Metodologia per la valutazione della cybersecurity della pubblica amministrazione: un'applicazione ai comuni lombardi

Danilo Bruschi[1], Silvana Castano[1], Alfio Ferrara[1], Onelia Rivolta[2], Nicla Ivana Diomede[3], De Corato Marzio[1], 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

Valutazione del livello di maturità dei Comuni rispetto a tre temi emergenti nel mondo digitale: cybersecurity, adozione di tecniche di intelligenza artificiale, utilizzo di big data/tecniche di analisi dei dati. Il progetto nel primo anno è stato dedicato alla cybersecurity poiché questa è il fattore abilitante per gli altri due temi.

Come valutare la cybersecurity ? Linee guida

- Non ci siamo soffermati sulle percentuali di istituzioni che hanno adottato particolari tecnologie, poiché il fattore chiave per la cybersecurity è quello umano. Questo infatti è l'elemento determinante per lo sviluppo di una strategia di cybersecurity davvero efficace.
- Abbiamo scelto i Comuni perché sono una delle componenti più importanti della Pubblica Amministrazione, quella più diffusa e la prima interfaccia con i cittadini. Di conseguenza il collaboratore naturale è stato ANCI/ANCILAB
- La valutazione del livello di sicurezza informatica coinvolge due componenti: una soggettiva in cui viene testata una conoscenza, e un'altra oggettiva che coinvolge l'infrastruttura IT e la sua gestione

Componente soggettiva

- La sicurezza informatica di un Comune coinvolge tre tipologie di figure: personale politico/manager (gruppo di governo G), personale amministrativo che deve svolgere anche compiti informatici (competenze informatiche di base - Gruppo tecnico di base T) e il personale tecnico (anche esterno) specializzato in compiti IT (competenze informatiche avanzate - TA gruppo tecnico avanzato). Sulla base di questa suddivisione sono stati organizzati tre focus group
- Per ciascun focus group è stato individuato un set di domande. Ai partecipanti è stato chiesto di rispondere utilizzando tre post-it.
- Sulla base dell'esperienza dei focus group è stata predisposta un'indagine online indirizzata tramite ANCILAB a tutti i comuni della Lombardia. Le domande poste erano le stesse dei focus group e le possibili risposte sono state scelte tra le parole chiave proposte dai partecipanti durante i focus group.
- La sicurezza informatica coinvolge tre aree di competenza: tecnica informatica (T), legale (J) e manageriale (A). Per ognuno dei tre temi sono stati selezionati degli esperti: a questi abbiamo sottoposto lo stesso questionario utilizzato per il personale dei comuni.
- Le risposte sono state valutate considerando la coerenza con quelle degli esperti. Inoltre è stato selezionato un gruppo di persone senza competenze specifiche in ciascuna delle tre aree di competenza: in questo modo, si è potuto valutare se vi è un guadagno di competenza del personale comunale rispetto alle risposte fornite in assenza di specifiche competenze

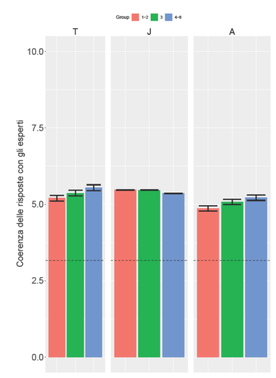
Componente Oggettiva

- Sono stati considerati i seguenti test: un vulnerability assessment e una campagna di phishing.
- Il vulnerability assessment è una procedura attraverso la quale è possibile simulare un utente malintenzionato che tenta di rilevare una vulnerabilità in un sistema per comprometterne il funzionamento. Esistono diversi modi per eseguire questo test. Nel nostro caso abbiamo adottato la modalità black-box, questo simula il comportamento di un attacker che non ha alcuna conoscenza preliminare del sito che sta per attaccare
- Oltre alla valutazione della vulnerabilità, è stata condotta una campagna di phishing volta a testare la consapevolezza dei lavoratori per questo tipo di attacco

Risultati

- COMPONENTE SOGGETTIVA: nei comuni esiste una conoscenza sufficiente della sicurezza informatica. Mancano però conoscenze specifiche, soprattutto nei piccoli comuni. Non sono chiari gli interlocutori istituzionali per i comuni circa le questioni di sicurezza informatica.
- COMPONENTE OGGETTIVA: i comuni sono stati in grado di installare direttamente o indirettamente siti web robusti. È stato rilevato un phishing meno robusto, soprattutto nei grandi comuni, dove la comunicazione tra dipendenti di diversi settori è più difficile. Questo fatto, però, non deve stupire: si tratta della la situazione in cui si trova oggi qualunque ente pubblico o privato
- Il quadro generale che emerge è che c'è consapevolezza del problema della sicurezza informatica nei comuni, ma emerge anche che non hanno gli strumenti necessari per poterlo affrontare
- La formazione è il problema più critico che emerge dalla nostra analisi: i comuni hanno svolto questo compito da soli, ma ora che le sfide ei problemi sono diventati così grandi, tale sforzo non è più sufficiente. I Comuni sono consapevoli di questi problemi e sono disponibili a porvi rimedio, ma sembra che manchi l'interlocutore

An example of an answer evaluation

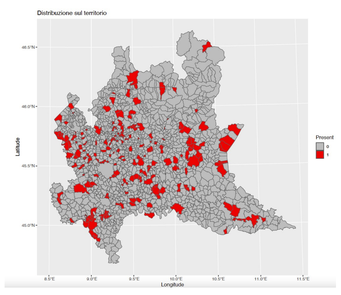


L'istogramma mostra il punteggio ottenuto nelle tre aree di competenza (T tecnica, J giuridica, A amministrativa) per i comuni piccoli (rosso), medi (verde) e grandi (blu). Il punteggio è stato calcolato in base alla coerenza delle risposte del personale dei comuni con le risposte date da un gruppo di esperti. La linea tratteggiata mostra il punteggio di un gruppo di persone senza competenze specifiche in materia.

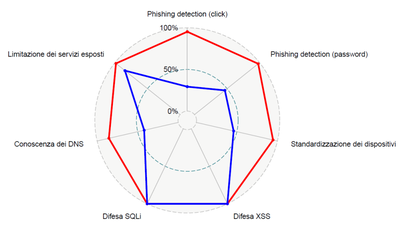
Full Report

Laser Group

Sondaggio on – line



Vulnerability assessment



Prestazioni dei comuni (linea rossa con popolazione < 10k, linea blu >10k), riguardanti i seguenti test: rilevamento del phishing (click), rilevamento del phishing (password), standardizzazione dei dispositivi, difesa XSS, difesa SQLi, DNS awareness, esposizione del servizio.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
MUSA