LegnanoNews
Le news di Legnano e dell'Alto Milanese

Attacco informatico all’ASST Rhodense

Valeria Arini · Thursday, June 6th, 2024

La scorsa notte, la **rete informatica dell’ASST Rhodense** ha **subito un importante attacco informatico che ha coinvolto tutte le sedi (presidi di Garbagnate Milanese, Bollate, Rho e Passirana** e servizi territoriali delle aree distrettuali Garbagnatese, Rhodense e Corsichese).

La Direzione – fa sapere l’Azienda – di concerto con i tecnici, sta lavorando per verificare la situazione garantendo nel contempo i servizi essenziali. L’ASST ha organizzato in ogni presidio un servizio di accoglienza degli utenti, in modo da informarli e prendere in carico ogni richiesta. È garantita l’erogazione delle prestazioni ambulatoriali già programmate, tranne quelle di medicina nucleare, ad esempio MOC, di radiologia (TAC, Risonanze, Radiografie e Mammografie) e di laboratorio analisi (compresi esami ematici).

Sono sospese – aggiunge l’ASST Rhodense – le attività relative a interventi chirurgici non urgenti e quelle di prenotazione presso i CUP, di ricovero programmato e dei Punti Prelievo (i pazienti TAO possono rivolgersi all’accoglienza dei Presidi Ospedalieri di Bollate, Garbagnate e Rho per avere informazioni sulle modalità di esecuzione degli esami necessari per la gestione della terapia). I Pronto Soccorso di Garbagnate e Rho rimangono attivi (è stato sospeso solo l’invio di ambulanze) ma, in caso di urgenza, si consiglia ai cittadini di rivolgersi ad altre strutture. Attualmente non è possibile stimare i tempi di ripristino della rete aziendale e si chiede la collaborazione di tutti, soprattutto in questi primi momenti di riorganizzazione delle attività.

Regione Lombardia ha coinvolto i tecnici di Aria che sono intervenuti sul posto questa mattinata ed hanno attivato la Task Force regionale di Cyber Security. È stata inoltre informata l’Agenzia di Cybersicurezza Nazionale che sta inviando i propri specialisti. Sono in corso le attività di analisi per comprendere le modalità con le quali si è svolto l’attacco, verificare la disponibilità di backup ‘puliti’ e la situazione di tutti i singoli sistemi e predisporre un piano di ripristino dei dati, dei servizi e degli applicativi.