ARCHITETTURA DEL SOFTWARE E DELL'INFRASTRUTTURA – WHISPER

SOFTWARE - La Thorsoft S.r.l. è la proprietaria e sviluppatrice esclusiva della Piattaforma Whisper per il Whistleblowing, che è stata completamente creata senza l'utilizzo di applicativi open source.

I linguaggi impiegati includono MySql per la gestione dei dati personali, mentre il backend è stato implementato in linguaggio JAVA su un serverlet container Tomcat. Il frontend, invece, è stato sviluppato in React.

Java è stato attentamente progettato con un focus sulla sicurezza. La Java Virtual Machine (JVM) applica restrizioni rigorose sull'accesso alla memoria e al database, offrendo meccanismi di sicurezza che preven-gono molti errori e vulnerabilità comuni.

HARDWARE - L'applicazione è in hosting su cloud server di AWS con SO Unix/Linux.

AWS è un hosting performante con risorse scalabili.

Il cloud server adotta dischi entreprise SSD NVMe che garantiscono le migliori performance per l'applicazione.

Attraverso AWS è stata implementata una procedura di disaster recovery che prevede la ridondanza di server e backup dati, con migrazione su un nodo alternativo in caso di necessità senza interruzione del servizio.

INFRASTRUTTURA - Le risorse di AWS sono fisicamente allocate a Milano e sono basate su prodotti enterprise e tecnologia certificata. AWS adotta le soluzioni di punta del mercato per garantire prestazioni elevate in termini di velocità, stabilità e sicurezza. La connettività dei sistemi è garantita al 99,99% di uptime.

FORNITORI (RESPONSABILI DEL TRATTAMENTO) INFRATTRUTTURE TECNOLOGICHE

I fornitori software sono designati Responsabili del Trattamento ai sensi dell'Art. 28 del Regolamento UE 679/2016.

AWS Presidi di sicurezza:

1) ***PROGETTAZIONE SICURA***

SELEZIONE DEL SITO

Prima di scegliere una sede, AWS esegue valutazioni preliminari di natura ambientale e geografica. AWS sceglie attentamente la sede dei propri data center per limitare il rischio di danni di natura ambientale, come alluvioni, condizioni climatiche estreme e attività sismiche. Le zone di disponibilità sono costruite in modo da essere indipendenti e fisicamente separate le une dalle altre.

RIDONDANZA

I data center sono stati progettati per anticipare e tollerare i guasti mantenendo gli stessi livelli di servizio. In caso di problemi, i processi automatizzati spostano il traffico dall'area colpita. Le applicazioni strategiche sono distribuite seguendo una configurazione N+1 standard; in questo modo, in caso di problemi al data center, viene garantita una capacità sufficiente per permettere al traffico di essere distribuito sui siti rimanenti.

DISPONIBILITÀ

AWS ha identificato i componenti di sistema essenziali, necessari per il mantenimento della disponibilità del sistema e il ripristino del servizio in caso di interruzione. Il backup dei componenti di sistema essenziali viene effettuato in più posizioni isolate note come zone di disponibilità. Ogni zona di disponibilità è stata progettata per operare in modo indipendente e garantire la massima affidabilità. Le zone di disponibilità sono collegate tra loro per consentire ai clienti di progettare applicazioni che eseguano il failover su diverse zone senza provocare interruzioni. Sistemi altamente resilienti e, di conseguenza, la disponibilità dei servizi sono funzioni integrate nella progettazione. Grazie all'uso di zone di disponibilità e di replica dei dati, i clienti AWS possono raggiungere obiettivi molto ambiziosi in termini di tempi brevi di ripristino e punti di ripristino, oltre a una

disponibilità del servizio molto elevata.

2) CONTINUITÀ AZIENDALE E DISASTER RECOVERY

PIANO DI CONTINUITÀ AZIENDALE

Il Piano di continuità aziendale AWS illustra le misure da adottare per evitare e ridurre l'impatto di eventi ambientali. Descrive inoltre nel dettaglio le diverse fasi da seguire prima, durante o dopo il verificarsi di un evento. Il Piano di continuità aziendale prevede dei test, tra cui la simulazione di scenari diversi. Durante e in seguito a tali test, AWS documenta le prestazioni di persone e processi, le azioni correttive e le lezioni apprese, con l'obiettivo di migliorare continuamente la nostra reazione.

RISPOSTA PANDEMICA

Nella propria pianificazione di disaster recovery AWS integra policy e procedure di risposta pandemica per reagire rapidamente a minacce di epidemie di malattie infettive. Le strategie di mitigazione dei rischi prevedono modelli alternativi di gestione del personale per trasferire processi strategici in altre regioni e l'attivazione di un piano di gestione della crisi a supporto di operazioni aziendali critiche. Nei piani pandemici si fa riferimento ad agenzie e normative sanitarie internazionali, nonché a punti di contatto di agenzie internazionali.

3) ACCESSO FISICO

ACCESSO AI DATA CENTER DEI DIPENDENTI

AWS offre l'accesso fisico ai data center solo ai dipendenti autorizzati. Tutti i dipendenti che devono accedere al data center devono prima richiedere l'autorizzazione all'accesso e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Le richieste vengono vagliate e approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite.

ACCESSO AL DATA CENTER DI TERZI

L'accesso di terzi deve essere richiesto da dipendenti AWS designati che devono chiedere l'autorizzazione e fornire una motivazione aziendale valida. L'autorizzazione di tali richieste viene fatta sulla base del principio del privilegio minimo, secondo cui è necessario specificare il layer del data center a cui il dipendente deve accedere, e ha una durata limitata nel tempo. Tali richieste vengono approvate da personale autorizzato e l'accesso viene revocato alla sua scadenza. Una volta ottenuta l'autorizzazione, le persone possono accedere solo alle aree consentite. Tutti coloro che sono autorizzati all'accesso con il badge visitatore devono presentare al proprio arrivo un documento d'identità, firmare al momento dell'ingresso ed essere scortati dal personale autorizzato.

ACCESSO AI DATA CENTER AWS GOVCLOUD

L'accesso fisico ai data center nella regione AWS GovCloud (Stati Uniti) è consentito solo ai dipendenti che hanno dimostrato di essere in possesso di cittadinanza statunitense.

4) MONITORAGGIO E REGISTRAZIONE DI LOG

REVISIONE DEGLI ACCESSI AL DATA CENTER

Gli accessi ai data center vengono regolarmente rivisti. L'accesso è revocato automaticamente quando il profilo di un dipendente viene eliminato dal sistema delle risorse umane di Amazon. Inoltre, quando l'accesso di un dipendente o di un appaltatore scade in base alla richiesta di durata approvata, alla persona viene revocato l'accesso, anche se continua a essere alle dipendenze di Amazon.

LOG DEGLI ACCESSI AI DATA CENTER

Ogni accesso fisico ai data center AWS è registrato, controllato e archiviato. In base alle esigenze, AWS mette in relazione le informazioni ottenute da sistemi logici e fisici di monitoraggio per migliorare la sicurezza.

MONITORAGGIO DEGLI ACCESSI AI DATA CENTER

Monitoriamo i data center grazie ai Security Operations Center (SOC) globali, di proprietà AWS, che monitorano, valutano e mettono in pratica programmi di sicurezza. Tali centri offrono un supporto globale 24 ore su 24, 7 giorni su 7, gestendo e monitorando le attività di accesso ai data center e offrendo ai team locali e ad altri team di supporto gli strumenti per reagire a incidenti di sicurezza e valutare, analizzare, consultarsi e fornire una risposta.

5) SORVEGLIANZA E RILEVAMENTO

VIDEOCAMERE A CIRCUITO CHIUSO (CCTV)

I punti di accesso fisico alle sale server sono controllati da videocamere a circuito chiuso (CCTV). Le immagini vengono archiviate in base a requisiti legali e di conformità.

PUNTI DI ACCESSO AI DATA CENTER

L'accesso fisico viene controllato presso i punti di ingresso dell'edificio dal personale addetto alla sicurezza che si avvale di sistemi di sorveglianza, di rilevamento delle intrusioni e di altri dispositivi elettronici. Per accedere ai data center il personale autorizzato utilizza meccanismi di autenticazione a più fattori. Gli ingressi alle sale server sono protetti da dispositivi che attivano un allarme e una risposta agli incidenti nel caso in cui la porta rimanga aperta o venga forzata.

RILEVAMENTO DELLE INTRUSIONI

Nel layer dei dati vengono installati sistemi elettronici di rilevamento delle intrusioni che monitorano, rilevano e avvisano automaticamente il personale preposto della presenza di incidenti di sicurezza. I punti di ingresso e di uscita delle sale server sono protetti da dispositivi che richiedono a ogni persona l'autenticazione a più fattori prima di autorizzare l'entrata o l'uscita. Tali dispositivi attivano un allarme nel caso in cui la porta rimanga aperta o venga forzata senza autenticazione. I dispositivi di allarme delle porte sono anche configurati per rilevare i casi in cui una persona entra o esce dal layer di dati senza fornire l'autenticazione a più fattori. Gli allarmi vengono immediatamente inviati ai Security Operations Center di AWS 24 ore su 24, 7 giorni su 7, per registrazione, analisi e risposta immediate.

6) GESTIONE DEI DISPOSITIVI

GESTIONE ASSET

Gli asset di AWS vengono gestiti centralmente attraverso un sistema di inventario che archivia e traccia proprietario, sede, stato, manutenzione e informazioni descrittive degli asset di proprietà AWS. Nella fase successiva all'acquisizione, gli asset vengono esaminati e tracciati, mentre gli asset sottoposti a manutenzione vengono verificati e monitorati per definirne proprietà, stato e risoluzione.

DISTRUZIONE DEI SUPPORTI MULTIMEDIALI

I dispositivi di storage multimediali utilizzati per archiviare i dati dei clienti sono classificati da AWS come Critici e ad alto impatto e devono essere trattati come tali per tutto il loro ciclo di vita. AWS segue standard rigorosi per l'installazione, l'utilizzo e infine lo smaltimento dei dispositivi quando non sono più utili. Quando un dispositivo di storage è alla fine del proprio ciclo utile di vita, AWS si occupa del suo smaltimento, utilizzando le tecniche illustrate nel dettaglio in NIST 800-88. I supporti multimediali in cui sono archiviati i dati dei clienti continuano a essere sotto il controllo di AWS fino al loro totale smaltimento.

7) SISTEMI OPERATIVI DI SUPPORTO

ALIMENTAZIONE

I sistemi di energia elettrica che alimentano i nostri data center sono completamente ridondanti e la loro manutenzione può essere eseguita senza alcun impatto sull'operatività, 24 ore al giorno. AWS garantisce che i propri data center sono dotati di generatori di back-up per non interrompere le operazioni di carichi strategici e critici in caso di interruzione dell'energia elettrica presso la struttura.

CLIMA E TEMPERATURA

I data center AWS utilizzano meccanismi di controllo del clima e della temperatura per garantire le condizioni ottimali per server e altro hardware, evitare eventuali surriscaldamenti e ridurre al minimo possibili disservizi. Il personale e i sistemi monitorano e verificano che umidità e temperatura rimangano entro i limiti stabiliti.

RILEVAMENTO ED ESTINZIONE DEL FUOCO

I data center AWS sono dotati di attrezzature automatiche per il rilevamento e l'estinzione delle fiamme. Tali sistemi utilizzano sensori di rilevamento del fumo all'interno di spazi dedicati alla rete, alle infrastrutture e a componenti meccanici. Tali aree sono anche protette da sistemi di estinzione delle fiamme.

RILEVAMENTO DI PERDITE

Per individuare la presenza di perdite, AWS installa presso i propri data center sistemi in grado di rilevare la comparsa di acqua. In questo caso, si attivano meccanismi in grado di rimuovere l'acqua per evitare eventuali danni aggiuntivi.

8) MANUTENZIONE DELL'INFRASTRUTTURA

MANUTENZIONE DELLE APPARECCHIATURE

AWS monitora le apparecchiature meccaniche e tecniche ed esegue manutenzioni di prevenzione per garantire la continuità dei sistemi presenti all'interno del data center AWS. Personale qualificato esegue e porta a compimento procedure di manutenzione delle apparecchiature secondo un piano definito e documentato.

GESTIONE DELL'AMBIENTE

AWS monitora i sistemi meccanici ed elettrici e le relative attrezzature per consentire un'identificazione immediata delle problematiche. Tale obiettivo viene raggiunto attraverso il continuo utilizzo di strumenti di controllo e di informazioni fornite da sistemi di monitoraggio delle componenti elettriche e di gestione degli edifici. La manutenzione di prevenzione viene eseguita per garantire un'operatività senza interruzioni delle apparecchiature.

9) GOVERNANCE E RISCHI

GESTIONE CONTINUA DEI RISCHI DEI DATA CENTER

Il Security Operations Center di AWS esegue con regolarità analisi delle minacce e delle vulnerabilità dei data center. Il monitoraggio continuo e la mitigazione di vulnerabilità potenziali vengono eseguite attraverso attività di valutazione dei rischi del data center. Tali operazioni si aggiungono al processo di valutazione dei rischi di livello Enterprise che ha lo scopo di individuare e gestire eventuali rischi del business nella sua interezza. Di questo processo fanno parte anche rischi normativi e ambientali a livello regionale.

ATTESTAZIONE DI SICUREZZA DI TERZI

I test dei data center AWS eseguiti da terze parti e documentati in report garantiscono la corretta implementazione delle misure di sicurezza, in linea con regole condivise, il cui rispetto è necessario per ottenere le relative certificazioni. A seconda del programma di conformità e dei relativi requisiti, revisori esterni possono eseguire test delle procedure di smaltimento di supporti multimediali, analizzare i filmati delle videocamere di sicurezza, osservare ingressi e corridoi del data center, verificare i dispositivi elettronici di controllo degli accessi ed esaminare le apparecchiature.

AWS CERTIFICAZIONI

AWS dispone di certificazioni di conformità ai sensi degli standard ISO/IEC 27001:2013, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 9001:2015 e CSA STAR CCM v4.0.

METODOLOGIA DI CALCOLO DEL RISCHIO RESIDUO

Sopra sono state individuate le componenti che concorrono al funzionamento per la raccolta e gestione delle segnalazioni per la piattaforma Whisper.

Il calcolo del rischio residuo che potrebbero arrecare pregiudizio ai diritti e lede libertà degli Interessati viene svolto tramite le seguenti fasi:

1) individuazione scenari di rischio;
2) valutazione dell'impatto potenziale che gli Interessati potrebbero subire in caso di violazione di dati personali;
3) valutazione delle misure tecniche ed organizzative adottate dal Titolare del Trattamento e da tutti i soggetti che concorrono all'erogazione del servizio;
4) individuazione, per ogni scenario di rischio (distinto per tecnologia/servizio), del rischio residuo per gli Interessati.

Il livello di rischio residuo è quindi determinato, sia dal livello di impatto che gli Interessati potrebbero subire, sia dalle eventuali carenze tecniche, organizzative e procedurali adottate per una o più componenti che concorrono al funzionamento della Piattaforma di Whisper.

Per la determinazione del livello di rischio residuo viene determinato il livello di "Vulnerabilità" delle componenti che concorrono alla realizzazione della finalità del trattamento e che esprime la verosimiglianza di accadimento di una minaccia considerate la presenza e l'efficacia delle misure a mitigazione

SCENARI DI RISCHIO

Di seguito gli scenari di rischio che potrebbero compromettere la Riservatezza, Integrità e Disponibilità dei dati personali trattati nella Piattaforma Whisper.

Componente	Scenari di rischio	
Software	Accesso illegittimo ai dati	SI
	Modifiche indesiderate	SI
	Perdita dei dati	SI
Hardware	Accesso illegittimo ai dati	SI
	Modifiche indesiderate	SI
	Perdita dei dati	SI
Infrastruttura	Accesso illegittimo ai dati	SI
	Modifiche indesiderate	SI
	Perdita dei dati	SI

IMPATTO PER GLI INTERESSATI A SEGUITO DI UNA VIOLAZIONE DEI DATI

livello impatto	conseguenze
1 - Basso	Gli individui possono andare incontro a disagi minimi, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).

2 - Medio	Gli individui possono andare incontro a disagi discreti, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
3 - Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
4 - Critico	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Considerata la tabella sopra descritta con i livelli, in relaziona al trattamento in esame, l'impatto per i diritti e le libertà degli Interessati è determinato come "Alto" in quanto la compromissione della riservatezza, integrità e disponibilità delle informazioni veicolate attraverso la Segnalazione potrebbe comportare per le persone fisiche coinvolte:

Compromissione della Riservatezza: la violazione dei dati personali può portare a una chiara violazione della privacy degli individui coinvolti. Questo può includere la divulgazione non autorizzata di informazioni sensibili o personali che avrebbero dovuto essere mantenute confidenziali;

Rischio di Ritorsioni: gli individui che segnalano comportamenti illeciti o scorretti (whistleblowers) potrebbero essere a rischio di ritorsioni da parte dell'azienda o dell'organizzazione oggetto della segnalazione. La violazione dei loro dati personali potrebbe esporli ancora di più a rischi, come il licenziamento ingiusto o l'isolamento sociale;

Danno alla Reputazione: la divulgazione non autorizzata di dati personali potrebbe danneggiare la reputazione degli interessati, in particolare se le informazioni divulgate sono compromettenti o imbarazzanti. Questo potrebbe influire negativamente sulla loro carriera o sulla loro vita personale;

Perdita di Fiducia: gli interessati potrebbero perdere la fiducia nella capacità dell'organizzazione di proteggere adeguatamente i loro dati personali e la loro privacy. Ciò potrebbe influire sulla loro volontà di segnalare futuri comportamenti illeciti o scorretti;

Impatto Emotivo e Psicologico: la violazione dei dati personali può avere un impatto emotivo e psicologico significativo sugli interessati. Possono sentirsi vulnerabili, esposti e angosciati a causa della divulgazione non autorizzata delle loro informazioni personali;

Rischi Finanziari: In alcuni casi, la violazione dei dati personali potrebbe comportare rischi finanziari per gli interessati, ad esempio se i loro dati finanziari vengono compromessi e utilizzati per scopi fraudolenti;

Problemi Legali: gli interessati potrebbero avere cause legali contro l'organizzazione che ha subito la violazione dei dati personali. Questo potrebbe comportare costi legali e ulteriori stress;

Perdita di Controllo: la violazione dei dati personali può far sentire agli interessati di aver perso il controllo sulle proprie informazioni personali, il che può essere fonte di ansia e disagio.

MISURE DI SICUREZZA IMPIEGATE PER LA MITIGAZIONE DELLE MINACCE

Di seguito sono descritte le misure di sicurezza impiegate per la mitigazione dei rischi della Piattaforma Whisper.

DEFINIZIONI

Al fine di migliore comprensione delle misure di sicurezza di seguito sono descritte alcune definizioni:

1) **“Firewall”:** Un firewall è un componente di sicurezza di rete che funge da barriera tra una rete interna o privata e una rete esterna o pubblica. Esamina il traffico di rete in entrata e in uscita e decide se consentire o bloccare determinate comunicazioni in base a un insieme di regole predefinite. Le regole del firewall specificano quali pacchetti di dati sono consentiti o rifiutati in base a criteri come indirizzi IP, porte, protocolli e altro; nella presente valutazione sono omessi la versione ed il nome del firewall utilizzati al fine di evitare la diffusione di potenziali informazioni preziose a terzi;
2) **Web Application Firewall (“WAF”):** Un Web Application Firewall è un dispositivo o un'applicazione software che si trova tra un'applicazione web e il traffico di rete in ingresso. Il suo compito principale è rilevare, filtrare e bloccare minacce informatiche specifiche che mirano alle applicazioni web, come attacchi SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) e altri; nella presente valutazione sono omessi la versione ed il nome del WAF utilizzati al fine di evitare la diffusione di potenziali informazioni preziose a terzi;
3) **Chiave di Cifratura:** Per utilizzare l’algoritmo AES, è necessario specificare una chiave di cifratura. Questa chiave è una stringa segreta che viene utilizzata per crittografare e decrittografare i dati. È importante proteggere questa chiave con estrema cura poiché il suo accesso non autorizzato potrebbe compromettere la sicurezza dei dati.

MISURE PER ASSICURARE LA RISERVATEZZA DELLE INFORMAZIONI

- **SPECIFICI RUOLI DI ACCESSO** L’accesso al Software è riservato esclusivamente al personale autorizzato (incaricati e responsabili al trattamento appositamente designati) in possesso di specifiche ed individuali credenziali di accesso.
- **ACCESSO DEGLI AMMINISTRATORI DI SISTEMA** solo sempre tramite connessione protetta mediante protocollo SSH da IP espressamente autorizzati;
- **FIREWALL** Presenza di un Firewall che opera il filtraggio del traffico di rete, inclusi input, output e regole forward;
- **WAF** per la protezione dalle Vulnerabilità delle Applicazioni Web: Il WAF rileva e protegge dalle vulnerabilità comuni delle applicazioni web, come SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF) e molti altri attacchi web;
- **WAF** per il blocco delle Richieste Maliziose, compreso analisi di IP Reputation: Il WAF rileva e blocca automaticamente le richieste HTTP/HTTPS dannose o sospette prima che raggiungano l'applicazione web. Ciò include la protezione contro bot malevoli, scanner di vulnerabilità e attacchi brute force;
- **WAF** per il controllo del Traffico: Il WAF analizza il traffico HTTP/HTTPS in entrata e in uscita per individuare attività sospette o comportamenti anomali. Ciò consente di identificare e mitigare minacce in tempo reale;
- **WAF** per il rilevamento dei DDoS WAF include anche una protezione DDoS (Distributed Denial of Service) che può aiutare a mitigare gli attacchi DDoS contro il server;
- **ANALISI DEI LOG CONTINUO** al fine di rilevare eventuali attacchi di tipo SQL Injection o XSS;
- **Sviluppo del Software secondo le migliori prassi** mediante anche l’utilizzo di PreparedStatement in Java, al fine di prevenire potenziali attacchi di tipo SQL e/o XSS Injection e seguendo le linee guida OWASP;
- **Accesso consentito** previa doppia autenticazione con codice temporaneo (OTP) [se abilitato dall’utente];
- **Cifratura** delle informazioni delle Segnalazioni e di ogni altra informazione, registrate nel database e nel backup dei database, mediante algoritmo AES256 Encryption e specifica chiave di cifratura;
- **LOG DI NAVIGAZIONE**
- Registrazione dei log delle operazioni del personale addetto alla gestione del Sistema di Segnalazione;

- Registrazione dei log di login falliti;
- Le Chiavi di Cifratura sono detenute da AWS, creata con l'algoritmo SHA256
- Crittografia dei dati in transito dal Server della Piattaforma al cliente mediante protocollo SSL/TLS che impedisce a terze parti non autorizzate di intercettare e leggere il contenuto delle comunicazioni. SSL/TLS utilizza algoritmi di crittografia avanzati come RSA, DHE (Diffie-Hellman Ephemeral), ed ECC (Elliptic Curve Cryptography) per proteggere i dati. (Cryptazione end-to-end)

MISURE PER ASSICURARE LA DISPONIBILITÀ ED INTEGRITÀ DEI DATI

Database distribuito, allineato in tempo reale su cluster con nodo master situato su diverse ridondanze di AWS nella regione di Milano;