A methodology for cybersecurity assessment of public administration: a case study on Lombardy municipalities

De Corato Marzio[1], Danilo Bruschi[1], Silvana Castano[1], Alfio Ferrara[1], Onelia Rivolta[2], Nicla Ivana Diomede[3], Luca Bramati[2], Maurizio Piazza[2], Davide Rusconi[1], Matteo Zoia[1]

1) Dipartimento di Informatica, Università degli Studi di Milano
2) ANCILAB
3) Dipartimento di Cybersecurity e Sicurezza Urbana, Comune di Roma

PROJECT FOCUS

Assessment of the maturity level of municipalities compared to three emerging themes in the digital world: cybersecurity, adoption of artificial intelligence techniques the use of big data/data analysis techniques. The project during the first year was dedicated to cybersecurity since this is the habilitating factor for the other two topics.

How to evaluate cybersecurity? Guidelines

•We did not mainly focus on the percentages of institutions that have adopted particular technologies since **the key factor for cybersecurity is the human one.** Indeed this is the determining element for the development of a truly effective cybersecurity strategy
• **We chose the municipalities because they are one of the most important components of Public Administration**, the most widespread one, and the first interface with citizens. On this basis, the natural collaborator was ANCI/ANCILAB
• The assessment of a cybersecurity level involves two components: one subjective in which a knowledge is tested, and another one objective that involves an IT infrastructure and its management

Subjective component

• The IT security of a municipality involves three types of figures: personnel politician/manager (governance group G), administrative staff who must also carry out IT tasks (basic IT skills) (Group basic technician T), technical personnel (including external) specialized in IT tasks (advanced IT skills) (TA Advanced Technical Group). Based on this division, three focus groups were organized
• For each focus group, a set of questions was identified. The participants were asked to respond using three Post-it notes.
• Based on the experience of the focus groups, an online survey was prepared and addressed via ANCILAB to all municipalities in Lombardy. The questions asked were the same as those in the focus groups, and the possible answers were chosen from the keywords proposed by the participants during the focus groups.
• **Cyber security involves three areas of expertise: IT technical (T), legal (J), and managerial (A).** For each of the three topics, experts were selected: we submitted to them the same questionnaire that was submitted to the municipal staff.
• **The answers were evaluated considering the coherence of the answers provided by municipal staff with those of experts.** Furthermore, a group of people without specific skills in each of the three areas of competence was selected: in this way, it can be evaluated if there is a gain in the competence of municipal staff with respect to the answers provided in the absence of specific skills

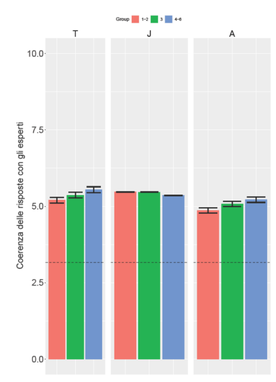
Objective component

• The following tests were considered: **a vulnerability assessment** and a **phishing campaign.**
• The vulnerability assessment is a procedure through which one can simulate an attacker who tries to detect a vulnerability in a system to compromise its functioning. There are several ways to carry out this test. In our case, **we adopted the black-box mode, which simulates the behavior of an attacker who hasn't any prior knowledge about the site that is going to attack**
• Besides the vulnerability assessment, a **phishing campaign was conducted** aimed at testing the awareness of workers for this type of attack

Results

• SUBJECTIVE COMPONENT: **There is sufficient knowledge of cybersecurity in the municipalities. However, specific knowledge, especially in small municipalities, is lacking.** The privileged interlocutors of common information security issues are not clear.
• OBJECTIVE COMPONENT: **Municipalities were able to install directly or indirectly robust websites. Less robust phishing has been detected, especially in large municipalities, where communication between employees from different sectors is more difficult. However, this fact should not be surprising: it is the situation in which any public or private body sufferers today**
• The general picture that emerges is that there is awareness of the cybersecurity problem in municipalities, but it also comes out that they do not have the necessary tools to be able to deal with it
• **Training is the most critical problem emerging from our world analysis: the municipalities have done this task themselves, but now that the challenges and problems have become so big, such an effort is no longer enough. The municipalities are aware of such issues, and they are available to remedy it, but the interlocutor seems to be missing**

An example of an answer evaluation

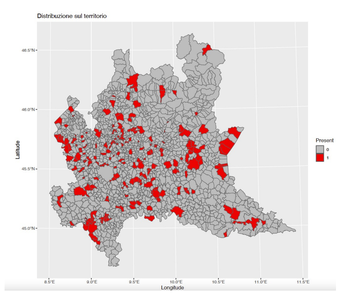


The histogram shows the score obtained in the three areas of competence (T technical, J legal, A administrative) for small (red), medium (green) and large (blue) municipalities. This score was calculated according to consistency with the answers to the same questions provided by a group of experts. The dotted line shows the score of a group of people without specific expertise in the subject.

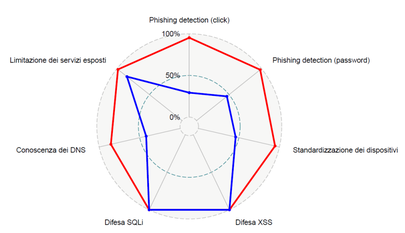
Full Report

Laser Group

On-line survey



Vulnerability assessment



Performances of municipalities (red line with a population < 10k, blue line >10k), concerning the following test: phishing detection (click), phishing detection (password), device standardization, XSS defence, SQLi defence, DNS awareness, service exposure.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
MUSA
Missione 4 - Istruzione e ricerca