IVR TECHNISCH BULLETIN

CYBERSECURITY IN DE BINNENVAART

BEVEILIGING TEGEN CYBERAANVALLEN

Met de toenemende technologische ontwikkelingen in de binnenvaart is het essentieel om na te denken over het minimaliseren van de risico's rond cyberaanvallen. Een goed doordacht cybersecurity plan is een fundamenteel onderdeel van de bescherming van uw schip en uw organisatie.

Daarom heeft IVR dit bulletin samengesteld om u enkele tips en trucs te geven voor het implementeren van een duurzaam cybersecurity plan.

CYBERSECURITY

- IDENTIFICEER
- BESCHERM
- DETECTEER
- REAGEER
- HERSTEL

1 Identificeer

Welke systemen zijn kwetsbaar voor aanvallen, welke systemen zijn essentieel voor de bedrijfsvoering en wie is daarvoor verantwoordelijk?

- Brug

ECDIS-systemen maken mogelijk gebruik van online bij te werken 'pay-as-you-sail' foliotoegang, maar zijn ze veilig?

- Laad- en stabiliteitsprogramma's

Het kopiëren of uitvoeren van geautoriseerde programma's van derden, zoals een beladingsprogramma, kan schadelijke software op het systeem introduceren.

- Machinekamer

Elk apparaat met een ingebouwde computer kan worden aangevallen - laat geen enkel systeem kwetsbaar.

IS UW WACHTWOORD EEN VAN DE MEEST GEBRUIKTE?

- 123456
- qwerty
- letmein
- admin
- dragon
- companyname123

Tip: een reeks van drie willekeurige woorden zorgt voor een sterk, gemakkelijk te onthouden wachtwoord.

2 Bescherm

Neem onderstaande maatregelen om cyberaanvallen te voorkomen.

- Werk apparaten regelmatig bij om beveiligingsproblemen te verhelpen.
- Beveilig alle apparaten met een wachtwoord en houd ze vergrendeld wanneer ze niet worden gebruikt.
- Sta alleen de aangewezen bemanning toe om belangrijke systemen te gebruiken.
- Moet het apparaat online en verbonden zijn?
- Zijn firewalls op het hele netwerk geïnstalleerd?
- Download geen software van verdachte bronnen.
- Open geen bijlagen bij e-mails van onbekende afzenders.
- Gebruik geen externe apparaten op het systeem zonder een beveiligingsscan.
- Als het er verdacht uitziet of lijkt, STOP dan direct.

3 Detecteer

Als er toch een aanval plaatsvindt, kan de schade worden beperkt door deze snel te herkennen.

- Een up-to-date antivirusprogramma kan eventuele gevaren controleren.

- Scan computers, laptops en andere externe apparaten regelmatig.

- Heeft een download afwijkend gedrag veroorzaakt? Wees achterdochtig en isoleer het systeem.

- Bereid een checklist voor om ervoor te zorgen dat er geen apparaten worden gemist.

4 Reageer

Plan een duidelijke manier om zo snel mogelijk weer aan de slag te gaan met een tweede systeem. Secundaire apparaten en systemen moeten:

- Geïsoleerd zijn van het hoofdsysteem.
- Up-to-date gehouden worden en klaar staan voor gebruik.
- Geschikt zijn voor het uitvoeren van alle kritieke bedrijfsprocessen.

HANDIGE LINKS

- https://www.ccr-zkr.org/13020152-en.html
- https://twitter.com/Cybersec_EU
- https://www.pianc.org/publications/inland-navigation-commission/tg204
- https://europa.eu/european-union/about-eu/agencies/enisa_en
- https://www.shipownersclub.com/lossprevention/cyber-security

5 Herstel

Zet het primaire systeem weer aan en analyseer de oorzaak.

RESET HET SYSTEEM → HERSTEL VAN BACKUP → ONDERZOEK OORZAAK → UPDATE PROCEDURES

Blijf op de hoogte

IVR zet zich in om waardevolle bijdragen te leveren op het gebied van schadepreventie in de binnenvaart.

Zorg ervoor dat u een plan heeft, dat u voorzorgsmaatregelen treft en bereid bent om te reageren. Dit kan voorkomen dat uw organisatie het volgende slachtoffer wordt van een cyberaanval.