How to Protect Public Administration from Cybersecurity Threats: the COMPACT Project

Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano, Luigi Sgaglione

Department of Engineering University of Naples Parthenope Naples, Italy
luigi.coppolino, salvatore.dantonio, giovanni.mazzeo, lrom, luigi.sgaglione@uniparthenope.it

***Abstract*—The advent of the Internet has been opening new opportunities for Local Public Administrations (LPAs) to improve their efficiency while providing better services to citizens via an ever larger set of specialized network applications, including e-government, e-health, and more. Indeed, as a potential channel of accessing personal information, these specialized applications also expose the public sector to new risks. The cybersecurity landscape is changing, and Local Public Administrations are rapidly becoming an attractive target for cybercriminals, who might access some sets of personal data or gain control over smartly operated city resources through LPAs infrastructures. The consequences of cyber-threats have the potential to be considerable causing business interruptions, data losses, and thefts of intellectual property, significantly impacting both individuals and organizations. This paper provides an overview of the EU H2020 COMPACT (Competitive Methods to protect local Public Administration from Cyber security Threats) project, that aims to increase LPAs awareness, skills, and protection against cyber threats through risk assessment, game-based education, monitoring and knowledge sharing services that are highly usable, interoperable with major Commercial Off-The-Shelf (COTS) solutions, cloud-enabled and cloud-ready.**

Keywords—Local Public Administration, Risk Assessment, gamification, security awareness, threat intelligence

I. INTRODUCTION

It is claimed that cyber threats are the most significant and rising risk that public sector organisations are facing. Reports demonstrates that nearly 40% of malware attacks and in general cyber threats to which public bodies have been subject [1] are against public sector organisations [2], i.e. more than sectors (e.g. finance) which have traditionally been thought of as top targets. The interconnection of operational environment systems, used by the public bodies in ever growing scale, exacerbates the problem, especially as malware distribution periods (both fixed and mobile) are becoming increasingly short [3]. The increase in severity of cyber-attacks coincides with a boom in the different types of connected devices, as well as with a huge expansion in virtualisation and public clouds. The issues that have been identified and that hamper the ability of Local Public Administration (LPA) organizations of improving their cyber security level, most notably are [4] [5] [6] [7] [8]:

1. Lack of standardized data classification – 45% of public sector respondents do not use standardized data classification techniques/procedures. As a consequence, LPAs run a higher risk of accidentally exposing private data in their rush to comply with emerging regulations – both at the national and at the EU level – promoting transparency of the Public Sector.

2. Lack of effective Non-Disclosure Agreements (NDAs) – 40% of public sector organizations still rely on paper-based NDAs, and use them inconsistently. This amplifies risks related to the human factor, which is already one of the biggest security issues since malicious or disgruntled personnel with access to important information assets can be a significant threat to the security of those assets.

3. Lack of plans for responding to security breaches and for disaster recovery – 36% of public sector organizations do not have a plan for responding to security breaches, and only 10% of public sector organizations test for the worst-case scenario.

4. Lack of uniformly enforced security policies – 33% of public sector organizations do not have uniformly enforced security policies.

5. Lack of adequate policies and practices for data disposal – 76% of public sector organizations do not have adequate policies and practices for secure and reliable data disposal. The enforcement of strong policies to govern the proper disposal of electronic and paper records - based on sound technical and organizational guidelines and best practices - is the prerequisite for protecting private data from unauthorized disclosure.

6. Lack of effective access control mechanisms – 20% of public sector organizations do not use roles to manage access, and more than 26% of public sector organizations have no official procedure for terminated or reassigned employees. This create vulnerabilities, since it allows inappropriate access to resources.

7. Large set of legacy unmaintained and undocumented systems representing an attack surface of unknown dimension.

8. Inappropriate management of security updates (patches), as well as usage of out of date software in computers, mobile devices and central servers.

9. Limited capacity, and motivation, of LPAs personnel in detecting and reporting cyber-attacks. This is due to a

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

number of interconnected factors including (i) the aging of the LPAs workforce, (ii) its limited technological skills and (iii) the lack of acknowledgment of employees' achievements.

The EU H2020 COMPACT (Competitive Methods to protect local Public Administration from Cyber security Threats) project aims at providing a service-based platform, including education services, to improve the level of protection of LPAs. COMPACT will provide effective protection against the most relevant threats to which LPAs are exposed, some of which are briefly described in Section II. COMPACT will develop four types of tools/services, which include: (i) Risk assessment tools - Tailored to the LPAs context that will allow LPAs to evaluate and monitor their exposure to the most relevant (i.e. with the highest impact) cyber treats; they will enable LPAs to prioritize the adoption of preventive and reactive countermeasures, for maximum efficiency of resource usage for cyber protection purposes; (ii) Education services - Through dedicated game-based training, focused not only on specific cyber-threats but also on psychological and behavioural factors, to maximize the effectiveness of the learning experience, while also containing the training time; (iii) Monitoring services – That continuously process events related to the status of the infrastructure and correlate them with information from threat intelligence feeds to timely spot anomalies and also suggest recovery actions that can be implemented; (iv) Knowledge Sharing services – These will include best practices and guidelines, focused on the specific needs of LPAs, that can be easily adopted to quickly increase the cyber security level of the organization.

The remainder of this paper is structured as follows. Section II provides a survey of cybersecurity threats concerning Local Public Administrations. In Section III the COMPACT cybersecurity framework is presented, while Section IV illustrates the COMPACT cybersecurity management methodology based on the PDCA (Plan-Do-Check-Act) cycle. The use case-driven approach adopted by COMPACT to validate projects results is presented in Section V along with an example of validation pilot. Finally, Section VI gives some concluding remarks.

II. A SURVEY OF LOCAL PUBLIC ADMINISTRATION CYBERSECURITY THREATS

OMISSIS

III. COMPACT CYBESECURITY FRAMEWORK

COMPACT will deliver a set of tools in an integrated platform, that will collectively provide five categories of tools/services, that will represent the "building blocks" of the cyber security improvement of LPAs. This framework will be devised focusing on selected areas in which some innovative leaps are going to be performed to obtain a result that makes the difference through the "wow" effect, just like the pieces of a puzzle: once combined together they create a meaningful picture.

A. *Real Time Security Monitoring*

Real Time Security Monitoring solutions have always been represented by an autonomous component completely detached by the human factor that detects or prevents a hazardous situation and mitigates its effects. By the way, detection logics, the related intervention and the protection processes linger in the automation context without significant influences on the human awareness. An innovative leap is given by the transposition of this kind of tool in the context that feeds the system's module that mainly interacts with the user to guide him/her during the learning process, leading him/her during the activities, correcting bad practices and filling dangerous gaps. The breakthrough thinking behind this transposition [14] enables the exchange of feedback in the human-system interaction to better suggest what to do to improve and to check each progress.

B. *Security Awareness Training and Information sharing*

Security Awareness Training and Information sharing are two concepts that belong to the core of the solution against cyber threats and social hacking exposition. Protection software in this case is essential but "the best protection is knowledge: security through education" [15]. The use of a personalized learning platform accounts for the best way to deliver knowledge with a high level of flexibility and ubiquity (i.e. via apps for smartphones and tablets). COMPACT makes a step further introducing cutting edge approaches (such as gamification and role playing features, entertaining tasks and adaptive content delivery which will be explained more in detail in the following lines) to improve user's awareness. Once the user earns a richer knowledge and gains experience about cyber and social defence techniques, it is appropriate to give him/her the opportunity to share this experience with other user. Here comes another innovative leap: let the sharing process travel onto 2 levels: the first one allows the information spreading among the members of a single PA organization, the second one extends this possibility to the communication layer that link all those PAs that want to embrace the same ideals that are the pivot of the COMPACT project [16].

C. *Cybersecurity Awareness Training, based on Gamification principles*

"Game" by definition is an entertaining activity. Whenever many people hear about "serious games" hide the misconception that those interactive experiences are everything but funny. Serious games have both an educational component and an entertaining component that can be more or less developed. Overall, the more engaging and immersive the game is, the more chances to be successful it has, and this is a rule that applies to every kind of game: a triple-A title like Assassin's Creed by Ubisoft, classifiable as serious game due to its historical content, has now even a solid fandom and a worldwide diffusion. COMPACT will use gaming content to better accomplish its mission of knowledge infusion and

diffusion, betting on such an immersive and powerful media. The macro-factors that shape the fate of a game are: gameplay, re-playability, co-operation/competition between players, graphics power, level design, plot, technical, artistic and sound aspects. All these elements do not have to be necessarily coexistent; a couple of them are enough for a game to be "catchy". COMPACT relies on gamification, real-life simulation, team work and competition to allow users to be immersed into an experience that helps them to absorb key concepts, behaviours and a surveillance stance against cyber threats and related menaces.

D. Risk Assessment

Risk assessment "is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyses the risk in term of consequences and their probabilities before deciding on whether further treatment is required" [17]. In recent years, a number of risk assessment techniques (also listed in IEC/ISO 31010 international standard) have been developed to identify and describe the threats a system is exposed to, as well as to evaluate consequences and probability related to the materialization of a given risk. Relevant examples include techniques based on scenarios (like the Root Cause Analysis or the Business Impact Analysis), as well as those based on qualitative and semi-quantitative risk ratings (like the Consequence/probability matrix).

E. Threat Intelligence

Every organization nowadays needs to protect its own data behind an unbreakable shield. Unfortunately, there is neither magic nor special protection to stay safe against those cyber menaces that jeopardize user privacy, information security and the robustness of computer infrastructures. The real weakness is often represented by the lack of a manoeuvre that takes measures wide enough to cover almost all the possible kinds of attack and threat; organizations are used to invest in interventions strictly related to their own IT systems, without considering an extended view on the worldwide context of the digital security. That is the main reason why Cyber Threat Intelligence (CTI) systems were born. They are platforms and services that gather data from heterogeneous sources to generate a richer and up-to-date awareness about current activities and possible risks. COMPACT adopts and improves CTI concepts to deliver the best solution to the organizations managing the widest range of threat handling and applying the most specific plan for the risk treatment case by case.

IV. PDCA CYCLE-BASED CYBERSECURITY MANAGEMENT

COMPACT proposes a specialization of the well-known and consolidated Plan-Do-Check-Act (PDCA) cycle which enables LPAs – during the operational phase following the development of the COMPACT technology – to innovate their cyber security improvement process, also – importantly – in compliance to the EN ISO/IEC 27001 and BS ISO/IEC 27005 standards. The four phases in the Plan-Do-Check-Act Cycle are:

- Plan: Identify and analyse the problem.
- Do: Develop and test a potential solution.
- Check: Measure how effective the tested solution was, and analyse whether it could be improved.
- Act: Implement the improved solution fully.

According to the BS ISO/IEC 27005 standard a systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements as well as to create an effective Information Security Management System (ISMS). Even though there exist many approaches by which an information security management process can be successfully performed in an organization, BS ISO/IEC 27005 proposes the PDCA cycle as driving methodology for the implementation and ongoing operation of an ISMS and aligns the information security risk management activities with the four phases of the PDCA cycle-based ISMS process.

Specifically, according to BS ISO/IEC 27005 context establishment, risk assessment, risk treatment plan development, and risk acceptance compose the "Plan" phase, while the "Do" phase consists of all the actions included in the risk treatment plan. In the "Check" phase a continuous monitoring is performed and the need for a revision of the risk assessment and treatment is evaluated in the light of incidents and changes of the context. Finally, the "Act" phase comprises any actions needed to maintain and improve the information security risk management process. COMPACT takes into account this alignment in order to design a cybersecurity framework fully compliant with the BS ISO/IEC 27005 recommendations and correctly position technical and procedural achievements in an effective ISMS process.

A. Plan

The Plan phase of the COMPACT methodology aims at estimating the risk affecting the LPA being protected and specifying the security policies that will be enforced in order to mitigate the estimated risk during the subsequent methodology steps. During this phase the context of the organization is established by collecting and analysing information related to both technological and human aspects. Specifically, assets will be identified and profiles of the LPA personnel will be created. This information will be correlated in a real time fashion with the data from external sources, such as vulnerability databases and security information sharing platforms, and business process monitoring applications in order to perform the risk assessment task.

B. Do

The objective of this phase is to implement the risk treatment strategy that has been designed in the PLAN phase. This objective will be achieved by performing the following main actions:

- Policy Enforcement: aimed at executing the security policies specified in the risk treatment plan and coping with the risk estimate produced by the dynamic risk assessment.

- Game-based Security Awareness and Training: allowing users to gain first-hand experience of the different risks and threats. The training module educates employees about their role, the most common attacks and how they can protect their system. Games will be tailored to different roles in the LPAs, to better adapt to the education needs of different profiles, as well as focus on specific kinds of threats (i.e. Social Engineering, Ransomware and Data Breaches). The deployed tools will be a trade-off between cost-effectiveness and user-friendliness, thus simplifying as much as possible their adoption.

C. Check

The objective of the Check phase is to assess the effectiveness of the risk treatment actions implemented during the previous step. Real Time Security Monitoring and Threat Intelligence will allow for effectively and timely detecting weaknesses in the adopted risk treatment strategies, thus measuring the residual risk generated by their application. A new estimate of the risk level is produced and the security policies are updated accordingly. Tests will also be conducted to collect users' feedback about the usability of the COMPACT tools and identify possible improvements.

D. Act

In the Act phase the previously adopted countermeasures and risk treatment strategies are adjusted in accordance with the update of the security policies performed in the Check phase. The implementation of this adjustment will result in a new residual risk.

V. COMPACT VALIDATION PILOTS

COMPACT validates its approach by evaluating the different strands of its work (i.e. increase in awareness, skills, and protection; favour information exchange at the local PA level; and link local PA level to EU level) through selected use cases.

Collectively, the use cases address a variety of:

- Technical challenges, such as: confidentiality and integrity of organization assets, availability of information and systems, access control, unauthorized access to sensitive information, ransomware blocking work capacity, data access policies, secure data exchange, logical and physical security of the infrastructure, dynamic management of risks, compliance to standards and regulations, user authentication, secure data exchange, user profiling, awareness about specific cyber threats and ability to identify them, personalized training programs, thorough cyber risk analysis, real-time monitoring of security-related events and information, user training on safe use of applications, business continuity management, issues related to interaction among heterogeneous hardware and software platforms/products.
- Psychological aspects, such as: exchange of information between technical and non-technical employees, barrier to requesting help among departments, barrier to requesting help between different hierarchical levels, avoiding asking for help too frequently, confidence building of employees.
- Policy, legal and privacy implications, such as privacy and data protection of individuals, privacy and data protection of employees of LPA organisations, organisational security policies, user empowerment by access by user profile.

The description provided below is done in a "story telling" approach, using fictitious characters to convey the main focus of the scenarios, and refers to the use case focused on the interaction between expert and non-expert employees.

Maria is one of the employees of a Municipality in charge of filing applications – from citizens and enterprises – for construction authorization. This involves gathering documents from applicants (both paper-based and paper-less), extracting relevant information, feeding it to the information system of the municipality, interfacing with offices and employees (of the municipality and possibly of other PA organizations) as well as with the public. Intuitively, Maria knows that she handles sensitive data. In the current approach, when Maria is uncertain about what she should do, she asks her boss Anna for a final decision. As head of office, Anna knows that Maria (and her colleagues) are conscientious workers, but lack the comprehensive and up to date background needed to address the inherent security issues of their job. She is also aware that, in case Maria (or another colleague) makes a mistake, she – as the boss – would ultimately be liable for the consequences of it. Anna would very much appreciate being able to improve the process consistently, for her entire team, by including expert guidance, supporting – and possibly driving – employees throughout the process. She would also like to ensure that any changes and new issues to take into account are easily included in the process, but she does not have the right knowledge to create this expert guidance, due to the complexity of cyber-security issues involved and to the continuous evolution of threats. Carlo is an engineer in the IT department of the municipality, recently recruited for his cyber-security skills. But he has a) not the time b) not the means and most of all c) not the training in how to educate non-technical/non-expert individuals - such as Anna, Maria, and the others - to provide guidance and/or transfer knowledge. Furthermore, there is a real barrier in that Anna, Maria, and the team of employees who are experienced in the process and who interact with the citizens do not readily accept that the process needs to be completely, and dynamically, revised to constantly take into account new cyber risks. This situation creates psychological barriers that limit (if not prevent altogether) the possibility for Carlo, Anna, Maria, and the rest of Anna's team to interact in a constructive way, and improve their respective skills.

Maria, Anna, and Carlo are informed of the COMPACT project. They all get very excited about the advantages that will be brought to them by COMPACT approach and technology, but for different reasons. COMPACT's risk assessment features will allow Maria to take informed

decisions about the data that she handles. In case of doubt, she will have access to COMPACT training features and will be able to sort problems out without having to disrupt Anna from her activity. The gaming approach of COMPACT's training tools will increase the background knowledge of Maria and her colleagues and their ability to cope with cybersecurity issues. It increases the level of confidence of Maria, and her autonomy. This in turn benefits Anna in reducing the level of risk she is exposed to, and this is a great relief to her. It also reduces the time spent by Anna to answer requests, and frees her time to move from reactive answering to proactive investments. Overall, this is a low-cost investment with a huge benefit. COMPACT information exchange features provide Maria with the opportunity to get help/support from her colleagues and/or inspiration by accessing COMPACT best practices data bank. It also creates a collaborative approach to solving problems across colleagues, that is beneficial in terms of the office human dynamics and easing the effectiveness of services offered by the LPA. With more time available for her own tasks, Anna will use COMPACT's threat intelligence features, as well as COMPACT guidelines and best practices repository, to identify security bottlenecks in the process. Carlo can easily convey the cyber-security knowledge and updated cyber-security risks using the COMPACT tools, but without spending time (which he does not have) to also train and continuously support non-technical employees. Carlo is possibly most excited by the new level visibility he acquires: with the availability of COMPACT's advanced real-time security monitoring features, he will have everything under control at all times, and will be able to timely spot any potential security issue.

VI. Conclusions

Local Public Administrations need to understand the cyber risks to which they are exposed and take proper actions to protect their infrastructures from cyber disruptions, to safeguard citizen's and enterprises' information they manage. This paper presented the COMPACT project that will provide tools and services to help LPAs improve their cybersecurity level. COMPACT tools and services will compose an integrated platform offering a didactic framework enriched by gaming aspects, advanced security monitoring techniques, risk assessment functionality, and threat intelligence functions.

Acknowledgment

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740712 (COMPACT - COmpetitive Methods to protect local Public Administration from Cyber security Threats). This paper reflects only the authors' views and the Community is not liable for any use that may be made of the information contained therein.

References

[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[2] http://www.publicfinance.co.uk/opinion/2016/03/time-face-cyber-risk

[3] CCN-CERT, Threats and Risk Analysis in Industrial Control Systems (ICS), Report IA-04/16, Centro Criptologico Nacional: Madrid, 28 Jan 2016 (in Spanish),https://www.ccn-cert.cni.es/informes/informesccncert-publicos/1381-ccn-cert-ia-04-16-amenazas-y-analisis-de-riesgos-en-sistemas-de-control-industrialics/file.html

[4] "Security trends in public sector: Key findings and recommendations", Microsoft,2013,http://download.microsoft.com/download/C/B/0/CB07EFE4-875A-4AD0-8FB0-90959B21E4F8/Security-Trendsin-Public-Sector.pdf

[5] "Open government may exceed prudent boundaries", https://firstamendmentcoalition.org/2009/06/open-government-may-exceed-prudent-boundaries/

[6] "Deflecting and Responding to Data Security Breaches", https://www.irmi.com/articles/expertcommentary/deflecting-and-responding-to-data-security-breaches

[7] "IT Horror Stories: What's the Worst That Could Happen?", http://www.business2community.com/business-intelligence/horror-stories-whats-worst-happen-0856003

[8] R. Lavigna, Why government workers are harder to motivate, Harvard Business Review, 28 Nov 2014, https://hbr.org/2014/11/why-government-workers-are-harder-to-motivate

[9] CCN-CERT, Cyber-Threats 2015 / Trends 2016, Report IA-09/16, Centro Criptologico Nacional: Madrid, 12 May 2016, https://www.ccn-cert.cni.es/en/reports/public/1554-ccn-cert-ia-09-16-cyber-threats-2015trends-2016-executive-summary/file.html

[10] http://campus.ie/surviving-college/government-hit-extortion-wave-new-cyber-attacks

[11] https://www.symantec.com/security-center/threat-report

[12] "FOCA" http://www.informatica64.com/herramientas.aspx

[13] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, Towards automating social engineering using social networking sites, IEEE Xplore CSE'09, pp.117-124(2009)

[14] D. Perkins, "Archimede's Bathtub"

[15] Christopher Hadnagy , "Social Engineering – The art of human hacking

[16] Magic Quadrant for Social Software in the Workplace – Mike Gotta, Nikos Drakos, Jeffrey Mann – 26 Oct 2015

[17] IEC/ISO 31010, Risk management – Risk assessment techniques, Edition1.02009-11
http://www.iso.org/iso/catalogue_detail?csnumber=51073