Handbook on SektorCERTs 25 recommendations

Published: November 2024

TLP:CLEAR

Recommendations

SEKTOR CERT

General

SektorCERT has developed 25 concrete recommendations that we recommend all critical infrastructure organisations to implement in their management network/IT environment and production network/OT environment.

Reading guide

For more information about the structure of the recommendations, the intent of the implementation steps and a glossary, please refer to the reading guide on page 30.

The background behind the '25 recommendations'

The 25 recommendations are concrete suggestions for improving cybersecurity based on an in-depth analysis of known, successful cyberattacks against critical infrastructure companies in Europe and three years of data from SektorCERT's sensors. The recommendations therefore contribute to a good defense against known attack techniques.

The preparation of the 'Handbook on SektorCERT's 25 recommendations' has been done in collaboration with selected members of SektorCERT. The members were selected based on their sector and organization size. The selected members therefore represent most of the sectors SektorCERT covers, as well as small, medium and large companies.

The recommendations describe how you, as actors within Danish critical infrastructure, can best prevent cyber attacks and prepare for a cyber attack.

Delimitation

SektorCERT has cyber security as our primary focus area. In many cases, there may be borderline cases or even overlap between physical security and cyber security (e.g. physical access to network ports or USB ports). SektorCERT does not address physical security measures in this handbook of 25 recommendations.

Good cyber security

It is important to emphasize that the recommendations are not an exhaustive list, but should be seen as a set of minimum recommendations that all actors within critical infrastructure in SektorCERT's view should consider. The recommendations are recommendations from SektorCERT - they are neither requirements nor expectations - and should be seen as an aid to improving cybersecurity.

Cloud

Many companies choose to put parts of their OT in the cloud. The reasons for this can be many, but the ultimate responsibility for security remains with our members. Regardless of how you have chosen to set up your infrastructure, the 25 recommendations are still relevant and management must ensure that each recommendation has been addressed.

Due diligence

The implementation of the recommendations should take place regardless of the current threat level, as it will be too late to start implementing the selected actions once the need arises. The list of recommendations should therefore be seen as an opportunity to check that you either already have all the recommendations implemented - or to refocus on getting the missing recommendations implemented.

Use SektorForum

If you need sparring on good ways to implement the recommendations, you can use the SektorForum, where both we at SektorCERT and your colleagues in other critical infrastructure companies can be found.

RECOMMENDATIONS

1 Firewall

Firewall is implemented and kept up to date - preferably with geo-blocking of countries not needed to receive traffic from.

Why is it important

A firewall provides basic protection against unauthorized access and attacks from the internet. The main role of the firewall is to ensure that only internet traffic relevant to the business is allowed. All other traffic is blocked. Therefore, if your company infrastructure has access to the internet, you need a firewall.

Recommendations – IT

The firewall must be configured and kept up-to-date with the latest software and/or firmware updates. In addition, firewall rules that allow and block certain types of data traffic from the Internet should be updated to match the current threat landscape and company operations (including the use of VPN).

Firewalls can be used to geo-block traffic from countries or regions other than those with which the company (and possibly your suppliers) normally communicate, such as Asia, Africa and South America. It is recommended that geo-blocking is implemented with an allow list rather than a deny list.

If your firewall offers additional functionalities, consider filtering traffic based on content, protecting against denial of service attacks (DDoS), logging data traffic and performing intrusion detection.

Recommendations – OT

Firewalls are used to separate the different layers of the OT infrastructure as well as to separate OT from the rest of the company's IT infrastructure (see Purdue model - see glossary).

Deployment steps

Level 1

- ❑ Install firewalls on all connections to the internet.
- ❑ Verify that the firmware on firewalls is kept up-to-date.
- ❑ Verify that firewall rules are kept up to date.

Level 2

- ❑ Implement geo-blocking on both inbound and outbound connections.
- ❑ Verify that all ports (both inbound and outbound) are closed by default so that only necessary ports are open.
- ❑ Do not expose the web interface for managing the firewall to the Internet.
- ❑ Disable responses to ICMP packets against the firewall.
- ❑ Use static IP on the outside of the firewall.
- ❑ Restart the firewall regularly.

Level 3

- ❑ Enable DDoS protection.
- ❑ Implement firewalls in cloud services.
- ❑ Enable logging of who and when changes were made to rules.
- ❑ Collect logs from all firewalls (if multiple) to a central location.
- ❑ Perform ongoing analysis of collected log data.
- ❑ Document all firewall rules outside the firewall (see recommendation 18).

Level 4

- ❑ Install internal firewalls (at least between IT and OT, but preferably between multiple layers).
- ❑ Perform regular external pentests against the company's external firewall (see recommendation 25).
- ❑ Make regular copies of the latest firewall configurations and rules. The copies should be secured offline (see recommendation 4).

2 Exposure of services

Only absolutely necessary services are exposed to the Internet.

Why is it important

An internet exposed service is e.g. websites, APIs, remote desktop access, web interfaces on devices and camera feeds. Many development departments use both existing services (e.g. APIs) and develop new services for communication and/or data transfer. A service that is open from the internet into the company risks becoming an open door for the hacker. The company reduces the risk of cyberattacks by exposing only the necessary services to the internet.

Recommendations – IT

The company must continuously make sure to review all internet-facing services and clarify which ones need to be exposed to the internet to support business operations.

Recommendations – OT

Make sure there is no direct access to the OT network from the internet-facing services.

Deployment steps

Level 1

- ❑ Create an overview of all services on all devices that are exposed to the internet.
- ❑ Make sure there is no direct access from an internet-exposed service to devices in the OT network.

Level 2

- ❑ Make sure that only services that are necessary for business operations are exposed to the internet.
- ❑ By default, disable all services on new internet-facing devices.

Level 3

- ❑ Ensure that all internet-exposed services are documented, evaluated and approved by a relevant manager.
- ❑ Use 'security by design' when (further) developing services (e.g. new features and/or new products).
- ❑ Block automated scans (such as SHODAN, Nessus, Qualys or similar - possibly performed via TOR exit nodes) on all open services; unless automated scans are actively used in the company.

Level 4

- ❑ Perform regular scans for exposed ports and services (see recommendation 25).
- ❑ Follow up all scans with an evaluation. Assess if the right services are exposed to the internet or if additional blocking is needed.
- ❑ Make sure that the exposed services that are proprietary are tested against a framework such as the OWASP Application Security Verification Standard.

3 Endpoint protection

Endpoint protection and firewall enabled and updated on all systems.

Why is it important

Many attacks start on a computer via phishing emails, visiting a malicious website, inserting an unauthorized USB stick or similar. Endpoint protection minimizes the risk of individual devices in the network being compromised. If one device is compromised, endpoint protection ensures that the attack does not spread to other devices on the network.

Recommendations – IT

All devices must be hardened before connecting to the network. In addition, you can have log collection from the device and monitor network traffic for abnormal traffic. The local firewall on the device must also be activated and maintained.

In addition, you can choose to install EDR (Endpoint Detection & Response) on all IT systems - both clients and servers - and have it centrally controlled. EDR is similar to a traditional antivirus scanner, but with far better protection options.
Remember to log and alert when endpoint protection is disabled as this can be a sign of a ransomware incident.

Recommendations – OT

Be aware that EDR may require an internet connection and may shut down the device on which it is installed. In the OT environment, EDR can therefore be limited to devices that do not directly power the critical infrastructure (e.g. engineering workstations, jump hosts, etc.).

Deployment steps

Level 1

- ❑ Make sure all devices (both IT and OT) have been hardened before deployment.

Level 2

- ❑ Install endpoint protection on all devices in the IT network.
- ❑ Install endpoint protection on relevant devices in the OT network.

Level 3

- ❑ Ensure that relevant logs from each device (both IT and OT) are collected centrally and analyzed at regular intervals.

Level 4

- ❑ Alerts centralized team if local EDR installations and/or local firewalls are disabled.
- ❑ Verify hardening using a pentest.

4 Backup

Backup is present (including off-site backup) and restore is tested regularly.

Why is it important

Backup creates backups of company data and therefore gives the company an opportunity to recover from e.g. ransomware attacks. If an actor succeeds in installing ransomware and encrypting data on company systems, a backup can make it possible to restore systems and data and thus secure the company's operations.

Recommendations – IT

Decide from which devices to backup, how often to backup and how long to store the backup. The backup should go back far enough in time to be loaded without the risk of restoring systems with compromised data. The decision can be made using a criticality matrix or similar prioritized order.

Store a copy of the backup offsite and offline so that it is not affected by a ransomware attack or physical events (e.g. fire).

The backup and restore process should be regularly tested and evaluated. The backup must include all data (including configurations and documentation) needed to restore business-critical systems. The recovery procedure must be practiced so that the company is confident that business-critical systems can be restored within a set timeframe.

Recommendations – OT

It is not always possible to implement automated backup of OT devices (such as PLCs and RTUs), so they must be protected in other ways. This could be by having up-to-date documentation of these OT devices, as well as a copy of the configuration files (and not of the entire device). The SCADA system must also be backed up.

Deployment steps

Level 1

- ❑ Clarify which data and systems are needed from the IT and OT network to restore business-critical services.
- ❑ Backup the most business-critical data and systems.

Level 2

- ❑ Verify that the backup is working as intended.
- ❑ Review all relevant business areas and prioritize critical systems and data within each business area.
- ❑ Store the backup offsite and offline.

Level 3

- ❑ Verify that the backup is encrypted both in transit (from relevant devices to the storage media) and "at rest" (when data is stored on the storage media).

Level 4

- ❑ Introduce the backup restoration procedure into your contingency planning.
- ❑ Test the backup procedure, focusing on:
  - to measure the time spent
  - A clear description of who (employees) can perform the individual steps and how they are performed.
- ❑ Introduce time-based firewall rules that are only active during backup.
- ❑ Ensure that any 'backup service accounts' follow the recommendations regarding limited rights (see recommendation 19) and password length (see recommendation 5).

5 Password length

Passwords are designed according to current standards - i.e. rather very long passwords that are changed rarely than shorter passwords that are changed frequently.

Why is it important

A weak password is often a short password. A common attack technique is brute force attacks, where an attacker attempts to log into a company's systems and/or network by testing a series of usernames and passwords to find a 'weak' combination. Long passwords reduce the risk of the attack succeeding.

Recommendations – IT

Define internal requirements for passwords and make sure these requirements are applied throughout the company. Length is the key parameter for a strong password. Requirements to use numbers and special characters (like $ or @) in the password and to change it frequently are now considered outdated.

A strong password...

- is longer than 15 characters and can contain spaces. Feel free to think of a sentence that you can remember yourself.
- does not contain known words or phrases that can be easily guessed.
- is longer than 20 characters if it is an administrator or service account.
- should only be changed if there is an indication that the password has been compromised.

A bad password...

- consists of known words or phrases such as "summervacation123456" or "passwordpassword".

The above practices should be implemented on all systems where possible, including accounts on all clients and servers as well as external systems with suppliers, e.g. in the cloud (see also recommendation 22).

Recommendations – OT

Some OT devices, especially older ones, only offer limited options for passwords, and therefore it may be necessary to have less strict requirements for e.g. password length. Be careful with the use of special characters, spaces and Danish letters (æ, ø, å) as some OT devices have difficulty handling these.

Deployment steps

Level 1

- ❑ Introduce password length requirements for all accounts on all systems.

Level 2

- ❑ Introduce stricter password requirements for administrator and service accounts than for general accounts.

Level 3

- ❑ Make a password manager available to all employees. Make sure that employees do not use private password managers to manage company passwords.
- ❑ The password manager used in the OT environment must be 'on premise' (i.e. installed in your own environment).
- ❑ Implement Security Group Policy on all AD and standalone systems that addresses password length and complexity requirements.

Level 4

- ❑ Implement password compliance checks for both IT and OT environments.
- ❑ Ensure that all password hashing methodologies used are of a slow type that is difficult to compromise. Opt out of fast and/or insecure methodologies.

6 No password reuse

No password reuse - especially across IT and OT.

Why is it important

Reusing passwords gives a malicious actor better opportunities to move across websites, applications and systems in the company and increases the risk of the actor succeeding in their attack. Once the actor has gained access to one system by guessing or stealing a password, it can potentially be exploited to log into other systems using the same password.

Password reuse can take place internally within a company (the same password gives access to multiple systems), but it can also happen when employees reuse passwords across private access (e.g. Facebook, LinkedIn etc.) and company systems.

Single Sign On (SSO) is an authentication technology where a user only has to log in once and then gains access to several independent systems. SSO is basically a practical and secure technology, but requires that users' logins are handled securely - e.g. in the form of strong passwords that are not reused.

Recommendations – IT

Implement SSO where possible. For systems that do not support SSO, ensure that passwords are not reused on different IT systems or user accounts.

Recommendations – OT

Implementing SSO in OT environments can be a practical challenge. Never reuse passwords from corporate IT systems (including SSO) in OT. This reduces the risk of an attack spreading from IT to OT. Never use the same password to log in to different OT systems.

Deployment steps

Level 1

- ❑ Implement SSO in the IT network where possible.

Level 2

- ❑ Make a password manager available to all employees to mitigate the risk of password reuse. When choosing a password manager, consider whether the solution should be online or offline.
  See also recommendation 5.

Level 3

- ❑ Introduce measures that prevent password reuse across applications and time. Examples include SSO, awareness training and password managers.
- ❑ Implement measures to prevent reuse of passwords for administrator and service accounts across applications and time. Examples include SSO, awareness and password managers.

Level 4

- ❑ Introduce measures that prevent password reuse across IT and OT. Examples include SSO, awareness and password managers.

7 No shared logins and default passwords

No common login and no default passwords.

Why is it important

Shared logins (also called generic logins) is when a user account is used by multiple employees, making the company infrastructure vulnerable to attack. Using shared logins also opens up the possibility for former employees to continue to access the company's systems after their employment has ended.

Please note that shared logins, in this context, are different from SSO, which is a technology where one login can be used to log into many other systems.

Default passwords set by the manufacturer (e.g. username and password Admin/Admin) pose a significant security risk, as the password can often be found in manuals available online.

Standard passwords set by the company using the device pose a significant security risk as they are often easy to crack, for example by using a brute force or dictionary attack and as the password may be known by several employees.

Recommendations – IT

All employees should have their own accounts with their own logins. There should be no shared accounts used by multiple employees - even if these accounts have minimal rights. Passwords should be personal and not shared with others.

Default passwords set by either the manufacturer or the company should be disabled.

Recommendations – OT

As a company, you should strive to avoid common logins and default passwords in OT. However, be aware that parts of the OT environment may have special priorities and requirements, such as accessibility and shift change/monitoring, which may make it more difficult to implement.

Deployment steps

Level 1

- ❑ Verify that there are no shared accounts on the IT and OT network.
- ❑ Disable default passwords when implementing new equipment and systems.

Level 2

- ❑ Verify that system and firmware updates do not reactivate default passwords.
- ❑ Introduce SSO where possible.
- ❑ Make it easy to create new temporary accounts for external employees and interns.

Level 3

- ❑ Introduce restriction where possible and applicable so that any account can only log in to one place at any time.
- ❑ Introduce GPO on all service accounts that prevents the use of default passwords.

Level 4

- ❑ Perform regular checks that account settings meet internal requirements.
- ❑ Evaluate login logs for irregularities.
- ❑ Introduce, as far as possible, that all IT accounts are domain accounts and not local accounts.
- ❑ Perform regular pentests to identify default passwords (see recommendation 25).

8 Remove inactive users

User accounts that are not used are removed or disabled.

Why is it important

An inactive user account is a potential attack vector for a malicious actor. This can include accounts of former employees of the company that have not been removed or deactivated after termination of employment.

Recommendations – IT

Regularly (and always at the end of employment) check that there are only active user accounts for current employees of the company and any relevant subcontractors and contract workers. User accounts that are no longer in use should be deleted or deactivated immediately.

Recommendations – OT

In general, the same recommendations apply for OT as for IT.

Deployment steps

Level 1

- ❑ Have an overview of current (internal and external) employees and user accounts.

Level 2

- ❑ Regularly review all user accounts and verify if they are still valid. The review involves both HR and IT operations and can be either manual or automated.

Level 3

- ❑ Regularly review internal systems for employees who are no longer employed in the same role (including internal rotations, other work areas, promotions, terminations, etc.) In this context, also pay attention to external systems and access.
- ❑ Decide at management level whether accounts for employees on leave or maternity leave should be deactivated or kept open. The decision can differentiate between external and internal employees.

Level 4

- ❑ Introduce scripts where possible and relevant that deactivate all unused accounts after e.g. 3 or 6 months.

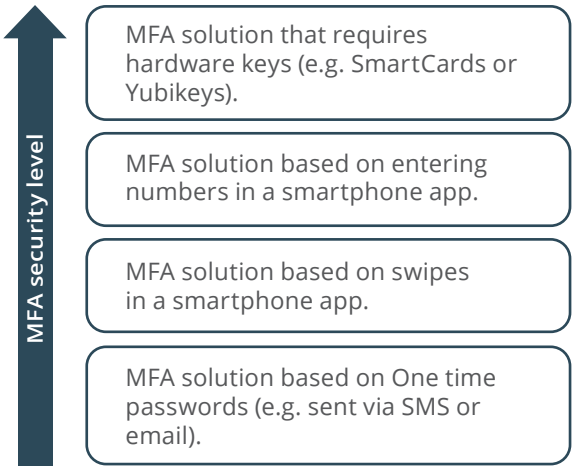
9 Multifactor validation

All services with login exposed to the Internet are secured with multifactor validation and remote access is limited as much as possible.

Why is it important

Multi-factor validation (MFA) adds an extra layer of security when logging into company systems via the internet. Multi-factor validation uses the principle of "something you know, something you have and something you are". In addition to a password, authentication via an authenticator app is also required. This makes it more difficult for a malicious actor to break into the company's systems, as it is no longer enough to guess or steal a password.

Be aware that there are different technical categories of multi-factor validations, each with their own advantages and disadvantages. The specific choice of a multi-factor solution in your organization may depend on a specific risk assessment.



Recommendations – IT

Use multi-factor validation on all web-facing and internal services where possible.

Recommendations – OT

In some cases, OT environments consist of legacy systems from a time when security was not a focus. Therefore, securing OT systems with multi-factor validation can be more challenging, but should be done where possible and where it makes sense.
Be aware that some MFA solutions require internet access, which is not recommended in OT environments.

Deployment steps

Level 1

- ❑ Enable MFA for all remote systems (access via the internet).

Level 2

- ❑ Clarify which internal systems (both IT and OT) can and should have MFA enabled.
- ❑ Enable MFA for all administrator accounts.
- ❑ Introduce MFA app that complies with the company's IT security policy.

Level 3

- ❑ Enable MFA for all users in relevant systems in IT.
- ❑ Enable MFA for all users in relevant systems in OT.
- ❑ Introduce elevated MFA security implementation (see graph on the left) on relevant systems.

Level 4

- ❑ Use contextual MFA controls that also take into account the user's physical location, device ID and/or behavioral patterns.
- ❑ Make use of offline MFA devices (e.g. smart cards and Yubi-keys) rather than online (smartphone app) whenever possible.

10 Update

The systems are kept up to date / patched - including third-party software.

Why is it important

Software vendors and security researchers regularly discover security holes in programs, which are then closed by the vendor issuing updates/patches. If companies don't keep their software portfolio up to date, the software is left with vulnerabilities that can potentially be exploited by malicious actors to gain access to the company's infrastructure.

Recommendations – IT

Make sure to keep IT devices up to date, updates can be verified before installation to avoid unintended consequences.

Pay attention to different categories of updates. Security updates for critical vulnerabilities should be verified and installed faster than feature updates, for example.

Enable automatic updates on all systems where possible and where new updates do not risk causing operational disruptions.

Recommendations – OT

OT devices may have different risk, testing and functional requirements (including certifications) than IT devices. Updates to OT devices must therefore be handled separately to ensure continuous availability and stability of operations, among other things.

Deployment steps

Level 1

- ❑ Enable autoupdate on all systems where possible and where new updates do not risk causing operational disruptions.
- ❑ Verify that information about new updates is received from suppliers.

Level 2

- ❑ Be ready to patch devices quickly in both IT and OT networks for critical vulnerabilities.
- ❑ Verify that updates do not lead to operational disruptions.
- ❑ Keep internet-exposed devices and devices that can receive emails updated.

Level 3

- ❑ Keep all IT devices up-to-date with verified updates.

Level 4

- ❑ Keep all OT devices updated with operational stability in mind.

11 Identify outdated systems

Vulnerable systems that cannot be patched (end-of-life e.g.) are identified and appropriate countermeasures are implemented to protect them.

Why is it important

Hardware (including firmware) and software (e.g. applications and operating systems) are eventually replaced by new versions. After a period of time, support for the older version of the software is discontinued, which usually means that the vendor no longer provides updates and patches security holes. This is called end-of-life (EOL) and failure to identify these types of systems increases the risk of attacks on vulnerable devices in the infrastructure.

Recommendations – IT

Maintain an up-to-date overview of the company's IT systems (see recommendation 17) and identify the systems that are facing EOL. Develop a plan for what to do with the specific systems (including selecting a vendor and suitable replacement for the device). This should be done in a timely manner as it can be a time-consuming process.
If a system that is still necessary for business operations cannot be replaced, a decision must be made on alternative security measures (e.g. segmentation and/or implementation of firewalls).

Recommendations – OT

In general, the same recommendations apply for OT as for IT. However, be aware that there are often many EOL devices in OT environments that need to be secured with segmentation and/or firewalls.

Deployment steps

Level 1

- ❑ Maintain an EOL list for all systems (both software and hardware).

Level 2

- ❑ Identify the processes that will be affected when a product and/or system is either at or approaching EOL.
- ❑ Appoint an 'OT asset manager' (see recommendation 17).
- ❑ Appoint an 'IT asset manager' (see recommendation 17).

Level 3

- ❑ Make a plan, in collaboration with process owners and management, for how to handle EOL systems.

Level 4

- ❑ Perform regular reviews of lists of devices approaching EOL.
- ❑ Plan ahead for EOL management so that new systems can be EOLed in time (or alternatively, that EOL systems are supplemented with security measures).

12 Contingency plan

A contingency plan is drawn up and maintained.

Why is it important

A contingency plan sets out in writing what the company should do in the event of a cyberattack. The contingency plan should reflect the company's strategy to ensure primary operations (security of supply) in a crisis situation.

Recommendations – IT

For building a good contingency plan, we refer to CFCS' *Cyberforsvar der virker* from 2023[1]. SektorCERT also refers to applicable legislation within critical infrastructure.

Test the contingency plan regularly and keep it regularly updated (including contact details of relevant employees). Make sure to inform and train new employees so that they know the contingency plan.

Recommendations – OT

The contingency plan should focus on keeping the OT environment completely cut off from the consequences of a cyberattack so that operations can continue with minimal disruption.

Deployment steps

Level 1

- ❑ Define the company's overall strategy during a cyber incident. The strategy must take into account security of supply.
- ❑ Designate an OT incident response manager.
- ❑ Designate an IT incident response manager.

Level 2

- ❑ Based on the strategy, create a contingency plan that covers incidents in the IT environment. The plan must account for a critical incident at all times of the day and night.
- ❑ Create a contingency plan based on the strategy that covers incidents in the OT environment. The plan must account for a critical incident at all times of the day and night.
- ❑ Enter into an agreement with a third party for assistance in the event of a cyber incident.

Level 3

- ❑ Keep the IT contingency plan up to date.
- ❑ Keep the OT contingency plan up to date.
- ❑ Regularly test parts of both the IT and OT contingency plan (e.g. limited to functions or departments). Use evaluations from the exercises to improve the contingency plans.

Level 4

- ❑ Build the specified incidents (both IT and OT) based on recognized scenarios (e.g. ROS).
- ❑ Regularly test the entire IT and OT contingency plan (across functions and departments). Use evaluations from the exercises to improve the contingency plans.

[1] The publication (in Danish) can be downloaded for free from the CFCS website: https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-cyberforsvar-der-virker-2023-.pdf

13 Log collection

Monitoring/logging implemented so attacks can be detected and responded to in a timely manner - e.g. via SektorCERT sensors, honeypots on the OT network, and extended, internal monitoring.

Why is it important

Network monitoring and log collection are essential to detect and respond to cyberattacks in time. Without this in place, organizations risk missing obvious indicators of malicious activity in the IT or OT environment.

Be aware that there are different types of logs (audit logs, client event logs, security logs for administrative login attempts and actions, network logs, industrial device logs, etc.) It must therefore be defined which logs are relevant to collect, manage and store.

Recommendations – IT

Enable log collection on all relevant devices in the network, such as firewalls, servers and gateways. SektorCERT offers installation of network sensors that monitor traffic to and from the company and can help log and detect threats to the infrastructure so that countermeasures can be taken in time.

You can also consider installing extended monitoring from SektorCERT, which includes logging and monitoring processes in selected IT devices.

Recommendations – OT

Honeypots can be installed on the OT network (see glossary). While a malicious actor attempts to compromise a honeypot, attention is diverted from the company's real OT network. A honeypot can also reveal knowledge of an actor's attack techniques.

You may also consider installing extended monitoring from SektorCERT, which includes monitoring of processes in selected OT devices.

Deployment steps

Level 1

- ❑ Enable logging on all internet-facing services or ensure that network traffic is logged.
- ❑ Decide which logs to collect - including different types of logs from different segments - for example
  - Criticality level
  - IT and OT
  - Audits
  - Login attempts.

Level 2

- ❑ Introduce logging on all key internal IT systems - e.g. via SektorCERT Extended Monitoring.
- ❑ Ensure that all logs have a common time source and time zone.
- ❑ Define
  - how logs should be used
  - how long logs should be stored
  - how logs are deleted.

Level 3

- ❑ Introduce logging on selected OT systems (e.g. jump hosts) - e.g. via SektorCERT's Extended Monitoring.
- ❑ Ensure that all logs are collected and stored centrally.
- ❑ Restrict access to logs.
- ❑ Manage relevant logs (e.g. critical alarms) 24/7 via a SIEM or SOC system.

Level 4

- ❑ Make sure log collection follows current best practices (e.g.
  - NSA et al. *Best Practices for event logging and threat detection*
  - CFCS' *Logning – en del af et godt cyberforsvar*
  - CIS Control No. 6.
- ❑ Introduce log backup (see recommendation 4) or make sure logs are replicated on multiple systems.
- ❑ Introduce logging on relevant PLCs, RTUs, etc.

14 Awareness

Awareness training of employees is conducted on an ongoing basis to ensure focus on OT and IT security.

Why is it important

Everyday attention to IT and OT security is essential to reduce the risk of cyberattacks. If employees don't demonstrate continuous security awareness, the company risks creating gaps in the bulwark that protects the company's IT and OT environment.

Awareness campaigns can take the form of regular information campaigns, posters, phishing tests, etc.

Recommendations – IT

Keep an ongoing focus on maintaining awareness among employees.

Awareness can include the use of strong passwords, awareness of phishing emails or potential dangers of using public WiFi.

Awareness campaigns should be based on the current threat level the company is experiencing. Change focus areas regularly to ensure coverage of multiple topics.

Recommendations – OT

In general, the same recommendations apply for OT as for IT. However, you should consider adapting the awareness training to the current environment in OT.

Deployment steps

Level 1

- ❑ Educate all employees about the risk of cyber incidents and review basic precautions.
- ❑ Organize cybersecurity awareness campaigns.

Level 2

- ❑ Introduce differentiated awareness campaigns that are customized to specific groups of employees and partners. The individual campaigns are aligned with the current threat picture against the relevant group.
- ❑ Ensure that all employees regularly go through training and refresh the company's IT security policy.
- ❑ Conduct tests after completing training.

Level 3

- ❑ Conduct unannounced exercises (e.g. phishing campaigns) and document the results.
- ❑ Take into account special needs of employees (e.g. dyslexia) using e.g. videos.
- ❑ Build awareness campaigns with a positive attitude and praise for employees (not 'management by fear').

Level 4

- ❑ Introduce awareness campaigns as gamification.
- ❑ Set goals for awareness training and document progress.

15 Map network entries

All network entries to the production network are mapped.

Why is it important

Mapping all network entries to the IT and OT environment provides an overview of which ports need to be monitored and possibly closed to network traffic. This allows the organization to ensure that only business-critical network ports are open and monitored, reducing the risk of attacks.

The mapping will also provide a basis for implementing the right firewalls (see recommendation 1) and segmentation (see recommendation 16).

In addition, it is easier to go live when all network accesses are mapped. This can reduce the risk of an attack spreading from IT to OT (see recommendation 24).

Recommendations – IT

Create an overview of network accesses from the IT infrastructure towards OT (the production network). Make sure to keep this overview updated when changes occur on the network.

Recommendations – OT

Map all network accesses in and out of the production network (to IT as well as to other segments and to the internet). Remember to consider alternative connections (WiFi, 4G modems, serial connections, bluetooth, satellite connections, etc.).

Deployment steps

Level 1

- ❑ Map all network accesses to the production network with direct connection to the internet.

Level 2

- ❑ Map all network accesses to the production network from other segments (IT, DMZ, etc.).

Level 3

- ❑ Identify and close network accesses to the production network that are not necessary for business operations.
- ❑ Consider whether some network accesses should only be used sporadically (e.g. for support). Close them when they are not in use.
- ❑ Make sure that network accesses are described in the contingency plan (see recommendation 12) to streamline operations.

Level 4

- ❑ Map alternative network accesses such as WiFi, 4G modems, satellite connections etc. and decide if these are necessary.
- ❑ Regularly review connection lists.

16 Segmentation

The network is segmented into several layers - at least so that OT is separated from IT. Consider further isolation or segmentation to contain or limit the potential of an incident.

Why is it important

Dividing a network into smaller segments prevents users from accessing parts of the network that are not relevant to their work. Segmentation can also slow down a malicious actor or virus/malware from spreading from one part of the network to another. This is especially important to prevent attacks on the IT infrastructure from spreading to the OT environment.

A physical segmentation of networks includes separate network cables, switches, etc. Logical segmentation is the division of the network into separate VLANs, typically handled in switches. Physical segmentation is generally more secure than logical segmentation, but will have a higher financial cost.

Recommendations – IT

Review the IT infrastructure and identify subsets of the network, which can be divided into business-related sub-networks that are segmented from each other. A subnetwork could be guest WiFi, info screens, printers, HR department, etc.

Make sure that the Internet-exposed services are in a separate segment (e.g. a DMZ).
The individual segments should only communicate with each other via authorized connections - e.g. via a firewall.

Recommendations – OT

Make sure to segment IT and OT with a firewall so that there is only controlled network access between the two segments. Consider further segmenting the OT network by using the Purdue model as a reference architecture.

Deployment steps

Level 1

- ❑ Make sure the IT environment is segmented from the OT environment.
- ❑ Create separate segment for guest networks.

Level 2

- ❑ Make sure that internet-facing services are in a separate segment.
- ❑ Introduce firewalls between segments and define how (if at all) to communicate between each segment.
- ❑ Implement a strategy that defines the purpose of each segmentation, including whether it should be physically or logically segmented.
- ❑ Strive for each segmentation to be built according to the 'least privilege' principle.

Level 3

- ❑ Use the Purdue model (or a similar model) as a reference architecture in the current OT infrastructure.
- ❑ Use the Purdue model (or a similar model) as a reference architecture for future expansions/upgrades of the OT environment.

Level 4

- ❑ Conduct regular audits and/or tests to ensure segmentation is working as expected.

17 Identify devices

All units in the production environment are identified and documented.

Why is it important

New vulnerabilities in software and firmware for computers and network equipment are regularly discovered and exploited by malicious actors. Identifying and documenting all devices in the production environment makes it easier for companies to get an overview of which devices are vulnerable and need patching. It also provides an overview of devices that are, or are approaching, end-of-life, so the company can better prepare for their replacement (see recommendation 11).

Keep in mind that devices include physical devices (e.g. computers, PLCs and RTUs), software, virtual machines and network components (firewalls, switches, etc.).

Recommendations – IT

Build and maintain an inventory of devices (both hardware and software) including PCs, servers, operating systems, applications, network equipment, etc. in the IT infrastructure that support operations in the production network.

Recommendations – OT

Build and maintain an inventory of devices (both hardware and software) including PCs, servers, operating systems, applications, network equipment, etc. in the OT network.

Deployment steps

Level 1

- ❑ Create an inventory of the most critical physical devices in the production environment.

Level 2

- ❑ Identify the associated devices needed to keep the most critical devices in the production environment running.
- ❑ Identify the devices in IT that are necessary for the critical processes in the production network to function.
- ❑ Appoint an OT asset manager who is responsible for maintaining the list.
- ❑ Appoint an IT asset manager who is responsible for maintaining the list.

Level 3

- ❑ Build a system for automated passive scanning in relevant segments of the production environment to detect new and unknown devices.

Level 4

- ❑ Introduce an asset management system.
- ❑ Conduct regular technical tests to identify devices in the production network - for example, to identify devices that are not actively communicating on the network.

18 Documentation

Both logical and physical documentation of the architecture is produced.

Why is it important

Documentation of the architecture provides an overview and understanding of how devices in the IT and OT environment are connected and communicate with each other. Maintained documentation makes it easier to develop measures that increase security and limit the consequences in the event of a cyberattack.

Recommendations – IT

It can be a great internal help if the documentation follows a standard. This can be an international standard (e.g. NIST, ISO or others) or your own standards (e.g. naming of devices).

The architecture should be documented at a level that includes all physical network devices in the architecture. Documentation can include hardware specifications, software and firmware versions. The logical documentation of the architecture should include communication between devices on the network.

Prioritize the creation and maintenance of critical documentation to be included in a contingency plan (see recommendation 12) and used during a disaster recovery.

Recommendations – OT

In general, the same recommendations apply for OT as for IT.

Deployment steps

Level 1

- ❑ Create the most critical documentation to be used in an emergency situation.
- ❑ Update the critical documentation on a regular basis.

Level 2

- ❑ Document the logical structure of relevant parts of both the IT and OT network infrastructure.

Level 3

- ❑ Document the physical architecture - including network devices - of relevant parts of both the IT and OT environment (see recommendation 17) and the physical network entries (see recommendation 15).
- ❑ Ensure that critical documentation is available in a crisis situation (e.g. when IT is unavailable).

Level 4

- ❑ Conduct regular audits of documentation to ensure timeliness and accuracy.

19 Limit rights

Limiting rights on user accounts - special focus on limiting administrative rights for users when not necessary.

Why is it important

The fewer rights a user has on a system, the fewer opportunities a malicious actor has to abuse a compromised user account to move further into the company's IT or OT infrastructure.
Restricting privileges also reduces the risk of human error, which can lead to cybersecurity breaches.

Recommendations – IT

Limit users' rights to what is needed (principle of least privilege) by the employee to perform their job duties. This includes both what systems they can use and what resources (e.g. network drives) they have access to.

Only grant admin rights to those who need them - including relevant IT administrators. Also, limit administrator rights so that the principle of least privilege is applied here too.

If an employee is given new work areas, their access to the IT network should be reassessed. The purpose is to ensure that the employee has the correct rights adapted to their work tasks and that they do not, over time, accumulate rights to systems.

Recommendations – OT

In general, the same recommendations apply to OT as to IT. It must be ensured that the employees who are responsible for the operation of the critical infrastructure have the opportunity to make the changes that are necessary in a crisis situation - for example via "break the glass" accounts.

Deployment steps

Level 1

- ❑ Make sure users are not local administrators on their PC in both IT and OT.
- ❑ Only create admin accounts for selected employees with a work-related need.

Level 2

- ❑ Create user accounts according to the principle of least privilege.
- ❑ Categorize employees into roles (such as management, administration, IT and operations) for which necessary tasks are defined. Create accounts according to these roles.
- ❑ Introduce different degrees of IT administrator accounts, such as local administrator, domain administrator and system administrator.
- ❑ Introduce separate accounts for the IT and OT environment.
- ❑ Ensure that service accounts do not have administrator rights but are created according to the principle of least privilege.

Level 3

- ❑ Introduce restrictions in the OT environment so that users in the OT environment cannot edit systems used for the operation of the critical infrastructure without a work-related need.
- ❑ Perform regular checks on all roles and accounts, ensuring that roles only have sufficient rights to perform their tasks. In addition, ensure that all accounts are still relevant (see recommendation 8) and that all accounts are associated with a relevant role.

Level 4

- ❑ Monitor all activities performed by administrator accounts.
- ❑ Set time limits on the use of administrator accounts.

20 Access policy

Policy on access to the production network is established.

Why is it important

An access policy describes access to company OT environments by ensuring that only the right people have access to the relevant systems at the necessary times. The policy should include logical access. A lack of an access policy risks giving employees and external suppliers access to parts of the production network that they should not have access to. This access could potentially be exploited by a malicious actor who has compromised an employee or supplier's user account.

Recommendations – IT

A production network does not generally include IT. However, there may be cases where the production network receives data from IT systems and services (including weather data and tariffs), which must therefore also be covered by the production network's access policy.

Recommendations – OT

Create and enforce a policy for access to the company's OT production network. This includes logical access to systems through user logins as well as any remote access to the production network.

Especially in larger companies, it can be beneficial to define roles and privileges based on company workspaces as a way to manage all employees and ensure a higher level of security. The access policy should assign access rights based on the person's role in the organization and always limit access to only the absolutely necessary resources in the production network.

Deployment steps

Level 1

- ❑ Define user roles and responsibilities based on the principle of least privilege.

Level 2

- ❑ Introduce RBAC (Role Based Access Control) for all accounts in OT. Rights should be assigned to roles and not to individuals.

Level 3

- ❑ Make sure the policy covers all user accesses and verify that these are in the right category and that the categories cover assigned tasks.
- ❑ The access policy must take into account i.e. VPN access into the OT environment.

Level 4

- ❑ Ensure that the Access Control Configuration is password protected, at least at administrator level (see recommendation 5).
- ❑ Ensure that only OT devices have access to the production network AD.

21 Policy for changes

Policy for changes to the digital part of the production network is established.

Why is it important

A policy for changes in the digital part of the production network describes changes so that it is specified who can make changes and when they can be made. This minimizes the risk of errors and ensures roll-back procedures in case of unforeseen errors.

Recommendations – IT

A production network does not generally include IT. However, there may be cases where the production network receives data from IT systems and services (including weather data and tariffs), which must therefore also be covered by the production network's access policy.

Recommendations – OT

Create and implement roles and processes for who in the organization is allowed to make which changes to the OT infrastructure.

Changes can include, but are not limited to:

- Updates/upgrades
- Patches
- Network topology
- Rolling out new applications
- System/user access

Consider following established change management standards (e.g. ITIL).

Deployment steps

Level 1

- ❑ Document all configuration changes in the OT environment.

Level 2

- ❑ Inform relevant staff and partners about changes in the production network.

Level 3

- ❑ Use a template for all types of changes in the OT environment.
- ❑ Implement a policy for changes in OT.
- ❑ Introduce a change management process.

Level 4

- ❑ Establish a Change Advisory Board (CAB) to help prioritize changes.
- ❑ Introduce systemic support for change management processes.

22 Vendor management

Vendor management policy, including how to verify that vendors meet your security requirements, is established.

Why is it important

Vendor management increases the likelihood that the company's IT and OT vendor(s) meet the company's cybersecurity requirements.

Recommendations – IT

The company must appoint an employee responsible for setting security requirements for suppliers and ensuring that the IT supplier complies with these requirements.
The security requirements for suppliers must reflect the company's own requirements and policies, including update requirements (see recommendation 10), access policy (see recommendation 20) and exposure of services (see recommendation 2).

The requirements for the supplier must be based on a specific assessment of, for example, the supplier's IT solutions and the supplier's procedures for handling a cyber incident. The assessment must also reflect whether the supplier's IT systems handle the company's business-critical processes and/or sensitive personal data.
Documentation of the supplier's solutions and associated responsibilities can be handled by auditors' statements.

As a company, you need to consider the chain responsibility of your suppliers (i.e. the supplier's suppliers). Consider to what extent documentation should be required for this chain responsibility.

The Center for Cybersecurity has published a guide on cybersecurity in supplier relationships, which provides an introduction to supplier management.

Recommendations – OT

In general, the same recommendations apply for OT as for IT, but be aware that a lack of security requirements for OT vendors can have a greater impact on operational stability.

Deployment steps

Level 1

- ❑ Designate an employee (possibly per vendor) responsible for security-related vendor management.
- ❑ Document and maintain a list of suppliers for IT and OT environments.
  The list should divide vendors into relevant categories, such as:
  - Influence on operations
  - Continuous access to your own systems.

Level 2

- ❑ Set requirements for relevant suppliers (both current and future). The requirements should be:
  - Specific
  - Measurable
  - Indicative
  - Relevant
  - Time-bound.
- ❑ Make a concrete assessment of all suppliers' influence and responsibility for relevant parts of your business processes and infrastructure.

Level 3

- ❑ Create a separate assessment for critical suppliers - including supplier influence and responsibility.

Level 4

- ❑ Make sure you only contract with suppliers that can meet the criteria.
- ❑ Ensure a clear division of roles and responsibilities with the supplier - both in normal operations and during a cyber incident.
- ❑ Establish a process for dialog with the supplier.
- ❑ Conduct checks with the supplier.

23 Alternative communication channels

Alternative communication methods, e.g. satellite phone or SINE radio to complement email and telephone, are established.

Why is it important

Cyberattacks against critical infrastructure can potentially affect internet and telephony. With alternative communication channels available, your business can maintain the ability to communicate with employees, partners, authorities and customers in a crisis situation.

Recommendations – IT

Introduce alternatives to internet or mobile networks, such as satellite phone, satellite internet or SINE radio.

Periodically test that the alternative means of communication are working as intended. Make sure to clearly communicate to relevant business partners that the company can be contacted via these communication channels in emergency situations.

Recommendations – OT

In general, the same recommendations apply for OT as for IT.

Deployment steps

Level 1

- ❑ Clarify the need (i.e. set up different scenarios) for alternative communication channels - e.g. in cases where internet and cell phones are no longer available.

Level 2

- ❑ Introduce alternative communication channels so that necessary operations can be maintained.
- ❑ Describe concrete procedures for different scenarios (e.g. SMS broadcasts to all employees).

Level 3

- ❑ Test and evaluate the alternative communication channels regularly.

Level 4

- ❑ Regularly reassess the need for and implementation of alternative communication channels to ensure business continuity.

24 Emergency procedures

Emergency procedures for all business-critical processes are drawn up so that the function can be performed in case of prolonged IT outages, including a plan for operation in island mode.

Why is it important

Emergency procedures can be crucial in reducing the damage caused by a cyberattack. In the event of prolonged disruption to IT operations as a result of an attack, contingency procedures for business-critical processes can help your business keep essential operations running while the attack is dealt with.

Recommendations – IT

Develop relevant emergency procedures for your business critical processes and continuously test that they are working as intended.

Emergency procedures can include:

- Paying salary without IT. This can be handled, for example, by paying the last month's salary manually and then adjusting later.
- Communicating to customers about outages in case the internet is unavailable. This can be handled by always having enough paper and toner in stock for manual distribution of information to households.
- Emergency power from generators or UPS systems. This can be handled by installing your own system or by entering into an agreement with a supplier who can install a generator system within a specified timeframe.

The emergency procedures must include a plan for island operation. This plan can describe how business-critical IT systems are isolated from other IT systems and how the company headquarters are isolated from subsidiaries/ remote locations.

Recommendations – OT

The emergency procedure must describe how the OT environment can be isolated from the company's IT network, including how operations are secured.
In addition, a plan must be made to isolate and keep the OT environment running in the event that the company's OT provider is unavailable.

Deployment steps

Level 1

- ❑ Identify your company's core services in a crisis situation.

Level 2

- ❑ Set up different crisis situations.

Level 3

- ❑ Describe the procedures needed to maintain the core service in the crisis situations outlined.

Level 4

- ❑ Regularly test the described procedures for each of the listed crisis situations.
- ❑ Hold a drill at least once a year for changing scenarios. The exercises are documented and evaluated.

25 Vulnerability scans

Ongoing vulnerability scans and possible penetration tests are conducted to provide an overview of the attack surface towards the internet.

Why is it important

Scans and penetration tests of the company's internet-facing and internal systems can help reveal vulnerabilities in the scanned part of the IT & OT infrastructure.
A vulnerability scan can help to identify publicly known security holes in your system and determine available patches. A penetration test can clarify a potential way into the infrastructure.

Recommendations – IT

Vulnerability scans of the company's internal services as well as the company's internet-facing services should be performed on an ongoing basis. For example, scans can reveal whether exposed services are configured in an insecure manner or whether related protocols and software contain vulnerabilities that can be patched.
In addition, a vulnerability scan can help confirm that only authorized services have access to the internet.

Prior to a vulnerability scan and/or a penetration test, the purpose must be clarified. The activity can have different focus areas, such as:

- Vulnerability scanning of internet-facing systems.
- Vulnerability scanning of internal IT systems.
- Penetration tests from the internet into the company infrastructure.

Recommendations – OT

Be aware that OT devices can be more vulnerable to active scans and penetration tests than IT devices. Therefore, scans and penetration tests in OT environments should always be done with operational stability in mind.
The focus area for a vulnerability scan of internal OT systems can therefore be, for example, a passive scan.

Deployment steps

Level 1

- ❑ Uncover the need for a vulnerability scan.

Level 2

- ❑ Describe in as much detail as possible the purpose and scope of a vulnerability scan - for example, whether the purpose is only to get a list of exposed vulnerabilities or whether these must also be exploited (penetration testing).

Level 3

- ❑ Perform a vulnerability scan or penetration test and list the vulnerabilities found by criticality.
- ❑ Implement necessary actions that were identified during the vulnerability scan or penetration test.
- ❑ Appoint a 'patch manager'.

Level 4

- ❑ Perform regular vulnerability scans or penetration tests, with varying areas of focus.

READING GUIDE

Structure of the recommendations

All recommendations follow the same structure.

Why it is important
A brief description of why it is important to consider this recommendation in relation to the company's other security measures.

Recommendations - IT
For some recommendations, the same recommendations apply to IT as to OT. For other recommendations, there are special conditions that apply to OT rather than IT.
In this section we will describe the recommendation according to the administration network.

Recommendations - OT
In general, the same recommendations apply to OT as to IT. For some recommendations, there may be special conditions that apply to OT rather than IT, which will be described in this section, which relates to the production network.

Implementation levels
Concrete measures, listed with the basic measures in level 1 and increasing security requirements towards level 4.

13 Log collection

Monitoring/logging implemented so attacks can be detected and responded to in a timely manner - e.g. via SektorCERT sensors, honeypots on the OT network, and extended, internal monitoring.

Importance

Network monitoring and log collection are essential to detect and respond to cyberattacks in time. Without this in place, organizations risk missing obvious indicators of malicious activity in the IT or OT environment.

Be aware that there are different types of logs (audit logs, client event logs, security logs for administrative login attempts and actions, network logs, industrial device logs, etc.) It must therefore be defined which logs are relevant to collect, manage and store.

Recommendations – IT

Enable log collection on all relevant devices in the network, such as firewalls, servers and gateways. SektorCERT offers installation of network sensors that monitor traffic to and from the company and can help log and detect threats to the infrastructure so that countermeasures can be taken in time.

You can also consider installing extended monitoring from SektorCERT, which includes logging and monitoring processes in selected IT devices.

Recommendations – OT

Honeypots can be installed on the OT network (see glossary). While a malicious actor attempts to compromise a honeypot, attention is diverted from the company's real OT network. A honeypot can also reveal knowledge of an actor's attack techniques.

You may also consider installing extended monitoring from SektorCERT, which includes monitoring of processes in selected OT devices.

Deployment steps

Level 1

- ❑ Introduce logging on all internet-facing services or ensure that network traffic is logged.
- ❑ Decide which logs to collect - including different types of logs from different segments - for example
  - Criticality level
  - IT and OT
  - Audits
  - Login attempts.

Level 2

- ❑ Introduce logging on all key internal IT systems - e.g. via SektorCERT Extended Monitoring.
- ❑ Ensure that all logs have a common time source and time zone.
- ❑ Define
  - how logs should be used
  - how long logs should be stored
  - how logs are deleted.

Level 3

- ❑ Introduce logging on selected OT systems (e.g. jump hosts) - e.g. via SektorCERT's Extended Monitoring.
- ❑ Ensure that all logs are collected and stored centrally.
- ❑ Restrict access to logs.
- ❑ Manage relevant logs (e.g. critical alarms) 24/7 via a SIEM or SOC system.

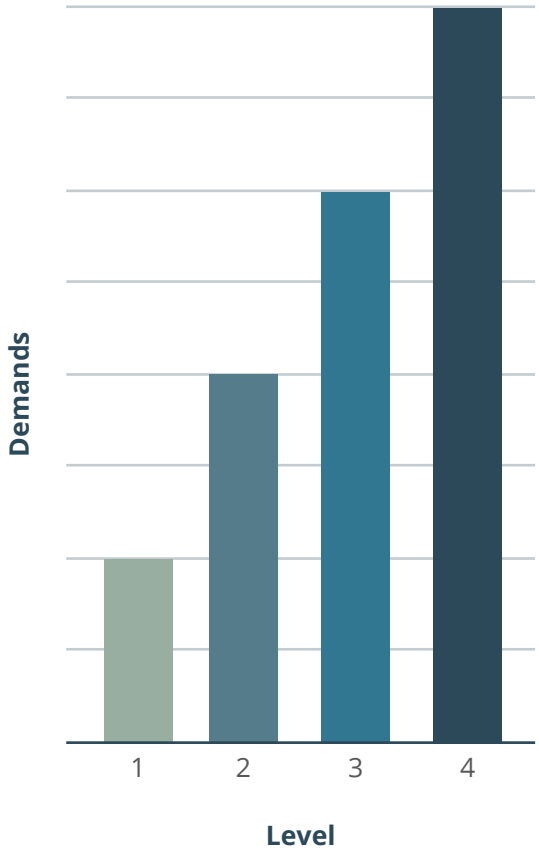
Level 4

- ❑ Make sure log collection follows current best practices (e.g.
  - NSA et al. *Best Practices for event logging and threat detection*
  - CFCS' *Logning – en del af et godt cyberforsvar*
  - CIS Control No. 6.
- ❑ Introduce log backup (see recommendation 4) or make sure logs are replicated on multiple systems.
- ❑ Introduce logging on relevant PLCs, RTUs, etc.

Deployment steps

For each recommendation, we have listed a number of concrete actions and divided them into levels. Level 1 is the basic level where we expect many of our members to be able to fulfill all the actions.

It becomes progressively more difficult to fulfill all the actions in levels 2, 3 and 4. To be at a given level, you need to fulfill all the listed actions as well as all the actions in the underlying levels.



Deployment steps

Level 1

- ❑ Basic measures to protect against basic cyberattacks.

Level 2

- ❑ Simple measures that protect against deliberate, yet uncomplicated, cyber attacks.

Level 3

- ❑ Measures that protect against intentional and more complex cyberattacks.

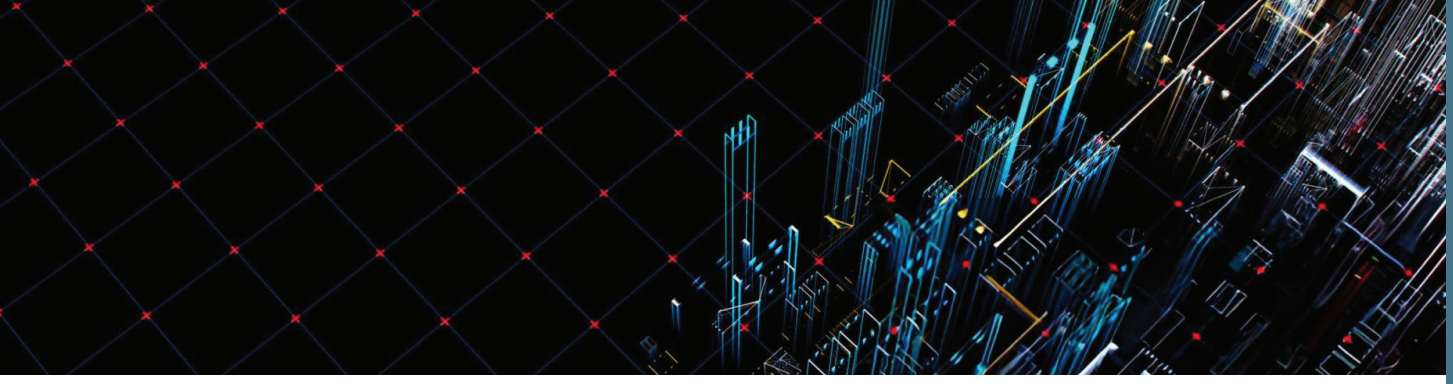
Level 4

- ❑ Advanced measures that protect against sophisticated attacks.

The purpose of the implementation levels is for you, as members, to actively decide to what extent you want to implement the specific recommendation - and to provide an opportunity to measure how far you are with the implementation.

It is important to emphasize that not all members need to be at level 4 in all 25 recommendations. The need can be weighed in relation to e.g. finances, available resources, consequences of a hacker attack, weighted risk analysis and more.

SektorCERT recommends our members to make an assessment of each recommendation, which, together with knowledge of the company's organization and infrastructure and risk tolerance, helps to define the specific implementation (including relevant implementation steps).



Glossary

The list below is an explanation of some of the professional and/or technical terms that appear in the 25 recommendations.

There is not necessarily agreement among professionals on the definition of all the words in the glossary. In these cases, the purpose of the list is to clarify the definition or meaning that SektorCERT is working with.

The list is not exhaustive and only reflects the technical terms mentioned in relation to the above recommendations. The explanations below do not necessarily elaborate on the particular word in the list.

Purdue-model

Purdue Enterprise Reference Architecture (PERA) - more popularly known as the "Purdue model" - is a reference model for segmenting (separating) a company's industrial control systems (ICS) from its other business software and from the internet.

Honeypot

A honeypot is a hardware device that can be programmed to look like a server or OT hardware from manufacturers such as ABB, Siemens, Microsoft or Schneider Electric. A honeypot is used to detect attack attempts against the company's infrastructure and build knowledge about the attacker's techniques and tactics.

Hardening

Hardening is both a strategy and a procedure for minimizing the potential attack surface of a device. Hardening can include:

- Removal of unnecessary software
- verifying that only relevant services are enabled
- installing security patches
- disabling USB ports or other physical access
- restricting rights
- encrypting hard disks and databases
- disabling unnecessary network ports

Single-Sign-On (SSO)

Single sign-on (SSO) is an authentication technology that allows a user to log in with only a single ID and then access multiple related, yet independent, software systems.

Notes

SektorCERT is a non-profit association, owned and funded by Danish critical infrastructure companies. SektorCERT collaborates with Europe's other CERTs and is part of a number of security organisations, which gives us extensive knowledge about attacks against critical infrastructure

digital trust

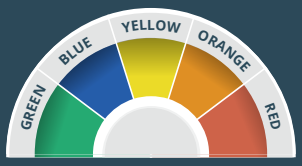
This report should give you answers to the following questions:

- Why is it important for SektorCERT members to implement the 25 recommendations?
- What specific cybersecurity measures does SektorCERT recommend to members?
- What are the differences between cybersecurity in IT and OT environments?
- How do SektorCERT members decide the order in which they prioritize the implementation of specific cybersecurity measures?

Threat levels

SektorCERT uses a 5-point scale to indicate the threat level.

The scale is based on an international standard developed by the Centre for Internet Security (CIS).



Our environmental focus

CO2 neutral
CLIMATECALC
CC-000091/DK

NORDIC SWAN ECOLABEL
Printed matter
5041 0200

FSC
www.fsc.org
MIX
Papir | Støtter ansvarligt skovbrug
FSC® C109833

SektorCERT has more than 300 sensors in Danish critical infrastructure.

SektorCERT is the cyber security centre for critical sectors. We help detect and respond when critical infrastructure is exposed to cyber attacks.

This document is TLP:CLEAR

TLP:**CLEAR**
The information can be shared unlimited.

Read more about Traffic Light Protocol at FIRST: www.first.org/tlp/

Target audience

All SektorCERT members with strategical and operational responsibility for cyber security in Danish critical infrastructure.

- [x] **Strategic**
- [x] **Operational**
- [ ] **Tactical**

The 'Handbook on SektorCERTs 25 recommendations' was developed in collaboration with selected members of SektorCERT. The members were selected based on their sector and organization size. The selected members therefore represent most of the sectors SektorCERT covers, as well as small, medium and large companies.

SEKTOR CERT

Phone number:

+45 88 32 71 40

E-mail:

info@sektorcert.dk

PGP key:

C2EF 6314 7860 2B1E 2341 ACF4 DBC3 511D 3D06 BB3A

Visiting and mailing addresses:

Sommerfuglevej 2A
6000 Kolding

Bredgade 45
1260 København K

CVR number:

41369841

Satellite phone number:

+88 16 22 45 60 29

SINE radio

73 12 056

SVANEMÆRKET
Tryksag
5041 0200

FSC
www.fsc.org
MIX
Papir | Støtter ansvarligt skovbrug
FSC® C109833

CO2 neutral
CLIMATECALC
CC-000091/DK