DOMANDE FREQUENTI SU CRITTOGRAFIA E LOG

- **Viene mantenuto il logging di tutte le attività?**

Il progetto realizzato si basa su un progetto di ricerca avanzata in materia privacy e sicurezza. Come tale, i log effettuati sono ricercati per essere *privacy preserving by design*. Ergo, per ogni azione registrata è previsto di mantenere l'id dell'utente che l'ha effettuata il tipo di azione e l'oggetto dell'azione. Per le ragioni descritte alcune delle implementazioni dei log sono ancora in fase di completamento.

Lo stato completo dell'implementazione e della ricerca è visibile all'indirizzo: https://github.com/globaleaks/GlobaLeaks/issues?q=audit+log.

- **I log sono cifrati?**

I log mantenuti non contengono elementi sensibili e come tale non è implementata crittografia. È in corso di ricerca continua l'estensione di questo modello, aggiungendo eventuali dati a maggiore sensibilità che richiederebbero dunque opportuna cifratura.

Vedasi corrente stato della ricerca in materia audit log: https://github.com/globaleaks/GlobaLeaks/issues?q=audit+log.

- **Quali sono i soggetti che possono accedere ai log?**

Due soli amministratori, tra cui il CTO di progetto.

- **Tramite i log di accesso si può dedurre l'identità del segnalante?**

No, nessuno dei log mantiene informazioni sensibili a livello privacy. Ad esempio, non viene mantenuto IP, lingua, user agent o altre informazioni sensibili per il segnalante.

- **Il fornitore garantisce la continuous availability?**

Si. Ogni istanza è monitorata per rilevare anomalie ogni 5 minuti, con intervento entro 3 minuti e backup giornalieri, settimanali e mensili per coprire gli ultimi 3 giorni, le ultime 3 settimane e gli ultimi 3 mesi.

- **Chi detiene le chiavi di crittografia?**

Per quel che concerne le segnalazioni queste sono crittografate secondo modello crittografico qui dettagliato: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

Solo i soggetti riceventi possono accedere al contenuto delle segnalazioni.

Solo gli amministratori possono eventualmente supportare i riceventi nel recupero del proprio account senza però avere visibilità diretta alle segnalazioni e avendo le proprie stesse azioni soggette a tracciamento.

- **Quali le caratteristiche relative alla creazione e alla gestione delle credenziali del segnalante?**

Il segnalante in fase di segnalazione riceve una ricevuta anonima (codice a 16 cifre) valido nel tempo di vita della segnalazione a sistema (1 anno e 6 mesi, rinnovabile a discrezione del ricevente).

Vedasi https://docs.globaleaks.org/en/main/security/ApplicationSecurity.html.

- **Sono stati condotti Vulnerability Assessment e Penetration test? A quando risale l'ultimo?**

Il progetto gode di 6 penetration test di fama internazionale: https://docs.globaleaks.org/en/main/security/PenetrationTests.html.

Ciascun progetto realizzato partecipa tipicamente nel finanziare un audit indipendente; non tutti i report sono purtroppo pubblici/pubblicabili.

- **È stata svolta una DPIA approfondita? A quando risalgono la DPIA e l'ultima rivalutazione effettuata?**

Sì, ad esempio in progetti realizzati nel settore privato nel 2020 con RINA, ENAV, Gruppo Sole 24 Ore, Cameo.

È in corso di realizzazione un template DPIA esauriente che verrà reso pubblicamente fruibile per fini di assessment e documentazione interna da parte degli enti aderenti.