



# UNIVERSITÀ DEGLI STUDI DI MILANO

## Cybersecurity: la situazione dei comuni lombardi è incoraggiante ma non rassicurante

*Negli enti locali c'è una diffusa consapevolezza dell'importanza della cybersecurity, ma è necessario supportare i comuni per aumentare il livello di sicurezza informatica con nuove strategie di protezione dati. È quanto emerge dalla ricerca coordinata dall'Università degli Studi di Milano, in collaborazione con AnciLab, all'interno del progetto PNRR Musa. Tra le verifiche sperimentali effettuate, simulazioni di attacchi web e attacchi di social engineering ai siti web dei Comuni: nessun sito ha manifestato criticità tali da poterne compromettere il corretto funzionamento, ma le campagne di phishing rimangono un punto di attenzione.*

Milano, 13 febbraio 2024 - **La cybersicurezza dei comuni lombardi è incoraggiante ma non priva di rischi.** La consapevolezza della sua importanza è diffusa, ma occorre supportare gli enti locali affinché compiano un necessario salto qualitativo, anche nei confronti degli attacchi più comuni che colpiscono e mietono vittime tanto nel settore pubblico quanto in quello privato. È questo il frutto della ricerca coordinata da **Danilo Bruschi**, direttore del Dipartimento di Informatica dell'**Università degli Studi di Milano**, all'interno delle attività del [MEIEC - Milan Economic Impact Evaluation Center](#) dell'Ateneo milanese, in collaborazione con **AnciLab**, società coordinata da ANCI Lombardia per rispondere alle esigenze di sviluppo e innovazione della Pubblica Amministrazione locale. **Lo studio "La Cybersecurity negli enti locali"**, presentato oggi presso la Sala Napoleonica della Statale di Milano, nasce all'interno dello Spoke n. 4 del progetto del PNRR [MUSA - Multilayered Urban Sustainability Action](#), imperniato sulle analisi di impatto economico e finanza sostenibile.

*"La presentazione dei dati di oggi", ha dichiarato **Carlo Fiorio**, direttore del Dipartimento di Economia, Management e Metodi Quantitativi dell'Università degli Studi di Milano e del centro [MEIEC](#) "inaugura gli studi del MEIEC, finanziato con fondi del PNRR del progetto MUSA, che hanno l'obiettivo di convogliare e diffondere la cultura dell'analisi d'impatto nelle istituzioni, nelle aziende e nel Paese, affinché i decisori possano fare scelte più consapevoli".*

Grande importanza è stata data alle **persone che operano negli enti locali**, fondamentali per poter sviluppare una strategia di cybersecurity efficace. Più precisamente, **si è analizzato quali fossero le conoscenze presenti negli enti locali sul tema cybersecurity e quale fosse il livello di preparazione nell'affrontare le sfide imminenti della digitalizzazione dei processi e del passaggio al cloud.**

A seguito di tre distinti **focus group**, mirati a valutare il livello di consapevolezza e preparazione sul tema della cybersecurity nei comuni tra il personale politico e manageriale, il personale tecnico amministrativo con mansioni informatiche e i tecnici informatici dedicati, è stato realizzato un questionario al quale hanno contribuito complessivamente più di **200 rispondenti**. Le risposte sono state in seguito validate tramite un confronto con quelle fornite da 15 esperti del settore. Elemento caratterizzante dell'indagine è stato il fatto che, una volta ottenuti i risultati ed aver proceduto alla loro analisi, ne sia stata appurata sperimentalmente la loro validità, **testando direttamente i siti web dei comuni attraverso una simulazione di attacchi web e attacchi di social engineering condotti dai ricercatori al fine di verificarne la robustezza.**



# UNIVERSITÀ DEGLI STUDI DI MILANO

Ecco i principali risultati della ricerca:

- **la consapevolezza del problema cybersecurity è molto diffusa tra i comuni**, anche tra quelli di piccole dimensioni;
- la tipologia di competenze più diffusa è quella che privilegia gli aspetti tecnici della disciplina ed è una **conoscenza tipicamente "fai da te"**;
- **emergono deficit di formazione e competenze soprattutto nei comuni di piccole dimensioni** e principalmente in relazione a temi fortemente innovativi come il cloud;
- per contro i **comuni di più grandi dimensioni mostrano una maggiore fragilità** rispetto agli attacchi di social engineering;
- **nessuno dei siti web dei comuni** che si è sottoposto al vulnerability assessment condotto dal Laboratorio Sicurezza e Reti del Dipartimento di Informatica dell'Università degli Studi di Milano **ha manifestato criticità tali da poterne compromettere il corretto funzionamento**, confermando il dato ottenuto analiticamente rispetto al livello di consapevolezza sul problema e in contrasto con un "sentire" diffuso;
- **la simulazione di campagne di phishing**, sempre condotte dal Laboratorio di Sicurezza e Reti della Statale di Milano, **hanno invece messo in evidenza diverse criticità**, ma non si tratta certo di una peculiarità dei comuni testati visto che di fatto stiamo parlando del principale vettore di attacchi informatici usato in questi ultimi anni e che ha mietuto vittime illustri sia in ambito pubblico che privato.

*“Il quadro che emerge dall'indagine è dunque incoraggiante ma non rassicurante”* ha dichiarato **Danilo Bruschi**. *“Incoraggiante perché è evidente l'impegno dei comuni ad affrontare la tematica in tutti i suoi aspetti. Non rassicurante perché il gap di conoscenze non è trascurabile e da soli non possono farcela”*.

*“Comuni, cybersecurity e utilizzo dell'Intelligenza Artificiale. È molto interessante il tema del convegno di oggi, anche e soprattutto alla luce del lavoro che stiamo svolgendo in Regione Lombardia”,* ha spiegato **Alessandro Fermi, assessore all'Università, Ricerca, Innovazione di Regione Lombardia**. *“La sicurezza informatica è sempre più cruciale per tutti e anche gli Enti locali non sono immuni da rischi. È importante dunque sapere quali sono i limiti entro i quali ci si può muovere e i rischi che si corrono. È per me dunque di cruciale importanza l'indagine del Dipartimento di Informatica dell'Università degli Studi di Milano in collaborazione con AnciLab, svolta su più di 200 Comuni lombardi, che ha indagato le competenze di cybersecurity presenti. Lo dico soprattutto perché ho recentemente comunicato alla Giunta l'avvio di una iniziativa di governance dedicata all'intelligenza artificiale, un'iniziativa denominata “LombardIA”, e uno degli obiettivi di questo tavolo di lavoro sarà proprio quello di fornire un aiuto agli Enti locali. Il lavoro svolto dalla Statale di Milano, in collaborazione con AnciLab, dunque, rappresenta un esempio virtuoso di come la ricerca e il mondo degli enti locali possano concretamente contribuire alla sicurezza informatica delle nostre amministrazioni. Le attività si realizzano nell'ambito del progetto Musa, che vede coinvolte tutte le università milanesi ed è un'iniziativa che la Regione Lombardia sostiene con convinzione”*.



## UNIVERSITÀ DEGLI STUDI DI MILANO

*“Non si può immaginare la digitalizzazione degli enti locali senza prestare la dovuta attenzione alla cybersicurezza, presupposto indispensabile per l’affidabilità verso i cittadini. Impegnarsi in questo campo vuol dire puntare su formazione e consapevolezza, processi tecnologici e organizzativi, ambiti in cui l’ACN sta portando avanti una molteplicità di iniziative a favore delle amministrazioni centrali e locali, anche attraverso le risorse messe a disposizione dal PNRR”, Gianluca Ignagni, Capo di Gabinetto dell’Agenzia per la cybersicurezza nazionale.*

*“In un mondo sempre più connesso, la sicurezza informatica nella Pubblica Amministrazione non è più un’opzione, ma una necessità”, ha spiegato **Giovanna Iannantuoni, presidente di MUSA**. Anche per questo, come Musa, abbiamo voluto accendere un faro anche su questo tema, che chiama in causa una serie di questioni delicate, dalla protezione dei dati a quella delle infrastrutture. Temi, questi, che oggi non sono solo una questione tecnica ma diventano un imperativo etico, che chiama in causa la fiducia dei cittadini nei confronti delle istituzioni. I risultati dell’indagine presentata oggi, se da un lato mostrano l’importanza cruciale del fattore umano nella costruzione di una strategia di cybersecurity robusta e la consapevolezza dell’importanza di una cultura della sicurezza digitale, dall’altro evidenziano significative lacune di formazione e competenza, soprattutto nei comuni di piccole dimensioni. In questo contesto, dunque, diventa sempre più urgente la presa di coscienza della necessità di un impegno collettivo per elevare la cultura della sicurezza informatica a tutti i livelli della Pubblica Amministrazione. Impegno che veda tutti, esperti del settore e istituzioni a vario livello, unire le forze per costruire un sistema pubblico capace di resistere alle minacce informatiche e di proteggere i diritti e le libertà delle cittadine e dei cittadini”.*

*L’amministratore Unico di AnciLab, **Alessio Zanzottera**, che ha portato i saluti del Presidente di Anci Lombardia Mauro Guerra, ha sottolineato la necessità di preparare e supportare i Comuni attraverso la diffusione della cultura sicurezza informatica: “Perché la PA non sia vulnerabile, l’approccio alla sicurezza informatica non deve essere quello dell’adempimento. I dati dei Comuni sono un patrimonio importante e bisogna lavorare perché non accadano incidenti che possono creare danni a servizi e cittadini. I Comuni nei prossimi mesi dovranno guardare al digitale e all’intelligenza artificiale consapevoli delle opportunità e delle criticità che si possono presentare. La stagione del PNRR ha certamente dato una spinta importante al tema della digitalizzazione dei Comuni, ma è necessario che questo balzo in avanti sia accompagnato da percorsi adeguati di formazione che offrano al personale dei Comuni competenze adeguate”.*

Ufficio Stampa Università Statale di Milano

Chiara Vimercati, cell. 331.6599310

Glenda Mereghetti, cell. 334.6217253

Federica Baroni, tel. 02.5031.2567

[ufficiostampa@unimi.it](mailto:ufficiostampa@unimi.it)