Cyber Security Policy

DOCUMENT updated Wednesday, May 31, 2019

Table of Contents

WHAT IS CYBER SECURITY

Computer security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection, and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.

The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies, wireless networks such as Bluetooth and Wi-Fi - and the growth of "smart" devices, including smartphones, televisions and tiny devices as part of the Internet of Things.

CYBER SECURITY ONBOARD SHIPS

The safety, environmental and commercial consequences of not being prepared for a cyber incident may be significant. Responding to the increased cyber threat, a group of international shipping organizations, with support from a wide range of stakeholders, have developed the document; “THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS”, which are designed to assist companies develop resilient approaches to cyber security onboard ships.

Furthermore, “THE INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT” issued by IMO provide high-level recommendations on maritime cyber risk management to safeguard shipping and include functional elements that support effective cyber risk management. Based on these two documents and IT security in general, NAVTOR has acted and implemented a risk control process to protect the e-navigation products and services distributed to the bridge systems.

NAVTOR AND CYBER SECURITY

Even though we have acted to protect the NAVTOR e-Navigation products and services, it is essential that the users establish their own Cyber Security Procedures and follow the recommendations and guidelines related to NAVTOR products and services in this document.

NAVTOR E-NAVIGATION SOLUTIONS

Using the most efficient e-Navigation technology and delivery platforms, NAVTOR simplify tasks, increase efficiency and improve operations. Every day we work on fine-tuning our services. This makes life easier for navigators, and safer, clearer and more efficient for ship-owners, ship managers and operators. Hence, we have developed these guidelines and recommendations to support your company's Cyber Security Policy.

NAVBOX

STANDARD SECURITY FEATURES

- Data is downloaded over an encrypted connection (HTTPS)
- No executable files are transferred
- If data should be tampered with during transmission, it will be discarded by the NavBox (fails CRC)
- No Auto-Play functionality is enabled on the NavBox
- NavBox uses NTFS for file system security and integrity
- NavBox only reads files from USB that have been digitally signed
- Unique admin passwords for each NavBox to prevent unauthorized logons. Passwords are automatically changed every 30 days
- User accounts are automatically locked out after 3 failed password attempts.
- The NavBox share used for loading ENCs on ECDIS is read-only
- If ECDIS is connected to NavBox via LAN, the need for USB is eliminated

IEC61162-460 TYPE APPROVED

- NavBox runs Windows Firewall which only allows required traffic to pass
- The NavBox share used for loading ENCs on ECDIS is password protected and read-only
- SMBv1 support is disabled
- Only USB mass storage devices will be recognized. Other USB devices like keyboard, mouse, Wi-Fi dongles++ will not be recognized by the NavBox
- NavBox runs UAC (User Access Control) meaning that all user-initiated processes will run non-elevated

STANDARD REQUIREMENTS

- None other than the NavStick USB drive must be connected to the NavBox, unless instructed to by NAVTOR
- The NavBox should not be logged on to locally (connecting KVM), unless instructed to by NAVTOR
- The NavStick must not be used for other purposes than updating the ECDIS.
- The crew must always ensure proper USB hygiene (ref. BIMCO cyber security policy)
- If connecting GPS/AIS signals, only Rx pins should be used on the NavBox (NavBox does not transmit data to GPS/AIS)

IEC61162-460 TYPE APPROVED REQUIREMENTS

- The NavBox must be mounted in a physically protected location requiring a key or tool to gain access (e.g. a bridge console or cabinet)
- GPS/AIS serial connection to NavBox must be made via supplied opto isolator plug
- Network cables used with NavBox must be shielded (STP). Minimum CAT5e
- Email cannot be used as a communication bearer, only HTTPS
- The NavBox must have static IP addresses assigned on both network adapters ("ECDIS" and "INTERNET"). The IP addresses must be in one of the following IP ranges:
    - 10.0.0.0 – 10.255.255.255
    - 172.16.0.0 – 172.31.255.
    - 192.168.0.0 – 192.168.255.255

RECOMMENDATIONS

- The NavBox should preferably be connected to the admin/business LAN (not crew LAN), for optimal security and performance
- NavBox should be placed behind a physical firewall and no incoming connections from internet must be allowed through the firewall to the NavBox
- For enhanced security, only outgoing traffic to the two required NAVTOR IPs/URLs should be allowed from the NavBox through the vessel's firewall

NAVSYNC

SECURITY FEATURES

- Data is downloaded over an encrypted connection (HTTPS)
- No executable files are transferred
- If data should be tampered with during transmission, it will be discarded by NavSync (fails CRC)
- NavSync scans for and deletes all unknown files from the NavStick after each update

REQUIREMENTS

- The PC running NavSync should be running an updated antivirus/antimalware solution
- The NavStick must not be used for any other purposes than running NavSync and updating the ECDIS
- The NavStick should be stored in a safe place when not in use
- The crew must always ensure proper USB hygiene (ref. BIMCO cyber security policy)

RECOMMENDATIONS

- The PC running NavSync should have the "AutoPlay" functionality in Windows turned off
- The PC running NavSync should be kept updated with the latest OS patch updates

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS

Download from the BIMCO website: https://www.bimco.org

THE INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

Download from the IMO website: http://www.imo.org