Sispi

Palermo, 09/06/2022 prot. Registro Emergenza n. 102/2022

al Signor Direttore Generale/Segretario Generale

al Vicesegretario generale e Dirigente del Servizio Innovazione

del Comune di Palermo

Oggetto: richiesta mail dell'8.06.2022

Con riferimento alla richiesta da Lei formulata ieri sera via mail, si produce la seguente relazione che, anche ai fini di eventuali rendicontazioni da produrre per Enti di vigilanza, descrive l'incidente derivante dall'attacco ransomware subito dal Data center di Codesta Amministrazione, dando evidenza dell'attività svolta dalla scrivente dal momento della constatazione dell'attacco ad oggi nonché di ogni elemento disponibile per delineare le attività previste per il prossimo futuro fino a conclusione del primo turno del procedimento elettorale.



Lo scorso 2 giugno alle ore 6.30 del mattino il responsabile del servizio Architetture Sispi ha verificato che il Data center del Comune di Palermo aveva subito un Attacco informatico di tipo Ransomware con Potenziale Data Exfiltration (non accertata) dei dati di Titolari (Comune di Palermo e Sispi) e del responsabile (Sispi).

L'attacco ha colpito l'intera infrastruttura telematica del Data center, comprese tutte le postazioni di lavoro distribuite presso le sedi dell'Amministrazione comunale di Palermo ad essa collegate, rendendola indisponibile e determinando la totale interruzione dei servizi resi. Risulta indisponibile anche il server Veeam con il backup delle configurazioni.

Viene invece verificata sia la presenza dei backup effettuati tramite arcserve (back up su nastroteca) sia l'accessibilità dei dati su DB e storage NetApp.

Dopo la prima analisi della situazione viene dunque predisposto un primo un piano di azioni per il contenimento dell'incidente provvedendosi tempestivamente a:

- isolamento dei sistemi colpiti da malware (Infrastruttura VmWare, Server Veeam, pc sede Sispi, pc ripartizioni comunali)

**Sistema Palermo Innovazione SpA**
Sede Legale e Uffici
Via Amm. S. Denti di Piraino, 7 - 90142 Palermo
t. 091 6319811 f. 091 6371706
sispi@sispi.it - sispispa@cert.sispi.it
Cap. Soc. 5.200.000,00 I.V.
Reg. Imprese Palermo e P.I. 03711390827
**Socio Unico Comune di Palermo**

CERTIFICAZIONE SISTEMA DI GESTIONE DNV ISO 27701 - ISO 50001 ISO 22301
MANAGEMENT SYSTEM CERTIFICATION DNV ISO 9001 - ISO/IEC 27001 ISO/IEC 20000-1

- isolamento del database Oracle e degli Storage NetApp per la salvaguardia dei dati contenuti.
- verifica del corretto funzionamento degli apparati di rete.

Viene quindi costituito un Comitato di crisi aziendale, presieduto dal Direttore Generale, nel quale vengono individuate le attività da avviare senza indugio sia dal punto di vista strettamente tecnico sia necessarie a dar corso ad ogni adempimento di legge.

Così, a partire dalle ore 8.30 vengono contattati per ogni conseguente attività:

- le funzioni apicali dell'Amministrazione (Direzione Generale, Innovazione, Webmaster);
- la DIGOS, presso la quale si è provveduto, nel corso della mattina, a sporgere la denuncia dell'accesso abusivo al sistema, tempestivamente trasmessa alla Polizia Postale che ha poi svolto una prima attività di indagine in sede la mattina successiva;
- il DPO Sispi, anche per l'avvio di ogni attività di predisposizione della notifica preliminare del Data breach al Garante Privacy, che sarà inviata il successivo giorno 3 giugno;
- il DPO del Comune di Palermo per supportare l'Amministrazione nell'attività di notifica al Garante quale titolare dei dati oggetto di attacco, (anch'essa inviata il giorno 3);
- Cisco, partner tecnologico di Sispi, e Axians fornitore di sistemi di videosorveglianza specializzato in sistemi di sicurezza fisica e logica,



vengono inoltre predisposte:

- le comunicazioni riservate dell'incidente a tutti i Titolari di dati coinvolti recante una Relazione tecnica di dettaglio, predisposte anche con il supporto del DPO;
- la procedura di attivazione del registro di emergenza Sispi per il protocollo;
- le indicazioni di supporto al Responsabile della Gestione documentale dell'Amministrazione comunale per l'attivazione del Registro di emergenza per garantire continuità alle attività di protocollazione dell'Amministrazione e le stampe del registro di emergenza dell'A.C.;
- la comunicazione al Direttore Generale del Comune contenente l'indicazione dei contatti attivi e le raccomandazioni per la gestione della prima fase dell'emergenza.

Dal punto di vista tecnico

- si è richiesta a fastweb la produzione delle LOG del firewall acquisite per l'espletamento del servizio SIEM con analisi log e valutazione dell'incidente;
- esecuzione Test di integrità, con esito positivo, su storage su NetApp e Oracle;
- avvio copia backup locali di Oracle su HD esterni.

Sispi

Dopo gli ulteriori approfondimenti, ritenuta non sicura l'attivazione dell'ambiente di recovery e verificata la non percorribilità di un processo di ripartenza su cloud per via dei tempi richiesti dai gestori (Aruba, TIM...) per l'attivazione degli spazi necessari, la strategia adottata è stata quella condurre i processi di seguito sintetizzati, avvalendosi della competenza specialistica di società esperta in materia (Axians SpA):

- predisposizione di una rete chiusa accessibile solo ad utenti selezionati da postazioni fisiche collegate direttamente alla rete per ricostruire l'infrastruttura logica del Sistema;
- reinstallazione della infrastruttura di base (server virtuali) per consentire la fase di installazione dell soluzioni applicative di Sispi e dei terzi fornitori;
- reinstallazione graduale delle applicazioni tramite le quali si gestiscono i servizi resi all'Amministrazione comunale;
- bonifica di tutte le postazioni di lavoro distribuite.

Il piano d'azione così delineato è stato avviato tenendo conto della massima priorità che richiede la ormai prossima consultazione elettorale.

Per tale ragione le prime reinstallazioni sono state dedicate ai servizi demografici e, già a partire da lunedì, avvalendosi di una task force tecnica appositamente creata:



- è stata riattivata la procedura Demos
- è stata resa disponibile la procedura Sipal per la rilevazione dei dati da comunicare al Ministero degli Interni
- è stata predisposta la procedura per il cd. "insediamento ai seggi", necessaria alla raccolta dei dati relativi a presidenti e scrutatori
- è nuovamente disponibile il Protocollo informatizzato.

Le attività così intraprese proseguono seguendo lo schema sopra richiamato, senza soluzione di continuità, tenendo conto delle situazioni legate a specifiche emergenze ed a specifiche scadenze di legge. Tutto ciò seguendo le direttive architetturali ed applicative del consulente IT specializzato, in quadro di rafforzata policy di sicurezza che coinvolge anche gli utenti operatori dell'Amministrazione.

Distinti saluti

Il Direttore Generale

ing. Salvatore Morreale

distribuito p.p.e.