Attacco informatico – Comunicazione agli interessati ([1])

Coopservice S. Coop. p. A. (di seguito, la Società o l'Azienda) è stata vittima di un attacco informatico. L'azione malevola è stata realizzata da una pericolosa organizzazione criminale ben nota alle cronache ([2]), che si è dimostrata in grado di insidiare anche i più elevati standard di sicurezza informatica come quelli adottati dalla nostra Società ([3]). L'attacco, avendo comportato il blocco di alcune risorse del sistema informativo aziendale, ha causato dei temporanei disservizi. Alla richiesta di riscatto fatta pervenire dall'organizzazione criminale, l'Azienda non ha dato alcun seguito: al contrario, in linea con i valori cooperativi ed aziendali e con i principi contenuti nei propri codici etici e modelli di gestione, ha presentato immediata denuncia alla competente Autorità Giudiziaria ed ha attivato un contatto diretto con il Garante per la protezione dei dati personali e l'Agenzia per la Cybersicurezza Nazionale, accompagnato dalla adozione di immediate misure via via illustrate nel dettaglio a dette Autorità per il contenimento dell'azione criminale subita.

Ciò nonostante, per come ricostruito sulla base delle analisi condotte, l'attacco potrebbe aver comportato anche la estrazione di copia di documenti elettronici contenenti dati personali conservati sul sistema informativo aziendale. Con la presente comunicazione si intende quindi fornire le dovute informazioni a tutti coloro che potrebbero essere indirettamente coinvolti, anche al fine di permettere l'adozione di iniziative a propria tutela:

1. gli unici dati esposti al rischio sono quelli contenuti in file movimentati nel periodo 10.09.24/10.02.25: la presente comunicazione riguarda dunque, presumibilmente, soltanto coloro che hanno intrattenuto rapporti con l'Azienda in tale arco temporale;
2. I dati possono esser stati memorizzati sul sistema informativo aziendale per diverse ragioni legittime (es: contratto di lavoro, appalto, fornitura), ed in alcuni limitati ambiti oltre ai dati personali comuni (es: nome, cognome, data di nascita, copia per immagine di documenti di identità o del codice fiscale/tessera sanitaria), la Società conserva anche dati particolari (es: assenze per malattia di un proprio dipendente) o relativi a condanne penali e reati (es: certificato del casellario giudiziale nell'ambito della documentazione necessaria alla gestione delle gare di appalto).

Fermo quanto sopra, per proteggersi da eventuali conseguenze della violazione, consigliamo di valutare, sulla base della presente comunicazione, la presentazione di una specifica denuncia-querela relativa alla possibile sottrazione fraudolenta dei dati trattati dalla Società.

Per ogni questione attinente alla presente comunicazione, è possibile prendere contatto con l'Azienda attraverso i seguenti canali dedicati: e-mail: databreach@coopservice.it; - PEC databreach-coopservice@legalmail.it

Alla luce di quanto sopra, è nostra intenzione continuare a contrastare con tutti gli strumenti possibili gli effetti dell'azione criminale diretta in danno dell'Azienda, senza piegarsi ad alcun ricatto.

La presente comunicazione, nei medesimi termini, è resa anche dalla società Istituto di Vigilanza Coopservice Spa per la quale la Società eroga servizi informativi infragruppo (e-mail: databreach.IVC@vigilanzacoopservice.it – PEC: databreach-vigilanzacoopservice@legalmail.it).

Istituto di Vigilanza Coopservice Spa

Coopservice S. Coop. p. A.

[1] Art. 34 par. 3 lett. c) del Regolamento UE 2016/679 (di seguito, GDPR)

[2] Il gruppo criminale agisce utilizzando un cd. ransomware denominato Akira – Per ogni informazione si rinvia alle attività svolte dall'Agenzia Cybenetica Nazionale, e segnatamente all'ultimo report consultabile a questo indirizzo: https://www.acn.gov.it/portale/w/csirt-italia-pubblica-il-rapporto-di-gennaio-sullo-stato-della-minaccia-in-italia

[3] Coopservice è un'azienda certificata ISO 27001 ed oltre alla adozione delle più elevate misure di sicurezza, si avvale del supporto di primari operatori di mercato per la gestione di ogni profilo legato alla cybersicurezza (nello specifico, un Security Operation Center attivo 24 ore su 24).