# CERT-WM

## Computer Emergency Response Team WaterManagement

## Collaboration on operational information security

[TLP:WHITE]

CERT-WM

# CERT-WM

- What is it?
- Where is it located??
- How it works?
- What does it do?

# What is CERT-WM?

- Partnership between HWH en Rijkswaterstaat(RWS)
- What is HWH?
- What is Rijkswaterstaat?

# Wat is HWH?

HetWaterschapshuis

- The Waterboardhouse.
- The Waterboardhouse is the directing and implementing organization for the 21 water boards in the field of ICT.
- The Waterboardhouse works on the basis of programs. The CERT-WM is partof the HWH program IV & P (for now).

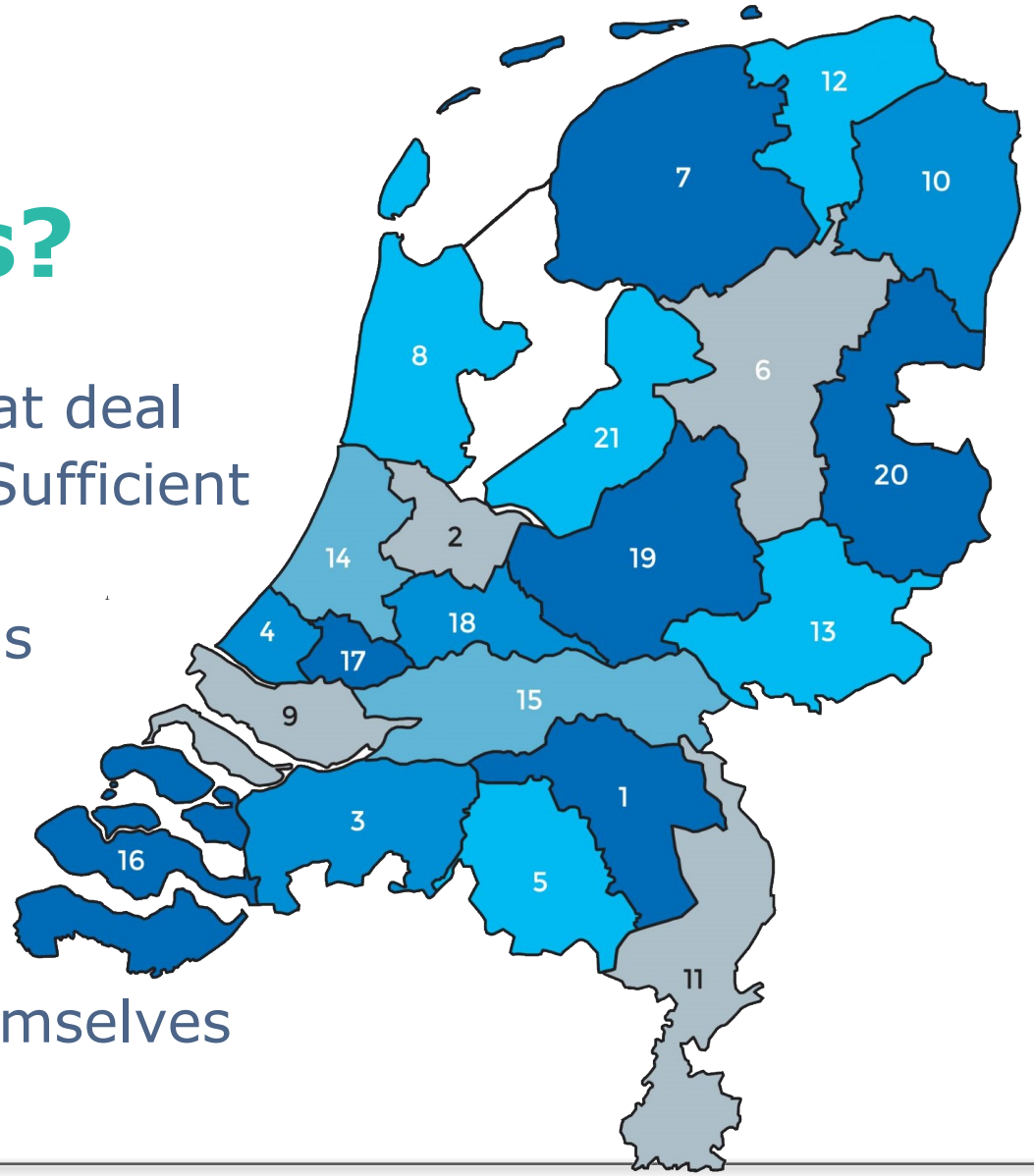
# What are waterboards?

The waterboards are local authorities that deal with water quality and water quantity. (Sufficient and clean water, dry feet*)

- Dikes, weirs, sluices, pumping stations
- Waste water treatment plants
- Road management

**What doesn't?  Drinking water!**

This is provided by water companies themselves



# What is Rijkswaterstaat?

Rijkswaterstaat is the executive agency of the Ministry of Infrastructure and Water Management.

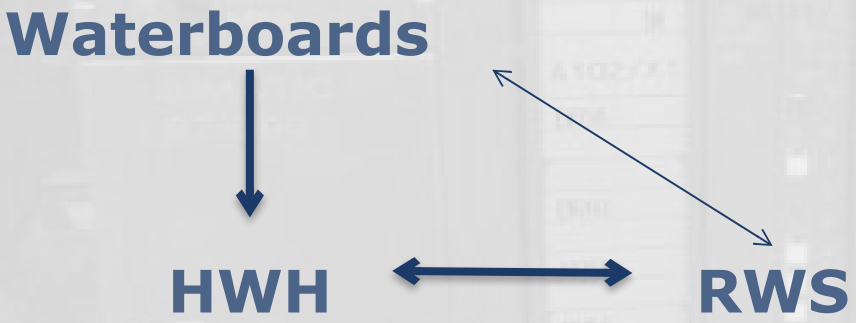
Manages and develops the main roads, main waterways and main water systems on behalf of the Ministry.

Rijkswaterstaat
*Ministerie van Infrastructuur en Waterstaat*

[TLP:WHITE]

CERT-WM

# CERT-WM




A lot of similarity in terms of discipline (water cycle), therefore a great chance of synergy, especially in the intended Operational Technology part.

# Where is it located?

In the Security Operations Centre (SOC) of Rijkswaterstaat
(The SOC is part of the Security Center and is located in Delft)

- Leverages existing connections and tools from RWS's SOC
- Knowledge sharing between SOC employees and CERT-WM employees
- Sparring/consulting SOC colleagues in the event of incidents

# The CERT-WM team

Two coordinators:

- 1 Tactical \ Strategic coordinator as contact person between the water boards, the CERT-WM (kind of account manager), coordination RWS, Ministries, Water Sector, etc. Promotion CERT WM within Waterboards and External Affairs

- 1 Operational coordinator CERT-WM and contact person between RWS

- Line-up CERT-WM:
  Employees from various waterboards are detached to HWH and fulfil a role in CERT-WM, which effectively results in more than 1 FTE staff. 6 employees are active in the CERT-WM.

# Services CERT-WM

## Advisories

Sending advisories is one of the core activities of the CERT-WM. When sending advisories, information regarding vulnerabilities or threats is shared with the participants, whereby the participant is not only specifically informed about a threat, it also receives advice on how to act.

The targeted information of the participants is done because the advisories are written for specific products and only participants with these products actually receive the information (based on submitted CMDB of the organization)

# Services CERT-WM

## Handling RD (Responsible Disclosure) reports

The CERT-WM acts as a contact person for a participant towards the reporter of a vulnerability and the participant.
In this way, the participant is relieved of communication with the reporter and the CERT-WM provides the participant with a detailed analysis of the report, including a recommended solution.

# Services CERT-WM

## Incident advising

- The CERT-WM supports cyber incidents that occur among participants.
- The CERT-WM takes an advisory role in this.
- Advising on the steps to be taken helps the participant to resolve the incident as quickly as possible.

# Services CERT-WM

## Vulnerability scanning (Pilot phase)

- Vulnerability scanning is a service that automatically scans websites and web services for anomalies.
  Reportable deviations pose a risk to the security of the website or web service.
- In the event of such deviations, the CERT-WM provides the participant with a detailed analysis of the deviation, including a recommended solution.

# Services CERT-WM

## Pentesten (Pilot fase)

- In order to ensure the information security of a specific part of the infrastructure, we can offer a pentest from the CERT-WM on that part.

# Diensten CERT-WM

## Forensics

- In the event of a (cyber) incident, it is important to find out what happened. In some cases, this means finding out what has been done on a specific system or who has performed these actions.
- Forensic examination of such a system can help answer these questions, to prevent recurrence in the future.

# Diensten CERT-WM

## Information and knowledge sharing

- The purpose of this service is to provide the constituency with information and sound advice. Think of advice on a technical level, in the field of procedures, best practices, etc.

- The CERT-WM uses various channels for this, such as White Papers, the CERT-WM Blog and LinkedIn.

  https://www.cert-wm.nl/ or follow us uphttps://www.linkedin.com/company/cert-wm/

# CERT-WM participate in:

- National Coverage System (LDS), to enable mutual exchange of information within the framework of the law. It makes it possible to pass on information received from the NCSC to the participants of CERT-WM.

- Impact of NIS2 and associated mandatory sectoral tasks(N-CSIRT & S-CSIRT)
  - Attain maturity level – SIM3
  - Specialization PA / OT / ICS / SCADA - Expansion of tasks (mandatory and opportunities)

# CERT-WM participate in:

- CERT-WM participated in the set-up of TIBER-Water Guide
  TIBER stands for Threat-Intelligence based Ethical Red Teaming (TIBER). When performing a TIBER test, advanced cyberattacks are carried out by specialized companies based on the most up-to-date threat information. The purpose of this test is the learning experience of the participating organisations. Participating organisations in the sector exchange lessons learned from the tests in order to increase the combined cyber resilience.

  Conducting TIBER Water tests, or the lighter method, contributes to the requirement in the NIS 2 to “assess the effectiveness of cybersecurity risk management measures”

  Link to TIBER-Water Guide

# CERT-WM participate in:

Threat scenario for the sector Keren en Beheren

- A collaboration between the NCSC, RWS, CERT-WM and the participants to create 11 threat scenarios based on the risk management methodology MASKeR of the NCSC. The scenarios help the participants to prioritize measures to be taken.

Impact of NIS2

- associated mandatory sectoral tasks(N-CSIRT & S-CSIRT)
- Attain maturity level – SIM3
- Specialization PA / OT / ICS / SCADA - Expansion of tasks (mandatory and opportunities)

# CERT-WM participate in:

Threat scenario for the sector Keren en Beheren(Flood risk management)

- A collaboration between the NCSC, RWS, CERT-WM and the participants to create 11 threat scenarios based on the risk management methodology MASKeR of the NCSC

Impact of NIS2

- Associated mandatory sectoral tasks(N-CSIRT & S-CSIRT)
- Attain maturity level – SIM3
- Specialization PA / OT / ICS / SCADA - Expansion of tasks (mandatory and opportunities)

# CERT-WM participate in:

## CSIR: CyberSecurity Implementation Guideline

A collaboration between RWS and the Waterboards, to take the appropriate measures based on risks.

The CSIR stands for Cyber Security Implementation Guideline and has been specially developed to cybersecure objects (water treatment plants, pumping stations, bridges, barriers, locks, etc.).

It is based on the BIO (Government Information Security Baseline), IEC62443 and best practices.
https://www.cert-wm.nl/csir

# [EOF]