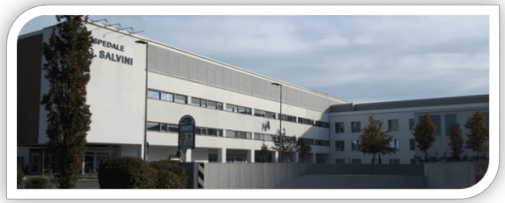
CYBER ATTACK ALLA SALUTE

Sicurezza informatica e continuità assistenziale nell'esperienza dell' ASST Rhodense

Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

Giorgia Saporetti - Direttore Sanitario ASST Rhodense

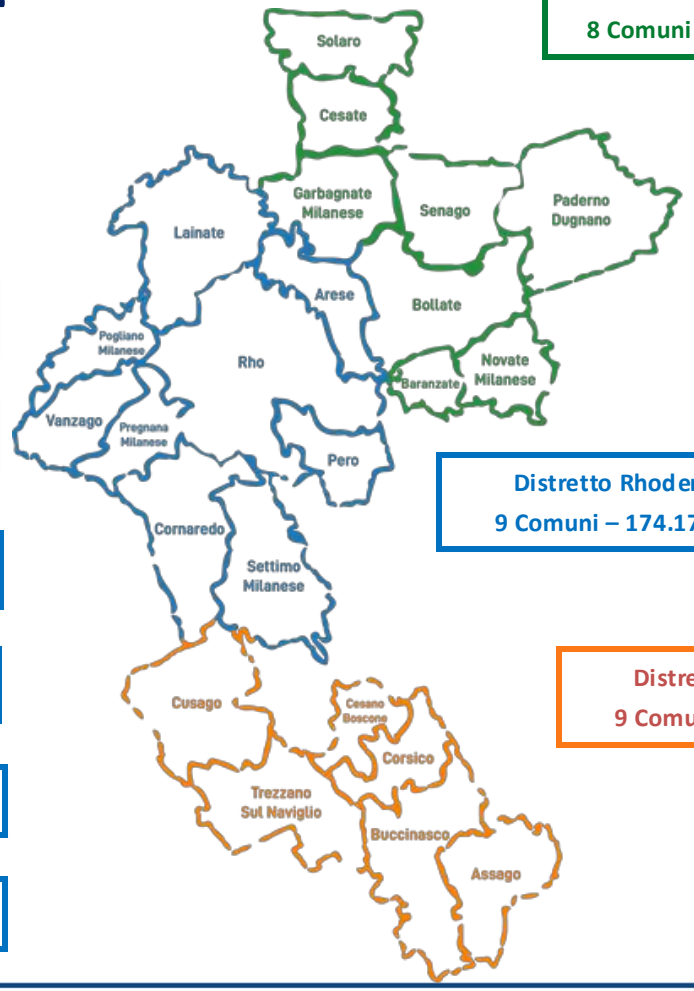


IL CONTESTO AZIENDALE

Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

Personale 3.677 unità

Polo ospedaliero	**Polo territoriale**
Presidi 4	Distretti 3 – 487.028 ab
Prestazioni ambulatoriali 2.939.179	Strutture, UDO e servizi territoriali 53
Posti letto 802	CdC 5 OdC 1
Accessi PS 97.000	Posti letto -416
Ricoveri 21.802	MMG-265 PLS-53



Distretto Garbagnatese
8 Comuni – 192.587 ab

Distretto Rhodense
9 Comuni – 174.174 ab

Distretto Rhodense
9 Comuni – 174.174 ab

** Cosa è successo? **

I tuoi computer e server sono crittografati, i tuoi backup sono stati eliminati.
Utilizziamo algoritmi di crittografia avanzati, quindi non sarai in grado di decrittografare i tuoi dati.

Puoi recuperare tutto acquistando da noi uno speciale programma di recupero dati.
Questo programma ripristinerà l'intera rete.

Attenzione non modificare o tentare di ripristinare alcun file da solo.
Ciò potrebbe causare la loro perdita permanente.

** Perdita di dati **

Abbiamo scaricato più di 1000 GB dei dati della tua azienda.
Contattaci o saremo costretti a pubblicare tutti i tuoi dati su Internet e a inviarli a tutte le autorità di regolamentazione del tuo paese, nonché ai tuoi clienti, partner e concorrenti.
Siamo pronti a:
- Fornirti la prova che i dati sono stati rubati;
- Eliminare tutti i dati rubati;
- Aiutarti a ricostruire la tua infrastruttura e prevenire attacchi simili in futuro;

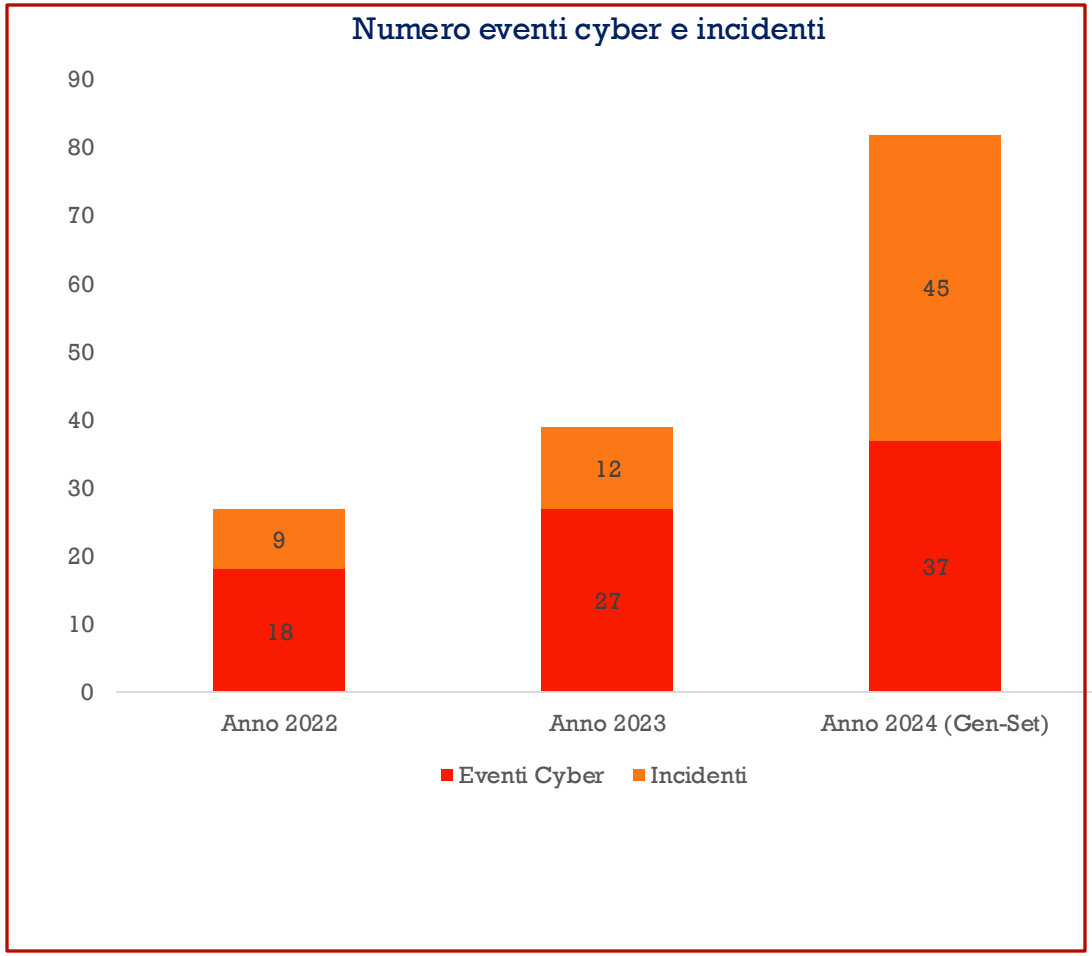
** Quali garanzie? **

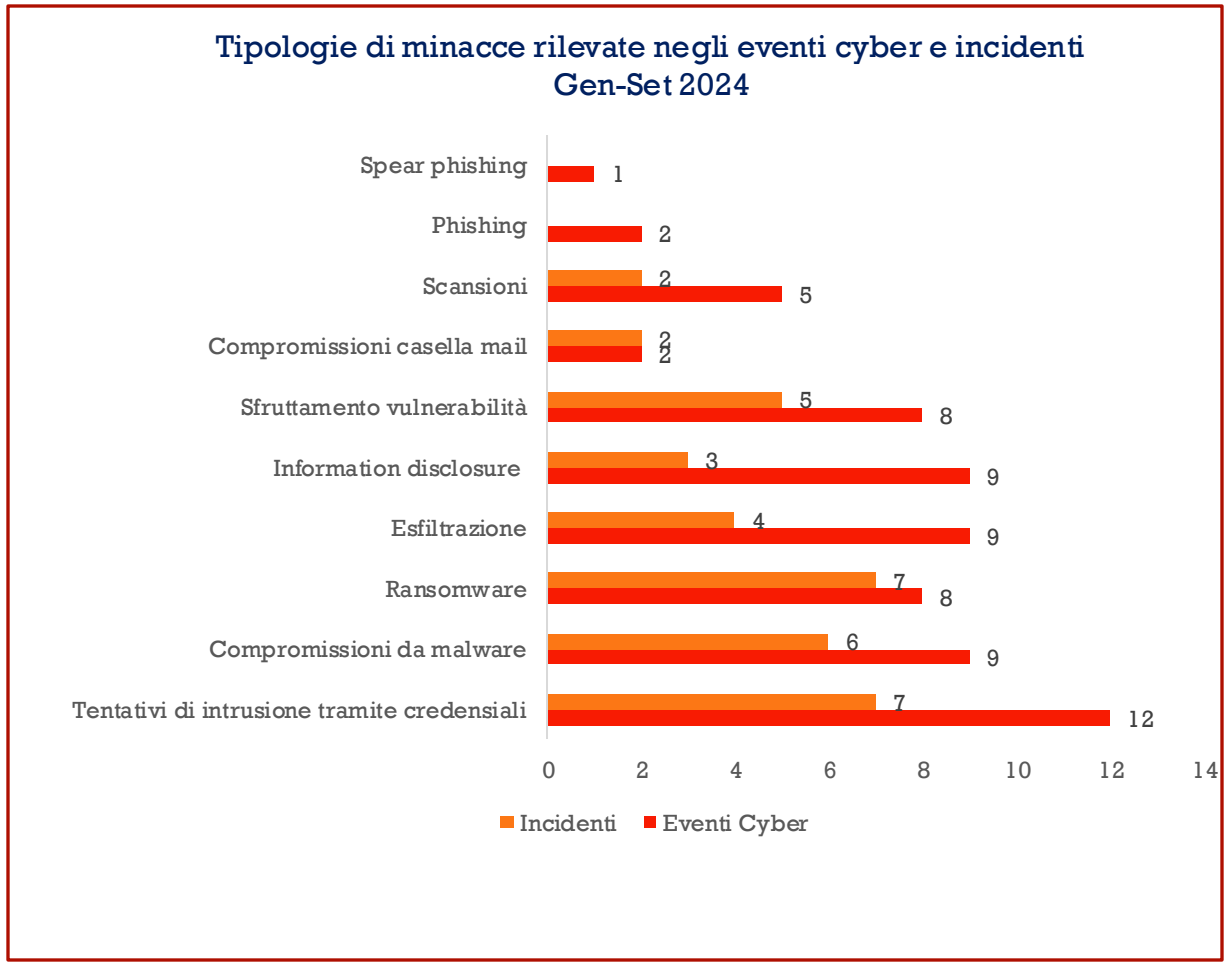
La nostra reputazione è di fondamentale importanza per noi.
Non adempiere ai nostri obblighi significa non lavorare con te, il che è contro i nostri interessi. Stai tranquillo, i nostri strumenti di decrittazione sono stati testati a fondo e sono garantiti per sbloccare i tuoi dati.
In caso di problemi, siamo qui per supportarti. Come gesto di buona volontà, siamo disposti a decriptare un file gratuitamente.

** Come contattarci? **

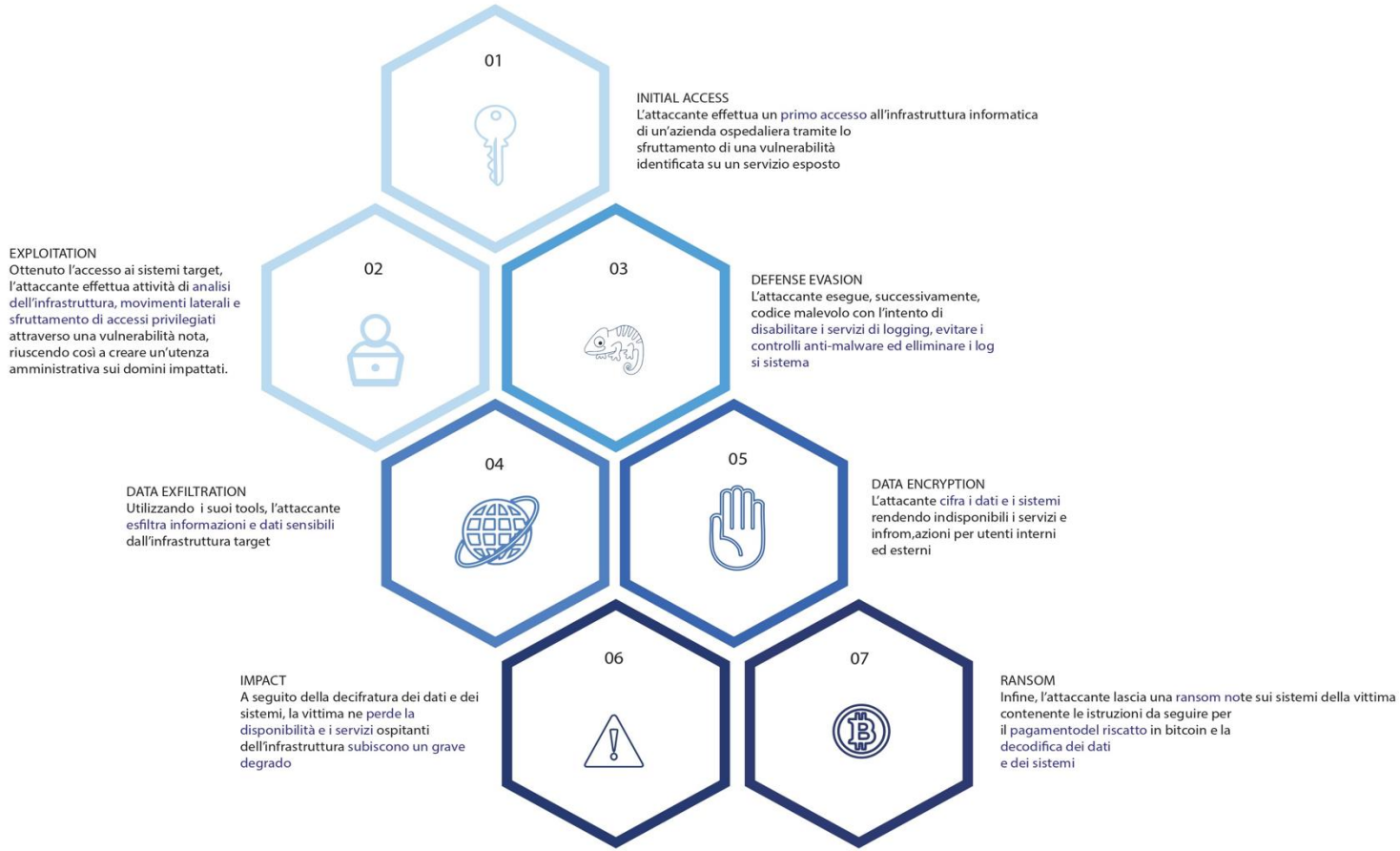
Utilizzo del browser TOR:
1) Puoi scaricare e installare il browser TOR da questo sito:
https://torproject.org/
2) Apri il nostro sito web:
http://cicadaxousmk6nbntd3ucxefmfgt2drhtfdvh7gmdeh3ttvudam6f2ad.onion/pgfy2q2xxzhuzaokvmmomvmagm9l4s54h408ndmrduuxl7h9fcc8jkmffjalni4m3c920svfe1ozg26a

IL PANORAMA DEGLI ATTACCHI





RANSOMWARE ALL'ATTACCO



PER UNA BUONA CYBERSICUREZZA

COSA FARE E COSA NON FARE

Assenza di autenticazione multi fattore sulle Visual Private Network (VPN)		Implementazione dell'autenticazione multi fattore
Utilizzo di protcolli di autenticazione e cifratura		Utilizzo di versioni recenti di protocolli di autenticazione e comunicazione e disabilitazione protocolli obsoleti sui Dominian Controller
Password Policy inadeguata		Creazione di password policy che rispetti le best practice anche supportata dagli strumenti proposti quali password manager
Errata gestione dei privilegi utente		Applicazione el principio del privilegio minimo su account utente e di servizio e revisione periodica dei privilegi ad essi assegnati
Assenza di inventario dei servizi critici		Redazione e costance aggiornamento di una lista aggiornata dei servizi IT critici e una lista delle funzionalità e dati critici degli ospedali
Prodoti non aggiornati		Creazione di un asset inventory dei dispositivi con relativa versione del software e firmware in uso; applicazione degli aggiornamenti di sicurezza ed eventuali patch rilasciati dai produttori; isolamento o dismissione dei dispositivi non pi supportati e non aggiornabili.

Errata gestione di Microsoft Active Directory		Corretta architettura e gestione dell'AD secondo le indicazioni di hardening fornite dal Vendor e utilizzo di tool specofoco che consentano il monitoraggio e il rilevamento di cricità nella configurazione.
Errata gestione dei log		Redazione di una policy di gestione dei log per il rilevamento e l'analisi degli eventi, adozione di strumenti dedicati quali SIEM, SOAR, XSOAR e log collector e backup dei log e corretta conservazione degli stessi
Errata gestione dei backup		Rete isolata e segmentata per gestire proattivamente la sicurezza e la conformità, e utilizzo approccio Zero Trust in caso di gestione decentralizzata dall'infrastruttura IT.
Rete non segmentata		Implementazione di una politica di gestione dei backup per la memoriazazzione in proporzioni di rete segregate ed una frequenza di backup proporzionata alla criticità delle informazioni memorizzate, nonchè un piano di ripristino in caso di perdita dei dati.
Mancanza di procedure di incidenti Response		Redazione e aggiornamento costante di un piano di risposta agli incidenti informatici che individui ruoli e responsabilità di tutti i soggetti incaricati nelle varie fasi della gestione degli incidenti, e che includa elenchi di eventuali fornitori di servizi, di hardware e di software
Assenza di Endpoint Detection and Response		Adozione di soluzioni EDR o XDR in grado di rilevare e bloccare comportamenti anomali negli host.

RHODENSE SOTTO ATTACCO

Blocco

- Distruzione rete aziendale completa
- PC e programmi informatici inutilizzabili
- Blocco telefonia fissa

Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

Continuità operativa

SALVAGUARDATE

* Attività di **ricovero urgente**
* **Attività operatoria** non ha mai subito interruzioni, salvaguardando le urgenze
* I due **PS di Rho e Garbagnate** sono stati sempre operativi, è stata sempre garantita l'attività agli **autopresentati** in PS.

RIDOTTE

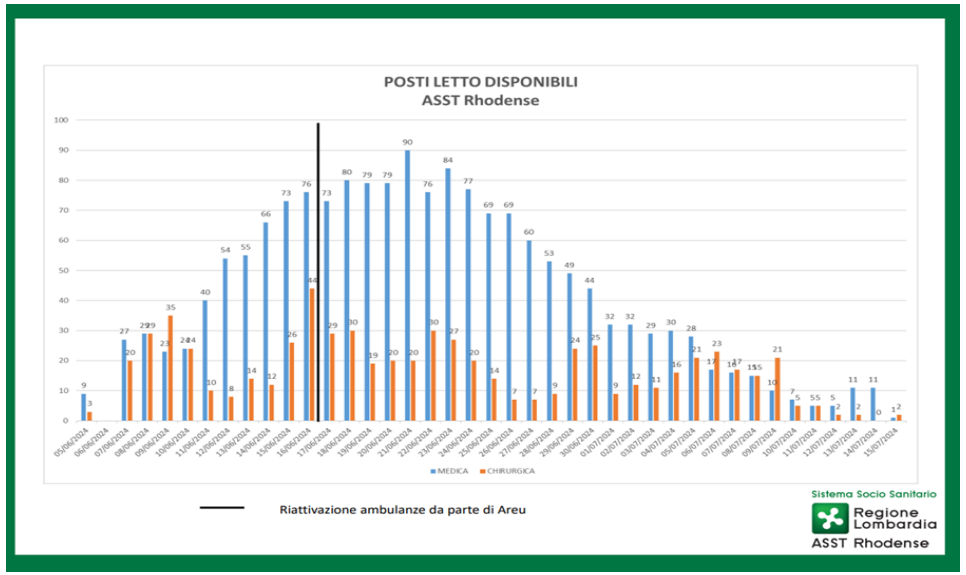
Attività ambulatoriale è stata assicurata, con notevoli **rallentamenti** e linee di attività non pienamente operative

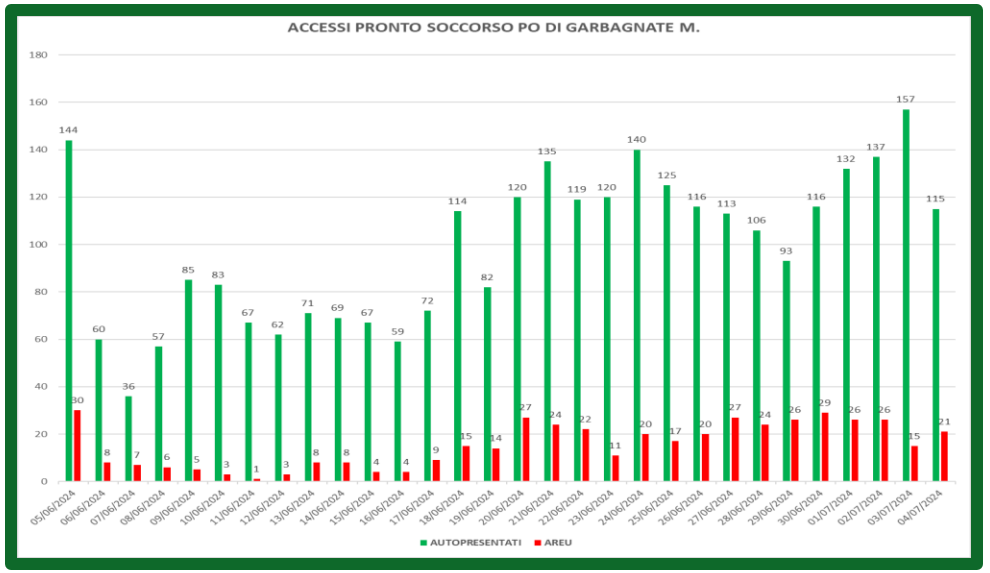
SOSPESE

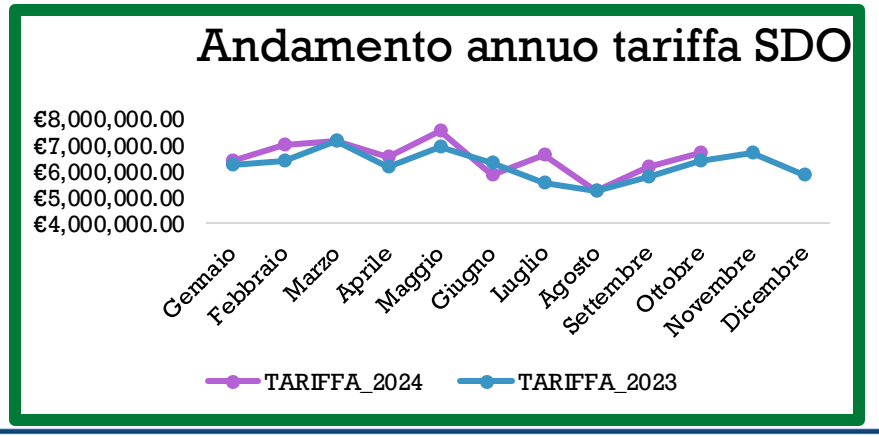
-7 gg	-15 gg	- 20 gg
* Attività di ricovero programmato * Laboratorio * Anatomia Patologica	* CUP * Sistema Informativo PS * Radiologia * Punti Prelievo * Donazione del sangue * Accesso internet	* Posta e PEC * Sportelli MMG

Il **sistema di archiviazione e l'accesso** a tutta la **documentazione** aziendale è stato bloccato per **66 giorni.**

IMPATTO SULL'ATTIVITA' SANITARIA







Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

MANCATI RICAVI E COSTI EMERGENTI

MANCATI RICAVI			
	Tariffa con cyber attack	**Tariffa senza cyber attack**	**Delta tariffa**
ATTIVITA' DI RICOVERO	€ 5.868.909	€ 6.723.612	€ 854.703
ATTIVITA' AMBULATORIALE	€ 2.711.319	€ 4.275.584	€ 1.564.265
TOTALE			**€ 2.418.968**

COSTI EMERGENTI	
Tipologia di costo	**Importo IVA inclusa**
APPARECCHIATURE	€ 11.953,44
ATTIVITA' VARIE DI RIPRISTINO	€ 120.311,67
TOTALE	**€ 132.965,11**

Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

CHECK LIST - FASE POST CYBER ATTACK -				
Blocco totale ICT - applicativi aziendali, posta elettronica, sito internet, telefonia fissa-				
DEFINIZIONE DELLE PRIORITA' PER LA CONTINUITA' OPERATIVA	**DESCRIZIONE DELLE ATTIVITA'**	**STATO DELLE ATTIVITA' AL T0**	**STATO DELLE ATTIVITA' AL T1 E**	**NOTE**
PRIORITA' STRATEGICHE	Creazione e uso gruppi WA	v -ESEMPIO DI COMPILAZIONE		..... .
	Convocazione UdC			.....
	Cartellonistica "NON ACCENDERE" sui PC			.....
	Allerta e attivazione DG Welfare-ARIA-ACN-Polizia			.....
	Comunicazione DPO e data bridge			.....
	Comunicazione con stampa/social media			.....
	Convocazione collegio di Direzione			.....
PRIORITA' SANITARIE				
Attività di Pronto Soccorso	Blocco ambulanze AREU			.....
	Mantenimento pazienti autopresentati			.....
Attività di degenza	Passaggio ad accettazione/dimissione CARTACEA			.....
	Accesso alle cartelle cliniche in back up - se cartella			.....
	Richiesta esami solo urgenti			.....
	Istituzione reperibilità radiologica			.....
	Visione immagini radiologiche solo in locale			.....
Blocco operatorio	Blocco interventi chirurgici in elezione			.....
	Mantenimento interventi in urgenza			.....
Attività ambulatoriale	Blocco attività di radiologia e medicina nucleare per			.....
	Blocco punti prelievo ospedalieri e territoriali			.....
	Blocco PRENOTAZIONI			.....
Sedi territoriali	Mantenimento attività sanitarie			.....
Documentazione sanitaria e gestione richieste	Redazione completamente cartacea			.....
	Richieste lab/rx/consulenze cartacee			.....
Trasmissioni tra i servizi	Istituzione pedonaggio interno			.....
Attività di lavorazione ematica	Trasferita in altra ASST			.....
Attività di anatomia patologica	Trasferita in altra ASST			.....
PRIORITA' DI COMUNICAZIONE	Distribuzione PC/WiFi portatili			.....
	Distribuzione cellulari aziendali			.....
	Attivazione hotspot aziendali e personali			.....
	Definzione GMAIL nuove			.....
	Affissione avvisi cyber attack in tutta ASST			.....
	Servizio di accoglienza ai varchi in ospedale			.....
	Pagina web nuova provvisoria			.....
PRIORITA' TECNICO-AMMINISTRATIVE	Acquisizione memorie esterne per radiologia			.....
	Bonifica PC aziendalei			.....
	Riattivazione posta PEC			.....
REDAZIONE INDICAZIONI SCRITTE UDC	Diffusione cartacea tramite autisti			.....
	Diffusione tramite WA			.....
	Diffusione tramite nuovi indirizzi GMAIL			.....

Governance Cyber Attack

UNITA' DI CRISI

Composizione:

- Direzione Strategica
- Sistemi Informativi
- Comunicazione
- DMP
- DAPSS
- Ingegneria clinica
- Accoglienza
- Dipartimento Amministrativo
- Affari generali

Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

STRATEGIE VINCENTI PRE E POST ATTACCO

Focus sull'obiettivo, disciplina, compatezza, proattività, senso di appartenenza.

Fiducia, comunicazione, supporto reciproco, consapevolezza.

Sistema Socio Sanitario
Regione Lombardia
ASST Rhodense

Grazie per l'ascolto

Giorgia Saporetti – Direttore Sanitario ASST Rhodense

Si ringraziano Marco Bosio, Emiliano Gaffuri e Paola Bianco