Interreg
ADRION
ADRIATIC-IONIAN
EUROPEAN UNION
European Regional Development Fund - Instrument for Pre-Accession II Fund

TRANSCPEARLYWARNING

TransCPEarlyWarning Civil Protection Early Warning Platform

IT SUPPORT MANUAL

"TRANSCPEARLYWARNING": Establishment of "TRANSnational Civil Protection EARLY WARNING System" to improve the resilience of Adrion territories to naturaland man-made risks.

JUNE 2022

Disclaimer

This document has been produced with the financial assistance of the European Union. The content of the document is the sole responsibility of ADRION TransCPEarlyWarning partnership under the coordination of partner Industrial Systems Institute for the compilation of the specific document and can under no circumstances be regarded as reflecting the position of the European Union and/or ADRION programme authorities.

TRANSCPEARLYWARNING: Establishment of "TRANSnational Civil Protection EARLY WARNING System" to improve the resilience of Adrion territories to natural and man-made risks (ADRION 979)

Programme Priority 2. Sustainable Region

Specific Objective: Enhance the capacity in transnationally tackling environmental vulnerability, fragmentation, and the safeguarding of ecosystem services in the Adriatic-Ionian area
WP T2 – Civil Protection & Early Warning Platform linked to the EU Civil Protection Mechanisms
Activity T2.1 – Development of Civil Protection Early Warning Platform
Deliverable T2.1.2 – Civil Protection Early Warning Platform with semantics interface

Responsible Author: PP3 - Athanasios Kalogeras, Christos Anagnostopoulos, Agorakis Bombotas, Georgios Mylonas, Christos Alexakos, Kyriakos Stefanidis, Georgios Kalogeras, Georgios Raptis, Stella Markantonatou, Miranda Dandoulaki, Georgios Lefteriotis

Editors: External expert Dynamic Vision - Ioannis Mardikis, Natalia Tsami

Project Coordinator: ***LP – Regione Molise***

INTERREG ADRION Programme

2014-2020

Contents

❖ Executive Summary

This manual elaborates on the checks need to be performed to ensure proper and secure use of the TransCPEarlyWarning Civil Protection Early Warning Platform (**TransCPEW platform**).

❖ Introduction

The **TransCPEW platform** aims to unify and automate the various Civil Protection (CP) processes regarding the prevention of natural and man-made disasters. **It serves the purpose of offering a focal point of reference for the Civil Protection stakeholders in ADRION territories** enabling the integration of different information sources and systems and will make it possible for CP stakeholders to perform the relevant experimentation through pilot implementations.

For the proper and secure use of the platform, a number of checks need to be performed at regular intervals. Depending on their complexity and the risk, those checks can be performed daily, weekly, or even once per year.

Usually, the system administrator is the authorized personnel to perform the regular checks. For some of the more complex ones, an external security engineer can be contracted for the duration of those.

The current document, "IT SUPPORT MANUAL", addresses any authorized personnel for performing the regular checks.

1. Maintenance and Security

1.1. Infrequent Maintenance (1/year)

1.1.1. Penetration testing

Penetration testing is the simulated cyberattack against the platform to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment the web application firewall (WAF).

Penetration testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

The PenTest should be performed by an external expert under contract. Prior to the actual PenTest, the scope and goals of the test need to be defined, including the systems to be addressed and the testing methods to be used. The PenTester needs to be able to gather intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

1.1.2. Security policies audit

A security audit needs to be performed yearly, along with the penetration testing. The basic goals of the audit are:

- Identify security problems and gaps, as well as system weaknesses.
- Establish a security baseline that future audits can be compared with.
- Comply with external regulatory requirements.
- Determine if security training is adequate.
- Identify unnecessary resources.

The audit is preferably done by an external contracted entity and should cover the following

- Network vulnerabilities
- Security controls
- Access control policies
- Information processing

1.2. Regular Maintenance (1/month or week)

1.2.1. Software updates

All the software that is part of the platform, including the third-party libraries should be regularly updated. The following packages should be checked and updated accordingly

- Infrastructure

- Operating System
- Miscellaneous services such as SSH, email server, etc.
- Web server and application server

- Application
  - Database
  - Application components such as the Camuda modeler
  - Libraries that have been used for the application development

The application-level updates should be performed by a software developer and tested before going into production. The infrastructure updates should be performed by the systems administrator.

1.2.2. Password safety audits

Ensuring that the used passwords, especially the ones that are used by administration accounts, are not vulnerable to brute force or dictionary attacks is paramount to the overall security of the platform.

At regular intervals, the system administrator, should perform an audit on the strength of the password database. This should be done by passing the password database through a password cracker like HashCat and JohnTheRipper, using the most common dictionaries that exist at the time of the audit.

Also, the system administrator should monitor the emails of the existing accounts and check if they appear in a recent breach (as presented in "';--have i been pwned?"1). Since users frequently reuse their passwords in multiple platforms, the existence of those emails in a breach is an indication of potential threat for the platform.

1.2.3. Access control audits

The system administrator should perform regular audits on the access control policies of the platform. More specifically, they should make sure that the principle of least privileges is closely followed by the rest of the platform administrators. Unnecessary or suspicious privilege grands should be crosschecked with the relevant users and superfluous privileges should be revoked.

1.2.4. Backup and backup validation

The platform backups belong to two different categories. The full system backup and the incremental backup.

The full system backup should be performed each month and should include the full virtual machine including the file system. The database should also be backed up using its own mechanism. The database dump should be automatically copied in the same folder as the rest of the system backup files.

Twice per year, a validation of the most recent backup should be performed. The goal of this validation is to make sure that the backups are usable and there is no corruption in the backup or storage mechanisms. The full system should be deployed on the test server suing only the provided backup files and a simple check that everything is operational should be performed by the system administrator.

1 https://haveibeenpwned.com/

The incremental backup should be performed only on the platform data which includes the part of the file system that is used for application data and the database. The incremental backup does not include application or infrastructure system files.

Incremental backups are performed daily and the whole process should be fully automatic. The database dump should be performed using the database application mechanisms and not any external tools. The database dump is then stored along the file system backup in timestamped folders. The number of incremental backups equals twice the number of days between full system backups.

1.3. Daily checks (1/day)

1.3.1. Logs and Alerts

The system administrator should perform a daily check on the logs and alerts that are produced by the platform's security mechanisms. The first check should be whether the mechanisms are operational and produce logs. Then, the following three types of logs, and their respective alerts, should be checked and, if necessary, act upon:

- Anti-malware logs and alerts
- Network traffic and NIDS logs and alerts
- Firewall logs and alerts

Any critical alert or suspicious activity should be documented, and the relevant incident response action should be followed.

1.3.2. Backup

See chapter "Backup and backup validation" on daily incremental backups.