Reglyze

Esercitazione tabletop NIS 2 / DLgs 138/2024 — Briefing — Ransomware nel Sistema di Cartella Clinica Elettronica (CCE)

IT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-06-03T19:10:10.311Z

Classification: Confidential

Ransomware nel Sistema di Cartella Clinica Elettronica (CCE)

Esercitazione tabletop NIS 2 — Articolo 21(2)(f) · DLgs 138/2024 art. 24 c. 2 e art. 25

Settore	**Sanità**
Gravità	Significativo (incidente notificabile)
Durata suggerita	90 minuti
Identificativo	`it-ospedale-ransomware-cce`
Emesso il	03/06/2026

Contesto

Un ospedale pubblico italiano, qualificato come soggetto essenziale ai sensi del DLgs 138/2024 (Allegato I — sanità), opera una Cartella Clinica Elettronica (CCE) on-premises, PACS di radiologia, portale del paziente, sistema di gestione del laboratorio e circa 180 postazioni cliniche. L'ospedale impiega circa 1100 dipendenti, con circa 75 medici specialisti. L'ospedale è inserito nell'elenco dei soggetti NIS ai sensi dell'art. 7 DLgs 138/2024 e dispone di un punto di contatto designato presso l'ACN.

Il contesto di questo esercizio è una campagna ransomware coordinata che colpisce simultaneamente la CCE, la farmacia ospedaliera e parte del blocco operatorio. L'esercizio esplora l'articolazione tra continuità clinica (operatività in modalità cartacea), pre-notifica di incidente significativo al CSIRT Italia entro 24 ore dalla rilevazione (art. 25 c. 4 DLgs 138/2024), notifica al Garante Privacy per violazione di dati personali particolari (art. 33 GDPR), e comunicazione pubblica.

La squadra deve lavorare contro il cronometro: la pre-notifica (preallarme) di 24 ore decorre dal momento in cui il soggetto viene a conoscenza dell'incidente significativo (art. 25 c. 4 DLgs) — non dall'attacco in sé.

Sequenza di iniezioni (T+0 → T+72h)

I tempi seguono il cronometro dell'art. 25 DLgs 138/2024 (pre-notifica 24h / notifica 72h). Il facilitatore legge ciascuna iniezione al momento indicato oppure comprime l'esercizio in un blocco di 60-90 minuti.

Momento	Iniezione	#
T+0	05:38. Il responsabile IT dell'ospedale riceve un allarme dal SIEM: attività anomala di cifratura su 23 server nel segmento della cartella clinica elettronica (CCE). I terminali del pronto soccorso mostrano una nota di riscatto in inglese. Il sistema di gestione dei posti letto non risponde. I PACS di radiologia funzionano ma con latenza elevata.	1
T+15min	T+15min. Il primario di turno chiede se gli interventi programmati per le 08:00 devono essere cancellati. Non si accede alla lista dei farmaci somministrati né alle allergie note. Il fornitore della	2

Momento	Iniezione	#
	CCE conferma segnalazioni analoghe da altri tre ospedali italiani. Il DPO viene allertato.	
T+1h	T+1h. Il CSIRT Italia contatta il punto di contatto dell'ospedale dopo una correlazione trasversale nei sensori nazionali. La direzione IT conferma cifratura su 31 dei 48 server. Il backup più recente verificato ha 28 ore. Non esiste procedura documentata di operazione in modalità degradata per la CCE.	3
T+4h	T+4h. La squadra IT avvia il ripristino dal backup offsite. Gli interventi elettivi sono cancellati; il pronto soccorso opera con registro cartaceo. Il Direttore Generale convoca il Comitato di Crisi. L'Azienda Sanitaria Locale (ASL) chiede un punto di situazione. RAI TG Regione e Il Sole 24 Ore hanno giornalisti al telefono.	4
T+24h	T+24h. Ripristinati 36 dei 48 server. La CCE è operativa in sola lettura; la gestione farmaci ancora no. La pre-notifica (preallarme) al CSIRT Italia è stata inviata tramite la piattaforma ACN entro le 24 ore dalla rilevazione (art. 25 c. 4 DLgs 138/2024). Il Garante Privacy non è ancora stato notificato — l'ambito di esposizione dei dati personali (potenzialmente dati sanitari particolari) è sotto valutazione.	5
T+72h	T+72h. Notifica completa (art. 25 c. 5 lett. b) DLgs) trasmessa al CSIRT Italia tramite piattaforma ACN. Valutazione iniziale conferma incidente significativo (impatto sostanziale su servizio essenziale sanitario + rischio per i pazienti). Ripristino tecnico al 91%; la squadra forense ha identificato il vettore iniziale (allegato phishing aperto da operatore della farmacia ospedaliera). Notifica GDPR art. 33 consegnata al Garante Privacy nella 70ª ora. Comunicazione proattiva ai pazienti in corso.	6

Domande per la discussione

Il facilitatore legge verbatim. Far emergere le lacune — non fornire risposte.

1. Chi è il soggetto designato per trasmettere la pre-notifica al CSIRT Italia tramite la piattaforma ACN? Chi è il supplente?
2. Il backup offsite verificato ha 28 ore. Qual è la finestra di perdita dati clinici accettabile? Esiste una procedura documentata per ricostruire quell'intervallo da registri ausiliari?
3. In quale momento si decide di notificare il Garante Privacy? Chi coordina con il DPO? Qual è la base giuridica della notifica se l'esposizione effettiva non è ancora confermata?
4. Il punto di contatto unico con il CSIRT Italia è disponibile 24/7? Ha credenziali valide sulla piattaforma ACN al momento dell'incidente?
5. Chi approva la comunicazione alla stampa? L'organo di amministrazione è stato informato nei tempi necessari per la validazione (art. 23 c. 1 DLgs)?
6. Se l'incidente terminasse in meno di 2 ore, sarebbe comunque necessaria la pre-notifica al CSIRT Italia? (Suggerimento: art. 25 c. 8 DLgs.)
7. Quali prove si raccolgono nelle prime 24 ore per supportare la relazione finale (art. 25 c. 5 lett. d) DLgs)? Dove si centralizza la catena di custodia?

Azioni attese (chiave di correzione post-esercizio)

Riferimento di ciò che un'organizzazione matura fa in questo scenario. Confrontare con le prestazioni della squadra durante il debriefing.

1. Contenimento immediato: isolare la VLAN della CCE, sospendere RDP in uscita, disattivare le utenze compromesse. Mappatura della propagazione tramite EDR/SIEM.
2. Attivare il piano di continuità clinica in modalità cartacea; designare il responsabile IT di turno + il referente clinico in servizio continuo fino alla risoluzione.
3. Inviare la pre-notifica (preallarme) al CSIRT Italia tramite la piattaforma ACN (servizi.acn.gov.it) entro 24 ore dalla rilevazione (art. 25 c. 4 + c. 5 lett. a) DLgs 138/2024) — conservare la ricevuta del ticket.
4. Valutare l'esposizione di dati personali (dati sanitari = categoria particolare GDPR art. 9); notificare il Garante Privacy entro 72 ore se confermata (art. 33 GDPR). Coordinare con il DPO.
5. Ripristinare il servizio dal backup offsite verificato; documentare l'età del backup, l'ambito del ripristino, i controlli di integrità.
6. Comunicare ai pazienti tramite SMS/portale + linea di supporto dedicata; mantenere portavoce unico; allineare il comunicato stampa con l'ASL e il CSIRT Italia prima della pubblicazione.
7. Trasmettere la notifica completa (72h) al CSIRT Italia (art. 25 c. 5 lett. b) DLgs) con valutazione di gravità, indicatori di esposizione, misure di mitigazione applicate.
8. Dopo la cessazione dell'impatto significativo: preparare la relazione finale entro un mese (art. 25 c. 5 lett. d) DLgs 138/2024); archiviare le evidenze forensi per la catena di custodia.

Riferimenti normativi

Funzioni Misure ACN (proxy NIST CSF)	RS · RC
Articoli della Direttiva (UE) 2022/2555	• Article 21(2)(b) • Article 21(2)(c) • Article 21(2)(h) • Article 23(4)(a) • Article 23(4)(b) • Article 23(4)(d)
Articoli del DLgs 138/2024	• art. 24 c. 2 DLgs 138/2024 (misure di sicurezza — gestione incidenti) • art. 24 c. 2 DLgs 138/2024 (continuità operativa e gestione crisi) • art. 24 c. 2 lett. g) DLgs (crittografia) • art. 25 c. 4 DLgs 138/2024 (pre-notifica 24h) • art. 25 c. 5 lett. a) DLgs (preallarme) • art. 25 c. 5 lett. b) DLgs (notifica 72h) • art. 25 c. 5 lett. d) DLgs (relazione finale entro un mese) • art. 23 c. 1 DLgs 138/2024 (obblighi organo di amministrazione)

Questo documento è un briefing di scenario Reglyze per esercitazione offline. Non costituisce consulenza legale. Per i casi complessi consulti il suo legale o contatti l'ACN tramite servizi.acn.gov.it.

Reglyze · https://reglyze.com