POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

ULTIMO AGGIORNAMENTO : 14/11/2024

SOMMARIO

1. SCOPO

La presente Policy definisce l'assetto interno ad UNGUESS necessario a garantire **la sicurezza e la protezione delle informazioni**, patrimonio dell'organizzazione, in riferimento anche ai requisiti della **norma ISO/IEC 27001** e a garantire il **sicuro** trattamento dei dati personali dei soggetti interessati, come previsto dal Modello Privacy adottato dalla società in conformità al Regolamento Europeo per la protezione dei dati personali, GDPR .

Tale documento indica l'insieme delle politiche, procedure, documenti, registri, piani, linee guida, accordi, contratti, processi, pratiche, metodi, attività, ruoli, responsabilità, relazioni, strumenti , tecniche, tecnologie, risorse, e strutture che l'organizzazione utilizza per proteggere e conservare le informazioni, per gestire e controllare i rischi di sicurezza delle informazioni e per raggiungere gli obiettivi aziendali di adeguatezza e conformità. Il tutto attraverso un controllo delle comunicazioni e trasmissioni sui diversi canali (web, internet, cloud) e sui diversi utilizzatori, interni ed esterni, per garantire protezione e sicurezza, ai fini del pericolo di "fuga di informazioni", accidentale o volontaria, che genera conseguenze negative sia per il business dell'organizzazione, sia per la sua reputazione e immagine.

I principi a cui si ispira la Politica riguardano la **riservatezza, l'integrità** e la **disponibilità** delle informazioni oggetto di trattamento e di comunicazione all'interno e all'esterno, e nel rispetto delle leggi nazionali ed europee vigenti, come ad esempio lo stesso **Regolamento Europeo per la protezione dei dati personali : GDPR** .

La partenza verso la Certificazione ISO/IEC 27001 è avvenuta a seguito di un'analisi del contesto in cui l'organizzazione opera, delle parti interessate, delle opportunità

e dei possibili rischi sul mancato adeguamento ad uno standard ISO che permette di garantire la sicurezza delle informazioni.

2. LEADERSHIP, RUOLI E RESPONSABILITÀ

La Direzione Generale è responsabile della definizione e revisione continua degli obiettivi della suddetta Policy, in relazione alle strategie di adeguatezza e sviluppo. Essa garantisce anche il coinvolgimento di tutte le parti interessate comunicando prima di tutto la presente Policy attraverso i canali interni tradizionali, quindi lo stato di applicazione del Sistema di Gestione, l'importanza del miglioramento continuo, l'impegno a sostenere e guidare tutti i processi a sostegno di tutti coloro che partecipano, direttamente e indirettamente, alla vita dell'organizzazione.
Tra l'altro, la Leadership si impegna a:

- garantire il rispetto delle normative vigenti e i requisiti della norma;
- rendere disponibili le risorse, umane e tecniche, necessarie al perseguimento degli obiettivi della sicurezza delle informazioni;
- comunicare regole, procedure, policy e altra documentazione per la gestione della politica aziendale per la sicurezza delle informazioni ;
- sviluppare e garantire la consapevolezza e la conoscenza alle persone, interne ed esterne, che interagiscono con la sicurezza;
- fissare obiettivi sempre aggiornati e condivisi, e riesaminare annualmente l'intero Sistema di gestione.

La Leadership, o Alta Direzione, assegna ruoli e responsabilità a figure professionali ben definite e li comunica al personale e ai collaboratori attraverso i canali tradizionali interni all'organizzazione.

I ruoli che qui sono elencati sono quelli pensati ad hoc per la realtà aziendale di UNGUESS e coincidenti anche con i ruoli ricoperti dal Team Privacy di UNGUESS :

- **Direzione Generale** - determina le strategie per la gestione della sicurezza delle informazioni, stabilisce gli obiettivi, si impegna nel mettere a disposizione le risorse necessarie per la corretta applicazione di suddetta Policy, governa e autorizza processi e politiche, promuove il miglioramento continuo, effettua il riesame e ne valuta le prestazioni;
- **Responsabile della politica di sicurezza delle informazioni** – nella figura del **RPD/ DPO** (**R**esponsabile **P**rotezione **D**ati/ **D**ata **P**rotection **O**fficer) che occupandosi della sicurezza dei dati si occupa anche della gestione della sicurezza delle informazioni e nominato dalla Direzione. Vigila sui processi di attuazione di suddetta Policy, affida responsabilità di asset e processi gestionali, partecipa alle attività di audit e verifica, supervisiona politiche e procedure per l'approvazione da parte della Direzione;
- **Responsabile Risorse Umane** – gestisce le competenze del personale coinvolto nei processi di attuazione della sicurezza delle informazioni, definisce i Piani della formazione e ne garantisce l'esecuzione.
- **Amministratori di Sistema -** due dipendenti di UNGUESS in qualità di esperti informatici interni nominati con formali atti di nomina, che supportano il DPO nell'attuazione e aggiornamento delle misure di sicurezza implementate al fine di garantire la sicurezza delle informazioni .

3. OBIETTIVI DELLA SICUREZZA DELLE INFORMAZIONI

L'organizzazione ha individuato gli obiettivi per la sicurezza delle informazioni che sono qui sinteticamente elencati :

- sviluppare competenze in ciascuna figura professionale in tema di Sicurezza delle informazioni;
- attivare a proposito un Piano della Formazione che intervenga con corsi ad hoc sulla tematica;
- sviluppare un Piano della Comunicazione in cui siano inseriti eventi e campagne di sensibilizzazione;

- assegnare le necessarie risorse per tutti gli aspetti della sicurezza, fisica, logica e organizzativa;
- sviluppare la documentazione di supporto e integrarla con documenti già presenti e di valido utilizzo per la gestione della sicurezza delle informazioni;
- individuare le figure professionali già impegnate per la sicurezza e ridefinire i profili secondo competenze e responsabilità proprie dei ruoli stabiliti per la Sicurezza delle informazioni;
- migliorare l'attuale gestione di incidenti o eventi dannosi attraverso lo sviluppo di un processo di gestione e controllo adeguati;
- gestire l'intera strategia di gestione della sicurezza delle informazioni da un punto di vista del rischio e di tutte le sue articolazioni (pianificazione, valutazione, gestione contromisure, rischio accettato).

4. ATTENZIONE FOCALIZZATA SULLA SICUREZZA DELLE INFORMAZIONI E SULLE PARTI INTERESSATE

Le informazioni aziendali a cui fa riferimento la presente Policy riguardano tutte le informazioni raccolte, conservate e trasmesse su qualsiasi supporto, cartaceo ed elettronico, per garantire l'operatività dell'organizzazione.
Ai fini del trattamento a cui possono essere sottoposte le informazioni aziendali, la garanzia della loro sicurezza tiene in considerazione le seguenti caratteristiche:

- il **Valore**, ossia l'importanza dell'asset informativo a livello di business e di strategia dell'organizzazione (ad esempio un brevetto o un piano di sviluppo);
- la **Cogenza**, in termini di proprietà valoriale insita nell'informazione stessa, da un punto di vista normativo e di conformità (ad esempio un regolamento, una policy);
- la **Criticità**, in termini di Riservatezza, Integrità e Disponibilità per cui la vulnerabilità ad attacchi e minacce ne comprometterebbero la sicurezza.

5. ASSET E REQUISITI BASE PER LA SICUREZZA DELLE INFORMAZIONI E INFRASTRUTTURA IT

Tra i processi più rilevanti per garantire la sicurezza delle informazioni c'è il processo di gestione degli asset: le Informazioni, o asset informativi, sono un patrimonio fondamentale per l'organizzazione, e la loro sicurezza e protezione è irrinunciabile.

Gli Asset Informativi si dividono in due categorie di appartenenza:

- **Asset Primari,** che riguardano dati, processi e attività di business, informazioni aziendali, dati di mercato e vendita, del personale, di procedure, aspetti amministrativi, e così via. In UNGUESS gli Asset primari sono rappresentati da :
    1. Server Cloud AWS: RDS, S3, EC2 che ospitano la piattaforma principale
    2. Hubspot
    3. Holistics.io
- **Asset di Supporto,** che possono essere Sistemi IT (reti, infrastrutture, dispositivi), Software, Network, Sedi e Aree Riservate, e così via. In UNGUESS gli Asset di Supporto sono rappresentati da:
    1. Server Cloud AWS: EC2: che ospitano un documentale, una piattaforma di BI
    2. Google Workspace
    3. Factorial HR

La sicurezza delle informazioni, garantita dal rispetto di suddetta Policy, avviene nel rispetto dei tre requisiti base citati in premessa, cioè la **Riservatezza,** l'**Integrità** e la **Disponibilità** delle informazioni (R.I.D.):

- **Riservatezza:** si tratta di non divulgare informazioni ai non autorizzati, individui, entità o processi, quindi ci deve essere un processo di autorizzazioni che indichi chi può e chi non può accedere alle informazioni.

- **Integrità:** riguarda la conservazione e protezione da danni o modifiche delle informazioni, quindi alla loro salvaguardia e alla completezza delle informazioni.
- **Disponibilità:** le informazioni sono rese disponibili solo a entità autorizzate, si ritorna alla definizione di processi di autorizzazione per cui un'informazione può essere Pubblica o Riservata.

L'obiettivo è quello di identificare gli asset dell'organizzazione e definire adeguate responsabilità per la loro protezione e sicurezza.

L'infrastruttura IT di UNGUESS é in cloud. Essa infatti non è su dei server fisici in nostro possesso ma in Cloud, distribuita quindi su più servizi di AWS (Amazon Web Services), il Cloud Vendor da noi scelto. L'intera infrastruttura è dettagliatamente descritta all'interno dell' allegato, annesso allo stesso Modello Privacy a cui tale Policy è a sua volta allegata, intitolato ''*Infrastruttura IT UNGUESS*'' .

6. OUTSOURCING E FORNITORI

I fornitori sono partner insieme ai quali lavorare per raggiungere obiettivi che soddisfino e garantiscano una crescita reciproca e continua, essendo la Direzione consapevole dell'interdipendenza dell'organizzazione con i suoi fornitori e sicura che l'instaurazione di rapporti di mutuo beneficio siano atti ad aumentare, per entrambe le parti, la capacità di creare valore aggiunto.

Per questo la presente Politica si pone come obiettivo anche la buona gestione delle attività in outsourcing e dei fornitori, garantendo che:

- siano attentamente selezionati, qualificati e monitorati i fornitori di prodotti che possano incidere in modo significativo sulla sicurezza delle informazioni nell'offerta di outsourcing;

- effettuare esami sulla conformità normativa del fornitore;
- prevedere eventuali audit presso il fornitore per verificare la conformità agli accordi contrattuali e ai requisiti di sicurezza delle informazioni. È necessario che la valutazione dei fornitori avvenga con cadenza periodica (o con continuità) rispetto a criteri predefiniti. I risultati della valutazione e rivalutazione dei fornitori devono essere tenuti aggiornati e devono consistere nelle modalità di gestione degli ordinativi, nelle specifiche di prodotto, nelle risultanze di audit, sui dati prestazionali o su eventuali reclami.

7. AZIONI PER LA GESTIONE DEI RISCHI E DELLE OPPORTUNITÀ

Secondo la metodologia adottata dall'organizzazione, dopo aver definito un elenco dei rischi ed effettuato una valutazione del loro impatto sulla gestione degli Asset informativi, la correlazione tra questi ultimi e i rischi avviene considerando le vulnerabilità con impatto sulla Riservatezza, Integrità e Disponibilità.
Questa metodologia permette di condurre una valutazione del rischio partendo dalle specifiche vulnerabilità insite nell'Asset informativo, dalle minacce rilevate e dalla loro frequenza, e dalle probabilità di manifestarsi.
Questo conduce suddetta Policy ad effettuare un vero e proprio trattamento del rischio decidendo le quattro strategie su cui viene anche formulato un apposito Piano di Trattamento del Rischio. Questo l'elenco delle strategie che sono messe in atto:

- **Evitare i rischi** – modificare o non intraprendere attività per fare in modo che non si presentino.
- **Controllare/Mitigare i rischi** – ridurre la probabilità o l'impatto, o entrambi, con contromisure appropriate.
- **Accettare il rischio** – decidere di non intervenire sugli effetti del rischio in quanto troppo costoso.

La gestione dei rischi rientra nelle attività svolte in coordinamento tra il DPO aziendale (Responsabile protezione dati) e i due amministratori di sistema, figure nominate e previste ai sensi del GDPR, a cui UNGUESS si impegna a essere compliant alla luce anche del Modello organizzativo e di gestione della Privacy adottato internamente, e di cui tale Policy per la sicurezza delle Informazioni risulta essere parte integrante.

8. MIGLIORAMENTO, RIESAME E AUDIT

La presente Policy è oggetto di monitoraggio con cadenza almeno annuale con cui la Direzione, **attraverso il supporto del DPO (Responsabile per la protezione dati ex. art 37 GDPR) e dei due amministratori di sistema interni**, verifica le politiche, le procedure organizzative e le registrazioni opportunamente aggiornate dai relativi responsabili.

Il processo con cui si effettua il monitoraggio e la valutazione della Policy è l'Audit interno. È uno strumento con cui misurare il livello di sicurezza del sistema, ma è anche un'indagine strutturata e metodica poiché ispeziona ogni elemento oggetto di rischio.

L'Audit interno mira a:

- individuare eventuali vulnerabilità che rendono la sicurezza delle informazioni inefficiente;
- verificare e assicurare le conformità a politiche, norme o leggi;
- rivedere e migliorare la politica per la sicurezza delle informazioni;
- verificare il reale raggiungimento degli obiettivi della sicurezza.

L'Audit viene condotto da personale interno qualificato e competente, come il DPO e gli amministratori di sistema, figure nominate ai sensi del GDPR, in grado di rilevare le criticità e i punti di forza della strategia di gestione della sicurezza delle informazioni, per poi esporle in un report che funga da guida, per la Direzione, nel formulare nuove strategie e nuovi traguardi per la sicurezza delle informazioni.

Il risultato di un Audit, infatti, può portare alla scoperta di non conformità, come criticità o vulnerabilità di un servizio o di un processo, quindi dover intervenire con opportune azioni correttive.

9. SINGOLE MISURE DI SICUREZZA IMPLEMENTATE

UNGUESS prevede l'applicazione di una serie di misure di sicurezza utilizzate per garantire la concreta sicurezza delle informazioni conservate internamente e anche per garantire il consequenziale e sicuro trattamento dei dati previsto dal Regolamento Europeo GDPR . Di seguito vengono descritte le misure più rilevanti implementate.

Gestione e monitoraggio degli accessi agli asset it

La gestione degli accessi previene gli accessi non autorizzati, evitando che tali tipi di accessi non monitorati, possano portare alla violazioni dei dati.
All'interno di UNGUESS ci sono tre utenti con poteri di amministrazione dell'account AWS, all'interno del quale ci sono tutti gli asset critici per il funzionamento della piattaforma.
Questi tre utenti sono admin ma non fanno uso del root account, che è condiviso tra il CTO e il Tech Lead e permette in caso di account takeover di entrare come root e resettare eventuali utenze compromesse.
Tutto il resto del team ha credenziali fortemente limitate, i tre admin sopracitati hanno ampi poteri ma non di cancellazione dell'account.
Inoltre UNGUES si impegna al fine di rendere sempre più granulare e restrittiva la configurazione degli IAM.
Inoltre UNGUESS in tutti i sistemi utilizzati obbliga all'utilizzo di MFA e possiede una ridondanza di admin con l'obiettivo di aumentare la velocità di risposta e non avere un *single point of failure*.

Misure in atto per protezione contro malware e attacchi esterni

Al fine di proteggere gli asset da minacce esterne e non renderli vulnerabili a tali tipi di attacchi, l'Infrastruttura e i software di UNGUESS sono costantemente testate contro intrusioni e attacchi.
Per ciò che concerne i software in cloud, presenti su Amazon e Google, già é presente un sistema di protezione contro attacchi esterni impostato e aggiornato in base agli standard di sicurezza informatica internazionale riconosciuti .
Per tutti i device dei dipendenti non c'è una politica stringente di antivirus ma ogni dipendente deve averne uno installato e deve mantenerlo aggiornato secondo quanto previsto dalla Politica di Sicurezza delle Informazioni adottata da UNGUESS.

Esecuzione intelligente dei backup e del ripristino dati

Al fine di un'esecuzione intelligente dei backup e del ripristino dati, il sistema di gestione dei backup è altamente strutturato e sicuro. I backup vengono eseguiti automaticamente più volte durante il giorno, e gli snapshot risultanti sono archiviati in modo sicuro su S3. È importante sottolineare che non ci sono API Key con permessi root disponibili pubblicamente, riducendo significativamente il rischio di account takeover tramite chiavi API.
In caso di compromissione di un account tramite API Key, i backup rimangono intatti, in quanto sono protetti da modifiche non autorizzate. Inoltre, solo tre amministratori hanno accesso alla console, garantendo una gestione controllata e sicura del sistema. Questa limitazione di accesso è pensata per mitigare il rischio di perdita di accesso da parte degli amministratori.

Sono state implementate pratiche avanzate di sicurezza, evitando l'uso del root account per operazioni quotidiane. Questo approccio contribuisce a mantenere un ambiente più sicuro e a ridurre la vulnerabilità del sistema.
Sebbene non vengano condotte ufficialmente esercitazioni di disaster recovery, vengono seguite le migliori pratiche di blue-green deployment e infrastructure as code. Ogni settimana, viene creata una nuova infrastruttura da zero, inclusi i dati salvati. Dopo aver verificato il corretto funzionamento,l'infrastruttura precedente viene distrutta.

Pur non essendo completamente automatizzato al 100%, si ha piena fiducia nel processo manuale che consente di poter effettuare una rapida e efficace disaster recovery quando necessario. Questo approccio fornisce una sicurezza operativa solida e riduce il rischio di perdita di dati in situazioni di emergenza.

Procedure per la formazione e la sensibilizzazione del personale sulla sicurezza delle informazioni

Il team di Cyber Security interno ad UNGUESS implementa regolarmente attività di phishing interno al fine di valutare la preparazione e la consapevolezza degli utenti/dipendenti. Queste simulazioni vengono condotte periodicamente, almeno una volta ogni trimestre, coinvolgendo l'intero personale. L'obiettivo è quello di valutare la capacità degli utenti di riconoscere e gestire potenziali minacce di phishing, oltre a identificare eventuali aree di miglioramento.

Dopo ogni simulazione, i risultati vengono attentamente analizzati e condivisi con l'intera organizzazione. Questo processo non solo evidenzia le performance individuali, ma fornisce anche un'opportunità per sensibilizzare gli utenti su nuove tattiche e metodi utilizzati dagli attaccanti. Successivamente, si organizzano sessioni di formazione mirate per rafforzare le competenze e le conoscenze necessarie per affrontare minacce di phishing in modo efficace.

Parallelamente, il team di Cybersecurity mantiene un monitoraggio costante delle attività email all'interno dell'organizzazione. Attraverso l'utilizzo di strumenti avanzati di analisi del traffico, vengono individuati e anticipati potenziali rischi derivanti da email sospette o attività anomale. Nel caso in cui vengano rilevati eventi di rischio, il team contatta direttamente gli utenti coinvolti per fornire spiegazioni dettagliate sulle minacce potenziali e istruzioni su come evitare di cadere in trappole.
Infine i dipendenti vengono costantemente aggiornati su canale interno aziendale tramite comunicazioni ufficiali riguardo le novitá adottate dall'azienda in tema di sicurezza aziendale

Questa combinazione di attività di simulazione, monitoraggio proattivo e comunicazione diretta con gli utenti crea un approccio completo alla gestione della sicurezza delle email. Non solo mira a rafforzare la sicurezza informatica dell'organizzazione, ma contribuisce anche a creare una cultura di consapevolezza della sicurezza tra i membri del team.

Gestione intelligente delle patch e degli aggiornamenti software

Tutti i software utilizzati per l'operatività aziendale sono SaaS quindi UNGUESS non si occupa direttamente degli aggiornamenti.
Per quanto riguarda invece i software di proprietá di UNGUESS, cioè unguess.io e tryber.me, quelli vengono gestiti internamente e sono perció aggiornati costantemente, al fine del loro funzionamento, da UNGUESS stessa.

Per quanto concerne i dispositivi dei dipendenti, questi sono a carico degli stessi per quanto riguarda aggiornamenti e patch di sistema. Gli aggiornamenti non vengono forzati ma sono fortemente consigliati. Sui dispositivi dei dipendenti, come da policy accettata in fase di assunzione, è proibito il salvataggio di dati sensibili inerenti all'azienda e/o dei clienti. UNGUESS di prassi cerca di avere una longevità molto corta delle macchine, massimo 3 anni. Periodicamente i dipendenti possono passare dall'IT support per check up e aggiornamenti.

Procedure in caso di violazione della sicurezza o incidenti

UNGUESS in caso di violazioni della sicurezza o di incidenti, attiva la procedura, come da best practice per la gestione di incidenti secondo il GDPR, rispettando quanto previsto in tal senso anche dal proprio Modello Privacy e prevedendo di attivare il DPO e gli Amministratori di Sistema, al fine sia di mettere in quarantena utenze o il server in base al caso, e sia di comunicare tempestivamente al Garante per la privacy ex GDPR e eventualmente agli utenti se dovuto in base a quanto riscontrato.

Monitoraggio e registrazione degli eventi di sicurezza

UNGUESS gestisce 3 tipi di monitoraggi e log diversi per eventi di sicurezza:

- Accessi e comportamenti malevoli di email e dati (Google Enterprise Workspace);
- Accessi e modifiche dati (Wordpress admin);
- Tentativi di connessioni malevoli (WAF e cloudwatch) .

Il primo punto si riferisce al blocco automatico del fishing; il secondo e il terzo punto si riferiscono al sistema dei nostri server che ci permette di individuare l'attacco.

Gestione degli account privilegiati e delle credenziali

UNGUESS, al fine di limitare l'accesso alle risorse critiche da parte di account con privilegi elevati, limita l'accesso solo a chi ne ha effettivamente bisogno.

In tal senso tutte le utenze vengono gestite secondo il principio di minima e progressiva divulgazione. I dipendenti non hanno mai accesso a caso a dati dei dipendenti stessi o di clienti e utenti se non riguardanti il proprio diretto lavoro.
Ci sono livelli di accesso sia in Google Workspace, sia in piattaforma, sia in Hubspot e in tutti i sistemi che utilizziamo quotidianamente per lavorare.Ognuno di questi ha sempre almeno 2 admin e prevede per le utenze di amministrazione l'accesso con MFA (Multi-Factor Authentication).

Politiche in atto per la gestione delle password

Per gestire le password al fine di prevenire l'accesso non autorizzato, anche se non è imposto un obbligo di rotazione periodica delle password, si promuove, tuttavia, attivamente l'adozione di misure avanzate di sicurezza, in particolare attraverso l'obbligo di utilizzo della Multi-Factor Authentication (MFA) sulla piattaforma proprietaria e sui profili utente di Google Workspace. Questa pratica aggiuntiva di autenticazione contribuisce significativamente a rafforzare la sicurezza degli account, richiedendo ulteriori livelli di verifica oltre alla tradizionale combinazione di nome utente e password.

Per quanto riguarda gli altri software utilizzati, si è optato per l'integrazione con il Google Single Sign-On (SSO). Questa soluzione centralizzata semplifica l'accesso agli utenti attraverso un'unica identità di autenticazione, offrendo al contempo un elevato standard di sicurezza, dato il solido sistema di autenticazione gestito da Google.
Tale approccio mira a migliorare l'efficienza operativa e la sicurezza complessiva, riducendo il rischio di accessi non autorizzati e semplificando la gestione delle credenziali per gli utenti. è previsto, all'interno di UNGUESS, l'utilizzo forzato di MFA sulla piattaforma proprietaria e sull'utenza Google Workspace, e l'utilizzo di Google SSO su tutti gli altri software.

Sistemi di cifratura in atto per proteggere i dati sensibili

UNGUESS adotta un sistema di cifratura per proteggere i dati sensibili da accessi non autorizzati, in quanto dati non cifrati possono essere letti se compromessi.

In tal senso UNGUESS utilizza software in cloud come Amazon Web Service e Google Workspace. Tutti i documenti, contenenti possibili dati personali del cliente, sono gestiti da UNGUESS nel cloud Google Workspace in cui vengono utilizzati i strumenti di crittografia standard di Google, come ad esempio, per Gmail, Google Workspace usa TLS di default per crittografare la connessione quando i messaggi viaggiano tra server di posta elettronica.
In particolare, sia Amazon Web Service che Google Workspace hanno completato l'aggiornamento globale per supportare anche TLS 1.3, oltre che il precedente giá supportato TLS 1.2
Quindi per i motivi sopra elencati, possiamo confermare che UNGUESS utilizza, in relazione ai software sui quali girano dati sensibili del cliente, protocolli non deprecati quali TLS 1.3 o TLS1.2 .

Gestione dei dispositivi mobili e accesso da remoto

In virtù dell'assenza di reti aziendali, è importante sottolineare che la compromissione di un dispositivo mobile non presenta il potenziale di generare

impatti sui sistemi utilizzati dall'organizzazione. La possibile esposizione, se si verificasse, è circoscritta esclusivamente ai client mail dei dipendenti.

Tuttavia, l'organizzazione adotta una strategia proattiva nella gestione di eventuali comportamenti malevoli di natura simile. Tale approccio è guidato e sorvegliato con attenzione attraverso l'implementazione di sofisticati sistemi di detection nell'ambito di Google Workspace Enterprise. Questi meccanismi avanzati di monitoraggio consentono di identificare e rispondere tempestivamente a potenziali minacce, garantendo così un livello elevato di sicurezza.

La decisione di affidarsi a Google Workspace Enterprise per la gestione della sicurezza rappresenta un'ulteriore tappa nell'ottimizzazione delle misure di protezione. Questo approccio mirato non solo fornisce una protezione aggiuntiva, ma contribuisce anche a mitigare in modo efficace il rischio associato a eventuali minacce, creando un ambiente di lavoro più sicuro e protetto per l'organizzazione nel suo complesso.

Protocolli in atto per la gestione delle vulnerabilità e la loro mitigazione

UNGUESS, al fine di assicurare una risposta tempestiva alle vulnerabilità, che se non gestite possono essere sfruttate dagli attaccanti, ha implementato un Piano di Divulgazione delle Vulnerabilità, attivo 24/7, che consente la ricezione continua di segnalazioni. Il team interno di triage valuta attentamente le segnalazioni pervenute. In situazioni di criticità, vengono immediatamente adottate azioni di mitigazione, mentre le segnalazioni meno urgenti vengono inserite nel nostro backlog per una successiva analisi approfondita.
Indipendentemente dalla gravità, ogni segnalazione è sottoposta a una valutazione del rischio entro le prime 24 ore dal suo ricevimento, garantendo una rapida risposta alle potenziali vulnerabilità.

L'intera infrastruttura dell'organizzazione è ospitata su AWS in un ambiente cloud. L'adozione di best practice, come la riduzione degli accessi e la segregazione delle

reti, contribuisce a garantire una robusta sicurezza nell'ambiente cloud. Inoltre, l'organizzazione si impegna costantemente a utilizzare sistemi operativi e dipendenze aggiornate per mantenere al massimo il livello di sicurezza.

Per mitigare ulteriormente i rischi, gli amministratori di sistema evitano l'utilizzo del Root admin di AWS. Questa precauzione è stata adottata per prevenire eventuali conseguenze negative in caso di compromissione di una chiave o di un account amministrativo subordinato, riducendo così la possibilità di essere espulsi dall'ambiente di lavoro.

Protocolli in atto per lo smaltimento sicuro dell'hardware obsoleto o danneggiato

Al fine di prevenire la fuga di informazioni e rispettare le normative ambientali l'organizzazione mette in atto con regolarità un processo di cancellazione totale dei dati immagazzinati su macchine e dispositivi mobili al momento della conclusione del rapporto di lavoro di un dipendente o della dismissione di un dispositivo. Questo approccio sistematico mira a garantire la tutela delle informazioni sensibili, riducendo al minimo il rischio di accessi non autorizzati e contribuendo a preservare la sicurezza dei dati aziendali.

Per quanto riguarda le normative ambientali, attualmente l'organizzazione ha adottato un approccio mirato al corretto smaltimento esclusivamente dei dispositivi in leasing, affidando questa responsabilità al fornitore di servizi. Per i dispositivi di proprietà, l'organizzazione si propone di adottare un approccio altrettanto responsabile attraverso la Raccolta Differenziata degli Apparecchi Elettrici ed Elettronici (RAE). È importante notare, tuttavia, che attualmente non sono disponibili documenti storici o bolle che attestino la pratica di smaltimento in passato.
L'impegno dell'organizzazione nella gestione ambientale e nella sicurezza dei dati riflette la sua profonda attenzione alla conformità normativa e alla responsabilità

sociale. L'organizzazione si propone di adottare le migliori pratiche in entrambi i settori, con l'obiettivo di garantire il rispetto delle normative ambientali.

Gestione intelligente del monitoraggio e dei punti di accesso verso l'esterno

La configurazione per l'applicativo principale è descritta nell'allegato ''UNGUESS System" rientrante negli allegati che fanno parte del Modello di Gestione Privacy adottato da UNGUESS. Tale Allegato descrive l'infrastruttura IT in Cloud di UNGUESS e i sistemi di protezione insiti dell'infrastruttura stessa ed è possibile affermare che, per il tipo di infrastruttura adottato, tutto il controllo è elaborato a livello di firewall e non di gateway.

Gestione delle politiche di backup e disaster recovery per i server nel cloud

UNGUESS al fine di evitare che la mancanza di backup adeguati o piani di Disaster Recovery, in relazione ai servizi nel cloud, possa portare a perdita di dati o interruzioni prolungate, prevede che l'integralità della struttura tecnologica sia minuziosamente delineata attraverso l'approccio di Infrastructure as Code (IaC) mediante l'utilizzo del AWS Cloud Development Kit (CDK).

Tale metodologia permette di esprimere le componenti dell'infrastruttura come codice, facilitando la gestione, la documentazione e la riproducibilità del setup. Benché il processo non sia completamente automatizzato, la capacità di ricostruire l'intera infrastruttura da zero in pochi minuti rappresenta un aspetto cruciale dell'efficienza operativa. Questa flessibilità consente all'organizzazione di adattarsi rapidamente a cambiamenti, implementare miglioramenti e rispondere prontamente alle esigenze in continua evoluzione.