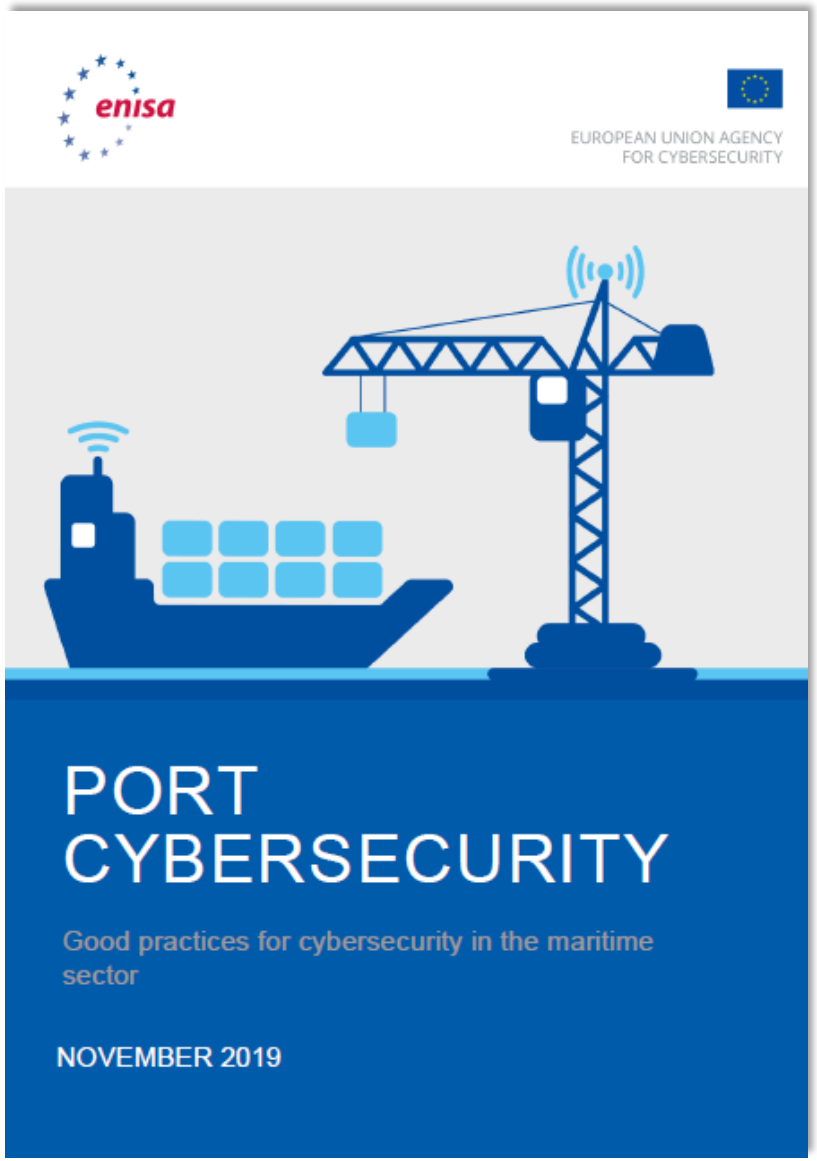
Toimijat	Motiivit
Aktivistit (ml. tyytymätön työntekijä)	Maineen tuhoaminen Toiminnan keskeytys
Rikolliset	Taloudellinen hyöty Kaupallinen ja teollinen vakoilu
Opportunistit	Haasteen hakeminen
Valtiot Valtioiden tukemat organisaatiot Terroristit	Poliittinen hyöty Vakoilu

Kohdentamattomat kyberhyökkäykset

- Kohteena mikä tahansa organisaatio tai alus
- Hyödynnetään internetissä saatavilla olevia työkaluja ja tekniikoita
  - Huijaukset
    - Manipuloidaan ihmisiä
  - Kalastelu
    - Sähköpostit, joilla yritetään saada tietoa
  - Haittaohjelmat
    - Kiristys-, varastus- ja vakoiluohjelmat, virukset, troijalaiset
  - Ulkoiset verkkosivut
    - Väärennetyt sivut tai oikeille sivuille lisätty haitallinen sisältö
  - Haavoittuvuuksien etsintä ja hyväksikäyttö
    - Skannataan verkkoa ja hyödynnetään havaittuja haavoittuvuuksia
  - ...

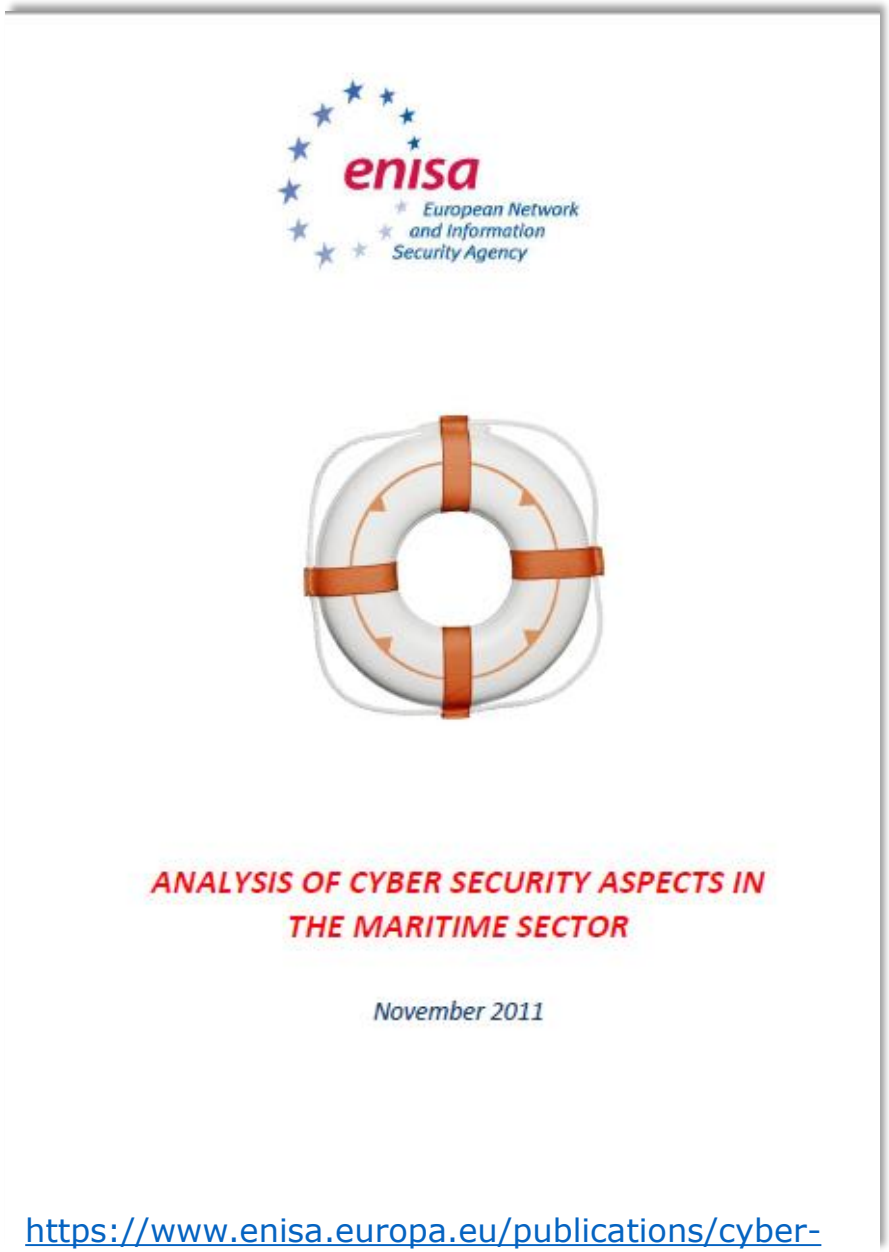
Kohdennetut kyberhyökkäykset

- Tietty organisaatio tai tietty alus tarkoituksellisena kohteena
- Hyödynnetään kehittyneitä työkaluja ja tekniikoita, jotka muokattu tai luotu kohdetta varten
  - Huijaukset
    - Manipuloidaan ihmisiä esim. sosiaalisen median kautta
  - Spear-phishing
    - Kalastelu, jossa kalastelu kohdistetaan mahdollisimman tarkasti kohteeseen
  - Toimitusketjut
    - Hyödynnetään laitetta, ohjelmistoa tai palveluita, jotka toimittaja toimittaa organisaatioon tai alukseen
  - Brute-force
    - Kokeillaan ohjelmallisesti eri salasanoja oikean salasanan löytämiseksi. Käytössä esim. heikot salasanat, salasanavuodoista löydetyt salasanat ja sanakirjasanat, niiden muunnokset ja yhdistelmät.
  - Palvelunestohyökkäys (DoS)
    - Estetään palvelun käyttö sen oikeutetuilta käyttäjiltä esim. lähettämällä palveluun paljon dataa
  - ...



https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Figure 6: Threat taxonomy



https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

5 APPENDIX B Summary of key findings and recommendations

Finding	Recommendations	Time line
Low awareness and focus on maritime cyber security	• Design and launch awareness raising campaigns • Develop appropriate trainings	Short term Mid term
Complexity of the maritime ICT environment	Build strategies and good practices defining security requirements for ICT implementations in the maritime sector.	Short term
Fragmented maritime governance context	• International level: align and harmonize international and European policies on maritime cyber security requirements; • European level: define clear roles and responsibilities for addressing cyber security matters in the maritime sector; • National/regional level: enforce European standards (develop standards and enforce rules in the core text) for ports requirements on ICT systems.	Long term Mid term Long term
Inadequate consideration of cyber security in maritime regulation	Take appropriate measures in order to add considerations towards cyber security in the regulatory frameworks governing the maritime sector.	Mid term
Absence of a holistic approach to maritime cyber risks	Define and implement a holistic, risk-based approach to address the subject of maritime cyber security.	Mid term
Overall lack of direct economic incentives to implement good cyber security in the maritime sector	Stimulate dialogue and information exchange between key stakeholders in the maritime sector and connected stakeholders (e.g. insurance brokers).	Short term
Inspiring initiatives	Establish information exchange platforms based on the ISAC model (trust-based public-private partnerships).	Long term

Merenkulun kyberturvallisuusuhkien taustaa

- Paljon toimijoita, jotka vuorovaikutuksessa toisiinsa ”system of systems”
- Nojaa salaamattomaan viestintään (esim. navigaatio), joka toteutettu saatavuus edellä
- Aluksissa yhä enemmän digitalisaatioon, integraatioon ja automaatioon perustuvia järjestelmiä
- Aiemmin käytetty suurilta osin spesifisiä laitteita ja ohjelmistoja. Digitalisaation myötä muodostuu uudenlainen digitaalinen ympäristö, jota ei tunneta
- Digitaali- ja viestintäteknologian kehitys on mahdollistanut informaatiojärjestelmien (IT) ja operatiivisten järjestelmien (OT) integroinnin
- OT-järjestelmät, joita käytetään mm. moottoreiden ja niihin liittyvien järjestelmien hallinnointiin, lastinkäsittelyyn ja navigointiin, ovat perinteisesti olleet eristettyinä toisistaan ja ulkoisista järjestelmistä, mutta niitä integroidaan yhä enenevissä määrin.
- IT- ja OT-järjestelmien yhdentyminen aluksissa ja niiden yhteydet internetiin lisäävät hyökkäyspinta-alaa
- Kyberhyökkäykset voivat vaikuttaa OT-järjestelmiin ja uhata esim. navigoinnin turvallisuutta (safety) tai koko aluksen turvallisuutta (security)
- Muilta turvallisuuden (safety ja security) osa-alueilta on historiaa saatavilla, mutta kyberhyökkäyksistä ja niiden vaikutuksista on vain vähän tietoa saatavilla. Tekee kyberuhkien hallinnasta monimutkaisempaa

Merenkulun OT-järjestelmiä

- Vessel Integrated Navigation System (VINS)
- Global Positionin System (GPS)
- Satellite Communications
- Automatic Identification System (AIS)
- Power generation
- ...

OT-järjestelmien haasteita kyberturvallisuuden näkökulmasta

- OT-järjestelmillä reaaliaikainen suorituskykyvaatimus ja toiminta aikakriittistä
- OT-järjestelmien turvallisuus (safety) ja vikasietoisuus välttämätöntä
- Pääsy OT-järjestelmiin on valvottava, mutta ihmisen ja koneen vuorovaikutus varmistettava
- Käyttökatkot eivät ole välttämättä hyväksyttävissä
- OT-järjestelmien päivitykset ja korjaukset usein toteutettava ilman huoltokatkoa ja toimittajan toimesta
- OT-järjestelmien pitkä elinkaari
- OT-järjestelmät ovat monimuotoisia - omat protokollat ja käyttöjärjestelmät ilman sulautettuja tietoturvaominaisuuksia
- OT-järjestelmät on suunniteltu tukemaan tiettyä operatiivista prosessia eikä niissä ole välttämättä tarpeeksi muistia ja laskentaresursseja tietoturvaominaisuuksien lisäämiseksi

Kybersää Heinäkuu 2020

Tietomurrot ja -vuodot

- Havaintoja suomalaisista murretuista PulseSecure- ja Netscaler-palvelimista ja haavoittuvista BIG-IP-palvelimista.
- Office 365 –tietomurtojen määrä jälleen nousussa kesän hiljaisemman ajan jälkeen.

Huijaukset ja kalastelut

- Tietojenkalastelu on ammattirikollisten aktiivisesti käyttämä työkalu, jonka merkitys verkkohuijauksissa on korostunut.
- Puhelinhuijaukset ovat palanneet karanteenitauon jälkeen. Suomeen tulee satojatuhansia huijauspuheluita.

Haittaohjelmat ja haavoittuvuudet

- Ransomware-toimijat huutokauppaavat varastettuja tietoja tavoitteenaan rahastaa tiedoilla.
- Heinäkuussa julkaistiin kriittisiä haavoittuvuuksia ja verkkolaitteisiin kohdistuneita haavoja käytettiin aktiivisesti hyväksi.

Automaatio

- Yhdysvaltain viranomaiset varoittivat lisääntyneestä kyberhyökkäysten uhkasta automaatiojärjestelmiä vastaan.
- Automaatiojärjestelmiä koskevia haavoittuvuuksia löytyy entistä useammin.

Verkkojen toimivuus

- Vain kolme merkittävää yleisten viestintäpalveluiden häiriötä.
- DigiCert mitätöi useita varmenteita 11.7., mikä vaikutti myös useiden suomalaisten palveluiden toimintaan.
- Heinäkuu oli palvelunestohyökkäysten osalta Suomessa rauhallinen.

Vakoilu

- EU on ryhtynyt ensimmäistä kertaa aktiivisiin vastatoimiin valtiollisia kyberhyökkäyksiä vastaan pakotteiden muodossa.
- Kohdistettujen hyökkäysten tavoitteena ei ole vain vakoilu, vaan myös vaikuttaminen ja ydinaseohjelman rahoittaminen.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Automaatio

- Automaatiojärjestelmien VPN-tuotteista paljastui kriittisiä haavoittuvuuksia.
  - Haavoittuvuuksien hyväksikäytäjä voi ottaa hallintaansa useita osia internetiin kytketyistä automaatiojärjestelmistä.
  - https://www.claroty.com/2020/07/28/vpn-security-flaws/
- USB-muistitikut ovat edelleen keskeisiä haittaohjelmien leviämisessä automaatiojärjestelmiin.
  - Honeywellin tekemä tutkimus osoitti, että 45 %:iin automaatiojärjestelmistä on vuoden aikana yritetty hyökätä USB-muistitikun välityksellä.
  - https://www.scmagazine.com/home/security-news/vulnerabilities/usb-prevalent-industrial-vector-vulnerability-for-ot-systems/

ANALYYSI

- Haavoittuvuuksia löytyy enemmän paitsi lisääntyneiden hyökkäysten myötä myös siksi, että tietoturvatutkijat käyttävät entistä enemmän aikaa automaatiotuotteiden tutkimiseen. Myös IT-järjestelmien VPN-tuotteiden haavoittuvuuksia on tutkittu runsaasti viimeisten 12 kk aikana.
- Järjestelmien omistajien täytyy nopeuttaa korjaavien ohjelmistopäivitysten käyttöönottoa.

Automaatio

- Yhdysvaltain turvallisuusviranomaiset varoittivat kyberhyökkääjien kasvaneesta mielenkiinnosta automaatiojärjestelmiä kohtaan.
  - Internetin kautta automaatiojärjestelmiin hyökkäämisestä on tullut entistä helpompaa.
  - Varoituksessa on kuvattu hyökkääjien toimintaa sekä tehokkaita keinoja hyökkäysten torjumiseksi.
  - https://us-cert.cisa.gov/ncas/alerts/aa20-205a

ANALYYSI

- Kyberhyökkääjät ovat edelleen kiinnostuneita automaatiojärjestelmistä. Järjestelmät kiinnostavat sekä nopean rahanteon motivoimia rikollisia että strategiseen vaikuttamiseen pyrkiviä toimijoita.
- Toiminnan keskeytyminen on yleensä suurin riski.
- Torjuntakeinot ovat tuttuja ja pääosin teknisesti yksinkertaisia, mutta valitettavan usein niiden huolelliseen toteuttamiseen ei ole riittäviä resursseja.

Top 5 kyberuhat – merkittävät pidemmän aikavälin ilmiöt

1

Laajavaikutteiset kiristyshyökkäykset (Big Game Hunting) uhkaavat liiketoiminnan jatkuvuutta. Yksittäisten tapausten vahingot ovat nousseet kymmeniin miljooniin euroihin.

- Tapauksia myös Suomessa. Suurin osa organisaatioista valikoituu kohteeksi heikon tietoturvan takia.
- Kyberrikolliset etsivät jatkuvasti verkosta haavoittuvia palveluita ja huonoja salasanoja sekä levittävät haittaohjelmia sähköpostitse.
- Uusia ilmoituksia laajoista kiristyshaittaohjelmatartunnoista tulee kansainvälisesti viikoittain. Lisäksi uusia toimijoita tulee jatkuvasti. Esimerkkinä tästä on ICS-toimijoihin kohdistuva EKANS.
- Kiristyshyökkäysten uutena ilmiönä kohdetta kiristetään myös hyökkääjän haltuun saamien tietojen myymisellä, vuotamisella tai julkaisemisella lunnasvaatimuksen tehostamiseksi.

CASE

UUSI

Satelliittipaikannuslaitteita valmistava Garmin joutui 23.7. WastedLocker-kiristyshaittaohjelman uhriksi. Hyökkäys keskeytti Garminin palvelut useaksi päiväksi ja vaikutti muun muassa älyurheilukellojen toimintaan sekä ilmailun navigointiin ja palveluihin.

Lunnasvaatimuksen kerrotaan olleen 10 miljoonaa dollaria. Uutissivusto Bleepingcomputer sai haltuunsa Garminin käyttämän palautustyökalun, joka viittaa siihen, että Garmin olisi maksanut lunnaat.

CERT-EU: Kiristyshyökkäyksiä liikennesektorilla

- CERT-EU: Ransomware in the transportation sector, Threat Memo - TM 20-009 - Date: 21/01/2020 - Version: 1.0, TLP:WHITE
  - Liikenne ja logistiikkasektorin toimijat ovat erityisen houkuttelivia kohteita kiristyshaittaohjelmatoimijoille. Onnistuneita hyökkäyksiä on ollut usein.
  - Liikennesektorin organisaatiot voivat olla opportunisten rikollisten kohde siinä missä mikä tahansa organisaatio millä tahansa sektorilla.
  - Liikennesektorin infrastruktuuri on osa kriittistä infrastruktuuria ja on siksi ollut valtiollisten toimijoiden kiristyshyökkäyksien kohteina. Ko. hyökkäyksien tavoitteena on aiheuttaa vieraalle valtiolle sekasortoa ja kaaosta.
  - Big game hunting (BGH) –taktiikan hyödyntäminen, joissa yhdistetään kohdistettu hyökkäys ja kiristyshaittaohjelma, on lisääntynyt. BGH-hyökkäyksien tavoitteena on saada rahaa. Niiden kohteena on tyypillisesti organisaatiot, joilla ei ole varaa häiriöihin.
  - Hyökkääjien kiinnostuksen kohteena ovat todennäköisimmin ilmailun lennonjohdon järjestelmät, rahtiprosessit ja lentokoneet sekä merenkulun isot infrastruktuurit kuten satamat.

Yhdysvaltain turvallisuusviranomaiset ovat varoittaneet merenkulkualaa

- Haittaohjelma oli vaikuttanut laajasti aluksen tietokonejärjestelmään, mutta ei välttämättömiin aluksen ohjausjärjestelmiin
- Kyberhyökkäyksen jälkeisissä tutkimuksissa oli todettu
  - Aluksessa ei ollut toimivia kyberturvallisuussuojauksia kyseistä hyökkäystä vastaan
  - Merkittäviä haavoittuvuuksia kriittisissä aluksen ohjausjärjestelmissä
- Turvallisuusriski oli miehistön tiedossa jo ennen tapahtumaa
- Useimmat miehistöstä eivät olleet käyttäneet aluksen tietokoneita henkilökohtaiseen sähköposti-, verkko-ostamis- ja pankkiasiointikäyttöön
- Alusverkkoa oli käytetty viralliseen liiketoimintaan kuten sähköisten karttojen päivittämiseen, lastitietojen hallintaan ja kommunikointiin eri sidosryhmien kanssa
- Yhdysvaltain turvallisuusviranomaiset julkaisivat tapahtuman jälkeen turvallisuusvaroituksen (marine safety alert) https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf
- Varoituksessa suositeltiin
  - Tietoverkkojen segmentointia
  - Käyttäjäkohtaisia profiileja ja salasanoja
  - Ulkoisten medioiden kuten usb-tikkujen suhteen varovaisuutta
  - Antivirusohjelmistojen asentamista
  - Päivityksistä huolehtimista

Maersk

- Maersk joutui laajan kyberhyökkäyksen kohteeksi kesäkuussa 2017
- NotPetya-kiristyshaittaohjelma
- 300 milj. USD vahingot
- Organisaation tietojärjestelmät ympäri maailman oli hetkessä pois käytöstä. Vaikutti kaikkiin liiketoimintayksiköihin.
- Kahdeksan päivän päästä hyökkäyksestä Maersk onnistui jatkamaan online-varausten tekemistä, vaikka joitain terminaaleja jouduttiin käsittelemään manuaalisesti.

https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/
https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO

Oppimaa

- Kyberuhkalla on aina mahdollisuus päästä sisään. Organisaatioiden tulee rakentaa kyvykkyys vastata hyökkäykseen ja toipua hyökkäyksestä.
- Liiketoiminnan jatkuvuuden kannalta ylimmän johdon ohjaus ja päätökset operatiivisella tasolla ja median käsittelyssä elintärkeitä.
- Kaikkien työntekijöiden tulee olla tietoisia kyberuhkista ja reagointisuunnitelmista.
- Reagointi- ja palautumissuunnitelmat tulee testata ja päivittää usein huomioiden uusien kyberuhkien lieventämistoimet.
- Ennakoiva toiminta välttämätöntä. Organisaation turvaaminen ja työntekijöiden tietoisuuden lisäämisen on edullisempaa kuin kyberhyökkäyksestä aiheutuneet kustannukset.

Kiitos!

virpi.tuulaniemi@traficom.fi

TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus