BLU-MAN-006-R01
Allegato 01-R00
Aggiornamento del 08/09/2026

Hardening

INDICE

1 INTRODUZIONE AL DOCUMENTO 3
1.1 Contesto 3
1.2 Scopo 3
2 Hardening 4
2.1 Minimizzazione della superficie di attacco 4
2.2 Access Control & Privilege Management 4
2.3 Configurazioni sicure 5
2.4 Aggiornamento e patching 5
2.5 Crittografia dei dati 5
2.6 Sicurezza della Rete 6
2.7 Monitoraggio e auditing 6
2.8 Backup e Recovery 6
2.9 Formazione e consapevolezza 7
3 ACCESS CONTROL & PRIVILEGE MANAGEMENT 8
3.1 Utenti, Gruppi e Permessi 8
3.2 ACL 8
3.3 Accessi non essenziali 8
3.4 Time-out di autenticazione 8
3.5 SICUREZZA DELLA RETE 8
3.5.1 Firewall 8
3.5.2 HTTPS 9
3.6 CONFIGURAZIONI SICURE 9
3.6.1 Ambiente di esecuzione 9
3.6.2 Sicurezza di OS e DB 9
3.7 SECURITY CHECKLIST 9
3.8 DENIAL OF SERVICE 9
3.8.1 LDAP 9
4 Databricks 10
4.1 ACCESS CONTROL & PRIVILEGE MANAGEMENT 10
4.1.1 Workspace 10
4.1.2 Administrator 10
4.1.3 Permessi e controllo degli accessi 10
4.2 CRITTOGRAFIA 10
4.3 GESTIONE DEI SECRET 11
4.4 SICUREZZA DELLA RETE 11

Italgas S.p.A - Informazioni Interne

5 Apache Spark & PySpark 11
5.1 SPARK REMOTE PROCEDURE CALL 11
5.2 CRITTOGRAFIA LOCAL STORAGE 11
5.2.1 Cifratura dei Dati con PySpark 11
5.3 WEB UI 12
5.3.1 Access Control & Privilege Management 12
5.3.2 SSL 13
5.3.3 HTTP Security Headers 13
5.4 SICUREZZA DELLA RETE 13
5.5 KERBEROS 13
5.6 LOGGING 13
6 Azure Data Factory (ADF) 13
6.1 NETWORK SECURITY 14
6.2 IDENTITY MANAGEMENT 14
6.3 PRIVILEGED ACCESS 14
6.4 DATA PROTECTION 14
6.5 ASSET MANAGEMENT 14
6.6 LOGGING AND THREAT DETECTION 14
6.7 BACKUP AND RECOVERY 15
7 PowerBI 16
7.1 ACCESS CONTROL & PRIVILEGE MANAGEMENT 16
7.1.1 Autenticazione 16
7.1.2 Storage e accessi ai dati 16
7.1.3 App Workspaces 17
7.2 SICUREZZA DELLA RETE 17
7.2.1 Service Tags 17
7.2.2 Private Link 17
7.2.3 Rete VNet 17
7.2.4 Transport Layer Security (TLS) 18
7.3 MONITORAGGIO E AUDITING 18
7.3.1 Monitoraggio dei Data Gateway 18
7.3.2 Audit Logs 18
8 ESRI ArcGIS 19
8.1 SICUREZZA APPLICATIVA 19
8.2 IDENTITY AND ACCESS MANAGEMENT (IAM) 19
8.3 INFRASTRUTTURA DI SUPPORTO 19
8.4 DATA PROTECTION 19
8.5 INVENTORY AND MANTAINANCE 20
8.6 DETECTION AND RESPONSE 20
8.7 PRIVACY 20
9 TIBCO BW, TIBCO BWCE & TIBCO Mashery 21
9.1 ACCESS CONTROL & PRIVILEGE MANAGEMENT 21
9.1.1 Ruoli e Permessi (TIBCO BW) 21
9.1.2 OAuth2 (Mashery) 21
9.2 SICUREZZA DELLA RETE 22
9.2.1 Sicurezza per HTTP (BW e BWCE) 22
9.2.2 Sicurezza per SOAP (BW e BWCE) 22
9.2.3 HTTPS e Mutua Autenticazione (Mashery) 22
9.3 MONITORAGGIO E AUDITING 23
10 Link utili 23

Italgas S.p.A - Informazioni Interne

1 INTRODUZIONE AL DOCUMENTO

1.1 Contesto

Questo documento è uno degli allegati al Manuale Operativo Sviluppo Sicuro e si colloca all'interno di un articolato sistema di linee guida volte a garantire la sicurezza nello sviluppo dei prodotti commissionati da Italgas. L'obiettivo è assicurare che tali prodotti siano solidi e resistenti alle minacce informatiche. Nello specifico, vengono trattate le linee guida di hardening che è necessario seguire per vari prodotti software di terze parti identificati da Italgas come asset da proteggere e tenere in sicurezza.

1.2 Scopo

Questo documento ha lo scopo di illustrare i principi e le tecniche del processo di Hardening da attuare su specifici sistemi ed applicativi, con l'obiettivo di incrementarne e rafforzarne la sicurezza.
Per ogni aspetto di sicurezza dei vari prodotti viene fornita una descrizione, eventualmente degli esempi e le corrispettive contromisure e gli accorgimenti da adottare al fine di migliorare il livello di sicurezza di ciascuna delle tecnologie riportate. Per ogni tematica trattata, l'obiettivo è quello di fornire agli sviluppatori e agli architetti una lista delle possibilità offerte da ciascun prodotto per migliorare la sicurezza dei sistemi.
Si rimanda comunque alle documentazioni ufficiali dei vendor per approfondimenti e linee guida sempre aggiornate, che sono riportate in coda ad ogni capitolo nella sezione *"Link utili"*.

Italgas S.p.A - Informazioni Interne

2 Hardening

Il processo di hardening in ambito sicurezza informatica si riferisce a una serie di strategie e tecniche utilizzate per rafforzare la sicurezza dei sistemi informatici.
L'obiettivo principale dell'hardening è ridurre la superficie di attacco di un sistema, ovvero il numero di punti vulnerabili che potrebbero essere sfruttati da un attaccante.

L'hardening è misura preventiva che mira a proteggere i sistemi prima che possano essere compromessi, aumentando la difficoltà per gli attaccanti di penetrare le difese e accedere a dati sensibili. In un contesto in cui le minacce informatiche sono in continua evoluzione, l'hardening rappresenta un passo fondamentale per garantire la resilienza e la sicurezza delle infrastrutture IT.

2.1 Minimizzazione della superficie di attacco

Il principio di hardening di **minimizzazione della superficie d'attacco** è una strategia fondamentale nella sicurezza informatica. Questo approccio si concentra sulla riduzione del numero di punti vulnerabili che un attaccante potrebbe sfruttare, limitando così le possibilità di accesso non autorizzato. In pratica, questo significa ridurre il numero di servizi e porte aperte su un sistema al minimo indispensabile. Ogni servizio in esecuzione su un sistema rappresenta un potenziale ingresso per un attaccante; quindi, meno servizi sono attivi, minore è il rischio. Questo non solo implica la disattivazione di servizi non necessari, ma anche la configurazione di quelli essenziali affinché operino in modo sicuro, ad esempio, eseguendo gli aggiornamenti più recenti e applicando le patch di sicurezza.

Un altro aspetto importante è la configurazione dei servizi in modo che siano accessibili solo dalle reti che ne hanno effettivamente bisogno. Ad esempio, un database interno dovrebbe essere raggiungibile soltanto da reti interne fidate e non dall'intero internet. Questo limita significativamente l'esposizione a potenziali attacchi provenienti dall'esterno. Inoltre, l'implementazione di **firewall** e **liste di controllo di accesso (ACL)** può fornire un ulteriore livello di difesa, assicurando che solo il traffico autorizzato possa raggiungere i servizi critici.

La minimizzazione della superficie d'attacco non si ferma alla gestione dei servizi e delle porte. Include anche la riduzione dei privilegi degli utenti al minimo necessario per compiere le loro funzioni (il **principio del minimo privilegio**), l'uso di **sandboxing** per isolare le applicazioni, e la **segmentazione della rete** per limitare il movimento laterale di un attaccante all'interno di una rete.

2.2 Access Control & Privilege Management

Il principio di hardening di **Access Control & Privilege Management** è fondamentale per garantire la sicurezza informatica all'interno di un'organizzazione. Questo processo implica il rafforzamento dei sistemi limitando l'accesso alle risorse solo agli utenti autorizzati e gestendo attentamente i privilegi.

Implementare un robusto **controllo degli accessi** significa assicurare che ogni tentativo di accesso sia verificato e che solo le sessioni legittime siano mantenute, prevenendo così possibili sfruttamenti. La **gestione delle sessioni** è altrettanto critica; monitorare e registrare le attività degli utenti durante le sessioni può aiutare a identificare e mitigare rapidamente eventuali comportamenti sospetti.

Adottare il **principio del privilegio minimo** è essenziale per ridurre la superficie di attacco. Questo principio sostiene che agli utenti dovrebbe essere concesso solo il livello di accesso strettamente necessario per svolgere le loro funzioni. Ciò limita il potenziale danno che un utente malintenzionato potrebbe causare se dovesse ottenere l'accesso a un account. Inoltre, una **gestione efficace delle password**, che include la rotazione regolare delle stesse e l'uso dell'autenticazione multi-fattore, può prevenire l'accesso non autorizzato.

Un altro aspetto cruciale è la gestione delle credenziali privilegiate; queste dovrebbero essere condivise il meno possibile e protette con **sistemi di gestione delle identità e degli accessi (IAM)**. Inoltre, è

importante avere una visione centralizzata dell'accesso privilegiato in tutta l'organizzazione, che può essere ottenuta attraverso soluzioni di **Privileged Access Management (PAM)**.

Queste soluzioni forniscono strumenti per il monitoraggio continuo delle attività privilegiate, generando log dettagliati e allarmi per qualsiasi comportamento sospetto o violazione delle politiche, permettendo così una risposta rapida alle minacce.

2.3 Configurazioni sicure

Il principio di hardening delle **Configurazioni Sicure** si basa sull'idea di rafforzare la sicurezza dei sistemi informatici attraverso la regolazione delle impostazioni predefinite per renderle più sicure.

Questo processo include la disabilitazione di funzionalità non necessarie che potrebbero presentare rischi di sicurezza. L'hardening è una strategia preventiva che mira a ridurre le opportunità per gli attaccanti di penetrare nei sistemi, identificando e correggendo configurazioni errate o vulnerabili.

È un processo complesso che richiede un'analisi attenta e un aggiornamento costante per assicurare che i sistemi informatici siano protetti dalle minacce emergenti. Attraverso l'hardening, le organizzazioni possono ridurre significativamente i rischi per la sicurezza e migliorare la fiducia nell'utilizzo dei servizi online.

2.4 Aggiornamento e patching

Il principio di hardening attraverso l'aggiornamento e il patching è una componente critica della sicurezza informatica. Questo processo implica la costante revisione e aggiornamento del software e del firmware per mitigare le vulnerabilità note.

Mantenere i sistemi aggiornati con le ultime patch di sicurezza è fondamentale per proteggere le reti e i dispositivi da attacchi informatici che sfruttano falle di sicurezza precedentemente identificate. Le patch di sicurezza sono rilasciate dai fornitori di software per correggere specifici problemi di sicurezza che sono stati scoperti nei loro prodotti. Queste patch possono includere aggiornamenti per chiudere vulnerabilità che potrebbero essere sfruttate da malware o hacker per ottenere accesso non autorizzato o causare danni.

Un aspetto è la **gestione delle patch**, che richiede un processo organizzato per garantire che tutte le patch di sicurezza siano applicate tempestivamente e correttamente. Questo può includere il test delle patch in ambienti di prova prima del loro rilascio nella produzione per assicurarsi che non causino problemi di compatibilità o altri errori. La gestione delle patch è particolarmente critica per i sistemi che eseguono applicazioni proprietarie o personalizzate, dove le patch devono essere attentamente valutate per evitare di interrompere le operazioni critiche.

2.5 Crittografia dei dati

Il principio di hardening nella **crittografia dei dati** si riferisce al rafforzamento delle misure di sicurezza per proteggere i dati sensibili.

La crittografia gioca un ruolo fondamentale in questo contesto, convertendo i dati da un formato leggibile a un formato cifrato, inaccessibile senza la chiave di decrittazione corretta. Questa trasformazione è essenziale sia per i dati in transito, come quelli scambiati su internet o in una rete aziendale, sia per i dati in riposo, come quelli archiviati su un disco fisso o in un database.

La crittografia in transito si occupa di proteggere i dati mentre vengono trasferiti da un punto all'altro, assicurando che, anche se intercettati, rimangano incomprensibili senza la chiave appropriata. Questo è particolarmente importante per le comunicazioni su internet, dove i dati possono attraversare diversi nodi e reti prima di raggiungere la loro destinazione. La crittografia in riposo, d'altra parte, si concentra sulla protezione dei dati quando non sono in movimento, come quando sono salvati su un dispositivo di storage.

Questo previene l'accesso non autorizzato in caso di furto fisico del dispositivo o di attacchi informatici che mirano a bypassare le difese di rete.

L'hardening attraverso la crittografia richiede l'implementazione di algoritmi robusti e la gestione sicura delle chiavi crittografiche. Gli algoritmi devono essere aggiornati e resistenti contro gli attacchi moderni, mentre le chiavi devono essere conservate in modo sicuro, accessibili solo agli utenti autorizzati e regolarmente aggiornate per prevenire compromissioni.

2.6 Sicurezza della Rete

Il principio di hardening nella **sicurezza della rete** si riferisce al processo di rafforzamento dei sistemi informatici e delle reti per ridurre la superficie di attacco e aumentare la resistenza contro le minacce informatiche.

Questo processo include una serie di tecniche e strategie che mirano a identificare e mitigare le vulnerabilità potenziali, configurando i sistemi in modo da minimizzare le possibilità di accesso non autorizzato e di attacchi. L'hardening è fondamentale per proteggere dati sensibili e infrastrutture critiche, e si basa sull'adozione di protocolli di comunicazione sicuri come **HTTPS**, che utilizza SSL/TLS per crittografare i dati trasmessi tra il client e il server, garantendo così confidenzialità, integrità e autenticazione delle informazioni scambiate.

HTTPS, acronimo di HyperText Transfer Protocol Secure, è un protocollo che stabilisce una connessione criptata su Internet, assicurando che i dati inviati siano accessibili solo alle parti legittime. Questo protocollo è essenziale per transazioni online sicure, come quelle bancarie o di e-commerce, poiché previene l'intercettazione dei dati da parte di terzi. La crittografia SSL/TLS, che sta alla base di HTTPS, funge da strato di sicurezza aggiuntivo, utilizzando algoritmi matematici complessi per codificare i dati, rendendo estremamente difficile per gli hacker decifrarli senza la chiave corretta.

La crittografia **SSL (Secure Sockets Layer)** e il suo successore **TLS (Transport Layer Security)** sono protocolli crittografici che forniscono sicurezza nelle comunicazioni su reti di computer, come Internet. Questi protocolli sono progettati per prevenire l'ascolto non autorizzato (eavesdropping) e la manomissione (tampering) dei dati, attraverso l'uso di certificati digitali che autenticano l'identità delle parti comunicanti e l'impiego di chiavi di crittografia per proteggere i dati scambiati.

2.7 Monitoraggio e auditing

Il principio di hardening nel contesto del **monitoraggio e auditing** si focalizza sull'incremento della sicurezza attraverso la riduzione delle superfici di attacco e la minimizzazione delle vulnerabilità.

Questo processo implica l'implementazione di sistemi di monitoraggio robusti che possano rilevare attività sospette in tempo reale, consentendo agli amministratori di reagire prontamente a potenziali minacce. Parallelamente, gli audit regolari giocano un ruolo cruciale nell'identificazione di punti deboli che potrebbero essere sfruttati da attori malintenzionati.

Attraverso l'analisi sistematica e periodica dei sistemi, è possibile scoprire configurazioni errate, aggiornamenti mancanti o altre lacune che compromettono la sicurezza.

2.8 Backup e Recovery

Il principio di hardening nel contesto di **backup e recovery** si riferisce al rafforzamento dei sistemi informatici per ridurre la loro vulnerabilità agli attacchi esterni.
Questo processo implica l'adozione di una serie di misure di sicurezza che vanno dalla gestione delle configurazioni di sistema, alla regolazione delle impostazioni predefinite, fino all'implementazione di politiche di sicurezza rigorose.

L'obiettivo è quello di minimizzare la superficie di attacco, ovvero l'insieme di tutti i punti potenzialmente sfruttabili da un attaccante, come password deboli, software non aggiornato o dati non crittografati. In particolare, per quanto riguarda il backup e il recupero dei dati, l'hardening può includere l'uso di crittografia per proteggere i backup, la verifica dell'integrità dei dati per assicurarsi che i backup non siano stati manomessi e la limitazione dell'accesso ai backup solo a personale autorizzato.

Implementare un'efficace strategia di hardening è fondamentale per garantire che, in caso di attacco, i dati possano essere recuperati in modo sicuro e affidabile.

2.9 Formazione e consapevolezza

Questo principio di hardening si basa sull'idea che la sicurezza informatica non sia solo una questione di tecnologie e strumenti avanzati, ma anche e soprattutto di persone informate e consapevoli.

La **formazione e la consapevolezza** sono essenziali per creare una cultura della sicurezza all'interno di un'organizzazione, dove ogni membro del personale comprende l'importanza della sicurezza e il proprio ruolo nella protezione delle risorse digitali.

Educare il personale sull'importanza della sicurezza significa trasmettere la conoscenza delle minacce informatiche, delle tecniche di attacco più comuni e delle migliori pratiche per prevenire violazioni e incidenti. Le pratiche di hardening, come la configurazione sicura dei sistemi, la gestione delle patch e l'implementazione di politiche di accesso restrittivo, sono fondamentali per ridurre la superficie di attacco e rafforzare le difese contro gli attacchi informatici.

La formazione deve quindi essere vista come un investimento strategico, che non solo aumenta la sicurezza ma dimostra anche responsabilità nei confronti dei propri utenti e partner commerciali, influenzando positivamente la fiducia nell'utilizzo dei servizi online e nella condivisione di informazioni cruciali. Inoltre, un personale ben informato è meno incline a cadere vittima di tecniche di ingegneria sociale e contribuisce attivamente alla sicurezza complessiva dell'ecosistema digitale.

3 ACCESS CONTROL & PRIVILEGE MANAGEMENT

Il controllo degli accessi e la gestione dei privilegi assicurano la confidenzialità dei dati, e che le operazioni su questi siano definite da una rigorosa policy. Se quest'ultima è troppo lasca, o se il sistema presenta debolezze che ne minano la robustezza, c'è il serio rischio di incorrere in vulnerabilità quali information disclosure a individui non autorizzati o privilege escalation.

3.1 Utenti, Gruppi e Permessi

Le tre entità gestite dal sistema sono:

- **Utenti**, che individuano una singola utenza nel sistema
- **Gruppi**, che raccolto più utenti diversi sotto un'unica etichetta
- **Permessi**, che definiscono per utenti e gruppi le azioni lecite eseguibili

Nota: sono presenti alcune utenze, gruppi e permessi di default. È doveroso cambiare le password preimpostate e sistemare i permessi in base alle necessità, per non esporre il sistema ad attacchi che coinvolgano credenziali note e configurazioni di default.

3.2 ACL

Le Access Control List (ACL) sono strutture dati tabellari che definiscono quali utenze possono accedere alle risorse di un sistema e quali operazioni su queste possono eseguire.

Di default, nella piattaforma tutte le utenze hanno almeno accesso Read-Only alla totalità degli asset. Una prima misura di hardening richiede di restringere l'accesso solo alle utenze autenticate sul sistema.

3.3 Accessi non essenziali

In ottica di limitare la superficie d'attacco e rendere più solida l'intera infrastruttura, si dovrebbero limitare tutti quegli accessi remoti ai servizi non essenziali. Dovrebbero restare disponibili verso l'esterno solamente quelli indispensabili al corretto funzionamento del prodotto.
Oltretutto, per quei servizi esposti, è possibile siano

3.4 Time-out di autenticazione

Il sistema dispone di una funzionalità di time-out globale legato all'autenticazione, per la quale ad un utente loggato è richiesto di effettuare nuovamente l'accesso.

3.5 SICUREZZA DELLA RETE

La sicurezza dell'infrastruttura di rete dipende soprattutto dall'organizzazione logica e fisica, dal percorso intrapreso dal flusso di dati prima di arrivare a destinazione e dalla solidità delle configurazioni scelte per il sistema, sia a livello globale che locale.

3.5.1 Firewall

Il firewall è una componente imprescindibile all'interno di un sistema di rete, che si occupa di proteggere i dispositivi e la rete stessa da attacchi informatici. Regola il traffico in entrata come quello in uscita, prevenendo accessi non autorizzati e sventando potenziali infezioni malware. Il suo funzionamento si basa su un set di regole ben definite.

Il tool differenzia il firewall in due sottocategorie, in funzione del loro utilizzo:

- **Internal Firewall**, per consentire a determinati componenti del sistema (ad esempio, istanze applicative, database) di comunicare con altri elementi interni della piattaforma.
- **External Firewall**, per consentire l'accesso a Internet a determinati URL necessari al funzionamento del sistema.

È importante che il firewall supporti proxy servers e/o un'ispezione stateful. Quest'ultima in particolare permette di tracciare lo storico di una connessione, tenendo memoria del suo stato passato e presente, e risulta essere molto più efficace, ma ovviamente anche più onerosa, che una semplice single packet inspection.

3.5.2 HTTPS

HyperText Transfer Protocol Secure (HTTPS) è lo standard attuale per lo scambio di messaggi richiesta – risposta sicuri in un contesto web. Utilizza la porta 443 ed il suo funzionamento consiste nella comunicazione tramite il protocollo HTTP incapsulato in una connessione criptata. È da preferire rispetto alla sua controparte insicura per proteggere l'integrità e la confidenzialità del messaggio trasportato.

3.6 CONFIGURAZIONI SICURE

3.6.1 Ambiente di esecuzione

L'esecuzione del sistema deve avvenire in modalità "Production Ready", pensata appositamente per un ambiente di produzione. Questa modalità di esecuzione non solo configurerà automaticamente l'istanza per aderire alle best practice di sicurezza, ma rimuoverà anche tutte le applicazioni e le configurazioni di esempio non necessarie.

3.6.2 Sicurezza di OS e DB

Così come è consigliato mantenere aggiornate tutte le componenti della propria infrastruttura con le ultime versioni rilasciate, si consiglia di fare riferimento ai vendor del proprio sistema operativo e del proprio database per le linee guida di hardening e linee guida per una corretta configurazione.

3.7 SECURITY CHECKLIST

Il sistema dispone di una security checklist da applicare in modalità top-down, dall'alto al basso, nella quale vengono trattati i passi per assicurarsi che l'istanza sia sicura. Si rimanda al link in coda al capitolo.

3.8 DENIAL OF SERVICE

Un attacco Denial of Service (DoS) è un tipo di attacco informatico mirato a rendere un servizio, una rete o un sistema inaccessibile agli utenti legittimi. Questo viene realizzato sovraccaricando il sistema con un'enorme quantità di traffico o richieste, fino a quando non riesce più a gestirle e diventa non operativo.

3.8.1 LDAP

Il **Lightweight Directory Access Protocol (LDAP)** è un protocollo standardizzato per l'interrogazione e la modifica di qualsiasi raggruppamento di informazioni che può essere espresso come record di dati e organizzato in modo gerarchico. È inoltre utilizzato da alcune piattaforme come fonte per l'interrogazione sui gruppi e sugli utenti, e come mezzo per eseguire l'autenticazione tramite password.

Un attaccante potrebbe deliberatamente fallire l'autenticazione con un account più volte, fino a quando il server LDAP non lo blocca, causando così un disservizio all'utente legittimo.

Una contromisura efficace consiste nell'implementazione di un meccanismo di **lock-out time**, che blocca i tentativi per un determinato periodo di tempo prima che il blocco arrivi direttamente dal server LDAP.

4 Databricks

Databricks è una piattaforma analitica unificata e aperta che consente di costruire, distribuire, condividere e mantenere soluzioni di dati, analisi e intelligenza artificiale su larga scala. Questa piattaforma integra lo storage cloud e la sicurezza nel proprio account cloud, gestendo e distribuendo l'infrastruttura cloud per conto dell'utente. Databricks è utilizzato per connettere fonti di dati a una piattaforma unica per elaborare, memorizzare, condividere, analizzare, modellare e monetizzare i set di dati con soluzioni che vanno dall'intelligenza aziendale all'intelligenza artificiale generativa.

4.1 ACCESS CONTROL & PRIVILEGE MANAGEMENT

Il controllo degli accessi e la gestione dei privilegi assicurano la confidenzialità dei dati, e che le operazioni su questi siano definite da una rigorosa policy. Se quest'ultima è troppo lasca, o se il sistema presenta debolezze che ne minano la robustezza, c'è il serio rischio di incorrere in vulnerabilità quali information disclosure a individui non autorizzati o privilege escalation.

4.1.1 Workspace

Un workspace, traducibile come spazio di lavoro, è una distribuzione di Databricks in un account di servizio cloud. Fornisce un ambiente unificato per lavorare con le risorse Databricks per un insieme specifico di utenti.

4.1.2 Administrator

Databricks mette a disposizione due differenti tipologie di amministratori all'interno del proprio sistema:

- Gli **amministratori di account**, che hanno privilegi sull'intero account Databricks. In qualità di amministratore dell'account, è possibile creare spazi di lavoro, configurare le risorse del cloud, visualizzare i dati di utilizzo e gestire le identità, le impostazioni e le sottoscrizioni dell'account.
  Gli amministratori degli account possono anche delegare i ruoli di amministratore dell'account e di amministratore dello spazio di lavoro a qualsiasi altro utente.
- Gli **amministratori di workspace**, che invece hanno privilegi di amministrazione all'interno di un singolo workspace. Possono gestire le identità a livello di workspace, regolare l'uso del calcolo e attivare e delegare il controllo degli accessi basato sui ruoli.

4.1.3 Permessi e controllo degli accessi

Gli amministratori di workspace sono responsabili dell'assegnazione dei permessi agli utenti all'interno di un workspace, di modo che abbiano accesso solo alle funzionalità e ai dati a loro strettamente necessari.
Gli amministratori possono anche abilitare alcune funzionalità come il **single-sign on** (SSO) per un'autenticazione forte e l'**autenticazione multi-fattore**.

4.2 CRITTOGRAFIA

La crittografia è una tecnica adottata nella sicurezza informatica utilizzata per garantire la confidenzialità dei messaggi. Ne consegue che i dati crittografati siano leggibili ed interpretabili solo dalle parti autorizzate.
Databricks stesso fornisce diversi servizi per la crittografia, che differiscono in base al contesto di applicazione, e sono:

- **Chiavi gestite dall'utente**, che possono proteggere sia i servizi (es. Notebook ed access tokens) sia lo storage dei workspace (es. Amazon S3 bucket);
- Criptazione delle **query**, **storico delle query** e **risultati di queste**
- Criptazione del traffico tra i **nodi worker** del cluster

4.3 GESTIONE DEI SECRET

I secrets vengono utilizzati ovunque. Chiavi API (Application Programming Interface), credenziali di database, autorizzazioni IAM (Identity and Access Management), chiavi SSH (Secure Shell), certificati e così via. Molte organizzazioni le hanno codificate all'interno del codice sorgente in chiaro, disseminate nei file di configurazione e negli strumenti di gestione della configurazione.

Tuttavia, una corretta gestione di questi è necessaria per evitare esfiltrazioni di dati sensibili e esposizione ad attori malevoli delle risorse protette.

Infatti, si possono usare i Databricks secrets per memorizzare le credenziali e farvi riferimento nei notebook e nei lavori. Per gestire i segreti, è possibile utilizzare la CLI di Databricks per accedere all'API Secrets.

4.4 SICUREZZA DELLA RETE

La sicurezza infrastrutturale della rete permette di proteggersi dalle minacce in arrivo da questa, che sfruttano nella maggior parte dei casi un'organizzazione semplicistica e pertanto debole delle configurazioni di sicurezza. Per proteggere la rete all'interno della quale Databricks lavora, è necessario ad esempio implementare liste di accesso di IP fidati e policy VPC restrittive.

5 Apache Spark & PySpark

Apache Spark, un potente framework open-source per l'elaborazione di grandi quantità di dati. PySpark è l'API Python per questo strumento. PySpark è particolarmente utile per le operazioni di data analytics, machine learning e real-time processing, offrendo una serie di librerie specializzate per diverse applicazioni. Con PySpark, è possibile gestire formati di dati diversi, eseguire operazioni analitiche complesse e garantire la tolleranza ai guasti, il tutto mantenendo un'elevata scalabilità e prestazioni ottimizzate. È uno strumento indispensabile nell'ambito del big data e dell'intelligenza artificiale, utilizzato da data engineers e data scientists per trasformare e interpretare grandi volumi di dati.

Nota: diverse configurazioni di sicurezza non sono abilitate di default. Prima di esporre l'applicativo ad una rete esterna è necessario mettere in sicurezza l'accesso al cluster.

5.1 SPARK REMOTE PROCEDURE CALL

Spark permette la comunicazione tra differenti processi tramite un protocollo di Remote Procedure Call (RCP). Questo viene utilizzato per la chiamata e l'esecuzione di procedure su sistemi remoti raggiungibili tramite una rete di comunicazione, le cui connessioni vanno però criptate tramite AES o SASL. Per poter usufruire del servizio, però, è necessaria l'autenticazione tramite uno shared secret, il cui meccanismo di creazione e distribuzione resta deployment-specific.
Sulla documentazione ufficiale è possibile consultare le configurazioni in ambiente YARN e Kubernetes, oltre alle modalità di cifratura disponibili.

5.2 CRITTOGRAFIA LOCAL STORAGE

Spark supporta inoltre la criptazione dei dati in lettura e scrittura sul dispositivo di archiviazione di massa.

5.2.1 Cifratura dei Dati con PySpark

La cifratura dei dati è un elemento cruciale nella protezione delle informazioni digitali.
Questa tecnica consente di trasformare i dati sensibili in un formato illeggibile a chiunque non disponga della chiave di decifratura corretta.

La cifratura garantisce la riservatezza dei dati, preservando la loro integrità e autenticità attraverso l'utilizzo di algoritmi complessi e chiavi di crittografia. Inoltre, la cifratura aiuta a proteggere le informazioni durante la trasmissione e l'archiviazione, assicurando che solo gli utenti autorizzati possano accedere ai dati originali.

PySpark permette di effettuare la cifratura dei dati utilizzando, utilizzando ad esempio funzioni di crittografia simmetrica. Segue un esempio che mostra come cifrare e decifrare un *Dataframe* utilizzando l'algoritmo di cifratura AES:

```
from pyspark.sql import SparkSession
from pyspark.sql.functions import expr

# Inizializzazione di SparkSession
spark = SparkSession.builder.appName("CifraturaDati").getOrCreate()

# Chiave di cifratura e vettore di inizializzazione (IV)
key = '0123456789abcdef'  # 16 byte chiave
iv = 'abcdef9876543210'  # 16 byte IV

# Creazione di un DataFrame di esempio
dataframe = spark.createDataFrame([("dato sensibile",)], ["plaintext"])

# Cifratura dei dati
dataframe_encrypted = dataframe.selectExpr(
    "plaintext",
    f"aes_encrypt(plaintext, unhex('{key}'), unhex('{iv}')) as ciphertext"
)

# Decifratura dei dati
dataframe_decrypted = dataframe_encrypted.selectExpr(
    "ciphertext",
    f"aes_decrypt(ciphertext, unhex('{key}'), unhex('{iv}')) as plaintext"
)

# Visualizzazione dei risultati
dataframe_encrypted.show()
dataframe_decrypted.show()
```

5.3 WEB UI

5.3.1 Access Control & Privilege Management

L'autenticazione per l'interfaccia web è implementata tramite javax servlet filters, in quanto spark non propone alcun filtro di autenticazione proprietario.
Una volta implementato, è possibile configurare delle Access Control Lists (**ACL**) all'interno delle quali specificare i permessi per gli utenti o i gruppi.

5.3.2 SSL

Secure Socket Layer (**SSL**) è un protocollo crittografico che garantisce la sicurezza, in particolar modo la confidenzialità e l'integrità, dei messaggi scambiati tra due entità solitamente di rete. L'utente può specificare le configurazioni di default per il protocollo come mostrato nella guida ufficiale.

5.3.3 HTTP Security Headers

Il protocollo HTTP mette a disposizione alcuni header specifici per la sicurezza del trasporto dei dati e del contenuto stesso. Questi includono la protezione dagli attacchi xss, l'utilizzo della Strict Transport Security etc. Tramite Spark è possibile includerli nelle risposte http/https.

5.4 SICUREZZA DELLA RETE

In accordo con la documentazione, un cluster Spark e i suoi servizi non sono distribuiti su Internet. Sono generalmente servizi privati e dovrebbero essere accessibili solo all'interno della rete dell'organizzazione che distribuisce Spark. Pertanto, l'accesso agli **host** e alle **porte** utilizzate dai servizi Spark deve essere limitato agli host di origine che devono accedere ai servizi.

5.5 KERBEROS

Kerberos è un protocollo di autenticazione per reti informatiche che utilizza dei *ticket* per permettere ai nodi di comunicare su una rete non sicura e dimostrare la propria identità in modo sicuro.
Questo protocollo mira a fornire autenticazione reciproca, dove sia l'utente che il server verificano l'identità dell'altro. Kerberos è particolarmente utile in ambienti Client-Server e viene impiegato per proteggere le credenziali degli utenti, mantenendo le password lontane dalle reti insicure durante la verifica delle identità.

Il processo di autenticazione Kerberos si articola nei seguenti passaggi:

1. Un utente che vuole accedere a una risorsa di rete richiede un Ticket Granting Ticket (TGT) al Key Distribution Center (KDC), fornendo le proprie credenziali in forma criptata.
2. Utilizzando il TGT ricevuto, l'utente richiede al KDC un Service Ticket (ST) per il servizio specifico a cui desidera accedere.
3. Con il ST ottenuto, l'utente può autenticarsi presso il servizio desiderato, che verifica il ticket e concede l'accesso alla risorsa.

Apache Spark supporta Kerberos; per maggiori dettagli sulla integrazione di Apache Spark con Kerberos fare riferimento alla documentazione ufficiale: Kerberos - Spark 3.5.1 Documentation (apache.org).

Nota: Se l'applicazione Spark interagisce con servizi Hadoop come HDFS o WebHDFS, anche questi servizi devono essere protetti con Kerberos.

5.6 LOGGING

Essendo disponibile la funzionalità di logging degli eventi, i relativi file di log presenti sul File System devono disporre di permessi restrittivi. Questo per permettere a tutte le utenze di scrivere sui file, ma anche per prevenire accessi non autorizzati a file che l'utente non possiede.

6 Azure Data Factory (ADF)

Azure Data Factory è un servizio cloud gestito che consente di orchestrare e operazionalizzare processi complessi di estrazione, trasformazione e caricamento (ETL), estrazione, caricamento e trasformazione (ELT) e integrazione dei dati. Questo strumento è essenziale per progetti di integrazione dati complessi e ibridi, in quanto fornisce una piattaforma per la movimentazione e la trasformazione dei dati da molteplici fonti di dati. Con Azure Data Factory, è possibile creare flussi di lavoro guidati dai dati, chiamati pipeline, che possono

ingerire dati da archivi dati disparati e costruire processi ETL complessi che trasformano i dati visivamente con flussi di dati o utilizzando servizi di calcolo come Azure HDInsight Hadoop, Azure Databricks e Azure SQL Database.

6.1 NETWORK SECURITY

Il capitolo "Network Security" della guida ufficiale Microsoft tratta lo stabilire i confini della segmentazione di rete, come l'integrazione delle reti virtuali e le regole di sicurezza di reti e sottoreti, e i servizi cloud sicuri con controlli di rete, come i link privati Azure e la visibilità pubblica e privata dell'accesso alla rete.

6.2 IDENTITY MANAGEMENT

La gestione delle identità rientra nel campo più grande del controllo degli accessi e della gestione dei privilegi, che si occupano di definire quali utenze possono accedere a determinate risorse e con quali permessi. Nello specifico, Microsoft tratta l'utilizzo di un sistema di identità e autenticazione centralizzato, l'automazione e la sicurezza delle identità e la restrizione delle risorse in base alle condizioni nel contesto, oltre a discutere sull'esposizione di credenziali e secrets.

6.3 PRIVILEGED ACCESS

Una delle fondamenta della corretta gestione dei permessi in un sistema informatico è l'adozione del principio noto come *"Least Privilege"*, per il quale un'utenza dovrebbe disporre solo e solamente dei privilegi necessari al suo scopo, senza nulla in eccesso o in difetto. ADF raccomanda infatti la separazione e la limitazione di utenze altamente privilegiate sulle risorse del sistema, per ridurre la potenziale superficie d'attacco ed effettuare un corretto hardening del prodotto.

6.4 DATA PROTECTION

Una corretta protezione dei dati impone alle organizzazioni gestioni rigorose dei dati in loro possesso, per prevenire esfiltrazioni e manomissioni di dati sensibili, personali e di business. In Europa è regolata principalmente dal **G**eneral **D**ata **P**rotection **R**egulation (**GDPR**) per quanto riguarda i dati personali. Sono trattati numerosi aspetti della materia, riassunti qui di seguito:

- Riconoscimento e classificazione dei dati sensibili
- Monitoring delle anomalie e vulnerabilità riguardanti i dati sensibili
- Crittografia dei dati in transito, a riposo e in uso
- Utilizzo di un processo di gestione sicura delle chiavi

6.5 ASSET MANAGEMENT

La gestione delle risorse riguarda i controlli per garantire la visibilità e la governance della sicurezza sulle risorse, comprese le raccomandazioni sulle autorizzazioni per il personale di sicurezza, l'accesso di sicurezza all'inventario delle risorse e la gestione delle approvazioni per i servizi e le risorse (inventario, tracciamento e correzione).

Microsoft suggerisce l'utilizzo esclusivo di servizi approvati rispetto alle Policy Azure.

6.6 LOGGING AND THREAT DETECTION

I controlli per il rilevamento delle minacce nel cloud e l'abilitazione, la raccolta e l'archiviazione dei registri di audit per i servizi cloud comprendono l'abilitazione dei processi di rilevamento, indagine e bonifica con controlli per la generazione di avvisi di alta qualità con il rilevamento nativo delle minacce nei servizi cloud; comprende anche la raccolta dei registri con un servizio di monitoraggio del cloud, la centralizzazione dell'analisi della sicurezza con un SIEM, la sincronizzazione temporale e la conservazione dei registri.

In particolare, vengono discusse l'abilitazione dei servizi per la threat detection ed il logging per le investigazioni di sicurezza.

6.7 BACKUP AND RECOVERY

Infine, viene posto l'accento sull'importanza di effettuare regolarmente copie di backup automatiche e regolari, sfruttando quelle che sono le funzionalità native del prodotto.

Italgas S.p.A - Informazioni Interne

7 PowerBI

Power BI è un servizio di analisi aziendale offerto da Microsoft che consente di visualizzare i dati e condividere informazioni all'interno di un'organizzazione o di incorporarli in un'app o un sito web. Questo strumento trasforma i dati grezzi in informazioni significative attraverso dashboard interattivi e report, facilitando la comprensione e l'analisi delle tendenze. Power BI si collega a una vasta gamma di fonti di dati, da file Excel semplici a database complessi, e offre strumenti per trasformare, aggregare e visualizzare i dati in modo che possano essere esplorati con semplici drag-and-drop. Gli utenti possono creare report personalizzati e condividerli con altri membri del team, permettendo una collaborazione e una presa di decisioni basate sui dati più efficace.

7.1 ACCESS CONTROL & PRIVILEGE MANAGEMENT

Il controllo degli accessi e la gestione dei privilegi assicurano la confidenzialità dei dati, e che le operazioni su questi siano definite da una rigorosa policy. Se quest'ultima è troppo lasca, o se il sistema presenta debolezze che ne minano la robustezza, c'è il serio rischio di incorrere in vulnerabilità quali information disclosure a individui non autorizzati o privilege escalation.

7.1.1 Autenticazione

L'**autenticazione** degli utenti in Power BI si basa sull'utilizzo di Microsoft Entra ID, che gestisce le identità degli utenti e fornisce token per le connessioni client successive al servizio Power BI. Inizialmente, gli utenti si autenticano attraverso il cluster Web Front End (WFE), che gestisce la connessione iniziale e l'autenticazione al servizio Power BI. Una volta autenticati, il cluster Back-End gestisce tutte le interazioni successive dell'utente. È importante notare che solo i ruoli di Azure API Management e Gateway sono accessibili tramite Internet pubblico, fornendo autenticazione, autorizzazione, protezione DDoS, bilanciamento del carico, routing e altre capacità.

L'importanza dell'autenticazione a più fattori (MFA) in PowerBI è cruciale nel contesto della sicurezza informatica. La MFA aggiunge un livello di sicurezza essenziale proteggendo l'accesso ai dati e ai report critici. In PowerBI, l'implementazione della MFA può prevenire efficacemente gli accessi non autorizzati, poiché richiede agli utenti di fornire due o più credenziali di verifica prima di concedere l'accesso. Questo metodo di autenticazione va oltre la semplice password, includendo qualcosa che l'utente conosce (come una password), qualcosa che possiede (come un token di sicurezza o un telefono cellulare), e/o qualcosa che è (come l'impronta digitale).

Per maggiori dettagli fare riferimento alla documentazione ufficiale: User Authentication - PowerBI Security.

7.1.2 Storage e accessi ai dati

Power BI assicura un elevato livello di sicurezza per lo **storage dei dati**, utilizzando una combinazione di **sicurezza a livello di riga (RLS)**, **sicurezza a livello di oggetto (OLS)** e autenticazione. La sicurezza a livello di riga permette di limitare l'accesso ai dati per determinati utenti, con filtri che restringono l'accesso ai dati a livello di riga, definibili all'interno dei ruoli. La sicurezza a livello di oggetto protegge tabelle o colonne sensibili, nascondendo anche i nomi degli oggetti e i metadati.

Inoltre, la gestione dello storage dei dati e dei metadati, è realizzata mediante Azure BLOB e Azure SQL Database. Queste misure sono parte di una soluzione di sicurezza multilivello, nativa del cloud, che fornisce una protezione completa e ermetica per i dati.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: Data and Service Security - PowerBI Security.

7.1.3 App Workspaces

Gli **App Workspaces** in Power BI sono ambienti collaborativi che consentono ai team di lavorare insieme su insiemi di dashboard, report e modelli semantici.

Dal punto di vista della sicurezza informatica, offrono un controllo granulare degli accessi attraverso ruoli definiti come Admin, Membro, Collaboratore e Visualizzatore, che permettono di gestire chi può fare cosa all'interno dello spazio di lavoro.
Questo aiuta a proteggere i dati sensibili e a garantire che solo gli utenti autorizzati possano accedere a informazioni specifiche o eseguire determinate azioni. Inoltre, la possibilità di creare App template consente di distribuire contenuti in modo sicuro ai clienti esterni all'organizzazione, che possono connettersi ai propri dati con l'app template.

7.2 SICUREZZA DELLA RETE

La sicurezza di rete è una componente fondamentale della sicurezza informatica che si concentra sulla protezione delle reti di computer contro le minacce informatiche. Questo campo si occupa di prevenire l'accesso non autorizzato, rilevare e bloccare gli attacchi informatici e assicurare che gli utenti autorizzati possano accedere in modo sicuro alle risorse di rete necessarie. Utilizza tecnologie come firewall, sistemi di prevenzione delle intrusioni e software anti-malware per creare una difesa multilivello contro le varie tipologie di attacchi, garantendo così l'integrità, la disponibilità e la riservatezza delle informazioni trasmesse attraverso la rete.

7.2.1 Service Tags

I **service tag** in Power BI sono utilizzati per gestire gruppi di indirizzi IP definiti che consentono connessioni in entrata e in uscita con servizi specifici di Azure, come un'istanza gestita di SQL. Questo è particolarmente utile per semplificare la configurazione e la gestione delle regole di sicurezza della rete, riducendo la complessità e il bisogno di aggiornamenti frequenti.

Utilizzando i service tag, è possibile, ad esempio, abilitare un'istanza gestita di SQL per accettare connessioni dal servizio Power BI, configurando un endpoint pubblico, creando una regola del gruppo di sicurezza di rete per consentire il traffico in entrata e inserendo le credenziali in Power BI.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: Service Tags - PowerBI Security Whitepaper.

7.2.2 Private Link

I **Private Link** in Power BI sono una funzionalità di sicurezza che permette di accedere ai servizi di Power BI attraverso un endpoint privato all'interno di una rete virtuale Azure (VNet). Questo significa che i dati possono transitare attraverso una connessione privata, senza passare attraverso Internet pubblico, aumentando così la sicurezza e la privacy.

Utilizzando i Private Link, è possibile configurare connessioni sicure per client on-premises, estendendo la rete locale al VNet di Azure tramite un circuito ExpressRoute o una VPN site-to-site.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: Private Link - PowerBI Security Whitepaper.

7.2.3 Rete VNet

Una **rete VNet** in Power BI si riferisce all'uso di un gateway dati di rete virtuale che permette ai modelli semantici di importazione o di query diretta di connettersi ai servizi dati all'interno di una rete virtuale Azure senza la necessità di un gateway dati locale.

Questo tipo di configurazione è particolarmente utile per le organizzazioni che desiderano mantenere i loro dati in sicurezza all'interno del cloud di Azure, garantendo al contempo la flessibilità e la potenza analitica di Power BI. Per utilizzare i gateway dati VNet, è necessario disporre di una licenza Power BI Premium con capacità (SKU A4 o superiore o qualsiasi SKU P).

Inoltre, i gateway dati VNet consentono una gestione semplificata degli amministratori e delle origini dati, simile a quella dei gateway dati standard, ma con il vantaggio aggiuntivo della sicurezza e dell'integrazione nel cloud.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: VNet Connectivity - PowerBI Security Whitepaper.

7.2.4 Transport Layer Security (TLS)

Il protocollo **TLS (Transport Layer Security)** è essenziale per garantire la sicurezza delle comunicazioni su internet, e il suo utilizzo con Power BI è fondamentale per proteggere i dati durante il trasferimento. Power BI supporta TLS 1.2, che è la versione raccomandata per mantenere una connessione sicura al servizio Power BI.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: Enforcing TLS version usage - PowerBI Security.

7.3 MONITORAGGIO E AUDITING

Il monitoraggio delle componenti di un sistema è cruciale per la sicurezza informatica poiché consente di rilevare e rispondere rapidamente a potenziali minacce. Attraverso l'analisi continua del traffico di rete e dei registri di sistema, è possibile identificare comportamenti sospetti e agire per mitigarli. Questo tipo di monitoraggio proattivo è essenziale per proteggere i dati sensibili e la proprietà intellettuale, riducendo il rischio di violazioni dannose e mantenendo l'integrità delle risorse digitali.

7.3.1 Monitoraggio dei Data Gateway

Il **monitoraggio dei data gateways** in Power BI è un processo cruciale per garantire la sicurezza e l'efficienza del trasferimento dei dati tra le origini dati locali e i servizi cloud. I gateway fungono da ponte, permettendo a Power BI di accedere ai dati che non sono direttamente raggiungibili via internet. Questi gateway possono essere gestiti e monitorati per assicurare che le prestazioni siano ottimali e che non ci siano interruzioni nel servizio. Gli amministratori dei gateway hanno il compito di implementare, gestire e sorvegliare queste connessioni, assicurandosi che siano sicure e affidabili. Inoltre, è importante pianificare attentamente l'uso dei gateway per mitigare eventuali rischi futuri e garantire la governance dei dati.

7.3.2 Audit Logs

Gli **Audit Logs** in Power BI sono strumenti essenziali per la sicurezza informatica, poiché consentono di monitorare e registrare tutte le attività degli utenti all'interno della piattaforma. Questo tipo di tracciamento è fondamentale per garantire la conformità alle normative, come il GDPR, e per rilevare eventuali comportamenti sospetti o non autorizzati che potrebbero indicare una violazione dei dati. Attraverso l'analisi degli Audit Logs, gli amministratori possono verificare quali dati sono stati accessi, modificati o eliminati, chi ha eseguito queste azioni e quando.

Questo livello di dettaglio è cruciale per la diagnosi rapida di problemi di sicurezza e per la prevenzione di future minacce. Inoltre, gli Audit Logs supportano le aziende nell'implementazione di politiche di sicurezza efficaci e nell'adottare misure proattive contro gli attacchi informatici.

8 ESRI ArcGIS

ESRI ArcGIS è una piattaforma geospaziale completa che fornisce un insieme di strumenti GIS (Geographic Information System) per la visualizzazione, l'analisi e la condivisione di dati geografici. Utilizzato da aziende e governi, ArcGIS aiuta a comprendere meglio i dati spaziali attraverso la creazione di mappe interattive che possono rivelare tendenze e schemi. Questo software supporta la presa di decisioni informate in vari settori, dall'urbanistica alla gestione delle emergenze. Con ArcGIS, gli utenti possono raccogliere, gestire e analizzare dati geografici, trasformandoli in informazioni utili per il proprio contesto lavorativo o di ricerca.

ESRI mette a disposizione una esaustiva guida (Technical Paper) di hardening che comprende la maggior parte dei principi di hardening presentati: ArcGIS Enterprise - Hardening Guide - ESRI Technical Paper.

8.1 SICUREZZA APPLICATIVA

Le impostazioni di sicurezza di ArcGIS sono configurabili direttamente dall'utente e permettono di:

- Rafforzare le funzionalità di sicurezza delle applicazioni
- Disabilitare i servizi/le funzionalità utilizzati di rado
- Disabilitare gli account di configurazione

8.2 IDENTITY AND ACCESS MANAGEMENT (IAM)

Per utilizzare i servizi di ArcGIS Enterprise, è necessario concedere agli utenti e alle applicazioni l'accesso alle risorse. Le operazioni di produzione richiedono una solida gestione delle identità e delle autorizzazioni per garantire che le persone giuste abbiano accesso alle risorse giuste nelle condizioni giuste. ArcGIS Enterprise offre un'ampia gamma di funzionalità che aiutano a gestire le identità di utenti e applicazioni e le relative autorizzazioni.
Le best practice per queste funzionalità rientrano nelle seguenti aree:

- Identità degli utenti e delle applicazioni
- Gestione centralizzata delle identità
- Gruppi di utenti e attributi
- Gestione dei permessi

Quando si discute di tematiche IAM, è necessario conoscere come l'applicativo gestisce tematiche quali autenticazione, gestione dei privilegi ed eventuali token d'accesso. Questo è coperto nella documentazione ufficiale, ed è possibile trovare il link d'accesso nel paragrafo IDENTITY AND ACCESS MANAGEMENT della sezione *"Link utili"*.

8.3 INFRASTRUTTURA DI SUPPORTO

La sicurezza dell'infrastruttura comprende tutti i controlli che si applicano alla rete, al sistema operativo, al database e al server web che supportano l'applicazione, e server web che supportano l'applicazione. Si deve tenere presente che mantenere aggiornati i componenti dell'infrastruttura di supporto è importante quanto l'utilizzo dell'ultima versione del software applicativo ArcGIS Enterprise.
Gli elementi trattati includono i seguenti:

- Linee di base della sicurezza Zero Trust
- Protezioni dei confini
- Amministrazione ad accesso privilegiato basata sulla rete

8.4 DATA PROTECTION

Il NIST descrive la protezione dei dati in parte come l'istituzione di un controllo dell'accesso a grana fine per le risorse di dati, la protezione dei dati a riposo, la protezione dei dati in transito e la corretta gestione dei backup.

I paragrafi trattati dalla documentazione tendono a coprirne le seguenti casistiche:

- Gestione dei dati e backup
- Protezione dei dati a riposo
- Protezione dei dati in transito
- Controllo degli accessi a grana fine

8.5 INVENTORY AND MANTAINANCE

L'obiettivo dell'inventario e della manutenzione del sistema è quello di proteggere l'integrità delle piattaforme software critiche di fronte alla divulgazione di nuove vulnerabilità ed exploit. Per quanto riguarda ArcGIS Enterprise, ciò significa che i clienti devono fare quanto segue:

- Identificare e mantenere un inventario dei sistemi ArcGIS Enterprise1 e delle integrazioni.
- Utilizzare versioni del prodotto a disponibilità generale (GA) supportate.
- Implementare la gestione e la verifica delle patch.
- Assicurare una solida gestione della configurazione e una convalida regolare.

8.6 DETECTION AND RESPONSE

ArcGIS Enterprise fornisce agli amministratori e ai responsabili una guida per individuare, rispondere e ripristinare rapidamente le minacce e gli incidenti che hanno un impatto sulla riservatezza, l'integrità dei dati e la disponibilità del sistema offerto da ArcGIS Enterprise.
Le indicazioni riguardano:

- Rilevamento e monitoraggio dei registri
- Risposta agli incidenti

8.7 PRIVACY

L'aspetto della privacy dei dati richiede un'attenta considerazione quando si ha a che fare con infrastrutture geospaziali, in particolare quelle che utilizzano la tecnologia ArcGIS Enterprise. La Guida all'hardening di ArcGIS Enterprise fornisce indicazioni fondamentali sugli approcci critici che i clienti dovrebbero adottare per la protezione delle informazioni private.

Un processo di garanzia della privacy di successo richiede il rigoroso rispetto dei protocolli di privacy stabiliti e l'adozione di misure adeguate a ridurre al minimo i rischi associati alla divulgazione involontaria o alle violazioni dolose dei dati sensibili archiviati nell'ArcGIS Data Store.

9 TIBCO BW, TIBCO BWCE & TIBCO Mashery

TIBCO BusinessWorks (BW) è una piattaforma di integrazione aziendale che consente alle organizzazioni di connettere applicazioni, dati e dispositivi in modo fluido. Offre un ambiente di sviluppo visivo e basato su modelli, che facilita la progettazione, il dispiegamento e la gestione di soluzioni di integrazione senza richiedere un'estesa codifica. TIBCO BusinessWorks Container Edition (BWCE) è una versione ottimizzata per container di TIBCO BW, che permette di costruire applicazioni native per il cloud con un approccio API-first e di distribuirle su piattaforme PaaS basate su container come Cloud Foundry, Kubernetes e OpenShift.

TIBCO Mashery è una piattaforma API full-life cycle che fornisce le capacità di gestione delle API necessarie per le iniziative di trasformazione digitale, inclusi la creazione, il packaging, il test, la governance, la sicurezza e la gestione del traffico delle API, oltre al supporto per un ecosistema di sviluppatori interni ed esterni. Insieme, questi strumenti offrono un framework robusto per l'integrazione e la gestione delle API, essenziali per le moderne architetture IT e le strategie di digitalizzazione.

9.1 ACCESS CONTROL & PRIVILEGE MANAGEMENT

Il controllo degli accessi e la gestione dei privilegi assicurano la confidenzialità dei dati, e che le operazioni su questi siano definite da una rigorosa policy. Se quest'ultima è troppo lasca, o se il sistema presenta debolezze che ne minano la robustezza, c'è il serio rischio di incorrere in vulnerabilità quali information disclosure a individui non autorizzati o privilege escalation.

9.1.1 Ruoli e Permessi (TIBCO BW)

TIBCO BW mette a disposizione una gestione dei privilegi associati ad un utente che determinano quali azioni può eseguire sull'interfaccia grafica amministrativa (Admin UI).

Un amministratore può assegnare permessi ad utenti e gruppi attraverso un ruolo; ad ogni ruolo sono assegnati dei permessi. Un utente o gruppo riceve tutti i permessi associati al ruolo.

Sono definiti i seguenti ruoli: BW User, BW Operator, and BW Administrator.

Nella Admin UI, i permessi sono definiti su due distinti livelli:

- **Entity Based**: il permesso è valido per una intera entità come un dominio o un AppSpace.
- **Instance Based**: il permesso è valido per una particolare istanza di una entità.

Esistono tre diversi tipi di permessi:

- **Read**: Permesso di sola lettura.
- **Lifecycle**: Permesso di avviare o stoppare una entità (AppSpace, AppNode, appplications, etc.). Assegnabile ad un utente che ha già il permesso *Read*.
- **Full_control**: Garantisce il controllo completo su una entità.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: Roles and Permissions - TIBCO BW

9.1.2 OAuth2 (Mashery)

OAuth2 è uno standard di autorizzazione aperto che permette a siti web e applicazioni di accedere a risorse ospitate da altre applicazioni web per conto di un utente.
OAuth2 fornisce accesso consensuale e limita le azioni che l'applicazione cliente può eseguire sulle risorse per conto dell'utente, senza mai condividere le credenziali dell'utente.

Un vantaggio significativo di OAuth2 è che utilizza token di accesso, che sono dati che rappresentano l'autorizzazione ad accedere alle risorse per conto dell'utente finale. I token possono avere una data di scadenza per motivi di sicurezza e, sebbene OAuth2 non definisca un formato specifico per i token di accesso, spesso si utilizza il formato JSON Web Token (JWT) che permette di includere dati nel token stesso.

OAuth2 introduce il concetto di "scope", utilizzato per specificare esattamente il motivo per cui può essere concesso l'accesso alle risorse. I valori di scope accettabili e le risorse a cui si riferiscono dipendono dal server delle risorse. Inoltre, OAuth2 consente agli utenti di autorizzare esplicitamente le applicazioni per azioni specifiche e di revocare l'accesso in qualsiasi momento, dando loro il controllo sui propri dati e sulla privacy.

TIBCO Mashery supporta OAuth; per maggiori dettagli sulla configurazione fare riferimento alla documentazione ufficiale: OAuth - TIBCO Mashery.

9.2 SICUREZZA DELLA RETE

La sicurezza di rete è una componente fondamentale della sicurezza informatica che si concentra sulla protezione delle reti di computer contro le minacce informatiche. Questo campo si occupa di prevenire l'accesso non autorizzato, rilevare e bloccare gli attacchi informatici e assicurare che gli utenti autorizzati possano accedere in modo sicuro alle risorse di rete necessarie. Utilizza tecnologie come firewall, sistemi di prevenzione delle intrusioni e software anti-malware per creare una difesa multilivello contro le varie tipologie di attacchi, garantendo così l'integrità, la disponibilità e la riservatezza delle informazioni trasmesse attraverso la rete.

9.2.1 Sicurezza per HTTP (BW e BWCE)

TIBCO consiglia di impiegare una policy *Basic Authentication* per assicurare che l'utente sia autenticato quando effettua richieste HTTP, REST e SOAP. Inoltre, sarebbe opportuno attuare una policy *Basic Credential Mapping* che permette di mappare le credenziali con diversi tipi di utenti.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: HTTP Security - TIBCO BW e HTTP Security - TIBCO BWCE.

9.2.2 Sicurezza per SOAP (BW e BWCE)

TIBCO consiglia di impiegare una policy *WSS Consumer* per assicurare che la confidenzialità, integrità ed il timestamp di una richiesta siano sicuri. Inoltre, è consigliato utilizzare una policy *WSS Provider* per garantire autenticazione, confidenzialità, integrità e time stamp per messaggi server-side.

Per maggiori dettagli fare riferimento alla documentazione ufficiale: SOAP Security - TIBCO BW e SOAP Security - TIBCO BWCE.

9.2.3 HTTPS e Mutua Autenticazione (Mashery)

L'utilizzo di HTTPS permette di stabilisce un canale di comunicazione criptato tra il client e il server, garantendo che i dati trasmessi siano protetti da intercettazioni e manipolazioni.
Questo protocollo utilizza la crittografia SSL/TLS per proteggere l'integrità e la riservatezza delle informazioni durante il loro transito attraverso la rete.
Inoltre, HTTPS fornisce un meccanismo di autenticazione del server, assicurando agli utenti che stanno connettendosi al sito web autentico.

La mutua autenticazione HTTPS coinvolge anche l'autenticazione del client da parte del server. Questo è particolarmente utile in ambienti aziendali o in applicazioni che richiedono un alto livello di sicurezza, poiché assicura che entrambe le parti nella comunicazione siano chi dichiarano di essere, prevenendo così attacchi come il phishing o l'intercettazione di identità.

TIBCO Mashery permette la configurazione della comunicazione HTTPS, con e senza mutua autenticazione; per maggiori dettagli fare riferimento alla documentazione ufficiale: HTTPS Configuration - TIBCO Mashery.

9.3 MONITORAGGIO E AUDITING

Il monitoraggio delle componenti di un sistema è cruciale per la sicurezza informatica poiché consente di rilevare e rispondere rapidamente a potenziali minacce. Attraverso l'analisi continua del traffico di rete e dei registri di sistema, è possibile identificare comportamenti sospetti e agire per mitigarli. Questo tipo di monitoraggio proattivo è essenziale per proteggere i dati sensibili e la proprietà intellettuale, riducendo il rischio di violazioni dannose e mantenendo l'integrità delle risorse digitali.

TIBCO Mashery permette il monitoraggio di tutte le sue componenti attraverso diverse metriche; per maggiori dettagli fare riferimento alla documentazione ufficiale: Monitoring Mashery Local Components - TIBCO Mashery.

10 Link utili

- **ACCESS CONTROL & PRIVILEGE MANAGEMENT**
  - **Utenti, Gruppi e Permessi**
    - User Administration and Security | Adobe Experience Manager
    - User, Group and Access Rights Administration | Adobe Experience Manager
- **SECURITY CHECKLIST**

Security Checklist | Adobe Experience Manager

- **ACCESS CONTROL & PRIVILEGE MANAGEMENT**
  - Databricks administration introduction | Databricks on AWS
  - Get started with Databricks administration | Databricks on AWS
  - Manage users, service principals, and groups | Databricks on AWS
  - Manage your workspace | Databricks on AWS
- **CRITTOGRAFIA**
  - Data security and encryption | Databricks on AWS
- **GESTIONE DEI SECRET**
  - Secret management | Databricks on AWS
- **SICUREZZA DELLA RETE**
  - Best practices for security, compliance & privacy | Databricks on AWS
- Security and compliance guide | Databricks on AWS
- Best practices for security, compliance & privacy | Databricks on AWS
- **SPARK REMOTE PROCEDURE CALL**
  - Security - Spark 3.5.1 Documentation (apache.org)
- **CRITTOGRAFIA LOCAL STORAGE**
  - Security - Spark 3.5.1 Documentation (apache.org)
- **WEB UI**
  - Security - Spark 3.5.1 Documentation (apache.org)
- **SICUREZZA DELLA RETE**
  - Security - Spark 3.5.1 Documentation (apache.org)
- **KERBEROS**
  - Security - Spark 3.5.1 Documentation (apache.org)
- **LOGGING**
  - Security - Spark 3.5.1 Documentation (apache.org)
  - Security - Spark 3.5.1 Documentation (apache.org)
- Security considerations - Azure Data Factory | Microsoft Learn
- Azure security baseline for Data Factory | Microsoft Learn
- **NETWORK SECURITY**
  - Azure security baseline for Data Factory | Microsoft Learn
- **IDENTITY MANAGEMENT**
  - Azure security baseline for Data Factory | Microsoft Learn
- **PRIVILEGED ACCESS**
  - Azure security baseline for Data Factory | Microsoft Learn

- **DATA PROTECTION**
  - Azure security baseline for Data Factory | Microsoft Learn
- **ASSET MANAGEMENT**
  - Azure security baseline for Data Factory | Microsoft Learn
- **LOGGING AND THREAT DETECTION**
  - Azure security baseline for Data Factory | Microsoft Learn
- **BACKUP AND RECOVERY**

Azure security baseline for Data Factory | Microsoft Learn

- **ACCESS CONTROL & PRIVILEGE MANAGEMENT**
  - **Autenticazione**
    - User Authentication - PowerBI Security
  - **Storage dei Dati**
    - Data and Service Security - PowerBI Security
  - **App Workspaces**
    - Workspaces in Power BI - Microsoft Learn
- **SICUREZZA DELLA RETE**
  - **Service Tags**
    - Service Tags - PowerBI Security Whitepaper
  - **Private Link**
    - Private Link - PowerBI Security Whitepaper
  - **Rete VNet**
    - VNet Connectivity - PowerBI Security Whitepaper
  - **Transport Layer Security (TLS)**
    - Enforcing TLS version usage - PowerBI Security
- **MONITORAGGIO E AUDITING**
  - **Monitoraggio dei Data Gateways**
    - Gateway - Microsoft Learn
  - **Audit Logs**
    - Track user activities in Power BI - Microsoft Learn
- ArcGIS Enterprise - Hardening Guide - ESRI Technical Paper
- ArcGIS security—ArcGIS Trust Center | Documentation
- **IDENTITY AND ACCESS MANAGEMENT**

Introduction to security and authentication | Documentation | Esri Developer (arcgis.com)

- **ACCESS CONTROL & PRIVILEGE MANAGEMENT**
  - **Ruoli e Permessi (TIBCO BW)**
    - Roles and Permissions - TIBCO BW
  - **OAuth2 (Mashery)**
    - OAuth - TIBCO Mashery
- **SICUREZZA DELLA RETE**
  - **Sicurezza per HTTP (BW e BWCE)**
    - HTTP Security - TIBCO BW
    - HTTP Security - TIBCO BWCE
  - **Sicurezza per SOAP (BW e BWCE)**
    - SOAP Security - TIBCO BW
    - SOAP Security - TIBCO BWCE
  - **HTTPS e Mutua Autenticazione (Mashery)**
    - HTTPS Configuration - TIBCO Mashery
- **MONITORAGGIO E AUDITING**
  - Monitoring Mashery Local Components - TIBCO Mashery