**AZIENDA SANITARIA DI POTENZA**

**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.**

Nella seconda metà di gennaio - come già reso noto in precedenti comunicati – le Aziende del Servizio Sanitario Regionale e la Regione Basilicata sono state vittime di un attacco informatico (Hacker) che ha permesso a cyber criminali di accedere illegalmente ai sistemi informatici e sottrarre documenti contenenti dati personali. La violazione è stata bloccata non appena rilevata.

**Cosa è successo e come abbiamo reagito?**

Dopo aver rilevato le attività non autorizzate, abbiamo:

* coinvolto prontamente le forze dell'ordine competenti (Polizia Postale) - che ci hanno supportato nelle indagini - e proceduto ad informare l'Agenzia Nazionale Cybersecurity (ACN) 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, con 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 ampia diffusione sui siti web istituzionali delle Aziende e della Regione Basilicata: la notizia è stata rilanciata dai quotidiani e dalle TV locali.

**Quali dati personali sono stati violati?**

Potenzialmente potrebbero essere stati coinvolti tutti gli interessati (cioè le persone) dei quali le Aziende e la Regione trattano dati personali (ovvero utenti, pazienti, dipendenti, collaboratori e via dicendo) e tutte le categorie di dati personali trattati, comprese le categorie più delicate, come i dati sanitari e giudiziari.

**Con riferimento specifico alla nostra Azienda ASP**, le attività di indagini seguite all'intervento di ACN e Polizia Postale, con il supporto fornitori specializzati in incident response, a tutt’oggi non consentono di precisare nè le categorie di interessati nè le categorie dei dati personali effettivamente coinvolti: a fine aprile il CSIRT Italia (Computer Security Incident Response Team) comunicava di esser venuto a conoscenza di avvenuta pubblicazione nel dark web di documenti verosimilmente afferenti anche alla nostra Azienda. L’analisi di questi documenti evidenziava tuttavia che i documenti di nostro interesse sono solo 2, mentre la quasi totalità dei documenti è afferente ad altre Aziende del Servizio Sanitario Regionale. I 2 documenti in questione consistono in: 1) ASP Giacenze 2013, contenente le giacenze di farmaci, materiali diagnostici, prodotti dietetici, presidi chirurgici e simili presso varie strutture aziendali, senza alcun dato personale; 2) INVIO RESOCONTO ASP gennaio - aprile 2016 contenente l’ammontare dei compensi dovuti a 3 operatori indicati con nome e cognome (quindi non esattamente identificabili) per Consulenza nel monitoraggio ambientale nel periodo marzo-aprile 2016. Naturalmente non è possibile escludere che in un futuro prossimo o remoto vengano pubblicati altri documenti di tutt’altra portata e criticità, che potrebbero anche contenere categorie di interessati e relativi dati personali di cui al momento non vi è evidenza alcuna: in tal caso provvederemo ad integrare la presente comunicazione secondo le previsioni della normativa vigente, anche con comunicazioni specifiche alle persone i cui dati personali risultassero violati.

Giova ricordare 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, ma tuttavia continueremo ad esaminare 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: si tratta di un'attività complessa e prolungata nel tempo, ma è il solo modo per tentare di determinare entità e potenziale impatto di quanto accaduto e provvedere alle dovute comunicazioni agli interessati coinvolti.

Per tutti gi altri, che non hanno ricevuto e non riceveranno alcuna comunicazione personalizzata, Regione ed Aziende provvedono con informativa pubblica, come consente la normativa allorché lo sforzo per comunicazione ad ogni singola persona coinvolta dalla violazione sarebbe obiettivamente sproporzionato.

**Cosa rischio? Cosa posso fare per proteggermi?**

Come accennato, non possiamo escludere che, in base ai dati personali, possano verificarsi tentativi di furto d'identità, phishing ed eventualmente frodi in generale.

Di seguito riportiamo alcune misure da adottare per proteggervi:

* Valutare attentamente ogni e-mail, SMS, messaggio istantaneo e telefonata in cui vi vengono richiesti 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 alle e-mail contenenti collegamenti ipertestuali incorporati, che possono essere utilizzati per indirizzare l'utente verso siti Web dannosi;
* valutare con attenzione le e-mail che contengono allegati inaspettati;
* diffidare 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?**

Informazioni circa la natura dei dati violati riferiti alle singole persone interessate possono essere richieste all'indirizzo di posta elettronica del Responsabile della Protezione Dati della nostra Azienda rpd@aspbasilicata.it, allegando copia di un documento di identità in corso di validità; allo stesso indirizzo e-mail è possibile rivolgere le richieste di esercizio dei diritti di cui agli articoli da 15 a 21 del GDPR, sempre allegando copia di un documento di identità in corso di validità.