L'EVENTO

A partire dalle prime ore mattutine dell'8 dicembre 2023, venivano riscontrati malfunzionamenti bloccanti dell'infrastruttura cloud fornita dal Fornitore Westpole S.p.A., sui entrambi i nodi di Roma e Milano, su cui sono installati gli applicativi che consentono l'erogazione dei servizi connessi al processo di fatturazione elettronica di Gruppo Dylog e Gruppo Buffetti e per i servizi verso la Pubblica Amministrazione erogati da PA Digitale S.p.A..

L'indicazione ricevuta dal fornitore è che un'azione ransomware, condotta da un attore ostile, avrebbe cifrato le basi dati.

Il Fornitore Westpole S.p.A. rappresentava, da ultimo in tarda serata dell'11 dicembre 2023, di aver subito un attacco informatico che aveva, in sintesi, colpito tutte le macchine virtuali ospitate nei centri di Roma e Milano (circa 1.500) impedendone la funzionalità.

Westpole S.p.A., quindi, specificava:

I firewall non hanno evidenziato, né durante il periodo di esecuzione dell'attacco, né durante i giorni precedenti, alcun traffico riconducibile alla esfiltrazione di dati.

Per tutti i servizi che prevedevano l'utilizzo di una componente repository di tipo NAS, i dati non risultano essere compromessi, e, allo stato attuale delle analisi, non risultano accessi dell'utenza compromessa o di altre utenze sospette o non coerenti con il normale utilizzo di business delle applicazioni nei giorni precedenti all'attacco.

Sulla base delle evidenze riportate e disponibili allo stato attuale, da confermare e arricchire attraverso analisi forensi più approfondite, riteniamo poco probabile l'esfiltrazione dei dati da parte dell'attaccante, evidentemente interessato al blocco dell'infrastruttura, non al contenuto dei dati, di tipo indifferenziato, presenti sui nostri repository e all'interno delle circa 1.500 macchine virtuali in essa presenti.

LA GESTIONE DELL'INCIDENTE

L'incidente ha avuto un impatto significativo su numerosi clienti del Gruppo Dylog, in termini principalmente di indisponibilità delle piattaforme di fatturazione elettronica e di servizi erogati a pubbliche amministrazioni centrali e locali.

Data la dimensione degli impatti, è necessario procedere a comunicazioni pubbliche, essendo impossibile raggiungere tutti i possibili interessati dell'evento, fermo restando che sono attive linee di comunicazione esterne, che consentono di rispondere a specifici quesiti individuali degli interessati che possano non trovare soddisfazione nei comunicati

L'attività di gestione dell'incidente si svolge su diversi piani, per garantire, da un lato, il rientro della piena funzionalità dei sistemi; dall'altra per adottare tutte le azioni indispensabili per ridurre i rischi sull'ambiente operativo di esercizio ed evitare il ripetersi dell'evento.

PA Digitale S.p.A. | Via Leonardo da Vinci 13, 26854 Pieve Fissiraga (LO) | www.padigitale.it
Tel. 0371.5935.780 | Fax 0371.5935.790 | protocollo.pec.padigitalespa@legalmail.it
Soggetta a Direzione e Coordinamento di Gruppo Buffetti S.p.A.
Registro Imprese di Lodi | Codice Fiscale e Partita IVA n° 06628860964
C.C.I.A.A. di Lodi R.E.A. n° 1464686 | Capitale Sociale 4.825.382,00 Euro i.v.

1. Ripristino dell'infrastruttura Cloud

Westpole S.p.A. ha comunicato che la messa fuori linea dei propri sistemi, adottata come prima azione di contenimento, ha risposto ad una esigenza precauzionale.

La società Westpole S.p.A., quindi, ha assicurato la reinstallazione da zero dell'infrastruttura virtuale e dei sistemi operativi e questo significa che i sistemi di fatturazione elettronica e gli altri applicativi del Gruppo Dylog/Buffetti e PA Digitale S.p.A possono essere installati in un ambiente che è certamente immune da potenziali compromissioni;

2. Definizione di un modello di rilevamento e monitoraggio di sicurezza delle informazioni

Westpole S.p.A., già tenuta all'adozione delle necessarie misure di sicurezza ex art. 32 GDPR, ha comunicato di aver rafforzato il proprio presidio di controllo, avvalendosi anche del supporto di un Security Operation Center della società controllante CEGEKA Group e di tecnologie avanzate per la rilevazione dei vettori di attacco.

Sono state richieste integrazioni puntuali rispetto all'evento descritto e sulle misure di sicurezza necessarie a garantire la disponibilità, integrità e riservatezza delle informazioni.

3. Azioni delle società del Gruppo Dylog/Buffetti

Il ripristino della ricostruzione degli applicativi e delle basi dati, anche con il supporto dell'Agenzia delle Entrate e dei partner implementativi è iniziato sin dall'8 dicembre e sta proseguendo, non solo con l'ottica di ripristinare le funzionalità su ambienti Westpole S.p.A., ma anche definendo politiche di selezione alternativa di fornitori, per modo da garantire i più alti livelli di affidabilità e continuità operativa. In questo senso:

a. Sono state individuate ulteriori misure di sicurezza richieste a Westpole S.p.A. per assicurare la disponibilità, l'integrità e la riservatezza delle informazioni;
b. È stato richiesto al Fornitore un dettaglio di tutte le misure di sicurezza poste in essere;
c. È stata accelerata la migrazione dei servizi critici su piattaforma Microsoft Azure.
d. Sono state condotte specifiche analisi sui sistemi del Gruppo, che hanno escluso la propagazione di azioni malevole nei riguardi dei sistemi server e client di pertinenza delle società ascrivibili a questa vicenda.

ANALISI DELLA DISPONIBILITA' DEI DATI

Il quesito fondamentale è se siano stati irreversibilmente cifrati dati personali degli interessati.

Su questo tema, ad oggi, non è possibile fornire una risposta unitaria, poiché i dati contenuti su storage tipo NAS risultano intatti e immediatamente disponibili, mentre per altri sono in corso analisi.

Gruppo Dylog ha richiesto a Westpole S.p.A. di poter ottenere i files delle macchine virtuali che ospitavano i sistemi di interesse per poter condurre autonome analisi e fornire successivamente una risposta chiara ed esaustiva.

Le informazioni relative al servizio di conservazione sostitutiva risultano invece integre e correttamente conservate.

PA Digitale S.p.A. | Via Leonardo da Vinci 13, 26854 Pieve Fissiraga (LO) | www.padigitale.it
Tel. 0371.5935.780 | Fax 0371.5935.790 | protocollo.pec.padigitalespa@legalmail.it
Soggetta a Direzione e Coordinamento di Gruppo Buffetti S.p.A.
Registro Imprese di Lodi | Codice Fiscale e Partita IVA n° 06628860964
C.C.I.A.A. di Lodi R.E.A. n° 1464686 | Capitale Sociale 4.825.382,00 Euro i.v.

INTERVENTO DELLE AUTORITA'.

Westpole S.p.A., in quanto vittima diretta dell'incidente, ha presentato denuncia all'Autorità Giudiziaria per il tramite della Polizia di Stato, Servizio Polizia Postale e delle Comunicazioni.

Westpole S.p.A. ha inviato anche notifica preliminare di violazione della disponibilità dei dati all'Autorità Garante per la protezione dei dati personali.

Dylog Italia S.p.A., Gruppo Buffetti S.p.A. e PA Digitale S.p.A. hanno, ciascuna per il proprio ruolo ed ambito, presentato notifica preliminare di violazione della disponibilità dei dati all'Autorità Garante per la protezione dei dati personali

QUALI ALTRE INFORMAZIONI CI SI DEVE ATTENDERE?

Gruppo Dylog ha assunto un impegno di totale trasparenza e seguiranno puntuali informazioni sull'evoluzione della vicenda e sulle modalità con le quali intendiamo assistere e garantire gli interessi dei nostri clienti, in particolare a seguito delle integrazioni di informazione puntualmente richieste a Westpole S.p.A.

Pieve Fissiraga (LO), 13/12/2023

PA Digitale S.p.A

Il Legale Rappresentante

Ing. Renato Trapattoni

Amministratore Delegato

PA Digitale S.p.A. | Via Leonardo da Vinci 13, 26854 Pieve Fissiraga (LO) | www.padigitale.it
Tel. 0371.5935.780 | Fax 0371.5935.790 | protocollo.pec.padigitalespa@legalmail.it
Soggetta a Direzione e Coordinamento di Gruppo Buffetti S.p.A.
Registro Imprese di Lodi | Codice Fiscale e Partita IVA n° 06628860964
C.C.I.A.A. di Lodi R.E.A. n° 1464686 | Capitale Sociale 4.825.382,00 Euro i.v.