REPORT AGGIUNTIVO – PIANO DI DISASTER RECOVERY (SCENARIO: BLOCCO E-COMMERCE PER 2 ORE)

Cliente: Nencini Sport S.P.A
Data: 10/07/2025
Consulente di Sicurezza Informatica: Andrea Giovannoni

---

1. Obiettivo del documento

Il presente documento definisce un piano di Disaster Recovery (DR) specifico per l'infrastruttura e-commerce, volto a garantire il ripristino del servizio entro 2 ore in caso di indisponibilità totale derivante da incidente informatico (es. attacco DDoS, infezione ransomware, failure infrastrutturale).

Il piano è costruito in conformità alle best practice di business continuity secondo i framework:

- **ISO/IEC 27001:2022**
- **NIST SP 800-34 Rev.1**
- **Cyber Resilience Act (EU)**

---

2. Obiettivi critici: RTO & RPO

Obiettivo	Descrizione
RTO (Recovery Time Objective)	2 ore – tempo massimo entro cui deve essere ripristinato il servizio
RPO (Recovery Point Objective)	15 minuti – perdita massima accettabile di dati

3. Analisi di impatto (BIA)

Voce	Valore stimato
Fatturato medio per minuto	€ 1.500
Durata interruzione prevista	120 minuti
Perdita stimata	**€ 180.000**

Oltre alla perdita economica diretta, si considerano impatti reputazionali, SLA violati e deterioramento della customer experience.

---

4. Inventario degli asset critici

Asset	Funzione
Web Application (frontend e backend)	Interfaccia utente e logica e-commerce
Database e ordini	Gestione ordini, clienti, prodotti
API di pagamento	Integrazione con circuiti bancari
DNS e CDN	Distribuzione del traffico
SIEM / SOAR	Monitoraggio e risposta agli incidenti

---

5. Struttura del team di risposta

Ruolo	Responsabilità
Disaster Recovery Manager	Dichiarazione stato di emergenza, coordinamento
Responsabile Infrastruttura IT	Attivazione backup, replica o failover
Security Analyst (SOC)	Analisi root cause, verifica integrità post-evento
Responsabile Comunicazione	Comunicazioni interne ed esterne
Supporto esterno	Provider cloud, DNS, WAF, SOC as a Service

6. Strategia di Recovery

6.1. Replica e Failover

- Attivazione di un **sito secondario** preconfigurato (warm site) in ambiente cloud.
- Replicazione asincrona dei dati (con RPO ≤ 15 min).
- Configurazione DNS con **TTL ≤ 300s** per switching rapido.
- Infrastruttura containerizzata per garantire provisioning immediato.

6.2. Backup & Storage

- Backup giornalieri full + incrementali ogni 15 min.
- Archiviazione cifrata su storage off-site con retention minima di 7 giorni.
- Testing mensile dei backup con validazione file system e integrità dati.

---

7. Procedura operativa (Runbook semplificato)

Minuto	Azione
0’	Allerta automatica SIEM / SOAR
+5’	DR Manager dichiara stato di emergenza
+10’	Attivazione replica DB e redirect DNS
+30’	Deploy automatico del sito secondario
+60’	Test funzionali e accesso interno QA
+90’	Ripristino operativo e monitoraggio attivo
+120’	Completamento Recovery – fase post mortem

8. Comunicazione e coordinamento

- **Comunicazione interna**: aggiornamenti via Slack/Teams ogni 30 minuti.
- **Comunicazione clienti**: avviso tramite banner applicativo e newsletter.
- **Stakeholder**: invio report riepilogativo entro 4 ore dalla chiusura dell'incidente.

---

9. Testing e validazione

- Esecuzione di test DR completi **trimestralmente**, con validazione dei tempi reali di RTO e RPO.
- Simulazione failover DNS + recovery da warm-site in ambiente isolato.
- Reporting e aggiornamento continuo del playbook di recovery.

---

10. Integrazione con architettura esistente

Il piano DR è progettato per integrarsi con:

- **SIEM** (Wazuh o Sentinel) e **SOAR** (TheHive + Cortex) per automazione alerting.
- **Firewall e WAF** configurati per riconfigurazione rapida delle ACL in fase di recovery.
- **Segmentazione DMZ/rete interna** per garantire isolamento delle fasi di recovery.

---

11. Misurazione delle prestazioni (metriche di resilienza)

Metrica	Obiettivo	Misura
MTTR (Mean Time to Recovery)	≤ 120 min	Monitorato
MTTD (Time to Detect)	≤ 1 min	SOAR alert
MTTA (Time to Acknowledge)	≤ 10 min	SOC operativo

RTO	≤ 2 ore	Verificato in test trimestrale
RPO	≤ 15 min	Validato via snapshot

---

12. Conclusione

Il presente piano consente all’organizzazione di rispondere con rapidità e precisione ad attacchi informatici o guasti critici, garantendo il ripristino dell’e-commerce entro 2 ore, con perdita dati minima e un impatto contenuto sulla continuità operativa e sulla reputazione aziendale.

Il piano è pronto per essere attivato, testato e continuamente aggiornato secondo evoluzione tecnologica e rischio aziendale.