Security
Technologien

Der elektronische Mitarbeiterausweis
Zentrale Bereitstellung von Sicherheitsmechanismen

Autoren: **Dr. Chandima Costa, Dr. Harald Ritter**
Version: **1.0**

Zusammenfassung:
Die moderne Arbeitswelt ist geprägt von digitalen Prozessen. Zugriffe auf die unterschiedlichen Systeme eines Unternehmens erfolgen häufig über Zugangskennungen der Mitarbeiter. Der Einsatz eines elektronischen Mitarbeiterausweises kann diese Zugangskennungen System übergreifend vereinheitlichen und die zugehörigen Prozesse entscheidend vereinfachen. Zusätzlich zu diesem Einsparungspotential erhöht sich die Sicherheit für das Unternehmen. Das vorliegende Dokument analysiert diesen Nutzen und beschreibt die zu Grunde liegenden Technologien sowie mögliche Anwendungsgebiete eines elektronischen Mitarbeiterausweises.

NOVOSEC
Aktiengesellschaft

Sulzbacher Straße 29-39
65824 Schwalbach am Taunus
Telefon 06196/88289-0
Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

NOVOSEC Aktiengesellschaft

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

Traum oder Wirklichkeit?

Montag, 9:00 Uhr: Mitarbeiter M. erscheint an seinem Arbeitsplatz und schließt sein Notebook an das Netzwerk an. Er möchte seine eMails lesen, vorliegende Bestellungen eingeben und ein paar Berichte drucken, um für das 10-Uhr-Meeting präpariert zu sein. Einmal angemeldet und durchgängig authentifiziert, entfallen lästige weitere Passworteingaben für die unterschiedlichen Applikationen. Keine Zeitverluste durch ständige Anmeldungen. Keine vergessenen Passwörter. Vorbei sind die Zeiten, als man für jede Anwendung Freischaltungen brauchte und diese bei unterschiedlichen Administratoren beantragen musste, die zufällig gerade nicht anwesend, sondern zum Admin-Training waren!

Montag, 10:00 Uhr: Meeting. Der Beamer ist angeschlossen. Powerpoint-Dateien präsentieren, zwischendurch mal im Internet was nachschauen. Und dann noch einen Blick auf die Verkaufs-Statistiken der letzten Woche werfen! Das Team ist berechtigt, die eigenen Verkäufe sowie die Gesamtverkäufe anderer Teams zu sehen.

Montag, 11:00 Uhr: Die neue Kollegin kommt. Deren schönste Begrüßung: Sie erhält nur eine Zugangsberechtigung. Hiermit kann sie auf alle Applikationen und Daten zugreifen, für die sie berechtigt ist. Es war denkbar einfach, diese Berechtigung zu organisieren: Eine eMail, unterzeichnet von der Betreuerin der Neuen. Keine Laufzettel, keine Unterschriften, keine Lauferei und Warterei. Da freut man sich besonders auf die neue Kollegin, und die sich natürlich auch.

Montag, 12:30 Uhr: Mittagspause. Die Arbeitsplatzrechner bleiben verwaist, aber gesichert zurück. Keine Chance für Unbefugte, ins Netz zu kommen!

Montag, 14:00 Uhr: Kundentermin. Rasch mal während des Gesprächs ins Firmennetz einwählen, Auskünfte einholen, dann die Bestellung eingeben. Der Zugriff erfolgt über VPN; die Bestellung wird authentisiert und vom Verkäufer namentlich gekennzeichnet. Die Verbindung für den Zugriff ist verschlüsselt und damit sicher. Die Transaktion ist verbindlich, nachvollziehbar und revisionssicher.

Montag, 18:00 Uhr: Sachbearbeiter M. befindet sich bereits auf dem Heimweg. Der Auftrag von 14:00 hat ein sattes Volumen, bedarf aber noch der Bestätigung durch den Vorgesetzten. Dieser bekommt den Vorgang automatisch zur Weiterverarbeitung, signiert digital und freut sich nicht nur über den schönen Auftrag, sondern besonders auch über den effizienten Workflow. Keine Ablage, keine Unterschriftsmappen, kein Suchen nach Dokumenten und Federhaltern!

Montag, 18:15 Uhr: Der Chef geht nach Hause und wundert sich über die kurzen Arbeitszeiten.

Der Traum könnte bereits heute in Ihrem Unternehmen Wirklichkeit sein! Vereinheitlichte Administration, zentrale Nutzerverwaltung, Single Sign-On, hierarchische Rollenkonzepte, erhöhte Zugriffssicherheit – alles machbar mit einem elektronischen Mitarbeiterausweis.

Wie kann dieser gestaltet sein? Muss es eine Chipkarte sein? Reicht ein einheitliches Passwort? Wie komplex ist die benötigte Infrastruktur? Eine pauschale Antwort gibt es nicht. Es gibt jedoch Basistechniken, mit denen jeder elektronische Mitarbeiterausweis ausgestattet ist, sowie Standardabläufe zu deren Verwaltung.

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

Basistechnologie

Die grundlegenden Technologien, die stets durch einen elektronischen Mitarbeiterausweis bereitgestellt werden müssen, sind Mechanismen zur Verschlüsselung und Authentisierung.

Verschlüsselung

Die am stärksten genutzten Mittel zur elektronischen Kommunikation sind die E-Mail und das World Wide Web. Vor allem innerhalb eines Unternehmens werden zunehmend mehr Daten per E-Mail ausgetauscht oder auf Servern hinterlegt. Häufig sind diese Daten vertraulich. Eine Verschlüsselung verhindert das Mitlesen durch Unbefugte.

Authentisierung

Unter einer Authentisierung versteht man die Vorlage eines Nachweises, in dem bestätigt wird, dass eine Person (bzw. ein Rechner etc.) tatsächlich diejenige ist, die sie vorgibt zu sein. Ohne Authentisierung und die damit verbundene eindeutige Feststellung der Identität des Kommunikationspartners ist eine vertrauenswürdige elektronische Kommunikation über offene Netze nicht möglich.

Transaktionsfreigabe

Soll eine Transaktion ausgelöst werden, für die eine explizite Willenserklärung benötigt wird, so ist eine Transaktionsfreigabe erforderlich. Diese kann z.B. mittels einer elektronischen Signatur erfolgen.

Elektronische Signatur und Zertifikate

Eine Möglichkeit zur Implementierung der genannten Mechanismen besteht in der Verwendung von elektronischen Signaturen und Zertifikaten. Die elektronische Signatur gewährleistet die Authentizität der Nachrichten, der Einsatz digitaler Zertifikate erlaubt auch die Überprüfung der Identität des Kommunikationspartners. Qualifizierte elektronische Signaturen sind dabei per Gesetz rechtsverbindlich; bei anderen elektronischen Signaturen kann eine Verbindlichkeit durch vertragliche Regelungen erreicht werden.

Die „Verschlüsselung“ wird beispielsweise von Sachbearbeiter M. eingesetzt, wenn er die Bestellung beim Kunden vor Ort eingibt und in das Firmennetz übermittelt. Greift M. auf vertrauliche Dokumente, wie z.B. die Statistiken der letzten Woche, innerhalb des Firmennetzes zu, authentisiert er sich gegenüber dem Server.

Der Einsatz dieser Technologien kann Vorgänge innerhalb einer Firma beschleunigen und dem Mitarbeiter eine einfache, komfortable und damit effiziente Möglichkeit der Arbeitsabwicklung bieten. Der Mitarbeiter darf dabei nicht mit Fragen zu technischen Problemen wie etwa zur Installation, Wartung und Anwendung belastet werden. Wie aber werden diese Technologien dem Mitarbeiter am Besten zur Verfügung gestellt? Wie sehen die erforderliche Infrastruktur und die Abläufe innerhalb eines Unternehmens aus?

Abläufe

Für den Einsatz eines elektronischen Mitarbeiterausweises in einem Unternehmen sind folgende Abläufe erforderlich:

- Erstellung/Verwaltung der Mitarbeiterausweise
- Festlegung/Administration des Berechtigungsmodells
- Steuerung der Authentifizierung

Erstellung/Verwaltung der Mitarbeiterausweise

Die Aufbereitung der Mitarbeiterdaten aus unterschiedlichen Datenbeständen im Unternehmen (Personaldaten, Zugangsberechtigungsdaten, etc.) stellt den ersten Schritt zur Erstellung eines elektronischen Mitarbeiterausweises dar. Zusätzlich werden Funktionalitäten zum Sperren und Erneu-

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

ern von Mitarbeiterausweisen benötigt, um die Mitarbeiterausweise zentral zu verwalten.

Festlegung/Administration des Berechtigungsmodells
Für jedes Unternehmen wird in Anlehnung an die Unternehmensstruktur und die Geschäftsprozesse ein Berechtigungsmodell definiert. Auf Basis dieses Modells werden für jeden Mitarbeiter je nach Aufgabe und Rolle Berechtigungen definiert und verwaltet. Anhand dieser Berechtigungen lässt sich der Zugriff des Mitarbeiters auf die Applikationen bzw. Geschäftsprozesse steuern.

Steuerung des Workflows
Um die Workflows beim Einsatz des elektronischen Mitarbeiterausweises effizient steuern zu können, sollte eine Trennung zwischen Authentifizierung des Mitarbeiters und der Prüfung bzw. Gewährung von Berechtigungen erfolgen. Bei der Authentifizierung wird anhand der im Mitarbeiterausweis enthaltenen Daten festgestellt, um welchen Mitarbeiter es sich handelt. Nach Feststellung der Identität des Mitarbeiters wird auf Basis des vorher festgelegten Berechtigungsmodells ermittelt, ob er die Berechtigung für die gewünschte Applikation verfügt. Um die Revisionssicherheit und Nachvollziehbarkeit zu gewährleisten, sollten die Authentifizierungsdaten protokolliert werden.

Anwendungen

Ein elektronischer Mitarbeiterausweis kann für zahlreiche Aufgaben unterschiedlichster Ausprägung verwendet werden, von denen einige im Folgenden exemplarisch erläutert werden.

Zugangskontrolle
Nur autorisierte Mitarbeiter dürfen bestimmte PCs in der Firma nutzen (*Zugangskontrolle zu Rechner und Server*).

Außerdem sollen Applikationen und Daten innerhalb einer Firma oftmals nur einem eingeschränkten Mitarbeiterkreis zur Verfügung gestellt werden (*Zugangskontrolle auf Daten über Netze*).

VPN-Zugang
Ein virtuelles privates Netzwerk ermöglicht z. B. Außendienstmitarbeitern den gesicherten Zugang von außen zu allen erforderlichen Informationen und Geschäftsprozessen.

Single Sign-On
Man spricht von Single Sign-On, wenn ein Nutzer nach einmaliger Authentisierung Zugriff auf alle Systeme, Anwendungen und Daten erhält, für die er eine Berechtigung besitzt. Für die eigentlichen Zugriffe muss er keine weiteren Aktionen wie etwa eine erneute Passworteingabe durchführen.

Zutrittskontrolle
Es ist möglich, dass die Berechtigung eines Mitarbeiters, in bestimmte Bereiche eines Unternehmens zu gelangen, anhand des elektronischen Mitarbeiterausweises überprüft wird.

Wird der elektronische Mitarbeiterausweis physisch ausgestellt (z.B. in Form einer Chipkarte), so ergeben sich weitere „mobile“ Anwendungsmöglichkeiten:
Eine mögliche Anwendung ist das automatische Sperren von Arbeitsplatzrechnern beim Herausziehen des Mitarbeiterausweises aus dem Kartenleser. Ist der Mitarbeiterausweis auch zum Betreten von Gebäuden erforderlich, wird der Mitarbeiter diesen zwangsläufig immer mitnehmen, wenn er seinen Arbeitsplatz verlässt. Dadurch ist es einem Angreifer unmöglich, über einen „verwaisten“ und nicht gesicherten Rechner in das Firmennetzwerk einzudringen.
Weitere Anwendungsfelder sind die automatische Zeiterfassung (Monitoring) z.B. beim Betreten und Verlassen des Bürogebäudes oder beim Login und Logout am

Sulzbacher Straße 29-39, 65824 Schwalbach am Taunus
Telefon 06196/88289-0, Telefax 06196/88289-11
contact@novosec.com, www.novosec.com

Arbeitsplatzrechner, sowie die Kantinenabrechnung.

Nutzen

Die Einführung eines elektronischen Mitarbeiterausweises bringt einige Vorteile für das Unternehmen und den einzelnen Mitarbeiter.

Nutzen aus Sicht des Unternehmens

Durch die Kapselung der Authentisierung und Transaktionsfreigabe von der Applikations- bzw. Geschäftslogik lassen sich erhebliche Kosteneinsparungen sowohl bei der Neueinführung von Anwendungen als auch bei der Wartung und Pflege erzielen. Daten zur Nutzerverwaltung werden zentral gespeichert, die Pflege der Daten und Nutzerrechte kann jedoch hierarchisch organisiert sein und dezentral erfolgen. Zugriffsrechte können „vor Ort“ (z.B. vom Projektleiter für projektbezogene Daten und Systeme) vergeben werden. Dadurch lässt sich die Administration vereinfachen und transparenter gestalten, was zu erheblichen Kosteneinsparungen führen kann. Letztlich wird die Fehleranfälligkeit reduziert und auch die Sicherheit im Unternehmen erhöht. Beispielsweise entfällt das Sicherheitsrisiko, dass Mitarbeiter einige der zahlreichen Kennwörter notieren und am Arbeitsplatz aufbewahren. In Notfällen („Verlust“ des Mitarbeiterausweises, Ausscheiden des Mitarbeiters, etc.) können sämtliche Berechtigungen mit einer einzigen Aktion (Sperre des Mitarbeiterausweises) entzogen werden. Durch die Möglichkeit der unternehmensweit eindeutigen Zuordnung von Transaktionen zum jeweiligen Mitarbeiter sind Revisionssicherheit und Transparenz gewährleistet.

Nutzen aus Sicht des Mitarbeiters

Nicht nur das Unternehmen profitiert von der Einführung eines elektronischen Mitarbeiterausweises; auch der Mitarbeiter hat einen greifbaren Vorteil. Im Vordergrund steht für ihn dabei der Aspekt der leichten Bedienbarkeit. Das Einprägen und lästige Eintippen immer neuer Kennwörter kann ebenso entfallen wie das Mitführen verschiedenster Dokumente/Karten für unterschiedliche Zwecke (Kantinenkarte, Zutrittsausweis für Firmengelände, etc.). Darüber hinaus können wesentliche Arbeitsabläufe für den Mitarbeiter vereinfacht und der Zugriff auf relevante Informationen erleichtert werden, wodurch die Effizienz der Arbeit gesteigert wird.

Fazit

Nicht alles, was technisch machbar ist, ist auch organisatorisch oder wirtschaftlich sinnvoll. Auf Grund der Vielzahl der Anwendungsmöglichkeiten setzt die Einführung eines elektronischen Mitarbeiterausweises eine detaillierte Analyse der Gegebenheiten im Unternehmen voraus. Erst auf dieser Basis ist es möglich, die optimale betriebliche Umsetzung zu ermitteln. Bei richtiger, individuell auf das Unternehmen zugeschnittener Umsetzung birgt der elektronische Mitarbeiterausweis ein großes Potential, dessen Ausschöpfung lohnenswert ist.

Wünschen Sie nähere Informationen zu diesem Thema? Wir freuen uns auf Ihre Anfragen.
chandima.costa@novosec.com
harald.ritter@novosec.com

Weitere Artikel finden Sie unter:
www.novosec.com/downloads