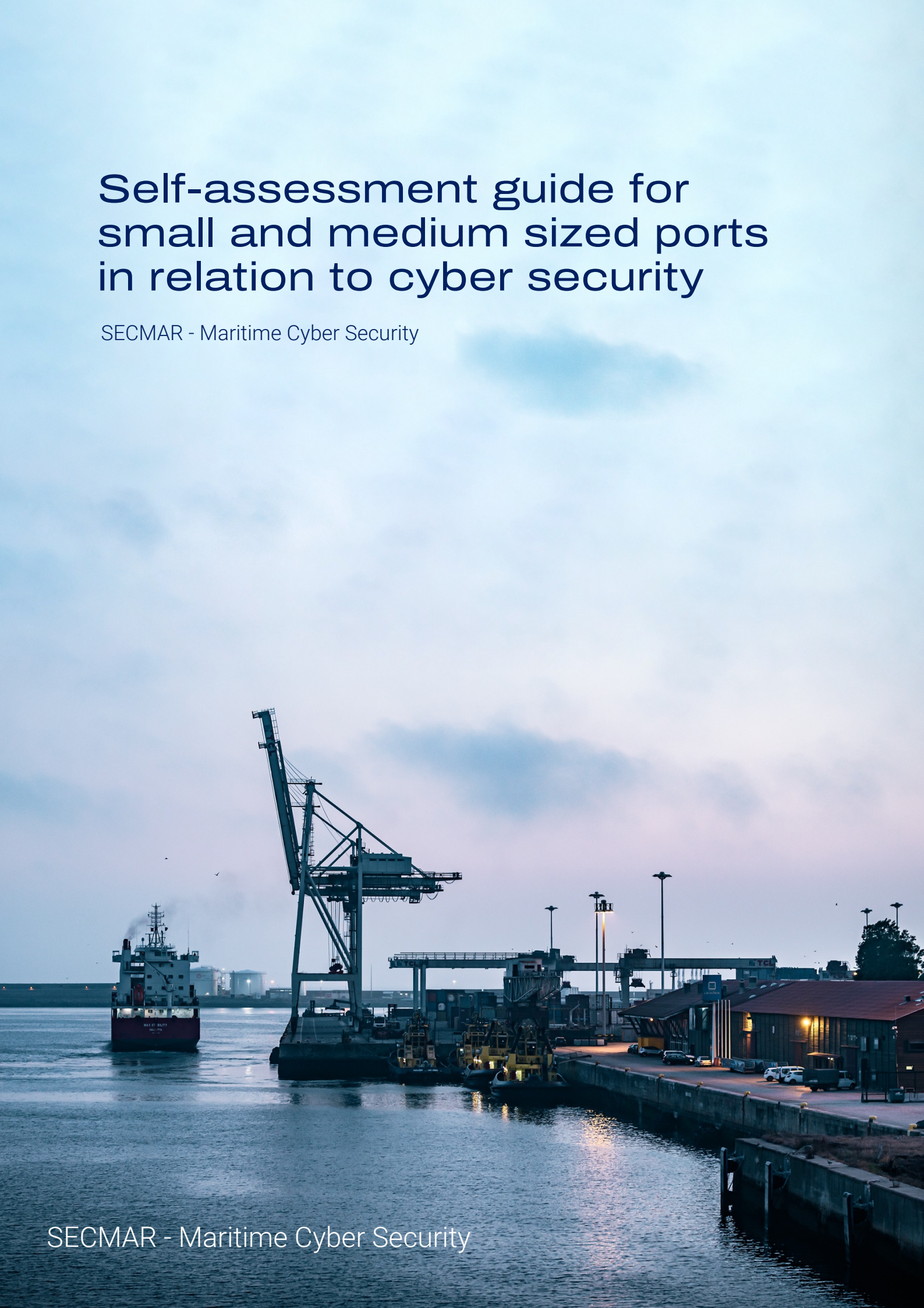
Self-assessment guide for small and medium sized ports in relation to cyber security

SECMAR - Maritime Cyber Security



SECMAR - Maritime Cyber Security

Table of Contents

Introduction

Hey! Do you work with IT in relation to ports? Let us have a couple of minutes of your time. The world of the maritime transport sector is undergoing a rapid digital transformation. But as dataflows grow in number, and devices, systems and global maritime networks start to interconnect we also become more vulnerable to cyberattacks. Therefore, the InterReg South Baltic Programme 2014-2020 decided to fund the SECMAR project. SECMAR (or Secure Digitalisation for Sustainable Maritime Transport) deals with the emerging field of maritime cybersecurity. The aim of SECMAR is to increase the level of security and build up the competence on cyber security in the South Baltic Sea area, in the ongoing digitalisation of the shipping and logistics sector. One of the problem areas that the project has defined is a lack of basic knowledge regarding cyber security in the maritime industry. That is why SECMAR put together this cyber security self-assessment checklist for ports. To help guide IT-professionals in the maritime industry and enable them to safeguard their road to a more digitized industry. Safe at sea, safe IT. We hope you find it useful!

Definitions

Throughout the document, the terms Software and Hardware are used in various contexts. For the avoidance of doubt, the terms are defined as below.

*** Software includes applications, operating systems, firmware, and drivers**

** Hardware includes computers, servers, printers, mobile phones, switches or wireless access points, and firewalls

*** Critical systems include all assets that are defined as critical to the business processes, including but not limited to, infrastructure components such as firewalls, Domain Controllers, Active Directory, File shares, DNS and DHCP, ERP-systems, HR-system and production systems.

Section 1: Governance & Organization

In order to secure the IT estate, it is crucial that each company has a detailed understanding of which assets are part of the estate, and what their functions are. It is also necessary to have dedicated owners to each asset, to make sure that each asset is kept up to date and removed when no longer needed. Further, it is important that all employees have an understanding of the importance of cyber security and privacy, and that IT staff are fully aware of how the company protects its estate.

1.1 You have a complete inventory of all software* used by your company, to ensure that you have a complete insight into the estate.

1.2 You have a complete inventory of all hardware** used by your company, to ensure that you have a complete insight into the estate.

1.3 All software used within your company have an internally named owner that is responsible for user onboarding/offboarding, supplier relations, lifecycle management, maintenance including patch management, risk management, and decommissioning for that application.

1.4 All hardware used within your company have an internally named owner that is responsible for user onboarding/offboarding, supplier relations, lifecycle management, maintenance including patch management, risk management, and decommissioning for that application.

1.5 You know which software and hardware are business critical for your company.

1.6 All software is still supported by the vendor and all hardware is supported by the manufacturer. If you have any software that is out of support, this should be documented and a plan to replace the software created.

1.7 Software and hardware that are considered legacy or cannot be actively updated are protected by extra security controls. Examples of these could be isolation through an air gap or offline implementations.

1.8 All security updates to software and hardware (including Operational Technology) are applied not later than a month from when they are released from their manufacturer or software supplier.

1.9 All Internet exposed systems patches are applied within a week from release.

1.10 You have adopted a roadmap with planned improvements for the coming years which is presented to the company board on an annual basis.

1.11 All employees are trained in cyber security awareness and privacy awareness at least on an annual basis.

1.12 All employees with privileged access rights are trained in the implemented cyber security controls to ensure sufficient knowledge about the protection of the environment.

1.13 You have created a Disaster Recovery Plan for cyber incidents with clear actions and responsibilities that outlines how you as a company will act in case of an IT emergency. The plan must be documented and approved by the board or executive management. Make sure to have paper copies available in strategic locations.

1.14 There is a written Business Continuity Plan, produced by the operational part of the company, reviewed and approved by the board or executive management that outlines how operations will be maintained without the support of IT.

Section 2: Detection and logging

In order to counter an attack, it is necessary to have ways to detect anomalous activity on the networks. This will allow you to understand the nature of the attack, as well as take the appropriate measures to mitigate the attack. By not having relevant and necessary means to detect malicious activity, a company will be completely reliant on its ability to keep attackers outside of the network, an effort that is considered impossible.

Log creation and storage is a critical component of detecting ongoing potentially harmful activity, as well as investigating how an actual incident happened. It is also necessary to ensure that an attacker is safely removed from the network.

Increasing detection capabilities is one of the quickest ways to achieve some level of resilience towards cyber-attacks, while an organization is working to increase its cyber security capability in other areas.

2.1 You have the ability to actively detect and respond to intrusions on clients, servers, and services 24/7/365.

2.2 An Endpoint Detection & Response (EDR)-platform is deployed, covering all servers that are capable of carrying an EDR.

2.3 An EDR-platform is deployed, covering all endpoints that are capable of carrying an EDR.

2.4 All critical systems*** log access attempts (both successful and denied) and privileged activities.

2.5 Logfiles are protected in such a way that they can't be accessed from the system that created them.

2.6 All log files have a retention period of no less than 100 days.

In addition to the above, each company is also encouraged to implement Network Detection & Response (NDR) capabilities for network segments that don't support EDR implementations, as well as deploying Security Incident Event Management (SIEM) capabilities on cloud services and web-based systems.

Section 3: Backup and disaster recovery

The vast majority of ransomware attacks include attacks on the backups of the victim's networks. If this part of the attack is successful, the restoration time after the attack is significantly longer than if backups can be restored, multiplying the financial and reputational impact of the attack.

3.1 All data used by critical systems*** within your company must exist in 3 copies. One copy is the live data you are using. Then backup is made to two different media, like disk and tape for example. One of these backups is stored off-site and offline, completely separated from your production environment.

3.2 Restore verification tests are performed regularly, where the verification involves more than just individual file restorations.

3.3 Backups of critical systems*** are made at least on a daily basis.

Section 4: Malware protection

While traditional means of protecting against malicious software are considered inadequate as the sole defence layer, they still form part of the defence strategy and protect the company from less sophisticated attacks. By filtering malicious emails, a company can avoid allowing an attacker to establish a foothold on the network.

4.1 All clients and servers have updated and running antivirus/antimalware software.

4.2 All clients and servers have the local firewall configured and turned on.

4.3 There are tools and processes in place to ensure that all e-mail attachments and links are scanned and reviewed before released to the user´s mailbox.

4.4 Autorun on attachable media is by default turned off.

Section 5: Access Management

A very common component of attacks includes the use of elevated privileges. This means that an attacker acquires the credential of a legitimate employee, and then uses these credentials for access to the network. Commonly, this involves accounts of employees that have left the organization, or of employees that have been given rights to perform certain actions on the network, so called privileged users. By restricting access to the needs of every user, the chance for an attacker to succeed in establishing a foothold on the network is greatly reduced.

5.1 Employees are only granted enough access to files, folders, and applications to perform their job responsibilities.

5.2 All accounts are unique accounts per individual and never shared between individuals.

5.3 No employees or IT staff are local administrators on computers with their normal account that is used on a daily basis. There are tools and processes in place to ensure that elevated access rights are granted only temporarily.

5.4 There is an implemented off-boarding process that secures that all user rights are revoked when a user leaves the company.

5.5 All user accounts and rights are reviewed, at least on an annual basis.

5.6 All privileged accounts are reviewed continuously.

5.7 There is a password policy in place that requires users' passwords to be of a minimum length of 15 characters and include special characters and upper- and lower-case characters.

5.8 There is a password policy in place that requires privileged account passwords to be of a minimum length of 25 characters and include special characters and upper- and lower-case characters.

5.9 External access to all applications (not including from internal networks), regardless of software vendor, is protected by multi-factor authentication.

5.10 All privileged accounts, where possible, are managed by a Privileged Access Management Solution (PAM) that supports the principles of just in time and just enough rights.

5.11 All administration of the IT environment is performed from a separate computer, such as a Privileged Access Workstation (PAW) or a dedicated Virtual Machine, rather than from the computer where the employee reads e-mail or surfs the web.

5.12 All company guests are allowed access only to separated Wi-Fi with internet access, no access to company internal resources.

This document has been prepared for general purposes only and does not purport to be and is not a substitute for specific professional advice. While the matters identified are believed to be generally correct, before any specific action is taken, specific advice on the circumstances in question should be obtained.

About SECMAR

Project SECMAR deals with the emerging field of maritime cybersecurity. As the maritime transport sector is undergoing rapid digital transformation, the issues of security are falling behind. The aim of SECMAR is to increase the level of security and build up the competence in the Baltic Sea area in the ongoing digitalisation of the shipping and logistics sector, through connecting maritime stakeholders with the IT-sector and the academic fields of cybersecurity, Big Data and Internet of Things.

If you want to get in contact with us, please drop us a line at:
David.Appelberg@bluesciencepark.se, Project Manager

Developed in co-operation with Truesec

As a global cybersecurity company, we're proud to be at the forefront of protecting organizations and our society against cyber threats. Our purpose has been clear since day one: Creating safety and sustainability in a digital world by preventing cyber breach and minimizing impact.

Our team consists of 180+ cyber specialists, covering the full spectrum of cybersecurity. Through our collaborative approach, we come together as one team to help defend your most valuable data assets every day. Each of us contributing with our expertise, strong sense of purpose and willingness to make a difference. We never cease to challenge and reinvent ourselves to stay ahead of cybercriminals and find the best solution for you.
www.truesec.com

Interreg South Baltic

EUROPEAN UNION

TRUESEC