EPICODE

GRUPPO BCC ICCREA

S4 - L1

Gestione del rischio informatico per un caso aziendale specifico - Prepare

17 maggio 2024

Team

- Alessio D'Ottavio
- Lisa Bonato
- Manuel Di Gangi
- Maria Flavia Minotti
- Oliviero Camarota

INDICE

Traccia

1. Progetto guidato settimanale

In questo progetto svilupperemo un piano di gestione del rischio informatico per un caso aziendale specifico che durerà tutta la settimana. Faremo uso di SimpleRisk e seguiremo NIST SP 800-37r2 RMF, attraversando tutte le fasi*:

- Prepare
- Categorize
- Select
- Implement
- Assees
- Authorize
- Monitor

Si consiglia la suddivisione in gruppi a partire già da oggi. * Sono stati selezionati un sottoinsieme di task per far rientrare l'intero processo in una settimana.

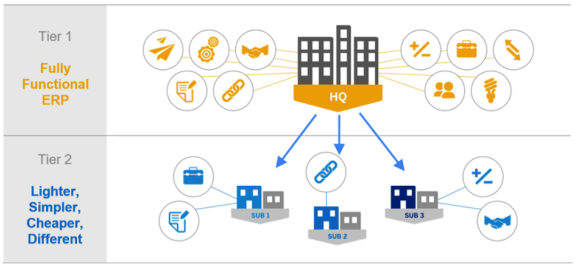
2. Caso aziendale

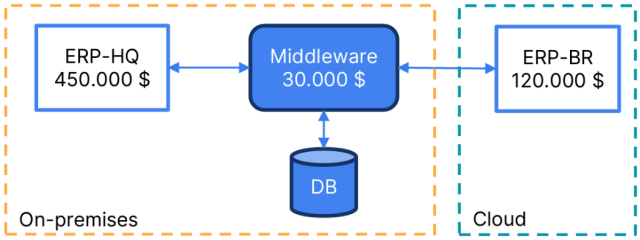
Un'organizzazione ha sviluppato, in outsourcing, un'integrazione (middleware), tra il suo Enterprise Resource Planning (ERP) per la sede centrale (headquarter, HQ) e l'ERP di filiale (branch, BR), implementando un two-tier ERP.

- **ERP**: software di gestione che integra tutti i processi aziendali e tutte le funzioni aziendali rilevanti, ad esempio vendite, acquisti, gestione magazzino, finanza o contabilità.
- **Two-tier ERP**: approccio alla gestione delle risorse aziendali (ERP) che utilizza due sistemi software distinti per soddisfare le esigenze delle grandi aziende con molteplici sedi e/o filiali. Tier 1: ERP di sede centrale, centralizzato e robusto, in grado di gestire le

operazioni e i requisiti generali dell'organizzazione. Tier 2: Nelle filiali o stabilimenti remoti viene implementato un sistema ERP separato. Questo sistema è più snello e flessibile, e permette alle filiali di avere una certa autonomia nella gestione delle loro operazioni, tenendo conto dei processi localizzati. Solitamente un ERP Tier 2 non è in grado di vedere gli altri ERP Tier 2.

- **Middleware**: software che funge da intermediario tra diverse applicazioni, nel caso specifico sincronizzazione utenti, ordini e magazzino. L'integrazione si è rese necessaria perché sono ERP di fornitori diversi e non esiste un'integrazione nativa. L'organizzazione non valuta di sostituire gli ERP.





3. Specifiche middleware

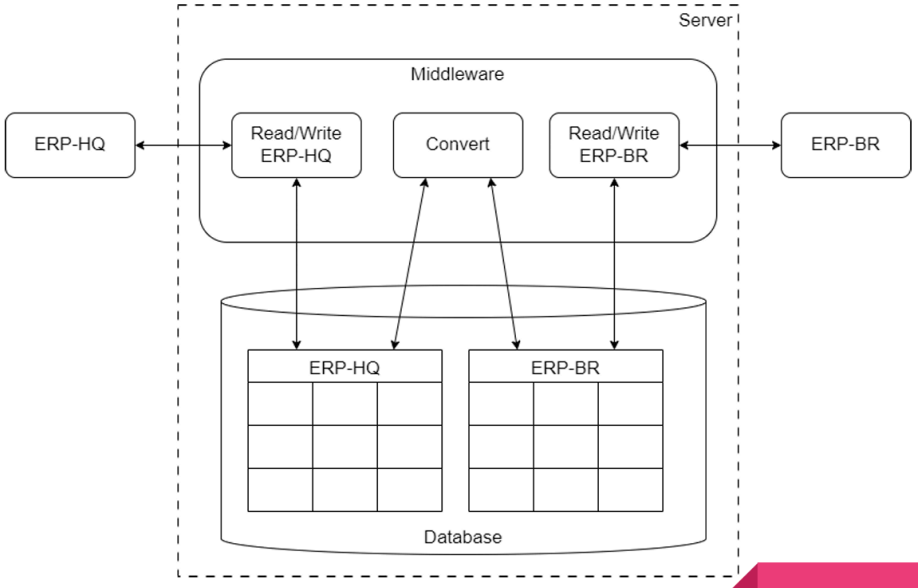
L'organizzazione conosce il funzionamento di alto livello del middleware. All'interno del middlware è presente il modulo Convert che si occupa di tradurre i record dell'ERP-HQ in record validi per l'ERP-BR e viceversa. Convert si attiva quando rileva delle modifiche nelle tabelle del proprio database interno. Nel database interno sono presenti le tabelle ERP-HQ e ERP-BR che conservano tutti i record che transitano tra ERP-HQ e ERP-BR (ERP-HQ e ERP-BR sono indipendenti e hanno un proprio database). I due moduli Read/Write ERP-HQ e ERP-BR si occupano di leggere/scrivere i dati di transito nel db interno tra ERP-HQ/Middleware e ERP-BR/Middleware. Middleware e database di supporto, risiedono sullo stesso server on-premises, ma differente dall'ERP-HQ. Il Middleware riesce a soddisfare un carico massimo di 250 transazioni all'ora (tx/h) (complessive da/verso ERP-HQ/ERP-BR), l'attuale traffico si aggira sulle 100 tx/h.

4. Scenario attuale

Da qualche giorno, l'azienda che ha sviluppato il middleware custom è stata chiusa, non offrendo più supporto e aggiornamenti. E' presente solamente il codice sorgente, non ci sono guide, manuali e progetti. ERP-HQ e ERP-BR sono soluzioni proprietarie closed-source di altre aziende che continuano ad offrire supporto e aggiornamenti. ERP-HQ e ERP-BR non saranno oggetto di migrazioni (resteranno, rispettivamente, on-premises e su cloud). Il middleware è di fondamentale importanza perché permette di sincronizzare i due ERP, ad esempio, magazzino, impianti di produzione, utenti, fatturazione, ecc. Adesso, l'organizzazione deve valutare se:

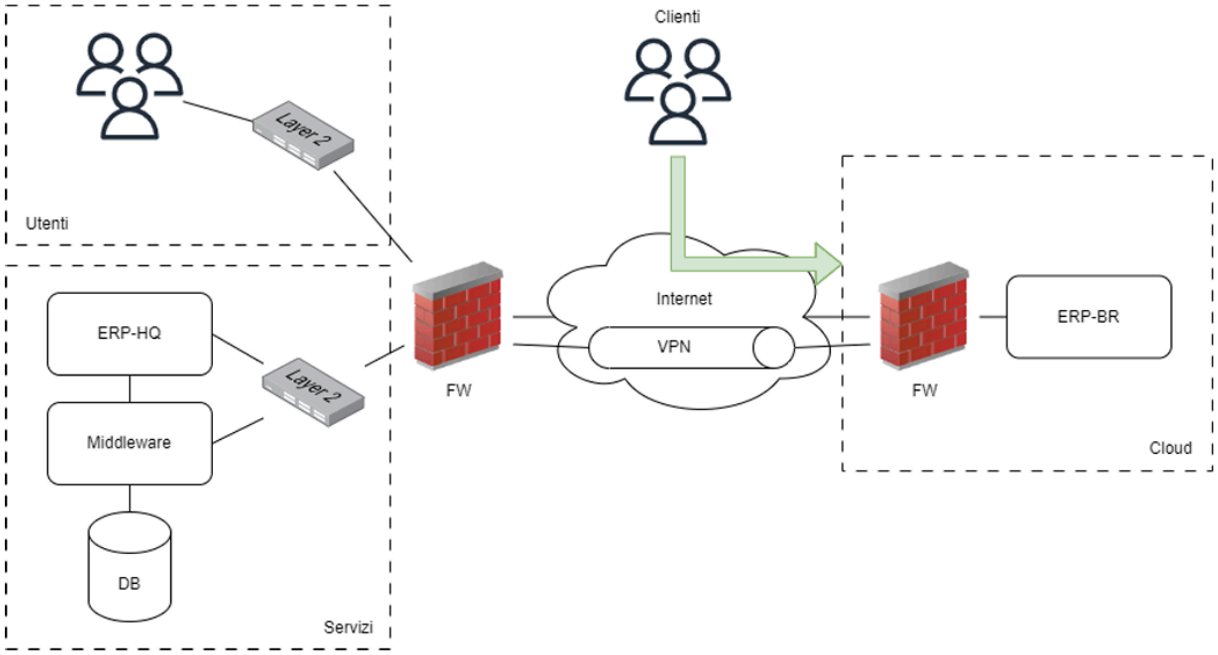
1. continuare a manutenere questo middleware on-premises, di cui non conosce molto, trovando un nuovo fornitore in grado di fare un'analisi approfondita (compreso reverse engineering) per poterne continuare lo sviluppo, oppure,
2. sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, possibilmente low-code/no-code per evitare l'affidamento ad un'altra software house e gestire il solo mapping delle strutture dati con le risorse interne (dipendenti). In occasione del riesame, si valuta anche la possibilità di aumentare le misure di sicurezza, se necessario.

Utilizzeremo NIST SP 800-37r2 RMF per impostare una strategia di gestione del rischio e dare un'indicazione al management/direzione su quale opzione, tra le due, è la più coerente rispetto al profilo organizzativo.



5. Creazione dell'architettura di partenza (opzione 1)

Ipotizzate un'architettura di rete (fisica e logica) di partenza. Ad esempio, nella figura mostrata in basso, i servizi sono in una rete separata rispetto agli utenti interni della sede centrale (HQ). Gli utenti interni possono accedere all'ERP-HQ per la gestione interna e l'ERP-HQ può collegarsi a Internet solo per aggiornamenti (non per comunicare con l'ERP-BR). Solo il middleware può collegarsi all'ERP-BR tramite VPN. I Clienti della filiale si collegano all'ERP-BR, in cui è presente un portale web. Solo l'ERP-BR è in cloud. Il CED on-premises non dispone di nessuna misura di continuità operativa (BC) se non un UPS per interruzioni elettriche di breve durata.



6. Creazione dell’architettura alternativa (opzione 2)

Definite un’architettura che rispecchia gli obiettivi emanati dalla direzione nel punto 2:

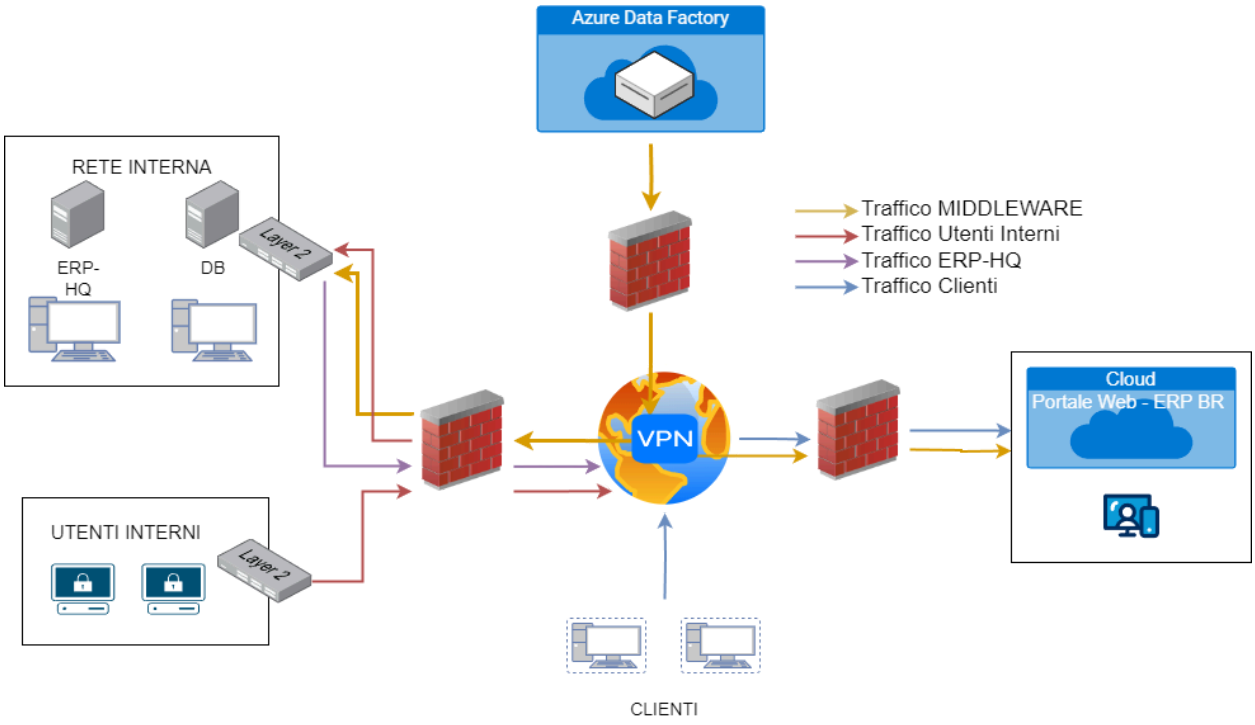
2. sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, possibilmente low-code/nocode per evitare l’affidamento ad un’altra software house e gestire il solo mapping delle strutture dati con le risorse interne (dipendenti).

Scegliete una soluzione SaaS/iPaaS che permetta di riprodurre il funzionamento del Middleware, in particolare il modulo Convert che si occupa della trasformazione dei dati da una struttura dati ad un’altra (i rischi correlati all’utilizzo di un SaaS si equivalgono, basta sceglierne uno come riferimento). Potete scegliere anche di indirizzarvi verso una soluzione open source, in questo caso potrebbe essere a carico vostro la gestione dell’infrastruttura o della piattaforma cloud (IaaS/PaaS).

Esempi di data integration/pipeline/automation/ETL:

- https://azure.microsoft.com/en-us/products/data-factory
- https://www.bytesroute.com/
- https://airbyte.com/
- https://dataddo.com/
- https://marjory.io/

Proposta di design di rete



Come si può dedurre dallo schema di rete ideato, si è deciso di analizzare l'opzione 2 prevedendo che il middleware sia sostituito da una soluzione SaaS basata su cloud.

Al centro si è inserita la connessione internet con la VPN che consente il collegamento tra le varie della rete aziendale. In alto, la soluzione SaaS protetta da Firewall in modo da controllare il flusso verso il Provider del servizio.

A destra si rappresenta il software ERP-BR, anch'esso in cloud, con relativo portale web a cui hanno accesso i clienti dell'organizzazione.

A sinistra vediamo l'intranet aziendale con la VLAN dei dipendenti e la VLAN dei servizi nella quale permane il server che ospita l'ERP-HQ ed il DB.

Soluzione SaaS in Cloud

Si è scelto di sostituire il middleware con **ADF (Azure Data Factory)** che è una soluzione SaaS, cioè un servizio offerto da Microsoft per l'estrazione, trasformazione e trasferimento dei dati basato su cloud Azure. Quindi, sostituisce il ruolo del modulo covert permettendo il **trasferimento dei dati da un sistema gestionale all'altro**.

In particolare, ADF permette di eseguire una serie di operazioni come unione, filtraggio, aggregazione e trasformazioni personalizzate, per preparare i dati per l'analisi o il caricamento in una destinazione senza problemi legati alla compatibilità delle singole fonti dati.

Questo servizio integra sistemi di monitoraggio e gestione dell'andamento dei flussi di lavoro che consentono di identificare eventuali anomalie e ottimizzarne immediatamente le prestazioni.

La soluzione scelta incontra le esigenze aziendali anche dal punto di vista del **no-code**. Infatti, la funzionalità Mapping Data Flows permette la trasformazione dei dati senza la necessità di scrivere codice, rendendo il processo accessibile anche a chi non ha competenze di programmazione avanzata.

Azure Data Factory fornisce, inoltre, diverse funzionalità di sicurezza, tra cui l'integrazione con Azure Active Directory per l'autenticazione e l'autorizzazione, la crittografia dei dati a riposo e in transito e il controllo degli accessi basato sui ruoli (RBAC) per gestire l'accesso ai dati e alle pipeline.

Essendo un servizio PaaS, la responsabilità del software intermediario e del relativo database è esclusivamente a carico del provider del servizio, Microsoft, liberando l'organizzazione della manutenzione di hardware e l'aggiornamento di OS e dalla gestione del software.

Note Finali

L'architettura di rete garantisce la separazione dei servizi interni da quelli degli utenti, limitando l'accesso e migliorando la sicurezza. La VPN (virtual private network) viene implementata per le

comunicazioni sicure tra ADF, ERP-HQ ed ERP-BR, mentre il portale web fornisce l'interfaccia per i clienti senza esporre direttamente l'infrastruttura interna. L'implementazione di firewall, IDS/IPS e aggiornamenti regolari aumenta la sicurezza complessiva del sistema. Per migliorare la continuità operativa, si dovrebbe considerare l'implementazione di soluzioni aggiuntive come backup regolari e disaster recovery.

Politiche di Accesso

- **Utenti Interni**: Accesso completo all'ERP-HQ, con accesso diretto a internet ma non all'ERP-BR
- **ERP-HQ**: Può collegarsi ad internet per aggiornamenti software, e non per comunicare con ERP-BR.
- **Middleware**: Unico punto di connessione tra ERP-HQ e ERP-BR tramite VPN
- **Clienti**: Accesso al portale web dell'ERP-BR per interagire con i servizi che offre l'azienda.

Prepare –Organization Level

Dopo aver creato l'architettura di partenza e quella da valutare, avviate la fase Prepare di RMF. Concentratevi solamente sui task in grassetto(basta inserire una descrizione non troppo estesa). Dove richiesto, riportate task a Simple Risk. Per differenziare le entità relative a opzione 1 e 2, utilizzate tag.

Task	Descrizione	Simple Risk
TASK P-2 Risk Management Strategy Establish a risk management strategy for the organization that includes a determination of risk tolerance.	Stabilire una strategia di gestione del rischio che guidi e informi le decisioni basate sul rischio, incluso come il rischio di sicurezza e privacy è inquadrato, valutato, affrontato e monitorato. Deve descrivere la tolleranza al rischio, metodologie di valutazione e risposta al rischio accettabili e approcci per il monitoraggio continuo. La strategia deve considerare la gestione del rischio della catena di approvvigionamento (SCRM). Inoltre, deve includere le decisioni e le considerazioni a livello strategico su come i leader senior e i dirigenti devono gestire i rischi di sicurezza e privacy (inclusi i rischi della catena di approvvigionamento)	Configurare i valori di rischio, matrici, formula, ecc.

Prepare –System Level

Task	Descrizione	Simple Risk
TASK P-8 Mission or Business Focus Identify the missions, business functions, and mission/business processes that the system is intended to support.	Coinvolgere gli stakeholder per comprendere a fondo missioni, funzioni e processi aziendali, specialmente dal punto di vista della sicurezza e privacy. Le missioni e le funzioni aziendali determinano la progettazione e lo sviluppo dei processi aziendali. La prioritizzazione di queste missioni e funzioni guida anche le decisioni sul rischio, comprese quelle relative all'architettura aziendale, e di sicurezza e privacy correlate.	
TASK P-9 System Stakeholders Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	Identificare gli stakeholder che sono interessati al sistema in tutte le sue fasi, inclusa la progettazione, lo sviluppo, l'implementazione e l'operatività, compresi tutti gli aspetti della supply chain. Assicurare il coinvolgimento e la comunicazione degli stakeholder durante tutte le fasi del ciclo di vita del sistema e durante la gestione del rischio per garantire che i requisiti di sicurezza e privacy siano soddisfatti, le preoccupazioni siano affrontate e i rischi siano gestiti in modo efficace.	
TASK P-10 Asset Identification Identify assets that require protection.	Identificare e proteggere gli asset critici per garantire la sicurezza e la continuità operativa di un sistema. Gli asset possono essere tangibili o intangibili e includono tutte le risorse di valore per il raggiungimento degli obiettivi aziendali (informazioni, processi, hardware e software).	Asset management*

	La scelta di protezione degli asset deve basarsi sulle preoccupazioni degli stakeholder e sui contesti operativi, inclusi missioni e funzioni aziendali e altri sistemi che interagiscono con il sistema.	
TASK P-11 Authorization Boundary Determine the authorization boundary of the system.	Definire chiaramente i confini di autorizzazione del sistema per garantire la responsabilità, la sicurezza e la gestione efficace del rischio, specialmente nell'interazione con fornitori esterni. Quindi, In caso di sistemi gestiti, mantenuti o operati parzialmente o interamente da fornitori esterni, stabilire accordi formali per garantire l'accountability e la categorizzazione della sicurezza, specialmente quando si collegano sistemi a diverso impatto.	
TASK P-12 Information Types Identify the types of information to be processed, stored, and transmitted by the system.	Identificare i tipi di informazioni necessari per supportare le missioni organizzative, le funzioni aziendali e i processi aziendali per determinare la categorizzazione della sicurezza. Il programma di Informazioni non Classificate Controllate (CUI) [NARA CUI] definisce i tipi di informazioni che richiedono protezione, in conformità con leggi, regolamenti o politiche a livello governativo.	Anche le informazioni sono asset.
TASK P-13 Information Life Cycle Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system.	Identificare e comprendere le fasi del ciclo di vita delle informazioni: creazione, elaborazione, diffusione, utilizzo, archiviazione e smaltimento. Utilizzare strumenti come mappe dei dati per valutare i rischi di sicurezza e privacy e applicare controlli mirati. Assicurarsi di definire i confini	

	di autorizzazione e considerare l'interazione del sistema con altri. Durante il testing e l'integrazione del software, optare per dati sintetici per ridurre i rischi senza compromettere l'efficacia dei test.	
TASK P-16 Enterprise Architecture Determine the placement of the system within the enterprise architecture.	Implementare l'architettura aziendale, pratica di gestione per massimizzare l'efficacia dei processi e delle risorse informative, garantendo la resilienza dei sistemi e l'ottimizzazione degli asset informativi e tecnologici attraverso la standardizzazione e la consolidazione. Esaminare dettagliatamente il posizionamento del sistema all'interno dell'architettura aziendale per valutare eventuali rischi rispetto ai requisiti di sicurezza e privacy dell'organizzazione. Il risultato è la configurazione di sistemi trasparenti e agevolmente proteggibili, e la possibilità di stabilire una diretta correlazione tra gli investimenti effettuati e i miglioramenti nelle prestazioni misurabili.	

* Anche se i sistemi da gestire in SimpleRisk sono due (opzione 1 e 2), questi condividono molte componenti e i medesimi rischi (es. ERP-HQ e ERP-BR non variano). Inserite l'asset (o il rischio per l'esercizio di domani) una sola volta e utilizzate i tag per organizzarvi sull'applicazione (es. Opzione 1, Opzione 2, Entrambi).