Reglyze

Esercitazione tabletop NIS 2 / DLgs 138/2024 — Briefing — Compromissione fornitore OT — catena di fornitura idrica

IT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-06-03T19:09:18.664Z

Classification: Confidential

Compromissione fornitore OT — catena di fornitura idrica

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

Settore	**Acqua**
Gravità	Significativo (incidente notificabile)
Durata suggerita	75 minuti
Identificativo	`it-acquedotto-supply-chain-mfa`
Emesso il	03/06/2026

Contesto

Un'azienda idrica comunale (circa 40 dipendenti, tre stazioni di pompaggio e due serbatoi) qualificata come soggetto essenziale ai sensi del DLgs 138/2024 (Allegato I — acque potabili). Lo SCADA e i PLC delle stazioni sono gestiti da un integratore OT esterno (stile NETisON), con accesso remoto continuo tramite VPN per la gestione del firmware e la configurazione dei PLC.

Il contesto dell'esercizio è una catena di eventi classica: l'integratore viene compromesso da ransomware nelle proprie reti, e l'accesso remoto dell'integratore verso i clienti diventa un vettore di propagazione. L'esercizio esplora il riflesso del tipo 'il nostro fornitore è stato attaccato — siamo vittime per estensione' e obbliga la squadra a motivare la decisione di notifica di incidente significativo ai sensi del DLgs 138/2024, anche in assenza di impatto effettivo sulla qualità dell'acqua.

È anche lo scenario in cui il widget di pre-compilazione della notifica ACN (Task 4.2 it-market-parity) offre valore operativo concreto — la squadra deve usare i dati pre-compilati come punto di partenza per la pre-notifica.

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	T+0. 13:42. L'integratore OT che gestisce lo SCADA dell'azienda idrica comunale invia un bollettino urgente: ransomware rilevato nella propria infrastruttura interna la notte precedente. L'accesso remoto che l'integratore utilizza per gestire i PLC della stazione di pompaggio potrebbe essere stato compromesso. L'integratore ha sospeso tutte le sessioni, ma il registro degli accessi indica tre login recenti da IP non abituali nelle ultime 40 ore.	1
T+15min	T+15min. L'operatore SCADA verifica che le ultime modifiche ai setpoint delle pompe P-02 e P-04 sono state effettuate 21 ore fa dal canale dell'integratore. Le modifiche appaiono tecniche e normali a prima vista. Non esiste un registro indipendente che confermi l'autorizzazione dell'ingegnere di turno di quella notte.	2

Momento	Iniezione	#
T+1h	T+1h. Il responsabile della cybersicurezza del Comune contatta l'azienda. Il Sindaco vuole sapere se c'è rischio per la qualità dell'acqua. Le analisi di laboratorio vengono intensificate. Il CSIRT Italia conferma di stare indagando un cluster di incidenti legati allo stesso integratore presso altri enti.	3
T+4h	T+4h. La revisione forense del log del PLC mostra che uno dei comandi inviati ha tentato di modificare il dosaggio di ipoclorito da 1,0 mg/L a 0,2 mg/L — è fallito perché ha superato il limite hardcoded nel PLC. Non c'è stata alterazione effettiva della qualità dell'acqua. Ma il tentativo è avvenuto. La direzione discute se questo configuri un incidente significativo ai sensi del DLgs 138/2024.	4
T+24h	T+24h. Pre-notifica (preallarme) al CSIRT Italia trasmessa circa 8 ore fa tramite piattaforma ACN (la decisione è stata presa dopo la riunione dell'organo di amministrazione: il tentativo di alterazione del dosaggio con potenziale impatto sulla salute pubblica qualifica). Il contratto con l'integratore è in revisione giuridica. Il Comune ha emesso un comunicato rassicurante. Il giornale locale pone domande sull'audit degli altri fornitori OT.	5
T+72h	T+72h. Notifica completa (72h) al CSIRT Italia (art. 25 c. 5 lett. b) DLgs) trasmessa con valutazione completa: vettore d'origine identificato (accesso remoto dell'integratore senza MFA), nessun utente colpito, misure applicate (revoca credenziali, MFA obbligatorio su tutti i canali dei fornitori OT, audit della catena di fornitura avviato). Piano di rientro da presentare nella relazione finale entro un mese dalla cessazione dell'impatto (art. 25 c. 5 lett. d) DLgs).	6

Domande per la discussione

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

1. Quanti fornitori esterni hanno accesso remoto all'infrastruttura OT? Il registro è aggiornato? Esiste MFA obbligatorio su tutti i canali?
2. Qual è lo SLA contrattuale di notifica incidente dell'integratore? È documentato? È stato rispettato in questo esercizio?
3. Il limite hardcoded nel PLC che ha bloccato la modifica del dosaggio è un controllo di sicurezza intenzionale o un caso fortunato? È documentato come controllo di sicurezza formale?
4. Chi nell'organizzazione ha l'autorità per decidere che un incidente è significativo ai sensi del DLgs? È decisione dell'organo di amministrazione (art. 23 c. 1) o può essere delegata?
5. Il tentativo di modifica del dosaggio (fallito) configura un incidente significativo? Quali criteri dell'art. 25 c. 2 DLgs si applicano?
6. Come si comunica con il Comune senza generare panico pubblico? Chi è il portavoce unico?
7. Il contratto con l'integratore OT prevede audit di cybersicurezza? Include clausole di notifica immediata? Include responsabilità per compromissione delle credenziali?

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. Revocare immediatamente le credenziali e i token VPN dell'integratore OT; forzare il reset MFA su tutte le utenze amministrative; bloccare gli IP sospetti identificati nei log.
2. Ripristinare tutti i setpoint dei PLC P-02 e P-04 ai valori di riferimento noti; intensificare il campionamento di laboratorio in tutti i punti a valle delle stazioni interessate.
3. Convocare la riunione dell'organo di amministrazione per la decisione formale sulla qualificazione dell'incidente come significativo (art. 23 c. 1 DLgs — responsabilità non delegabile); verbalizzare la decisione e la motivazione.
4. Trasmettere la pre-notifica al CSIRT Italia tramite piattaforma ACN entro 24 ore dalla decisione (art. 25 c. 4 + c. 5 lett. a) DLgs), anche in assenza di impatto effettivo — il tentativo è sufficiente.
5. Coordinare con il Comune come ente responsabile dell'operazione; allineare la comunicazione pubblica con il CSIRT Italia prima della diffusione.
6. Valutare il contratto con l'integratore OT alla luce dell'art. 24 c. 2 lett. d) DLgs (sicurezza della catena di approvvigionamento) — prassi di cybersicurezza del fornitore, MFA obbligatorio, monitoraggio accessi, clausola di incidente.
7. Trasmettere la notifica completa (72h) al CSIRT Italia (art. 25 c. 5 lett. b) DLgs) e programmare la relazione finale entro un mese dalla cessazione dell'impatto significativo (art. 25 c. 5 lett. d) DLgs).
8. Avviare audit di tutta la catena di fornitura OT — quanti fornitori hanno accesso remoto? Qual è il controllo degli accessi? Esiste MFA? Qual è lo SLA di notifica incidenti del fornitore?

Riferimenti normativi

Funzioni Misure ACN (proxy NIST CSF)	ID · PR · DE · RS
Articoli della Direttiva (UE) 2022/2555	• Article 21(2)(d) • Article 21(2)(i) • Article 21(2)(j) • Article 23(4)(a) • Article 23(4)(b)
Articoli del DLgs 138/2024	• art. 24 c. 2 lett. d) DLgs 138/2024 (sicurezza catena di approvvigionamento) • art. 24 c. 2 lett. h) DLgs (controllo degli accessi e gestione degli attivi) • art. 24 c. 2 lett. i) DLgs (MFA e comunicazioni sicure) • 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