



BESSERE ZUGANGSKONTROLL

Starke Authentifizierung mit ESSO

INHALTSVERZEICHNIS

Einführung	2
Starke authentifizierung auf dem vormarsch	2
Stellenwert einer sicheren zwei-faktor-authentifizierung mit esso.....	3
Führende authentifizierungsverfahren.....	4
Vergleich starker authentifizierungsmethoden	5
Wichtige, zu berücksichtigende faktoren.....	5
Kosten-nutzen-vergleich führender authentifizierungsmethoden	6
Integrieren einer starken authentifizierung mit esso	7
Integrationskosten und erforderliche ressourcen	7
Implementieren einer starken authentifizierung mit onesign	7
Kundenmeinungen zur starken authentifizierung mit onesign.....	9
Sicher in die sukunft	9

EINFÜHRUNG

Für Unternehmen jeder Art und Größe, die ihre IT-Sicherheit erhöhen und zugleich die Produktivität der Benutzer fördern wollen, hat sich ESSO (Enterprise Single Sign-on) im Laufe der letzten Jahre als einfache, intelligente und kostengünstige Lösung entwickelt. Aufgrund immer strengerer gesetzlicher Regelungen und Vorschriften suchen Unternehmen nach Wegen, ihre IT-Sicherheit durch starke Passwörter und oftmals auch durch eine zusätzliche Form der Identifizierung zu erhöhen, beispielsweise durch smart cards oder -Token oder sogar fingerbiometrische Verfahren.

Verwendet man neben einem Passwort einen weiteren Sicherheitsfaktor, ist eine zuverlässige und sichere Authentifizierung möglich. Jeder Computer im Netzwerk eines Unternehmens wird so mit einer wirkungsvollen Zugangskontrolle ausgestattet, die ihn noch besser vor unbefugten Benutzern schützt. Diese strikteren Sicherheitsmaßnahmen haben jedoch Auswirkungen auf das gesamte Unternehmen – sowohl auf alle Computerbenutzer als auch auf die Helpdesk-Mitarbeiter, die diese Benutzer betreuen. ESSO reduziert nicht nur den Aufwand für die Verwaltung der Vielzahl von Passwörtern, die für den Zugriff auf Anwendungen erforderlich sind, sondern arbeitet auch Hand in Hand mit einer starken Authentifizierung, um sicherzustellen, dass alle Zugänge zum Unternehmen so sicher wie möglich sind.

Doch welches Authentifizierungsverfahren ist für Sie und Ihr Unternehmen am besten geeignet? Und wie leicht lässt sie sich in Ihre ESSO-Lösung einbinden? Dies sind nur zwei der zahlreichen Fragen, die es zu bedenken gilt, wenn Sie die Alternativen für eine starke Authentifizierung beurteilen. Das vorliegende Strategiepapier befasst sich mit diesen Fragen und zeigt auf, wie Unternehmen eine starke Authentifizierung mit ESSO – einfach und kostengünstig – realisieren können, um ihr Sicherheitsniveau deutlich zu erhöhen, ohne dass IT-Mitarbeiter oder Endbenutzer hierdurch beeinträchtigt werden.

STARKE AUTHENTIFIZIERUNG AUF DEM VORMARSCH

Vor nicht allzu langer Zeit waren Authentifizierungstechnologien wie Scanner für biometrische Fingerabdrücke und smart cards ausschließlich in streng geheimen Regierungsbehörden und in James-Bond-Filmen anzutreffen. Doch mittlerweile sieht das anders aus. Laut IDC hatten das Identitäts- und Zugriffsmanagement im Jahr 2003 ein Marktpotenzial von 2,21 Milliarden US-Dollar, das 2008 voraussichtlich auf bis zu 3,5 Milliarden anwachsen wird. In einer kürzlich von Network Computing durchgeführten Umfrage gaben 62 % der Befragten an, dass sie über einfache Passwörter hinausgehende Sicherheitsmaßnahmen implementieren wollen.

Dieses steigende Interesse an einer starken Authentifizierung hat verschiedene Gründe, darunter:

Wachsende Zugriffszahlen

Firmeneigene IT-Umgebungen sind längst keine in sich geschlossenen Einheiten mehr. Immer mehr interne und externe Benutzer greifen lokal, host-basiert und Web-basiert auf firmeneigene Anwendungen zu, und es werden immer mehr Zugriffsmethoden und Gerätetypen genutzt. Hierdurch ist auch das Risiko durch unbefugte Zugriffe dramatisch angestiegen.

Wachsendes Bewusstsein

Angesichts gefährlicher Viren, Würmer, Spyware und sogar interner Attacken sind sich Unternehmensleitungen der sehr realen Bedrohung ihrer Informationsressourcen und der daraus entstehenden gravierenden Konsequenzen für den reibungslosen Geschäftsbetrieb, ihre Kundenbeziehungen und ihr Budget bewusst geworden.

Wachsende Regulierung

Innerhalb der letzten Jahre haben Regierungen auf der ganzen Welt eine Reihe neuer IT-Sicherheitsmaßnahmen und -prozesse verabschiedet, die Bestandteil von Gesetzen und Verordnungen sind (wie Gramm-Leach-Bliley, Sarbanes-Oxley und Health Insurance Portability & Accountability (HIPAA) in den USA sowie Data Protection Act in Großbritannien). Branchenspezifische Vorschriften wie Basel II, FDIC und die US-amerikanischen Code of Federal Regulations (CFR) sowie Industriestandards wie BS7799 in Großbritannien und BS7799-2 und ISO 17799 weltweit verlangen ebenfalls nach einer stärkeren Authentifizierung. Unternehmen und Vorstandsmitglieder sind für die Einhaltung dieser Vorschriften verantwortlich, da sonst mit Geldstrafen, rechtlichen Konsequenzen und/oder negativen Kundenreaktionen zu rechnen ist.

Auch Analysten raten dringend zu einer stärkeren Authentifizierung. Ein von Gartner veröffentlichter Bericht („Assess Authentication Methods for Strong System Security“, August 2004) gibt zwei primäre Empfehlungen zur Steigerung der Sicherheit und zur Reduzierung von Passwortproblemen: 1) Implementieren eines Passwortmanagements und 2) Verwenden einer sicheren Zwei-Faktor-Authentifizierung, auch „Starke Authentifizierung“ genannt.

STELLENWERT EINER SICHEREN ZWEI-FAKTOR-AUTHENTIFIZIERUNG MIT ESSO

Die zwingende Notwendigkeit für die Implementierung einer starken Authentifizierung (Zwei-Faktor-Authentifizierung) mit ESSO ist bereits auf den ersten Blick offensichtlich: Sie sorgt für einen höheren Schutz vor unbefugten Zugriffen. Wie der sichere Tresorraum in einer abgeschlossenen Bank bietet der zweite Authentifizierungsfaktor genau dort zusätzlichen Schutz, wo er am dringendsten benötigt wird.

Doch es gibt weitere, ähnlich überzeugende Gründe für die Implementierung einer Zwei-Faktor-Authentifizierung mit ESSO. Hierzu gehören:

Eliminierung von Passwörtern

ESSO reduziert deutlich die Probleme und Kosten, die mit dem Passwortmanagement verbunden sind. Durch Hinzufügen eines weiteren Authentifizierungsfaktors können Unternehmen ihren Benutzern den Umgang mit Passwörtern vollständig abnehmen. Gleichzeitig wird eine zuverlässigere Passwortkontrolle in die Hände der IT-Organisation gelegt. Ein Imprivata OneSign Kunde aus dem Gesundheitswesen berichtete kürzlich

„Wir planen, die Fingerabdruck-Biometrie für unsere Benutzer – Ärzte in der Notaufnahme, Pflegepersonal und Radiologen – so schnell wie möglich einzuführen. Das bedeutet, dass sie sich in Zukunft nur noch ihren Benutzernamen, aber keine Kennwörter mehr merken müssen. Dies erspart allen Beteiligten viel Zeit. Zudem gibt es uns die Möglichkeit, Kennwörter im Back-End zu erstellen und zu verwalten, wodurch die Sicherheit weiter erhöht wird.“

---Stefan Hopper, Chief Information Officer, Gateway Health System

Schnellere und höhere Rentabilität

Die Implementierung einiger Authentifizierungstechnologien kann sehr teuer sein, sodass die Rechtfertigung der Kosten für manche Unternehmen schwierig ist. Durch die Kombination aus preisgünstigem ESSO und einem stärkeren (oder zweiten) Authentifizierungsfaktor erzielen Unternehmen eine höhere und schnellere Rentabilität, da sie von den zusätzlichen Vorzügen und Kosteneinsparungen der Passwortverwaltung (z. B. niedrigere Helpdesk-Kosten und höhere Produktivität der Benutzer) profitieren.

Nachweisbare Einhaltung von Vorschriften

Einige Unternehmen haben Maßnahmen (z. B. starke Kennwortrichtlinien) zur Einhaltung von Bestimmungen wie HIPAA und Sarbanes-Oxley implementiert. Ein objektiver, dokumentierter Nachweis, dass diese Maßnahmen befolgt und durchgesetzt werden, fehlt jedoch. Daher besteht für sie weiterhin das Risiko, als nicht konform eingestuft zu werden. Eine starke Authentifizierung mit ESSO kann dagegen die Einhaltung von

FÜHRENDE AUTHENTIFIZIERUNGSVERFAHREN

Mit steigender Nachfrage nach starken Authentifizierungsverfahren nimmt auch die Zahl der angebotenen Lösungen zu. Folgendes sind die gängigsten Authentifizierungsverfahren, die derzeit im Einsatz sind:

Passwörter

Passwörter sind das älteste und einfachste Authentifizierungsverfahren, das sich durchsetzte, weil sie einfach und relativ wirkungsvoll waren. Solange die Benutzer ihre Passwörter geheim hielten, waren die Anwendungen vor unbefugten Zugriffen geschützt. Da es jedoch immer mehr Anwendungen gab, die Passwörter erfordern, mussten sich die Benutzer zahlreiche Passwörter merken. Hinzu kam, dass die von den Benutzern festgelegten Passwörter häufig zu einfach waren, mehrmals verwendet wurden oder leicht zu erraten waren.

Starke Passwörter

Viele Unternehmen wollten das Problem zu einfacher Passwörter dadurch beheben, dass sie die Verwendung starker Passwörter vorschrieben – sie verlangten komplexere Passwörter, die nicht nur Buchstaben, sondern auch Ziffern und Sonderzeichen enthalten. Leider sind starke Passwörter oftmals so komplex, dass die Benutzer sie sich nicht merken können, was einen drastischen Anstieg teurer Anrufe beim Helpdesk zur Folge hat. Dies wirkt sich wiederum negativ auf die Produktivität der Benutzer aus, da sie von ihrer Arbeit abgehalten werden, während sie auf das Zurücksetzen ihrer Passwörter warten. Schlimmer noch: Die Benutzer tendieren dazu, die Kennwörter auf Zettel zu schreiben, die gestohlen und von Unbefugten verwendet werden können.

ID-Token

ID-Token sind kleine Geräte, die numerische Codes generieren, die für einen befristeten Zeitraum oder die einmalige Verwendung Zugriff gewähren. Einige ID-Token-Systeme erfordern als zusätzliche Schutzmaßnahme, dass der Benutzer einen Challenge-Code in das Token eingibt, bevor der Passcode generiert wird. Oftmals muss für die Zwei-Faktor-Authentifizierung zusätzlich zum OTP (Onetime Password – einmaliges Passwort) eine PIN eingegeben werden. Führende Anbieter von ID-Token sind RSA, Secure Computing und Vasco.

Smart cards

Wie ihr Name schon sagt, besitzen smart cards eine integrierte Intelligenz. Sie können eine Fülle von Daten für die Authentifizierung und Sicherheit enthalten. Smart cards sind nicht manipulierbar und können mehrere Funktionen erfüllen. So kann eine einzige Smartcard als Mitarbeiter-ID-Ausweis, Karte für den Gebäudezutritt, Windows Credential Store (Anmeldeinformationsfenster) und zur Bereitstellung von Passwörtern für Anwendungen dienen. Unternehmen wie ActivCard, Axalto und Gemplus bieten smart cards an. USB-Token dieser und anderer Hersteller wie Aladdin stellen eine intelligente und benutzerfreundliche Sicherheitsalternative dar, die kein Lesegerät erfordert.

Passive Proximity-Cards

Ähnlich wie smart cards sind passive Proximity-Cards Chipkarten für die kontaktlose Zugriffskontrolle, die Authentifizierungsdaten via RF-Technologie (Radiofrequenzen) bereitstellen. Wird eine passive Proximity-Card in die Nähe eines Kartenlesers gehalten und bewegt, liest das Gerät die Benutzerdaten der Karte, um den Karteninhaber zu identifizieren. Wie bei smart cards kann die passive Proximity-Technologie in traditionelle Mitarbeiter-ID-Ausweise und Karten für den Gebäudezutritt integriert werden. Passive Proximity-Cards werden von Unternehmen wie HID, MIFARE und Indala angeboten.

Aktive Proximity-Cards

Aktive Proximity-Cards enthalten einen drahtlosen Sender, den der Benutzer bei sich trägt. Dieser Sender steht in ständiger Kommunikation mit einem Empfänger, der mit der Workstation des Benutzers verbunden ist, wenn sich der Benutzer in der Nähe befindet. Entfernt sich der Benutzer von seiner Workstation, wird die Kommunikation unterbrochen und der Computer automatisch gesperrt. Auf diese Weise wird die Zugriffskontrolle rund um die Uhr sichergestellt. Einer der führenden Anbieter von aktiven Proximity-Cards ist Ensure, Hersteller der XyLoc-Karte.

Fingerbiometrische Verfahren

Die Fingerbiometrie identifiziert den Benutzer mithilfe von unverwechselbaren Merkmalen: seinen Fingerabdrücken. Die Benutzer registrieren den Abdruck eines oder mehrerer Finger mit einem Scanner, der bestimmte Charakteristika des Fingerabdrucks aufzeichnet, die den Identifikationsdaten jedes Benutzers zugeordnet sind. Danach wird der Finger des Benutzers bei der Anmeldung eingescannt und mit den vorhandenen Mustern verglichen, um die Authentifizierung durchzuführen. Fingerbiometrische Verfahren werden von Unternehmen wie UPEK angeboten und verstärkt in Produkte wie Tastaturen, Mäuse und Laptops integriert.

Alle oben genannten Authentifizierungsmethoden können dazu beitragen, unbefugte Zugriffe auf firmeninterne Informationssysteme zu verhindern. Es gibt jedoch weitere Aspekte, die zu bedenken sind, darunter die speziellen Vorteile jeder Methode für Benutzer und IT-Abteilungen, die Einhaltung von Vorschriften sowie die Anschaffungs- und Implementierungskosten. Wenn Sie diese Vorteile und Kosten kennen und im Hinblick auf die Anforderungen Ihres Unternehmens auswerten, können Sie die starke Authentifizierungsmethode wählen, die Ihre Zwecke am besten erfüllt.

VERGLEICH STARKER AUTHENTIFIZIERUNGSMETHODEN

Jedes Unternehmen will unbefugte Zugriffe auf seine Informationsressourcen verhindern – und alle Unternehmen können vom Einsatz einer starken Authentifizierung profitieren. Doch die individuellen Anforderungen sind vielseitig. Hier einige Beispiele:

- Eine Gesundheitsorganisation benötigt eine Authentifizierungsmethode, die die gemeinsame Nutzung von Workstations erlaubt und zugleich vertrauliche Patientendaten gemäß dem Health Insurance Portability & Accountability Act (HIPAA) schützt. Wenn das Büro klein oder mittelgroß ist, muss die starke Authentifizierungslösung preisgünstig sowie einfach zu implementieren und zu nutzen sein.
- Ein großer börsennotierter Finanzdienstleister benötigt eine Methode, die sich auf kosteneffektive Weise unternehmensweit implementieren lässt. Außerdem muss die Konformität mit Absatz 404 des Sarbanes-Oxley Act sichergestellt sein, der interne Kontrollen zum Schutz der Integrität von Mechanismen zur Finanzberichterstattung und eine Möglichkeit zum Nachweis der Qualität dieser Kontrollen vorschreibt.
- Ein Technologieunternehmen mit umfangreichem intellektuellem Kapital benötigt eine strenge Kontrolle des Zugriffs auf Forschungs- und Entwicklungsdateien, muss möglicherweise aber auch komfortablen und sicheren Fernzugriff für Außendienstmitarbeiter bereitstellen.
- Eine Strafverfolgungsbehörde benötigt eine Methode, die in einer offenen Büroumgebung leicht von Mitarbeitern verwendet werden kann, die nicht ständig am Schreibtisch sitzen.

WICHTIGE, ZU BERÜCKSICHTIGENDE FAKTOREN

Es ist wichtig, dass Sie sowohl den individuellen Sicherheitsbedarf Ihres Unternehmens als auch die Vorzüge und Kosten unterschiedlich starker Authentifizierungslösungen berücksichtigen. Hierzu gehören:

WICHTIGE, ZU BERÜCKSICHTIGENDE FAKTOREN

Es ist wichtig, dass Sie sowohl den individuellen Sicherheitsbedarf Ihres Unternehmens als auch die Vorzüge und Kosten unterschiedlich starker Authentifizierungslösungen berücksichtigen. Hierzu gehören:

IT-Vorteile

Lässt sich die Authentifizierungsmethode leicht unternehmensweit implementieren? Sind zusätzliche IT-Ressourcen erforderlich? Kann sie auf einfache Weise in vorhandene ESSO-Lösungen integriert werden? Unterstützt sie eine zentralisierte Verwaltung?

Benutzervorteile

Ist die Authentifizierungsmethode benutzerfreundlich? Werden die Endbenutzer den neuen Prozess akzeptieren? Steigert die Methode die Produktivität der Benutzer? Stellt sie für die Benutzer eine übermäßige Belastung dar? Müssen die Benutzer ein Gerät mit sich führen, das verloren gehen oder beschädigt werden könnte?

Konformitätsvorteile

In welchem Umfang unterstützt die Authentifizierungsmethode die Vorschriften von Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, CFR, Basel II, des britischen Data Protection Act oder BS7799? Geht sie über die einfache Zugriffskontrolle hinaus, indem sie Authentifizierungsereignisse protokolliert, um Prüfanforderungen und objektive Nachweise der Konformität zu unterstützen?

Branchenspezifische Vorteile

Weist die Authentifizierungsmethode Aspekte auf, aufgrund derer sie sich besser für bestimmte Branchen oder Funktionsbereiche eignet?

Anschaffungskosten

Rechtfertigen die zu erwartenden Verbesserungen der Sicherheit die Kosten der Authentifizierungsmethode? Gibt es Kosten pro Benutzer, die jedes Mal steigen, wenn ein neuer Benutzer hinzugefügt wird?

Implementierungskosten

Erfordert die Implementierung, dass Techniker die Lösung auf jeder Workstation an jedem Standort installieren? Muss die IT-Organisation angepassten Code schreiben, Middleware hinzufügen oder entstehen weitere Hardware- oder Softwarekosten, um die starke Authentifizierungsmethode mit ESSO zu integrieren?

Die folgende Matrix zeigt einen Vergleich der Authentifizierungsmethoden auf Basis dieser wichtigen Faktoren:

Kosten-Nutzen-Vergleich führender Authentifizierungsmethoden

Methode	Einfache Verwaltung* für IT	Einfache Nutzung für Mitarbeiter	Konformität/ Sicherheitsniveau	Anschaffungskosten	Implementierungskosten pro Benutzer
Passwort	Mittel	Mittel	Niedrig	€	€
Starkes Passwort	Niedrig	Niedrig	Mittel	€	€ €
ID-Token	Mittel	Mittel ¹	Hoch	€ €	€ €
Smart Card and USB Token	Niedrig ²	Mittel ¹	Hoch	€ €	€ € €
Passive Proximity	Mittel	Mittel ¹	Niedrig ³	€ € € ⁴	€
Aktive Proximity	Mittel	Hoch ⁵	Niedrig	€ € € €	€ €
Fingerbiometrische	Hoch	Hoch	Hoch	€ € €	€

*Zeit und Ressourcen, die aufgewendet wurden, um die Technologie zu implementieren und zu warten oder Endbenutzer zu unterstützen.

ANMERKUNGEN:

1. Gerät muss vom Benutzer getragen werden und kann verloren gehen oder beschädigt werden.
2. IT muss Geräte verwalten, die oft verloren gehen, vergessen oder versehentlich beschädigt werden.
3. Sofern diese nicht mit einem weiteren Authentifizierungsfaktor kombiniert wird
4. Karten sind preiswert, erforderliche Lesegeräte jedoch nicht.
5. Fingerabdrücke können nicht verloren gehen oder vergessen werden.

Durch eine Kosten-Nutzen-Analyse der verschiedenen starken Authentifizierungsmethoden können Sie ermitteln, welche Methode die Anforderungen und Präferenzen Ihres Unternehmens am besten erfüllt. Hier einige Beispiele:

- Wenn die Benutzerfreundlichkeit für die Mitarbeiter und IT-Beauftragten höchste Priorität hat, sind möglicherweise aktive Proximity-Cards die richtige Wahl.
- Wenn Ihr Unternehmen groß ist oder schnell wächst, ist es u. U. ratsam, die Implementierungskosten pro Benutzer durch Auswahl passiver Proximity-Cards niedrig zu halten.
- Wenn Ihr Unternehmen einer Branche angehört, bei der höchste Sicherheit unerlässlich ist, und die Benutzerzahl klein oder kein übermäßig großes Wachstum zu erwarten ist, sind smart cards oder ID-Token möglicherweise die richtige Wahl.
- Wenn Ihre Sicherheitsanforderungen je nach Standort oder Abteilung unterschiedlich sind, empfiehlt sich möglicherweise die Implementierung mehrerer Authentifizierungsmethoden basierend auf der Erfahrung und dem Bedarf der Benutzer.

INTEGRIEREN EINER STARKEN AUTHENTIFIZIERUNG MIT ESSO***Integrationskosten und erforderliche Ressourcen***

Die Auswahl einer Methode für die starke Authentifizierung in Ihrem Unternehmen ist nur der erste Schritt, um ein hohes Sicherheitsniveau beim Zugriff auf Unternehmensdaten sicherzustellen. Damit die Vorzüge einer starken Authentifizierungslösung optimal genutzt werden, müssen Sie diese mit einer starken, intelligenten und preisgünstigen ESSO-Lösung integrieren.

Bei einigen ESSO-Lösungen erfordert die Implementierung einer starken Authentifizierung zusätzliche Software, Server, Middleware, Unterstützung und Benutzeroberflächen. Hinzu kommt, dass einige ESSO-Lösungen nur bestimmte Formen der Authentifizierung unterstützen.

Implementieren einer starken Authentifizierung mit OneSign

Imprivata OneSign® ist anders. Imprivata OneSign ist eine preisgünstige Appliance, die keine Veränderungen der Infrastruktur erfordert und ESSO für alle Anwendungen bereitstellt – Web, Client/Server und traditionelle Anwendungen. Durch einen einzigartigen, zentralisierten Ansatz beim Passwortmanagement sorgt OneSign dafür, dass sichere SSO-Services schnell implementiert und einfach verwaltet werden können. So profitieren die Kunden von mehr Produktivität, optimierter Richtlinieneinhaltung durch die Benutzer und niedrigeren Helpdesk-Kosten.

Mit OneSign können Unternehmen jeder Größenordnung einfach und mühelos Passwortrichtlinien einführen und durchsetzen, denn OneSign ist speziell auf die Zusammenarbeit mit der ganzen Bandbreite an Authentifizierungslösungen ausgerichtet. Beispielsweise beschreiben die folgenden Schritte den gesamten Prozess der Implementierung eines fingerbiometrischen Verfahrens und der Registrierung eines Benutzers mit OneSign:

1. Schließen Sie einen Fingerabdruckscanner an den USB-Anschluss des PCs an.
2. Befolgen Sie die angezeigten Anleitungen. Es ist nicht erforderlich, Treiber zu installieren.
3. Fahren Sie den Computer herunter und starten Sie ihn neu, um eine OneSign Authentifizierung durchzuführen.
4. Folgen Sie den OneSign Aufforderungen, um einen oder mehrere Fingerabdrücke zu registrieren.
5. Scannen Sie den Finger, wenn Sie dazu aufgefordert werden.
6. Klicken Sie auf „Fertig“.

Für alle nachfolgenden Benutzeranmeldungen gilt:

1. Der Benutzer legt den Finger auf den Fingerabdruckscanner, der an den PC angeschlossen ist.
2. Der Benutzer wird mithilfe des registrierten Scans identifiziert und erhält Zugriff auf das Netzwerk.

Eine starke Authentifizierung lässt sich mit OneSign einfach und schnell realisieren.

OneSign unterstützt nicht nur die einfache Integration zusätzlicher Formen der Authentifizierung, sondern bietet zudem folgende Vorteile:

Nahtlose Integration

Unternehmen können OneSign implementieren, ohne dass Änderungen an vorhandenen Anwendungen oder am Anmeldeverhalten der Benutzer erforderlich sind.

Plug&Go-Installation

OneSign befindet sich in einem sicheren 1HE-Gehäuse, das für die Rack-Montage geeignet ist, sodass keine zusätzlichen Kosten entstehen (eine redundante Einheit wird mitgeliefert).

Unterstützung von Passwortrichtlinien

Die Kunden können Unterstützung für eindeutige Passwörter festlegen und die Passwörter automatisch im Hintergrund ändern.

Unterstützung für Sicherheitsrichtlinien

Unternehmen können unterschiedlichen Benutzern oder Benutzergruppen unterschiedliche Sicherheitsrichtlinien zuordnen.

Unterstützung für gemeinsame Credentials (Anmeldeinformationen)

Kunden können Anwendungen in Gruppen verwalten, die einen gemeinsamen Credential-Store (Anmeldeinformationsspeicher) nutzen.

Unterstützung für gemeinsame Workstations

Mehrere Benutzer können gleichzeitig an einer gemeinsamen Workstation angemeldet sein – vorheriges Abmelden ist nicht erforderlich.

Zugriffsprotokolle

Sicherheitsbeauftragte können Anwendungs- oder Zugriffsprotokolle überwachen, um festzustellen, welcher Benutzer wann auf welche Anwendung zugreift.

Selbst aktualisierender Agent

Diese Funktion erleichtert die Implementierung und Aktualisierung, ohne dass zusätzlicher Verwaltungsaufwand entsteht.

Integration von Geschäftsprozessen

Angepasste Arbeitsabläufe können mit SSO-Implementierungen werden. Beispiele hierfür sind personalisierte Nachrichten, Automatische Verbindungen von Benutzerverzeichnissen auf workstations, Bereitstellen dynamischer Roaming-Sitzungen usw.

KUNDENMEINUNGEN ZUR STARKEN AUTHENTIFIZIERUNG MIT ONESIGN

Ein OneSign Kunde beschreibt die Erfahrungen seines Unternehmens bei der Implementierung der starken Authentifizierung mit ESSO wie folgt:

„Es war denkbar einfach, OneSign in unsere biometrische Implementierung für die starke Authentifizierung einzubinden. Wir haben das System so konfiguriert, dass OneSign die Passwörter der Benutzer automatisch im Hintergrund ändert. Dies erhöht die Sicherheit, da die Passwörter komplex sind und aus bis zu 32 Zeichen bestehen können – von unseren Benutzern können wir nicht verlangen, dass sie sich so lange Passwörter merken. Hinzu kommt, dass die Benutzer ihre Kennwörter selbst nicht kennen und demzufolge auch nicht weitergeben können.“

*--- Steve Siress, Network Systems Manager
Enterprise Bank & Trust of St. Louis & Kansas City*

SICHER IN DIE ZUKUNFT

Durch Erstellen einer starken Authentifizierungslösung mit Imprivata OneSign steht Ihnen eine effiziente, einfache und preisgünstige Methode zur Verfügung, mit der Sie die Empfehlungen von Gartner umsetzen und ein Passwortmanagement implementieren und gleichzeitig die Zwei-Faktor-Authentifizierung nutzen können.

Wenn sich die Sicherheitsanforderungen künftig erhöhen, haben Imprivata OneSign Kunden die Gewissheit, dass sich ihre ESSO-Lösung bei Bedarf in eine Vielzahl von Authentifizierungsverfahren einbinden lässt.

Weitere Informationen zur einfachen Implementierung einer starken Authentifizierung mit OneSign erhalten Sie auf der Website <http://www.imprivata.com> oder telefonisch bei Imprivata unter der Nummer 1-800-ONESIGN oder 1-408-987-6072.



Niederlassungen in:
Belgien • Deutschland
Italien • Singapur
Großbritannien • USA

www.imprivata.com

WP-MSFD-GER-Ver2-0808