SYNLAB

www.synlab.it

16/07/2024

Spett.le IFM

OGGETTO: COMUNICAZIONE DELLA VIOLAZIONE DEI DATI DAL RESPONSABILE AL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

In considerazione del ruolo di responsabile del trattamento dei dati ai sensi dell'art. 28 del RGPD 2016/679, SYNLAB è a informare la Vostra organizzazione, quale titolare del trattamento dei dati ai sensi dell'art. 4 del RGPD 2016/679, dell'avvenuta violazione dei dati personali, conseguente all'attacco *cybercriminale* subito dalla Scrivente, affinché la Vostra organizzazione possa mettere in atto ogni azione necessaria.

Descrizione della violazione dei dati personali

Come già esposto e reso pubblico con i comunicati del 19 aprile, del 22 aprile, del 05 maggio, del 13 maggio, del 15 maggio 2024 e successivamente riportato da molti mass media nazionali e locali, SYNLAB è stata vittima di un attacco cybercriminale di tipo *ransomware, che ha* comportato la sottrazione illecita (c.d. esfiltrazione) di 1,5 Tb di dati conservati da SYNLAB, da parte di una organizzazione *cyber*criminale denominata "*Black Basta*".

In data 13 maggio 2024 i *cyber*-criminali hanno diffuso sul c.d. dark web i dati sottratti illecitamente.

All'esito delle prime verifiche svolte, SYNLAB ha appurato che all'interno di questi dati sono presenti anche informazioni che riguardano i dati personali anagrafici e relativi allo stato di salute dei pazienti che SYNLAB tratta, in qualità di responsabile del trattamento dei dati ai sensi dell'art. 28 del RGPD 2016/679.

Momento in cui il Responsabile è venuto a conoscenza della violazione

- Ore 07:00, del 18/04/2024 SYNLAB ha rilevato la cifratura dei dati personali in corso d'opera
- 05/05/2024, SYNLAB ha rilevato la rivendicazione dell'attacco da parte dell'attaccante e la relativa azione di esfiltrazione, comprovata dalla pubblicazione di limitate quantità di dati personali non riconducibili alla Vostra organizzazione
- 15/07/2024 all'esito delle prime analisi, SYNLAB ha rilevato l'avvenuta esfiltrazione e pubblicazione dei dati relativi alla Vs Organizzazione.

Natura della violazione

- Perdita di riservatezza

Causa della violazione

- Azione intenzionale esterna

Banche dati oggetto di violazione

Alla data di comunicazione, SYNLAB ha appurato che l'organizzazione cybercriminale ha esfiltrato e pubblicato alcuni *folder* con funzione di *repository* per l'applicativo SYNLABNET, contenente informazioni anagrafiche e sullo stato di salute dei pazienti.

Nello specifico, i dati erano ubicati all'interno di *folder* organizzati secondo la logica di AAAA/MM//GG e riguardano alcune prestazioni di laboratorio e di anatomia patologica erogate da SYNLAB attraverso il laboratorio analisi sito in Castenedolo (BS) tra Gennaio 2015 e Febbraio 2024.

Ai fini della determinazione del numero di interessati nonché delle categorie di dati personali oggetto della violazione, si specifica che per ogni accettazione di ogni singolo campione, il *repository* contiene 3 documenti digitali: il referto firmato digitalmente (.p7m) e due documenti contenenti i dati analitici strutturati (rispettivamente in formato *.ris* e *.rin*) ciascuno dei quali include

- Dati anagrafici del paziente
- Dati relativi allo stato di salute del paziente

Alla data di comunicazione SYNLAB ha rilevato che la violazione, in riferimento alla Vs Organizzazione, riguarda

- il seguente numero di registrazioni contenenti dati personali trattati da SYNLAB in qualità di Responsabile del trattamento per conto della Vs organizzazione: 8;
- il seguente numero approssimativo di interessati: 3.

Specifichiamo che il numero approssimativo di interessati sopra riportato è calcolato tenendo in considerazione il rapporto 1/3, in considerazione che per ciascun campione sono prodotte tre registrazioni (file .p7m, file .rin e file .ris). Ai fini di un più corretto calcolo del numero approssimativo (che riteniamo potrebbe essere ridotto) suggeriamo alla Vs organizzazione di voler calcolare un ulteriore coefficiente di riduzione, che tenga in considerazione che uno stesso interessato possa aver effettuato, nel periodo sopra indicato, più di un singolo prelievo.

A tal riguardo, richiamiamo tutte le precedenti note già inoltratevi, pubblicate sul nostro sito istituzionale, nei nostri centri e tramite i canali di comunicazione a nostra disposizione (peraltro riprese da tutte le principali testate giornalistiche locali e nazionali), attraverso le quali abbiamo fornito, tempestivamente e nel rispetto degli obblighi previsti dalla normativa, tutte le informazioni necessarie al fine di informare e tutelare gli interessati. A tal fine segnaliamo che non essendo

possibile valutare la posizione di ciascun interessato, abbiamo ritenuto di fornire tali informazioni attraverso comunicazione pubblica.

Misure tecniche e organizzative poste in essere al momento della violazione

1) Edifici: Sistemi di allarme; Sistemi di videosorveglianza; Società di vigilanza durante chiusura; Sistema antincendio; Sistema di autorizzazione per l'accesso ai piani tramite badge per la sede Monza e tutti i Laboratori;

(2) Uffici: Documenti archiviati in armadi o cassetti muniti di chiave; Chiave degli armadi o cassetti assegnata esclusivamente al personale preposto; Distruzione dei fascicoli mediante tritarifiuti; Distruzione dei fascicoli mediante fornitore certificato; TrustCode – distruzione; Crown – archiviazione e distruzione;

(3) Archivi: Conservazione presso fornitore;

(4) Dispositivi: Stampanti nei corridoi dotate di PIN o token per l'avvio della stampa;

(5) Formazione: Policy aziendali per l'utilizzo della posta elettronica e delle risorse informatiche; Formazione in tema di Privacy; Formazione in tema di Compliance; Formazione in tema cybersecurity awareness;

(6) Sistemi informativi: sistema di autenticazione centralizzato; politiche per la garanzia della complessità e lunghezza delle password; Virtual Private Network (VPN) per accesso da remoto; Impedimento riutilizzo della password; Profili di autorizzazione differenziati degli utenti per l'accesso ai dati; Procedure di backup; Verifica dell'esito positivo delle procedure di backup ad ogni salvataggio; Presenza soluzione antivirus regolarmente aggiornato; Implementati meccanismi di controllo dell'aggiornamento; Rete wireless ospiti separata dalla rete interna; Rete protetta da firewall con funzionalità web content filtering, di antivirus di rete, di intrusion prevention / intrusion detection; Controllo periodico dell'aggiornamento delle licenze; Revisione periodica regole di filtraggio; Divieto di installazione software da parte dell'utente; Cifratura dei volumi dei dispositivi mobili portatili; Autenticazione a 2 fattori per applicativi Cloud Office 365 – Medwork (in fase di attivazione); Contratto di assistenza per la manutenzione;

(7) Sala Server: Accesso ai locali mediante dispositivo (badge-token) assegnato al solo personale autorizzato; area sottoposta a videosorveglianza (Castenedolo e Monza); l'area è inaccessibile al cliente-utente-fornitore;

(8) Ulteriori misure adottate: (SOC) Security Operation Center; Endpoint Detection and Response (EDR) per contrastare infezioni malware; Utilizzo di frewall IDS IPS; Servizio esterno di threat intelligence che fornisce informazioni relative a potenziali attacchi e data breach; Security

information and event management (SIEM); Conduzione Vulnerability assessment e di penetration test interni e con avvalimento di terzi fornitori.

Possibili conseguenze della violazione

Allo stato non risulta possibile escludere che l'incidente possa portare a tentativi di furto d'identità, o altri tentativi di frode. Tali azioni potrebbero verificarsi nei confronti Vs e/o dei Va pazienti.

Misure adottate a seguito della violazione

Appena ricevuta la notizia dell'attacco, il team interno IT e il team esterno specializzato in *cybersecurity* hanno provveduto a mettere in sicurezza il sistema, scollegandolo dalla rete internet e spegnendo le macchine (server e client). L'accesso ad internet è stato attivato in modo tale che fosse raggiunta esclusivamente la piattaforma *cloud* dell'Endpoint Detection and Response (EDR) al fine di consentire al fornitore esterno del Security Operation Centre (SOC) di analizzare lo stato dell'infrastruttura IT e al team interno preposto alla gestione dell'infrastruttura IT e alla gestione di attacchi *cyber* di monitorare la struttura IT (con monitoraggio attivo 24 ore su 24) e di effettuare le verifiche necessarie.

SYNLAB ha isolato e neutralizzato il *malware*, che è ad oggi confinato in due postazioni, utilizzate esclusivamente per le verifiche da parte del team interno IT. In particolare, la società ha adottato le seguenti misure (ancora in corso di esecuzione): (i) verifica del funzionamento di ciascun *server*, (ii) verifica e utilizzo dei *backup*, (iv) modifica dei profili *firewall* (ove necessario), (v) interruzione dei servizi di posta elettronica, VPN e reti verso altri soggetti, e (vi) isolamento dei singoli segmenti IT. Quanto al punto *sub* (vi), SYNLAB ha rilevato che gli *asset* interessati dall'attacco sono server di virtualizzazione VMware ESXi e Server collegati e ha rimesso in funzione in modo graduale gli asset che, previa certificazione dei fornitori qualificati esterni, risultano non essere stati interessati dall'attacco o rispetto ai quali il malware è stato debellato. Tutti i sistemi messi in funzione sono stati verificati anche dal SOC gestito da fornitore previa conferma installazione del *software anti-malware*.

In terzo luogo, pendente il totale ripristino di sistemi e servizi, onde garantire per quanto possibile una erogazione dei servizi sicura, ancorché parziale, SYNLAB ha adottato misure volte a garantire la *business continuity*, mediante (i) refertazione di laboratorio con disconnessione dei sistemi, (ii) isolamento delle connessioni esterne relativamente ai servizi resi nell'ambito B2B e (iii) ripresa dei consulti medici che non richiedono strumentazione e utilizzo in modalità standalone degli strumenti che sono stati verificati.

Ancora, è stata adottata una procedura di messa in sicurezza della strumentazione di laboratorio e di servizi polidiagnostici propedeutica al ripristino delle attività, nelle misure che seguono:

- Verifica del dispositivo diagnostico da parte del servizio di assistenza tecnica del produttore:

è stato verificato che il *software* del dispositivo non fosse colpito da *malware.* Ove infetto è stato ripristinato il *software* originale;

- Aggiornamento del S.O. sul quale risiede l'applicativo di analisi clinica al fine che vi sia installato il *software anti-malware* centralizzato;
- Qualora il *software anti-malware* non fosse compatibile con il S.O., installazione di *software anti-malware* compatibile da parte del fornitore e/o ottenimento dichiarazione di tutte le misure tecniche di sicurezza in essere sul dispositivo;
- Ove le attività sopradescritte non fossero state possibile, i dispositivi sono rimasti isolati dalla rete e utilizzati in modalità *standalone.*

Il ripristino delle attività di SYNLAB è avvenuto in modo graduale, dando priorità alla messa in sicurezza dei *server* e alla fornitura di servizi a favore di reparti chemioterapici e operatori delle strutture clienti (e.g. ospedali). Alla data odierna è avvenuto il ripristino in sicurezza del sistema di accettazione e download referti nell'ambito B2B (service analisi di laboratorio), su cui è stata completata l'implementazione della misura della MFA per l'autenticazione dei clienti B2B.

Misure di cui si propone l'adozione per attenuare i possibili effetti negativi della violazione

Pertanto, SYNLAB invita a mettere in atto ogni misura che sia ritenuta necessaria per la tutela dei soggetti interessati, suggerendo di raccomandare loro di porre maggiore attenzione, rispetto all'ordinario, a qualunque interazione sospetta (*online* ma anche *offline*).

In tal senso SYNLAB invita a suggerire ai soggetti interessati di prendere visione 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

Gli eventuali tentativi di frode, in questi casi, possono essere di vario tipo: l'obiettivo è solitamente quello di utilizzare i dati personali per estorcere denaro e/o esfiltrare ulteriori dati personali attraverso l'invio di messaggi o telefonate contenenti false richieste provenienti da parte di amici o familiari oppure tentando di accedere agli *account* riconducibili alla vittima.

In questa fase, SYNLAB suggerisce mettere in atto alcune misure:

- valutare attentamente ogni e-mail, SMS, messaggio o telefonata in cui Vi venissero richiesti codici di accesso o ulteriori dati personali, valutando con attenzione l'attendibilità del

richiedente; gli Istituti bancari e, più in generale, i fornitori di servizi, non richiedono mai codici di accesso o *password* tramite SMS, E-mail o telefonate.

- valutare attentamente e-mail, SMS e di altri fonti di messaggistica contenenti collegamenti ipertestuali (link) o allegati sospetti-inusuali: potrebbero essere usati per indirizzare l'utente verso siti web dannosi o fargli scaricare software malevoli;
- sostituire le password dei propri account (e-mail, Social Network, forum, etc…) **e, se il sistema lo permette, attivare l'autenticazione a più fattori**. I meccanismi di autenticazione multifattoriale (es. i codici OTP che ricevete dalla banca dopo aver inserito *username e password* per accedere all'*home banking*) rafforzano la protezione da accessi indesiderati. I principali fornitori di servizi *online* offrono questo sistema: per attivarlo è sufficiente entrare nelle impostazioni di sicurezza dell'*account.*
- Informare i propri amici e familiari di essere stati vittima di questa violazione, suggerendo loro di porre attenzione al rischio di ricevere false richieste che paiono pervenire da Voi.

Il Responsabile del trattamento

Il Gruppo SYNLAB eroga servizi di *service* di laboratorio su tutto il territorio nazionale per il tramite di differenti società facenti parte dello stesso. Ai fini della Vs comunicazione all'Autorità Garante per la protezione dei dati personali sono di seguito forniti i dati societari di ciascuna società del gruppo, in modo che sia possibile indicare conformemente il "Responsabile del trattamento dei dati" che ha fornito la presente comunicazione.

SYNLAB Italia S.r.l.	Via Martiri delle Foibe, 1 - 20900 Monza (MB) - P.IVA 00577680176
Baluardo Servizi Sanitari S.r.l.	Piazzale Porta del molo, 2 – 16128 Genova (GE) – P.IVA 03803500101
Istituto Il Baluardo S.p.A.	Via Del Molo, 4 - 16128 Genova - P.IVA 02937630107
SYNLAB Data Medica S.r.l.	Via Zanchi, 89 - 35133 Padova - P.IVA 00477060289
SYNLAB Med S.r.l.	Via Case Nuove, 44 - 48018 Faenza (RA) - P.IVA 00463660399
SYNLAB Medical S.r.l.	Via C. Colombo, 13 - 35020 Albignasego (PD) - P.IVA 03220330280
SYNLAB Lazio S.r.l.	Via San Polo dei Cavalieri, 20 – 00159 Roma (RM) – P.IVA 12337751007
SYNLAB SDN S.r.l.	Via Francesco Crispi, 8- 80121 Napoli - P.IVA 01288650631