Reglyze

Esercitazione tabletop NIS 2 / DLgs 138/2024 — Briefing — Esfiltrazione credenziali — doppia notifica CSIRT Italia + Garante Privacy

IT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-06-03T19:09:30.306Z

Classification: Confidential

Esfiltrazione credenziali — doppia notifica CSIRT Italia + Garante Privacy

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

Settore	**Piattaforma SCADA / ICT**
Gravità	Significativo (incidente notificabile)
Durata suggerita	75 minuti
Identificativo	`it-esfiltrazione-doppia-notifica`
Emesso il	03/06/2026

Contesto

Un operatore italiano di telecomunicazioni (soggetto essenziale ai sensi del DLgs 138/2024, Allegato I — comunicazioni elettroniche) gestisce un portale clienti con circa 650.000 account attivi. Un ricercatore di sicurezza in divulgazione responsabile segnala l'esposizione di un indice Elasticsearch in un ambiente di sviluppo rimasto accessibile dall'esterno. Circa 45.000 utenti sono potenzialmente esposti.

Il contesto dell'esercizio è la sovrapposizione NIS2 + GDPR: l'incidente riguarda materia di cybersicurezza (art. 24 c. 2 lett. f) DLgs — igiene informatica e formazione, e lett. h) — controllo degli accessi e gestione degli attivi) ma anche materia di protezione dei dati personali (GDPR art. 32 + 33). La squadra deve gestire due scadenze distinte: 24 ore per il CSIRT Italia (art. 25 c. 4 DLgs) e 72 ore per il Garante Privacy (art. 33 GDPR).

L'esercizio evidenzia anche la particolarità italiana del coordinamento tra CSIRT Italia e Garante Privacy (art. 35 NIS2 — coordinamento tra le autorità per evitare il ne bis in idem in materia di sanzioni).

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. 08:54. Un ricercatore di sicurezza scrive all'azienda in divulgazione responsabile: il portale clienti dell'operatore di telecomunicazioni espone email + hash della password tramite un indice Elasticsearch in un ambiente di sviluppo dimenticato. Stima 45.000 account interessati.	1
T+15min	T+15min. La squadra conferma l'esistenza dell'indice e che è accessibile dall'esterno da almeno cinque settimane. Esegue il takedown immediato. L'hash utilizzato è SHA-256 con salt — ma nei log del bucket è stato rilevato scraping negli ultimi tre giorni.	2
T+1h	T+1h. Il DPO chiede un punto di situazione. La direzione convoca una riunione straordinaria. Non è ancora chiaro se questo configuri un incidente significativo ai sensi del DLgs 138/2024 — è	3

Momento	Iniezione	#
	principalmente un problema GDPR con sovrapposizione NIS2.	
T+4h	T+4h. L'analisi forense conferma 44.872 utenti esposti, con scraping di almeno 14.000 record identificati nei log. La direzione decide di notificare sia il CSIRT Italia (NIS2) sia il Garante Privacy (GDPR). Comunicazione agli utenti in preparazione con reset forzato della password alla prossima sessione.	4
T+24h	T+24h. Pre-notifica al CSIRT Italia trasmessa tramite piattaforma ACN (art. 25 c. 4 DLgs 138/2024). Notifica al Garante Privacy da completare entro le 72 ore (art. 33 GDPR). Comunicazione agli interessati in corso (art. 34 GDPR). La stampa specializzata ha già la notizia.	5
T+72h	T+72h. Notifica completa (72h) al CSIRT Italia (art. 25 c. 5 lett. b) DLgs) trasmessa. Notifica al Garante Privacy consegnata entro il termine di 72h GDPR. Comunicazione agli utenti finalizzata tramite email + banner sul portale. Reset forzato della password alla prossima sessione. Avviato audit di tutti gli ambienti di sviluppo — 11 ambienti identificati, 2 con esposizione residua da correggere.	6

Domande per la discussione

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

1. Qual è l'articolazione pratica tra il DPO e il punto di contatto CSIRT Italia? Si riuniscono con quale frequenza? Chi decide il contenuto delle notifiche?
2. I 44.872 record interessati sono titolari di dati italiani nella maggior parte? Vi sono giurisdizioni aggiuntive che devono essere notificate (Autorità di Protezione Dati di altri Stati membri)?
3. L'hash SHA-256 con salt mitiga il rischio per gli interessati? Giustifica la non comunicazione ai sensi dell'art. 34 GDPR?
4. Come si evita il ne bis in idem tra sanzione ACN (art. 38 DLgs) e sanzione Garante Privacy (art. 83 GDPR) per la stessa carenza di controllo? (Suggerimento: art. 35 NIS2.)
5. Chi è il portavoce unico? La stampa specializzata ha già la notizia — qual è la finestra tra notifica alle autorità e divulgazione pubblica?
6. Quanti ambienti di sviluppo esistono nell'organizzazione? Esiste un inventario? Qual è il ciclo di vita documentato di un ambiente dev?
7. Il reset forzato della password alla prossima sessione è tecnicamente fattibile in meno di 72 ore? Esiste un canale alternativo (SMS, email) per gli utenti che non effettuano il login?

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. Takedown immediato dell'indice Elasticsearch + IP block nell'infrastruttura perimetrale; raccolta dei log del bucket e del bilanciatore per l'analisi forense.

2. Convocare il DPO e l'organo di amministrazione per riunione congiunta — decisione formale di doppia notifica (NIS2 + GDPR) verbalizzata.
3. Trasmettere la pre-notifica al CSIRT Italia tramite piattaforma ACN (art. 25 c. 4 + c. 5 lett. a) DLgs 138/2024) entro 24 ore dalla decisione di qualificazione come incidente significativo. Criterio principale: art. 25 c. 2 DLgs, impatto sostanziale su dati personali.
4. Notificare il Garante Privacy ai sensi dell'art. 33 GDPR entro 72 ore, anche se la notifica NIS2 è già stata effettuata — sono procedure distinte. Il CSIRT Italia e il Garante si coordinano ai sensi dell'art. 35 NIS2.
5. Comunicare agli interessati ai sensi dell'art. 34 GDPR quando il rischio è elevato — banner sul portale + email + reset forzato della password alla prossima sessione.
6. Coordinare la comunicazione stampa con il portavoce unico; allineare il contenuto con il CSIRT Italia + Garante Privacy prima della diffusione.
7. Trasmettere la notifica completa (72h) al CSIRT Italia (art. 25 c. 5 lett. b) DLgs) con valutazione iniziale di gravità + indicatori di esposizione (14.000 record con scraping confermato).
8. Post-incidente: inventario completo degli ambienti di sviluppo; controllo degli accessi + segregazione delle reti; audit periodico aggiunto al piano annuale.

Riferimenti normativi

Funzioni Misure ACN (proxy NIST CSF)	DE · RS · ID
Articoli della Direttiva (UE) 2022/2555	• Article 21(2)(g) • Article 21(2)(i) • Article 23(4)(a) • Article 23(4)(b) • Article 35
Articoli del DLgs 138/2024	• art. 24 c. 2 lett. f) DLgs 138/2024 (igiene informatica e formazione) • art. 24 c. 2 lett. h) DLgs (controllo degli accessi e gestione degli attivi) • art. 25 c. 2 DLgs 138/2024 (criteri incidente significativo) • art. 25 c. 4 DLgs 138/2024 (pre-notifica 24h) • art. 25 c. 5 lett. b) DLgs (notifica 72h) • art. 35 NIS2 (coordinamento CSIRT Italia / Garante Privacy) • art. 38 DLgs 138/2024 (sanzioni)

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