Comune di Rho

Assessorato
Lavori pubblici edifici, Protezione civile,
Innovazione e Smart city, Illuminazione pubblica

Emiliana Brognoli
Assessore

Class. 2 – 3
Fasc. 2

Ai Consiglieri comunali Sigg.ri
Christian Colombo
Stefano Giussani

Rho, 11 marzo 2022

Oggetto: risposta all'interrogazione sulla sicurezza informatica del Comune di Rho.

Con riferimento alla Vostra interrogazione da trattare in Consiglio comunale, prot. n. 3083 del 18/01/2022, successivamente trasformata in interrogazione "con risposta scritta" in data 25/02/2022, si forniscono le seguenti informazioni.

La sicurezza informatica è un valore da perseguire nel tempo con la massima attenzione e, dunque, è un processo che richiede una costante attenzione e continue implementazioni per rimanere al passo dei rischi in continua evoluzione che minacciano i nostri sistemi.

Nel ripristinare la funzionalità del sistema informativo dopo l'attacco informatico subìto il 1° aprile 2021, è stato completamente rifatto il dominio e l'infrastruttura informatica del Comune, e già nella gestione dell'emergenza è stato incrementato il livello di protezione del sistema informatico così da proteggerlo da possibili ulteriori attacchi …. *Omissis* …. *

È evidente che uno dei canali principali di accesso degli hacker è costituito dall'account degli utenti. Si è dunque investito per introdurre delle tecniche di "strong authentication" o **autenticazione a due o più fattori**, perché un'autenticazione basata solo su password è intrinsecamente più debole. Le più comuni forme di autenticazione a due fattori usano "una cosa che conosci" (una password o un pin) come primo dei due elementi, mentre come secondo viene utilizzato o "una cosa che hai" (un oggetto fisico, un PC, un telefono, un token…) o "una cosa che sei" (una caratteristica biometrica come una impronta digitale).

Previa analisi delle diverse soluzioni offerte dal mercato è stato scelto un sistema di autenticazione a due fattori come misura di implementazione del sistema di sicurezza informatica con utilizzo di smart card. In un'ottica di razionalizzazione, sia organizzativa che economica, **nella smart card sono state implementate anche le funzioni di firma elettronica (per i dipendenti dotati di firma per le attività di servizio) e di timbratura del cartellino.**

Ogni dipendente ha ricevuto nello scorso mese di dicembre una smart card che dovrà utilizzare per timbrare, per firmare e per accedere al PC e a tutte le procedure unitamente a una password. **Le prime due funzioni sono già attive, l'autenticazione a due fattori è stata avviata ed è allo stato in fase di sperimentazione e messa a punto.**

Una ulteriore azione che sarà sviluppata è quella di proseguire con il passaggio in cloud delle diverse procedure in uso agli uffici per il quale sono previste apposite risorse nell'ambito dei finanziamenti del PNRR a cui il Comune mira ad accedere. Il cloud per la Pubblica Amministrazione, oltre ad essere una

direzione già tracciata nella Strategia per la crescita digitale del Paese e nel Piano Triennale per l'informatica nella PA - per una serie di vantaggi che contribuiscono a migliorare l'efficienza operativa dei sistemi ICT, a conseguire significative riduzioni di costi, a rendere più semplice ed economico l'aggiornamento dei software e a velocizzare l'erogazione dei servizi a cittadini e imprese - consente di migliorare la sicurezza informatica e la protezione dei dati personali.

Un altro aspetto fondamentale su cui si è investito è la **formazione del personale**, in materia di sicurezza e più in generale per l'utilizzo degli strumenti informatici, promuovendo anche la conoscenza del disciplinare dell'uso degli strumenti informatici già approvato dall'Amministrazione comunale. Oltre a una formazione specifica fatta per i due operatori del CED … *omissis* … *

Dal 1° febbraio 2022, inoltre, è stata avviata una **formazione sullo sviluppo delle competenze digitali dei dipendenti**, realizzata da FPA Digital School, specifica per i dipendenti pubblici.
Il percorso di formazione è on line su una specifica piattaforma dedicata ed è articolato in 11 corsi, per un totale di 128 ore di autoapprendimento, nelle materie previste dal *Syllabus "Competenze digitali per la PA"* del Dipartimento della Funzione Pubblica, che descrive il set minimo di conoscenze e abilità che ogni dipendente pubblico, non specialista IT, dovrebbe possedere nelle seguenti 5 aree di competenza del livello Base:

1. dati, informazioni e documenti informatici,
2. comunicazione e condivisione,
3. sicurezza,
4. servizi on-line,
5. trasformazione digitale.

Relativamente all'attacco informatico subito, in data 3 Aprile, è stata inviata al Garante della protezione dei dati personali una notifica preliminare di una possibile violazione di dati personali (nota come Databreach), successivamente integrata con una serie di informazioni e note tecniche sull'attacco e sulle sue conseguenze.

Nel mese di luglio 2021 il Garante privacy ha archiviato il procedimento di databreach che era stato aperto, non ravvisando responsabilità a carico del Comune di Rho e dando atto delle misure di sicurezza già attuate e di quelle già programmate dal Comune.

Successivamente all'attacco informatico, è stata presentata in data 27/04/2021 formale querela al Compartimento Polizia di Stato e delle Comunicazioni di Milano, per il tramite del Commissariato di Rho-Pero, nei confronti di tutti i soggetti responsabili per i reati che saranno ravvisati in relazione all'attacco subìto, chiedendone la punizione ai sensi di legge con riserva di costituzione di parte civile. Si è chiesto altresì, ai sensi dell'art. 408 cpp, di essere informati in caso di richiesta di archiviazione della querela.

Il Comune non ha ancora ricevuto in proposito alcuna notizia.

Cordiali saluti.

L'assessore
alla Innovazione e Smart city
Emiliana Brognoli

*Alcune parti della risposta sono state omesse per ragioni di tutela della sicurezza.