

S4 - L1

Gestione del rischio informatico per un caso aziendale specifico - Prepare

17 maggio 2024

Team

- Davide Di Turo
- Lisa Bonato
- Manuel Di Gangi
- Maria Flavia Minotti
- Oliviero Camarota

INDICE

Traccia - Giorno 1 - Prepare	3
1.1 - Progetto guidato settimanale	3
1.2 - Caso aziendale	3
1.3 - Specifiche middleware	4
1.4 - Scenario attuale	5
1.5 - Creazione dell'architettura di partenza (opzione 1)	6
1.6 - Creazione dell'architettura alternativa (opzione 2)	7
2. Infrastruttura di rete proposta	8
3. Prepare – Organization Level	9
4. Prepare – System Level	10
5. Inserimento Asset in SimpleRisk	12
6. Architettura di rete	15
6.1 - Analisi dell'architettura	15
6.2 - Note Finali	16
6.3 - Politiche di Accesso	17
Traccia - Giorno 2 - Prepare e Categorize	17
7. Categorize	18
7.1 Identificazione dei rischi	18
7.1.1 Attacchi informatici	18
7.1.2 Attacchi di social engineering & HUMINT	20
7.1.3 Disastri ed eventi naturali naturali	21
7.1.4 Altri tipi di minacce	21
7.2 Valutazione dei rischi con metodo DREAD	22
7.3 Inserimento dei rischi in simple risk	23
Data breach	23
Attacco DDos	24
Traccia - Giorno 3 - Select and Implement	25
8. Select	25
9. Implement	28

Traccia - Giorno 1 - Prepare

1.1 - 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
- Assess
- 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.

1.2 - 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 resa necessaria perché sono ERP di fornitori diversi e non esiste un'integrazione nativa. L'organizzazione non valuta di sostituire gli ERP.



1.3 - Specifiche middleware

L'organizzazione conosce il funzionamento di alto livello del middleware. All'interno del middleware 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

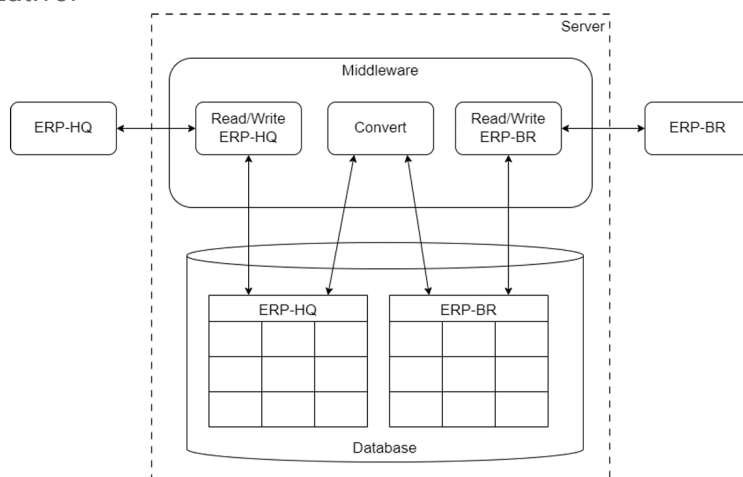
250 transazioni all'ora (tx/h) (complessive da/verso ERP-HQ/ERP-BR), l'attuale traffico si aggira sulle 100 tx/h.

1.4 - 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:

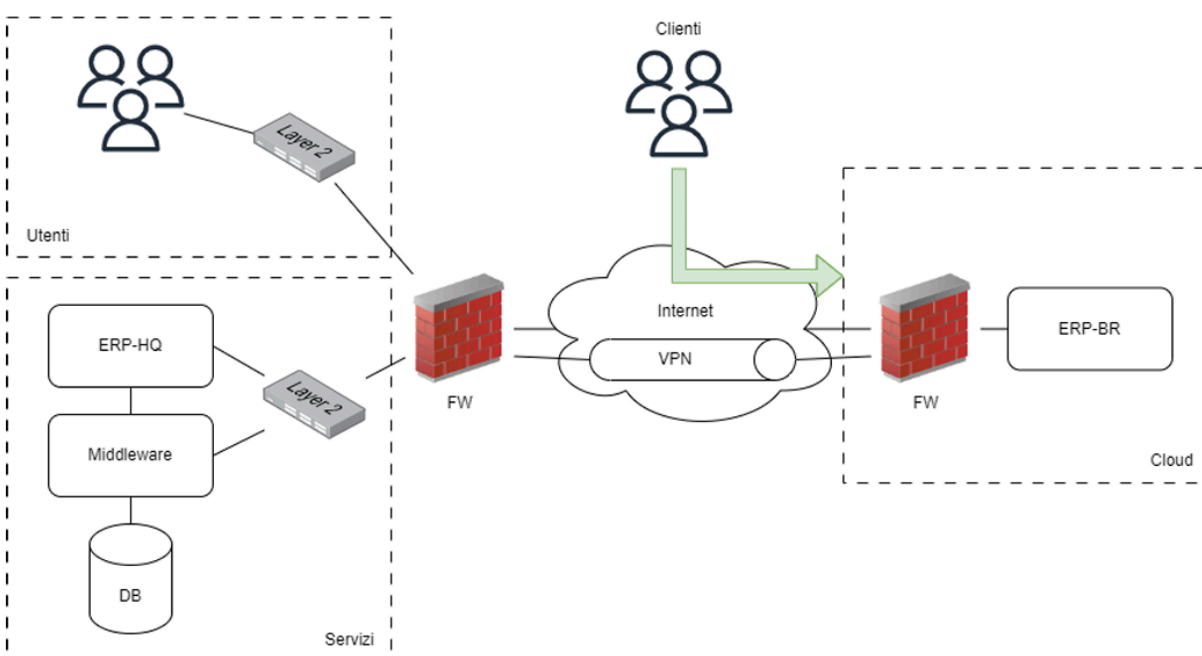
1. continuare a mantenere questo middleware on-premises, di cui non conosce molto, trovando un nuovo fornitore in grado di fare un'analisi approfondita (compreso reverse engineering) per poterne continuare lo sviluppo, oppure,
2. sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, 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.



1.5 - 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.



1.6 - Creazione dell'architettura alternativa (opzione 2)

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

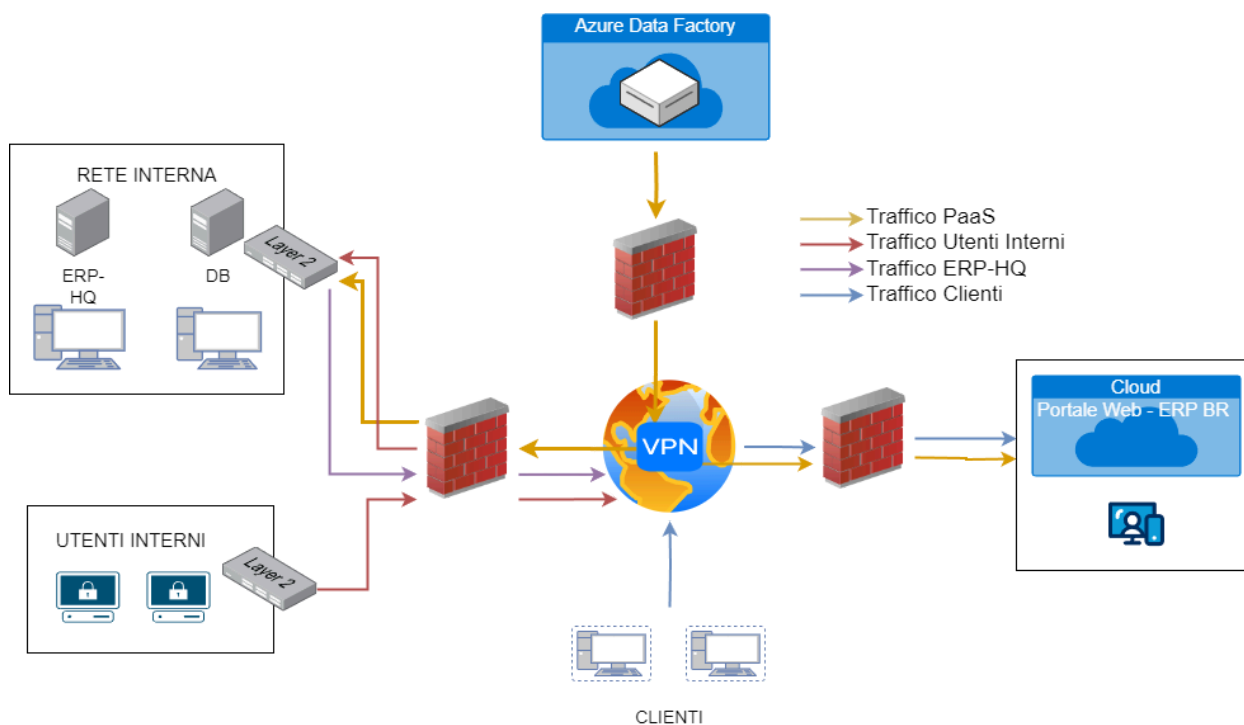
2. sostituire il middleware con una soluzione SaaS/iPaaS di data integration/automation, possibilmente low-code/nocode per evitare l'affidamento ad un'altra software house e gestire il solo mapping delle strutture dati con le risorse interne (dipendenti).

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/>

2. Infrastruttura di rete proposta



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 PaaS basata su cloud.

E' stata mantenuta la VPN per consentire il collegamento tra le varie della rete aziendale. In alto, la soluzione PaaS 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.

3. 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.	<p>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.</p> <p>L'azienda ha stabilito un livello di tolleranza del rischio medio-bassa, con l'obiettivo di minimizzare i rischi di sicurezza delle informazioni e garantire la business continuity. La strategia deve considerare la gestione del rischio della catena di approvvigionamento (SCRM).</p> <p>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)</p>	<p>Configurare i valori di rischio, matrici, formula, ecc.</p> <p>TAG: Opzione 1 e 2.</p>
TASK P-4 Organizationally-Tailored Control Baselines and Cybersecurity Framework Profiles (Optional) Establish, document, and publish organizationally-tailored control baselines and/or Cybersecurity Framework Profiles.	<p>L'organizzazione prevede l'uso del NIST SP 800-53 per selezionare e personalizzare i controlli di sicurezza rilevanti e del NIST CSF per sviluppare profili di cybersecurity adattati alle esigenze dell'organizzazione.</p> <p>Le attività principali includono: Identificare e adattare i controlli di sicurezza del NIST SP 800-53 in base alle esigenze specifiche dell'organizzazione. Sviluppare profili del NIST CSF per definire i livelli di implementazione dei controlli in base alla valutazione del rischio e ai requisiti operativi.</p> <p>Documentare dettagliatamente i baseline di controllo e i profili di cybersecurity, rendendoli accessibili agli stakeholder rilevanti. .</p>	<p>Definire i framework che si intendono utilizzare (tra quelli visti nel corso), Governance/1/Framework orks.</p>

	Stabilire un processo di revisione periodica per aggiornare e migliorare continuamente i controlli e i profili in risposta ai cambiamenti nelle minacce, nei requisiti normativi e nelle operazioni aziendali.	
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

4. 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.	<p>L'opzione 2 selezionata è progettata per supportare la funzione prioritaria di integrazione e sincronizzazione dei dati dei due ERP, in modo da ottenere una gestione integrata di ordini, vendite, inventario e fatturazione.</p> <p>Per comprendere efficacemente questa funzione aziendale è essenziale coinvolgere gli stakeholder (Identificazione al task P-9) in modo da guidare anche le decisioni sul rischio, comprese quelle relative all'architettura aziendale, e di sicurezza e privacy correlate.</p>	TAG: 2
TASK P-9 System Stakeholders Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system.	<p>Gli stakeholder coinvolti sono:</p> <ul style="list-style-type: none"> - Il team di sviluppo responsabile della configurazione del servizio iPaaS - Azure data factory - Il fornitore del servizio IPaaS - Azure data factory - Il team tecnico responsabile della gestione / manutenzione del sistema - Gli utenti interni - Il team di Security - I clienti 	TAG: 2
TASK P-10 Asset Identification Identify assets that require protection.	<ul style="list-style-type: none"> - PaaS - Azure Data Factory - Portale web - Configurazione e mappatura dei dati sul nuovo servizio PaaS - Infrastruttura di rete aziendale (Compresi Firewall perimetrali) 	<p>Asset management*</p> <p>TAG: 2</p>

	<ul style="list-style-type: none"> - Dati utenti - ERP -HQ - ERP -BR - Personale - Immagine aziendale 	
TASK P-11 Authorization Boundary Determine the authorization boundary of the system.	Responsabilità dell'utente: Sicurezza delle applicazioni. Gestione dei dati e protezione delle informazioni sensibili. Configurazione della sicurezza delle applicazioni. Controllo degli accessi e gestione delle identità.	Tag: 2
TASK P-12 Information Types Identify the types of information to be processed, stored, and transmitted by the system.	<p>Le informazioni maneggiate dall'organizzazione riguardano:</p> <ul style="list-style-type: none"> - Dati di inventario (prodotti, quantità, prezzi) - Dati di ordine (dettagli dell'ordine, informazioni di spedizione, informazioni di pagamento) - Dati di fatturazione (fatture, pagamenti, sconti) - Dati personali dei clienti (nome, indirizzo, informazioni di contatto). 	<p>Anche le informazioni sono asset.</p> <p>TAG: 2</p>
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.	<p>Creazione: I dati vengono creati in uno dei due ERP</p> <p>Elaborazione: I dati vengono elaborati e trasformati dal servizio PaaS per essere sincronizzati</p> <p>Memorizzazione: I dati vengono memorizzati nel servizio PaaS durante il processo di sincronizzazione</p> <p>Trasmissione: I dati vengono trasmessi tra ERP-HQ, PaaS e ERP-BR attraverso la VPN dedicata</p> <p>Archiviazione: I dati vengono archiviati nei database del PaaS</p> <p>Eliminazione: I dati vengono eliminati dai database solo su richiesta specifica</p>	TAG: 2
TASK P-14 Risk Assessment—System Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis.	Valutazione del rischio in caso di attacco DDos e Data breach	Risk Management/1
TASK P-16 Enterprise Architecture Determine the placement of the system within the enterprise architecture.	Architettura riportata al punto 2. <i>Architettura di rete proposta</i> , analizzata al punto 6. <i>Architettura di rete</i>	TAG: 2

* 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).

5. Inserimento Asset in SimpleRisk

The screenshot shows the SimpleRisk application interface. The top navigation bar includes: Governance, Risk Management, Compliance, Asset Management, Assessments, Reporting, and **Configure**. The left sidebar contains the following menu items: Settings, Content, Risk and Threat Catalog, Configure Risk Formula, Configure Review Settings, **Add and Remove Values** (highlighted with a red arrow), and Role Management. The main content area is titled 'Select: Site/Location'. Under the 'Site/Location:' section, there are three input fields: 'Add new item named:' with the value 'On-premise' and an 'Add' button; 'Change' with a dropdown menu showing '--' and an 'Update' button; and 'Delete item named:' with a dropdown menu showing '--' and a 'Delete' button.

This screenshot is similar to the one above, showing the SimpleRisk 'Configure' page. The top navigation bar and left sidebar are identical. The main content area is titled 'Select: Site/Location'. Under the 'Site/Location:' section, the 'Add new item named:' field now contains the value 'Cloud' and the 'Add' button is visible. The 'Change' and 'Delete item named:' fields remain the same as in the previous screenshot.

Per lo svolgimento del processo di gestione del rischio si utilizzerà SimpleRisk, una piattaforma integrata per la gestione della governance, del rischio e della conformità (GRC).

Il primo passo del processo è l'inserimento degli asset sulla base dei quali si procederà ad identificare e analizzare il rischio. Su "**Configure**", "**Add and Remove Values**" selezioniamo **Site/Location** per inserire (**Add**) il luogo, fisico o immateriale, in cui si trovano gli asset: On-premise e Cloud.

Add a New Asset

Asset Name: ADF - Azure Data Factory

IP Address:

Asset Valuation: \$0 to \$100,000

Site/Location: Cloud

Team: Collaboration

Associated Risks: None selected

Asset Details:

Soluzione iPaaS/SaaS che mette a disposizione servizio **Mapping Data Flows** per pianificare e gestire i flussi di lavoro di integrazione e trasformazione dei dati senza necessità di scrivere codice (**no-code**). Quindi, l'organizzazione ha il controllo completo sul mapping delle strutture dati e sulla configurazione delle attività di integrazione e i suoi dipendenti sono in grado di definire e gestire autonomamente il mapping dei dati senza fare affidamento su terze parti o sviluppatori esterni.

Current Maturity	Control	Actions

Tags: Opzione 2

Add

The maximum length of a tag is 255 characters.

Si procede poi all'inserimento degli Asset principali spostandosi nel tab **"Asset Management"** e **"Manage Assets"**.

Per ciascuno degli Asset, come si può vedere nell'esempio della figura sopra relativo all'**inserimento dell' ADF**, si sono inseriti, in ordine, il valore, il luogo, il team responsabile e i dettagli, nel quale si rinviene descrizione esplicativa degli stessi.







In "tag" si è inserito per tutti gli asset "opzione 2", visto che è quella in analisi.







Per finalizzare l'inserimento, ancora una volta si seleziona **"Add"**.

A questo punto sarà possibile visionare l'**elenco degli asset inseriti - ADF, Configurazione e mappatura dati sul PaaS, ERP-BR, ERP-HQ, Immagine aziendale, Network, Personale, Portale Web** - nella parte inferiore della schermata dell' "Asset Management".

Verified Assets

Delete All

Actions	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
 	ADF - Azure Data Factory		\$0 to \$100,000	Cloud	Collaboration	Soluzione iPaaS/SaaS che mette a disposizione servizio Mapping Data Flows per pianificare e gestire i flussi di lavoro di integrazione e trasformazione dei dati senza necessità di scrivere codice (no-code). Quindi, l'organizzazione ha il controllo completo sul mapping delle strutture dati e sulla configurazione delle attività di integrazione e i suoi dipendenti sono in grado di definire e gestire autonomamente il mapping dei dati senza fare affidamento su terze parti o sviluppatori esterni.	Opzione 2
 	Configurazione e mappatura dei dati sul PaaS		\$0 to \$100,000	Cloud	Data Center & Storage, Database, Information Security		Opzione 2
 	Dati degli utenti		\$400,001 to \$500,000	All Sites	Data Center & Storage, Database, Information Security	L'azienda gestisce informazioni sensibili degli utenti tra cui dati finanziari. Queste informazioni sono processate e archiviate sia su ERP-HQ che ERP-BR e sulla soluzione PaaS.	Opzione 2

 	ERP-BR		\$100,001 to \$200,000	Cloud	IT Systems Management	TIER 2: Gestionale delle filiali. Separato rispetto al ERP-HQ, è più snello, flessibile e permette di avere una certa autonomia nella gestione delle operazioni, tenendo conto dei processi localizzati. Costo: 120.000. Di solito un Tier 2 non è in grado di vedere altri Tier 2.	Opzione 1 Opzione 2
 	ERP-HQ		\$400,001 to \$500,000	On-premise	IT Systems Management	TIER 1: Gestionale della sede principale dell'organizzazione: centralizzato, robusto, in grado di gestire operazioni e requisiti generali dell'organizzazione. Costo: 450.000.	Opzione 1 Opzione 2
 	Immagine aziendale		\$900,001 to \$1,000,000			Per immagine aziendale si fa riferimento ad una categoria di asset intangibili - fiducia nell'organizzazione di clienti e stakeholders e, a cascata, la reputazione e il brand della stessa - che riveste un'importanza fondamentale poiché, se intaccata, genera costi ingenti per eventuali richieste di risarcimento, sanzioni, perdite di investimenti e profitti.	Opzione 2

	Network		\$400,001 to \$500,000	On-premise	Database, Information Security, IT Systems Management, Network	Si tratta dell'infrastruttura aziendale comprese le misure di sicurezza e dispositivi di rete.	Opzione 2
	Personale		\$900,001 to \$1,000,000	On-premise		L'organizzazione ha una sede centrale e molte filiali. Di conseguenza si ipotizza che il costo del personale sia ingente.	Opzione 2
	Portale Web		\$400,001 to \$500,000	Cloud	Collaboration	Il portale Web dell'ERP-BR è appaltato e gestito dal provider al quale si affida la nostra organizzazione.	Opzione 2

In seguito, per facilitare lo svolgimento del risk Assessment si è deciso di raggruppare gli asset individuati in 4 gruppi di Assets:

- **On-premise:** Network e ERP-HQ
- **Cloud BR e APP:** ERP-BR e Portale web
- **Cloud AZURE:** ADF e configurazione e mappatura dei dati sul PaaS
- **Beni intangibili:** immagine aziendale e personale

1 Automated Discovery
2 Manage Assets
3 **Manage Asset Groups**

+

Asset Groups (4)

Name
Beni intangibili
Cloud AZURE
Cloud BR e APP
On-premise

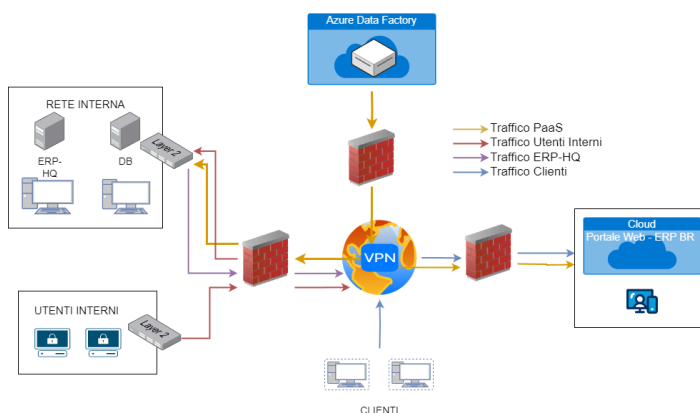
10
Page 1 of 1

6. Architettura di rete

6.1 - Analisi dell'architettura

Soluzione PaaS in Cloud

Si è scelto di sostituire il middleware con **ADF (Azure Data Factory)** che è una soluzione iPaaS, che offre un servizio per l'estrazione, caricamento, 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.

Inoltre, Azure Data Factory offre funzionalità di automazione avanzate che consentono all'azienda di pianificare e eseguire automaticamente i flussi di lavoro di integrazione dei dati in base a trigger temporali o eventi specifici. Ciò consente all'azienda di automatizzare i processi di integrazione dei dati, riducendo il carico di lavoro manuale e aumentando l'efficienza operativa. In aggiunta, sono integrati anche 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. Utilizzando gli strumenti drag-and-drop di ADF, i dipendenti

dell'organizzazione possono definire facilmente i mapping dei dati, associando i campi di dati tra le fonti dati e le destinazioni senza la necessità di scrivere codice SQL o script.

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 dalla manutenzione di hardware e l'aggiornamento di OS e dalla gestione del software.

In conclusione, tramite ADF, l'organizzazione ha il controllo completo sul mapping delle strutture dati e sulla configurazione delle attività di integrazione, e i suoi dipendenti sono in grado di definire e gestire autonomamente i mapping dei dati senza fare affidamento su terze parti o sviluppatori esterni, grazie alla natura no-code di ADF.

6.2 - 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.

6.3 - 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.

Traccia - Giorno 2 - Prepare e Categorize

Prepare

Dopo aver completato il task dell'esercizio di ieri, oggi continueremo il progetto ultimando la fase Prepare e proseguendo con Categorize. Definire Quali Framework l'organizzazione intende fare ed effettuare un risk assessment solamente a livello Systema (l'estensione livello organizzativo è un'estensione, TASK P-3):

- Identificare Il rischio, rispetto agli asset identificati ieri.
- Valutare il rischio, potete usare qualsiasi metodo.

Non inserite tutti i rischi con la stessa data ma scegliere un arco temporale, così da ottenere dei grafici in cui si possa vedere una variazione nel tempo.

Domani effettueremo il trattamento.

Nota: il risk assessment è ciclico, non è richiesta l'identificazione di tutti i rischi nella prima iterazione.

**** I punti P-4 e P-14 richiesti dalla traccia sono stati integrati nelle tabelle precedenti ****

Categorize

Produrre un piccolo documento che descrive due architetture (raccolgete il materiale prodotto ieri), utilizzare Simple Risk per la conservazione documentale tracciata (TASK C-1).

7. Categorize

Task	Descrizione	Simple Risk
TASK C-1 System Description Document the characteristics of the system.	Implementazione di Azure Data Factory (ADF) per l'integrazione dei dati tra ERP-HQ e ERP-BR. ADF è utilizzato per sincronizzare i dati operativi e finanziari tra i due sistemi ERP, migliorando l'efficienza e garantendo la sicurezza dei dati in transito e a riposo.	Caricare in Governance/2 (SimpleRisk non supporta report di questa categoria, per ovviare potete utilizzare il tipo «Guidelines»)

Framework

Di seguito si vede l'inserimento in SimpleRisk dei framework che l'azienda intende utilizzare nello svolgimento del risk assessment.

Framework Name	Framework Description
NIST 800-53 Rev.5	"Security and Privacy Controls for Information Systems and Organizations," framework per l'integrazione dei controlli di sicurezza e privacy.
NIST CSF	Cybersecurity Framework per la mitigazione dei rischi di sicurezza informatica organizzativa.

7.1 Identificazione dei rischi

7.1.1 Attacchi informatici:

Questa è una minaccia chiave per TechnoCorp, data la natura del settore in cui opera. Gli attacchi informatici possono provenire da attaccanti esterni, come hacker o gruppi criminali, che potrebbero mirare a violare i dati sensibili dell'azienda o interrompere le operazioni aziendali.

1. **Malware e ransomware:** Gli attacchi malware, compresi quelli che impiegano ransomware, sono una minaccia costante per TechnoCorp. Tali attacchi possono

causare la perdita di dati, la compromissione dei sistemi aziendali e il blocco delle operazioni aziendali fino al pagamento del riscatto.

2. **Exploit di vulnerabilità del software:** Le vulnerabilità del software nei server interni, nei servizi cloud utilizzati e nel sito web aziendale ospitato esternamente potrebbero essere sfruttate dagli attaccanti per ottenere accesso non autorizzato ai sistemi o per compromettere i dati aziendali.
3. **Violazioni della sicurezza dei dati:** La perdita o la compromissione dei dati sensibili dell'azienda o dei suoi clienti rappresenta una minaccia significativa. Le violazioni della sicurezza dei dati possono causare danni alla reputazione dell'azienda, sanzioni legali e perdite finanziarie.
4. **Accesso non autorizzato:** Gli attaccanti potrebbero cercare di ottenere accesso non autorizzato ai sistemi aziendali attraverso vulnerabilità della rete, credenziali rubate o altri mezzi. Questo potrebbe consentire loro di rubare dati sensibili, interrompere le operazioni aziendali o causare danni alla reputazione dell'azienda. Un caso specifico è lo **Spoofing**, una tecnica in un cui un individuo o un programma falsifica l'identità di un'altra persona, sistema informatico o risorsa, al fine di ingannare gli utenti o ottenere accesso non autorizzato.
5. **Attacchi DDoS:** Gli attacchi distribuiti di denial of service (DDoS) possono interrompere le operazioni aziendali, rendendo inaccessibili i servizi aziendali online o le risorse critiche. Questi attacchi possono essere condotti da attaccanti esterni con l'obiettivo di danneggiare l'azienda o estorcere denaro.
6. **Data Breach:** Un data breach è un attacco informatico che compromette la sicurezza dei dati aziendali, consentendo agli aggressori di accedere a informazioni sensibili o riservate. Tale intrusione può comportare la diffusione non autorizzata di dati personali o aziendali, mettendo a rischio la privacy degli utenti o delle organizzazioni coinvolte.
7. **USB Drop Attacks:** Gli attaccanti lasciano dispositivi USB infetti con malware in luoghi pubblici o all'interno dell'azienda stessa, contando sulla curiosità delle persone per inserire i dispositivi nei propri computer, consentendo così l'infezione.

7.1.2 Attacchi di social engineering & HUMINT:

1. **Phishing:** Gli attacchi di phishing rappresentano una minaccia significativa, in particolare per i dipendenti, gli attaccanti potrebbero cercare di ottenere accesso non autorizzato alle credenziali aziendali o di distribuire malware attraverso e-mail di phishing mirate. Nel caso specifico dello **Spear Phishing** gli attaccanti mirano a persone o organizzazioni specifiche, utilizzando informazioni precedentemente raccolte per rendere gli attacchi più convincenti e credibili.
2. **Vishing:** Gli attaccanti utilizzano telefonate ingannevoli verso gli uffici aziendali per convincere i dipendenti a condividere informazioni riservate, effettuare pagamenti non autorizzati o scaricare malware sui loro dispositivi.
3. **Infiltrazione fisica:** Gli attaccanti si fingono appartenenti al personale di manutenzione, consegna o altro personale esterno per ottenere accesso fisico non autorizzato a strutture o sistemi aziendali sensibili.
4. **Tailgating:** Gli attaccanti seguono un dipendente autorizzato attraverso l'accesso fisico controllato, come una porta con badge, sfruttando la cortesia o la mancanza di attenzione per guadagnare accesso non autorizzato alle strutture o ai sistemi aziendali.
5. **Smishing:** Gli attaccanti inviano messaggi di testo fraudolenti o ingannevoli alle vittime con lo scopo di ottenere dati sensibili, o indurre l'utente a compiere azioni dannose, come il download di contenuti o l'apertura di siti malevoli.
6. **Deepfake:** Gli attaccanti utilizzano (manipolazione di video, falsificazione di discorsi, truffe on-line, attacchi di phishing avanzati, falsificazione di prove) per creare video o registrazioni manipolate artificialmente in modo che sembri che una persona stia facendo qualcosa che in realtà non ha fatto.

7.1.3 Disastri ed eventi naturali naturali:

1. **Eventi meteorologici estremi:** Tempeste, uragani, alluvioni, terremoti e altre calamità naturali possono danneggiare fisicamente gli edifici, gli impianti e le infrastrutture dell'azienda IT. Questo potrebbe causare interruzioni dei servizi, perdita di dati e danni ai sistemi critici.

2. **Incendi:** Gli incendi possono distruggere attrezzature, server e infrastrutture di rete, causando interruzioni dei servizi e perdita di dati. La presenza di apparecchiature elettriche e dispositivi informatici all'interno di un'azienda IT aumenta il rischio di incendi, che possono essere causati da cortocircuiti, surriscaldamento o guasti hardware.
3. **Blackout e interruzioni dell'alimentazione elettrica:** Interruzioni di corrente a lungo termine o blackout possono influenzare gravemente le operazioni di un'azienda IT, causando la perdita di dati non salvati, l'interruzione dei servizi e danni alle apparecchiature elettriche sensibili.

7.1.4 Altri tipi di minacce:

1. **Minacce esterne:** Se un dispositivo personale viene compromesso durante l'utilizzo personale, potrebbe consentire a un attaccante di ottenere accesso non autorizzato alle risorse aziendali.
2. **Perdita fisica dei dispositivi:** La perdita o il furto di laptop, workstation o altri dispositivi aziendali potrebbe compromettere la sicurezza dei dati aziendali se i dispositivi contengono informazioni sensibili e non sono adeguatamente protetti con misure di sicurezza come la crittografia dei dati.

7.2 Valutazione dei rischi con metodo DREAD

Nelle immagini seguenti sono stati analizzati due rischi che potrebbero impattare sull'organizzazione: Il data breach, l'esfiltrazione di dati a causa di attacco esterno, e l'attacco di DDos che causa interruzione dei servizi.

Per l'inserimento nel tab "Risk management" e poi in "Submit risk" si è proceduto ad identificare i due rischi inserendo quanto richiesto in Subject, risk mapping, Threat mapping, Category, Site/Location, Control Regulation, Asset affetti, dove possibile tecnologie e team responsabile, e identificazione della fonte della minaccia (in entrambi i casi esterna).

Poi si è scelto il “Risk Scoring Method” in DREAD che è il metodo in base al quale si è valutato il **livello dei due rischi prima dell'implementazione dei controlli**:

- **5.8: livello medio** - rischio di Data breach
- **7.4: livello alto** - rischio di DDoS

DREAD è un acronimo che rappresenta cinque fattori per valutare il rischio di una minaccia:

Damage: Danno potenziale causato dalla minaccia.

Reproducibility: Facilità con cui la minaccia può essere riprodotta.

Exploitability: Facilità con cui la minaccia può essere sfruttata.

Affected users: Numero di utenti potenzialmente colpiti.

Discoverability: Facilità con cui la minaccia può essere scoperta.

7.3 Inserimento dei rischi in simple risk

7.3.1 Data breach

Risk Scoring with DREAD Calculator

DREAD Score	Categories
Damage Potential	8
Reproducibility	4
Exploitability	5
Affected Users	7
Discoverability	5
Overall DREAD Score	5.8

Submit

Help Desk

1 Submit Risk

2 Plan Mitigation

3 Perform Reviews

4 Plan Projects

5 Review Regularly

Inherent Risk: 5.8 Medium

Residual Risk: 5.8 Medium

ID #: 1001

Status: New

Subject: Data Breach

View Risk Scoring Details

Show Risk Score Over Time

Details Mitigation Review

Risk Mapping: Unauthorized access

Threat Mapping: Hacking & Other Cybersecurity Crimes

Submission Date: 05/20/2024

Category: Access Management

Site/Location: All Sites

External Reference ID:

Control Regulation: NIST 800-53 Rev.5

Control Number:

Affected Assets: ADF - Azure Data Factory, Dati degli utenti, ERP-BR, ERP-HQ, Immagine aziendale, Network, Portale Web

Technology: Backups, Datacenter, Network, Remote Access, Web

Team: Database, Information Security, IT Systems Management, Network

Additional Stakeholders:

Owner:

Owner's Manager:

Submitted By: Maria Flavia Minotti

Risk Source: External

Risk Scoring Method: DREAD

Risk Assessment:

Additional Notes:

Supporting Documentation: None

7.3.2 Attacco DDos

Risk Scoring with DREAD Calculator

SimpleRisk DREAD Calculator — Mozilla Firefox

https://192.168.1.67/management/dread_rating.php

scores. DREAD is a classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat. The DREAD acronym is formed from the first letter of each category below. DREAD modeling influences the thinking behind setting the risk rating, and is also used directly to sort the risks. The DREAD algorithm, shown below, is used to compute a risk value, which is an average of all five categories.

DREAD Score		Categories	
Damage Potential	7	Damage Potential	7
Reproducibility	5	Reproducibility	5
Exploitability	6	Exploitability	6
Affected Users	9	Affected Users	9
Discoverability	10	Discoverability	10
Overall DREAD Score	7.4	Submit	

[Help Desk](#)

1 Submit Risk
2 **Plan Mitigation**
3 Perform Reviews
4 Plan Projects
5 Review Regularly

Inherent Risk
7.4
High

Residual Risk
7.4
High

ID #: 1002
Status: New
Subject: Attacco DDos

View Risk Scoring Details
Show Risk Score Over Time

Details Mitigation Review

Risk Mapping: Business interruption
Threat Mapping: Hacking & Other Cybersecurity Crimes
Submission Date: 05/20/2023
Category: Environmental Resilience
Site/Location: All Sites
External Reference ID:
Control Regulation: NIST 800-53 Rev.5
Control Number:
Affected Assets: ADF - Azure Data Factory ERP-BR
ERP-HQ Network Portale Web
Technology:
Team: IT Systems Management
Additional Stakeholders:
Owner:
Owner's Manager:

Submitted By: Maria Flavia Minotti
Risk Source: External
Risk Scoring Method: DREAD
Risk Assessment:
Additional Notes:
Supporting Documentation: None

Traccia - Giorno 3 - Select and Implement

8. Select

Nella fase Select, selezionerete quali controlli utilizzare per i vostri due sistemi, se necessario potete adattare i controlli al vostro scenario (TASK S-2). Poi, allocate i vari controlli sulle componenti del sistema, facendo ad esempio una tabella Excel di mapping controllo/asset, (TASK S-3) e documentate le decisioni prese (TASK S-4). Inserite nel documento anche la strategia che utilizzerete per monitorare l'efficacia dei controlli (TASK S-5). Nella selezione dei controlli includete una stima del costo del controllo. Ricordate che non dovete per forza selezionare dei controlli, potete utilizzare altre tipologie di trattamento (es. accettazione).

Task	Descrizione	Simple Risk
TASK S-1 Control Selection Select the controls for the system and the environment of operation.	Controlli NIST SP 800-53 Rev. 5 <ul style="list-style-type: none"> - SC-7 Boundary Protection: Implementazione di misure di sicurezza per proteggere i confini della rete da accessi non autorizzati o compromessi, attraverso l'uso di firewall e altre tecnologie di protezione. Mitigation ratio: 35% - SC-5 Denial of Service Protection: Implementazione di contromisure per proteggere i servizi, le risorse e i sistemi informativi dagli attacchi di denial of service (DoS) e distributed denial of service (DDoS), inclusa l'adozione di tecnologie e politiche per rilevare, mitigare e rispondere tempestivamente agli attacchi al fine di garantire la disponibilità continua dei servizi e delle risorse digitali. Mitigation ratio: 32% - AC-2 Account Management: Sistema per l'identificazione ed il controllo degli accessi Mitigation ratio: 28% 	

	<ul style="list-style-type: none"> - RA-3 Risk Assessment: valutazione periodica dei controlli di sicurezza per identificare e mitigare le vulnerabilità, comprese quelle relative alla privacy, come specificato dal PL-4. Mitigation ratio: <i>variabile</i> - SC-13 Use of Cryptography: L'organizzazione implementa la protezione fornita dalla crittografia in conformità alle leggi federali, ordini esecutivi, direttive, politiche normative, standard e linee guida pertinenti. Mitigation ratio: 45% - SC-28: Protection of information at rest: Implementazione corretta e sicura della crittografia per proteggere le informazioni sensibili e le comunicazioni da accessi non autorizzati o compromessi. Mitigation ratio: 49% 	
TASK S-2 Control Tailoring Tailor the controls selected for the system and the environment of operation.	<p>Adattamento dei controlli di sicurezza e privacy al contesto aziendale.</p> <p>Data Breach:</p> <ul style="list-style-type: none"> - C1 - Firewall e Filtraggio del Traffico: Configurare un firewall robusto per proteggere l'intera rete aziendale. Impostare regole di filtraggio del traffico per limitare l'accesso non autorizzato sia dall'interno che dall'esterno della LAN aziendale. Costo stimato per hardware e licenze software: €15.000 - C2 - Crittografia dei Dati: Crittografare i dati sensibili sia durante il trasferimento attraverso la rete che durante il salvataggio nei sistemi di archiviazione. Questo include i dati memorizzati nel DB, nell'ERP-HQ e nel PaaS, nonché quelli trasmessi attraverso la VPN e il portale web. Costo stimato per hardware e licenze software: €10.000 - C3 - Accesso Basato sui Ruoli: Implementare un sistema di gestione degli accessi basato sui ruoli per garantire che solo i dipendenti autorizzati possano accedere ai dati sensibili Costo stimato per licenze software ed implementazione: €7.000 	

	<p>DDoS:</p> <ul style="list-style-type: none"> - C4 - Sistema di Rilevamento e Mitigazione DDoS: Implementare un sistema di rilevamento e mitigazione DDoS dedicato che possa monitorare costantemente il traffico di rete in entrata e uscita. Questo sistema dovrebbe essere in grado di riconoscere rapidamente i pattern di traffico anomali associati agli attacchi DDoS e attivare automaticamente misure di mitigazione per proteggere i servizi online dell'azienda. Costo stimato per hardware e licenze software: €15.000 - C5 - Limitazione del Traffico Sospetto: Impostare limiti sul numero di richieste o connessioni che possono essere fatte da singoli indirizzi IP o range di indirizzi IP. Questo può aiutare a mitigare gli effetti di un attacco DDoS distribuendo il carico e limitando l'impatto del traffico dannoso. Costo stimato per l'implementazione: €3.000 <p>Valutazione dei rischi:</p> <ul style="list-style-type: none"> - C6 - Valutazione dei rischi: Effettuare periodicamente la valutazione dei rischi e dei controlli con cadenza annuale (minima) Costo stimato se effettuato da personale interno: €7.000 Costo stimato se effettuato da terzi: €18.000 	
TASK S-3 Control Allocation Allocate security and privacy controls to the system and to the environment of operation.	<p>Rete Interna:</p> <ul style="list-style-type: none"> - Firewall e Filtraggio del Traffico (C1) - Crittografia dei Dati (C2) - Sistema di Rilevamento e Mitigazione DDoS (C4) - Limitazione del Traffico Sospetto (C5) - Accesso basato su ruoli (C3) <p>ADF:</p> <ul style="list-style-type: none"> - Crittografia dei Dati (C2) - Ulteriori misure di sicurezza sono rimandate al gestore del servizio (Shared responsibility model) - Accesso basato su ruoli (C3) <p>Cloud Web:</p> <ul style="list-style-type: none"> - Crittografia dei Dati (C2) - Ulteriori misure di sicurezza sono rimandate al gestore del servizio (Shared responsibility model) - Accesso basato su ruoli (C3) 	

<p>TASK S-4 Documentation of Planned Control Implementations Document the controls for the system and environment of operation in security and privacy plans.</p>	<p>Firewall e Filtraggio del Traffico: L'implementazione di firewall e filtraggio del traffico è essenziale per proteggere i confini della rete da accessi non autorizzati o compromessi. Queste misure di sicurezza permettono di controllare e monitorare il flusso di dati in entrata e in uscita, consentendo solo il passaggio del traffico autorizzato secondo le policy di sicurezza stabilite. Ciò aiuta a ridurre il rischio di intrusioni e violazioni della sicurezza, contribuendo a mantenere un ambiente operativo sicuro e protetto.</p> <p>Crittografia dei Dati: L'implementazione della crittografia dei dati è cruciale per garantire l'integrità e la confidenzialità delle informazioni sensibili. La crittografia protegge i dati tramite l'applicazione di algoritmi che rendono le informazioni incomprensibili a chi non possiede la chiave di decrittazione corretta. Questo significa che anche se i dati dovessero essere intercettati durante la trasmissione o l'archiviazione, rimarrebbero inutilizzabili per chiunque non sia autorizzato a accedervi.</p> <p>Accesso Basato sui Ruoli: L'adozione di un sistema di accesso basato sui ruoli è fondamentale per garantire che gli utenti possano accedere solo alle risorse e alle funzionalità del sistema necessarie per svolgere le proprie responsabilità. Questo approccio limita l'esposizione del sistema a potenziali rischi derivanti da accessi non autorizzati o da privilegi eccessivi. Attraverso l'assegnazione di ruoli specifici a ciascun utente in base alle proprie responsabilità e autorizzazioni, si riduce il rischio di abusi o di manipolazioni da parte di utenti non autorizzati.</p> <p>Sistema di Rilevamento e Mitigazione DDoS: L'implementazione di un sistema di rilevamento e mitigazione DDoS è essenziale per proteggere i servizi, le risorse e i sistemi informativi dagli attacchi di denial of service distribuiti (DDoS). Questi attacchi possono sovraccaricare i sistemi con un volume enorme di traffico dannoso, compromettendo la disponibilità dei servizi online e causando interruzioni gravi alle operazioni aziendali.</p> <p>Limitazione del Traffico Sospetto: La limitazione del traffico sospetto contribuisce a proteggere la rete e i sistemi informatici da potenziali minacce e attività dannose. Bloccando o limitando il traffico che è identificato come sospetto o</p>	
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

	<p>potenzialmente dannoso, si riduce significativamente il rischio di intrusioni, violazioni della sicurezza e danni ai sistemi e ai dati.</p> <p>Valutazione periodica dei Rischi: La valutazione periodica dei rischi è fondamentale per mantenere un'efficace postura di sicurezza informatica nel tempo. Questo processo ciclico consente di identificare e valutare le nuove minacce, i cambiamenti nell'ambiente operativo e le vulnerabilità emergenti che potrebbero influenzare la sicurezza dei sistemi e dei dati.</p>	
<p>TASK S-5 Continuous Monitoring Strategy—System Develop and implement a system level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy.</p>	<p>Firewall e Filtraggio del Traffico:</p> <ul style="list-style-type: none"> - Effettuare test di penetrazione regolari per verificare che il firewall sia configurato correttamente e che le regole di filtraggio del traffico siano applicate come previsto. - Monitorare i log del firewall per identificare eventuali tentativi di accesso non autorizzato e verificare che le regole di filtraggio siano state applicate correttamente. <p>Crittografia dei Dati:</p> <ul style="list-style-type: none"> - Verificare che tutti i dati sensibili vengano crittografati durante il trasferimento attraverso la rete utilizzando strumenti per lo sniffing dei pacchetti per analizzare il traffico di rete e assicurarsi che i dati siano illeggibili in caso di intercettazione. - Utilizzare strumenti di crittografia e decrittografia per verificare che i dati crittografati possano essere correttamente decifrati solo con le chiavi di crittografia appropriate. <p>Accesso Basato sui Ruoli:</p> <ul style="list-style-type: none"> - Effettuare audit regolari degli account utente per assicurarsi che siano correttamente assegnati ai ruoli appropriati e che non vi siano privilegi eccessivi o non necessari. - Testare i controlli di accesso eseguendo scenari di prova in cui vengono simulate varie situazioni di accesso, verificando se gli utenti ottengono solo l'accesso autorizzato alle risorse. <p>Sistema di Rilevamento e Mitigazione DDoS:</p> <ul style="list-style-type: none"> - Configurare scenari di test per simulare attacchi DDoS e verificare se il sistema di rilevamento e mitigazione DDoS riesce a rilevare e rispondere tempestivamente agli attacchi. 	

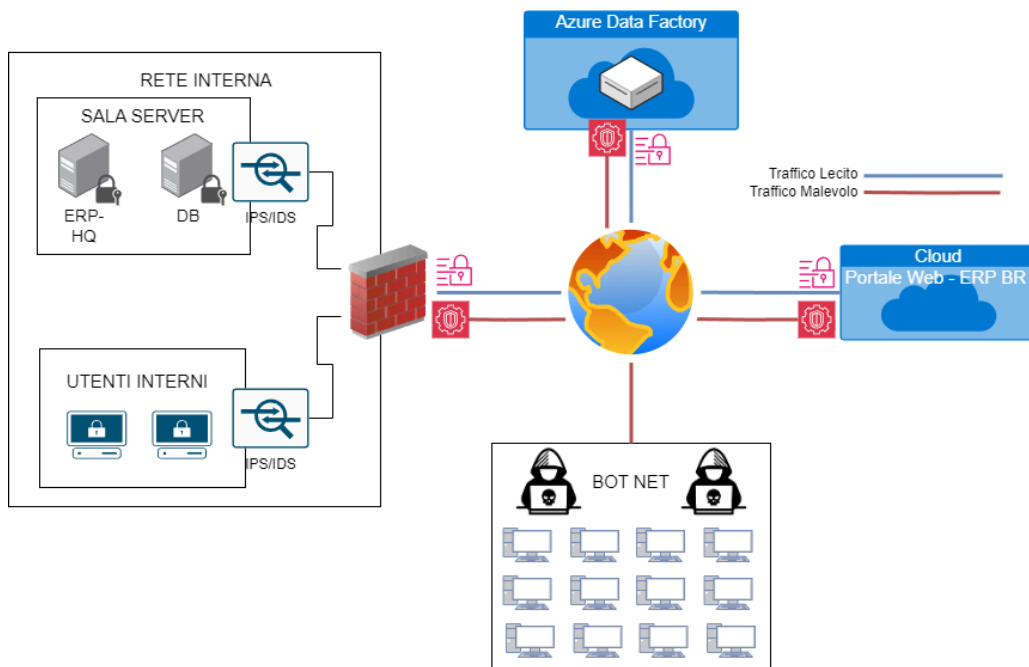
	<ul style="list-style-type: none"> - Monitorare il sistema di rilevamento DDoS durante il normale funzionamento per identificare eventuali anomalie nel traffico di rete che potrebbero indicare un possibile attacco in corso. <p>Limitazione del Traffico Sospetto:</p> <ul style="list-style-type: none"> - Utilizzare strumenti di monitoraggio del traffico di rete per identificare e analizzare il traffico sospetto e verificare se i limiti sul numero di richieste o connessioni vengono applicati correttamente. - Effettuare test di carico per verificare se i limiti imposti sul traffico sospetto sono in grado di proteggere efficacemente i servizi e le risorse dall'overload causato da attacchi DDoS. <p>Valutazione periodica dei Rischi:</p> <ul style="list-style-type: none"> - Condurre revisioni periodiche dei controlli di sicurezza per identificare e valutare nuove minacce e vulnerabilità. - Utilizzare il metodo NIST per identificare e analizzare i rischi in modo sistematico e documentato. 	
--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

9. Implement

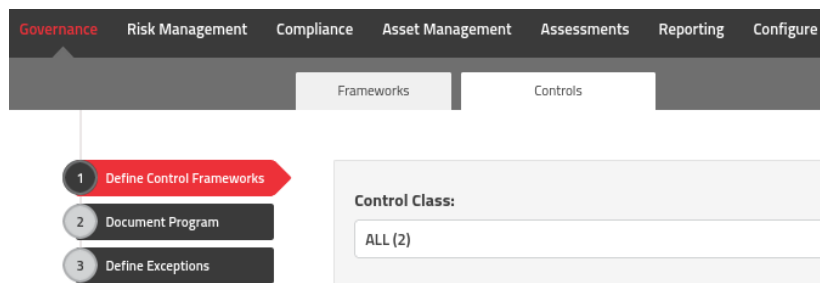
Implementati i Controlli in SimpleRisk (TASK I-1), effettuando così una mitigazione del rischio ottenendo dei valori di rischio residuo. Non concentrate tutti i controlli lo stesso giorno ma utilizzate un arco temporale, così da ottenere dei grafici in cui si possa vedere una variazione nel tempo. In questa fase, la risposta al rischio non è ancora stata sottoposta alla direzione per l'approvazione (non fate click su "Accept Mitigation" in Risk/Mitigation).

Task	Descrizione	Simple Risk
TASK I-1 Control Implementation Implement the controls in the security and privacy plans.	Implementazione dei sistemi di sicurezza all'interno dell'infrastruttura aziendale (vedere	Risk Management/2

figura seguente) e inserimento dei controlli su Simple Risk



9.1 Implementazione dei controlli su SimpleRisk



In "Governance", "Define control Frameworks" si è proceduto ad inserire i 5 controlli inseriti nella tabella al Task S-1, di cui si fornisce una prova nell'immagine seguente. Come si può vedere i controlli indicati sono 5.

+
Controls (5)
Delete Controls

Control Short Name: NIST SC-7 Boundary protection
Control Long Name: NIST SC-7 Boundary protection
Control Number:
Control Owner:
Control Priority:
Current Control Maturity: Not Performed
Desired Control Maturity: Not Performed
Control Class: Technical
Description: Implementazione di misure di sicurezza per proteggere i confini della rete da accessi non autorizzati o compromessi, attraverso l'uso di firewall e altre tecnologie di protezione.
Control Family: System and Communications Protection
Supplemental Guidance:

Control Phase: Technical
Control Family:
Mitigation Percent: 35
Control Type: Standalone
Control Status: Pass

☐
Mapped Control Frameworks

Framework	Control
NIST 800-53 Rev.5	For Informations Systems and privacy

☐
Mapped Assets

Current Maturity	Asset
Performed	Configurazione e mappatura dei dati sul PaaS.On-premise

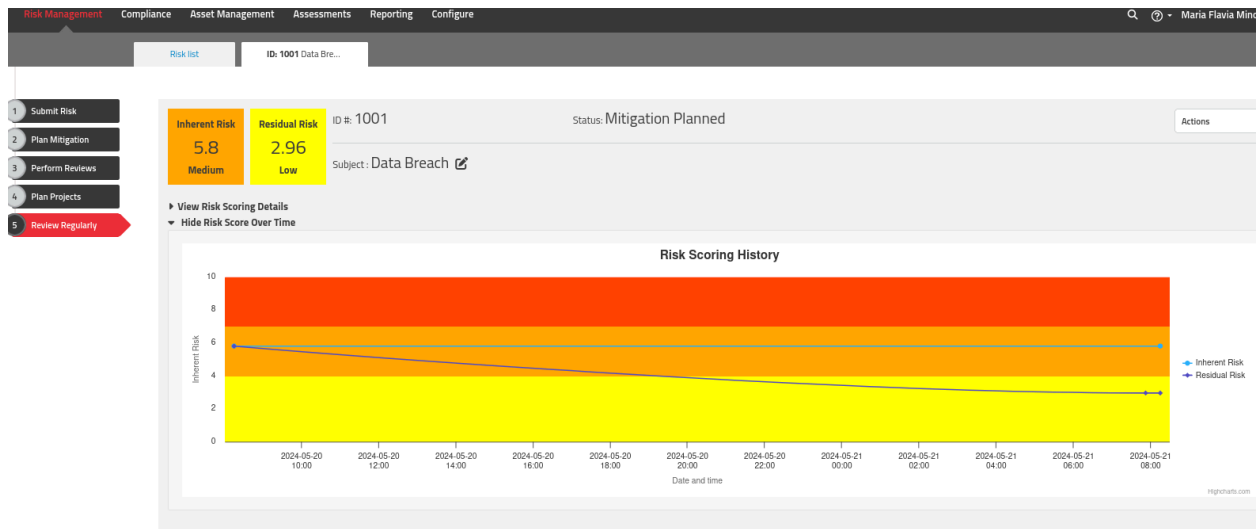
A questo punto si devono implementare i controlli applicandoli ai due rischi identificati e valutati nella giornata di ieri.

In “Risk Management”, “Review regularly”, dopo aver selezionato i due rischi tramite il loro ID (1001 e 1002), nella sezione “mitigation” si sono applicati i controlli per i due rischi ottenendo il **Rischio Residuo**:

- **Data Breach: 2.96 = Low**
- **Attacco DDoS: 4.49 = Medium**

In “View Risk Scoring Details” è possibile visualizzare un grafico che mostra nel tempo il risultato dell'applicazione dei controlli rispetto al rischio selezionato.

9.2 Risk Scoring History Data Breach



9.3 Risk Scoring History DDoS

