EXE.IT Srl Sb

cyberglobal italy

CASE STUDY

Sommario

Cliente 2

Richiesta 2

Case Study 2

Servizio 2

Obiettivo 2

La sfida 3

La soluzione CyberGlobal 4

I risultati 5

Dall'assessment alla remediation 6

La verifica finale: il Retest 6

Benefici per il cliente 7

Il valore aggiunto di CyberGlobal 7

La piattaforma Poolpo 8

A. Test di sicurezza - Penetration testing 9

B. Test di robustezza - Load Testing 9

C. Test di resilienza - Disaster Recovery e backup 9

C.1. Verifica Backup e DR 10

C.2. Verifica dei dati presenti nel DR 11

C.3. Verifica dei Punti di ripristino nel DR 11

Cliente

Istituto di Scienze e Tecnologie della Cognizione del Consiglio Nazionale delle Ricerche (ISTC-CNR Italia) d'ora in poi Cliente.

Richiesta

Valutazione tecnica della sicurezza, robustezza e resilienza della piattaforma Poolpo per garantire la solidità, la conformità alle normative e la continuità del servizio.

Case Study

Come un Web Application Penetration Test ha rafforzato la sicurezza di un'applicazione business-critical.

Servizio

Web Application Penetration Test, sviluppo, implementazione ambiente virtuale.

Obiettivo

Valutare in maniera indipendente il livello di sicurezza di una web application esposta su Internet, identificare le vulnerabilità potenzialmente sfruttabili e supportare il cliente nel percorso di remediation fino alla verifica dell'efficacia delle contromisure implementate.

La sfida

La trasformazione digitale porta le organizzazioni a rendere disponibili applicazioni sempre più complesse e accessibili via Internet. Sebbene queste piattaforme siano essenziali per il business, rappresentano anche uno dei principali punti di ingresso per potenziali attaccanti.

Il Cliente desiderava ottenere una valutazione indipendente della sicurezza della propria applicazione web per:

- comprendere il livello reale di esposizione ai rischi cyber;
- verificare la presenza di vulnerabilità sfruttabili;
- identificare eventuali debolezze nella logica applicativa e nelle configurazioni di sicurezza;
- ricevere indicazioni operative per ridurre il rischio prima che le vulnerabilità potessero essere sfruttate.

L'obiettivo non era semplicemente individuare vulnerabilità, ma migliorare concretamente la postura di sicurezza dell'applicazione attraverso un percorso strutturato di assessment, remediation e validazione.

La soluzione CyberGlobal

CyberGlobal ha eseguito un **Web Application Penetration Test** seguendo un approccio metodologico basato sui principali standard internazionali, tra cui **OWASP Testing Guide**, **PTES**, **OSSTMM**, **NIST**, **CREST**, **PCI DSS** e **OWASP ASVS**.

L'assessment è stato condotto da Security Consultant certificati attraverso un processo strutturato che combina competenze offensive, analisi manuali e strumenti specializzati.

L'intero assessment è stato eseguito attraverso un processo articolato in più fasi.

1. Intelligence Gathering

2. Vulnerability Assessment

3. Controlled Exploitation

4. Reporting e Remediation Guidance

I risultati

L'assessment ha individuato un totale di 18 finding, classificati secondo il livello di rischio.

Livello di rischio	Numero
Critical	0
High	0
Medium	4
Low	8
Informational	6

L'assenza di vulnerabilità **Critical** e **High** ha confermato che l'applicazione non presentava vulnerabilità immediatamente sfruttabili con impatti elevati.

Le vulnerabilità di livello **Medium** e **Low** hanno evidenziato opportunità di miglioramento relative principalmente a configurazioni di sicurezza, hardening dell'applicazione e rafforzamento dei controlli di protezione.

Le evidenze di tipo **Informational** hanno inoltre fornito indicazioni utili per incrementare ulteriormente la maturità complessiva della sicurezza applicativa.

Dall'assessment alla remediation

Uno degli elementi distintivi dell'intervento CyberGlobal è stato il supporto fornito durante la fase di remediation.

Per ciascun finding sono state condivise indicazioni tecniche dettagliate che hanno consentito al Cliente di:

- comprendere la causa della vulnerabilità;
- valutare il rischio associato;
- definire la priorità di intervento;
- implementare le contromisure più appropriate;
- adottare configurazioni allineate alle best practice OWASP e agli standard internazionali.

Questo approccio ha trasformato il penetration test in un vero percorso di miglioramento della sicurezza e non in una semplice attività di verifica.

La verifica finale: il Retest

Una volta completate le attività di remediation, CyberGlobal ha effettuato un Retest delle vulnerabilità precedentemente identificate.

L'obiettivo era verificare in modo indipendente che:

- le vulnerabilità fossero state effettivamente risolte;
- le contromisure implementate fossero efficaci;
- non fossero state introdotte regressioni;
- il livello di sicurezza dell'applicazione risultasse concretamente migliorato.

Il Retest rappresenta un passaggio fondamentale perché consente di validare l'intero processo di remediation e fornisce al cliente evidenze oggettive dell'efficacia degli interventi eseguiti.

Benefici per il cliente

Attraverso il progetto, il Cliente ha ottenuto:

- una valutazione indipendente e approfondita della sicurezza della propria web application;
- una chiara visibilità dei rischi reali associati all'applicazione;
- un piano di remediation strutturato e prioritizzato;
- indicazioni operative per il miglioramento continuo della sicurezza;
- la validazione indipendente delle attività correttive attraverso il retest;
- una riduzione della superficie di attacco e un rafforzamento della postura di cybersecurity.

Il valore aggiunto di CyberGlobal

CyberGlobal combina competenze offensive, metodologie riconosciute a livello internazionale e un approccio orientato al business per aiutare le organizzazioni a migliorare la propria resilienza cyber.

Ogni penetration test non rappresenta soltanto un'attività di verifica tecnica, ma un percorso strutturato volto a identificare, comprendere e ridurre il rischio, supportando il cliente dall'assessment iniziale fino alla validazione finale delle remediation implementate.

Security is not only about finding vulnerabilities. It's about enabling trust.

La piattaforma Poolpo

La piattaforma Poolpo, progettata e sviluppata da Indici Opponibili (www.indiciopponibili.com) all'interno dei progetti **Fostering Open Science in Social Science Research** (FOSSR) e **Growing Resilient, Inclusive and Sustainable** (GRINS) finanziati tramite i fondi del PNRR), è ospitata nel Data Center 00Gate di EXE.IT Srl Sb (www.exe.it), che si è occupata dell'implementazione dell'ambiente virtuale, delle attività di seguito descritte e del coordinamento con gli altri attori coinvolti (nello specifico CyberGlobal).

La piattaforma Poolpo è stata sottoposta a:

- Test di sicurezza (Penetration Testing) per identificare e mitigare vulnerabilità potenziali.
- Test di robustezza (Load Testing) per valutare la capacità della piattaforma di resistere a carichi elevati e scalare in base alle esigenze future.
- Test di resilienza (Disaster Recovery e backup) condotti dal team infrastrutturale di EXE.it Srl Sb, che hanno confermato l'efficacia delle procedure di backup, replica e ripristino. Sono stati verificati RPO (Recovery Point Objective) e RTO (Recovery Time Objective).

Questa valutazione rappresenta un punto di partenza fondamentale per assicurare che la piattaforma Poolpo operi in modo sicuro, affidabile e conforme alle aspettative, sia in condizioni normali che in scenari critici.

A. Test di sicurezza - Penetration testing

I risultati hanno evidenziato alcune vulnerabilità, prese in carico dal team di sviluppo della piattaforma Poolpo e con una roadmap di risoluzione concordata con gli stakeholders accademici.

I report finali dei test condotti, così come eventuali aggiornamenti, sono visibili presso la dashboard di monitoraggio dello stato della piattaforma consultando il tag “pen-test”: https://status.poolpo.it/reports/?tags=pen-test

B. Test di robustezza - Load Testing

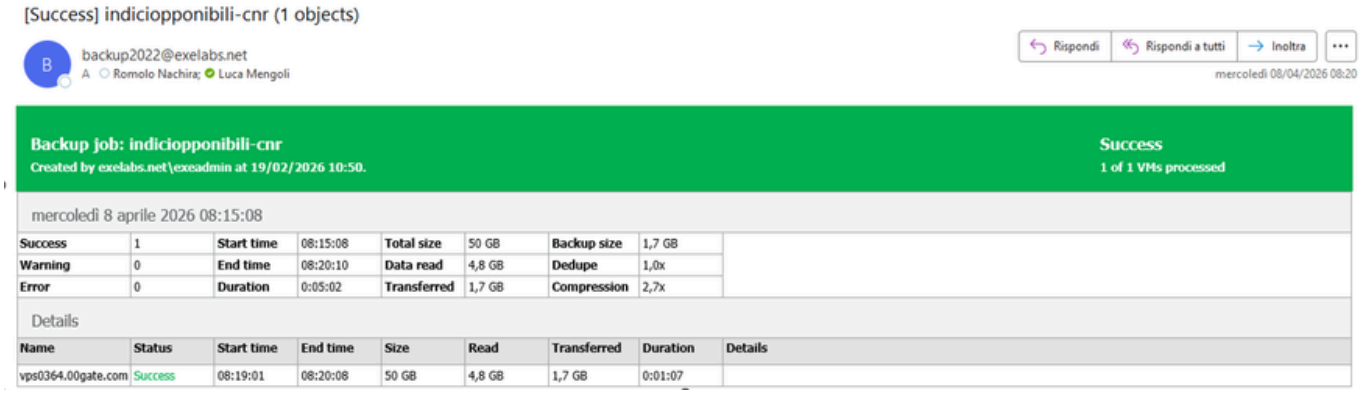
I test hanno provato la robustezza della piattaforma evidenziando tuttavia diverse possibili strade di miglioramento sia in termini di resistenza al carico che di scalabilità futura della piattaforma.

C. Test di resilienza - Disaster Recovery e Backup

La piattaforma Poolpo è stata sottoposta a una valutazione approfondita delle proprie procedure di Disaster Recovery (DR) e backup, al fine di garantire affidabilità e continuità del servizio in scenari critici. Nei paragrafi successivi si dettaglia quanto eseguito.

C.1. Verifica Backup e DR

L'ambiente virtuale ospitante app.poolpo.it ha un backup che viene effettuato ogni 4 ore, quando finisce viene fatta la replica nel datacenter a Ponte San Pietro (BG), sotto si possono vedere le immagini del backup e della successiva replica a Milano.



[Success] indiciopponibili-cnr (1 objects)

backup2022@exelabs.net
A Romolo Nachira; Luca Mengoli

Rispondi | Rispondi a tutti | Inoltra
mercoledì 08/04/2026 08:20

Backup job: indiciopponibili-cnr
Created by exelabs.net\exeadmin at 19/02/2026 10:50.

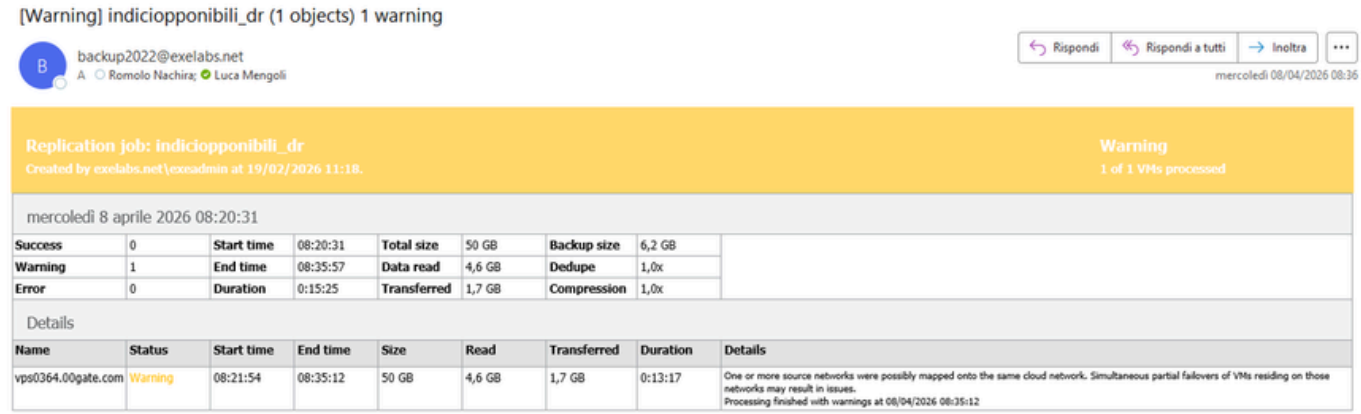
Success
1 of 1 VMs processed

mercoledì 8 aprile 2026 08:15:08

Success	1	Start time	08:15:08	Total size	50 GB	Backup size	1,7 GB
Warning	0	End time	08:20:10	Data read	4,8 GB	Dedupe	1,0x
Error	0	Duration	0:05:02	Transferred	1,7 GB	Compression	2,7x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
vps0364.00gate.com	Success	08:19:01	08:20:08	50 GB	4,8 GB	1,7 GB	0:01:07	



[Warning] indiciopponibili_dr (1 objects) 1 warning

backup2022@exelabs.net
A Romolo Nachira; Luca Mengoli

Rispondi | Rispondi a tutti | Inoltra
mercoledì 08/04/2026 08:36

Replication job: indiciopponibili_dr
Created by exelabs.net\exeadmin at 19/02/2026 11:18.

Warning
1 of 1 VMs processed

mercoledì 8 aprile 2026 08:20:31

Success	0	Start time	08:20:31	Total size	50 GB	Backup size	6,2 GB
Warning	1	End time	08:35:57	Data read	4,6 GB	Dedupe	1,0x
Error	0	Duration	0:15:25	Transferred	1,7 GB	Compression	1,0x

Details

Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
vps0364.00gate.com	Warning	08:21:54	08:35:12	50 GB	4,6 GB	1,7 GB	0:13:17	One or more source networks were possibly mapped onto the same cloud network. Simultaneous partial failovers of VMs residing on those networks may result in issues. Processing finished with warnings at 08/04/2026 08:35:12

Per il DR si può notare che c'è un messaggio di Warning che non è un problema, ma sta indicando che la VLAN in cui è stata creata la VM fa parte di una rete nella quale ci potrebbero essere altre VM ed è un messaggio che si può considerare normale dato che si trova in un datacenter utilizzato come destinazione di vari DR.

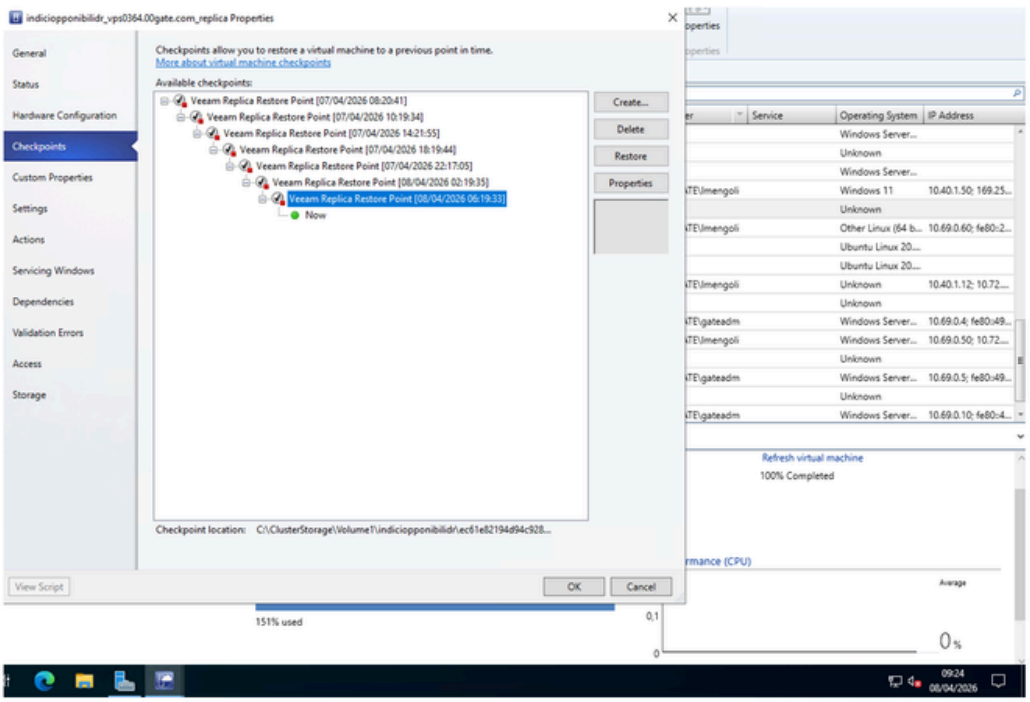
C.2. Verifica dei dati presenti nel DR

Per verificare la consistenza dei dati abbiamo acceso la VM nel datacenter remoto e siamo andati a verificare che nei log del sito sia appunto indicato come ultimo accesso l'orario antecedente al backup che abbiamo allegato al documento.



C.3. Verifica dei Punti di ripristino nel DR

Come ultima verifica abbiamo fatto un check dei recovery point presenti presso il datacenter a Ponte San Pietro (BG) in modo da verificare che ci siano i 7 punti che abbiamo impostato nella regola di DR in modo da avere in caso di bisogno la macchina allo stato del giorno precedente. Di seguito è possibile visionare lo screenshot.



Con queste informazioni possiamo indicare che abbiamo un RPO di 4 ore e un RTO al momento che si può attestare su un'ora circa.