Comunicazione pubblica ai sensi dell'art. 34, par. 3, lett. c), del Regolamento (UE) 2016/679 in merito all'attacco hacker subito dall'Azienda del Servizio Sanitario (Azienda Sanitaria di Matera, Azienda Sanitaria di Potenza, AOR San Carlo Potenza ed IRCCS-CROB Rionero in V.) e dalla Regione Basilicata nel gennaio 2024.

Gentili Utenti,

Vi scriviamo per integrare e aggiornare la precedente informativa dell'01/02/2024 relativa all'attacco informatico (hacker) di cui sono state vittime le Aziende del Servizio Sanitario Regionale e la Regione Basilicata e che ha permesso a cyber criminali di accedere illegalmente ai sistemi informatici e sottrarre documenti contenenti dati personali.

Tale aggiornamento segue gli elementi emersi nelle fasi di analisi e indagine che hanno seguito l'attacco.

Cosa è successo e come abbiamo reagito?

Dopo aver rilevato le attività non autorizzate, abbiamo:

- prontamente coinvolto le forze dell'ordine competenti, che hanno supportato nelle indagini, si è proceduto ad informare l'Agenzia Nazionale Cybersecurity nonché l'Autorità Garante per la Protezione dei Dati Personali, come richiesto dalla legge.
- immediatamente adottato misure per contenere, valutare e porre rimedio all'incidente, tra cui l'attivazione di un gruppo di emergenza in risposta agli incidenti, l'assunzione di principali esperti esterni di cybersecurity per supportare le attività di risposta e l'arresto temporaneo di tutti i sistemi IT che potevano essere interessati.
- proceduto a bonificare l'intero sistema informatico aumentando i livelli di sicurezza con nuovi strumenti informatici che tengono sotto controllo continuamente la rete e possono rilevare prima possibile eventuali nuove minacce;
- dato diffusione sui siti web istituzionali delle Aziende e della Regione Basilicata e la notizia è stata rilanciata dai quotidiani e dalle TV locali.

Quali dati personali sono stati violati?

Dalle nostre verifiche, i dati sottratti comuni e particolari, sia di natura sanitaria che amministrativa, riguardano principalmente pazienti ed operatori, costituiscono una minima parte del patrimonio informativo delle Aziende e spesso si tratta di dati parziali e destrutturati, raggruppati in 'riassunti', ovvero documenti riferibili a un gran numero di persone, spesso identificate in maniera incompleta o difficilmente riconducibile alla persona in assenza di altri elementi conoscitivi.
I criminali hanno pubblicato nel dark web diversi dati personali contenuti nei documenti conservati dalle Aziende e, pertanto, questi dati personali hanno perso la riservatezza.
Grazie alle copie di sicurezza che tutte le Aziende e la Regione effettuano senza interruzione, non sono stati perduti dati personali né sono stati modificati i documenti sanitari più importanti, come i fascicoli sanitari e le cartelle cliniche.
Ricordiamo che chiunque scarichi o entri comunque in possesso di dati pubblicati da organizzazioni criminali nel dark web e li utilizzi per propri scopi o li diffonda on-line, sui social network o in altro modo incorre in condotte illecite che possono costituire reato.
Per questi motivi, nonché per la difficoltà di accedere al dark-web, la possibilità che dalla violazione derivi un danno concreto è abbastanza remota, comunque, le Aziende e la Regione esaminano puntualmente tutti i documenti violati per poterli classificare in base al livello di delicatezza dei dati contenuti e verificare se possono essere riferiti a persone identificate o identificabili.
Considerate la quantità e la frammentarietà dei file violati, si tratta di un'attività complessa e prolungata nel tempo, tuttora in corso, ma è il solo modo per tentare di determinare entità e potenziale impatto di quanto accaduto, necessario per poter predisporre la comunicazione agli interessati coinvolti: alcuni interessati identificati univocamente vengono contattati direttamente e lo saranno man mano che procederà l'identificazione, per tutti gli altri, che non hanno ricevuto e non riceveranno alcuna comunicazione personalizzata, la Regione Basilicata comunica con questa informativa pubblica, come consente la normativa, allorché lo sforzo per ogni singola persona

potenzialmente coinvolta dalla violazione sarebbe obiettivamente sproporzionato.

Cosa rischio? Cosa posso fare per proteggermi?

Non possiamo escludere che, anche a seconda dei dati personali e particolari in possesso dei criminali a seguito dell'incidente possa portare a tentativi di furto d'identità, phishing ed eventualmente frodi in generale.

Di seguito vi riportiamo alcune misure che potete considerare di adottare per proteggervi:

- Valutate attentamente ogni e-mail, SMS, messaggio istantaneo e telefonata in cui vi vengono richiesti i vostri dati personali, anche se sembrano provenire dalla nostra Azienda: vi ricordiamo che, di norma, non vi chiederemo mai di fornire informazioni personali attraverso tali canali. Per ogni evenienza contattare/segnalare immediatamente il fatto alle Autorità competenti (Uffici della Polizia di Stato – Stazione dei Carabinieri);
- Attenzione per le e-mail contenenti collegamenti ipertestuali incorporati, che possono essere utilizzati per indirizzare l'utente verso siti Web dannosi;
- Valutate con attenzione le e-mail che contengono allegati inaspettati;
- Diffidate di qualsiasi e-mail sospetta, anche se sembra provenire da persone che conoscete o dalla nostra azienda, ad esempio e-mail con una grammatica/ortografia scorretta o un linguaggio non preciso;
- non dare seguito a richieste inusuali di contatto telefonico per offrire prodotti e/o prestazioni sanitarie e/o servizi diversi collegabili a prestazioni sanitarie.

Chi posso contattare per avere maggiori informazioni?

Per fornire a tutti i soggetti interessati maggiori informazioni sul trattamento dati, la Regione Basilicata ha predisposto una apposita pagina sul proprio sito internet: https://www.regione.basilicata.it/datipersonali ed è sempre possibile inviare una mail al Responsabile della Protezione Dati rpd@regione.basilicata.it .

Inoltre, per ottenere informazioni circa la natura dei dati violati riferiti alle singole persone oppure per esercitare i diritti, di cui agli articoli dal 15 al 21 del GDPR, gli interessati possono inviare, allegando copia di un documento di identità in corso di validità, le richieste al Responsabile della Protezione dei Dati delle singole Aziende del SSR, ai seguenti indirizzi di posta elettronica:

- Azienda Sanitaria di Matera - rpd@asmbasilicata.it
- Azienda Sanitaria di Potenza - rpd@aspbasilicata.it
- Istituto di Ricovero e Cura a Carattere Scientifico di Rionero in Vulture (CROB) rpd@crob.it;
- Azienda Ospedaliera Regionale San Carlo di Potenza - dpo@pec.ospedalesancarlo.it .