Reglyze

Esercitazione tabletop NIS 2 / DLgs 138/2024 — Briefing — Accesso prolungato post-uscita — lacuna nell'offboarding

IT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-06-03T19:09:04.763Z

Classification: Confidential

Accesso prolungato post-uscita — lacuna nell'offboarding

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

Settore	**Generico (trasversale)**
Gravità	Significativo (incidente notificabile)
Durata suggerita	75 minuti
Identificativo	`it-minaccia-interna-offboarding`
Emesso il	03/06/2026

Contesto

Una PMI italiana del settore tecnologico (qualificata come soggetto importante ai sensi del DLgs 138/2024 — medie imprese che prestano servizi critici), con circa 220 dipendenti e fatturazione annuale di circa 25 milioni di euro, si classifica nell'Allegato II del DLgs (fornitori di servizi gestiti / MSP). L'esercizio presenta lo scenario archetipico di minaccia interna post-uscita: un collaboratore tecnico è uscito sei settimane fa, il suo account non è mai stato revocato, e ci sono evidenze di accessi notturni da un IP estero.

L'azienda non dispone ancora di un PAM (Privileged Access Management) formale. Il processo di offboarding esiste sulla carta ma non è stato seguito. Il contesto obbliga la squadra a navigare tre ambiti giuridici contemporaneamente: NIS2 (notifica CSIRT Italia entro 24 ore), Codice Penale (denuncia alla Polizia Postale per accesso abusivo a sistema informatico — art. 615-ter c.p.), e GDPR (potenziale violazione di dati personali se i file consultati includono dati di dipendenti o clienti).

L'esercizio è particolarmente rilevante per le PMI italiane in fase di maturazione cyber — illustra che il soggetto importante non sfugge agli obblighi di notifica NIS2 solo perché è più piccolo (è soggetto unicamente a vigilanza ex post ai sensi dell'art. 34 DLgs 138/2024).

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. 10:15. Il nuovo amministratore di sistema nota accessi notturni alla VPN con l'account di un collaboratore che ha lasciato l'azienda sei settimane fa. L'account non è mai stato disattivato. I log mostrano 19 sessioni nelle ultime quattro settimane, tutte da un IP di un paese estero. Alcune sessioni hanno toccato file sul server di condivisione — disegni, proposte commerciali, elenchi fornitori.	1
T+15min	T+15min. L'amministratore disattiva l'account immediatamente. Convoca il responsabile IT e l'amministratore delegato. Documenta i timestamp di tutte le sessioni. Non si sa ancora cosa sia	2

Momento	Iniezione	#
	stato esfiltrato — si sa solo che c'è stato accesso.	
T+1h	T+1h. L'amministratore delegato chiede se questo è un incidente significativo. L'azienda ha 220 dipendenti, fattura circa 25 milioni di euro all'anno, qualifica come soggetto importante ai sensi del DLgs 138/2024. Il Direttore Risorse Umane conferma che il processo di uscita del collaboratore è stato normale — non conflittuale, ma la checklist di offboarding ha fallito alla voce di revoca delle utenze tecniche.	3
T+4h	T+4h. L'analisi forense dettaglia i file a cui si è avuto accesso — 380 file, inclusa la proposta commerciale per il cliente principale in corso. Non c'è ancora conferma di esfiltrazione ma il pattern degli accessi è compatibile con una copia verso l'esterno. La direzione discute se denunciare alla Polizia Postale e al CSIRT Italia. L'ufficio legale valuta l'art. 615-ter c.p. (accesso abusivo a sistema informatico).	4
T+24h	T+24h. Decisione presa: pre-notifica al CSIRT Italia tramite piattaforma ACN (incidente significativo, impatto sostanziale su informazioni commerciali riservate + perdita di riservatezza di informazioni del cliente). Denuncia presentata alla Polizia Postale. Audit forense della postazione dell'ex collaboratore per identificare il canale di uscita dei file. Cliente principale informato in riunione dedicata.	5
T+72h	T+72h. Notifica completa (72h) al CSIRT Italia trasmessa. Polizia Postale conferma l'apertura dell'indagine. Piano di rientro: checklist di offboarding rivista (include ora la revoca di TUTTE le utenze tecniche entro 2 ore dall'uscita, validazione da parte di due colleghi); gestione dei privilegi rivista (strumento PAM da valutare); audit trimestrale delle utenze dormienti aggiunto al calendario. Cliente principale rafforza il contratto con clausola di notifica immediata.	6

Domande per la discussione

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

1. Esiste un inventario documentato di tutte le utenze con privilegi tecnici? Quando è stato l'ultimo audit delle utenze dormienti?
2. La checklist di offboarding prevede la revoca di TUTTE le utenze (non solo l'account di posta principale)? Include la validazione da parte di due colleghi?
3. Chi decide la denuncia? La direzione da sola? L'avvocato dell'azienda è coinvolto nella decisione?
4. Quali file erano accessibili tramite la condivisione? Esiste una classificazione delle informazioni documentata? Esiste un controllo degli accessi basato sulla necessità di sapere?
5. Il cliente principale è stato informato in riunione dedicata — chi ha partecipato? Quale documentazione scritta è stata registrata?
6. L'organizzazione ha MFA su tutte le utenze tecniche? Su tutte le utenze amministrative? Sulla VPN? L'ex collaboratore è riuscito ad accedere — cosa ha fallito?
7. Come si documenta la decisione dell'organo di amministrazione (art. 23 c. 1 DLgs) di qualificare l'incidente come significativo, dato che il soggetto importante è soggetto a vigilanza ex post (art. 34 DLgs)?

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. Disattivare immediatamente l'account dell'ex collaboratore + forzare il reset MFA su tutte le utenze con privilegi tecnici.
2. Convocare Direzione + Risorse Umane + Ufficio Legale in riunione congiunta. Verbalizzare formalmente la decisione di qualificazione come incidente significativo (art. 23 c. 1 DLgs — responsabilità dell'organo di amministrazione).
3. Trasmettere la pre-notifica al CSIRT Italia tramite piattaforma ACN (art. 25 c. 4 DLgs 138/2024) — il soggetto importante notifica con le stesse scadenze del soggetto essenziale. Criterio: art. 25 c. 2 DLgs (impatto sostanziale su informazioni riservate).
4. Presentare denuncia alla Polizia Postale ai sensi dell'art. 615-ter c.p. (accesso abusivo a sistema informatico); preservare la catena di custodia per il supporto processuale.
5. Raccogliere prove forensi: immagine della postazione dell'ex collaboratore, log del server di condivisione, log della VPN, log del gateway email, registri dell'EDR.
6. Informare il cliente interessato in riunione dedicata — non via email — prima di qualsiasi diffusione pubblica; rivedere le clausole di riservatezza del contratto.
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. Revisione completa della procedura di offboarding: clausola di revoca entro 2 ore, validazione da parte di due colleghi, audit trimestrale delle utenze dormienti, policy PAM/MFA per utenze tecniche.

Riferimenti normativi

Funzioni Misure ACN (proxy NIST CSF)	PR · DE · RS · ID
Articoli della Direttiva (UE) 2022/2555	• Article 21(2)(g) • Article 21(2)(i) • Article 21(2)(j) • Article 23(4)(a) • Article 23(4)(b) • Article 33
Articoli del DLgs 138/2024	• art. 23 c. 1 DLgs 138/2024 (obblighi organo di amministrazione — soggetto importante ugualmente) • art. 24 c. 2 lett. f) DLgs (igiene informatica + formazione) • art. 24 c. 2 lett. h) DLgs (controllo degli accessi + gestione degli attivi) • art. 24 c. 2 lett. i) DLgs (MFA + comunicazioni sicure) • art. 25 c. 4 DLgs 138/2024 (pre-notifica 24h — anche per soggetto importante)

	• art. 25 c. 5 lett. b) DLgs (notifica 72h) • art. 25 c. 5 lett. d) DLgs (relazione finale entro un mese) • art. 34 DLgs 138/2024 (vigilanza ex post su soggetto importante)

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