Evidian

PROSPETTIVA

7 regole per un progetto SSO di successo

Basato su 15 anni di esperienza nell'ambito del single sign-on (SSO), questo libro bianco illustra best practice e insidie da evitare per una distribuzione di successo.

Distribuire un sistema SSO

L'SSO (single sign-on) rende gli utenti più produttivi, migliora la sicurezza, riduce i costi di help desk e facilita la conformità con i requisiti di legge.

Per ottenere questi risultati, però, un progetto SSO non può essere improvvisato. Solo una preparazione accurata assicura rapidità della distribuzione, rispetto degli obiettivi e adesione degli utenti al progetto.

In quasi 15 anni, Evidian e i suoi partner hanno distribuito centinaia di progetti SSO: questo documento rappresenta una sintesi della loro esperienza. Come potrete vedere, la maggior parte di queste regole d'oro riguardano l'organizzazione del progetto, al di là degli aspetti puramente tecnici.

1. **Stabilire** e condividere con chiarezza gli obiettivi di progetto
2. **Dimostrare** che il progetto migliorerà la conformità normativa
3. **Coinvolgere** attivamente gli utenti nel progetto
4. **Considerare** procedure e policy definite
5. **Puntare alla semplicità** in termini di architettura
6. **Pubblicare** con regolarità indicatori statistici
7. **Valutare** il raggiungimento degli obiettivi e pianificare l'ampliamento verso la gestione delle identità

Cos'è l'SSO?

L'SSO (*single sign-on*) consente l'accesso a tutte le applicazioni con un'unica modalità di autenticazione. Ad esempio, una password, un token USB o le impronte digitali, se si dispone di un lettore biometrico.

Tipicamente, un SSO utilizza sul PC un software non invasivo, che compila automaticamente le password delle applicazioni.

Se sono utilizzate solo applicazioni Web o si lavora in modalità thin client, il software SSO risiede su un server e inserisce le password da remoto. In questo caso, nessun software locale è necessario.

1. Stabilire e condividere con chiarezza gli obiettivi di progetto

In sintesi

Gli obiettivi di un progetto SSO di successo sono sempre molto concreti, ad esempio:

- Ridurre i costi di help desk
- Rendere gli utenti più produttivi: medici, commerciali, trader...
- Migliorare la sicurezza controllando l'accesso alle applicazioni critiche
- Rispettare leggi e regolamenti: riservatezza dei dati sanitari, PCI DSS (Payment Card Industry Data Security Standard)...

Ogni progetto SSO generalmente si prefigge uno o due obiettivi principali e alcuni obiettivi secondari precisi. È importante mettere nero su bianco i risultati concreti ottenuti.

Questo piano master SSO potrà essere soggetto a revisioni formali da parte dei partecipanti al progetto, o mediante decisione collettiva; i partecipanti possono essere esterni, come il fornitore del servizio, o interni: direzione finanziaria, controllo interno o gestione operativa.

Perché è importante?

Un obiettivo ben identificato e quantificato permette di avere sempre il supporto della dirigenza nel corso del progetto e servirà da riferimento per i partecipanti.

Il fornitore esterno può adeguare il suo lavoro per concentrarsi sulle priorità di business reali, o fornire suggerimenti per la loro realizzazione. A seconda degli obiettivi aziendali, certi strumenti e metodi saranno più adatti di altri.

Sarà garantita l'adesione della dirigenza, operativa o non, lavorando con quest'ultima per stimare i benefici attesi. Ciò faciliterà notevolmente la realizzazione del progetto e il coinvolgimento degli utenti.

Case study

Una società farmaceutica desiderava implementare un SSO. Il suo obiettivo concreto era la conformità alla legislazione statunitense. Il regolamento 21 CFR parte 11 richiede infatti di garantire che i documenti elettronici presentati alla Food and Drug Administration siano convalidati e firmati dai soggetti corretti.

Inizialmente, la società prevedeva di installare un SSO limitato alle applicazioni Web (il che richiedeva solo un gateway SSO sicuro). Tuttavia, rivedendo gli obiettivi di conformità con i responsabili operativi, il team di progetto ha rilevato che dalle applicazioni "client-server" derivavano numerosi rischi per l'integrità dei documenti. Dimostrare che il progetto migliorerà la conformità normativa

Evidian e il fornitore/integratore hanno quindi raccomandato l'implementazione di un SSO aziendale completo per le applicazioni client-server. Poiché questo approccio tiene conto anche delle applicazioni Web, sono stati raggiunti gli obiettivi funzionali iniziali, ma anche gli obiettivi di business reali.

2. Dimostrare che il progetto migliorerà la conformità normativa

In sintesi

Anche se l'obiettivo principale del SSO è operativo (produttività o riduzione dei costi, ad esempio) può essere utile interpellare il servizio di controllo interno. Un SSO, infatti, può consentire all'azienda di raggiungere obiettivi di conformità normativa, o di semplificare le procedure di controllo esistenti.

È facile comprendere perché l'SSO possa semplificare la vita agli utenti responsabili della conformità. In effetti, la maggior parte delle leggi e dei regolamenti sono volti a migliorare la riservatezza, l'integrità o la disponibilità delle informazioni.

- **Integrità**: l'SSO limita l'accesso alle risorse critiche, ad esempio finanziarie, ai soggetti il cui ruolo richiede tale accesso.
- **Riservatezza**: le applicazioni di gestione dei dati personali (cartelle cliniche, numeri di carte di credito) sono protetti dall'SSO. I log di accesso vengono conservati in una posizione centralizzata.
- **Disponibilità**: se la password dovesse essere dimenticata, PC e applicazioni restano disponibili attraverso un sistema di domande e risposte. ▪E l'SSO, se utilizza le directory esistenti, è facilmente incluso in un piano di disaster recovery.

Perché è importante?

L'inclusione della funzione di controllo interno nel progetto, anche a titolo consultivo, aumenta la credibilità dell'iniziativa. La conformità normativa è un obiettivo visibile della dirigenza, perché le sue implicazioni sono importanti per l'azienda.

Peraltro, fornendo il proprio parere nelle primissime fasi del progetto di distribuzione, il controllo interno è in grado di fornire suggerimenti di implementazione che saranno utili in seguito. Il modo in cui un SSO è implementato potrà facilitare il loro lavoro di controllo.

Case study

Una grande società di telecomunicazioni brasiliana desiderava implementare un SSO per rendere gli utenti più produttivi e adeguarsi alla normativa Sarbanes-Oxley, legislazione americana che mira ad assicurare l'integrità delle relazioni finanziarie.

Durante la preparazione del progetto, Evidian e il suo partner locale si sono consultati con il servizio di controllo interno del cliente, nonché con i revisori esterni. Questo esame ha evidenziato esigenze inizialmente non identificate.

Ad esempio, la verifica delle procedure di controllo avviene consultando i dati consolidati sull'accesso. I revisori hanno quindi richiesto che i dati SSO non venissero alterati, e che la loro origine fosse documentata sistematicamente.

Infine, il progetto ha definito procedure per la verifica delle informazioni raccolte, che hanno consentito di accelerare di alcuni giorni le verifiche annuali delle procedure di accesso.

3. Coinvolgere attivamente gli utenti nel progetto

In sintesi

I dipendenti sono i soggetti principalmente interessati dall'SSO. È quindi molto importante raccogliere le loro opinioni e tenerne conto nella distribuzione. Non è sufficiente interpellare i loro superiori!

È quindi necessario individuare le categorie di dipendenti più influenti. Questi utenti saranno diffidenti nei confronti di una novità come l'SSO, ma una volta convinti ne diventeranno il motore. Tutte le loro osservazioni consentiranno di anticipare le eventuali riluttanze nei confronti della distribuzione.

- Identificare i profili individuali cui l'SSO fornirà più vantaggi
- Tenere riunioni periodiche tra gli utenti pilota, con dimostrazioni
- Proporre loro di testare l'SSO in anteprima
- Non trascurare il fatto che alcuni potrebbero vedere l'SSO come un software "spia" sul PC
- Mostrare loro i vantaggi in termini di lavoro concreto, e non tecnici.

Perché è importante?

I dipendenti comprendono rapidamente i vantaggi apportati dall'SSO. Sarà quindi possibile trasformarli in promotori del progetto: gli utenti dell'SSO ne sono spesso i migliori sostenitori.

Viceversa, i commenti degli utenti consentono di scoprire e risolvere in anticipo eventuali blocchi. Ad esempio, un'applicazione fondamentale da considerare, esigenze locali, o bisogni inizialmente non identificati.

Case study

Una struttura ospedaliera francese desiderava fornire un'autenticazione unica al personale sanitario. In ambito ospedaliero, il tempo perso per inserire le password ha un impatto sulla qualità delle cure. Un SSO realizzato con l'aiuto del personale consente ai sanitari di dedicare più tempo ai pazienti.

Il team di progetto ha realizzato diverse demo rivolte ai rappresentanti del personale sanitario e ha condotto un test all'interno di un servizio.

È stato constatato che i medici, alcuni dei quali vedono il computer come una costrizione, desideravano che il sistema fosse il più discreto possibile. Per contro, apprezzavano l'accelerazione dell'avvio delle applicazioni, e il fatto che gli accessi fossero registrati. Allo stesso modo, gli infermieri si sono rapidamente adattati all'accesso SSO su un PC "mobile".

All'interno del reparto pronto soccorso, tuttavia, i medici hanno respinto il ricorso sistematico della smart card per l'autenticazione, che non facilitava la velocità di accesso. La soluzione è stata adottare una policy di sicurezza specifica all'interno del reparto pronto soccorso, basata su un time out della sessione e una funzione di roaming.

4. Considerare procedure e policy definite

In sintesi

Un SSO non è solo un "progetto tecnico": può cambiare la vita quotidiana delle organizzazioni e della loro gerarchia. La maggior parte di questi cambiamenti sono positivi.

Tuttavia, possono sorgere difficoltà quando i dirigenti scoprono di dover modificare le proprie procedure per tener conto dell'SSO. Ad esempio, può cambiare il modo in cui autorizzano ai dipendenti l'accesso alle applicazioni.

È quindi necessario garantire che questi cambiamenti siano ridotti al minimo e, quando siano inevitabili, anticiparli: meglio ancora, consentire a ogni organizzazione di pianificare progressivamente determinate tappe in base alle proprie esigenze.

Perché è importante?

Una distribuzione ben preparata, tramite il coinvolgimento dei responsabili di sede o di divisione, vi mette al riparo da imprevisti.

La riluttanza dei dirigenti in genere non è questione di inerzia: priorità e tempistiche non sono le stesse per tutti. Ad esempio, i responsabili finanziari o i commerciali preferiscono evitare di installare nuovi strumenti duante le fasi di chiusura del bilancio e dei forecast.

Anche se l'SSO semplifica le procedure (un'unica schermata gestisce l'accesso a tutte le applicazioni), bisogna però formare gli amministratori locali. Inoltre se una procedura esiste per motivi legali, è certamente documentata e verificata; modificarla avrà un costo.

Case study

Una società manifatturiera desiderava distribuire un sistema SSO su oltre 70.000 postazioni di lavoro. Malgrado il supporto all'SSO dei responsabili di divisione e di sede, è diventato presto evidente che tutti avevano priorità diverse e specificità di attuazione.

Pochi dirigenti erano disposti a modificare il proprio modo di gestire l'accesso alle applicazioni. Applicazioni come mySAP dovevano essere testate prima dell'integrazione nell'SSO, a scopo di conformità con la legislazione sulla sicurezza finanziaria.

La soluzione: definire, per ogni sito e organizzazione, da 10 a 20 applicazioni "base" da integrare immediatamente nell'SSO. Le applicazioni come mySAP sono state inizialmente escluse, per rispettare il ritmo delle organizzazioni. La decisione di "passare all'SSO" viene presa da ogni divisione.

Analogamente, l'SSO non modifica necessariamente l'amministrazione degli accessi. In una prima fase, si limita ad automatizzare l'accesso ad account già creati. La distribuzione dell'SSO è dunque avvenuta senza problemi, proprio perché ogni organizzazione era libera di definire autonomamente tempi e scelte: quali applicazioni integrare, quando farlo e come gestire i diritti di accesso.

5. Puntare alla semplicità in termini di architettura

In sintesi

Un progetto ha più probabilità di successo se il suo costo è ridotto e se c'è una buona integrazione nella tecnologia informatica esistente. È dunque necessario impiegare un'architettura più semplice possibile, ma non solo!

È importante sapere che la soluzione SSO di per sé rappresenta solo una parte dell'equazione. È necessario disporre inoltre di un elenco affidabile, e aggiornato, degli utenti. E, perché ogni utente lavori senza problemi, le informazioni SSO (password criptate, elenco delle applicazioni autorizzate...) devono risiedere in ogni sito primario.

Queste esigenze, però, non implicano necessariamente una soluzione complessa. Riutilizzando directory, server e risorse di rete già esistenti, il progetto può conseguire risparmi importanti in fase di installazione e di utilizzo.

Perché è importante?

Il controllo dei costi e della complessità di un progetto contribuisce al suo successo, perché consente di dimostrare più facilmente il ROI.

Probabilmente la vostra azienda dispone già di un repository di identità, ad esempio la directory LDAP: utilizzare nativamente anche questa risorsa e sfruttare le procedure esistenti per l'aggiornamento degli utenti.

Gli "appliance" consentono distribuzioni rapide su alcune centinaia di utenti; ma se la vostra azienda è organizzata su più sedi, si rischia di moltiplicare questi dispositivi hardware e anche il supporto associato. Utilizzando invece i database locali (directory) già esistenti, sfutterete al meglio il vostro hardware e le vostre competenze già acquisite.

Case study

Un ospedale britannico desiderava dotare di SSO i 5000 membri del personale sanitario e amministrativo. Gli obiettivi: ridurre i costi di help desk e tutelare l'accesso del personale sanitario tramite smart card. Naturalmente, l'alta disponibilità della soluzione è fondamentale in ambito ospedaliero.

E' stata installata una soluzione SSO basata su appliance. Tuttavia, a causa delle numerosi sedi e della complessità dell'organizzazione, l'ospedale ha constatato basse prestazioni e scarsa affidabilità. Prendendo in considerazione manutenzione e sostituzione, il costo di esercizio era superiore al previsto, e l'alta disponibilità non assicurata.

L'ospedale ha quindi preferito fare affidamento sull'archivio Active Directory esistente. Questo archivio, infatti, può ospitare agevolmente i dati SSO: non è stata necessaria l'aggiunta di nuovi componenti. I dati SSO sono così disponibili in ogni sede, vicino agli utenti; l'SSO è quindi più veloce. L'alta disponibilità dell'SSO coincide con quella già in essere per le directory; anche i piani di disaster recovery e le procedure di backup rimangono quelli già esistenti sempre per le directory.

6. Pubblicare con regolarità indicatori statistici

In sintesi

Come ogni progetto, anche l'SSO sarà oggetto di report di avanzamento. Ma la sua visibilità va al di là dell'IT: questi report devono essere comprensibili anche ai non tecnici, e contenere indicatori significativi anche per loro, ad esempio:

- Numero di PC su cui l'SSO è installato, utenti interessati
- Volume delle chiamate all'help desk e dei problemi risolti
- Dimensione e portata dei dati di auditing raccolti, funzionalità di sicurezza attivate
- Livello di soddisfazione degli utenti (questionario)
- Quantità di account applicativi dichiarati, in totale e per utente
- Numero di applicazioni considerate dall'SSO
- Numero di login "automatizzati" con stima del tempo guadagnato

I punti più tecnici sono ovviamente importanti, ma questi report sono strumenti di comunicazione e di monitoraggio. In molti casi, gli indicatori vengono raccolti da uno strumento di controllo automatizzato, il che facilita il lavoro di analisi e di ottimizzazione. In questo modo, diventa semplice, in generale, dimostrare il ritorno sull'investimento dell'SSO.

Perché è importante?

Questi report rendono visibili i progressi del progetto. Come abbiamo visto, sarà necessario conquistare la fiducia dei responsabili operativi, finanziari, dei revisori... che si aspettano risultati obiettivi: è importante fornirli in modo chiaro.

Non dimenticare che una distribuzione si svolge molto meglio con la partecipazione attiva dei reparti coinvolti. Una volta che le prime sedi sono state attivate, report e cifre concrete serviranno a convincere gli altri. E quando la distribuzione SSO sarà terminata, la credibilità acquisita vi permetterà di accelerare le ulteriori fasi... o altri progetti.

Case study

Nella filiale francese di una banca internazionale, la direzione sicurezza ha rilevato che la proliferazione delle password ha creato buchi di sicurezza e malcontento tra i 1200 dipendenti. È stato dunque avviato un SSO basato su tecnologia biometrica. Per ottenere l'OK al progetto, un argomento importante è stata la prevista riduzione dei costi di help desk.

Punti documentati hanno accompagnato la distribuzione. Dato che l'help desk è in outsourcing, è stato facile misurare l'evoluzione delle chiamate.

Valutando regolarmente le installazioni, il team di progetto ha rilevato che la diversità dei casi era superiore alle attese. È stato quindi deciso di dedicare tempo alla formazione degli utenti in relazione alla biometria e a risolvere i malfunzionamenti esistenti rivelati dall'SSO, ad esempio le password condivise.

7. Valutare il raggiungimento degli obiettivi e pianificare l'ampliamento verso la gestione delle identità

In sintesi

Al termine di un progetto SSO, è utile effettuare una valutazione circa la realizzazione degli obiettivi. Alcune questioni in sospeso, come l'autenticazione strong o la considerazione di nuove applicazioni, potranno essere oggetto di progetti futuri.

Evidian ha rilevato che i progetti SSO sono un ottimo punto di partenza per iniziative più ambiziose di gestione delle identità. In effetti, in capo a qualche mese si avrà a disposizione una preziosa base storica: quali account applicativi sono effettivamente utilizzati e da chi.

Perché è importante?

Un progetto SSO di successo offre l'opportunità di proporre passi successivi verso la gestione delle identità e degli accessi. Il motivo è semplice. Conoscendo oggi l'utilizzo reale delle applicazioni, è possibile definire una policy di sicurezza realistica. E prima di attuarla, è possibile prevedere quali saranno i suoi risultati.

Allo stesso modo, è possibile implementare il provisioning degli account, vale a dire il loro aggiornamento automatico, sotto il controllo di un circuito di approvazione. Le password di tali account saranno trasmesse all'SSO.

In questo modo, gli utenti si conformeranno naturalmente alla policy di sicurezza. I loro account saranno creati ed eliminati automaticamente in base al percorso compiuto in azienda.

Case study

Una grande azienda ferroviaria europea desiderava implementare una policy di sicurezza per gestire gli account di più di 150.000 utenti su 80 applicazioni, pari a più di un milione di account applicativi.

Aveva quindi avviato un inventario di tali account, che però si era rivelato irrealistico e costoso. Da un lato, la raccolta dei dati era stata più difficile del previsto; ma soprattutto, era difficoltoso stabilire chi usava un determinato account: un dipendente, un'intera squadra, nessuno? La società ha rapidamente compreso che, per continuare su questa via, sarebbero state necessarie migliaia di ore uomo.

Ha quindi preferito eseguire automaticamente un inventario degli account effettivamente utilizzati. A questo scopo, si è basata sul client SSO di Evidian. In questo modo, per 3 mesi sono state raccolte senza sforzo informazioni sull'impiego reale delle risorse informatiche. Ogni volta che un utente utilizzava un account, questo dato era inserito in un database centrale.

In una seconda fase, la società ha incrociato questo database con l'elenco degli account riportati nelle applicazioni. Questo ha permesso di rimuovere gli account obsoleti, e di costruire la propria policy di sicurezza su una base concreta.

Lo svolgimento del progetto SSO

Ogni progetto SSO è diverso, ma in generale tutti seguono lo stesso percorso. Si noti che, per una distribuzione su più di qualche centinaio di postazioni, è necessario affidarsi a un integratore.

1- Il modello

Prima di scegliere un fornitore, richiedete di testarne il prodotto su alcuni PC e su applicazioni rappresentative. Osservare le prestazioni: l'installazione è facile, l'integrazione delle applicazioni è semplice, cosa succederebbe in fase di produzione?

2- La pianificazione

Mettere per iscritto gli obiettivi concreti e funzionali. Fare un bilancio degli interlocutori interni con l'integratore, selezionare rappresentanti degli utenti. Eseguire un inventario delle sedi, delle applicazioni da integrare e dei requisiti specifici. Ne deriverà un calendario provvisorio.

3- Il pilota

Questo passaggio è importante: si tratta di scegliere un servizio rappresentativo. Ad esempio, provare il prodotto su 100 utenti per 30 giorni. Approfittare di questa fase per configurare l'SSO sulle applicazioni più comuni. E non dimenticare di fare un bilancio dettagliato e di trarne conclusioni utili per la distribuzione generale.

4- La distribuzione

In un primo momento, è necessario assicurarsi di avere una directory completa e affidabile degli utenti. Se non è così, esistono strumenti per creare e mantenere aggiornata questa fonte di informazioni.

In un secondo momento, l'installazione del client SSO sui PC avverrà gradualmente, ad esempio servizio per servizio. Informare chiaramente gli utenti in anticipo, proponendo corsi di formazione per alcuni di loro. Lasciare all'help desk il tempo di rispondere alle inevitabili domande prima di passare al servizio successivo.

Alla distribuzione, presentare periodicamente report fattuali ai responsabili gerarchici, che devono poter constatare i progressi del progetto e i risultati ottenuti.

5- Il bilancio

Al termine del progetto, redigere un bilancio della distribuzione. I punti ancora da trattare devono essere identificati e costituire l'oggetto di piani d'azione.

Questa è l'opportunità per pianificare le fasi successive, come la gestione delle policy di accesso o il provisioning degli account delle applicazioni.

Per ulteriori informazioni, visitare il sito www.evidian.com

39I2 33LV02