Trust delle applicazioni e dei privilegi

Questo articolo fa parte di una serie dedicata al modello Zero Trust. n questo approfondimento esploriamo il livello applicativo del modello, focalizzandoci sulla gestione dei privilegi, sulla sicurezza delle applicazioni moderne e sulle tecnologie per implementare efficacemente il Trust delle Applicazioni, riducendo i rischi di accessi non autorizzati e proteggendo i dati sensibili dell'organizzazione.

L'ultimo elemento essenziale per l'implementazione efficace dell'approccio Zero Trust riguarda il livello applicativo, considerando due componenti fondamentali: l'insieme delle applicazioni consentite e vietate all'interno dell'organizzazione e il livello di privilegio che ogni utente ottiene una volta connesso a un'applicazione, sia essa on-premise o in cloud.

Il controllo a livello applicativo è cruciale per la protezione dei dati, che siano dati personali soggetti al GDPR o dati strategici per l'organizzazione, come risultati di ricerca, brevetti o piani strategici. La protezione del dato secondo le tre direttive RID (Riservatezza, Integrità, Disponibilità) richiede una piena implementazione del modello Zero Trust per ridurre i rischi correlati.

Questo livello di controllo non è raggiungibile se i precedenti elementi del modello Zero Trust non sono stati affrontati correttamente dal punto di vista organizzativo. Ad esempio, non è praticabile creare una whitelist o blacklist di applicazioni senza che il dispositivo sia sotto la gestione dell'organizzazione e che siano implementate policy di compliance per gli applicativi permessi o vietati. Analogamente, risulta inefficace assegnare privilegi agli utenti senza verificare la loro identità e la modalità con cui

si collegano alla rete.

Gestione dei privilegi e principio del privilegio minimo

La gestione dei privilegi e l'applicazione del principio del privilegio minimo all'interno di un'organizzazione riducono il rischio di accessi non autorizzati o alterazioni ai dati, proteggendo anche da danni accidentali. Limitare l'operatività di ciascun utente a un contesto definito è fondamentale per minimizzare tali rischi. Per migliorare il controllo, è consigliabile segmentare ulteriormente i contesti operativi, assegnando ruoli specifici all'interno dei processi IT e aziendali. In situazioni che richiedono un livello più ampio di operatività, è preferibile limitare i ruoli per evitare conflitti (ad esempio, l'amministratore del backup non dovrebbe essere anche l'amministratore del sistema di identity management).

Nel caso di operatività su livelli di sicurezza diversificati, l'utilizzo di utenze separate per diversi layer di sicurezza può essere utile. Ad esempio, l'account utilizzato per le operazioni quotidiane di office automation dovrebbe essere distinto da quello per l'amministrazione dei sistemi, con ogni utenza associata a un differente livello di sicurezza. Potrebbero inoltre essere necessarie utenze "emergenziali" con privilegi elevati, destinate a situazioni critiche e protette da autenticazione multifattore o doppia verifica.

L'approccio moderno alla sicurezza delle applicazioni in un contesto Zero Trust si basa sul concetto di "Zero Trust Application Security" (ZTAS), che estende i principi Zero Trust al livello applicativo. Secondo le ricerche del SANS Institute, questo approccio richiede:

- Runtime Application Self-Protection (RASP): Integra la sicurezza direttamente nel runtime dell'applicazione,

permettendo il rilevamento e il blocco di attacchi in tempo reale.

- API Security: In un’architettura moderna basata su microservizi, la sicurezza delle API diventa cruciale, gli attacchi alle API potranno diventare uno dei vettori più comuni per le violazioni delle applicazioni enterprise.
- Secure Software Supply Chain: La recente enfasi sulla sicurezza della supply chain software, evidenziata da incidenti come SolarWinds, ha portato all’emergere di framework come SLSA (Supply chain Levels for Software Artifacts) al cui sviluppo partecipa anche Google.

Tecnologie per il Trust delle Applicazioni

La gestione dei privilegi associati agli utenti e ai sistemi è complessa, in parte anche a causa delle utenze applicative e di sistema. La concessione e la revoca tempestiva dei privilegi rappresentano un aspetto critico. I sistemi PAM (Privileged Access Management) o PAS (Privileged Access Security) sono fondamentali per gestire in modo efficace questi ambiti, insieme ai sistemi di Identity Management, che consentono di correlare le utenze alle persone fisiche, facilitando l’identificazione e la gestione dei diritti.

Questi strumenti non solo permettono una gestione efficace degli accessi, ma offrono anche funzionalità di monitoraggio per l’uso degli account privilegiati, agevolando l’analisi post-incidente. Un altro elemento chiave dei sistemi PAM è la gestione delle credenziali amministrative locali alle postazioni di lavoro, che possono essere rimosse, abilitate su richiesta o sottoposte a rotazione automatica frequente, per prevenire movimenti laterali all’interno della rete.

I sistemi PAM possono inoltre gestire gli accessi amministrativi mediati, nei quali l’utente non conosce la

password amministrativa, ma si connette tramite il sistema PAM, che genera una password one-shot in base al profilo di accesso dell'utente.

L'evoluzione del panorama applicativo moderno, caratterizzato da architetture cloud-native ed ibride implementate spesso tramite microservizi, richiede un approccio più sofisticato alla gestione della sicurezza applicativa e dei privilegi. Le tecnologie moderne per il Trust delle Applicazioni si sono evolute per affrontare queste nuove sfide.

Identity and Access Management (IAM) di Nuova Generazione

I sistemi IAM moderni hanno evoluto le loro capacità per supportare architetture applicative complesse in quanto l'orchestrazione delle identità in ambienti multi-cloud o ibridi richiede sistemi IAM capaci di gestire identità federate e policy di accesso granulari. Questi sistemi implementano funzionalità avanzate come la gestione del ciclo di vita delle identità delle applicazioni, l'automazione del provisioning e de-provisioning, e l'integrazione con sistemi di gestione delle identità cloud-native.

La gestione delle identità nelle applicazioni dovrebbe includere ogi alcune caratteristiche quali:

- Rotazione automatica delle credenziali
- Integrazione con vault crittografici
- Automazione del lifecycle delle identità applicative
- Federazione delle identità tra ambienti diversi

Runtime Application Self-Protection (RASP)

Le tecnologie RASP moderne forniscono protezione in tempo reale alle applicazioni:

- Analisi comportamentale del runtime applicativo
- Protezione contro attacchi applicativi in tempo reale
- Integrazione con sistemi di orchestrazione container
- Protezione delle API
- Identificazione e blocco di attacchi zero-day

Application Security Posture Management (ASPM)

Le piattaforme ASPM offrono una visione completa della sicurezza applicativa:

- Scansione continua delle vulnerabilità
- Analisi della configurazione di sicurezza
- Valutazione del rischio applicativo specialmente in contesti no-code
- Gestione delle policy di sicurezza
- Integrazione con pipeline CI/CD

Cloud Workload Protection Platforms (CWPP)

Per la protezione dei workload cloud, le CWPP moderne offrono:

- Protezione dei container e delle funzioni serverless
- Sicurezza dei microservizi
- Controllo delle comunicazioni est-ovest
- Hardening automatico dei workload
- Compliance monitoring continuo

API Security

La sicurezza delle API è diventata cruciale, con tecnologie che offrono:

- Discovery automatico delle API

- Protezione contro attacchi specifici alle API
- Gestione del ciclo di vita delle API
- Monitoring del comportamento delle API
- Controllo degli accessi granulare

Privileged Access Management (PAM)

Evoluto I sistemi PAM moderni hanno esteso le loro capacità per includere:

- Just-in-Time Access
- Sessioni privilegiate effimere
- Automazione della gestione dei privilegi
- Analytics avanzati sugli accessi privilegiati
- Integrazione con sistemi di orchestrazione

Container Security

Per la sicurezza dei container, sono disponibili tecnologie specifiche:

- Scansione delle immagini container
- Runtime container security
- Network policy enforcement
- Vulnerability management
- Compliance monitoring

Database Activity Monitoring (DAM)

I sistemi DAM moderni offrono:

- Monitoraggio delle query database
- Analisi comportamentale degli accessi
- Protezione contro attacchi SQL
- Audit degli accessi privilegiati
- Mascheramento dinamico dei dati

DevSecOps Tools

Gli strumenti DevSecOps moderni includono:

- Security testing automatizzato
- Code scanning continuo
- Dependency tracking
- Infrastructure as Code security
- Pipeline security automation

L’integrazione efficace anche solo di parte di queste tecnologie potrebbe richiedere una piattaforma di gestione centralizzata o una logic di security fabric.

L’orchestrazione di queste tecnologie deve essere guidata da una strategia che bilanci sicurezza e agilità operativa, permettendo alle organizzazioni di innovare mantenendo un controllo efficace sui rischi. La chiave del successo sta nella capacità di automatizzare la maggior parte delle operazioni di sicurezza, riducendo il carico operativo sui team di sviluppo e operations mentre si mantiene un elevato livello di sicurezza.

Rischi mitigati dal Trust delle Applicazioni

Una corretta gestione dei privilegi di accesso riduce il rischio di errori operativi accidentali, limitandone l’impatto sia in termini di ambito che di contesto. La definizione degli accessi in base alle reali necessità operative mitiga il rischio di movimenti laterali in caso di compromissione delle credenziali, rendendo più difficile per un attaccante espandere la propria presenza nella rete. Inoltre, la gestione delle password amministrative delle postazioni contribuisce alla mitigazione dei rischi connessi ai movimenti laterali.

La gestione moderna del Trust delle Applicazioni e dei Privilegi affronta una gamma sempre più complessa di rischi,

particolarmente rilevanti nell’era delle applicazioni cloud-native e delle architetture distribuite.

Compromissione delle Applicazioni Web

Le applicazioni web moderne sono esposte a minacce sofisticate che vanno oltre le tradizionali vulnerabilità OWASP Top 10. Un approccio Zero Trust alla sicurezza applicativa mitiga questi rischi attraverso controlli continui e contestuali. Le tecniche moderne di injection, che possono bypassare i controlli tradizionali, vengono identificate e bloccate attraverso l’analisi comportamentale del runtime applicativo. Il monitoraggio continuo delle interazioni con l’applicazione permette di identificare pattern di attacco sofisticati che potrebbero indicare tentativi di compromissione.

Supply Chain Applicativa

La sicurezza della supply chain software è diventata cruciale, come dimostrato da recenti incidenti di alto profilo. Il Trust delle Applicazioni moderno mitiga questi rischi attraverso il controllo continuo delle dipendenze software, la verifica dell’integrità dei componenti e il monitoraggio delle modifiche nel codice applicativo. L’implementazione di controlli sulla provenienza del software (Software Bill of Materials) e la verifica crittografica dei componenti riducono significativamente il rischio di compromissione attraverso dipendenze malevole.

Privilege Escalation

Gli attacchi di privilege escalation, sia verticali che orizzontali, rappresentano una minaccia significativa per le applicazioni moderne. L’implementazione di controlli granulari sui privilegi, combinata con l’analisi comportamentale degli accessi, permette di identificare e bloccare tentativi di escalation non autorizzati. L’approccio Just-in-Time all’assegnazione dei privilegi riduce drasticamente la

finestra temporale disponibile per gli attacchi.

API Abuse e Data Exposure

La proliferazione delle API ha introdotto nuovi vettori di attacco. Il Trust delle Applicazioni moderno protegge le API attraverso:

- Controllo granulare degli accessi basato sul contesto
- Identificazione di pattern di abuso delle API
- Protezione contro attacchi di rate limiting e DDoS applicativo
- Prevenzione dell’esposizione non intenzionale di dati sensibili

Microservizi e Container Security

L’architettura a microservizi introduce sfide specifiche che vengono mitigate attraverso:

- Isolamento dei workload
- Controllo delle comunicazioni tra servizi
- Gestione sicura delle credenziali dei servizi
- Protezione del runtime dei container

Session Hijacking e Account Takeover

Gli attacchi alle sessioni applicative vengono mitigati attraverso:

- Gestione sicura delle sessioni
- Tokenizzazione avanzata
- Rilevamento di anomalie nelle sessioni
- Protezione contro il replay degli accessi

Database Security

La protezione dei dati a livello applicativo include:

- Prevenzione del SQL injection avanzato
- Controllo degli accessi granulare ai dati
- Monitoraggio delle query anomale
- Mascheramento dinamico dei dati sensibili

Business Logic Flaws

Le vulnerabilità nella logica di business vengono mitigate attraverso:

- Analisi comportamentale delle transazioni
- Identificazione di sequenze di operazioni anomale
- Protezione contro la manipolazione del workflow
- Validazione contestuale delle operazioni

Cloud Misconfiguration

I rischi legati alla configurazione errata dei servizi cloud vengono mitigati attraverso:

- Scansione continua delle configurazioni
- Enforcement automatico delle policy di sicurezza
- Remediation guidata delle misconfiguration
- Monitoraggio dei cambiamenti di configurazione

Serverless Security

Le funzioni serverless introducono nuovi rischi che vengono mitigati attraverso:

- Controllo delle dipendenze delle funzioni
- Protezione del runtime serverless
- Gestione sicura delle variabili d’ambiente
- Monitoraggio delle esecuzioni anomale

Credential Exposure

L’esposizione delle credenziali viene prevenuta attraverso:

- Gestione centralizzata dei codici
- Rotazione automatica delle credenziali
- Controllo dell’accesso ai vault
- Monitoraggio dell’uso delle credenziali

L’efficacia di queste mitigazioni dipende dalla capacità dell’organizzazione di mantenere un approccio olistico alla sicurezza applicativa, che integri:

- Monitoraggio continuo
- Risposta automatizzata agli incidenti
- Adattamento dinamico delle policy di sicurezza
- Formazione continua dei team di sviluppo
- Integrazione della sec-ops all’interno della classica pipeline CI/CD

La chiave per una mitigazione efficace sta nella capacità di bilanciare la sicurezza con la velocità di sviluppo e deployment richiesta dai moderni cicli di sviluppo software. L’automazione gioca un ruolo cruciale, permettendo di implementare controlli di sicurezza senza introdurre ritardi significativi nel processo di sviluppo.

In questo approfondimento abbiamo esaminato il ruolo cruciale del Trust delle Applicazioni nell’implementazione del modello Zero Trust, analizzando come una gestione efficace dei privilegi e l’adozione di tecnologie moderne possano proteggere le applicazioni, le API e i dati dell’organizzazione. L’approccio Zero Trust richiede un controllo granulare degli accessi e una verifica continua basata sul contesto, combinando sicurezza e agilità operativa. Vi invitiamo a seguire il prossimo approfondimento della nostra serie dedicata al modello Zero Trust, dove esploreremo le tecniche di misurazione, monitoraggio e ottimizzazione del modello.

Per approfondire ulteriormente questi concetti, scaricate il white paper “Zero Trust – solo un problema tecnologico?” del

Dott. Ing. Fioravanti, che offre una visione completa e dettagliata dell’architettura Zero Trust e delle sue applicazioni nel contesto aziendale moderno.

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/trust-applicazioni/