Evidian

PERSPEKTIVEN

7 Regeln für ein erfolgreiches SSO-Projekt

Dieses White-Paper basiert auf 15 Jahren Erfahrung mit Single Sign-On und beschreibt den Umgang mit möglichen Hürden um eine erfolgreiche Verteilung zu gewährleisten.

SSO in Ihrem Unternehmen

Single sign-on (SSO) erhöht die Produktivität der Benutzer, verstärkt die Sicherheit, senkt Helpdeskkosten und hilft rechtliche Auflagen zu erfüllen.

Ein SSO-Projekt sollte gut vorbereitet werden, um eine schnelle Umsetzung und das Erreichen der Projektziele unter Einbeziehung der Anwender zu gewährleisten.

Evidian und dessen Partner haben seit mehr als 15 Jahren eine Vielzahl von SSO-Projekten implementiert. Die Ergebnisse dieser jahrelangen Erfahrungen sind in diesem Dokument beschrieben. Die meisten dieser "goldenen Regeln" betreffen die Projektorganisation:

- Eine klare Definition und Diskussion der Ziele des Projektes
- Aufzeigen, dass das Projekt die Compliance-Einhaltung erfüllt
- Aktive Einbeziehung der Anwender am Projekt
- Berücksichtigung der bestehenden Richtlinien und Verfahren
- Ziel: eine einfache Architektur
- Regelmäßige Veröffentlichung von Statusreports
- Überprüfen der Ziele und die Erweiterung des Identity Management Planes

Was versteht man unter Single Sign-On?

Durch Single Sign-On oder SSO können Sie auf alle Ihre Applikationen durch die Verwendung einer einmaligen Authentifizierungmethode zugreifen, z.B. Passwort, USB Token oder Ihr Fingerabdruck, sofern Sie ein biometrisches Eingabeprogramm nutzen.In der Regel verwendet Single Sign-On eine diskrete Softwareanwendung auf einem PC, die Anmeldevorgänge an Anwendungen für den Nutzer übernimmt.

Wenn Sie nur mit Webanwendungen oder Thin Clients arbeiten, kann SSO von einem ausgelagerten Server aus die Anmeldung durchführen. In diesem Fall benötigen Sie keine lokale Installation.

1. Klare Definition und Diskussion der Ziele des Projektes

Zusammenfassend

Die Ziele eines erfolgreichen SSO-Projektes sind immer konkret, z.B.:

- Reduzierung der Helpdeskkosten
- Verbesserung der Produktivität der Anwender: Ärzte, Fachverkäufer, Händler, usw.
- Verstärkung der Sicherheit durch die Zugangsüberwachung zu kritischen Anwendungen
- Die Einhaltung von Gesetzen und Verordnungen: Ärztliche Schweigepflicht, PCI DSS, etc.

Im Allgemeinen hat jedes SSO Projekt ein oder zwei Hauptziele mit mehreren genauen Unterzielen. Die erwarteten Resultate sollten schriftlich definiert werden.
Die Teilnehmer können den SSO-Zielplan formal kommentieren. Es können auch gemeinsame Entscheidungen getroffen werden, zum Beispiel durch externe Teilnehmer, sowie Systemintegratoren und interne Teilnehmer: Finanzen, interne Kontrolle oder Operationsabteilungen.

Warum ist dies wichtig?

Ein klar definiertes Ziel mit Kostenabschätzungen hilft Ihnen, die Unterstützung Ihrer Verwaltung im Verlauf des Projekts zu bewahren, und kann als Referenz für Projektteilnehmer dienen.

Externe Dienstleister werden in der Lage sein, Ihre Anfragen zu bearbeiten, damit Sie sich auf die tatsächlichen Geschäftsprioritäten konzentrieren können bzw. Vorschläge machen, um ihre Verwirklichung zu gewährleisten. Je nach den wirtschaftlichen Zielen sind einige Tools oder Methoden besser geeignet als andere.
Sie stellen die Beteiligung einer Betriebsabteilung und eventuell weiterer Abteilungen sicher, indem Sie mit ihnen die erwarteten Vorteile bewerten. Dies wird die Durchführung des Projekts und der Beteiligung der Anwender erheblich verbessern.

Praktisches Beispiel

Ein Pharmakonzern führt eine Single Sign-On Lösung ein. Sein Hauptziel dabei lautet: Einhaltung der US Richtlinie 21 CFR Part 11, diese erfordert, dass in der Nahrungs- und Medikamentenverwaltung vorgelegte elektronische Belege von den richtigen Personen ausgewertet und unterschrieben werden.

Zunächst hatte das Unternehmen eine SSO Lösung nur für Webanwendungen geplant (dies erfordert ein sicheres SSO "Portal"). Während der Überprüfung der Ziele mit dem Operationsteam, stellten die Projektteilnehmer fest, dass viele Risiken bezüglich der Datenintegrität von Client-Server-Anwendungen verursacht werden.
Evidian und die Integrationsserviceanbieter empfahlen eine vollständige Enterprise SSO Lösung für die Client Server Anwendungen einzusetzen. Da dieser Ansatz auch Webanwendungen berücksichtigt, werden die ursprünglichen Ziele wie auch eine Verbesserung der Integrität erreicht.

2. Verbesserung der Compliance-Anforderung durch SSO demonstrieren

Zusammenfassend

Auch wenn das Hauptziel des SSO-Projektes den laufenden Betrieb betrifft, wie z.B. Produktivitätssteigerung und Kostensenkung, kann es nützlich sein, sich an die interne Verwaltung (Betriebsrat o.Ä.) zu wenden. In der Tat kann eine SSO-Lösung dem Unternehmen ermöglichen, die Einhaltung gesetzlicher Vorschriften oder die Vereinfachung der bestehenden Kontrollverfahren zu erreichen.
Die meisten Gesetze und Bestimmungen haben das Ziel, die Integrität, Vertraulichkeit und Verfügbarkeit von IT-Systemen zu verbessern. Es wird schnell klar, wie eine SSO-Lösung den Verantwortlichen helfen kann:

- **Integrität**: SSO begrenzt die Zugriffe auf kritische Ressourcen (z.B. finanzielle Ressourcen) auf Personen mit den benötigten Rechten.
- **Vertraulichkeit**: Anwendungen, die persönliche Daten verwalten (med. Daten, Kreditkarten, usw.) werden von SSO geschützt. Zugriffsprotokolle werden an einer zentralen Stelle abgespeichert.
- **Verfügbarkeit**: Wenn ein Kennwort vergessen wird, bleiben PCs und Anwendungen, dank eines Systems von Sicherheitsabfragen und Antworten verfügbar. Des weiteren lässt sich die SSO Lösung einfach in den bestehenden Notfallplan einbinden da schon vorhandene Verzeichnisse genutzt werden.

Warum ist dies wichtig?

Firmeninterne Controller in das Projekt mit einzubinden wird die Akzeptanz des Projektes erhöhen. Gesetzliche Bestimmungen sind auch für das Management von großer Bedeutung, da eine Nichteinhaltung gravierende Folgen für das Unternehmen haben kann. Beteiligte Controller können schon in der Anfangsphase des Projektes hilfreiche Empfehlungen für den späteren Verlauf geben. Im Gegenzug wird die Bereitstellung von SSO ihnen helfen ihre Auditaufgaben wahrzunehmen.

Praktisches Beispiel

Ein großes brasilianisches Telekommunikationsunternehmen wollte SSO bereitstellen, damit ihre Nutzer produktiver arbeiten können und um „Sarbanes-Oxley" einzuhalten. Dieses US-Recht erfordert die Integrität des finanziellen Reportings zu gewährleisten.
Bei der Vorbereitung des Projektes konsultierten Evidian und seine lokalen Partner sowohl die interne Operationsabteilung als auch externe Sicherheitsprüfer des Clients. Diese Beratung offenbarte weitere Bedürfnisse, die Anfangs noch nicht identifiziert worden waren.

Z.B. überprüfen Revisoren das Kontrollverfahren, indem sie konsolidierte Zugangsdaten ansehen. Die Prüfer forderten, dass SSO Daten unverändert bleiben, und dass ihr Ursprung systematisch dokumentiert werden muss.
Schließlich schrieb das Projektteam Verfahren zur Überprüfung der gesammelten Informationen. Dies ermöglichte, die jährlichen Prüfungen der Zugangsverfahren um einige Tage zu beschleunigen.

3. Aktive Einbeziehung der Anwender am Projekt

Zusammenfassend

Die Angestellten sind die wichtigsten Personen, die von einer SSO-Lösung betroffen sind. Somit ist ihre Meinung für die Umsetzung des Projektes von großer Bedeutung. Man sollte sich hierbei nicht allein mit Aussagen ihrer Manager zufrieden geben!

Deshalb sollten Sie die einflussreichsten Gruppen von Angestellten identifizieren. Anfangs eventuell etwas unsicher mit einer Veränderung wie SSO werden sie zu den stärksten Befürwortern sobald sie überzeugt sind. Alle ihre Beobachtungen werden es Ihnen erleichtern die Reaktionen der Anwender abzuschätzen.

- Identifizieren Sie Personen, die am meisten von SSO profitieren werden.
- Halten Sie regelmäßige Pilotnutzer-Treffen mit Demonstrationen ab.
- Ermutigen Sie diese, die SSO-Lösung schon vor der Freigabe zu testen.
- Beachten Sie die Tatsache, dass einige der Anwender SSO als "Spion" auf ihrem PC betrachten könnten.
- Präsentieren Sie ihnen die praktischen und nicht die technischen Vorteile.

Warum ist dies wichtig?

In der Regel verstehen Mitarbeiter schnell die Vorteile die ihnen SSO bietet. Sie können sie anschließend als Promotoren des Projekts nutzen: SSO Nutzer sind oft die besten Fürsprecher für dieses Thema.

Auf der anderen Seite können Anmerkungen der Anwender helfen, Pannen im Voraus zu erkennen und zu korrigieren. Sie werden frühzeitig kritische Anwendungen identifizieren können und auf lokale Anforderungen reagieren.

Praktisches Beispiel

Ein französisches Krankenhaus wollte Single Sign-On für seine Mitarbeiter einsetzen. Der Zeitverlust bei der Eingabe von Passwörtern hatte Auswirkungen auf die Qualität der medizinischen Versorgung. Single Sign-On in Kombination mit den Chipkarten der Angestellten ermöglicht es ihnen den Patienten mehr Zeit zu widmen.
Das Projektteam demonstrierte mehrere Lösungen und führte einen Test in einer Abteilung durch.

Einige Ärzte, welche Informationssysteme als Einschränkung betrachten, sprachen für ein möglichst diskretes System. Anderseits schätzten viele Ärzte das schnelle Starten von Anwendungen und die Tatsache, dass Zugriffe protokolliert werden. Außerdem erkannten Krankenschwestern schnell den Vorteil sich mit SSO anzumelden. Auf Notfallstationen wurde aber die systematische Verwendung von Chipkarten zur Identifikation abgelehnt, da diese die Zugriffsgeschwindigkeit verringere.

Die Lösung war eine Sicherheitsrichtlinie für die Notaufnahme auf Grundlage von grace period und der Möglichkeit eine Session über mehrere Rechner zu verwenden. Da der Zugang zur Notaufnahme physikalisch durch Chipkarten kontrolliert wird, war es möglich, Geschwindigkeit und Sicherheit zu kombinieren

4. Berücksichtigung bestehender Richtlinien und Verfahren

Zusammenfassend

SSO ist nicht nur ein "technisches Projekt": es kann das Alltagsleben eines Unternehmens verändern. Die meisten dieser Änderungen sind positiv.

Jedoch können einige Schwierigkeiten auftreten, wenn Manager entdecken, dass sie ihre gewohnten Abläufe ändern müssen, um SSO in Betracht zu ziehen. Zum Beispiel wenn sich die Art der Verteilung der Zugriffsrechte auf Anwendungen ändert.

Deshalb sollten Sie sicherstellen, dass diese Änderungen auf ein Minimum reduziert sind. Noch besser wäre es jeder Organisation zu erlauben, einige Phasen allmählich entsprechend ihrem eigenen Bedarf zu planen.

Warum ist dies wichtig?

Eine gut vorbereitete Verteilung mit der Beteiligung von Standort- oder Abteilungsleitern hat eine ausgezeichnete Erfolgswahrscheinlichkeit.

Zögerliches Verhalten bei Managern liegt häufig an unterschiedlichen Prioritäten und Terminen. Zum Beispiel vermeiden Finanz- oder Verkaufsabteilungen die Installation von neuen Hilfsprogrammen gegen Ende eines Geschäftsjahres.

Auch wenn SSO Verfahren vereinfacht - man kann den Zugriff auf alle Anwendungen von nur einem Bildschirm verwalten - müssen lokale Administratoren entsprechend trainiert werden. Sofern ein Prozess aus rechtlichen Gründen existiert, ist er dokumentiert und überwacht, Änderungen hier sind kostspielig.

Praktisches Beispiel

Ein Industrieunternehmen wollte SSO auf über 70,000 PCs verteilen. Die Abteilungs- und Betriebsleiter unterstützten das SSO Projekt. Jedoch wurde bald klar, dass jede der Abteilung verschiedene Prioritäten und Implementierungsansprüche hatte.

Nur wenige Manager stimmten zu, die Verwaltungsmethoden der Anwendungszugriffe anzupassen. Anwendungen wie mySAP mussten, gemäß der Sicherheitsrichtlinien der Finanzbranche, Tests unterzogen werden bevor sie mit SSO genutzt werden konnten.
Die Lösung: für jeden Standort sollten ca. 10 bis 20 Standardanwendungen sofort in SSO integriert werden. Anwendungen wie mySAP wurden zunächst von dieser Liste genommen, um die Gangart des Unternehmens zu berücksichtigen. Der Entschluss und der Zeitpunkt SSO einzuführen wurde von jeder Abteilung selbstständig getroffen.
Genauso ändert SSO nicht zwangsläufig die Art der Zugriffsverwaltung. Es kann auch, im ersten Schritt, nur den Zugang für bestehende Accounts automatisieren.

SSO wurde einwandfrei verteilt. Jede Abteilung bestimmte selbstständig den Zeitpunkt und den Umfang: welche Anwendungen integriert werden, wann sie integriert werden und wie die Zugriffsrechte verwaltet werden.

5. Ziel: Eine einfache Architektur

Zusammenfassend

Ein Projekt hat bessere Erfolgschancen, wenn seine Kosten niedrig sind und wenn es sich an die vorhandene IT-Umgebung gut anpassen kann. Deshalb sollte die Architektur so einfach wie möglich sein!

Bedenken Sie, dass eine SSO-Lösung selbst nur ein Teil des Konzepts ist. Sie brauchen eine zuverlässige und aktuelle Liste aller Benutzer. Außerdem müssen, um ungehindert arbeiten zu können, für jeden Benutzer die SSO-Informationen (verschlüsselte Kennwörter, Liste berechtigter Anwendungen, usw.) an jedem wichtigen Arbeitsplatz verfügbar sein.

Aber all diese Anforderungen erzwingen nicht unbedingt eine komplexe Lösung. Durch das Verwenden von schon vorhandenen Verzeichnissen, Servern und Netzwerkressourcen kann das Projekt beträchtliche Einsparungen während der Installation und im Betrieb machen.

Warum ist dies wichtig?

Die Kosten und die Komplexität eines Projekts zu kontrollieren, trägt zu dessen Erfolg bei. Somit lässt sich einfacher ein schnelles ROI belegen.
Ihr Unternehmen hat schon eine Benutzeridentitätsverwaltung: das LDAP-Verzeichnis. Sie könnten diese Ressource verwenden und von vorhandenen Benutzerupdate Verfahren profitieren.

Auf dieselbe Weise, können „appliances“ eine schnelle Verteilung für Hunderte von Benutzern ermöglichen. Aber, wenn Ihr Unternehmen in mehreren Standorten aufgeteilt ist, kann es sein, dass Sie mehrere diese Einheiten einsetzen müssen. Durch die Verwendung von bestehenden lokalen Datenbanken können Sie die Vorteile der lokalen Logistik und Kompetenz ausnutzten.

Praktisches Beispiel

Ein britisches Krankenhaus wollte SSO für seine 5000 Mitarbeiter im medizinischen Bereich und in der Verwaltung einsetzen. Die Ziele: Reduzierung der Helpdeskkosten und sichere Zugriffe über einen Mitarbeiterausweis gewährleisten. Natürlich ist eine hohe Verfügbarkeit der Anwendungen im Krankenhausumfeld zwingend erforderlich.

Eine Appliance-basierte SSO-Lösung wurde eingesetzt. Jedoch wurden im Krankenhaus einige Leistungs- und Zuverlässigkeitsprobleme bemerkt. Es wurde festgestellt, dass die Betriebskosten höher als geplant wären und Hochverfügbarkeit nicht garantiert werden könnte.
Daher entschied man sich die Architektur zu ändern und das vorhandene Active Directory zu verwenden. Dieses Verzeichnis kann SSO-Daten speichern ohne neue Hardware beschaffen zu müssen. Somit waren die SSO-Daten an jedem Standort verfügbar, und erlaubten eine schnelle SSO-Lösung. Die hohe Verfügbarkeit der SSO-Lösung entsprach der des Verzeichnisses. Des weiteren existierten schon Notfallpläne und Backupprozeduren: Ebenfalls die des ADs.

6. Regelmäßige Veröffentlichung wichtiger Ergebnisse

Zusammenfassend

Wie jedes Projekt, wird auch der Verlauf Ihres SSO-Projektes dokumentiert. Aber die Bedeutung von SSO geht über den IT Bereich hinaus: diese Berichte sollten deshalb auch für Nichttechniker verständlich sein und Fakten hervorheben, die für diese von Bedeutung sind. Zum Beispiel:

- Anzahl von PCs mit SSO-Lösung installiert, Anzahl an betroffenen Benutzern
- Anzahl von Helpdesk-Calls, gelöste Probleme
- Größe und Bereich von erfassten Auditdaten, aktivierte Sicherheitsfunktionen
- Benutzer Zufriedenheit Indizes (Umfragen usw.)
- Anzahl der angelegten Anwendungskonten (gesamt und pro Benutzer)
- Anzahl der Anwendungen die von SSO profitieren können
- Anzahl der automatisierten Anmeldungen mit einer Schätzung der gesparten Zeit

Weitere technische Punkte sind wichtig. Aber Berichte sind sowohl Kommunikation als auch Managementtools. In vielen Fällen erfasst ein automatisiertes Audittool die erforderlichen Fakten. Dies erleichtert die Analyse- und Optimierungsarbeit. Auf diese Art ist es im Allgemeinen leicht, den schnellen ROI von SSO zu demonstrieren.

Warum ist dies wichtig?

Berichte geben eine Übersicht über den Projektstatus. Sie müssen das Vertrauen von Finanzvorständen, Controllern usw. gewinnen, die objektive Ergebnisse erwarten: liefern Sie diese verständlich.
Vergessen Sie nicht, dass der Start leichter ist, wenn die betroffenen Abteilungen aktiv teilnehmen. Sobald die Lösung in den ersten Standorten und Abteilungen installiert ist, werden die daraus resultierenden Zahlen und Fakten die anderen überzeugen. Bis zum Ende des SSO-Deployments werden Sie genügend Vertrauen gewonnen haben, um zukünftige Phasen oder weitere Projekte zu beschleunigen.

Praktisches Beispiel

In der französischen Tochtergesellschaft einer internationalen Bank stellte die Sicherheitsabteilung fest, dass die Vielzahl an Kennwörtern Sicherheitslücken mitbrachte und die 1200 Mitarbeiter irritierte. So führte man ein SSO-Projekt mit biometrischer Authentifizierung ein. Eine wichtige Bedingung war der erwartete Rückgang der Helpdeskkosten.
Die Bereitstellung wurde von regelmäßigen Berichten begleitet. Durch den ausgelagerten Helpdesk war es leicht die Entwicklung der Anfragen zu verfolgen. Ein regelmäßiges Auswerten der Installationen zeigte, dass es mehr unterschiedlichere Konfigurationen gab als erwartet. Es wurde beschlossen mehr Zeit in die Schulung der Benutzer mit Biometrie und zum beseitigten bestehender Probleme zu investieren. Diese wurden durch SSO aufgedeckt, wie zum Beispiel gemeinsam genutzte Passwörter.
Dank dieser Nchuntersuchungen wurde das Budget nicht überschritten und SSO wurde durch die Back-Office-Dienstleistungen sehr gut angenommen. Die praktischen Erfahrungen halfen dabei die Muttergesellschaft zu überzeugen, das Tool global einzusetzen.

7. Überprüfen der Ziele und die Erweiterung des Identity Management Planes

Zusammenfassend

Am Ende eines SSO-Projektes sollte ermittelt werden ob die Ziele erreicht wurden. Noch ausstehende Punkte, wie z.B. starke Authentifizierung und Integration neuer Anwendungen, kann zu weiteren Projekten führen.

Für Evidian ist SSO ein guter erster Schritt hin zu ehrgeizigeren Identity-Management-Projekten. Denn nach ein paar Monaten werden Sie eine Datenbank mit nützlichen SSO Aktivitäten haben. Hierdurch wissen Sie, welche Anwendungskonten tatsächlich genutzt werden, und von wem.

Warum ist dies wichtig?

Ein erfolgreiches SSO-Projekt ist der Ausgangspunkt für ein Identity und Access Management. Der Grund dafür ist einfach. Da Sie jetzt wissen, wie Anwendungen verwendet werden, können Sie sinnvolle Sicherheitsrichtlinien definieren. Sie können somit schon vor der Umsetzung die Ergebnisse vorhersagen.

Sie werden in der Lage sein Zugriffsrechte zu verteilen ("provisionieren"), also eine automatische Aktualisierung unter Kontrolle des "approval workflow". Die erzeugten Accounts werden automatisch an die SSO Lösung übermittelt.

Die Konten der Benutzer werden, entsprechend der Sicherheitsrichtlinien, automatisch erstellt und gelöscht, abhängig von ihrem Status im Unternehmen.

Praktisches Beispiel

Eine große europäische Bahngesellschaft wollte eine Sicherheitspolitik implementieren, die mehr als 150,000 Benutzer und 80 Anwendungen umfasst (d.h. über einer Million Anwendungskonten).
Geplant war zuerst eine Inventur aller Konten vorzunehmen. Schnell wurde klar das dies teuer und sehr aufwendig sein würde. Es war schwierig die Accountdaten zu sammeln und dann stellte sich die Frage „Wer verwendet Account "sch002": Ein Angestellter, ein ganzes Team, niemand? Das Unternehmen realisierte schnell, dass auf diesem Weg Tausende von Arbeitsstunden nötig würden.

Stattdessen entschied sich das Unternehmen für eine automatische Inventur der tatsächlich verwendeten Konten. Evidian's SSO Client führte diese Aufgabe durch. Über drei Monate sammelte sie Informationen ohne weiteren Arbeitsaufwand. Jeder Benutzerzugriff auf eine Anwendung, wurde in einer zentralen Datenbank protokolliert.

In einer zweiten Phase verglich das Unternehmen diese Datenbank mit der Liste aller, in den Anwendungen erklärten, Konten. Dies ermöglichte dem Unternehmen, veraltete Konten zu entfernen und die Sicherheitspolitik auf eine beständige Grundlage aufzubauen.

Implementieren Ihres SSO-Projekts

Jedes SSO-Projekt ist anders, aber alle folgen demselben allgemeinen Muster. Beachten Sie, dass Sie schon für die Bereitstellung für ein paar Hundert PCs, auf Unterstützung durch Systemintegratoren zurückgreifen sollten.

1. Modell

Vor der Wahl des Anbieters bitten Sie diesen, sein Produkt auf einigen Ihrer PCs mit typischen Anwendungen zu installieren und zu testen. Achten Sie besonders auf folgende Punkte: ist das SSO-Tool schnell zu installieren, kann es Anwendungen leicht integrieren, lässt sich der Funktionsumfang im Einsatz ohne Aufwand anpassen?

2. Planung

Definieren Sie die funktionellen Ziele und die zugehörigen Kosten schriftlich. Fertigen Sie eine Liste von internen Gesprächspartnern mit dem Systemintegrator an und wählen sie einige Benutzervertreter. Erstellen Sie eine Inventarliste der Standorte und Anwendungen die integriert werden sollen inkl. der spezifischen Anforderungen. Dies wird Ihnen helfen, einen Zeitplan auszuarbeiten.

3. Pilotphase

Diese Phase ist wichtig und sollte in einer repräsentativen Abteilung implementiert werden. Lassen Sie das Produkt z.B. von 100 Benutzern für 30 Tage testen. Nutzen Sie diese Phase als Gelegenheit, die SSO Lösung für die wichtigsten Anwendungen zu konfigurieren. Vergessen Sie nicht detaillierte Bewertungen zu machen und verwenden Sie die Erfahrungen für den Einsatz im gesamten Unternehmen.

4. Einsatz

Zu allererst überprüfen Sie, ob Sie ein vollständiges und zuverlässiges Benutzerverzeichnis haben. Wenn dies nicht der Fall ist, gibt es Tools, die diese Informationsquelle erstellen und aktuell halten können.

Zweitens, sollte der SSO-Client Stück für Stück auf PCs installiert werden, z. B. je Abteilung. Informieren Sie den Anwender im Vorfeld und bieten Sie Trainings an. Geben Sie den Helpdesk einige Zeit, um die unvermeidbaren Fragen zu beantworten, bevor Sie sich mit der nächsten Abteilung beginnen.

Während der Bereitstellung sollten Sie den Managern regelmäßige Berichte erstellen. Sie müssen über den Fortschritt des Projektes und die erzielten Ergebnisse informiert sein.

5. Bewertung

Bewerten Sie den Einsatzbetrieb am Ende des Projektes. Die noch offenen Punkte müssen identifiziert und in Aktionsplänen das weitere Vorgehen beschrieben werden.
Nun haben Sie die Gelegenheit weitere Phasen, wie das Verwalten der Zugriffsrichtlinien oder das Provisioning für Anwendungsaccounts zu planen

Für weitere Informationen, besuchen Sie bitte www.evidian.com.

39 D2 33LV 01