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 comunica l'avvenuta violazione dei Suoi dati personali (data breach) che si è verificata in data 26 marzo 2020; la comunicazione è effettuata dall'Ospedale spontaneamente al fine di fornirLe i necessari chiarimenti in merito ai reali fatti occorsi e smentire le informazioni non corrette e pretestuose che sono state divulgate tramite i media.

In data 20 maggio 2020 il gruppo di hacker italiani "LulzSec" sul proprio account Twitter (https://twitter.com/LulzSec_ITA) dichiarava di aver eseguito un attacco alla rete di Ospedale San Raffaele; tali dichiarazioni venivano riprese da diversi articoli di stampa in data 21 maggio 2020 diffondendo notizie non verificate e non corrette sui fatti accaduti.

Pertanto, a seguito del clamore mediatico di tali articoli di stampa, Ospedale San Raffaele interloquiva con il Garante Privacy al fine di chiarire la reale portata e ambito degli accadimenti, e successivamente decideva di effettuare la presente comunicazione rivolta ai soggetti i cui dati sono stati violati.

Descrizione della natura della violazione:

- L'attacco hacker ha avuto ad oggetto un vecchio sito web "SPP Formazione" di Ospedale San Raffaele in previsione di dismissione e dedicato alla formazione obbligatoria dei dipendenti in materia di salute e sicurezza sul lavoro; il sito "SPP Formazione" è stato sostituito da una nuova piattaforma; al momento dell'attacco hacker il sito "SPP Formazione" veniva utilizzato in maniera residuale per un numero limitato di corsi obbligatori e in attesa di aggiornamento.
- Gli hacker hanno avuto accesso al database locale contenente le vecchie user id applicative con le relative password di accesso. Le utenze/password a cui gli hacker hanno avuto accesso permettono di accedere esclusivamente al sito "SPP Formazione" di OSR e registrare l'avvenuto completamento dell'obbligo formativo (ossia non permettono di accedere a nessun altro server aziendale e a nessun dato personale o particolare).
- I dati a cui gli hacker hanno avuto accesso sono solamente nomi e cognomi di alcuni dipendenti/ consulenti e ex dipendenti/consulenti, email aziendali, codici fiscali (in un numero limitato di casi), vecchie user id e password di accesso ai corsi di formazione.
- Nessun dato appartenente a categorie particolari (c.d. sensibile) e nessun dato relativo ai pazienti è stato oggetto dell'attacco.

Conseguenze della violazione:

La conseguenza della violazione sopra descritta è la conoscenza da parte di terzi non autorizzati dei dati oggetto della violazione.

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

Gruppo San Donato

Tale violazione non presenta rischi elevati per i Suoi diritti e le Sue libertà, risultando improbabile l'avverarsi di effetti avversi significativi a Suo danno (intesi quali danni fisici, materiali o immateriali), per le seguenti motivazioni:

- gran parte dei nominativi di dipendi e collaboratori dell'Ospedale sono ed erano già pubblici per ragioni di servizio;

- la email è costruibile aggiungendo il suffisso @hsr.it al cognome.nome, e inoltre molte email si riferiscono a rapporti cessati e pertanto disabilitate;

- le password non sono relative a sistemi di autenticazione ma servivano solamente a tracciare l'avvenuta formazione sulla piattaforma;

- la nomenclatura delle stesse (cognome.nome) non è utilizzabile per il sistema di autenticazione single-sign-on dell'Ospedale, che richiede criteri di complessità elevati;

- nessun dato particolare (c.d. sensibile) è stato oggetto dell'attacco.

Misure tecnologiche e organizzative a seguito della violazione:

In seguito all'evento è stato inibito l'accesso da internet al vecchio sito "SPP Formazione", è stato ripristinato lo stato dei server all'ultimo backup non compromesso, isolando le macchine compromesse per una successiva analisi, sono state cambiate le password dell'applicativo ed effettuato il presente comunicato.

Ad ogni buon conto l'Ospedale ha presentato un esposto denuncia all'autorità giudiziaria competente a tutela della stessa e di tutti i dipendenti.

* * *

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

Milano, 25 giugno 2020

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

Ing. Elena Bottinelli