

Ferrara 28/03/2024

Al consigliere comunale Davide Nanni

Gruppo consigliere PD

e, p.c. Al Sindaco, al Vicesindaco

Ufficio Consiglio (Paola Marzola)

Ufficio Assistenza agli Organi

Al Segretario Generale

Ufficio di Presidenza del

Consiglio Comunale

Alla Segreteria del Sindaco

Al Direttore Generale

All'Ufficio Stampa

Gentile consigliere,

In merito alla Sua interpellanza PG 134380/23 si è risposto tardivamente in quanto si è attesa la conclusione del processo di segnalazione al Garante, che per la sua complessità ha richiesto un lavoro di parecchi mesi.

Il processo di segnalazione si è concluso lo scorso 15 marzo ed ora siamo in grado di fornire in maniera completa le informazioni richieste. Parte di esse sono descritte in maniera esaustiva nella segnalazione conclusiva all'Autorità Garante.

**DOMANDA:** quanti e quali siano i Database a cui hanno avuto accesso gli hacker, contenenti dati personali di particolare sensibilità (ad es.: dati anagrafici e fiscali, multe, pratiche edilizia, dichiarazioni anticipate di trattamento, etc.);

**RISPOSTA:** i Settori interessati sono stati: Polizia Locale, Servizi alla Persona, Affari Istituzionali, OO.PP. Patrimonio, Cultura e Turismo, Governo del Territorio, Programmazione Finanziaria e del Personale. Per i dati di dettaglio si rimanda alla segnalazione conclusiva all'Autorità Garante.

**DOMANDA:** quante caselle di posta elettronica di dipendenti e amministratori comunali sono state scaricate illegalmente e rese note, con violazione della privacy di utenti anche esterni all'amministrazione;

**RISPOSTA:** il sistema di posta elettronica, come del resto tutti gli ambienti applicativi in cloud, non è stato coinvolto nell'attacco che ha riguardato solo l'infrastruttura interna

**DOMANDA:** quali iniziative sono state intraprese o si intendono promuovere per tutelare la privacy dei dipendenti comunali e dei cittadini ferraresi danneggiati dall'attacco informatico subito dal Comune di Ferrara;

**RISPOSTA:** dal punto di vista giuridico-normativo sono state intraprese tutte le misure previste dal regolamento europeo GDPR, in particolare le informative personali e generali in relazione alla tipologia dei dati pubblicati. Dal punto di vista tecnico si è proceduto ad una serie di misure, tuttora in corso, per il drastico irrobustimento della postura di sicurezza dell'Ente. Per le informazioni di dettaglio si rimanda alla segnalazione conclusiva all'Autorità Garante.

**DOMANDA:** se le verifiche interne, condotte da esperti informatici, abbiano già individuato o meno la vulnerabilità e la postazione specifica che ha consentito agli hacker l'accesso al sistema

**RISPOSTA:** il team di risposta all'incidente, intervenuto tempestivamente, ha condotto analisi sia durante le operazioni di contrasto che di ripristino. La necessità di garantire un'operatività delle strutture comunali ad un livello dapprima accettabile (obiettivo raggiunto in una ventina di giorni) e in seguito quasi ottimale (obiettivo raggiunto in circa due mesi) non ha consentito l'analisi di tutte le postazioni di lavoro compromesse. L'analisi forense ha stabilito come la più probabile fonte di infezione sia stata un phishing su una postazione utente, non identificata, ove fosse presente un'utente con privilegi di amministratore locale.

Tale vulnerabilità è stata sanata in fase di ricostruzione dell'ambiente di dominio Windows.

**DOMANDA:** quali siano i costi sinora sostenuti, in termini di consulenze e interventi di personale tecnico esterno, per la messa in sicurezza del sistema informatico del Comune di Ferrara;

**RISPOSTA:** i costi, da ritenersi definitivi, sono elencati nella tabella seguente. Si segnala che il Comune di Ferrara ha presentato domanda di ammissione ai finanziamenti del bando n. 8/2024 dell'Agenzia per la Cybersicurezza Nazionale finalizzato al rafforzamento della sicurezza di alcune tipologie di ente, tra cui le cosiddette "grandi città" di cui Ferrara fa parte. Se saremo ammessi potremo recuperare in parte alcune spese già sostenute.

<b>1) DANNI DIRETTI DATA BREACH</b>				
		costo netto	costo I.C.	det 2023
<b>SERVIZI</b>				
prestazioni da VEM-Certego	Response e attività post incidente	24.780,00	30.231,60	
licenze Carbon Black	licenze temporanee (fino 15/10) prodotti di sicurezza	11.230,00	13.700,60	det. 1819
ulteriori prestazioni da VEM	Attività post incidente	14.000,00	17.080,00	det. 2701
licenze temporanee 888 (OO.PP.)	programma Matrix gestione opere pubbliche. Licenze per installazioni di emergenza su PC dei tecnici	7.400,00	9.028,00	det. 1612
manodopera da Eurosystem	35 giornate di assistenza tecnica	12.250,00	14.945,00	det. 1657
manodopera da Sistemi e Progetti	7 giornate di assistenza tecnica	2.800,00	3.416,00	det. 1798
manodopera da Lepida	40 giornate di assistenza tecnica	10.400,00	10.400,00	det. 1663
servizi Yarix	servizi specializzati per gara decifrazione	6.500,00	7.930,00	det. 1698
Manodopera Ferrara Tua	Rimborso a Ferrara Tua degli straordinari del Personale in convenzione in servizio presso Servizio Sistemi Informativi	5.693,67	5.693,67	
		<b>95.053,67</b>	<b>112.424,87</b>	
<b>NON QUANTIFICABILE</b>	MANODOPERA INTERNA (luglio circa 400 ore di straordinari, agosto circa 440, circa 150 non saranno pagati perché svolti dalla E.Q., una consistente quantità non sarà pagata ma recuperata; non quantificato lo straordinario del Dirigente, non monetizzabile)			
GRATUITO da Unife	82 giornate di assistenza tecnica			
<b>GESTIONE PRATICA GARANTE</b>				
Elaborazione dati Deepcyber srl	Elaborazione dei dati esfiltrati per individuazione interessati	18.000,00	21.960,00	det. 2337
Studio legale e-lex di Roma	Consulenza legale specializzata per gestione pratica Garante	31.096,00	37.937,12	det. 2559/23+338/24
Stampa, radio, tv, social	Inserzioni per informative generali	1.362,00	1.661,64	
Spese postali	Spedizione delle informative individuali	7.855,74	7.855,74	
		<b>58.313,74</b>	<b>69.414,50</b>	
<b>2) ACQUISTO PC (INVESTIMENTO RIMASTO A PATRIMONIO)</b>				
58 PC portatili da Multicopia e Arredaufficio srl + accessori		41.557,50	50.700,15	det. 1560
40 PC fissi da CNA		19.800,00	24.156,00	det. 1785
		<b>61.357,50</b>	<b>74.856,15</b>	
<b>3) INCREMENTO SICUREZZA (ATTIVITÀ PREVISTE PER IL 2024, ANTICIPATE)</b>				
licenze Fortinet per accesso VPN sicuro	100 licenze perpetue con MFA	5.129,00	6.257,38	det. 1819
licenze AnyDesk per assistenza remota sicura	contratto triennale 3 accessi contemporanei	4.961,75	6.053,34	det. 2005
anticipo progetto sicurezza 2024-26	contratto triennale piattaforma Panoptikon di Certego: primo anno	138.913,10	169.473,98	det. 2057
		<b>149.003,85</b>	<b>181.784,70</b>	

DOMANDA: se sia stata inviata una relazione sull'accaduto all'Autorità Nazionale Garante della Privacy con richiesta, in caso di risposta affermativa, di prenderne visione.

RISPOSTA: sono state inviate le seguenti segnalazioni:

- Preliminare: 13/7/23
- 1° integrativa: 28/7/23
- 2° integrativa: 11/8/23
- 3° integrativa: 13/9/23
- 4° integrativa: 20/10/23
- 5° integrativa: 27/11/23
- 6° integrativa: 19/1/24
- 7° integrativa e conclusiva: 15/3/24

Nella segnalazione conclusiva sono riportate tutte le informazioni relative all'incidente. Tale segnalazione è a disposizione dei signori Consiglieri tramite un semplice accesso agli atti. Sentito a riguardo il DPO si ritiene indispensabile segnalare che tale documento contiene informazioni riservate la cui divulgazione, anche involontaria, può compromettere la sicurezza della rinnovata infrastruttura informatica del Comune di Ferrara, nonchè causare ulteriori danni agli interessati.

Tale documento è da ritenersi riservato e strettamente confidenziale e ne è vietata qualsiasi forma di riproduzione e di divulgazione. Il suo utilizzo è intendersi per esclusivo utilizzo personale del/dei Consiglieri nell'ambito dei propri compiti istituzionali.