COMPACT

CYBERSECURITY FOR PUBLIC ADMINISTRATIONS

Cybersecurity Solutions for Public Administrations

COMPACT Final Workshop
Major Cities of Europe - Venice
June 14 | 14:00 - 16:45

Part I - 14:00

The COMPACT project

- Paolo Roccetti | Engineering Ingegneria Informatica S.p.A.
- Luigi Coppolino | CINI - Consorzio Interuniversitario Nazionale per l'Informatica

Cybersecurity Challenges in Public Administration

- Davor Meersman | Open & Agile Smart Cities
- Fabio Massacci | UniTrento
- David Goodman | Trust in Digital Life

Part II - 15:15

The COMPACT Platform

- **Psychological factors in cybersecurity**
  Human Factor Profiling
  Daniela Wurhofer | Austrian Institute of Technology

- **Cybersecurity Awareness Training**
  A gamified approach
  Amedeo D'Arcangelo | Kaspersky Lab Italia

- **Knowledge Sharing**
  The COMPACT Information Hub
  Barbara Pirillo | Engineering Ingegneria Informatica S.p.A.

COMPACT Public demonstration

@COMPACTproject

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 740712.

Subscribe to
our newsletter:

COMPACT

Cybersecurity Solutions for Public Administrations

COMPACT Final Workshop
Major Cities of Europe - Venice | June 14 | 14:00 - 16:45

COMPACT brings to you a panel of cybersecurity experts to discuss the challenges faced by Public Administrations.

Davor Meersman is the General Manager of Open & Agile Smart Cities (OASC), a global initiative counting 117 member cities from 24 countries. OASC and its member cities are shaping the global smart cities data and services market in collaboration with partners such as the European Commission, the United Nation's International Telecommunications Union, the European Telecommunications Standards Institute, TM Forum, etc. Davor is also Co-Chair of the BDVA Task Force on Smart Cities, Ambassador of the International Society of Service Innovation Professionals, and a senior consultant on smart city technology, strategies, and funding. As senior researcher at the world's leading nano and digital technologies research institute IMEC, Davor was one of the founders of City of Things, the largest smart city IoT living lab in Europe. Davor holds a PhD in Information Systems from Curtin University, Australia.

Fabio Massacci has been at Cambridge, Siena and Toulouse and he is now full professor at UNITN. He has published more than 250 peer-reviewed papers and has an h-index of 36. For his research on security engineering, he got the 10 years most influential paper award by the IEEE RE’15 Conference. His research interests are at the crossroads between formal models for computer security, malware and vulnerability prediction models and security economics. Currently he is working on predictive models for vulnerabilities, empirical validation of risk and security methodologies. He was the coordinator of SECONOMICS and local coordinator of the EIT MSc Programme on Security & Privacy.

David Goodman has over twenty-five years IT and telco experience in senior management positions at Lotus (IBM), Tivoli (IBM), Nokia Siemens Networks and Ericsson, at University College London, various start-up companies in Europe and North America and as a consulting analyst at KuppingerCole and TechVision Research. He has specialised primarly in the areas of identity and security and more recently privacy/data protection, EU regulations (GDPR, PSD2, eIDAS et al.), blockchain and artificial intelligence. He brings experience in collaborating closely across multiple disparate teams, active communication with stakeholders, senior management and developers, as well as industry press and analysts. For 13 years, he was chairman of EEMA, a European industry association, and has had close links to the European Commission.

Psychological factors in cybersecurity
Human Factor Profiling

The increased use of digital technologies and internet connections in organizations brings with it a growth in potential cyber-attacks (Jang-Jaccard & Nepal, 2014). At the same time, human behavior is argued to be the weakest link in the security chain (Crossler et al., 2013; European Commission, Directorate-General for Home Affairs & TNS Opinion & Social, 2015; Yan et al., 2018). Thus, to maintain cybersecure behavior at the workplace, it is imperative to have a profound understanding of the concept of cybersecure behavior and how it is influenced.

Within COMPACT we conducted several psychological studies and investigated the following central research questions: What are individual/psychological predictors of security-related behavior of employees? How and to which extent do these human factors influence security-related behavior? Why do people in one situation behave in a security-conscious manner and in another they do not? What are contextual factors that influence security-related behavior? Within the talk we present results of this studies and a survey instrument developed to assess these predictors of security-related behavior.

Cybersecurity Awareness Training
A gamified approach

Supporting the "learning by doing" approach by John Dewey, wishing to improve the student's motivation and lead to deeper understanding and learning, COMPACT aims to increase the cyber security awareness of LPA employees. By educating them about the cyber risks that they are most exposed to and by empowering them to decide which approaches to adopt: the strengthening of the weakest link in the security chain elevates the cyber-security level of the LPA.

The COMPACT modules on Security Awareness Training embrace the gamification approach to be more attractive to employees and are customized for specific categories of LPA employees, taking into consideration gender issues, personality traits and more. Within the talk we present the Security Awareness Trainings we implemented, with a special focus on the gamified educational contents.

Knowledge Sharing
The COMPACT Information Hub

The new community space, called the Information Hub is one of the main results of the Knowledge Sharing Services delivered by the COMPACT project. This is about enabling an interactive exchange of information across LPAs and providing them with instruments, best practices and the necessary knowledge to handle with cyber security issues. The final aim is to increase the cyber security awareness and level of understanding of the LPA's employees.

Learn more about the Information Hub during the dedicated session and join us! It will become your instrument to:

- disseminate and promote your cyber security awareness events and campaigns as well as news and results;
- get input and inspiration from the best practices published by the European local public administrations part of the community;
- get further understanding about the most common cyber threats LPAs suffer from and the related solutions.