UNIVERSITÀ
DEGLI STUDI
DI PADOVA

DIPARTIMENTO
DI INGEGNERIA
DELL'INFORMAZIONE

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

CORSO DI LAUREA IN INGEGNERIA INFORMATICA

ANALISI DEI REQUISITI IN AMBITO AZIENDALE: IMPLEMENTAZIONE DI UN PASSWORD MANAGER A FINE CERTIFICAZIONE ISO 27001

Relatore: Prof. Migliardi Mauro

Laureando/a: Spinosa Diego

ANNO ACCADEMICO 2021 – 2022

Data di laurea 20 Luglio 2022

SOMMARIO

INTRODUZIONE

Il problema affrontato dalla tesi riguarda la tematica della sicurezza dei segreti in ambito aziendale. In particolare, l'azienda dove l'attività è stata svolta intende certificarsi secondo gli standard ISO 27001, i quali prevedono l'implementazione di rigide politiche per assicurare la sicurezza delle informazioni in genere durante la loro circolazione interna all'organizzazione. Come sarà approfondito successivamente, i miei compiti hanno riguardato la gestione dei segreti su supporti elettronici, concretamente credenziali d'accesso custodite dai dipendenti. Le richieste della certificazione obbligano l'azienda a dotarsi di un mezzo che permetta il salvataggio e la comunicazione di questi segreti in maniera il più sicura possibile. Per questo si è valutata l'adozione di un password manager da estendere all'intera azienda e da integrare il più possibile con i sistemi informativi e gestionali esistenti.
Tuttavia, l'offerta di tali software nel mercato è più che ampia: da questo punto è iniziato il lavoro di selezione, analizzando i requisiti imposti della certificazione e successivamente da parte dell'azienda e dei dipendenti. Dai confronti e dai test effettuati è stato possibile individuare un pool di possibili soluzioni, fornendo per quella più viabile un progetto d'integrazione nelle dinamiche aziendali rivelatosi attuabile con buoni risultati anche nel lungo termine.

L'AZIENDA

Il tirocinio si è svolto alla ATON S.p.A. Società Benefit nella sua sede principale di Villorba (TV).
ATON si occupa principalmente di *store automation,* curando l'informatizzazione della grande distribuzione a tutto tondo: dalla gestione dei flussi logistici alla raccolta ed elaborazione delle statistiche di vendita.
Tra i propri clienti annovera grandi realtà come Parmalat, Bricoman, gruppo Aspiag, oltre ad altri marchi nazionali ed esteri. Il gruppo conta all'incirca 200 dipendenti di cui più della metà nella sede centrale di Villorba. Altre sedi del gruppo sono a Torino ed in Spagna.
Il *core business* di ATON è legato all'automazione della logistica e dei flussi merci: l'implementazione di tecnologie di tracciamento come barcode e RFID permette una semplificazione importante nelle operazioni di movimento ed inventario, comportando all'utente finale notevoli vantaggi in termini di tempo e precisione.
In tale ambito l'azienda offre un servizio completo, dalla fornitura dei terminali per la scansione delle merci e loro assistenza alla gestione completa dei sistemi informativi nei siti di vendita finale.
La progettazione, implementazione e mantenimento di tali sistemi è compito principale del grande reparto IT di ATON, suddiviso a sua volta in assistenza e progettazione-sviluppo. Coerentemente col percorso di studi da me intrapreso, il mio tirocinio si è svolto in tale reparto, precisamente nella zona *supporto IT*, dedicata all'assistenza dei sistemi interni.

ATON dal 2019 è certificata *Great Place To Work*: la maggior parte dei dipendenti ha valutato l'azienda come luogo di lavoro eccellente.
L'azienda dal 2021 è *Società Benefit*: ha incorporato nel proprio statuto sei obiettivi ispirati all'Agenda 2030 delle Nazioni Unite, legati alle tre dimensioni, sociale, ambientale ed economica, definiti dai valori *People, Planet, Prosperity*.

LA CERTIFICAZIONE ISO/IEC 27001

La famiglia di standard ISO/IEC 27000 riporta centinaia di controlli e meccanismi di controllo per aiutare le organizzazioni di ogni tipo e dimensione a mantenere protette le loro risorse di informazioni.
Dal momento che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. L'obiettivo dello standard ISO 27001 è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.
Le norme non si limitano a definire le linee guida per la sicurezza delle informazioni su supporto informatico ma include indicazioni sulla sicurezza fisica, ambientale e organizzativa da applicare nell'ambito aziendale.
L'impostazione dello standard ISO/IEC 27001 si basa sull'approccio per processi, identificando le fasi di:

- Definizione politica per la sicurezza
- Identificazione dei rischi
- Analisi dei rischi
- Valutazione dei rischi
- Trattamento dei rischi
- Riesame e rivalutazione post-trattamento
- Implementazione strumenti per il miglioramento continuo: definizione di audit interni, azioni preventive, sorveglianza

Questi punti vanno attuati rispettando una serie di *best practice* che riguardano svariati aspetti: dai requisiti della documentazione prodotta alla suddivisione delle responsabilità, dal controllo degli accessi ai dati alla formazione del personale.
L'obiettivo principale è quello di progettare un sistema per la gestione del rischio, la protezione delle informazioni e degli asset aziendali, in modo da aiutare l'organizzazione a conformarsi a requisiti normativi nonché legali correlati alla sicurezza delle informazioni. La norma è applicabile a tutte le imprese o aziende pubbliche.

IMPORTANZA DELLA CERTIFICAZIONE
Perché certificarsi?

La certificazione ISO 27001 è oggetto di investimenti da parte di molte aziende di medie e grandi dimensioni. Ad esempio: Xerox, Vodafone, Pfizer.

I motivi che spingono un'azienda a certificarsi si possono riassumere in:

1. Ragioni economiche.
   L'investimento che l'azienda deve sostenere per l'adeguamento e la certificazione agli standard è considerato ripagato dal minor rischio di perdite di dati.
   Tali eventi possono infatti portare a disservizi e ripercussioni economiche notevoli, se non addirittura azioni legali e sanzioni.

2. Soddisfazione di requisiti legali.
   L'ottenimento della certificazione assicura alti standard di privacy. In genere, un'organizzazione certificata ISO 27001 adotta protocolli e principi che la portano al rispetto delle normative europee GDPR: la loro violazione comporta per le aziende sanzioni fino a diversi milioni di euro.

3. Espansione nel mercato e apertura a nuovi clienti.
   Specialmente nei settori in cui vi è costante necessità di trattare dati personali, affidarsi ad un'azienda certificata diventa consigliabile se non obbligatorio. La sicurezza che una tale azienda può offrire è un notevole valore aggiunto.
   Considerata la limitata diffusione della certificazione ad oggi, può diventare un mezzo per emergere nel mercato e differenziarsi dai competitor.

4. Vantaggi d'immagine e reputazione.
   Eventi di violazione della sicurezza dei dati possono inoltre comportare un grave danno d'immagine all'azienda, con conseguenti perdite di clienti. Un'azienda certificata ISO 27001 garantisce ai propri clienti un solido modello organizzativo interno, mirato a conservare al meglio i dati da loro affidati.

LA CERTIFICAZIONE SECONDO ATON
Azioni e obiettivi

A scopo di ottenere la certificazione ATON ha analizzato le dinamiche aziendali, evidenziando i flussi informativi in cui l'azienda è coinvolta.
L'analisi tratta molteplici aspetti, tra cui:

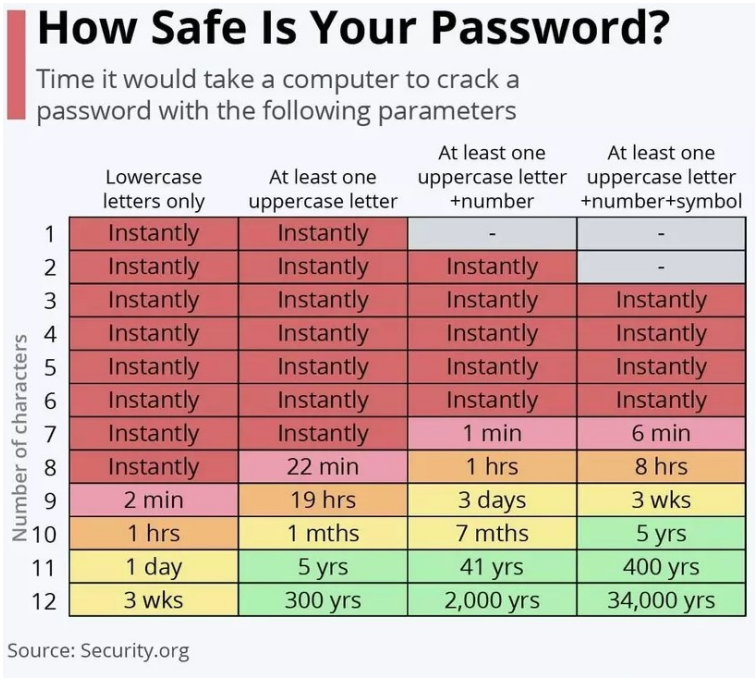
- Gestione degli accessi agli ambienti
- Classificazione delle informazioni e delle comunicazioni
- Gestione agli accessi logici

Inoltre, è stata redatta una *Politica per la sicurezza delle informazioni* in cui sono sintetizzati i comportamenti che il personale dell'azienda deve mantenere quando a contatto con dati personali e non.
Trattandosi di un'azienda altamente informatizzata nei flussi interni e avendo continuamente contatto con altre realtà e servizi tramite mezzi informatici, buona parte dei segreti da salvaguardare è costituito da credenziali (coppie *nome utente-password*).
Nell'ultimo punto, *gestione agli accessi logici*, l'azienda definisce con precisione i ruoli coperti dal personale dal punto di vista della sicurezza. Viene posta enfasi sull'importanza delle buone pratiche di gestione e igiene delle credenziali: si raccomanda la custodia di tali oggetti esclusivamente in forma protetta, sconsigliando l'annotazione su carta e preferendo il salvataggio su supporto elettronico cifrato.
Nel punto precedente si tratta invece la comunicazione interna all'azienda delle informazioni. In particolare, la *circolazione interna delle credenziali* è un aspetto di essenziale importanza, in quanto l'esistenza di credenziali condivise o l'assegnazione di nuove credenziali presuppone un costante bisogno di comunicare dati estremamente riservati.
L'azienda prescrive l'uso di appositi canali elettronici che implementino autenticazione, cifratura e tracciabilità, a scapito di mezzi più vulnerabili come quelli cartacei.

Dopo una valutazione da parte del reparto IT di ATON, si è deciso come l'implementazione di un *password manager* per uso interno a livello aziendale possa rispondere a tali esigenze. Recentemente l'azienda si è già trovata ad introdurre l'uso di nuovi strumenti elettronici per la condivisione di risorse fra gli utenti, con ottimi risvolti organizzativi: le aspettative dall'azienda sono le medesime per l'implementazione di questo nuovo strumento.

PASSWORD MANAGER: PRINCIPI

Con *password manager* s'intende un programma per la custodia, la generazione e la gestione delle proprie credenziali d'accesso a programmi e siti.
Queste funzionalità si rivelano particolarmente utili quando si vuole mantenere un alto standard di sicurezza. A tal fine, si raccomanda sempre di usare password complesse e uniche.
Come spesso richiesto dai servizi stessi in fase di registrazione, idealmente le password dovrebbero consistere in una stringa di ragionevole lunghezza composta da caratteri alfanumerici e simboli non legati tra loro, variegati e alternati nella tipologia.
Un esempio di password sicura potrebbe essere `!xq7^@ZzVvX%`, senz'altro complicata da ricordare, ma altrettanto complicata da indovinare: secondo un articolo del World Economic Forum, il *cracking* della password soprastante richiederebbe 34'000 anni.



How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

I password manager possono aiutare sia nella generazione di password così complesse sia nella loro custodia: all'utente non sarà richiesto di imparare stringhe così complesse, mantenendo però i benefici dal loro uso.
Anche l'inserimento nei moduli di accesso è agevolato: l'inserimento di caratteri speciali può risultare difficoltoso, per questo i password manager talvolta offrono funzionalità di *autofill*, con cui la giusta coppia *username-password* è automaticamente posta nei campi corrispondenti delle pagine web.

PASSWORD MANAGER: SICUREZZA

Essendo pensati appositamente per scopi di sicurezza, questi programmi utilizzano avanzati algoritmi di cifratura e protezione per le password salvate al loro interno.
L'accesso al database delle proprie credenziali (spesso definito *cassaforte* o *vault*) avviene inserendo una *master password*, con cui i propri dati verranno decriptati. La convenienza da parte degli utenti nell'uso di questi programmi si riconduce al dover ricordare una e una sola password con cui accedere ad ogni sito nella maniera più sicura possibile.

Inoltre, la sicurezza di alcuni di questi strumenti è data da una politica *zero-knowledge* che adottano: nemmeno il programma conosce la *master password* degli utenti; ciononostante, riesce a riconoscere se la password inserita durante un tentativo di accesso alla propria cassaforte è corretta o meno. Se ne deriva che anche se malintenzionati dovessero entrare in possesso del database usato dal password manager, non ne potrebbero ricavare alcuna informazione significativa in assenza della *master password* associata (a meno di attacchi *brute-force* di durata impensabile).
L'uso di tali principi comporta uno svantaggio di rilevante importanza: questi programmi spesso non presentano una funzione per il recupero della *master password* in caso la si dimenticasse. Ne consegue che in caso di smarrimento della chiave d'accesso l'utente perde completamente e irrimediabilmente l'accesso alla propria cassaforte.
D'altra parte, il meccanismo del recupero password è spesso impiegato da malintenzionati per ottenere l'accesso agli account: questi non potranno accedere alla cassaforte nemmeno avendo accesso alla casella mail principale dell'utente.

Queste caratteristiche di sicurezza rispondono perfettamente alle esigenze di protezione e cifratura rilevate da ATON per quanto riguarda la custodia delle credenziali.

PASSWORD MANAGER: ALTRE FUNZIONALITA'

Il mercato offre una vasta scelta di password manager, accomunati dallo stesso scopo di gestione credenziali, ma con diversi servizi accessori offerti all'utente.
Si possono identificare principalmente due categorie di programmi: quelli ideati per uso personale e quelli invece progettati per l'implementazione in un ambiente aziendale.
Questi ultimi offrono spesso una serie di funzionalità dedicate al *teamworking* come la condivisione di credenziali fra membri di uno stesso gruppo.
Queste funzionalità coincidono con quelle richieste dall'azienda per quanto concerne la sicurezza durante la *circolazione interna delle credenziali*.

Soddisfatte queste esigenze fondamentali, è confermato come un password manager possa aiutare l'azienda nei suoi bisogni. Giunti a questo punto, il pool di software disponibili è ancora molto vasto.
È necessario effettuare un'analisi più approfondita per comprendere appieno le preferenze dell'azienda e poter scegliere il software più adatto, espandendosi verso esigenze secondarie che comunque possono influenzare la scelta finale.

ANALISI DEI REQUISITI: ESIGENZE E PREFERENZE

Il lavoro eseguito finora ha fatto emergere le seguenti esigenze fondamentali:

- Custodia e protezione delle credenziali
  Il compito è svolto da qualsiasi password manager in quanto principale scopo del programma.
- Condivisione credenziali fra gruppi di utenti
  Questa funzione è svolta dalla maggior parte dei password manager per ambito aziendale.

Un colloquio col *security manager* di ATON ha prodotto alcuni requisiti preferenziali aggiuntivi:

- Integrazione SSO
  Nell'uso dei sistemi informatici dell'azienda, i dipendenti possono accedere al proprio computer, alla propria casella mail aziendale e tutti gli altri portali interni con una sola coppia *username-password* gestita in modo centralizzato tramite un apposito server d'autenticazione. Questo meccanismo prende il nome di *Single Sign On*.
  Sarebbe comodo per i dipendenti riuscire con le medesime credenziali ad accedere anche al password manager per visionare la propria cassaforte.
- Integrazione Active Directory
  Active Directory è il servizio di Microsoft che l'azienda sfrutta per la gestione logica dei dipendenti all'interno dei sistemi informativi. Lo strumento permette di creare dei gruppi che rispecchiano le divisioni interne dell'azienda (i vari reparti).
  Ogni gruppo è caratterizzato da una serie di permessi e può accedere ad una serie di risorse. Nei gruppi sono ripartiti i dipendenti secondo il loro ruolo nell'organizzazione.
  Sarebbe elemento preferenziale poter importare la struttura dei gruppi direttamente nel password manager, sincronizzando automaticamente il bacino degli utenti qualora questi escono o entrano nell'organico aziendale.

Altro nodo fondamentale è rappresentato dalle risorse a disposizione per la creazione del sistema:

- Costo del sistema: ATON è disposta ad impiegare soluzioni a pagamento entro un certo budget di spesa. Tuttavia, sono da preferirsi soluzioni gratuite o a basso costo.

ANALISI DEI REQUISITI: CONFRONTO DELLE SOLUZIONI

Durante la ricerca del software, è emerso un altro fattore potenzialmente discriminante: l'hosting del servizio (e sua modalità di fruizione). Si distinguono:

- Servizi cloud (o *hosted*)
  La serie di dati e applicativi che formano il servizio vengono eseguiti nel cloud, ovvero su una macchina remota gestita da terzi. La configurazione è totalmente delegata ai gestori del servizio e gli utenti si limitano a godere del servizio.
  Conseguentemente, questa tipologia di soluzioni prevede sempre dei costi quantomeno legati al mantenimento delle macchine su cui il servizio si appoggia.
  La gestione della sicurezza è compito esclusivo di chi offre il servizio, assumendosi tutte le responsabilità.

- Servizi self-hosted (o *on-premises*)
  L'organizzazione che intende sfruttare il servizio deve predisporsi di una macchina adatta da adibire a server per il password manager. La configurazione è a carico dell'azienda, ma i produttori dell'applicativo possono fornire assistenza.
  Le responsabilità per la sicurezza ricadono tutte sull'organizzazione, che resta però in stretto possesso di tutti i suoi dati, senza affidarli a terzi.
  Essendo l'azienda ad occuparsi della gestione del server, questo scenario può rivelarsi più economico, con abbonamenti scontati se non addirittura gratuiti.

Nella ricerca si è scelto di includere tutte le soluzioni, sia *hosted* che *on-premises*, in modo da ottenere una panoramica più ampia dei software disponibili: sarà compito successivo valutare quello più adatto.

Possibili soluzioni trovate

La ricerca è avvenuta via internet utilizzando i principali motori di ricerca.

Caso speciale è Bitwarden, proposto dai membri IT dell'azienda ancora prima del mio arrivo.

Il prodotto dell'attività è riassunto nella tabella sottostante:

Nome	SSO	Sharing	Prezzo	Cloud?	AF	Gratuitamente?
Bitwarden	Si	Si	$5/m/u	Si	Si	Funz. base, on-prem
1password	Si	Si	$7.99/m/u	Si	Si	Niente (prova)
ManageEngine PM..	Si	Si	Preventivo	No	Si	Niente (prova)
Passbolt	No	Si	~€600/m	Si (+€9/m)	Si	Funz. base, on-prem, sharing
Keeper	Si	Si	€45/a/u	Si	Si	Niente (prova)
LastPass	Si	Si	€5.7/m/u	Si	Si	Niente (prova)
Onelogin	Si	Si	$2/m/u	Si	Si	Niente (prova)
Passwork	Si	Si	Preventivo	No	Si	Niente (prova)
Psono	Si	Si	€2/m/u	Si (+€1/m/u)	Si	Niente (prova)
Pleasant PW Server	Si	Si	$14'739	No	Si	Niente (prova)
Dashlane	Si	Si	€8/m/u	Si	Si	Niente (prova)

Significato delle colonne:

- SSO: Indica se il programma supporta il *single-sign-on* (spiegato precedentemente)
- Sharing: Indica se il programma supporta la condivisione credenziali tra utenti
- Prezzo: indica il costo della soluzione. Il costo è indicato, ove possibile, per soluzione con hosting *on-premises* e funzioni preferenziali (SSO e sharing) dove disponibili.
  I prezzi sono indicati come "per mese/per utente", "per anno/per utente" o "per mese".
  Ove non specificato, il prezzo è una tantum.
- Cloud: Indica se la soluzione include o può includere hosting da parte di terzi.
- AF: Indica se la soluzione offre funzionalità di autofill (spiegato precedentemente)
- Gratuitamente: indica le funzioni di cui si dispone gratuitamente.
  Alcuni software, infatti, offrono le loro funzioni base con licensing *open-source*: permettendo a chiunque di contribuire al progetto vi è un costante apporto di modifiche e miglioramenti (anche nella sicurezza) totalmente gratuito.

Resoconto della ricerca

Le soluzioni identificate soddisfano tutte, in maniera più o meno completa, le richieste fondamentali e preferenziali dell'azienda. Il *security manager* ha manifestato propensione per una soluzione gratuita, consigliando la prova della suite *Bitwarden* per valutare la sua applicabilità al contesto aziendale di ATON.

PROVA: BITWARDEN

Bitwarden è una suite password manager nata nel 2016 e prodotta negli Stati Uniti.

La suite è incentrata sull'accesso multipiattaforma: inizialmente accessibile esclusivamente via web, sono poi nate app dedicate per il mercato mobile e successivamente anche per mercato computer, sia Windows che Linux.
Sono disponibili inoltre le estensioni per tutti i principali (e non) browser con cui accedere in qualsiasi momento alla propria cassaforte durante la navigazione e prelevare le corrette credenziali.
La versione gratis, ovvero lo "zoccolo" open-source della suite comprende solamente un potente password manager con crittografia AES-256 bit *end-to-end* (i dati sono crittografati ancora prima del loro invio dal dispositivo dell'utente e decriptati solo alla visualizzazione).
L'interfaccia utente è molto intuitiva e auto esplicativa, aspetto da non sottovalutare vista la larga diffusione che il servizio dovrebbe avere a regime nell'azienda.
Come già specificato, il programma supporta l'integrazione con sistemi SSO e anche l'importazione di utenti e gruppi da *Active Directory*, tuttavia solamente nelle versioni a pagamento. Anche la condivisione delle credenziali fra i gruppi non è possibile senza abbonamento.
I processi di registrazione ad accesso al servizio sono molto semplici e non richiedono particolari attenzioni.
Bitwarden viene offerto dai produttori sia come servizio gestito sia come applicativo per l'uso in self hosting. Da notare che per entrambi gli scenari i costi degli abbonamenti premium sono gli stessi: il produttore considera il self hosting un valore aggiunto in quanto l'organizzazione gestendo autonomamente l'infrastruttura mantiene pieno controllo sui propri dati.

Setup di prova

Per il setup di prova, Bitwarden è stato installato su una macchina virtuale locale con ambiente Ubuntu 18.04 LTS. L'interazione con la macchina è avvenuta esclusivamente tramite shell SSH: il collegamento è stato effettuato mediante client PuTTY.
I requisiti minimi richiesti da Bitwarden per l'esecuzione sono modesti: sono richiesti un processore single-core, 2GB di memoria RAM e 10GB di spazio su disco.

Ulteriore requisito è che nel sistema siano installate le librerie Docker per fornire la piattaforma su cui viene eseguito Bitwarden.

Breve introduzione alla piattaforma Docker

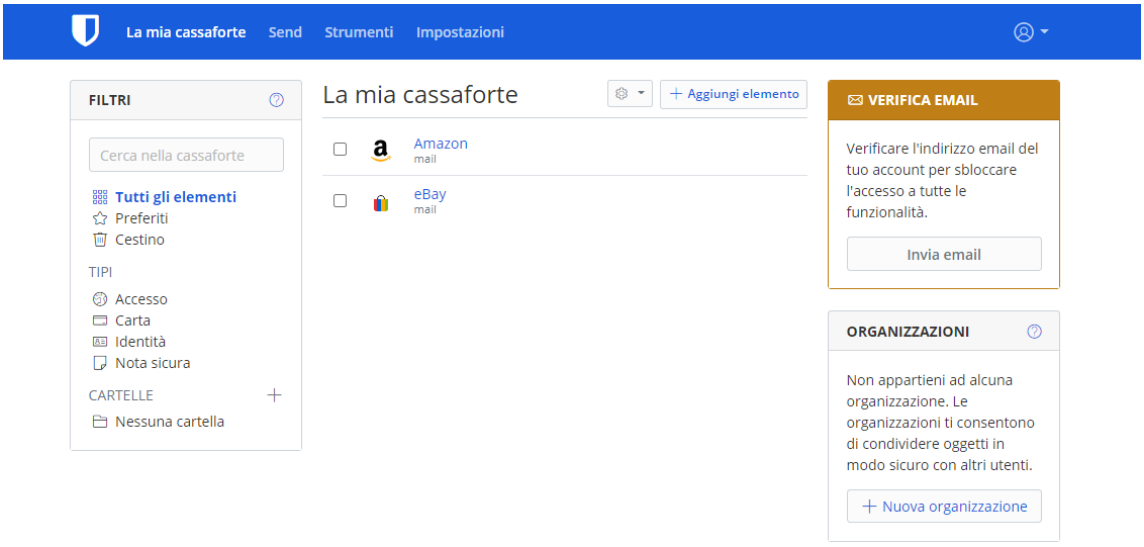
Docker è una piattaforma di virtualizzazione software che si pone tra il S.O. della macchina e gli applicativi in esecuzione. Docker offre il supporto all'esecuzione di applicazioni all'interno dei *container*, spazi virtuali (*sandbox*) dotati di risorse limitate ed esclusive dove un servizio andrà ad eseguirsi. Peculiarità della piattaforma è l'indipendenza dei container dalla macchina sottostante, permettendo ai container di essere replicati e distribuiti per l'esecuzione su diverse macchine fisiche senza pesanti riconfigurazioni.

Inoltre, un servizio in esecuzione in un container può usare solo e solamente le risorse a lui assegnate, in nessun caso generando situazioni di conflitto con altri container. Questo consente addirittura l'esecuzione sulla stessa macchina di più istanze praticamente identiche di un servizio senza che queste vadano accidentalmente ad interagire.

Rispetto ad una classica virtualizzazione offerta dalle macchine virtuali non c'è piena virtualizzazione di hardware e sistema operativo: questo consente in aggiunta di ottenere un livello di efficienza maggiore e una maggior semplicità di distribuzione delle immagini (un container integra l'applicativo e la configurazione dell'ambiente, mentre una VM include anche la configurazione dell'hardware virtuale e l'intera immagine del S.O.)

L'installazione su sistemi Ubuntu è completamente automatizzata mediante uno script bash. Il wizard iniziale guida l'utente nella configurazione preliminare, comprese le impostazioni per la certificazione SSL in uso dal server: viene data possibilità all'utente di caricare un certificato, di usare un certificato autofirmato o di non utilizzare un certificato.
L'accesso ai log ed ai file di configurazione è possibile ma non vi è molta libertà sulle modifiche apportabili.

Punti a favore	Punti a sfavore
• Presenza di un *core* molto solido dotato di eccellenti sistemi di sicurezza • Installazione relativamente semplice, configurazione lato server autonoma • Interfaccia molto curata e di semplice apprendimento	• Funzioni molto basiche se non si sottoscrive alcun abbonamento • Costo dell'abbonamento notevole, considerando 200 dipendenti • In mancanza di un piano premium, l'azienda non può soddisfare i requisiti di circolazione delle credenziali: mancano le funzioni di condivisione elementi tra utenti



Schermata principale di Bitwarden, con accesso alla cassaforte.

Bilancio preliminare

Dal test nella sua versione gratuita, Bitwarden è risultato abbastanza limitato nelle funzionalità, ma molto solido ed affidabile. Resta il nodo della condivisione credenziali, da risolvere. Si potrebbe valutare il compromesso dell'uso individuale, soddisfando i requisiti di conservazione ma non quelli di comunicazione delle credenziali.

D'altra parte, l'uso con licenza Premium permetterebbe il completo soddisfacimento delle esigenze aziendali, ed in più offrirebbe tutte le integrazioni coi sistemi informativi preesistenti. Purtroppo, il costo associato non sarebbe trascurabile: coprendo l'intera azienda si spenderebbero svariate migliaia di euro ogni anno.

A fronte di questa valutazione, si decide di proseguire con i test per valutare l'adozione eventuale di un altro software. L'altra soluzione preferenziale è Passbolt, in quanto unica altra opzione che dispone di un core *open source* e quindi gratuito per l'azienda.

PROVA: PASSBOLT

Passbolt nasce nel 2011 nel Lussemburgo spinto da due principi cardine: fornire un password manager dall'affidabilità professionale che fosse *open source* e che fosse completamente Made in Europe. Fin dalle prime versioni Passbolt è stato concepito proprio per un uso in ambito aziendale, in particolare per imprese dalle piccole e medie dimensioni.

L'intero progetto dietro Passbolt è definito *developer-centric*: viene data estrema importanza al contributo volontario degli sviluppatori al progetto.

Ciononostante, il fatto di avere una moltitudine di persone che continuamente lavora sul programma non deve in alcun modo inficiare sul livello di sicurezza offerto: Passbolt ogni anno si affida a specialisti e certificatori terzi per sottoporsi a profondi audit sul livello di sicurezza offerto, ambendo a fornire ai propri utenti la massima qualità possibile.

I protocolli di sicurezza utilizzati dal programma impongono l'uso tramite browser con estensione Passbolt per effettuare qualsiasi operazione: quest'ultima è responsabile della crittografia *end-to-end* dei dati. Di conseguenza, il processo di primo log in e cambio utente risulta abbastanza macchinoso, tuttavia si tratta di operazioni da effettuare raramente nel lungo termine. Queste estensioni sono disponibili anche per dispositivi mobili iOS e Android.

Maggior vantaggio di Passbolt rispetto a Bitwarden è l'inclusione nella versione base della gestione dei gruppi: è possibile creare gruppi in cui condividere le password, risolvendo finalmente anche l'aspetto della circolazione delle credenziali tra i membri aziendali.

D'altra parte, Passbolt non supporta l'integrazione con l'SSO aziendale e, nella versione gratuita, nemmeno dell'importazione dei gruppi da Active Directory.

Se si opta per un piano a pagamento, anche Passbolt offre una soluzione *hosted* che solleva l'azienda da ogni incarico tecnico. La versione gratuita ovviamente obbliga al *self-hosting*.

Setup di prova

Il setup avviene su una diversa VM da quella utilizzata per Bitwarden ma con le medesime caratteristiche. I requisiti per Passbolt sono essenzialmente gli stessi visti precedentemente.

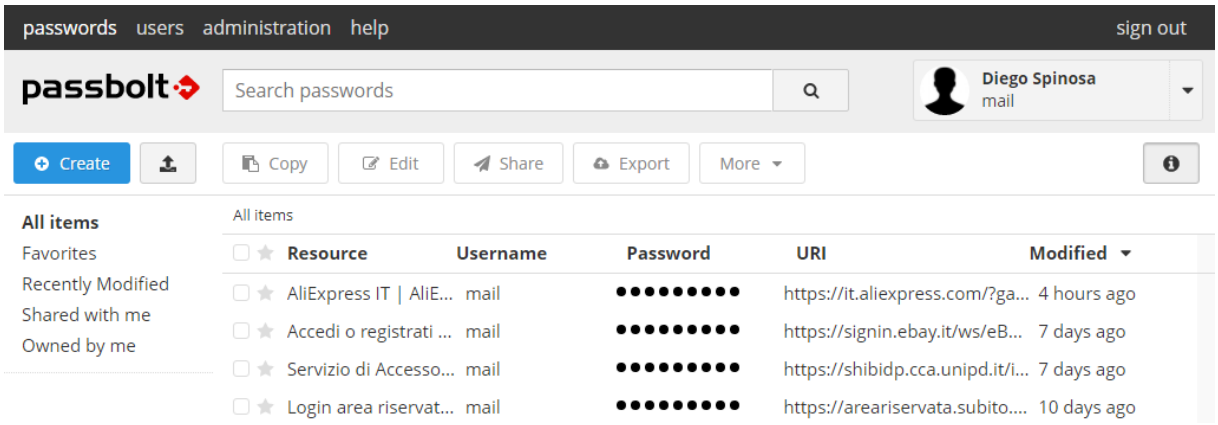
Anche Passbolt può essere eseguito all'interno di un container Docker ma, a differenza di Bitwarden, supporta anche l'esecuzione nativa su Ubuntu. Per comodità, è stato scelto di sfruttare quest'ultima opzione in quanto semplifica sensibilmente la configurazione.

L'installazione in questo caso non è gestita da script bash proprietario ma viene impiegato il gestore pacchetti standard APT. Il wizard che viene presentato all'utente al termine dello scaricamento permette la configurazione dei componenti di base di Passbolt:

- MariaDB
  Per il salvataggio di tutti i dati Passbolt si affida al *database manager* MariaDB.
  La configurazione comprende la creazione del database principale, specificando le credenziali dell'utente che Passbolt utilizzerà per l'accesso al DB.
- nginx
  Web server indispensabile per l'esecuzione dell'intera piattaforma Passbolt.
  Infatti il *core* del programma è sviluppato in linguaggio PHP.
  Vengono richiesti all'utente il nome di dominio a cui sarà raggiungibile il server e sono proposte le seguenti opzioni per quanto concerne la certificazione SSL:
  - Caricamento di una certificazione preesistente
    Vengono richiesti i file certificato e chiave di una certificazione preesistente valida sul dominio del server
  - Generazione autonoma di una certificazione valida
    Questa interessante opzione sfrutta il servizio *Let's Encrypt*, una *certificate authority* che rilascia certificati di sicurezza gratuitamente.
    Il processo però richiede la visibilità pubblica del dominio, non presente durante la prova.
  - Utilizzo senza certificazione
    Passbolt sarà raggiungibile esclusivamente tramite protocollo http (su porta 80 con trasmissione dati in chiaro)

Dopodiché, il server Passbolt è attivo. Accedendovi da browser, si potranno configurare le ultime opzioni, tra cui il server SMTP per l'invio di comunicazioni e notifiche.
Nonostante il wizard abbastanza completo, durante il test si è reso necessario cambiare la configurazione manualmente, agendo sui file di configurazione di nginx (impostazioni su indirizzo e porta a cui rispondere, impostazioni certificato e crittografia) e sul file configurazione di Passbolt (impostazioni SMTP e nome dominio della macchina).

Punti a favore	Punti a sfavore
• Supporto della condivisione elementi tra gruppi di utenti • Ottime funzioni di esportazione e importazione credenziali • Facilità di accesso ai vari file di configurazione e ampia disponibilità di risorse di supporto ufficiali	• Cambio utente macchinoso • Configurazione di default approssimativa, intervento obbligatorio • Avanzamento dello sviluppo generale della suite relativamente lento



Schermata principale di Passbolt, da cui accedere alle credenziali.

Bilancio preliminare

Fra le due opzioni testate, Passbolt è quella che meglio si adatterebbe al contesto aziendale. Considerando le loro versioni gratuite, quest'ultima offre una serie di funzioni dall'importanza cruciale, oltre ad altre caratteristiche utili.

L'adozione di Passbolt porterebbe ad un ottimo compromesso tra soddisfazione delle esigenze e costi: seppur non integrandosi con i sistemi informativi preesistenti, fornisce tutte le funzionalità essenziali a costo praticamente nullo.

Giunti a questo punto, dopo un confronto col *security manager*, si è deciso di proseguire definitivamente con Passbolt in quanto miglior candidato: il fattore costo è prevalso sugli aspetti negativi, anche considerando le molteplici restanti soluzioni individuate.

Segue quindi un progetto di implementazione nel contesto aziendale e una prova in un contesto semi-definitivo, con coinvolgimento più ampio degli *stakeholder*: oltre ai responsabili alla sicurezza, i dipendenti di ATON.

REQUISITI DI SISTEMA: MANUTENIBILITA'

Nell'ottica di un'applicazione definitiva, è fondamentale che nel lungo termine il sistema possa essere aggiornato e revisionato senza causare interruzioni nel servizio.
In aggiunta, è preferibile che i processi di manutenzione non richiedano una conoscenza particolarmente approfondita della piattaforma e/o delle tecnologie impiegate: l'avvicendarsi dei dipendenti nel reparto IT dell'azienda non deve portare a problemi nell'erogazione del servizio e allo stesso tempo non deve obbligare l'azienda a lunghi percorsi formativi.

Analizzando la soluzione identificata, i metodi di aggiornamento sono accuratamente documentati sul sito ufficiale, con guide dedicate per ogni piattaforma adottata dal server.
Lo stesso sito offre guide complete anche per eseguire il backup della piattaforma, comprendendo il database delle credenziali, le chiavi del server e la configurazione: con queste informazioni potrà essere ricreata un'istanza identica del server, permettendo operazioni di *disaster recovery*, essenziali vista l'importanza che Passbolt ricoprirà in azienda.

La documentazione presente nel sito copre anche la configurazione, tuttavia non in toto: ad esempio, è totalmente assente la parte di impostazione del web server integrato alla piattaforma. Inoltre, anche la parte relativa all'interfacciamento con server SMTP risulta abbastanza superficiale.

Sarà quindi d'importanza essenziale produrre una sostanziosa documentazione per guidare sistemisti e tecnici dell'azienda nelle operazioni di installazione, configurazione, backup e ripristino della piattaforma, da sfruttare in maniera complementare all'estensiva documentazione già provvista dagli sviluppatori della suite stessa.

PROGETTO D'IMPLEMENTAZIONE: ANALISI

Individuato Passbolt come valido candidato, è necessario stabilire una serie di politiche comuni su come impiegarlo all'interno dell'azienda, per evitare un uso improprio che possa portare a disguidi nel lungo termine. Segue una panoramica degli aspetti chiave da considerare nel progetto.

PRECISAZIONE: Nell'analisi il termine 'oggetto' riferisce genericamente ad una entry username-password, con opzionalmente alcuni campi aggiuntivi.

Categorie di utenti

Passbolt impiega una gestione degli utenti molto semplice.
Si limita a suddividere gli utenti in due categorie di permessi:

1. USER: Categoria di utente standard, può creare/eliminare oggetti, condividerli con altri utenti singoli, partecipa a dei gruppi in cui è stato incluso da cui legge/modifica oggetti, può condividere i propri oggetti in alcuno/tutti i gruppi di cui fa parte.
2. ADMIN: Oltre ai permessi in quanto user, ha il potere di creare/eliminare gruppi e di gestire le persone al loro interno (aggiungerne/rimuoverne). Può creare manualmente nuovi utenti ed eliminarne. Tuttavia, NON ha accesso agli oggetti altrui.

   Inoltre, gli admin non possiedono particolari vantaggi sul livello di accesso agli oggetti a loro condivisi: se un utente standard condivide con un admin una credenziale in sola lettura, quest'ultimo non avrà altri permessi che la lettura.

Questa gestione abbastanza semplicistica non fa uso di alcun tipo di gerarchie nella gestione di utenti e gruppi: solo gli admin gestiscono i gruppi e ogni admin può gestire tutti i gruppi afferenti allo stesso server.

Livelli di accesso agli oggetti usati nel programma

Ogni utente avrà accesso agli oggetti propri/condivisi con lui secondo uno dei seguenti profili:

- LETTURA: solo lettura.
- MODIFICA: lettura, scrittura, eliminazione globale di un oggetto.
- PROPRIETARIO (non sempre presente): tutte le operazioni, compreso cambio di permessi sull'accesso all'oggetto agli utenti e condivisione.

Precisazione: ogni oggetto è fisicamente salvato all'interno dell'account del creatore. Essere "proprietari" di un oggetto non equivale ad averlo salvato nel proprio account!

→ Può essere deleterio in alcune situazioni: il problema è affrontato in pag. 24

Tipi di condivisione

La condivisione degli oggetti con gli altri membri dell'organizzazione può avvenire in diversi modi:

- CONDIVISIONE UTENTE-UTENTE
    - Al momento della condivisione, l'utente creatore/proprietario dell'oggetto stabilisce i permessi da attribuire con chi viene condivisa.
    - I permessi sono individuali: posso avere in condivisione contemporaneamente utenti con permesso sola lettura e utenti con permesso modifica.
- CONDIVISIONE UTENTE-GRUPPO
    - Un utente facente parte di un gruppo vede gli oggetti condivisi nel gruppo dagli altri utenti.
    - Chi condivide un oggetto in un gruppo decide il livello di accesso di tutti gli altri membri.

Ad un utente non mai è concesso condividere elementi di cui non è proprietario (ri-condivisione).

Ciclo di vita degli utenti

I passaggi fondamentali di un account nella piattaforma corrispondono con le rispettive operazioni nell'azienda: inserimento, movimento interno e abbandono.

1. CREAZIONE DI UN NUOVO UTENTE

   I nuovi utenti possono inserirsi nella piattaforma in diversi modi:

   a. Registrazione libera: chiunque, collegandosi al server, può creare un nuovo account cliccando sul pulsante corrispondente e immettendo il proprio indirizzo e-mail.

      È possibile limitare le registrazioni ai membri aziendali restringendo l'accesso del server alla intranet o limitando il dominio degli indirizzi e-mail accettati a quello aziendale.

      Attivabile/disattivabile da configurazione.

   b. Registrazione su invito: gli admin posso creare manualmente gli utenti, i quali riceveranno per e-mail un link d'invito tramite cui perfezionare la propria registrazione.

2. INTERAZIONI COI GRUPPI

   Un amministratore dovrà inserire manualmente l'utente nei gruppi a cui appartiene. Anche per eventuali spostamenti fra gruppi l'intervento di un amministratore è sempre necessario.

3. ELIMINAZIONE DI UN UTENTE

   L'eliminazione degli utenti, per questioni di sicurezza (potrebbe possedere oggetti condivisi importanti, che quindi andrebbero persi) è compito esclusivo di un amministratore.

POSSIBILI PROBLEMI E SOLUZIONI IN UN SETUP DEFINITIVO

Nel lungo termine, potrebbero sorgere alcuni problemi riguardo alla conservazione e condivisione delle password in particolari scenari:

- Gli oggetti in nessun caso sono associati ad un gruppo ma sono sempre associati ad un utente:
  questo significa che, in un contesto reale, la mobilità degli utenti fra i gruppi è complicata quando si vogliono conservare degli oggetti condivisi
  (Esempio: Igor crea e condivide la password della mail "smtpsender" col gruppo "1". Igor cambia reparto: non farà più parte del gruppo "1". Igor avrà ancora salvata la password di "smtpsender" nel suo account, sebbene quest'ultima interessi solo e solamente al gruppo "1", di cui non fa più parte. Allo stesso tempo, gli altri membri del gruppo "1" non vedranno più la password.)
    - Una soluzione sarebbe individuare un utente fisso, di cui si abbia la sicurezza che non cambi gruppo (perlomeno nel futuro prevedibile). Tuttavia, un tale membro potrebbe non esistere per ogni gruppo, e questo non esclude futuri trasferimenti: il problema potrebbe presentarsi nuovamente in futuro.
    - Un'alternativa potrebbe consistere nel creare delle utenze *dummy*, ovvero non legate strettamente ad una persona. Ad esempio:
      - Una per l'intera organizzazione: si arriverebbe ad un controllo centralizzato, tale account però avrebbe accesso a tutti gli oggetti d'uso comune dell'azienda, condividendoli con i gruppi d'interesse. L'accesso all'account sarebbe eventualmente condiviso tra alcuni membri designati come amministratori. Una tale centralizzazione però potrebbe andar contro ai principi di sicurezza fini dell'attività.
      - Una per gruppo: si arriverebbe ad avere un'utenza "di gestione" che crea e gestisce gli oggetti condivisi con il proprio gruppo. Quest'utenza potrebbe essere unicamente utilizzata da un "amministratore" di gruppo, oppure le sue credenziali potrebbero essere condivise nel gruppo corrispondente per permette a tutti i membri di accedervi.

        - Unico problema è che chi si ritroverebbe a dover usare tale account dovrebbe continuamente scambiarsi tra il proprio e quello "di gestione".
          Per motivi di sicurezza, il cambio utente di Passbolt è abbastanza macchinoso (è necessario importare nel browser la corrispondente chiave privata, salvata in fase di registrazione: è un'ulteriore sicurezza aggiuntiva alla password)

            - Workaround: usare un diverso browser. Ogni browser può mantenere in memoria una diversa chiave privata: con un browser si accederà all'account personale, con un altro all'account di gestione.
              (Ad esempio: testato usando Edge e Chrome)

- Non è possibile rifiutare la condivisione di un oggetto.
  Rende più complicate le condivisioni temporanee: in caso di un accumulo di credenziali non più necessarie non si potrà rimuoverle in autonomia ma sarà necessario domandare al proprietario di venire esclusi dalla condivisione.
  Altra conseguenza è la funzione del tasto elimina: quando attivo, esegue SEMPRE un'eliminazione globale (non si può eliminare un oggetto "per sé")
  D'altro canto, considerando la condivisione via gruppi (e non quella individuale) come metodo principale adottato dall'azienda, questo non dovrebbe essere un problema sistematico.
  Non è inoltre possibile separare il permesso di modifica da quello di eliminazione.

Il progetto proposto è stato approvato dal *security manager* aziendale in quanto sostenibile nel lungo termine senza necessitare di interventi correttivi sistematici.
L'approvazione deve però essere unanime da parte dell'intero bacino utenti: è indispensabile interpellare per lo meno una loro rappresentanza.

GLI STAKEHOLDER: I DIPENDENTI DI ATON

Proseguendo col percorso di selezione, e avendo il *security manager* già espresso una preferenza assoluta, è necessario considerare l'opinione dei restanti stakeholder, in questo caso i dipendenti di ATON.
Saranno loro gli utenti finali della piattaforma: è fondamentale che la soluzione risponda alle loro esigenze.

Da un colloquio con alcuni di loro sono emerse alcune criticità e altre esperienze:

- Necessità di mantenere un alto livello di *igiene delle credenziali*
  Con igiene delle credenziali si intende una serie di buone pratiche fondamentali per l'ordine e la sicurezza. Analizzando la situazione aziendale, ci si è principalmente concentrati sui seguenti punti:
  - Non usare credenziali personali per accessi di gruppo
    Oltre a potenziali esposizioni dei dati personali del proprietario dell'account, in caso di mobilità del dipendente si rende obbligatorio il trasferimento dell'account su nuove credenziali: un processo spesso lungo e difficoltoso.
  - Non usare la stessa password per diversi account
    Per convenienza, spesso si tende ad utilizzare la stessa password per l'accesso a diversi account. Come già precedentemente specificato, è uno dei principali problemi di sicurezza causati dagli utenti
  - Non conservare copie delle credenziali in chiaro
    Durante la condivisione senza l'uso di mezzi specifici la comunicazione delle password senza alcuna cifratura diventa inevitabile.

  Definire delle regole chiare sulla creazione di account condivisi in aggiunta all'uso di un password manager può portare al sicuro raggiungimento degli obiettivi di sicurezza ricercati.

- Precedenti esperienze nell'uso di Password Manager

  Nel reparto Marketing di ATON è già stato sperimentato l'uso di un password manager. Il software utilizzato tuttavia era per uso personale, senza alcun tipo di funzionalità di condivisione, e gestito da terzi (che si occupavano dell'hosting).
  I dipendenti hanno evidenziato i seguenti aspetti:

  - Rapido inserimento delle credenziali ove richieste

    La funzionalità di autofill è stata particolarmente apprezzata per la sua comodità, specie utilizzando password univoche e complesse.
  - Rapida condivisione degli elementi con nuovo personale

    Per quanto fosse realizzato impropriamente, mantenendo le credenziali in un unico contenitore diventa pratico dare accesso agli elementi ad altri membri del gruppo semplicemente condividendo le informazioni necessarie all'accesso.
  - Dipendenza dal servizio

    Utilizzando un servizio con hosting gestito da terzi non si ha il controllo completo sul server che si va ad utilizzare. Ne deriva che in caso di problemi non si potrà fare altro che attendere l'intervento dei gestori.
    È un punto che scaturisce particolare preoccupazione in quanto se si va ad integrare lo strumento nelle dinamiche aziendali la sua indisponibilità può portare ad impedire di lavorare agevolmente.

  La soluzione candidata è dotata di funzionalità di autofill, soddisfando la prima richiesta. Le funzioni di condivisione di Passbolt si adattano perfettamente a quanto rilevato nel secondo punto. Infine, i problemi di dipendenza non si presenterebbero con un servizio gestito da ATON stessa, come sarà il password manager vista la modalità di installazione totalmente *on-premises*.

Esposto il progetto implementativo, anche i dipendenti hanno concordato pienamente per la soluzione che sfrutta account dummy di gruppo: assicura la maggior indipendenza nella mobilità degli utenti nell'azienda e contemporaneamente grava meno sugli amministratori e sui sistemisti.

PANORAMICA FINALE E RESOCONTO

Complessivamente, questo secondo colloquio ha confermato l'esigenza di utilizzare un password manager in azienda, la scelta di Passbolt come soluzione appropriata e l'approvazione al progetto implementativo proposto.
La soluzione approvata consente al contempo di soddisfare le esigenze fondamentali in maniera pressoché completa. Il progetto implementativo elaborato permette di sopperire ad alcune mancanze della licenza gratuita in maniera estremamente *cost effective*: il progetto rimane completamente gratuito, con licensing open source.
Gli unici compromessi riguardano la mancanza di funzionalità preferenziali, tra cui SSO e integrazione AD: si è valutato che non sarebbero comunque valse il prezzo di una licenza premium.

Il personale aziendale è in genere soddisfatto dalla soluzione indentificata e ne auspica una buona integrazione in azienda: la mancanza di un password manager era un problema da tempo sentito in maniera omogenea dai vari reparti.

Con l'intento di ottenere una panoramica più completa e capire lo stato dell'arte delle tecnologie offerte dai password manager moderni, il report è stato integrato con una breve ricerca delle soluzioni a pagamento. Ricordando la propensione mostrata in azienda per le soluzioni gratuite, si è voluto comunque volgere uno sguardo verso quelle a pagamento perlomeno per avere una stima dei diversi benefici che si ottengono o a cui si deve rinunciare.

Un riassunto sintetico delle soluzioni identificate finora si trova nelle tabelle presenti nelle pagine seguenti:

SOLUZIONI CLOUD-BASED (i fornitori del servizio provvedono a hosting e manutenzione)

Nome	Pro	Contro
Dashlane €8/m/u	• UI user friendly • Multipiattaforma • Include piano Family per i dipendenti	• Prezzo elevato (€8/m/u) • Integrazione AD e SSO poco sviluppata
Keeper (preventivo)	• Interfaccia discretamente user-friendly • Funzioni di condivisione con gruppi via cartelle • Multipiattaforma • Include piano Family per i dipendenti	• Prezzo a preventivo (serve il piano Enterprise per avere sync AD e SSO) • Mancanza di divisione netta fra elementi personali e condivisi
LastPass €5.7/m/u	• Interfaccia intuitiva e generale facilità d'uso, di configurazione e di amministrazione • Funzioni di condivisione con gruppi via cartelle • Include piano Family per i dipendenti • Alto rapporto qualità-prezzo • Integrazione con un eventuale account personale preesistente • Cloud con connector per sync	• Debole divisione fra elementi personali e condivisi
Bitwarden (versione a pagamento) ~€5/m/u	• Interfaccia estremamente semplice • Integrazione AD/SSO • Documentazione estensiva • Hosting incluso • Prezzo conveniente • Account famiglia incluso per gli utenti • Multipiattaforma	• Applicabilità non ai livelli di LastPass (Minore granularità delle impostazioni) • Periodo di prova molto limitato (7gg) con successivo addebito • Per ~200 utenze nessuno sconto sul volume (contattato reparto vendite)
Passwork €1.5/m/u	• Prezzo conveniente • Buona interfaccia e funzionalità	• Mancanza supporto AD

SOLUZIONI ON-PREMISES (ATON si occupa di hosting e manutenzione)

Nome	Pro	Contro
ManageEngine PM Pro (prezzo a preventivo)	• Basso prezzo • Prodotto parente di EventLog Analyzer, già usato • Divisione netta tra vault personale e aziendale	• Poco intuitivo, specie per un'utenza non tecnica • Autofill malfunzionante (come provato) • Sistema di condivisione ancora troppo legato all'utente
Password manager di Remote Desktop Manager (prezzo a preventivo)	• Prodotto parte di Remote Desktop Manager, già valutato per l'adozione in azienda	• Interfaccia estremamente complicata (progettata per l'uso con RDM da parte di un'utenza tecnica) • Per la nostra applicazione, per avere un'interfaccia più user-friendly, da adottare Password Hub (senza AD e SSO) oppure Password Server (on-premises) entrambi a pagamento. Ciononostante, resta progettato per l'uso da parte di utenza esclusivamente tecnica.
Bitwarden (versione a pagamento) *	• Interfaccia estremamente semplice • Integrazione AD/SSO • Documentazione completa • Hosting incluso • Buon prezzo ($5/m/u) • Account famiglia incluso per gli utenti • Multipiattaforma	• Applicabilità non ai livelli di LastPass (Granularità impostazioni minori) • Periodo di prova molto limitato (7gg) poi avviene direttamente l'addebito • Per ~200 utenze nessuno sconto sul volume (contattato reparto vendite)
Passwork (preventivo, acquisto in unica soluzione)	• Multipiattaforma • Buona interfaccia • Prezzo conveniente, soluzione con acquisto unico + aggiornamenti e supporto in abbonamento "opzionale"	• Diffusione limitata (ma fra i clienti presenti molti grossi nomi)
SOLUZIONI GRATUITE		
Passbolt	• Soluzione gratuita • Funzioni di condivisione (base) via gruppi	• Grandi limitazioni tecniche: nessuna sincronizzazione AD o integrazione SSO • Gestione dei gruppi rudimentale, amministrazione complicata
Bitwarden (versione grauita)	• Interfaccia estremamente semplice • Soluzione gratuita	• Nessun supporto AD/SSO • Nessuna funzione di condivisione/gruppi

CONCLUSIONI

Il prodotto della selezione sarà in futuro oggetto di ulteriore discussione in sede dirigenziale: vista l'inclusione delle soluzioni a pagamento, la scelta della suite da adottare coinvolge oltre ai reparti tecnici anche quelli finanziari dell'azienda. Tuttavia, il percorso di ricerca e selezione ha sempre incluso richieste di natura economica, risultate determinanti all'interno dell'intero percorso di analisi dei requisiti, ricerca e selezione.

Il lavoro svolto è infine stato oggetto di una dettagliata esposizione in conferenza con i diversi stakeholder di ATON finora coinvolti, i quali si sono ritenuti estremamente soddisfatti da quanto prodotto.

Il report nella sua versione finale, frutto di mesi di lavoro a stretto contatto con l'azienda e i suoi componenti, fornisce una panoramica quanto più estesa e al contempo dettagliata sull'intero percorso di analisi dei requisiti: prima concentrandosi sull'attuale situazione aziendale, evidenziandone bisogni e criticità, poi sulle diverse soluzioni al momento offerte dal mercato, poste a confronto con le necessità identificate dall'azienda, sia stabilite fin dall'inizio che emerse durante il percorso di analisi, identificando una soluzione candidata e proponendo un progetto d'integrazione.

BIBLIOGRAFIA E FONTI

Wikipedia: “ISO/IEC 27001”, <https://it.wikipedia.org/wiki/ISO/IEC_27001>, ultima consultazione 24/03/2022

Microsoft Docs: “Standard di gestione della sicurezza delle informazioni ISO/IEC 27001:2013”, <https://docs.microsoft.com/it-it/compliance/regulatory/offering-ISO-27001>, ultima consultazione 24/03/2022

ShieldQ: “ISO-27001 certification”, <https://www.shieldq.com/en/iso-27001-certification>, ultima consultazione 28/03/2022

Itgovernance.eu: “ISO 27001, lo standard internazionale della sicurezza delle informazioni”, <https://www.itgovernance.eu/it-it/iso-27001-it>, ultima consultazione 30/03/2022

Altalex: “GDPR: le sanzioni”, <https://www.altalex.com/documents/news/2018/04/04/gdpr-le-sanzioni-privacy>, ultima consultazione 1/04/2022

World Economic Forum: “Cybersecurity: How safe is your password?”, <https://www.weforum.org/agenda/2021/12/passwords-safety-cybercrime/>, ultima consultazione 3/04/2022

Portale d’aiuto Passbolt, <https://help.passbolt.com/>, ultima consultazione 20/04/2022

Nello svolgimento dell’attività si sono reperite la maggioranza delle informazioni dai siti delle rispettive suite, principalmente:

- https://www.dashlane.com/it/
- https://www.keepersecurity.com/
- https://www.lastpass.com/it
- https://bitwarden.com/
- https://passwork.pro/
- https://www.manageengine.com/
- https://devolutions.net/
- https://www.passbolt.com/

RINGRAZIAMENTI

Desidero ringraziare l'azienda ATON S.p.A. per avermi offerto questa opportunità di tirocinio in un ambiente professionale ma familiare.
Parte fondamentale dell'esperienza è stato il rapporto con i vari membri e colleghi dell'azienda: ringrazio tutti, in particolare Leonardo e Daniele per la loro compagnia, Igor per il supporto tecnico (e per la pazienza!), Michele per avermi guidato nella seconda parte del tirocinio e Giovanni per il supporto continuo ed amichevole in tutto il percorso di questa tesi.

Ringrazio il professor Mauro Migliardi per l'aiuto nella parte burocratica di questa esperienza e per gli ottimi consigli sulla stesura di questa tesi.

Ringrazio i miei cari compagni di corso, che hanno reso questi tre anni decisamente più felici. In particolar modo il mio amico Riccardo, senza cui non sarei giunto a questo punto e che mi ha sempre offerto ospitalità per tutte le proficue sessioni di studio congiunte. A tal fine, ringrazio anche Cinzia e Silvano per la generosità e la grande simpatia.

Ringrazio chi mi ha sostenuto: la mia famiglia, i miei parenti e la solita compagnia degli amici più cari.

Ringrazio chi mi ha spronato con le proprie parole ad intraprendere questo percorso: mia mamma Luciana e mio nonno Antonio.