I.R.C.C.S. Ospedale San Raffaele

Gruppo San Donato

Spett.le Interessato/a,

l'Ospedale San Raffaele S.r.l., titolare del trattamento, con la presente ai sensi dell'art. 34, paragrafo 3, lettera c) del Regolamento Generale sulla Protezione dei Dati (Reg. UE 16/679) comunica l'avvenuta violazione dei Suoi dati personali (data breach) che si è verificata tra il 5 giugno e il 18 giugno 2020; la comunicazione è effettuata dall'Ospedale spontaneamente al fine di fornirLe le dovute informazioni in merito ai fatti occorsi.

Nell'arco temporale sopraindicato ignoti attaccanti per mezzo di un attacco di phishing perpetrato attraverso tecniche di social engeneering, hanno avuto accesso all'account e-mail di un dipendente dell'Ospedale San Raffaele.

Descrizione della natura della violazione:

L'attacco ha avuto ad oggetto un account di Office 365 di un dirigente dell'Ospedale, circoscritto alla sola casella di posta elettronica, al cui contenuto gli hacker hanno verosimilmente potuto temporaneamente accedere.

Le categorie di dati personali oggetto della violazione sono dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro…), dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile, altro…), categoria particolari di dati personali (dati relativi alla salute, dati relativi all'appartenenza sindacale, altro…) relativi a pazienti, dipendenti, consulenti e collaboratori dell'Ospedale.

Conseguenze della violazione:

La conseguenza della violazione sopra descritta è la perdita di confidenzialità ovvero la conoscenza da parte di terzi non autorizzati dei dati oggetto della violazione, compresa la perdita di riservatezza di dati personali protetti da segreto professionale.

Sfruttando le informazioni personali carpite eventuali malintenzionati potrebbero effettuare ulteriori tentativi di phishing cercando di convincere i soggetti interessati che le mail provengono in realtà da fonti legittime, tentare frodi e/o furti/usurpazione di identità.

Misure tecnologiche e organizzative a seguito della violazione:

In seguito all'evento è stata effettuata la notifica al Garante per la Protezione dei Dati Personali, cambiata la passoword dell'account compromesso, ripristinata al configurazione originale e bonificati tutti i device della vittima, avviata insieme a Microsoft una approfondita analisi dei file di log per investigare sull'accaduto, è stato ripetuto un warning anti-phishing a tutte le utenze dei domini aziendali.

L'Ospedale ha altresì presentato un esposto denuncia all'Autorità Giudiziaria competente a tutela della stessa e di tutti i soggetti interessati.

I.R.C.C.S. Ospedale San Raffaele

Gruppo San Donato

* * *

Per ottenere maggiori informazioni o chiarimenti relativamente alla violazione in oggetto, può contattare il Titolare tramite il Responsabile della Protezione dei Dati (dott. Giorgio Presepio) ai seguenti indirizzi: dpo@hsr.it - hsrsanraffaele@hsr.postecert.it

Milano, 15 luglio 2020

Il Titolare - Ospedale San Raffaele S.r.l.

Ing. Elena Bottinelli