WHITEPAPER

Das Geheimnis verbundener Business-Systeme: Darstellung der ersten 5 entscheidenden Schritte

ZUTRITTSKONTROLLLE, SICHERER AUSDRUCK UND ANDERE WICHTIGE SYSTEME FÜR EIN BESSERES UND SICHERES BENUTZERERLEBNIS.

Der verbundene Arbeitsplatz
Der verbundene Arbeitsplatz ermöglicht es dem Arbeitgeber, die Identität des Arbeitnehmers einmal zu verifizieren und ihm dann Zutritt zu zahlreichen Systemen zu bieten – mit seiner vertrauenswürdigen Identität kann er so nahtlos auf völlig unterschiedliche Systeme zugreifen. Diese plattformübergreifende Identitätsabhängigkeit führt zu mehr Sicherheit und Komfort beim Zugriff.

Vertrauenswürdige Identität
Eine validierte Identität, die unter Verwendung von Biometrie oder Zugangsdaten auf einer Karte, einem Mobiltelefon oder einem tragbaren Gerät bereitgestellt wird.

Die Möglichkeit, sich beim Betreten eines Gebäudes zum Beispiel mit einer Smartcard zu legitimieren, galt vor Jahren als revolutionär. Inzwischen gibt es technisch hochentwickelte Methoden der Zugangskontrolle, so dass Menschen ihre Zugangsdaten benutzen können, um Gebäude zu betreten, um Zeit und Anwesenheit genau zu erfassen, sicher zu drucken usw. – so entsteht ein Gesamtsystem, das wir den verbundenen Arbeitsplatz (Connected Workplace) nennen.

Unternehmen profitieren von dem erhöhten Komfort und der Sicherheit durch die Verbindung mehrerer Systeme und Identitäten. Ihre Mitarbeiter erfreuen sich an der schnelleren Bewegung im gesamten Gebäude, der Nutzung flexibler Arbeitsplätze und der Bequemlichkeit von bargeldlosen Cafeterien und Verkaufsautomaten. Die Zunahme an verbundenen Arbeitsplätzen hat viele Hersteller von Business-Systemen mit einer wachsenden Nachfrage nach identitätsabhängigen Systemen konfrontiert – aber wo sollen sie ansetzen?

Dieses Whitepaper stellt die wichtigen erst fünf Schritte dar, durch die Business-Systeme identitätsabhängig werden, um Herstellern klar und deutlich zu zeigen, wie sie ihren Kunden die besten Dienstleistungen anbieten. Sie werden die Schlüsselfragen und die wichtigsten Überlegungen zur Sicherstellung der problemlosen Installation und Einführung von Identitätsprüfungsgeräten in einem Business-System kennenlernen.

Die Anzahl identitätsabhängiger Systeme ist in den letzten Jahren angestiegen. Zu den beliebtesten Einsatzmöglichkeiten von Identitätsnachweisen gehören:

Zeit und Anwesenheit
Schnelle und sichere An- und Abmeldung, niemand kann mehr „für Kollegen stempeln“

Sicheres Drucken
Sicherer Ausdruck von Dokumenten auf Abruf zur Kostensenkung und zur Verbesserung der Datensicherheit

Aufzug-/Drehtürsteuerung
Zutritt zu geschützten Bereichen und Verkürzung der Wartezeiten

Parkplatzmanagement
Schnelle Zu- und Ausfahrt auf Parkplätzen und Einlass für Besucher

Authentifizierung von Netwerkbenutzern
An- und Abmeldung an flexiblen Arbeitsplätzen, Vereinfachung der Zusammenarbeit und sicherere Fortbewegung

Verwaltung von Besprechungsräumen
Gewährung oder Verweigerung des Zugangs zum Besprechungszimmer für Besucher und Mitarbeiter

Schritt 1: Bewertung der aktuellen Organisationsanforderungen und Infrastruktur

Eine gründliche Untersuchung der aktuellen Möglichkeiten eines Unternehmens ist ein wichtiger erster Schritt. Idealerweise funktioniert eine Lösung in einem bestehenden System reibungslos und ohne größere Überholungen und Nachrüstungen. Noch besser ist es, wenn identitätsabhängige Lösungen von Anfang an in die Infrastruktur des Unternehmens integriert werden können. Bei der Bewertung der aktuellen Infrastruktur sollten Sie berücksichtigen:

Aktuelle Funktionen für vertrauenswürdige Identität. Wie werden vertrauenswürdige Identitäten derzeit benutzt und verwaltet? Lesegeräte greifen bei jeder Nutzung auf eine Datenbank zu, Unternehmen verfügen jedoch über unterschiedliche Richtlinien, die festlegen, welche Anwendungen mit welchen Datenbanken in Verbindung treten können. Es kann erforderlich sein, dass Sie mit dem Sicherheitsbeauftragten eines Kunden zusammenarbeiten müssen, um festzulegen, mit welchem Business-System auf eine zentrale Datenbank zugegriffen wird und ob ein neues Business-System geschaffen werden muss. Eine weitere Möglichkeit besteht darin, dass sich Benutzer selbst registrieren und schließlich selbst eine völlig neue Datenbank erstellen. Identitätsabhängige Lösungen wie Seos® von HID ermöglichen den Zugriff auf mehrere Anwendungen mit einer Karte.

Verfügbare Stellfläche für neue Lesegeräte. Ist ausreichend Platz vorhanden? Karten und Biometrie erfordern Lesegeräte zur Überprüfung der Identität. Berücksichtigen Sie, wie viel physischen Platz es für die Lesegeräte gibt, wie sie angebracht werden können und ob sie sich innerhalb oder außerhalb des Geräts befinden sollen. Manchmal hat ein Drucker im Inneren Platz für ein Lesegerät oder einen Chipsatz, oder er benötigt ein Lesegerät, das als separate Einheit in der Nähe aufgestellt wird.

Konnektivität. Auf welche Weise kommuniziert das Lesegerät mit der Datenbank? Jedes Lesegerät authentifiziert eine Karte, extrahiert die Kontrolldaten und gibt diese Daten an die verwendete Einheit weiter. Wie erfolgt diese Kommunikation und welchen Sicherheitsgrad erfordert sie? Welche Art von Hardware, Software und Kommunikationsprotokollen wird benötigt? Die heute gebräuchlichsten Optionen sind USB, UART (Universal Asynchronous Receiver Transmitter), Wiegand für die Konnektivität und die Protokolle CCID (Chip Card Interface Device) und KBW (Keyboard Wedge) für den Datentransfer.

Materialien zur Unterbringung von Geräten. Welcher Platz ist innerhalb des Geräts und/oder in der Umgebung verfügbar? Die Smartcard-Technologie funktioniert am besten in einer Freiluftumgebung, in der es keine zusätzlichen Gehäuse gibt, die die Kommunikation möglicherweise blockieren. Sollen Lesegeräte umbaut werden, so lässt Kunststoff Signale viel leichter passieren als Metall. Kundenspezifische Nachrüstungen sind möglich, können aber die Leistung beeinträchtigen. Bei biometrischen Messungen ist das Material weniger wichtig.

Stufe Zwei: Feststellen, was die Benutzer wünschen

Unternehmen erwarten, dass die Technologie problemlos *und* verlässlich funktioniert. Nehmen Sie sich die Zeit, herauszufinden, was Arbeitnehmer und Arbeitgeber wirklich brauchen, um die beste Lösung zu finden. Zu den allgemeinen Aspekten zählt beispielsweise:

Geschwindigkeit. Mit welcher Geschwindigkeit muss ein Lesegerät die Identität bestätigen? Das hängt vom Anwendungsfall ab. In extrem stark gesicherten Bereichen sind möglicherweise weitere Verifizierungsebenen nötig, z. B. das vollständige Einlegen einer Karte zuätzlich zu einem Fingerabdruckscan über einen biometrischen Authentifikator. In weniger gesicherten und stark besuchten Bereichen, wie z. B. dem Eingangsbereich, müssen die Mitarbeiter möglicherweise schnell durch eine Drehtür gehen und dabei eine Flash-Karte oder ein Mobiltelefon aus kurzer Entfernung nutzen oder kurz ein Wearable antippen.

Lesebereich. Wie nahe muss die Karte bei dem jeweiligen Anwendungsfall am Lesegerät sein? Lesegeräte können Karten und Geräte aus unterschiedlichen Entfernungen und mit verschiedenen Sicherheitsgraden überprüfen. Beispielsweise sind einige Lesegeräte so konzipiert, dass sie den Aufenthaltsort der Mitarbeiter erfassen, wenn diese ihre Legimitation am Körper tragen. Ein Ausweis muss dann nicht mehr vorgezeigt werden. Lesegeräte in Hochsicherheitsbereichen erfordern möglicherweise, dass eine Karte lang genug eingelegt wird, um mehrere Datenschichten zu übertragen. Dabei ist zu beachten, dass bei der Lesereichweite Wahrnehmung und Realität voneinander abweichen können – beispielsweise kann ein Mitarbeiter beeindruckt sein, dass er Zugang erhält, sobald er sein Telefon an das Lesegerät hält, aber in Wirklichkeit hat das Lesegerät das Signal seines Telefons bereits aufgenommen und mit der Überprüfung begonnen, als er einige Meter entfernt war.

Erfahrung des IT-Administrators. Hat das Unternehmen des Kunden ein solides und erfahrenes IT-Team? Häufig haben kleinere Unternehmen nicht die Personalstärke, um neue Datenbanken zu erstellen und zu verwalten oder neue Chipsätze zu installieren. Größere Unternehmen sind eventuell auf die Möglichkeit einer Aktualisierung per Fernzugriff angewiesen, da sie Tausende von Lesegeräten aktualisieren müssen, aber nicht Tausende von Technikern beschäftigen können.

Schritt Drei: Aktuelle Technologien kennen und nutzen
Die Technologie entwickelt sich ständig weiter, daher sollte ihre Beurteilung sowohl die aktuellen Möglichkeiten als auch Pläne für die Zukunft berücksichtigen. Das Ziel ist es, weitgehend mit dem zu arbeiten, was in einem Unternehmen bereits verwendet wird. Identitätsabhängige Systeme müssen daher Pläne für die Zukunft in bereits vorhandene Modelle einbinden. Mobiler Zugriff ist dabei einer der Schlüsselmomente – selbst wenn ein Unternehmen derzeit keine mobilen Geräte zur Authentifizierung verwendet, wird dies wahrscheinlich bald der Fall sein. Die meisten Unternehmen verwenden Kombinationen dieser gängigen Technologien:

RFID. Radio Frequency Identification ist eine weit verbreitete Technologie zur Identifizierung von Karten und Wearables und die vorherrschende und weitreichendste Sicherheitsoption.

NFC. Near Field Communication unterstützt die Zugangskontrolle für Karten, Mobilgeräte und Wearables.

BLE. Bluetooth Low Energy wird hauptsächlich zur Standort- und Zustandsüberwachung eingesetzt und ermöglicht den Zugriff über Mobilgeräte und Wearables.

Biometrie. Trotz der komplexen Integration ist dies die sicherste (und oft auch praktischste) Lösung, da man nichts mitnehmen oder dabeihaben muss.

Mobiler Zugriff
Mit mobilem Zugriff wird das Smartphone oder die Smartuhr eines Mitarbeiters zum Türöffner. Durch den Zugriff auf Systeme und Anlagen über Mobilgeräte sorgen Unternehmen für ein hohes Maß an Sicherheit und Komfort.

Schritt Vier: Herausfinden, welcher Formfaktor für das Lesegerät der Anwendung am besten ist.
Die Komplexität von identitätsabhängigen Systemen kann sehr unterschiedlich sein, ebenso auch die Möglichkeiten von Unternehmen. Am Vorteilhaftesten ist es, die technischen Möglichkeiten mit dem leitenden Ingenieur oder externen Auftragnehmer zu besprechen, um zu beurteilen, ob eine fertige Lösung geeignet wäre oder selbst ein System entwickelt werden soll. Für das Lesegerät gibt es folgende Möglichkeiten:

Lesegerät mit Chipsatz. Ein Chipsatz oder Secure-Element-Prozessor (SE) ist der kleinste gemeinsame Nenner aller identitätsabhängigen Produkte und gehört zu jedem Lesegerät. Unternehmen mit erfahrenen Technikern konzipieren die Platinen für ein Business-System so, dass der Chipsatz des Lesegeräts bereits darauf enthalten ist. Biometrische Authentifizierung wird von Lesegeräten mit Chipsatz nicht unterstützt.

Lesegerät mit Core. Diese Kombination aus Chips und Core-Komponenten ermöglicht einem Lesegerät (aber nicht den Antennen) die Kommunikation über RFID, BLE usw., unterstützt jedoch keine Biometrie. Lesegeräte mit Core werden bevorzugt von Herstellern verwendet, die ihre eigene Antenne so einrichten möchten, dass sie sich für das vorhandene Gebäude eignet.

Lesegerät mit Modul. Das Modul für das Lesegerät beinhaltet den Chipsatz und die Antennen, muss aber innerhalb des vorhandenen Business-Systems untergebracht werden. Lesemodule für Karten und Biometrie lassen sich nahtlos integrieren, damit das System identitsabhängig wird

Desktop-Lesegeräte. Dabei handelt es sich um ein völlig separates Gerät, das normalerweise auf dem Desktop oder einem vorhandenen Gerät angebracht wird. Desktop-Lesegeräte wie OMNIKEY® von HID Global sind praktisch schlüsselfertig und erfordern nur wenig Kenntnisse, nehmen aber viel Platz ein.

Schritt Fünf: Konzeption und Integration des Lesegeräts mit den bereits vorhandenen Geräten
Vor allem ist beim Auswahl- und Integrationsvorgang immer zu berücksichtigen, dass das aktuelle Gerät (der Drucker, der Aufzugsschalter oder die Zeituhr, für die das neue Lesegerät konzipiert wird) seine Funktionsfähigkeit behalten muss. Das neue identitätsabhängige System sollte die Benutzerfreundlichkeit erhöhen, und nicht die Komplexität. Folgendes ist zu beachten:

Backend-Kommunikation. Datenbank, Lesegerät und Zugangskarte müssen miteinander Daten austauschen können.

Ästhetik. Im Idealfall wird das Lesegerät als Teil des bestehenden Geräts wahrgenommen, nicht als zufällig angebracht oder unvorteilhaft nachgerüstet.

Tests und fortlaufender Support. Entwicklungs-Toolkits werden zusammen mit Testkarten für eine Vielzahl von Systemen geliefert, mit denen Administratoren vor dem Einsatz in der Praxis die Benutzerfreundlichkeit überprüfen können. Wir von HID Global bieten darüber hinaus über unser Portfolio an professionellen Dienstleistungen für Extended Access Technologies (EAT) kontinuierlichen Support für Originalhersteller, Integrators und Direktkunden.

Fazit

Erweitern Sie die Infrastruktur von heute für die Bedürfnisse von Morgen.

Eine vertrauenswürdige Identität mehrfach nutzen zu können, ist praktisch und benutzerfreundlich. Außerdem spart es auf lange Sicht viele Kosten und Frustrationen und reduziert den Spielraum für menschliche Fehler. Das Beste von allem: Die Integration bisher voneinander getrennter Systeme muss nicht mit einem vollständigen technologischen Umbau gleichbedeutend sein – der verbundene Arbeitsplatz kann auf der vorhandenen Infrastruktur aufbauen, genau auf die Bedürfnisse des jeweiligen Unternehmens zugeschnitten und entsprechend abgerechnet werden.

HID Global bietet ein vielfältiges Portfolio an Lesegeräten und Karten für jede Branche, mit Support und Service bei jedem Schritt. Weitere Informationen zu den Vorteilen eines identitätsabhängigen Business-Systems finden Sie in unserem Executive Brief *Der vernetzte Arbeitsplatz*, klicken Sie hier, oder besuchen Sie unsere Webseite.

2019-03-16-hid-eat-make-bus-syst-id-aware-wp-de

PLT-04748