Autore	Ufficio privacy
Approvazione	Alberto Cazzulani

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio privacy	01/11/2026	01/11/2026	Prima emissione

PARERE DPO OK

MY 231

RESPONSABILE DEL TRATTAMENTO					
Denominazione	Zucchetti Spa				
Partita Iva	05006900962				
Indirizzo	Piazza Mino Zucchetti,1				
Città	Lodi	**Cap**	26900	**PV**	LO
Legale Rappresentante	Alessandro Zucchetti preposto dalla società CONVERTENDO SRL, Legale rappresentante di Zucchetti SPA				

STRUTTURA ORGANIZZATIVA			
Divisione	Divisione HR	Responsabile Divisione	Uggeri Domenico
Area	Area Piattaforma Base HR & Tools	Responsabile Reparto	Alberto Cazzulani

INCARICATI DEL TRATTAMENTO
Addetti analisi, sviluppo, controllo qualità, help desk, consulenti applicativi, sistemisti

DATI DI CONTATTO			
Responsabile del trattamento	Zucchetti Spa	ufficio.privacy@zucchetti.it	03715941
Rappresentante del titolare	N/A		
Responsabile protezione dati (DPO)	Z Holding Spa	dpo@zucchetti.it	03715943191

DESCRIZIONE
My 231 è il software pensato per gestire il Modello 231 e le attività dell'Organismo di Vigilanza in maniera semplice e veloce. Tale software è indispensabile per supportare l'Organismo di Vigilanza nello svolgimento delle proprie attività, dalla revisione del modello e delle sue parti speciali alla gestione degli audit, alla calendarizzazione e verbalizzazione delle riunioni, alla gestione dei flussi informativi, alla predisposizione del piano di attività dell'OdV, alla verifica dell'implementazione dei diversi presidi. My 231 permette di gestire più efficacemente l'applicazione del modello all'interno dell'organizzazione: automatizza le attività e i processi legati all'applicazione del modello e rende più efficiente e «viva» la gestione e l'applicazione del modello all'interno dell'azienda fornisce una documentazione completa e aggiornata delle misure di prevenzione e controllo adottate supporta l'azienda nel documentare l'adozione delle misure di prevenzione e controllo ai fini della responsabilità amministrativa ai sensi del modello 231. Inoltre, grazie ai diversi strumenti di condivisione e informazione, è anche uno strumento fondamentale per l'informazione e la formazione di tutti i dipendenti e collaboratori

FINALITA' DEL TRATTAMENTO

Il Responsabile del trattamento tratta i dati per finalità di creazione utenza, assistenza e manutenzione al Titolare. Si fa presente che il Responsabile non ha accesso alle informazioni contenute all'interno dell'applicativo, che restano pertanto accessibili esclusivamente al Titolare

CATEGORIA INTERESSATI

Dipendenti, apprendisti, tirocinanti, stagisti, collaboratori, fornitori, appaltatori, visitatori, Gestori a seconda della scelta del Cliente su chi avrà accesso alla piattaforma My Governance.

CATEGORIE DI DATI PERSONALI

Come evidenziato, il Responsabile non ha accesso ai dati personali inseriti all'interno dei vari applicativi. Il Responsabile ha unicamente accesso, ai fini della registrazione all'interno del Sistema e per la sua manutenzione, al nome, cognome e indirizzo email degli utenti.

CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI

Aziende del gruppo Zucchetti
Subappaltatori
Amazon Web Service EMEA SARL come provider di DC
MongoDB, come Database.
PAR-TEC S.p.A. quale partner fornitore di attività di assistenza sistemistica estesa H24

TRASFERIMENTO DATI ALL'ESTERO

No

TERMINI PER LA CANCELLAZIONE DEI DATI

In ogni caso i dati conservati nel Data Center fornito in cloud da AWS saranno conservati per tutta la durata del contratto e successivamente, per il tempo e nelle modalità stabilite contrattualmente col Cliente oppure su richiesta del Titolare, potranno essergli consegnati con una estrazione unica entro 30 giorni dalla fine del contratto.
I dati relativi alla gestione amministrativa e giuridica del rapporto contrattuale saranno conservati per 10 anni dalla cessazione del rapporto contrattuale.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza già implementate o configurabili nel sistema applicativo sono:

- *Gestione delle credenziali di accesso:*

- E-mail: l'accesso al sistema avviene solo attraverso l'identificazione univoca del soggetto che vi accede.
- Password: password con requisiti minimi di sicurezza garantiti. Le regole di complessità della password sono quelli standard secondo le best practice di settore (minimo 15 caratteri, massimo 30, almeno una maiuscola, una minuscola, un carattere speciale e un numero).
- Criteri di complessità per le impostazioni delle credenziali: le credenziali di accesso possono essere impostate secondo diversi criteri di complessità dal Titolare.
- Il Sistema prevede la funzione di blocco account a tempo oppure il blocco account per superamento tentativi di login fail.
- Disattivazione/disabilitazione credenziali: non appena comunicato dal Titolare, il Responsabile entro le successive 24 ore provvederà alla cancellazione delle credenziali.
- È possibile implementare una two factor authentication attraverso un sistema di otp inviato tramite email.
- Profili di autorizzazione: il Titolare può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti, in particolare nella individuazione admin/user.

- *Minimizzazione:*

- Profili di autorizzazione: il Titolare può configurare l'accesso ad utenti basati su differenti livelli di configurazione, in base ai permessi ricevuti (admin/user) l'utente visualizzerà parti differenti dell'applicativo.

- *Identificazione di chi ha trattato i dati:*

- Strumenti di log: su richiesta del Titolare il Responsabile potrà scaricare i log al sistema.

- *Tecniche di crittografia:*

L'intero ciclo di gestione dei file viene crittografato utilizzando l'algoritmo di crittografia AES256 (Crypting protocol: "Advanced Encryption Standard" (lo stesso che usa il governo USA) AES / CBC / NOPADDING). Durante la comunicazione "in transito" tramite TLS / Protocolli HTTPS. Tutto lo spazio di archiviazione è crittografato AES256. Il DB è crittografato tramite crypting at rest.

- *Privacy by default*

- Attivazione profilo utente: gli utenti nel portale sono attivati secondo una logica di non assegnare alcun profilo autorizzativo sui dati trattati. Sarà il Titolare in autonomia a scegliere la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di

autorizzazione individuale. In particolare, il Titolare potrà individuare la funzione admin, ruolo che consente di di gestire i processi aziendali. Tale funzione viene assegnata o a un singolo ricevente, ovvero a un comitato di riceventi, a seconda delle necessità del Titolare.

- *Diritti degli interessati:*

- Diritti degli interessati: per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che potrà informare il Responsabile per provvedere alla cancellazione. Nei singoli applicativi saranno presenti quindi solo informazioni anonime non riconducibili neppure indirettamente ad alcun interessato. La funzione di cancellazione avviene per anagrafico soggetto.

ULTERIORI MISURE DI SICUREZZA

Misure di sicurezza	Commenti
Mettere in sicurezza lo stabile che ospita l'infrastruttura IT utilizzata per elaborare e trasferire i dati	I dati della piattaforma My Governance sono conservati sui server Europei di AWS.
Limitare il numero di soggetti autorizzati ad accedere ai dati e all'infrastruttura IT utilizzata per elaborare e trasferire i dati	La società che fa manutenzione alla piattaforma è stata debitamente individuata come Amministratore di Sistema. L'accesso fisico ai data center AWS viene registrato, monitorato e conservato. L'accesso fisico è controllato ai punti di ingresso dell'edificio da personale di sicurezza professionale che utilizza sistemi di sorveglianza, rilevamento e altri mezzi elettronici. Il personale autorizzato utilizza meccanismi di autenticazione a più fattori per accedere ai data center. Gli ingressi alle sale server sono protetti con dispositivi che emettono allarmi per avviare una risposta a un incidente se la porta viene forzata o tenuta aperta. I sistemi elettronici di rilevamento delle intrusioni sono installati all'interno del livello dati per monitorare, rilevare e avvisare automaticamente il personale appropriato di incidenti di sicurezza. I punti di ingresso e di uscita verso le sale server sono protetti con dispositivi che richiedono a ciascun individuo di fornire l'autenticazione a più fattori prima di concedere l'ingresso o l'uscita. Questi dispositivi emetteranno allarmi se la porta viene forzata aperta senza autenticazione o tenuta aperta. I dispositivi di allarme porta sono inoltre configurati per rilevare le istanze in cui un individuo esce o entra in un livello dati senza fornire l'autenticazione a più fattori.
Assicurare un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza	Grazie alla società terza che garantisce la continuità del Data Center (DC) si assicurerà un approvvigionamento energetico continuo all'infrastruttura IT utilizzata per elaborare i dati, in particolare dotandola di sistemi energetici di emergenza
Assicurare che l'accesso ai dati avvenga in maniera controllata	L'accesso ai dati può avvenire solo in maniera controllata, grazie agli alti standard di sicurezza con cui viene protetto il DC e alla criptazione dei dati.

	L'accesso fisico al data center è fornito solo ai dipendenti autorizzati. Tutti i dipendenti che necessitano dell'accesso al data center devono prima richiedere l'accesso e fornire una giustificazione aziendale valida. Queste richieste vengono concesse in base al principio del privilegio minimo, in cui le richieste devono specificare a quale livello del data center l'individuo deve accedere e sono limitate nel tempo. Le richieste vengono esaminate e approvate da personale autorizzato e l'accesso viene revocato allo scadere del tempo richiesto. Una volta concessa l'ammissione, le persone sono limitate alle aree specificate nelle loro autorizzazioni.
Assicurare che i dati siano protetti da perdita o distruzione accidentale	Per assicurare che i dati siano protetti da perdita o distruzione accidentale si utilizzano copie di backup dislocate in posizioni geografiche differenti. Tale livello di protezione ridurrà al minimo la possibilità di perdita e comunque nel caso dovesse avvenire sarà sicuramente molto limitata.
Assegnare credenziali di autenticazione univoche	Ogni soggetto coinvolto nel trattamento avrà assegnate credenziali di autenticazione composte da un codice per l'identificazione ("User ID") associato a una parola chiave ("password") secondo gli standard migliori oggi presenti sul mercato. Password con sicurezze minime garantite
Garantire complessità della password	La password di accesso dovrà rispettare quantomeno i seguenti requisiti: ● almeno 16 caratteri ● almeno una lettera maiuscola ● almeno una lettera minuscola ● almeno un simbolo speciale ● almeno un numero Al terzo tentativo errato di inserimento di una password l'utenza verrà bloccata per 30 minuti. La password di accesso al software deve essere cambiata ogni 90 giorni, con una password diversa dalle tre precedenti dello storico.
Assicurare che lo User ID assegnato ad un Utente non possa essere assegnato ad un altro incaricato in tempi diversi	Questo deve essere garantito dal Titolare in quanto lo user ID è l'indirizzo email

Assicurarsi che le credenziali vengano disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali	Questo dovrà essere eseguito dal Titolare che provvederà a rimuovere gli utenti dall'anagrafica. Tali utenti avranno in ogni caso accesso ai documenti già approvati. Ad ogni modo è possibile resettare la password oppure sospendere l'utente
Assicurare che: i. quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso venga utilizzato un sistema di autorizzazione. ii. i profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, siano individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. iii. periodicamente, e comunque almeno annualmente, verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	Confermato Con l'assunzione vengono resi disponibili i documenti di sistema per la nuova risorsa e più precisamente: - la politica di sicurezza delle informazioni; - la disciplina sul corretto utilizzo degli strumenti assegnati al fine di non compromettere la sicurezza delle risorse aziendali; - le procedure e le istruzioni relative al ruolo e ai compiti - sottoscrizione di accordo di riservatezza
Proteggere i dati dal rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale: i. mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza quotidiana; ii. effettuare aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti su base quotidiana	Confermato Per la valutazione delle vulnerabilità dei sistemi: - si può avvalere di consulenti esterni individuati allo scopo di effettuare test di penetrazione (con frequenza almeno biennale), ovvero utilizzando software ad hoc che effettueranno test di vulnerabilità automatici su base ricorrente; - ha implementato un processo di monitoraggio delle vulnerabilità e ha adottato una policy di patch che prevede la fornitura di patch di sicurezza periodiche, infine implementate anti-malware sui componenti; - permette al Cliente di condurre test di penetrazione, valutazioni di vulnerabilità e sopralluoghi presso le sedi.
Assicurare che il trattamento avvenga utilizzando software (ivi incluso il sistema operative, il middleware e le applicazioni) dotati di funzioni di sicurezza all'avanguardia	Confermato
Assicurare che sia effettuato un back-up almeno con frequenza quotidiana	Grazie alla società terza proprietaria dei server si assicurerà che sia effettuato un back-up almeno con

	frequenza quotidiana. Si possono distinguere 3 tipi di backup: infrastruttura, database e storage.
Assicurare che i dati possano essere recuperati entro un determinato termine massimo (non più di 7 giorni)	Sì è presente un piano di Business Continuity e Disaster Recovery
Garantire che i dati utilizzati per l'autenticazione siano protetti con efficaci misure di sicurezza crittografica	Sì
Assicurarsi che i dati trasferiti siano protetti utilizzando procedure di crittografia aggiornate	Sì Sono utilizzate le applicazioni di mongoDB atlas: https://www.mongodb.com/products/capabilities/security/encryption
Le categorie particolari di dati personali sono protette utilizzando procedure di crittografia aggiornate	Normalmente non vengono trattate categorie particolari di dati personali ma in ogni caso i dati in nostro possesso sono sempre crittografati
Assicurarsi che sia possibile verificare e stabilire se e chi ha avuto accesso o ha inserito, ha modificato o cancellato i dati nei sistemi di elaborazione dati. I log devono essere disponibili per almeno un anno	Confermato
Garantire che siano regolarmente eseguiti test di vulnerabilità e di penetrazione	Cadenza annuale (da soggetti esterni) o su base ricorrente mediante software ad hoc
Qualora una violazione o vulnerabilità sia identificata nell'ambito del trattamento o in qualsiasi sistema utilizzato per fornire i servizi del Responsabile, informare immediatamente il Titolare del trattamento in merito all'evento e alle misure adottare per porvi rimedio	Sì è presente una policy di gestione incidenti
Garantire che l'accesso ai dati sia limitato ai soli dati necessari per effettuare le operazioni di trattamento.	Sì by default
Limitare il numero di Incaricati autorizzati a svolgere attività connesse al trattamento dei dati	Sì by default
Erogare apposita formazione nei confronti degli Incaricati con riferimento alla normativa vigente in materia di tutela dei dati personali, alle misure di sicurezza	Sì E' prevista un'adeguata formazione sulla Cyber Security, al fine di garantire che tutto il personale sia informato sui rischi per la sicurezza incorsi nell'utilizzo delle risorse aziendali e adeguatamente formato per consentire allo stesso di riconoscere situazioni di potenziale e/o concreta minaccia per la sicurezza. Viene inoltre svolta una formazione specifica per i rischi di cybersecurity come quelli legati al phishing e tutte le problematiche connesse al GDPR. Il programma di formazione è costruito e adattato

	ai diversi ruoli e compiti svolti in azienda. L'efficacia di tale programma è verificata periodicamente, e comunque almeno annualmente, al fine di intraprendere le necessarie azioni correttive e/o integrarlo alle nuove esigenze conoscitive che possono sorgere.
Mantenere una lista aggiornata degli Incaricati	Presente
Mantenere una copia di riserva aggiornata dei dati e del software utilizzato per il trattamento	Presente
Garantire che i Dati vengano archiviati applicando misure idonee a proteggerli da accessi non autorizzati, modifiche, danni e distruzione	Presente
Assicurarsi che i dati vengano cancellati in modo irreversibile in caso di sostituzione o riutilizzo dell'hardware	Sì by default Al termine del rapporto di lavoro l'ufficio informatico, tempestivamente informato dalla funzione HR, provvede al ripristino dei dispositivi aziendali assegnati a ciascun dipendente e alla chiusura/cancellazione dei profili/utenti in nome dello stesso. Sono definite adeguate procedure per la restituzione dei beni (es. computer portatili, cellulari, documenti, software, manuali, carte di credito) assegnati al personale che ha cessato il rapporto di lavoro.
Escludere o limitare le copie dei dati (incluse le stampe) e assicurare la corretta distruzione dopo l'utilizzo	Sì by default
Proteggere i documenti cartacei contenenti dati utilizzati durante l'elaborazione al momento della stampa, archiviazione, distruzione e scambio	Non viene utilizzato alcun documento cartaceo
Garantire la sicurezza della rete su cui viene eseguito il trattamento (sistema firewall, proxy, sistemi di rilevamento delle intrusioni o altri dispositivi attivi o passivi)	Presente ✓ monitora il traffico sulle proprie reti e sui sistemi informatici al fine di rilevare possibili attacchi alla sicurezza informatica e interruzioni del sistema e informa il personale; ✓ mantiene registri ed effettuare prove adeguate per consentire l'indagine sugli incidenti e preserva la custodia di tali dati, anche per procedimenti giudiziari o di prova; ✓ ha una procedura di gestione dell'incidente

	(Rilevamento, classificazione, inizio indagine e contenimento, risoluzione incidente, chiusura dell'incidente, creazione di un quadro per risoluzione di incidenti simili e valutazione del quadro)

Queste misure di sicurezza devono essere correttamente impostate da parte del Titolare.

2. MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA DI PRIMO LIVELLO

ASSISTENZA ON SITE

Gli addetti Zucchetti offrono al Titolare formazione e sono disponibili a recarsi anche on site per eventuali supporti, ferma restando l'assistenza continua da remoto secondo gli SLA condivisi con il cliente.
In questo caso gli addetti My Governance lavorano come se facessero parte della struttura del Titolare ed adottano tutte le procedure di sicurezza implementate dallo stesso. I Titolari potranno generare utenze individuali per l'accesso ai loro sistemi, oppure potranno far accedere in affiancamento per formare il loro personale.
Qualora durante l'attività di assistenza l'addetto My Governance abbia la necessità di prelevare archivi o db di cui necessita per risolvere le problematiche evidenziate è necessario che informi il Titolari e registri tale attività sulla Nota di intervento..

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite email i tecnici Zucchetti rendono sempre disponibile tramite link la possibilità per Titolare di leggere l'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.
L'addetto Zucchetti non è autorizzato a farsi mandare le credenziali di accesso del Titolare via email né tantomeno potrà salvarle sullo strumento di ticketing.
Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico My Governance è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR. Quindi il tecnico My Governance dovrà richiedere credenziali individuali oppure collegamento tramite strumenti a ciò dedicati.

ASSISTENZA ATTRAVERSO COLLEGAMENTO DA REMOTO SU IP PUBBLICI OPPURE TRAMITE VPN

Qualora l'attività di assistenza debba essere svolta su sistemi cloud su IP pubblici oppure tramite VPN o accessi privati è necessario che gli addetti Zucchetti entrino nei sistemi dei Titolari:

- Previa autorizzazione del cliente
- Previa ricezione delle credenziali individuali e le stesse siano state attivate per il tempo necessario all'esecuzione delle attività richieste
- al termine dell'attività siano disattivate le credenziali da parte del Titolare

Personale di Help Desk

La creazione dell'utenza deve essere richiesta solo al Titolare che, attraverso l'amministratore di applicazione, potrà creare il nuovo utente.
Non deve mai essere utilizzato l'utente amministratore da parte degli operatori di assistenza.

3 MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS e AL DATA CENTER

Zucchetti pone i propri sistemi sul server certificato di AWS.
Relativamente ai servizi offerti da AWS, di seguito ulteriori specifiche:
- ***BACKUP:*** si distinguono tre diversi tipi di backup: infrastruttura, database e storage.
  - Infrastruttura: tutti i server utilizzati per eseguire la nostra applicazione
  - Database: contiene tutti i dati visualizzati sull'applicazione
  - Server di archiviazione: contiene tutti i file visualizzati sull'applicazione.

- *ZONE DI DISPONIBILITÀ*: Una zona di disponibilità è un data center logico in una regione disponibile per l'utilizzo da parte di qualsiasi infrastruttura AWS.
Ogni zona di una regione dispone di alimentazione, rete e connettività ridondanti e separate per ridurre la probabilità che due zone si guastino contemporaneamente. Ci sono tre AZ (Availability Zone) nella regione di Francoforte. Se uno dei nodi dell'infrastruttura si interrompe, gli altri 2 sono in esecuzione.

- *SICUREZZA PIATTAFORMA*: la piattaforma risiede su Amazon Virtual Private Cloud (VPC – nella fattispecie AWS EC2), ma con tecnologia Serverless (Fargate), pertanto la responsabilità è di AWS.

1) ECS Fargate {Serverless): AWS Fargate soddisfa la conformità ai fini PCI DSS Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3 e HIPAA.
Come servizio gestito, Amazon Elastic Container Service è protetto dalle procedure di sicurezza della rete globale di AWS.
L'utilizzo di ECS con i servizi Fargate non viene eseguito direttamente su un sistema operativo che può causare vulnerabilità alla nostra applicazione web.
Il codice della nostra applicazione viene verificato a livello di sviluppo prima di essere inviato alla finestra mobile; quindi, la protezione antivirus è una preoccupazione per gli sviluppatori della nostra applicazione web.
Poiché la nostra infrastruttura utilizza effettivamente immagini docker, i nostri sviluppatori verificano il codice prima di eseguire il commit.

2) Cloudflare Security Services:: offre le seguenti funzionalità:

Protezione DDoS avanzata per servizi e applicazioni esposte su Internet
Cloudflare fornisce una protezione DDoS always-on attraverso la propria rete globale distribuita, monitorando e analizzando in tempo reale il traffico in ingresso. I meccanismi di rilevamento basati su analisi comportamentale, threat intelligence e identificazione delle anomalie consentono di individuare e mitigare automaticamente attacchi volumetrici e tentativi di saturazione delle risorse, garantendo la continuità operativa dei servizi pubblicati.

Mitigazione degli attacchi in linea
Le funzionalità di mitigazione sono integrate nativamente nell'infrastruttura Cloudflare e vengono applicate in linea senza impatti significativi sulle prestazioni. Il traffico malevolo viene identificato e filtrato attraverso tecniche di rate limiting, traffic shaping, challenge automatici, reputazione degli

indirizzi IP e analisi del comportamento delle richieste. La protezione copre sia gli attacchi di rete (Layer 3 e 4) sia gli attacchi rivolti al livello applicativo (Layer 7).

Web Application Firewall (WAF) e protezione OWASP Top 10

Cloudflare integra un Web Application Firewall (WAF) con regole gestite e continuamente aggiornate per la protezione delle applicazioni web. Il servizio consente di prevenire e mitigare le principali vulnerabilità applicative individuate dall'OWASP Top 10, tra cui SQL Injection (SQLi), Cross-Site Scripting (XSS), Remote Code Execution (RCE), Path Traversal e altre minacce rivolte ai servizi web. Le richieste HTTP/HTTPS vengono analizzate in tempo reale e bloccate prima di raggiungere i sistemi esposti.

Protezione da bot e controllo degli accessi automatizzati

Cloudflare include funzionalità di identificazione e gestione del traffico automatizzato che consentono di mitigare attività malevole generate da bot, crawler non autorizzati e tentativi di abuso delle applicazioni. Tali funzionalità contribuiscono alla protezione delle risorse applicative da attività fraudolente, scansioni automatiche e tentativi di sfruttamento delle vulnerabilità.AWS Shield Standard fornisce un monitoraggio del flusso di rete sempre attivo che ispeziona il traffico in entrata ai servizi AWS e applica una combinazione di firme del traffico, algoritmi di anomalia e altre tecniche di analisi per rilevare il traffico dannoso in tempo reale. Shield Standard imposta soglie statiche per ogni tipo di risorsa AWS, ma non fornisce alcuna protezione personalizzata alle applicazioni dei clienti AWS.

3) Cloudflare Web Application Firewall (WAF): Cloudflare WAF è un firewall applicativo cloud-native che consente di monitorare, filtrare e proteggere il traffico HTTP(S) diretto alle applicazioni web pubblicate su Internet.

Sono state abilitate regole di sicurezza gestite e costantemente aggiornate, basate sulle migliori pratiche di settore e sulle vulnerabilità identificate dall'OWASP Top 10, al fine di proteggere le applicazioni web dai principali vettori di attacco, tra cui:

A01 - Broken Access Control

A02 - Cryptographic Failures (Sensitive Data Exposure)

A03 - Injection (SQL Injection, Command Injection, ecc.)

A04 - Insecure Design

A05 - Security Misconfiguration

A06 - Vulnerable and Outdated Components

A07 - Identification and Authentication Failures

A08 - Software and Data Integrity Failures

A09 - Security Logging and Monitoring Failures

A10 - Server-Side Request Forgery (SSRF)

Il servizio analizza in tempo reale le richieste HTTP(S) e applica controlli di sicurezza finalizzati all'identificazione e al blocco di traffico malevolo, tentativi di sfruttamento delle vulnerabilità applicative, scansioni automatiche e attività riconducibili a bot dannosi.

Cloudflare WAF integra, inoltre, funzionalità avanzate di Rate Limiting, Bot Protection, IP Reputation Filtering e regole personalizzabili, consentendo di adattare la protezione alle specifiche esigenze dell'applicazione e del contesto operativo.

La piattaforma mette a disposizione dashboard centralizzate per il monitoraggio degli eventi di sicurezza, la visualizzazione delle metriche di traffico, l'analisi dei tentativi di attacco e la gestione delle policy di protezione, garantendo piena visibilità e controllo sullo stato di sicurezza delle applicazioni esposte.

- ***INFRASTRUTTURA DI BACKUP E RIPRISTINO***

Sono presenti 3 zone di disponibilità, quindi 3 data center ridondanti.
E' prevista comunque una procedura di ripristino, le cui specifiche sono fornite su richiesta.
In ogni caso per il ripristino del DB si utilizza il servizio cloud Mongo Atlas, che garantisce di rispettare i tempi di RPO ed RTO.
Come storage si utilizza Amazon S3.

Per ulteriori informazioni tecniche relativamente ai servizi offerti da AWS si rimanda ai seguenti link

- https://aws.amazon.com/it/legal/
- https://aws.amazon.com/it/compliance/
- https://aws.amazon.com/it/s3/
- https://aws.amazon.com/it/backup/.