

Comunicato ai Clienti Dylog Buffetti

in relazione agli eventi dell'8 dicembre 2023 e giorni seguenti.

Gentile Cliente,

desideriamo riassumere in modo trasparente e puntuale quanto accaduto l'8 dicembre 2023 e descritto nei comunicati precedentemente pubblicati:

un attacco informatico di tipo ransomware ha colpito l'infrastruttura Cloud di Westpole S.p.A. a Roma e Milano, fornitore del nostro Gruppo.

Questo evento ha causato, a cascata, il blocco dei servizi di fatturazione elettronica del Gruppo Dylog e Buffetti.

Dalle informazioni in nostro possesso, l'attacco sembra essere stato mirato a bloccare l'infrastruttura senza sottrarre dati, ma ciò ha comportato notevoli disagi per i nostri Clienti.

Dell'accaduto hanno parlato anche autorevoli testate giornalistiche come Il Sole 24 Ore.

Westpole S.p.a., precedentemente nota come HITACHI Systems CBT, è oggi parte del Gruppo internazionale Cegeka, con sede in Belgio. È in possesso di tutti i requisiti e certificazioni tecnici richiesti a norma di legge e viene regolarmente sottoposta a processi di audit tecnico.

La società oggetto dell'attacco è stata selezionata sulla base di un processo di analisi delle competenze tecniche, periodicamente verificate e per le referenze, offrendo i propri servizi ad enti pubblici di primaria rilevanza, anche istituzionale e importanti società pubbliche e private nazionali. Westpole, tra l'altro, è soggetto specificamente qualificato per la fornitura dei servizi in cloud per la pubblica amministrazione dall'Agenzia per l'Italia Digitale (AgID) e, dal 19 gennaio 2023, dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Abbiamo immediatamente adottato misure precauzionali per i nostri Clienti, mettendo offline i sistemi e reinstallando l'infrastruttura virtuale. Dopo aver completato le necessarie procedure di sicurezza, la società PA Digitale S.p.a., che gestisce i servizi di fatturazione elettronica del Gruppo Dylog e Buffetti, ha convalidato con Sogei un nuovo protocollo per la connessione ai Sistemi di Interscambio, consentendoci di ripristinare i servizi gradualmente.

L'attacco ransomware a Westpole ci ha costretto a reinstallare completamente la nostra infrastruttura impegnando giorno e notte senza limiti di orario tutte le risorse disponibili dal momento della notifica.

Le attività sono ancora in corso e si protrarranno ancora nei prossimi giorni, week end compreso. Contiamo al più presto di poter riattivare tutti i servizi anche se non tutte le funzionalità saranno completamente fruibili al riavvio.

La procedura di riavvio prevede la rigenerazione delle credenziali dei portali per garantire la sicurezza dei nostri Clienti, anche se ciò sta comportando disagi nell'aggiornamento delle informazioni di accesso e tempi lunghi.

Abbiamo inviato una comunicazione formale all'Agenzia delle Entrate, una notifica al Garante della Privacy, e formali contestazioni e diffide alla società Westpole S.p.a.

Abbiamo inoltre richiesto ad Agenzia delle Entrate una deroga alle correnti scadenze fiscali per i nostri Clienti, motivata dalla sussistenza di una causa di forza maggiore per impossibilità di invio, peraltro prevista dallo Statuto del contribuente.

Ci rendiamo conto del disagio significativo causato e vogliamo esprimere il nostro più profondo rammarico per l'accaduto, seppur indipendente dalla nostra volontà.

Da subito ci siamo attivati senza limiti di orario e risorse per il ripristino più tempestivo possibile dell'operatività dei servizi e tutt'ora il nostro staff tecnico al completo sta operando senza sosta.

In conclusione, vogliamo ringraziare ancora tutti i nostri Clienti per la pazienza e la fiducia dimostrata durante questo periodo difficile.

Vogliamo ringraziare anche la preziosa collaborazione dell'Agenzia delle Entrate che si è prodigata per affrontare prontamente la questione e le Agenzie della Presidenza del Consiglio (AgID e ACN) per il supporto fornito.

Comprendiamo sinceramente i Clienti che hanno manifestato il loro dissenso e ci scusiamo nuovamente per l'inconveniente causato.