

Zero Trust Security: Gestione dell'Identità e Autenticazione Utente nell'Architettura Zero Trust

Questo articolo fa parte della serie dedicata all'architettura Zero Trust, un modello di sicurezza fondamentale per le organizzazioni moderne. In questo approfondimento, esploreremo il primo pilastro dell'architettura: la gestione dell'identità e della fiducia dell'utente. Analizzeremo le tecnologie chiave come l'autenticazione multi-fattore (MFA), il passwordless authentication, il Single Sign-On (SSO) e i sistemi avanzati di Identity Governance, evidenziando come questi elementi si integrino per creare un robusto sistema di gestione delle identità digitali.

Zero Trust e Gestione dell'Identità Utente: Principi e Implementazione

Al centro del modello Zero Trust vi è l'utente, o meglio la fiducia riposta nell'utente, non in modo generico ma in relazione al ruolo ricoperto all'interno dell'organizzazione. Ogni organizzazione, anche di media complessità, non può più permettersi di applicare privilegi di accesso uniformi. È essenziale raggruppare gli utenti in base ai loro ruoli e alle autorizzazioni necessarie per l'accesso ai servizi, definendo specifiche forme di autenticazione in funzione del profilo di rischio associato.

La fiducia negli utenti si basa sul garantire che l'utente sia effettivamente chi dichiara di essere e non un impostore. Tranne in rari casi, oggi si utilizza l'autenticazione multi-fattore (MFA), in cui si richiede all'utente di fornire una

combinazione di credenziali, come una password, un dispositivo fisico (smart card, chiave USB, dispositivo di prossimità) e un elemento biometrico (impronta digitale, riconoscimento facciale, iride). L'MFA è diventato uno standard per garantire un alto livello di sicurezza.

Per semplificare l'esperienza utente, è possibile adottare tecnologie come l'autenticazione senza password (passwordless) e il Single Sign-On (SSO); l'adozione di tali tecnologie se non correttamente gestite ad esempio nella durata delle sessioni SSO o senza implementare anche le ulteriori fasi dello zero trust potrebbero essere fonti di rischio anche se è indubbio, che riducono il numero di password da ricordare e richiedono un numero inferiore di autenticazioni un'unica autenticazione giornaliera per accedere ai sistemi. In determinati contesti, può essere richiesta un'autenticazione più forte utilizzando magari anche più di 2 fattori, ad esempio per l'accesso a sistemi critici, mentre per situazioni a basso rischio potrebbe essere sufficiente un'autenticazione più semplice limitandosi alla sola coppia username e password.

L'adozione di un modello fiduciario per l'utenza costituisce il primo passo verso un modello di sicurezza più complesso e completo, ma finché non si ha certezza dell'identità dell'utente, è difficile implementare ulteriori tecnologie avanzate per proteggere completamente il DAAS in esame secondo gli altri elementi del modello Zero Trust.

La gestione dell'identità in un contesto Zero Trust va oltre la semplice autenticazione multi-fattore che rimane comunque uno dei pilastri fondamentali. Secondo le ricerche del SANS Institute, un'implementazione efficace deve includere:

- Analisi comportamentale degli utenti (User Behavior Analytics – UBA)
- Autenticazione adattiva basata sul rischio
- Gestione del ciclo di vita delle identità
- Governance delle identità e degli accessi (IGA)

L'implementazione completa di tutti questi elementi richiede l'integrazione di diverse tecnologie e framework che spaziano da metriche collezionate sulle abitudini degli utenti, a metodologie avanzate di gestione dell'identità nell'intero ciclo di vita aziendale per ottenere un modello di autenticazione che si adatti in base alla situazione ed alla rilevanza del DAAS a cui si accede.

Al centro del modello Zero Trust vi è l'utente, o meglio la fiducia riposta nell'utente, non in modo generico ma in relazione al ruolo ricoperto all'interno dell'organizzazione. Ogni organizzazione, anche di media complessità, non può più permettersi di applicare privilegi di accesso uniformi. È essenziale raggruppare gli utenti in base ai loro ruoli e alle autorizzazioni necessarie per l'accesso ai servizi, definendo specifiche forme di autenticazione in funzione del profilo di rischio associato.

La fiducia negli utenti si basa sul garantire che l'utente sia effettivamente chi dichiara di essere e non un impostore. Tranne in rari casi, oggi si utilizza l'autenticazione multi-fattore (MFA), in cui si richiede all'utente di fornire una combinazione di credenziali, come una password, un dispositivo fisico (smart card, chiave USB, dispositivo di prossimità) e un elemento biometrico (impronta digitale, riconoscimento facciale, iride). L'MFA è diventato uno standard per garantire un alto livello di sicurezza.

Per semplificare l'esperienza utente, è possibile adottare tecnologie come l'autenticazione senza password (passwordless) e il Single Sign-On (SSO); l'adozione di tali tecnologie se non correttamente gestite ad esempio nella durata delle sessioni SSO o senza implementare anche le ulteriori fasi dello zero trust potrebbero essere fonti di rischio anche se è indubbio, che riducono il numero di password da ricordare e richiedono un numero inferiore di autenticazioni un'unica autenticazione giornaliera per accedere ai sistemi. In determinati contesti, può essere richiesta un'autenticazione

più forte utilizzando magari anche più di 2 fattori, ad esempio per l'accesso a sistemi critici, mentre per situazioni a basso rischio potrebbe essere sufficiente un'autenticazione più semplice limitandosi alla sola coppia username e password.

L'adozione di un modello fiduciario per l'utenza costituisce il primo passo verso un modello di sicurezza più complesso e completo, ma finché non si ha certezza dell'identità dell'utente, è difficile implementare ulteriori tecnologie avanzate per proteggere completamente il DAAS in esame secondo gli altri elementi del modello Zero Trust.

La gestione dell'identità in un contesto Zero Trust va oltre la semplice autenticazione multi-fattore che rimane comunque uno dei pilastri fondamentali. Secondo le ricerche del SANS Institute, un'implementazione efficace deve includere:

- Analisi comportamentale degli utenti (User Behavior Analytics – UBA)
- Autenticazione adattiva basata sul rischio
- Gestione del ciclo di vita delle identità
- Governance delle identità e degli accessi (IGA)

L'implementazione completa di tutti questi elementi richiede l'integrazione di diverse tecnologie e framework che spaziano da metriche collezionate sulle abitudini degli utenti, a metodologie avanzate di gestione dell'identità nell'intero ciclo di vita aziendale per ottenere un modello di autenticazione che si adatti in base alla situazione ed alla rilevanza del DAAS a cui si accede.

La sicurezza del modello passwordless si basa su alcuni principi fondamentali:

- Crittografia asimmetrica: ogni dispositivo genera una coppia di chiavi unica per ogni servizio. La chiave privata non lascia mai il dispositivo, mentre quella pubblica viene registrata sul server di autenticazione.
- Binding crittografico: le credenziali sono strettamente

legate all'origine (dominio) del servizio, prevenendo attacchi di phishing.

- Verifica locale: l'autenticazione dell'utente (tramite biometria o PIN) avviene localmente sul dispositivo, senza trasmissione di dati sensibili.

Un aspetto cruciale spesso sottovalutato è la gestione dei dispositivi fisici e del cosiddetto recovery flow. Le organizzazioni devono implementare procedure robuste per gestire scenari come:

- Perdita o danneggiamento del dispositivo primario
- Cambio del dispositivo
- Reset delle credenziali biometriche
- Compromissione delle credenziali

Per facilitare l'adozione, è consigliabile implementare un approccio graduale su più fasi, sul modello di quanto esemplificato di seguito.

Fase 1: Introduzione del passwordless come opzione aggiuntiva, mantenendo attivo il sistema tradizionale basato su password.

Fase 2: Incentivazione dell'uso del passwordless attraverso una user experience semplificata e feedback positivo.

Fase 3: Migrazione al passwordless, mantenendo procedure di fallback ben definite per casi eccezionali.

Dal punto di vista della sicurezza, l'autenticazione passwordless offre alcuni vantaggi significativi:

- Eliminazione completa degli attacchi basati su password (phishing, credential stuffing, password spraying)
- Resistenza agli attacchi man-in-the-middle grazie al binding crittografico
- Riduzione della superficie di attacco eliminando la necessità di memorizzare password su sistemi terzi

Tuttavia, come anche specificato in apertura, esistono anche

delle sfide ed alcune criticità di cui tenere conto:

- Necessità di gestire il ciclo di vita dei dispositivi di autenticazione
- Complessità nell'implementazione di procedure di recovery
- Potenziale resistenza degli utenti al cambiamento
- Requisiti hardware specifici per alcune forme di autenticazione biometrica

Una auspicabile evoluzione futura dell'autenticazione passwordless potrà vedere una maggiore integrazione con:

- *Continuous authentication* basata sul comportamento dell'utente
- *Adaptive authentication* che considera il contesto e il rischio
- Integrazione con sistemi di identity governance
- Supporto per scenari di edge computing e IoT

Implementazione del Modello Passwordless nella Zero Trust Architecture

Come introdotto in precedenza, tutte le tecnologie di MFA, inclusa la *passwordless authentication*, possono essere efficacemente utilizzate per implementare questa fase del modello. Inoltre, tecnologie per la centralizzazione delle utenze e della loro gestione oltre che per la gestione dell'autenticazione – ad esempio *Identity Access Management* (IAM), *Identity Governance and Administration* (IGA), *Privileged Access Management* (PAM), *Risk-Based Authentication* (RBA), etc – risultano fondamentali. In questo contesto, le identità degli utenti vengono raccolte e verificate, fornendo informazioni aggiuntive ai sistemi di autorizzazione, in modo da concedere solo i privilegi minimi necessari all'utente per la propria operatività.

Le tecnologie di SSO contribuiscono a semplificare la

quotidianità degli utenti, bilanciando l'adozione di metodi di autenticazione forte con una migliore esperienza dell'utente in termini di riduzione delle password da digitare. Sebbene l'adozione di MFA possa aumentare il livello di sicurezza, l'integrazione di SSO riduce la resistenza al cambiamento dell'utente, migliorando così l'efficienza operativa e l'esperienza complessiva senza compromettere la sicurezza.

L'ecosistema tecnologico per la gestione della fiducia degli utenti si è notevolmente evoluto negli ultimi anni, introducendo soluzioni sempre più sofisticate e integrate. Un'implementazione moderna del Trust degli Utenti richiede l'adozione di tecnologie complementari che lavorano in sinergia per creare un framework di sicurezza robusto e adattivo, in funzione del livello di trust che si intende raggiungere e del bilanciamento fra sicurezza ed esperienza utente. Alcuni elementi di uno stack tecnologico legato a questa gestione sono descritti di seguito.

Identity Governance and Administration (IGA)

I sistemi IGA moderni hanno evoluto le loro capacità ben oltre la semplice gestione delle identità. Le piattaforme IGA di nuova generazione incorporano funzionalità di analisi predittiva e machine learning per identificare pattern anomali nelle richieste di accesso e nei comportamenti degli utenti. Questi sistemi sono in grado di automatizzare il processo di certificazione degli accessi, suggerendo automaticamente modifiche ai privilegi basate sull'utilizzo effettivo delle risorse e sul confronto con profili simili all'interno dell'organizzazione.

Privileged Access Management (PAM) Evoluto e Privileged Identity Management

(PIM)

I sistemi PAM moderni hanno integrato capacità di gestione delle sessioni privilegiate, maggiormente correlati al PIM, con analisi comportamentale in tempo reale. Queste piattaforme non si limitano più a gestire gli accessi e le credenziali privilegiate, ma offrono funzionalità avanzate come:

- Session recording con analisi comportamentale
- *Automatic credential rotation* basata sul rischio
- Just-in-time privilege elevation
- Risk-based access approval workflows
- Integration con threat intelligence feeds

Continuous Authentication

L'autenticazione continua rappresenta un'evoluzione significativa rispetto ai tradizionali sistemi MFA. Questa tecnologia utilizza una combinazione di fattori biometrici comportamentali per verificare continuamente l'identità dell'utente durante una sessione. I fattori analizzati includono:

- Pattern di digitazione
- Movimenti del mouse
- Gesture su dispositivi mobili
- Postura fisica durante l'utilizzo dei dispositivi
- Pattern di navigazione e utilizzo delle applicazioni

Risk-Based Authentication (RBA)

I sistemi RBA moderni utilizzano modelli di machine learning per valutare dinamicamente il rischio di ogni richiesta di accesso. Questi sistemi considerano numerosi fattori contestuali:

- Geolocalizzazione e pattern di movimento

- Caratteristiche del dispositivo e della rete
- Comportamento storico dell'utente
- Sensibilità delle risorse richieste
- Anomalie comportamentali
- Threat intelligence in tempo reale

Customer Identity and Access Management (CIAM)

Per organizzazioni che gestiscono identità di clienti esterni, le piattaforme CIAM moderne offrono funzionalità specifiche per bilanciare sicurezza e user experience:

- Progressive profiling
- Social identity federation
- Privacy preference management
- Consent management
- Customer analytics
- Cross-device identity correlation

Decentralized Identity

Le tecnologie di identità decentralizzata basate su blockchain e standard aperti come *Decentralized Identifiers* (DID) e *Verifiable Credentials* (VC) stanno emergendo come una soluzione promettente per la gestione delle identità digitali tramite digital Wallet personali, pur essendo oggi in fase di sviluppo e di conseguenza con una adozione piuttosto limitata. In particolare, riportano sotto il controllo dell'utente la decisione di cosa condividere e con chi. Queste soluzioni offrono ad esempio:

- Self-sovereign identity management
- Privacy-preserving authentication
- Portable identity attributes
- Immutable audit trail

Security Orchestration and Response (SOAR)

L'integrazione di piattaforme SOAR con i sistemi di gestione delle identità permette di automatizzare la risposta a incidenti di sicurezza legati alle identità:

- *Automatic account suspension* in caso di comportamenti sospetti
- Orchestrazione di workflow di *investigation*
- Automated remediation actions
- *Integration* con sistemi di *incident management*
- *Correlation* con altri eventi di sicurezza

Analytics and Reporting

Le moderne piattaforme di analytics per la gestione delle identità forniscono insights approfonditi attraverso:

- User behavior analytics
- Access pattern analysis
- *Risk scoring* in tempo reale
- Compliance reporting automatizzato
- Predictive analytics per il provisioning
- Anomaly detection basata su machine learning

Zero Standing Privileges (ZSP)

L'implementazione di ZSP rappresenta un'evoluzione del principio del least privilege, dove:

- I privilegi vengono assegnati dinamicamente solo quando necessari
- L'accesso viene automaticamente revocato dopo l'uso
- Ogni elevazione di privilegio richiede una giustificazione
- Le sessioni privilegiate sono monitorate in tempo reale
- Il rischio viene continuamente valutato durante la

sessione

Queste tecnologie, o quota parte di esse, se implementate in modo integrato, creano un ecosistema di sicurezza coeso che supporta sia i requisiti di sicurezza che le esigenze operative dell'organizzazione. La chiave del successo sta nella capacità di orchestrare queste diverse tecnologie in modo da creare un sistema di controllo degli accessi fluido e adattivo, che bilanci sicurezza e usabilità in base al contesto e al rischio.

Soluzioni Moderne per l'Identity Governance in Zero Trust

L'adozione di un modello Zero Trust per la gestione degli utenti e della loro identificazione contribuisce a minimizzare o eliminare i rischi di phishing delle credenziali, mitiga e in certi casi elimina il problema delle password deboli o riutilizzate su più sistemi, spesso con livelli di rischio molto diversi. Inoltre, il modello Zero Trust consente di integrare ulteriori fattori di autenticazione basati su valutazioni estese, che considerano dispositivi, localizzazione dell'utente e modalità di connessione, sia usuale che atipica. Questi fattori aggiuntivi riducono ulteriormente i rischi, fornendo un livello di sicurezza superiore e adattivo che tiene conto del contesto dinamico di ciascun accesso.

La gestione moderna del Trust degli Utenti permette di mitigare una gamma sempre più ampia di rischi, che vanno ben oltre i tradizionali attacchi alle credenziali. L'evoluzione delle minacce cyber ha reso necessario un approccio più sofisticato alla mitigazione dei rischi legati alle identità digitali.

Gli attacchi basati sull'identità sono diventati sempre più sofisticati e multi-vettore. Secondo i dati del Verizon Data

Breach Investigations Report 2024, circa il 70% delle violazioni coinvolge il fattore umano e quindi spesso l'uso improprio di credenziali. Il modello Zero Trust, attraverso una corretta implementazione del Trust degli Utenti, permette di mitigare efficacemente questi rischi emergenti.

Mitigazione degli Attacchi Avanzati

L'architettura moderna di Trust degli Utenti fornisce protezione contro attacchi sofisticati come:

Business Email Compromise (BEC): Gli attacchi BEC sono diventati sempre più comuni e costosi per le organizzazioni. L'implementazione di controlli rigorosi sull'identità, combinata con l'analisi comportamentale, permette di identificare anomalie nelle comunicazioni email e nei pattern di accesso che potrebbero indicare un account compromesso. L'autenticazione forte e la verifica continua dell'identità rendono molto più difficile per un attaccante mantenere il controllo di un account compromesso.

Account Takeover (ATO): Gli attacchi ATO sono stati tradizionalmente difficili da rilevare, specialmente quando l'attaccante opera con discrezione. L'implementazione di sistemi di autenticazione adattiva e analisi comportamentale permette di identificare sottili variazioni nel comportamento dell'utente che potrebbero indicare un account compromesso. Il monitoraggio continuo del comportamento dell'utente, combinato con l'analisi del contesto di accesso, permette di rilevare e bloccare tentativi di takeover anche quando l'attaccante possiede credenziali valide.

Mitigazione dei Rischi Insider

Il Trust degli Utenti moderno affronta anche i rischi provenienti dall'interno dell'organizzazione:

Abuso di Privilegi: Il monitoraggio continuo dell'utilizzo dei

privilegi, combinato con l'implementazione di *Zero Standing Privileges*, riduce drasticamente il rischio di abuso di privilegi da parte di utenti interni. L'accesso viene concesso solo quando necessario e viene continuamente monitorato per identificare comportamenti anomali.

Data Exfiltration: L'integrazione di sistemi DLP con il framework di Trust degli Utenti permette di correlare l'accesso ai dati con i pattern comportamentali dell'utente, identificando potenziali tentativi di esfiltrazione dati. La granularità del controllo degli accessi permette di limitare l'esposizione dei dati sensibili solo agli utenti che ne hanno effettivamente bisogno.

Protezione contro Attacchi Emergenti

Il modello evoluto di Trust degli Utenti fornisce protezione anche contro minacce emergenti sempre più legate all'adozione di tecniche di AI.

Deepfake e Impersonazione Avanzata: L'uso di tecnologie biometriche avanzate, combinate con l'analisi comportamentale, permette di identificare tentativi di impersonazione anche quando vengono utilizzate tecniche sofisticate come i deepfake. La verifica multimodale dell'identità rende molto più difficile per un attaccante simulare contemporaneamente caratteristiche multiple biometriche e comportamentali.

Attacchi basati su AI: Con l'emergere di attacchi automatizzati basati su intelligenza artificiale, il Trust degli Utenti moderno implementa contromisure basate su AI per identificare pattern di attacco sofisticati. L'analisi comportamentale avanzata può distinguere tra interazioni umane genuine e attacchi automatizzati, anche quando questi ultimi sono orchestrati da sistemi AI avanzati.

Mitigazione dei Rischi di Compliance

Il Trust degli Utenti aiuta anche nella mitigazione dei rischi legati alla compliance normativa che spesso sfocia in ammende o reati.

Violazioni di Privacy: L'implementazione di controlli granulari sull'accesso ai dati personali, combinata con audit dettagliati, permette di aumentare la conformità verso normative sulla privacy come il GDPR. La capacità di tracciare e giustificare ogni accesso ai dati personali riduce il rischio di violazioni anche accidentali della privacy.

Segregation of Duties (SoD): Il monitoraggio continuo delle assegnazioni di ruoli e privilegi, combinato con analisi automatizzate delle violazioni, permette di mitigare conflitti di interesse e violazioni delle policy stabilite. L'automazione del processo di review degli accessi riduce il rischio di oversight umani nella gestione delle autorizzazioni.

Resilienza e Recovery

Il modello moderno di Trust degli Utenti migliora anche la resilienza organizzativa.

Compromissione Massiva: In caso di compromissione di massa delle credenziali, la presenza di multiple modalità di autenticazione e verifica continua dell'identità riduce significativamente l'impatto potenziale. La capacità di revocare rapidamente l'accesso e richiedere ri-autenticazione con fattori alternativi permette una risposta rapida agli eventuali incidenti di sicurezza.

Business Continuity: L'implementazione di procedure robuste di recovery e *fallback*, combinate con la capacità di scalare rapidamente i controlli di sicurezza in base al rischio, assicura la continuità operativa anche in scenari di

compromissione delle identità. La presenza di procedure di emergenza ben definite permette di mantenere l'operatività anche quando i sistemi primari di autenticazione non sono disponibili.

In questo articolo abbiamo esaminato approfonditamente come la gestione dell'identità rappresenti il fondamento di un'architettura Zero Trust efficace. Dalle tecnologie di autenticazione multi-fattore ai sistemi avanzati di Identity Governance, abbiamo esplorato gli strumenti e le strategie necessarie per implementare un modello di fiducia zero centrato sull'utente. Nel prossimo articolo della serie, approfondiremo il secondo pilastro fondamentale dell'architettura Zero Trust: il Device Trust e la sicurezza dei dispositivi. Per una comprensione completa dell'architettura Zero Trust e delle sue implementazioni, vi invitiamo a scaricare il white paper "Zero Trust – olo un problema tecnologico?" del Dott. Ing. Fabrizio Fioravanti, che offre un'analisi dettagliata di tutti gli aspetti di questa fondamentale strategia di sicurezza.

Profilo Autore



Fabrizio Fioravanti è attualmente responsabile dell'Unità di Processo Sistemi, tecnologie cloud e di sicurezza informatica presso l'Università degli Studi di Firenze.

Laureato in Ingegneria Elettronica, ha successivamente conseguito il dottorato di ricerca in Ingegneria Informatica e delle Telecomunicazioni e da oltre 25 anni lavora nel settore ICT.

Ha diverse pubblicazioni scientifiche al suo attivo sia su riviste italiane che internazionali, sia che in conferenze, oltre a monografie complete o contributi a monografie.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/zero-trust-utente/>