COMUNICAZIONE COINVOLGIMENTO INDIRETTO NOSTRA STRUTTURA NELL'ATTACCO HACKER SUBITO DA SYNLAB ITALIA

Gentili Utenti,

in riferimento all'attacco hacker subìto dal nostro fornitore SYNLAB Italia srl in data 18 aprile 2024, desideriamo fornirvi le seguenti informazioni.

SYNLAB Italia srl viene utilizzato per l'esecuzione di alcune prestazioni/analisi di laboratorio e anatomia patologica.

Appreso dell'attacco, abbiamo istituito una squadra dedicata per analizzare gli effetti dell'incidente, per mitigarne gli impatti e per attivarci con l'utenza. Inizialmente non abbiamo avuto conferma del diretto coinvolgimento dei dati dei nostri pazienti affidati al laboratorio SYNLAB Italia srl.

Ci teniamo a precisare che la violazione dei dati non ha riguardato i sistemi informatici di 3C, ma soltanto quelli del fornitore SYNLAB Italia srl.

SYNLAB Italia srl è stata vittima di un attacco informatico di tipo ransomware, ossia un programma informatico malevolo che ha "infettato" i sistemi informativi. L'attacco informatico subito ha inoltre comportato la sottrazione illecita (c.d. esfiltrazione) di dati conservati da SYNLAB, da parte di una organizzazione cybercriminale di matrice russa denominata "Black Basta". Abbiamo avuto notizia che i cyber-criminali avevano chiesto un riscatto e non avendo ricevuto alcunché da SYNLAB Italia srl, avevano provveduto a diffondere i dati sottratti in una parte di internet nascosta e non accessibile attraverso i tradizionali sistemi di navigazione online (cd. dark web). Sapevamo inoltre che SYNLAB Italia srl aveva prontamente denunciato l'accaduto alle autorità competenti (Polizia Postale, Procura della Repubblica e Autorità Garante per la protezione dei dati personali) con le quali collaborava per fornire ogni informazione utile (monitorando, ad esempio, le aree del dark web dove erano ubicati i dati personali rubati e segnalando tempestivamente i siti di cui i criminali si erano avvalsi per la pubblicazione affinché fossero oscurati dalla Procura della Repubblica). I dati coinvolti nell'attacco non sono andati perduti e SYNLAB Italia srl sta lavorando al recupero dei i dati esfiltrati (copiati) utilizzando anche copie di backup (ossia le copie dei dati eseguite per fronteggiare casi come questo).

I dati personali oggetto di violazione di cui 3C è titolare del trattamento sono relativi ad alcune prestazioni di laboratorio e di anatomia patologica erogate da SYNLAB tra gennaio 2015 e febbraio 2024. Includono, dunque, informazioni come dati identificativi e relativi alla salute. Si ritiene opportuno precisare che la perdita di riservatezza non ha riguardato la totalità delle informazioni dei soggetti interessati (pazienti) ma solo un sotto-insieme in riferimento all'arco temporale sopra indicato.

Solo da ultimo (via pec in data 08/07/2024) abbiamo avuto ufficiale comunicazione che l'esfiltrazione e la pubblicazione ha riguardato anche dati di nostri pazienti. A seguito di questa comunicazione da parte di SYNLAB Italia, a tutela di 3C e di tutti i suoi pazienti, abbiamo ritenuto di dover notificare l'accaduto all'Autorità Garante per la Protezione dei Dati pur non sapendo quali pazienti e dati fossero stati colpiti nell'attacco. Infatti a causa delle complessità operative emerse in fase di analisi, al momento il fornitore non ci ha comunicato elementi sufficienti per individuare con sicurezza e precisione gli interessati coinvolti dalla violazione. Nel rispetto della normativa in materia di protezione dei dati personal, abbiamo ritenuto opportuno pubblicare la presente comunicazione.

Sarà nostra cura continuare l'analisi in corso, onde raccogliere informazioni più precise in merito ai soggetti interessati e ai dati rimasti coinvolti nell'attacco per garantirvi un adeguato supporto.

In ogni caso, 3C ha avviato le attività necessarie a definire la natura, la tipologia e la quantità di dati personali affidati a SYNLAB Italia; ha interrotto il caricamento di dati personali tramite portale condiviso e la trasmissione di campioni raccolti fino alla totale e assoluta certezza di ripristino della sicurezza; ha chiesto formali informazioni a SYNLAB Italia dell'incidente subito con particolare riferimento ai dati personali affidati; ha avvisato dell'accaduto l'utenza e il personale interno dell'attacco a tutela dei pazienti.

Unitamente a SYNLAB Italia srl sconsigliamo fortemente di cercare se i vostri dati sono pubblicati sul dark web. Navigare su tali pagine comporta alti rischi di infezioni da malware (software malevoli che possono compromettere il vostro dispositivo e tutti i dati contenuti al suo interno). Inoltre, non vi è alcuna garanzia di sicurezza di quanto pubblicato da una organizzazione cybercriminale: i file pubblicati potrebbero infatti contenere a loro volta ulteriori malware. Infine, l'accesso a dati pubblicati sul dark web può comportare il download di materiale illecito (condotta che, nei casi previsti dalla legge, può costituire reato).

I dati personali esfiltrati e pubblicati sul dark web, possono essere, seppur illecitamente, consultati, prelevati e ulteriormente diffusi da terzi, anche ai fini di tentativi di furto d'identità, o altri tentativi di frode o utilizzi illeciti. I tentativi di frode che potrebbero derivarne possono essere diversi ma l'obiettivo solitamente è quello di utilizzare i dati personali per estorcere denaro e/o esfiltrare ulteriori informazioni tramite l'invio di e-mail, messaggi o telefonate contenenti false richieste apparentemente provenienti da amici/familiari oppure tentando di accedere agli account riconducibili alla vittima.

Vi invitiamo a prendere visione delle pagine di SYNLAB dedicate all'attacco informatico e delle seguenti pagine informative dell'Autorità Garante per la Protezione dei dati personali:

PHISHING

https://www.garanteprivacy.it/temi/cybersecurity/phishing

VISHING
https://www.garanteprivacy.it/temi/cybersecurity/vishing

SMISHING
https://www.garanteprivacy.it/temi/cybersecurity/phishing

SIM SWAPPING

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9572143

È importante prestare attenzione e valutare l'attendibilità di chi vi richiede tramite e-mail, SMS, messaggio o telefonata codici di accesso o ulteriori dati personali (anche se tali richieste riguardassero la conferma della modifica delle Vostre credenziali). Nessun Istituto bancario e, più in generale, nessun fornitore di servizi, richiede mai codici di accesso o password tramite e-mail, SMS o telefonate. È fondamentale esaminare sempre attentamente i contenuti di e-mail, SMS, messaggi evitando di aprire collegamenti ipertestuali (link) o allegati che potrebbero indirizzarvi verso siti web

dannosi o farvi scaricare software malevoli, sostituire ciclicamente le password dei propri account (e-mail, social network, forum etc. …) e attivare l'autenticazione multifattoriale che ne rafforzano la protezione. I principali fornitori di servizi online offrono questa possibilità e per attivarla normalmente è sufficiente accedere alle impostazioni di sicurezza del proprio account.

Siamo a vostra disposizione per qualsiasi ulteriore domanda, dubbio o richiesta di chiarimento.

Potete contattarci al seguente recapito: privacy3c@centroclinicochimico.it

Spinea, 10 Luglio 2024

Il Legale Rappresentante

Da Tos Francesco