HDI Risk Consulting

Cyberrisico's aan boord van schepen

www.hdi.global

INFORMATIEKAART

Voorkom schade door cyberrisico´s.

Tegenwoordig is de informatie en operationele technologie aan boord van schepen zeer complex. Schepen bevatten veel systeemnetwerken die in toenemende mate met elkaar verbonden zijn. Denk aan brugsystemen, voortstuwings- en machine-installaties, vermogenregelsystemen, etc. Maar ook systemen zoals passagiersservicesystemen, communicatiesystemen en dergelijke. Een belangrijk risico van deze systemen is de blootstelling aan kwaardaardige cyberaanvallen. Deze informatiekaart geeft een beeld van de kwetsbaarheden en bedreigingen van cyberaanvallen op schepen.

Cybercriminelen

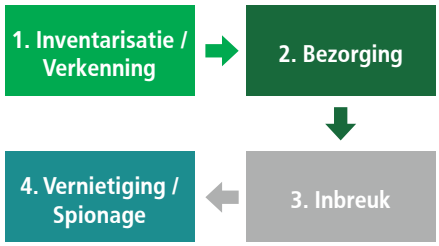
Cybercriminelen zijn naar motivaties en doelstellingen onder te verdelen in vier groepen:

Groep	Motivatie	Doelstelling
Activisten	Reputatieschade, verstoring van de activiteiten	Vernietiging van gegevens, publicatie van gevoelige gegevens, media-aandacht
Opportunisten	De uitdaging	Doorbreking van de beveiliging van cybersystemen, financieel gewin
Criminelen	Financieel gewin, bedrijfsspionage, industriële spionage	Verkopen van gestolen gegevens, gijzelen van gegevens of het volledig beheer van het systeem, frauduleus vervoer van vracht regelen.
Staten, door de staat gesponsorde organisaties, terroristen	Politiek gewin, spionage	Kennis vergaren, economie of kritieke nationale infrastructuur ontwrichten

Er zijn twee verschillende soorten aanvallen: doelgerichte en niet doelgerichte aanvallen. Niet doelgerichte aanvallen zijn aanvallen op de systemen en gegevens van schepen, zoals social engineering, phishing, scannen en ransomware. Doelgerichte aanvallen zijn aanvallen op specifieke systemen of gegevens. Denk aan spear phishing, (D)DoS aanvallen of het ondermijnen van de supply chain.

De anatomie van een cyberaanval

De anatomie van een cyberaanval die cybercriminelen normaal gebruiken is als volgt:



De eerste stap is het verzamelen van informatie hoe door te dringen in de systemen van een schip of bedrijf door aanwijzingen te zoeken in sociale media, technische forums, publicaties, enzovoorts. De tweede stap is het leveren van de malware door het te verzenden als een kwaadaardige bijlage in een e-mail of het verstrekken van geïnfecteerde draagbare media of andere methoden. De derde stap is het verkrijgen van toegang tot het systeem om volledige controle te krijgen of het stelen van gevoelige gegevens of iets anders. De vierde stap is het verkopen of vernietigen van de gevoelige gegevens.

Wat zijn de risico's?

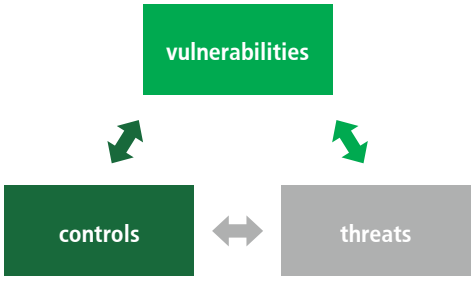
Aan boord van schepen zijn veel systemen beschikbaar die door cybercriminelen kunnen worden aangevallen:

- vrachtbeheersystemen;
- brugsystemen;
- voortstuwings- en machinebeheersystemen;
- electriciteitssystemen;
- toegangscontrolesystemen;
- systemen voor administratie van passagiers;
- openbare netwerken voor passagiers;
- administratieve systemen en systemen voor de bemanning;
- communicatiesystemen;
- belangrijke infrastructuursystemen.

Ook leveranciers en contractpersonen vormen een veiligheidsrisico, omdat zij op de hoogte zijn van de activiteiten op schepen en vaak volledige toegang hebben tot de systemen van een schip. Technici van derde partijen vormen ook een risico, omdat zij op afstand toegang hebben tot de systemen van het schip om gegevens te lezen voor onderhoudsdoeleinden.

Preventie

Om verlies als gevolg van een cyberaanval te kunnen voorkomen, moet het hoger management op de hoogte zijn van de verschillende soorten aanvallen. Het is belangrijk om objecten van een schip of bedrijf te beoordelen op cyberrisico's. Objecten zoals software, hardware, infrastructuur, bemanningsleden, etc. Identificeer de kwetsbaarheden van deze objecten en identificeer de bedreigingen die daarop van invloed zijn.



Bepaal de waarschijnlijkheid dat kwetsbaarheden door deze bedreigingen worden gebruikt. Maak een beschermingsplan en neem maatregelen om de risico's zo veel mogelijk te beperken.

Ontwikkel een incident response plan om de impact van bedreigingen op de veiligheid en beveiliging van het schip zoveel mogelijk te verminderen (calamiteitsplannen). Reageer op cyberincidenten met behulp van dit incident response plan. Beoordeel de impact van de effectiviteit van het incident response plan en evalueer bedreigingen en kwetsbaarheden opnieuw.

Cyber bewustwording

Bewustwording van cyber security is essentieel om cyberrisico's aan boord van schepen te verminderen. Opleiding, workshops en schriftelijke procedures kunnen bijvoorbeeld helpen om bemanningsleden bewuster te maken van de risico's en mogelijke gevolgen van cyberaanvallen.

Meer informatie is te vinden op:
www.bimco.org
www.nist.gov/cyberframework

Contact

Voor vragen kunt u contact opnemen met:
HDI Risk Consulting
T: +31 (0)10 – 40 36 328
hrc@nl.hdi.global
www.hrc-services.nl

Benefits of HDI Risk Consulting

- HDI Risk Consulting Professionals offer risk and safety related analysis to enable specific risk prevention action plans to be developed.
- Qualified international Risk Engineering network offers clients worldwide multi-discipline support in Risk Engineering.
- HDI Risk Consulting is a wholly owned subsidiary of HDI Global SE and thus part of the Talanx Group, one of the largest insurance groups in Germany and Europe.

403-HRC245NL 201907