leganet

Cybersicurezza negli Enti locali

Un approfondimento di Leganet - Dati tratti dal Rapporto CLUSIT 2025

www.leganet.net

leganet

Introduzione

La cybersicurezza rappresenta oggi uno dei fattori più critici per la resilienza delle pubbliche amministrazioni italiane. La digitalizzazione crescente, l'integrazione dei servizi, la diffusione delle piattaforme cloud e l'uso sempre più capillare delle tecnologie digitali nei processi amministrativi hanno ampliato notevolmente la superficie di attacco.

Nel contesto degli enti locali – Comuni, Unioni, Province, Città metropolitane – questa vulnerabilità assume una connotazione particolare. Si tratta infatti di amministrazioni caratterizzate da risorse economiche e competenze tecniche spesso limitate, ma al tempo stesso depositarie di dati sensibili, servizi essenziali e funzioni critiche per la sicurezza e il benessere delle comunità.

L'analisi dei dati emersi dall'ultimo aggiornamento del Rapporto CLUSIT e dalle analisi elaborate da Leganet evidenzia con chiarezza l'urgenza di rafforzare la postura cyber degli enti locali italiani.

1. Il contesto globale: l'accelerazione della minaccia cyber

La prima metà del 2025 ha segnato un'ulteriore e significativa intensificazione degli attacchi informatici: **2.755 incidenti gravi a livello mondiale**, con un aumento del **36% rispetto al 2024**. Non si tratta più di episodi isolati o di attacchi opportunistici: il panorama delle minacce è oggi dominato da gruppi organizzati, spesso internazionali, talvolta collegati a Stati stranieri o strutture paramilitari digitali.

Le tecniche utilizzate sono sempre più sofisticate e sfruttano vulnerabilità note ma non sanate, configurazioni errate, scarsa manutenzione dei sistemi ICT e, soprattutto, l'elemento umano. Parallelamente, la diffusione dell'**AI generativa** ha potenziato la capacità dei cybercriminali, rendendo più credibili le campagne di phishing, più efficaci gli attacchi automatizzati e più veloci i processi di compromissione.

Il settore pubblico è ormai da anni uno dei principali bersagli di questa escalation. La combinazione di valore informativo, importanza strategica e debolezza strutturale dei sistemi rende le amministrazioni pubbliche un obiettivo tanto appetibile quanto vulnerabile.

2. Italia: un Paese sotto pressione

I dati del 2025 mostrano un quadro preoccupante: l'Italia rappresenta **oltre il 10% degli attacchi gravi registrati nel mondo**, collocandosi tra i Paesi più colpiti in proporzione alla popolazione e alla dimensione del sistema economico.

Solo nel primo semestre dell'anno si contano **280 attacchi gravi**, pari ai tre quarti del totale registrato in tutto il 2024. Dal 2020, gli episodi censiti ammontano a **1.269**. Uno dei fattori strutturali che amplificano la vulnerabilità italiana è la carenza di **dati aggiornati e storici digitali completi**. La mancanza di log, di reportistica standardizzata e di monitoraggio continuo impedisce di individuare pattern, anticipare vulnerabilità e valutare correttamente il rischio. Questo deficit non è solo tecnologico, ma di **governance complessiva**: molte PA non dispongono di procedure formalizzate, ruoli chiave, processi di revisione e gestione del rischio, né di strumenti per la classificazione e protezione dei dati.

3. Settore pubblico: il bersaglio privilegiato

Il settore Government / Military / Law Enforcement si conferma tra i più attaccati al mondo, secondo solo ai multiple target. Nel caso italiano, nel primo semestre 2025 il comparto governativo e delle forze dell'ordine ha registrato il 38% degli attacchi totali, con un incremento impressionante del 600% rispetto al 2024.

Le ragioni sono molteplici:

- forte valore simbolico degli obiettivi pubblici;

- impatto mediatico immediato;
- possibilità di bloccare servizi essenziali;
- ricadute politiche e istituzionali;
- minore maturità cyber rispetto a grandi aziende o infrastrutture critiche.

Gli enti locali, pur meno esposti mediaticamente rispetto ai ministeri o alle agenzie nazionali, costituiscono un target ideale per gli attaccanti: detengono dati sensibili (anagrafi, tributi, servizi sociali), funzionano spesso con sistemi datati, e sono meno protetti rispetto alle strutture centrali dello Stato.

4. Il problema della governance digitale negli enti locali

La governance della cybersicurezza negli enti locali mostra criticità diffuse:

1. **Assenza di figure apicali dedicate** (CISO, DPO con competenze cyber).
2. **Mancanza di piani strategici pluriennali**.
3. **Inadeguatezza dei sistemi di monitoraggio continuo**.
4. **Competenze interne limitate**, con personale spesso sovraccarico.
5. **Insufficienza dei log e degli storici informativi**.
6. **Dipendenza da fornitori esterni** senza adeguati SLA cyber.
7. **Documentazione frammentata** e procedure non standardizzate.

Questi fattori generano una situazione paradossale: gli enti locali sono tra i principali responsabili della sicurezza dei cittadini (servizi anagrafici, reti locali, pagamento tributi), ma risultano tra i più esposti agli attacchi.

leganet

5. L'urgenza di un nuovo modello di difesa per le PA

Gli attaccanti dispongono oggi di:

- strumenti automatizzati;
- malware-as-a-service;
- intelligenza artificiale generativa;
- reti di bot globali;
- tecniche avanzate di social engineering.

Le PA locali, invece, continuano a soffrire per:

- sistemi obsoleti;
- cybersecurity considerata voce di spesa accessoria;
- difficoltà nel reclutamento di figure specializzate;
- limitata cooperazione interistituzionale;
- scarsa cultura della sicurezza digitale tra dipendenti e cittadini.

La **sfida strategica** è dunque duplice: da un lato, **il potenziamento immediato delle difese digitali**, con investimenti in infrastrutture, monitoraggio, segmentazione delle reti; dall'altro **la costruzione di una cultura cyber diffusa**, che includa dirigenti, tecnici, personale amministrativo e comunità locale.

Conclusioni: la cybersecurity come asse della resilienza territoriale

I dati del Rapporto CLUSIT e l'analisi condotta da Leganet convergono in una diagnosi chiara: la cybersicurezza non è più una variabile tecnica, ma un elemento centrale della governance territoriale.

Per gli enti locali italiani si apre una fase decisiva:

- o la sicurezza digitale viene integrata stabilmente nella gestione amministrativa, nella pianificazione degli investimenti e nella formazione del personale,
- oppure i Comuni continueranno a essere una delle aree più fragili dell'ecosistema pubblico italiano.

La protezione dei dati, dei servizi e delle infrastrutture locali è oggi una condizione essenziale per la qualità della democrazia, la tutela dei cittadini e la continuità dei servizi pubblici.