Bologna, 14 marzo 2025

Il presente documento descrive i servizi in oggetto in riferimento al “disciplinare tecnico in materia di misure minime di sicurezza ”, allegato B della legge 196.

Applicazione e Server

Il Mondo degli Elli è un'applicazione web based ospitata in un sistema ad architettura Cloud server ridondante multiprocessore multicore con connettività a banda illimitata, max 100MB/sec.
Il server è virtualizzato all'interno di un cluster: un eventuale crash di una macchina fisica non sarà percepito dall'utente finale in quanto tutto il sistema è replicato su un cluster di più macchine fisiche.

Backup del database e degli allegati

Indipendentemente dal clustering, ogni notte viene effettuato in automatico un backup del database consistente nel suo dump in formato SQL, compresso con compressione gzip: ad ogni backup viene creato un file nuovo in maniera tale da rendere possibile il reperimento di dati vecchi, o il ripristino della situazione ad una determinata data. Tali backup vengono mantenuti per un mese: superato il quale, viene mantenuto solo il backup relativo al primo giorno di ogni mese.

Sicurezza del Server

Il server che ospita l'applicazione ha aperte dall'esterno verso l'interno esclusivamente le seguenti porte:

- 22 per le comunicazioni SSH
- 80 per le comunicazioni HTTP
- 443 per le comunicazioni HTTPS

Il filtraggio dei pacchetti IP è affidato ad un firewall esterno.

Sistema di log

I log dell'applicazione sono salvati su file all'interno del database. I log di errori gravi vengono inviati automaticamente alle persone incaricate.
Per mantenere validi i log di accesso, l'orologio del server è mantenuto sincronizzato tramite timesyncd.

A ulteriore protezione

- Il monitoraggio sulla capacità e il funzionamento del server e dell'applicazione avviene in automatico ogni 5 minuti tramite CheckMk. Eventuali anomalie vengono segnalate immediatamente alle persone incaricate.
- Il server web è configurato con un blocco contro gli attacchi DOS;
- Il server web e il servlet container sono configurati per permettere l'accesso diretto solo alle servlet del programma e ai file relativi alla grafica dello stesso (GIF, CSS e simili). Ogni altro tipo di accesso (in particolare l'accesso a ogni tipo di allegato) è sempre filtrato dal gestore dei permessi dell'applicazione.

L'accesso SSH è consentito solo a tre account (nessuno dei quali è root) con password ad alta sicurezza.

Conformità alla legge 196

Ad ogni operatore è richiesta una credenziale di autenticazione tramite inserimento di username e password: la parola chiave deve essere composta obbligatoriamente da almeno otto caratteri e deve contenere almeno una lettera ed un numero. Tale parola chiave è impostata direttamente dall'operatore e deve essere aggiornata dallo stesso con cadenza trimestrale: il sistema stesso impone il cambio della password ogni 3 mesi, e non permette la registrazione della stessa password. Solo l'operatore conosce la propria password e neanche l'amministratore di sistema è in grado di poterla ricavare: sarà responsabilità dell'operatore stesso mantenere la segretezza sulla propria password. Credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate, ad eccezione di quelle preventivamente autorizzate per soli scopi di gestione tecnica.
I dati personali idonei a rivelare lo stato di salute e la vita sessuale sono separati dagli altri dati personali del paziente essendo allocati in diverse tabelle di un database relazionale.
Dal punto di vista tecnico, avranno possibilità di accesso ai dati per motivi di gestione e manutenzione i soli dipendenti Anastasis autorizzati dal cliente tramite compilazione e firma del modulo preposto fornito dal cliente stesso. In attesa, o in assenza di tale modulo, si notifica che le persone incaricate sono:

- Andrea Frascari, nato a Bologna il 23/0/1970, CF FRSNDR70P23A944M
- Vincenzo Carnazzo, nato a Milazzo il 2/9/1980, CF CRNVCN80P02F206D
- Enzo Ferrari, nato a Bologna il 30/09/1971, CF FRRNZE71P30A944H

Tale personale è formato a aggiornato sulle tematiche della sicurezza e riservatezza dei dati.
I server risiedono fisicamente in una web-farm: per ogni accesso ai server, sia fisico che software, il personale della web farm richiede autorizzazione scritta ad Anastasis.
Server, relativi strumenti anti-intrusione e applicazione sono aggiornati con cadenza almeno semestrale. Il salvataggio dei dati avviene su base giornaliera.
Il sistema prevede la possibilità di creare diversi profili di autorizzazione per l'accesso ai dati. Tali profili riguardano ciascun incaricato o classi omogenee di incaricati e sono individuati e configurati anteriormente all'attività operativa, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni previste. In particolare, l'operatore è riconosciuto ed abilitato a determinate operazioni su determinati dati in base ai gruppi a cui appartiene, e, indirettamente, in base ai profili associati a questi gruppi, che determinano i permessi.
In particolare ogni gruppo di operatori avrà accesso unicamente ai dati degli utenti da loro stessi inseriti ovvero agli utenti inseriti da operatori appartenenti allo stesso gruppo. Non sarà possibile in alcun modo avere accesso ad altri dati.
In aggiunta alla conformità alla legge 196, il sistema è stato progettato con criteri di robustezza rispetto ai principali tipi di attacchi web (SQL injection, cross-site scripting, command injection etc.).

Data Center in cui risiedono i dati

I data center su cui risiedono i dati del Mondo degli Elli sono collocati esclusivamente nei Paesi che appartengono all'Unione Europea, nello specifico:

- Il Mondo degli Elli è ospitato presso il datacenter di Francoforte (Germania) gestito da OVH.
- I backup sono ospitati presso il datacenter di Helsinki (Finlandia) gestito da Hetzner.

La percentuale di funzionamento del servizio che viene garantita in un anno è del 99,7%, che vuol dire all'incirca 1 giorno di down su 365.

OVH ha ricevuto le certificazioni ISO 27001, ISO 27017 e ISO 27018. Maggiori informazioni: https://www.ovhcloud.com/it/compliance/iso-27001-27017-27018/

Riferimenti per il Data Privacy Framework relativo ai servizi OVH: https://www.ovhcloud.com/it/compliance/ .

Hetzner ha ricevuto la certificazione ISO 27001. Maggiori informazioni: https://docs.hetzner.com/general/others/certificates/

Riferimenti per il Data Privacy Framework relativo ai servizi Hetzner: https://www.hetzner.com/legal/privacy-policy .

Soggetto designato ex art. 29 del GDPR al trattamento dei dati con funzione specifica e delega per la gestione e l'applicazione del Regolamento UE 779/2016, con apposita delibera del CdA in data 10/07/23

Tullio Maccarrone