Reglyze

Esercitazione tabletop NIS 2 / DLgs 138/2024 — Briefing — DDoS contro portale comunale — amministrazione pubblica

IT Tabletop Scenario

Organization: Reglyze

Version: v1

Date: 2026-06-03T19:08:03.473Z

Classification: Confidential

DDoS contro portale comunale — amministrazione pubblica

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

Settore	**Piattaforma SCADA / ICT**
Gravità	Mite (addestramento base)
Durata suggerita	60 minuti
Identificativo	`it-ddos-comune-pa`
Emesso il	03/06/2026

Contesto

Un Comune italiano (circa 550 dipendenti, circa 75.000 abitanti) gestisce i portali di servizio al cittadino online, la piattaforma di prenotazione appuntamenti, i servizi finanziari locali e indirettamente i servizi idrici comunali. Il Comune rientra nell'ambito soggettivo del DLgs 138/2024 in quanto amministrazione pubblica (art. 3 c. 2 lett. j — le amministrazioni pubbliche centrali e regionali, nonché gli enti locali con funzioni essenziali).

L'esercizio è un DDoS volumetrico + livello 7 che perturba i portali di servizio ma non tocca l'infrastruttura OT dell'acqua. È deliberatamente uno scenario 'mild' rispetto ai precedenti — l'obiettivo è allenare l'articolazione con il CSIRT Italia, il piano B di sportello fisico, la comunicazione ai cittadini tramite canali ufficiali, e il riflesso di notifica al CSIRT Italia anche quando l'impatto è principalmente di disponibilità amministrativa.

Illustra anche le specificità del DLgs 138/2024 per le amministrazioni pubbliche: l'art. 3 c. 2 estende l'ambito soggettivo della direttiva NIS 2 includendo le PA centrali e locali tra i soggetti essenziali — un'estensione specifica della trasposizione italiana rispetto alla NIS 2.

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. 09:10. I portali di servizio al cittadino del Comune iniziano a restituire errori 503. Il CDN segnala traffico anomalo: picco di 16 Gbps con pattern SYN flood + L7 GET burst sul portale di prenotazione online. I funzionari allo sportello informano che le liste di chiamata della piattaforma di prenotazione non funzionano.	1
T+15min	T+15min. Il CDN ha attivato la mitigazione automatica ma il traffico continua. Il portale principale è intermittente. Il centralino si riempie. L'Assessore alla Transizione Digitale chiede un punto di	2

Momento	Iniezione	#
	situazione.	
T+1h	T+1h. Il CSIRT Italia conferma di osservare un cluster di DDoS contro portali di enti locali in diverse regioni. Attribuzione preliminare a un gruppo hacktivista da messaggi su forum. Il Comune gestisce anche i servizi idrici — quei sistemi (OT) sono intatti. L'attacco è esclusivamente contro i servizi amministrativi.	3
T+4h	T+4h. Mitigazione CDN potenziata (regole WAF L7 + scrubbing center upstream). Traffico malevolo ridotto del circa 80%. I portali tornano a rispondere. Piano B di sportello fisico rafforzato: numeri su carta; procedimenti prioritari (certificati di stato civile, rilascio CIE) con precedenza. La stampa locale chiede dichiarazioni.	4
T+24h	T+24h. Pre-notifica trasmessa al CSIRT Italia tramite piattaforma ACN — il Comune in quanto amministrazione pubblica rientra nell'ambito soggettivo del DLgs 138/2024 (art. 3 c. 2 lett. j). L'Assessore comunica in conferenza stampa. Indagine preliminare con il CSIRT Italia in corso. Il piano di continuità dello sportello è stato mantenuto durante il picco.	5
T+72h	T+72h. Notifica completa (72h) al CSIRT Italia trasmessa. Mitigazione stabilizzata; portali operativi normalmente. L'attacco si è esaurito. Lezioni apprese: la capacità contrattata del CDN era sottodimensionata; il runbook di comunicazione ai cittadini necessita revisione; il piano B cartaceo ha funzionato ma ha limiti di scala. Relazione finale in preparazione entro un mese (art. 25 c. 5 lett. d) DLgs 138/2024).	6

Domande per la discussione

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

1. Il Comune rientra nell'ambito soggettivo del DLgs 138/2024? In quale categoria (art. 3 c. 2)? Chi è stato formalmente notificato di questo inserimento?
2. Qual è la capacità di scrubbing contrattata con il CDN? È stata sufficiente per il picco di 16 Gbps? Qual è lo SLA di escalation verso lo scrubbing center upstream?
3. Chi è il portavoce sui canali social ufficiali del Comune durante un incidente cyber? Esiste un runbook documentato per questa articolazione?
4. Il piano B di sportello fisico cartaceo — qual è la sua capacità reale? In quanto tempo si esaurisce se il portale è fuori servizio per 24 ore?
5. Il Comune gestisce i servizi idrici — quei sistemi hanno un punto di contatto distinto con il CSIRT Italia? C'è duplicazione di notifica?
6. Quali IOC si condividono con il CSIRT Italia? Su quale canale? In quale formato (MISP, STIX, email)?
7. Come si documenta la decisione dell'organo di amministrazione per qualificare l'incidente come significativo ai sensi dell'art. 25 c. 2 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. Attivare la mitigazione CDN/WAF ai livelli massimi contrattati; scalare verso lo scrubbing center upstream se disponibile.
2. Comunicare ai cittadini tramite SMS + canali social ufficiali + media locali: portali intermittenti, piano B di sportello fisico attivo, numeri prioritari.
3. Trasmettere la pre-notifica al CSIRT Italia tramite piattaforma ACN (art. 25 c. 4 DLgs 138/2024) — le amministrazioni pubbliche notificano con le stesse scadenze.
4. Mantenere lo sportello fisico rafforzato durante il picco; dare precedenza ai servizi critici (certificati di stato civile, CIE, urbanistica d'emergenza); registrare le pratiche manualmente per la sincronizzazione successiva.
5. Comunicare con la Prefettura e le autorità competenti; allineare le dichiarazioni pubbliche con il CSIRT Italia prima della conferenza stampa.
6. Coordinare con il CSIRT Italia nell'attività di attribuzione + firma tecnica dell'attacco (IOC condivisibili con altri enti colpiti).
7. Trasmettere la notifica completa (72h) al CSIRT Italia (art. 25 c. 5 lett. b) DLgs) con valutazione di gravità + indicatori; relazione finale entro un mese dalla cessazione dell'impatto (art. 25 c. 5 lett. d) DLgs).
8. Post-incidente: rivedere la capacità contrattata del CDN; rivedere il runbook di comunicazione ai cittadini; validare il piano B cartaceo in un esercizio di stress; documentare la decisione dell'organo di amministrazione.

Riferimenti normativi

Funzioni Misure ACN (proxy NIST CSF)	PR · DE · RC
Articoli della Direttiva (UE) 2022/2555	• Article 21(2)(c) • Article 21(2)(j) • Article 23(4)(a) • Article 23(4)(b)
Articoli del DLgs 138/2024	• art. 3 c. 2 lett. j) DLgs 138/2024 (amministrazioni pubbliche nell'ambito soggettivo) • art. 24 c. 2 lett. b) DLgs (continuità operativa e gestione delle crisi) • art. 24 c. 2 lett. i) DLgs (autenticazione 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. 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