

Local targeted event at the port of Ploče

Deliverable no. D.2.5.1
28th June 2023

Event summary

<i>Type of event</i>	<i>Physical</i>
<i>Location (if physical)</i>	<i>Ploče, Port of Ploče Authority, Port of Ploče Entrance terminal</i>
<i>Date of the event</i>	<i>28th of June 2023.</i>
<i>Time/Duration</i>	<i>11:00 – 12:30, 12:30 – 14:00</i>
<i>Purpose of the event (By whom was it organized? What was the objective?)</i>	<i>Port of Ploče Authority has organized a local targeted event as an educational lecture on information/cyber security with the aim of protecting information assets of the Ploče Port Authority Event was organized in front of the pilot action activity to Port of Ploče authority, Port of Ploče and Port Security. Also, the pilot activities result within the SUSPORT project focused on the project objectives has been presented.</i>
<i>Short description of the event (what happened during the event?)</i>	<i>During the Local event Port of Ploče authority has shared its experiences, challenges, priorities of the project activities in within the SUSPORT project. Pilot activities and results have been presented as educational lectures on information/cyber security with the aim of protecting information assets of the Ploče Port Authority. Event was organized as part of the pilot activity Development of conceptual design for Digital Green Incident Management – Incident Management with the aim of reducing incidents that have an impact on the environment and people in port areas.</i>
<i>Results/Outcomes of the event (What are the takeaways from the event?)</i>	<i>Information security and security in ports intertwined are areas that must be holistically addressed in order to protect port facilities, prevent interruptions, protect sensitive data and ensure the efficient and safe flow of goods and services through the global chain Supply. Within the EU project SUSPORT "Incident management with the aim of reducing incidents that have an impact on the environment and people in port areas", the Port of Ploče Authority aiming to achieve a higher level of information security and security with an emphasis on managing incidents that have an impact on the environment and people in port areas.</i>
<i>Number of attendees</i>	<i>18</i>

<i>Type of stakeholders/target groups that were represented</i>	<i>Terminal operators, local and public authorities, port Security</i>
---	--

Photos of the event:



Figure 1 Local Event Ploče

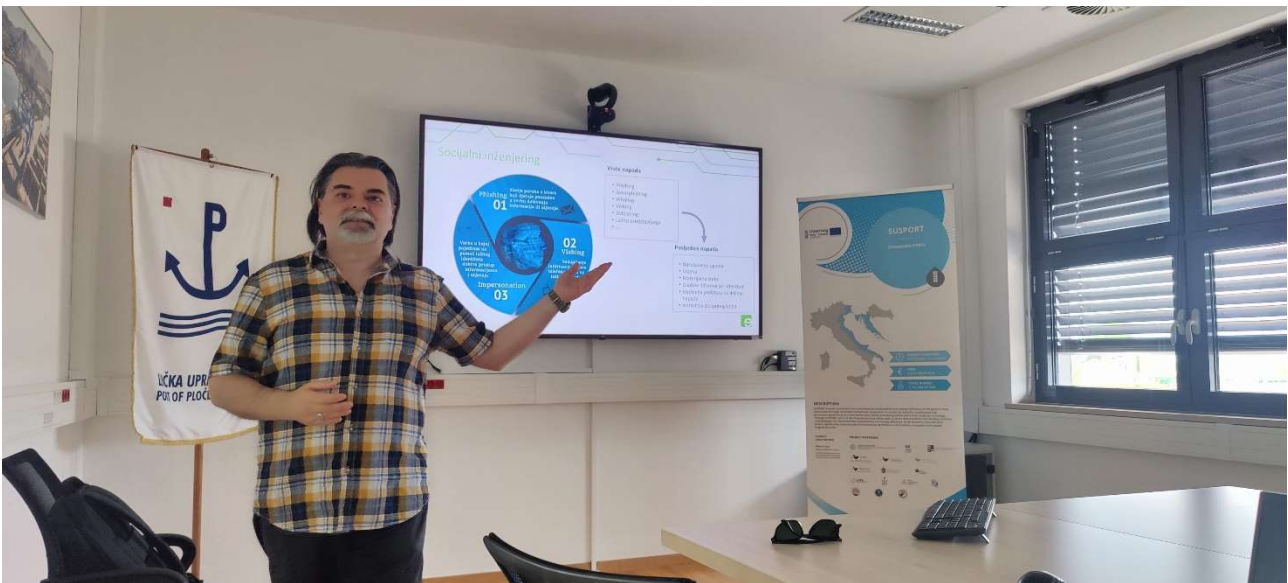


Figure 2 Local Event Ploče



Figure 3 Local Event Ploče

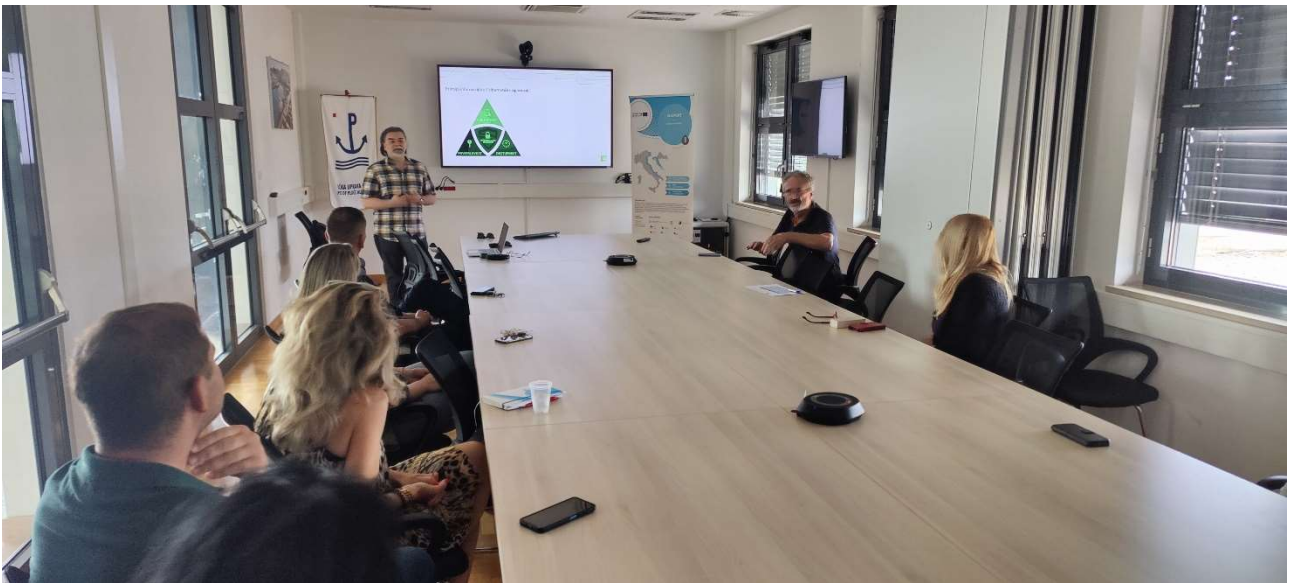


Figure 4 Local Event Ploče

Agenda:

Edukativno predavanje o informacijskoj/kibernetičkoj sigurnosti s cilje zaštite informacijske imovine Lučke uprave Ploče

Darko Plečaš <darko.plecas@ppa.hr>

Fri 6/23/2023 12:15 PM

To: Lučka uprava Ploče, obavijesti <ppa.obavijesti@ppa.hr>

Poštovani,

ovim putem Vas pozivamo na edukativno predavanje o informacijskoj/kibernetičkoj sigurnosti na kojem ćemo vas informirati o aktualnim kibernetičkim prijetnjama, te mogućnostima vašeg osobnog doprinosa zaštititi informacijske imovine Lučke uprave Ploče. S obzirom kako je riječ o mogućnostima Vašeg osobnog doprinosa zaštititi imovine Lučke uprave Ploče, molim da se na edukativno predavanje odazovete i istom prisustvujete.

Edukativno predavanje održat će se u dva slijedeća termina (T1, T2), srijeda 28.06.2023.

- T1: 11:00 sati - 12:30 sati
- T2: 12:30 sati - 14:00 sati

Informacijska sigurnost i zaštita i sigurnost (eng. safety & security) u lukama usko su međusobno povezane i oboje imaju ključnu ulogu u osiguravanju zaštite i nesmetanog rada lučkih objekata. Neke od ključnih točaka su upravljanje incidentima, zaštita kritične infrastrukture, integracija fizičke sigurnosti, kibernetička sigurnost operativnih tehnologija, zaštita osjetljivih podataka, te sigurnost lanca opskrbe.

srdačan pozdrav



Srdačan pozdrav / Best regards

Lučka uprava Ploče, u suradnji s ostalim lučkim sudionicima, razvija PCS kao centralni sustav za najefikasniju razmjenu elektroničkih dokumenata i ostalih podataka između svih lučkih korisnika i njihovih IT sustava, čime se olakšava njihovo poslovanje i ostvaruje dodatna poslovna vrijednost.



Darko Plečaš, dipl.Inf.

Odjel za digitalizaciju / Department for digitalization

Voditelj odjela za digitalizaciju / Head of Department for digitalization

Lučka uprava Ploče
Port of Ploče Authority

Trg kralja Tomislava 21,
20340 Ploče - HR

T: +385 20 414 535,
F: +385 20 670 271

E: darko.plecas@ppa.hr

W: www.ppa.hr

PCS W: <https://vccariloca.ppa.hr>

PCS E: pcs@ppa.hr



Be responsible. Think about the environment before printing this e-mail or its attachments.

Sadržaj ove poruke i eventualno priloženih datoteka je povjerljiv i namijenjen je samo osobama iz subjekta koji su navedeni u adresi. Ukoliko ste primili ovu poruku greškom, molimo Vas obavijestiti pošiljatelja, a poruku i sve njene priloge odmah, bez čitanja, trajno ukloniti s računala. Bilo kakvo prenošenje, kopiranje ili distribucija informacija sadržanih u poruci trećim osobama je zabranjeno i može biti zakonski kažnjivo. Sadržaj, stavovi i mišljenja izneseni u poruci su autorovi i ne predstavljaju nužno stavove Lučke uprave Ploče, Lučka uprava Ploče ne privlači nikakvu odgovornost za eventualnu štetu nastalu primikom ove poruke i priloga sadržanih u poruci.

DISCLAIMER: The contents of this email as well as any files attached to it are confidential and intended solely for individuals or entities which they are addressed to. If you have received this email message in error, please notify the sender and permanently remove the message and all attached files from the computer. Any disclosure, copying or distribution of all or a part of information contained herein to or by third parties is prohibited and may be unlawful. Please note that any views or opinions presented in this message are solely those of the author and do not necessarily represent the views and opinions of Port of Ploče Authority. Port of Ploče Authority accepts no liability for any potential damage caused by this message and files attached to it.

Presentation number 1: Information on cyber Security

Pilot activities in port of Ploče within the project SUSPORT

LOCAL EVENT "SUSPORT" PROJECT

Educational lecture on information/cyber security with the aim of protecting information assets of the Ploče Port Authority

Development of conceptual design for Digital Green Incident Management – Incident Management with the aim of reducing incidents that have an impact on the environment and people in port areas as part of the WPA project SUSPORT

Local event| Ploče| June 28th 2023
Port of Ploče Authority

Informacijska i kibernetička sigurnost



Što

• Informacijska vs. kibernetička sigurnost?

Zašto

• Zašto informacijska i kibernetička sigurnost?

Kako

• Kako možete doprinijeti sigurnosti?

ŠTO?



Definicija informacijske sigurnosti




Stanje povjerljivosti, cjelovitosti i raspoloživosti informacija, koje se postiže primjenom propisanih mjera i standarda te organizacijskom podrškom za poslove planiranja, provedbe, provjere i dorade mjera te standarda



Principi informacijske / kibernetičke sigurnosti



Gdje se te informacije nalaze?



Informacijska sigurnost



ZAŠTO?



Trendovi



Policija upozorava građane na novu internet prevaru: Ne nasjedajte na crnu email poruku
Smatra se da je to jedna od najopasnijih i najbržih metoda za pljačkanje javnih sredstava.



U 2 godine više od pola hrvatskih organizacija bile su žrtve prijevare i kriminala
Istraživači su otkrili da je u posljednja dva godišnja razdoblja broj organizacija koje su postale žrtve prijevare i kriminala porastao za 50 posto, što je odraz na globalnu razinu tih pojava.



Hrvatska među top 5 država zaraženih opasnim računalskim virusom
Ransomware – zloćudni program koji šifrira važne podatke u zločinu za njihovo vraćanje protivniku, jedna od najopasnijih aktivnosti u koje su...



Stotine milijuna dolara 45000 cyber pretnji saopćeno Hrvatsku

Trendovi

INFOGRAFIKA Oprez, hakeri su se usudili napasti i šibensku banku, a kamoli neće vašu aplikaciju

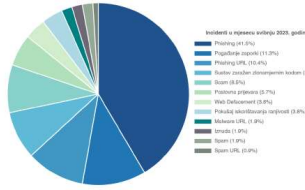
Ransomware napad na hrvatsku naftnu kompaniju INA

Hakeri napali kutinsku Petrokemiju, otežana elektronička komunikacija

LAŽNI E-MAIL Dakovo ostalo bez 50.000 eura: Uplatili novac prevarantima

Internetom kruži opasna aplikacija: više od milijun ljudi skinulo je lažni WhatsApp

Statistika po vrsti incidenta



izvor: www.cert.hr

Socijalni inženjering



Vrste napada

- Phishing
- Spearphishing
- Whishing
- Vishing
- SMSishing
- Lažno predstavljanje

Posljedice napada

- Narušavanje ugleda
- Utegna
- Materijalna šteta
- Osobne informacije i identitet
- Upotreba podataka za daljnje napade
- Instalacija zloćudnog koda

Kako se odvija phishing napad?



Elektronička pošta koja u sebi sadrži zlonamjerni privitak ili poveznicu.



U poruci je sadržaj koji šifrira navodi na pokretanje poveznice ili privitka.



Žrtva napravo pokreće rad određenog malicioznog programa.

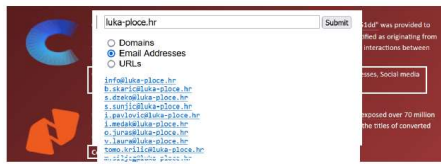


Maliciozni program kriptira sadržaj računala, a na ekranu se javlja poruka kojom se za povrat zaključanih podataka traži uplata određene svote novca.

KAKO SE ZAŠTITI?



Kako napadači dolaze do vaših kontakata?



Kako prepoznati phishing napad?

01

Lažno predstavljanje

Napadači vole imitirati institucije, sudionike u usluzi...
 Pojez pozivajući može biti lažna!
 Provjeri adresu u kojoj je poruka poslana i rasporedi je u kontekst informacija dostupnih na službenim stranicama.

04

Izzivaju ti tebi snažne osjećaje i teraju te na brzu reakciju

Izazivaju snažnih emocija (npr. strah) davanjem kratkog vremena za reakciju, napadači smanjuju sposobnost krug kritičkog razmišljanja i tako te teraju na greške.

02

Nudi ti se novac ili neka druga primamljiva ponuda

Otvoreni i ponudama koje izgledaju prodorno da bi bila istinite. Provjeri ih drugim sredstvima i potraži komentare korisnika.

05

Traže uplatu novca ili kriptovaluta

Ne uplati novac i kriptovalute osobama koje su te kontaktirale putem e-pošte, poziva ili poruka.

03

Moraš kliknuti poveznicu ili skenirati QR kôd

Napadač će te pokušati navesti na zlovoljenu web stranicu na kojoj će te tražiti unos osobnih podataka (npr. osobne ili poslovne kartice). Iako stranica može izgledati legitimno, ona je vjerojatno napravana s ciljem krađe osobnih podataka.

Primjer phishing napada

Prijatelj: IT podrška edcnet.cro@corpora.com

Naslov: Održavanje mail sustava

Redovno održavanje e-mail sustava.

Ova poruka generirana je automatski od strane IT podrške. Trebamo **unaprijedno** obavijestiti te e-mail sustava, s obzirom na **trajanje**!

Ukoliko e-mail sustava potrebno je napraviti redovno održavanje, koristeći se našim kôdima, te se obavezno ova poruka treba biti poslana.

Svi korisnici koji posjeduju korporativne e-mail račune moraju ažurirati svoj račun na najnoviju verziju uljudici upute navedene u ovdješnjem tekstu.

Potvrditi održavanje: [emailSentTime: 'F'] i [lo] /America/Chicago/ +1 hour

Potvrditi održavanje: [emailSentTime: 'F'] i [lo] /America/Chicago/ +2 hours

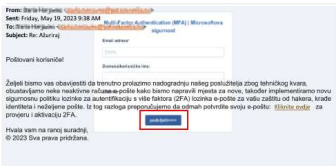
Obračunavanje: Redovno sigurnosno održavanje servera

Stignite svoj kôd kako bi unaprijediti svoj račun.

Ako ne uspijete uputiti: **Ukoliko** kôdovi račun neće biti aktivirani!

Thwa,
IT support
Software version: v.0.20.09

Primjer stvarnog phishing napada



Prepoznavanje phishing napada nije dovoljno!

- Vaš korisnički račun je samo vaša i vi ste odgovorni za njega.
- Lozinke moraju biti kompleksne i redovno se mijenjati.
- Poslovnu e-mail adresu i lozinke dovoljno je koristiti samo za poslovne potrebe.
- Primjenjujemo metode čitav stotak i čitav ekran.
- Označavamo ponovljenu dokumentaciju.
- Korištenje neprovjerenog i nelicenciranog softvera je zabranjeno.
- Prijavljujemo incidente.

Legislativni okvir

- 1 • NIS direktiva
- 2 • Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga
- 3 • Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga

NIS direktiva

- **Rezultat šire EU strategije o kibernetičkoj sigurnosti**
- Unapređenje pružanja usluga od posebne društvene i gospodarske važnosti na razini EU
- **CIU**
- Osiguravanje **visoke razine zaštite kibernetičke sigurnosti** u mrežnim i informacijskim sustavima čije bi kompromitiranje i/ili nedostupnost moglo imati snažan neželjeni utjecaj na stabilnost i ekonomiju zemlje članice Europske Unije

Zakon o kibernetičkoj sigurnosti

- Zakon kojim se :
- RH usklađuje sa zahtjevima NIS direktive
 - Osigurava provedbu Provedbene uredbe Komisije (EU) 2018/151 od 30. siječnja 2018. godine

- **CIU**
- Osigurati **provedbu mjera** za postizanje visoke zajedničke razine kibernetičke sigurnosti u davanju usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti, uključujući funkcioniranje digitalnog tržišta

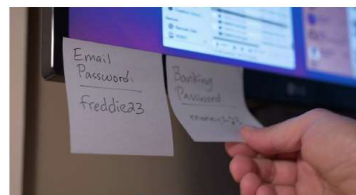
Zakon o kibernetičkoj sigurnosti – opseg primjene



Zakon o kibernetičkoj sigurnosti – opseg primjene

Sektor ključne usluge	Podsektor	Ključna usluga	Kriteriji za utvrđivanje važnosti negativnog učinka incidenta	Pragovi za utvrđivanje važnosti negativnog učinka incidenta
Prijevoz	Vodni prijevoz	Ukrcaj i skrcaj tereta u lukama u međunarodnom i domaćem prometu	Nedostupnost i ograničenost operativnog sustava Važnost održavanja dostatne razine usluge	Nemogućnost obavljanja ključnih operacija u periodu duljem od 3 dana Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od 3 dana može uzrokovati zastoje u ovisnim sektorima

Primjeri neprihvatljive prakse





IJOŠ...



1. Koji Zakon u Republici Hrvatskoj ima za cilj postizanje visoke razine kibernetičke sigurnosti ključne usluge?

- a) Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i pružatelja digitalnih usluga
- b) Zakon o zaštiti osobnih podataka
- c) Zakon o vodnim uslugama

2. Koja vrsta napada čini najveći udio incidenata informacijske sigurnosti?

- a) Malware
- b) DoS
- c) Phishing

3. Primarni cilj kibernetičke sigurnosti u Lučkoj upravi Ploče je zaštita:

- a) Informacija
- b) Ukrcaja i iskrcaja tereta u lukama u međunarodnom i domaćem prometu
- c) Evidencije imovine

4. Informacijska i kibernetičke sigurnost odgovornost su:

- a) Ravnateljstva
- b) Odjela za digitalizaciju
- c) Cijele organizacije

ZAKLJUČAK



**Kako i zašto se implementira
informatička / kibernetička sigurnost**

Zaštita povjerljivosti, cjelovitosti i dostupnosti
informatičke imovine i ključnih procesa radi:

- Osiguranje kontinuiteta poslovanja,
- Umanjenje poslovnih rizika
- Sukladnost sa zakonskim obvezama (GDPR, NIS/ZKS)
- Očuvanje reputacije institucije
- Očekivanja trećih strana – korisnika usluga



Kako možete doprinijeti

- Upoznatost s relevantnim upravljačkim okvirom
- Primjena propisanog okvira u svakodnevnom radu
- Prihvatanje odgovornosti
- Prepoznavanje i promptna prijava sumnjivih događaja



Vaši postupci izravno utječu na sigurnost.



Presentation number 2: Safety and Security



Pilot activities in port of Ploče within the project SUSPORT

LOCAL EVENT "SUSPORT" PROJECT
Educational lecture on information/cyber security with the aim of protecting information assets of the Ploče Port Authority

Development of conceptual design for Digital Green Incident Management – Incident Management with the aim of reducing incidents that have an impact on the environment and people in port areas as part of the WPA project SUSPORT

Local event | Ploče | June 28th 2023
Port of Ploče Authority




AGENDA

- INTRODUCTION
- PROJECT PARTNER BUDGET
- PILOT ACTIVITIES
- CONTACT US




INTRODUCTION

The main objective of SUSPORT is to enhance the environmental sustainability and energy efficiency of the ports in the Programme Area through increased institutional cooperation to create the basis for coordinated and permanent governance in the context of port environmental sustainability and energy efficiency at cross-border level, jointly developing action plans and a long-term strategy, increasing coordination and cooperation between ports to strengthen sustainability and competitiveness.

Through SUSPORT, ports of the Programme Area, will be able to share best practices and develop common methodologies for environmental sustainability and energy efficiency, to be tested in concrete pilot actions significantly improving the environmental performance of maritime transport in the whole Programme Area.




INTRODUCTION

Port of Ploče Authority

- Primary focus on creating and securing conditions for efficient management of maritime and public property.
- Creating preconditions for the transformation of the port from a transshipment port to a regional logistics center in which, in addition to the application of modern technologies, various distribution and additional services will be provided on goods that run through the port.








PROJECT PARTNER BUDGET

Max. ERDF amount of funding awarded	Approved Partners' cofinancing	Approved total project budget
€ 374,000,00	€ 66,000,00	€ 440,000,00
External services and Equipment (Pilot activities) € 280,000,00		
Staff costs € 76,000,00		




PILOT ACTIVITIES

- Replacement of the existing port lightning system with energy-efficient technology (A4.2) – 83,000,00 €
- Purchase and implementation of environment protection barriers (A4.2) – 42,500,00 €
- Replacement of the existing air condition system in Port of Ploče Authority data center with energy-efficient technology (A4.2) – 49,000,00 €
- Installation of sensors and stations for monitoring noise, air and water quality to measure concentrations in port areas and to display measurements with related development of IT platform to support data exchange within subsystems (A4.2) - 32,000,00 €




PILOT ACTIVITIES

- Micro Data Center solution for Data Recovery site with efficient cooling system and intelligent electrical power distribution. Will be located in port of Ploče area where physical protection is also needed against fire, water, dust, smoke and external access – scd 27,000,00 €
- Digital Green Incident Management - Slow and incorrect actions when dealing with an incident or disruption (e.g. accident on a port terminal) leads to the emergence from a small incident to a crisis and thus to unnecessary consumption of resources or consequences for people and the environment. This is exactly where every second / minute that is saved through a quick and structured incident management approach is crucial. Especially if dangerous hazards are involved in an incident analysis showed that each minute where the situation is cleared faster there is a significant protection of the surrounding environment. Furthermore, unnecessary CO2 consumption is significantly reduced due to a faster, more structured and optimized approach. – 23,000,00 €



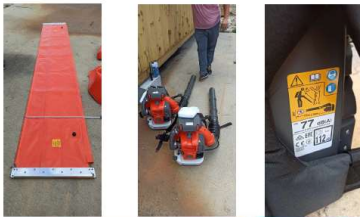

PILOT ACTIVITES – Technical documents

- Professional supervision services for the execution of electrical works for the facility: energy renovation of outdoor lighting on sections of port road 1 and 2, Shunting track 1 and 2
- Preparation of analysis and feasibility study of the use of renewable energy sources in the area of the entrance terminal of the Port of Ploče with the aim of energy efficiency
- Preparation of a feasibility study for the project of application of the power supply system (Cold ironing) for ships from the mainland in the Port of Ploče with the aim of energy efficiency

PILOT ACTIVITES – Technical documents

- Potential calculation, development of preliminary and main design of solar power plant 70-100kW
- Project of adaptation and air conditioning to a photovoltaic power plant
- Professional assistance service for external consultants in drafting documents TNA, Action plan
- The technical project documentation as prerequisite for the Replacement of the existing air condition system in Port of Ploče Authority data centre with energy efficient technology (A4.2)

PILOT ACTIVITES - Description



PILOT ACTIVITES - Description



PILOT ACTIVITES - Description



PILOT ACTIVITES - Description



PILOT ACTIVITES - Description



PILOT ACTIVITES - Description



PILOT ACTIVITES - Description

- Replacement of the existing air condition system in Port of Ploče Authority data center with energy-efficient technology (A4.2)
 - For the purpose of more efficient cooling of IT equipment for indoor units, modular, vertical cooling systems will be delivered. Cooling units will be placed at the full height of the server cabinets/racks. These are the most energy-efficient solutions that allow hot air from the equipment to be brought to the cooling modules in the shortest possible way. It enable distribution of cold air over the entire height of the server cabinets/rack.
 - They are placed between the racks and allow cooling of two or three racks depending on the total heat dissipation. According to the existing configuration of the data center, 8 server/communication cabinets/racks placed in two rows. For this kind of configuration, it will be installed 2 LCP (Liquid cooling device) DX devices per row or 4 devices in total. This achieves sufficient cooling capacity and achieves the necessary system redundancy.
 - The value of the equipment amounts to 49.000,00 EUR

PILOT ACTIVITES - Description

- Replacement of the existing air condition system in Port of Ploče Authority data center with energy-efficient technology (A4.2)
 - Installation has been made in The Port of Ploče Authority Data/Server room which is located in the new building of the new entrance terminal. Installation will cover installation of cooling units, power distribution system and project documentation. With the installation of the new IT cooling system Port of Ploče Authority will achieve significant energy savings.

PILOT ACTIVITES - Description

- Replacement of the existing air condition system in Port of Ploče Authority data center with energy-efficient technology (A4.2)



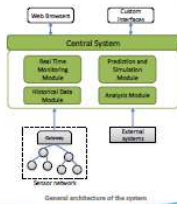
PILOT ACTIVITES - Description

- Replacement of the existing air condition system in Port of Ploče Authority data center with energy-efficient technology (A4.2)



PILOT ACTIVITES - Description

- Installation of sensors and stations for monitoring noise, air and water quality to measure concentrations in port areas and to display measurements with related development of IT platform to support data exchange within subsystems (A4.2)



PILOT ACTIVITES - Description

- Installation of sensors and stations for monitoring noise, air and water quality to measure concentrations in port areas and to display measurements with related development of IT platform to support data exchange within subsystems (A4.2)



PILOT ACTIVITES - Description

- Installation of sensors and stations for monitoring noise, air and water quality to measure concentrations in port areas and to display measurements with related development of IT platform to support data exchange within subsystems (A4.2)
- DATA MONITORING AND VISUALIZATION
 - The system will offer a web-based dashboard capable of showing the gathered data, both in a real-time view and in an historical view, where the user will be able to filter specific parameters or periods.
 - The dashboard will offer many control panels, represented with a cartographic layout, where the system operator will be able to select a single sensor/node, to read its measurements and to be warned when critical real-time events occur, like for example alerts (see Anomaly detection).
- ANOMALY DETECTION
 - The system will generate alerts based on custom rules defined by the users and when the data analysis module realize that the incoming data is not following the usual historical patterns. For example if the system receives an abnormally high reading of CO2 value from a set of sensors, or in avoid alerts for a malfunctioning single sensor, an alert is generated for the person in charge, by sending an email or showing an alert symbol in the dashboard.

PILOT ACTIVITES - Description

- Installation of sensors and stations for monitoring noise, air and water quality to measure concentrations in port areas and to display measurements with related development of IT platform to support data exchange within subsystems (A4.2)
- PREDICTION AND SIMULATION
 - The system will enable to carry on predictor analysis on the level of total emissions in the monitored areas, allowing the key actors of the present context (port and local public Authorities, etc.), through the use of DSS (Decision Support System), to plan an efficient movement of cargo, to prevent risks due to traffic congestion, to reduce the total environmental impact of the activities (i.e. carbon footprint, noise, vibrations, etc.).
 - This model will be built around the correlations between the environmental parameters measured by the sensors and the metadata generated by the information system of the port.
 - The model will allow to gather information on ship voyages from Port Management Information Systems, like for example the list of transported goods and the load/unload operations, and label each process or macro process with an environmental impact footprint based on the parameters under examination. In this way the system will not be limited to only measuring the pollution level in the port area, but it will also be able to constantly update a predictive model, which will be used by the port and public Authorities to simulate decision supporting scenarios and to forecast the trend of the examined environmental variables.

PILOT ACTIVITIES - Description

- Micro Data Center solution for Data Recovery site with efficient cooling system and intelligent electrical power distribution. Will be located in port of Ploče area where physical protection is also needed against fire, water, dust, smoke and external access. (AA.2)



PILOT ACTIVITIES - Description

- Digital Green Incident Management (AA.2)

- Information security and safety and security in ports are closely interconnected and both play a key role in ensuring protection and smooth operation port facilities.
- Here are some key points that highlight the link between information security and protection and security in ports:

- Protection of critical infrastructure
- Integration of the physical security
- Cybersecurity operational technology
- Protection of sensitive data
- Emergency response and incident management
- Supply chain security



PILOT ACTIVITIES - Description

- Digital Green Incident Management (AA.2)

Informacijska sigurnost i zaštita i sigurnost (eng. safety & security) u lukama usko su međusobno povezane i oboje imaju ključnu ulogu u osiguravanju zaštite i nesmetanog rada lučkih objekata. Evo nekoliko ključnih točaka koje ističu vezu između informacijske sigurnosti i zaštite i sigurnosti u lukama.

- Zaštita kritične infrastrukture: Luke se smatraju ključnom infrastrukturom zbog svoje ekonomske važnosti i uloge u globalnoj trgovini. I sigurnosne i sigurnosne mjere potrebne su za zaštitu ove vitalne imovine od fizičkih prijetnji, kibernetičkih prijetnji i potencijalnih poremećaja.
- Integracija fizičke sigurnosti: Sustavi informacijske sigurnosti i zaštite često se moraju integrirati kako bi pružili sveobuhvatnu zaštitu. Na primjer, sustavi kontrole pristupa, nadzorne kamere i alarmni sustavi koji se koriste za fizičku sigurnost mogu se povezati sa sustavima informacijske sigurnosti kako bi se osigurao siguran pristup osjetljivim područjima, otkrio i odgovorilo na kršenja sigurnosti i spriječila neovlaštene aktivnosti.



PILOT ACTIVITIES - Description

- Digital Green Incident Management (AA.2)

- Kibernetička sigurnost operativne tehnologije (OT): lučke operacije uvelike se oslanjaju na računalne sustave i međusobno povezane tehnologije poznate kao operativna tehnologija (OT). Osiguravanje kibernetičke sigurnosti OT sustava ključno je za sprječavanje neovlaštenog pristupa, povrede podataka i mogućih poremećaja koji mogu utjecati na sigurnost i radni kontinuitet u lukama.

- Zaštita osjetljivih podataka: Luke obrađuju značajnu količinu osjetljivih informacija, uključujući teretne manifeste, rasporede plovila, caniske podatke i financijske evidencije. Potrebne su snažne mjere sigurnosti informacija kako bi se ti podaci zaštitili od krađe, neovlaštenog pristupa, što bi moglo imati značajne sigurnosne implikacije ako se zlouporabi.



PILOT ACTIVITIES - Description

- Digital Green Incident Management (AA.2)

- Odgovor na hitne slučajeve i upravljanje incidentima: Sigurnost informacija i zaštita usko su povezane tijekom hitnih situacija. Učinkovito upravljanje incidentima zahtijeva koordinaciju između timova za fizičku sigurnost i zaštitu i osoblja za informacijsku sigurnost kako bi se ublažile prijetnje, odgovorilo na incidente i obnovilo normalno funkcioniranje.

- Sigurnost lanca opskrbe: osiguranje sigurnosti i zaštite globalnog lanca opskrbe ključno je za luke. To uključuje provjeru cjelovitosti robe, sprječavanje krijumčarenja i zaštitu od potencijalnih prijetnji poput terorizma. Mjere informacijske sigurnosti, uključujući sigurne komunikacijske kanale, enkripciju podataka i mehanizme provjere autentičnosti, ključne su za održavanje integriteta i sigurnosti opskrbnog lanca.



PILOT ACTIVITIES - Description

- Digital Green Incident Management (AA.2)

Informacijska sigurnost i sigurnost i zaštita (safety & security) u lukama predstavlja međusobno povezana područja koja se moraju holistički rješavati kako bi se zaštitili lučki objekti, spriječili prekidi, zaštitili osjetljivi podaci i osigurao učinkovit i siguran protok robe i usluga kroz globalni lanac opskrbe.

U sklopu EU projekta SUSPORT Lučka Uprava Ploče za cilj ima postizanje više razine informacijske sigurnosti i zaštite i sigurnosti s naglaskom na upravljanje incidentima koji u posljedici imaju utjecaj na okoliš i ljude u lučkim područjima.

Upravljanje incidentima u lukama s ciljem smanjenja njihovog utjecaja na okoliš i ljude zahtijeva sveobuhvatni pristup koji integrira pitanja sigurnosti, sigurnosti i okoliša.



PILOT ACTIVITIES - Description

- Digital Green Incident Management (AA.2)

- In short, information security and security in ports intertwined are areas that must be holistically addressed in order to protect port facilities, prevent interruptions, protect sensitive data and ensure the efficient and safe flow of goods and services through the global chain supply.

- Within the EU project SUSPORT "incident management with the aim of reducing incidents that have an impact on the environment and people in port areas", the Port of Ploče Authority aiming to achieve a higher level of information security and security and security with an emphasis on managing incidents that have an impact on the environment and people in port areas.



Contact

 Port of Ploče Authority, Glavna cesta 2, 20340 Ploče
 ppa@ppa.hr
 +385 20 414 535
 www.italy-croatia.eu/susport