Sylvia Johnigk

Industrie 4.0 in der Praxis

Identitäts-Management

Anfang der 1990er-Jahre hatten vorwiegend große Unternehmen eine IT-Infrastruktur (Banken, Versicherungen, Energieversorger, etc.), Organisationen, die fast ein geschlossenes System darstellten. Sie betrieben ein Intranet, ihre Websites waren meist Informationsseiten ohne ausführbare Inhalte mit wenigen Schnittstellen zum Intranet und den internen Datenbanken. Unternehmensdaten wurden, wenn überhaupt, nur über wenige definierte Schnittstellen via Internet ausgetauscht.

Unternehmenskultur früher

Damals gab es in Unternehmen noch viele festangestellte IT- und andere fachliche Mitarbeiter.innen. Sie arbeiteten in Büros in unternehmenseigenen Gebäuden. Es gab Desktop-Computer, Server oder Mainframes und die Software und Services waren firmeneigen, gemanagt von angestellten IT-Mitarbeiter.innen. Nur selten wurden externe hoch spezialisierte Mitarbeiter.innen ins Unternehmen geholt, um einzelne Arbeiten durchzuführen. Häufig wurden die externen dabei von internen Mitarbeiter.innen beaufsichtigt, wenn sie beispielsweise im Herz des Unternehmens arbeiten mussten, dem Rechenzentrum. Endgeräte, Server und Mainframes waren über ein firmenbetriebenes LAN zusammengeschlossen, das mit Hubs, Switches, Routern, Firewalls und Standleitungen verschiedene Standorte miteinander zu einem Intranet verband. Es hatte nur wenige Schnittstellen zum Internet, es gab kaum mobile Endgeräte, Laptops waren wenigen Mitarbeiter.innen vorbehalten. Remote-Zugänge wurden nur mit Begründung und per Einzelgenehmigung erlaubt. E-Mail und Surfen waren zwar im Intranet erlaubt, im Internet dagegen war das ebenfalls nur wenigen Mitarbeiter.innen vorbehalten, die diesen *speziellen* Zugriff begründen mussten.

Identitäts-Management war relativ einfach, alle Mitarbeiter.innen wurden von der Personalabteilung anhand eines amtlichen Ausweisdokuments und von Zeugnissen überprüft. Sie/er bekam mit der Anstellung einen Firmenausweis und eine firmeninterne ID, mit der sie/er sich im Firmennetz anmelden konnte. In der Regel benutzte man für die Anmeldung am Desktop-Rechner die ID und ein Passwort. Der Mitarbeiterausweis war entweder von menschlichen oder maschinellen Einlasskontrollen an den Eingängen der Gebäude oder des Firmengeländes geprüft worden. Es war normal, dass neue Mitarbeiter.innen von einer/einem Alteingesessenen den Kolleg.innen vorgestellt wurden. Mitarbeiter.innen hatten einen festen Arbeitsplatz in einem Büro, die Kolleg.innen in der Umgebung waren bekannt. Desktop-Rechner waren genau einer/einem Mitarbeiter.in zugeordnet, zusätzlichen Zugriff hatten nur wenige Administrator.innen. Desktop-Rechner waren per Kabel an das Intranet angeschlossen. So war sichergestellt, dass nur Mitarbeiter.innen des Unternehmens Zugriff auf Unternehmensdaten hatten. Ein Berechtigungssystem beschränkte diese Zugriffe auf Daten weiter, so dass der Zugriff auf streng vertrauliche Informationen nur wenigen Mitarbeiter.innen vorbehalten waren. Externe Mitarbeiter.innen wurden überprüft, bekamen eine Externen-ID und einen besonders gekennzeichneten Firmenausweis und wurden den unmittelbaren Kolleg.innen vorgestellt. Dieses *Zwiebelschicht*-Verfahren stellte sicher, dass sich weitgehend nur berechtigte Personen in den Gebäuden an den Desktop-Rechnern befanden. Es fiel auf, wenn eine fremde Person im Nachbarbüro war.

Unternehmensnetzwerke waren nach Bereichen segmentiert und vom Internet abgeschottet. Einzelne Unternehmensbereiche und ausländische Unternehmensteile wurden zusätzlich durch Firewalls voneinander getrennt. So waren Entwicklung, Test und der Betrieb der IT voneinander getrennt. Ein Austausch der Daten zwischen diesen Segmenten war, wenn überhaupt, nur über definierte Schnittstellen möglich. Grundsätzlich hatte man die räumliche und fachliche Trennung von Aufgaben, Gebäuden und Ländern technisch nachzubilden. Natürlich gab es schon damals Sicherheitslücken und Möglichkeiten, Sicherheitsmaßnahmen zu umgehen, dennoch waren die zu schützenden Systeme weniger vernetzt, komplex und interaktiv. Die Hürden für Angreifer.innen waren höher, unbemerkt Teil des Unternehmensnetzwerks zu werden.

Exzessives Outsourcing verändert die Unternehmenskultur radikal

Das Outsourcing von Dienstleistungen, Hardware und Software führte dazu, dass Unternehmen mehr und mehr Schnittstellen nach außen öffneten. Immer mehr unternehmensfremde Personen wurden in die Prozesse des Unternehmens integriert und erhielten so ebenfalls Zugriff auf die Unternehmensdaten. Anfangs wurden nur wenige einfache Tätigkeiten ausgelagert, wie die Support-Hotline für Mitarbeiter.innen. Sie half bei Problemen wie Passwortrücksetzung oder bei der Behebung von Fehlfunktionen der Hard- oder Software. Inzwischen kommen immer mehr ausgelagerte Aufgaben und Dienstleistungen hinzu. Unternehmen verfügen heutzutage in der Regel nicht mehr über eine eigene IT-Infrastruktur, fast alle Geräte und Services sind geleast. Laptops von dem einen *Partner*-Unternehmen, Smartphones vom nächsten Partner-Unternehmen, Server vom übernächsten, und natürlich wird auch der Betrieb der Geräte von Partnern übernommen. So haben Unternehmen in der Regel eine Vielzahl Partner und damit externe Mitarbeiter.innen, die den IT-Betrieb des Unternehmens aufrechterhalten. Häufig geschieht das mit Hilfe eines Partner-Unternehmens des Partners, über eine lange Kette unterschiedlicher Unternehmen.

Festangestellte Mitarbeiter.innen arbeiten immer häufiger im Home-Office an eigenen Endgeräten. Wird manchmal das Endgerät für festangestellte Mitarbeiter.innen noch physisch geliefert, so findet die Wartung in der Regel *remote* statt. Das Gerät wird ins Netzwerk gehängt, eine vorinstallierte Software meldet es im Netzwerk an, es holt sich die Arbeitsumgebung über ein Netzwerk (Intranet/Internet) von einem oder mehreren Servern. Immer häufiger erhält selbst die/der festangestellte Mitarbeiter.in kein Firmen-Endgerät mehr, sondern arbeitet mit ihrem/sei-

nem eigenen Endgerät. Auf dem Endgerät ist ein Client, der in einer virtuellen Maschine die Arbeitsumgebung entweder über eine kabelgebundene Verbindung im Büro oder im Home-Office über eine VPN-Verbindung remote lädt.

Wurden früher die Daten in einem abgeschotteten Unternehmensrechenzentrum gespeichert und verarbeitet, so ergibt das heute kaum noch einen Sinn, wenn die meisten Beschäftigten aus unterschiedlichen Unternehmen kommen oder aus dem Home-Office arbeiten. Um so arbeiten zu können, benötigt man kollaborative Plattformen, die man von überall ohne Probleme erreichen kann. Die Beschäftigten des fremden wie des eigenen Unternehmens brauchen dabei eine Lösung, die ihnen den Zugriff ermöglicht, ohne sich ständig mit einem anderen User-ID/Passwort oder Ähnlichem anzumelden.

Software in der Cloud

Immer mehr Software-Services sind (günstig) nur noch als Cloud-Anwendung zu erhalten. So gibt es eine *OfficeCloud,* eine *ShareFileCloud,* eine Cloud für das Assetmanagement der Geräte inklusive einer Cloud, um Geräte auf Schwachstellen zu prüfen, die sogenannte *Cloud-Appliance,* um das Firmennetzwerks auf Viren zu scannen. Wenn alle sowieso unternehmensübergreifend in Projekten arbeiten, bietet es sich einerseits an, eine Lösung zu wählen, die nicht an ein Unternehmen gebunden ist. Andererseits ist diese Art der kollaborativen Arbeit eine Herausforderung für das Identitäts-Management.

Die spannende Frage ist dabei das Vertrauen. Früher holten die Organisationen sich vertrauenswürdige Mitarbeiter.innen in das Unternehmen, indem sie die Partner-Unternehmen fragten, wie bei ihnen der Einstellungsprozess, die Vergabe von Benutzer-IDs, die Vergabe von Rechten, der Schutz der Gebäude und Eingänge, etc. funktionierten und das stichpunktartig prüften. Für den Rest mussten sie dem Partner und den externen Mitarbeitern.innen trauen. Anders kann man nicht outsourcen.

Street-documentary shot of the blind leading the blind by Lee Mclaughlin, CC BY 3.0

Geschäftsprozesse ohne Mitarbeiter

Heute kann man einer Autoversicherung seinen Kilometerstand mittels einer Web-Schnittstelle übermitteln. Das ließe sich zukünftig noch vereinfachen, indem das Auto zum Stichtag den Kilometerstand automatisch an die Versicherung schickt. Nachdem die Versicherung den Kilometerstand erhalten hat, berechnen Algorithmen die neue Versicherungsgebühr. Der Brief besteht aus Textbausteinen und dem neu berechneten Beitrag, er wird in Druckstraßen ausgedruckt, frankiert und automatisch in großen Kisten zum Abholen durch ein Zustellerunternehmen gepackt. Das transportiert den Brief weiter. Noch bringen Briefträger.innen den Brief nach Hause, zukünftig erhalten sie einen Hinweis ihres Autos, dass der Brief zu Abholung im Portal der Versicherung liegt, und können ihn über eine verschlüsselte Leitung abholen. Einige Tage später wird der Beitrag automatisch vom Konto abgebucht.

Dieser Vorgang basiert auf autonomen IT-Prozessen, die miteinander kommunizieren und sich gegenseitig anstoßen. Ein Mensch kommt nur noch ins Spiel, wenn der Endkunde eine Reklamation hat.

Wann haben Sie das letzte Mal die Buchungen auf ihrem Kontoauszug nachgerechnet, und geprüft, ob die Einzelbuchungen korrekt addiert und subtrahiert, die Zinsen genau berechnet wurden? Die meisten Buchungen werden nahezu ohne menschliche Aktionen ausgeführt. Viele Transaktionen bedürfen lediglich einer Initialaktion, danach agieren die Prozesse so lange autonom, bis eine Veränderung oder Korrektur nur durch Menschenhand durchgeführt werden kann.

In Zukunft wird der Mensch nur noch benötigt, wenn Hard- oder Software eine Fehlfunktion aufweisen, wenn Algorithmen Anomalien feststellen oder aber der Kunde Zweifel an der Richtigkeit der Rechnung erhebt und deshalb geprüft werden muss, ob die Berechnung korrekt ist.

Innerhalb eines Unternehmens wird es zukünftig immer weniger festangestellte Mitarbeiter.innen geben. Gleichzeitig werden immer mehr Geschäftsprozesse nicht nur digitalisiert, sondern lassen sich weitgehend ohne Mitarbeiter.innen bewältigen.

Was bedeutet das für das Identity-Management?

Drei Themen sind zentral:

1. Wie kann man in einem Unternehmen, das nur noch für einen Teil seiner Beschäftigten das Identity Management selbst in der Hand hat, sicherstellen, dass die externen Mitarbeiter.innen und Kund.innen ausreichend identifiziert und authentisiert wurden? Wie stellt man Vertrauen *(Trust)* zwischen den verschiedenen Unternehmen her?

2. Bei der Authentisierung ist die spannende Frage: Welche *Credentials* (Passwort, Token, Chipkarte, Biometrie) sind für welchen Fall ausreichend?

3. Wie stellt man sicher, dass sich die Software-Services identifizieren und gegenüber Personen oder anderen Services

authentifizieren lassen? Zuletzt: Wie stellt man sicher, dass die Softwareprozesse identifiziert und authentisiert werden?

Identifizieren, Authentisieren und Trust

Wenn man heute in einem Unternehmen eingestellt wird, so wird in der Regel mindestens der Ausweis überprüft und man bekommt eine Unternehmens-ID, die innerhalb des Unternehmens eindeutig ist. Diese Unternehmens-ID wird selbstverständlich digitalisiert und dient zukünftig als eindeutiges Merkmal in der digitalen Welt des Unternehmens. Neben der primären ID haben Mitarbeiter.innen in der Regel mindestens eine weitere digitale ID, die ebenfalls eindeutig sein muss und der primären ID zugeordnet wird.

Mit diesen IDs lässt sich ein/e Mitarbeiter.in innerhalb des IT-Systems eindeutig identifizieren. Damit sie nur von der/dem berechtigten Mitarbeiter.in genutzt werden kann, wird sie mindestens mit einem Passwort geschützt. Ein/e Mitarbeiter.in erhält, nachdem sie/er sich angemeldet hat, von einem internen *Identity Provider* ein ID-Software-Token, das sie/er bei anderen Prozessen, zum Beispiel beim Drucker oder beim File-Server, vorzeigt. Diese Services fragen beim Identity Provider, ob das Token echt/gültig ist. Bei einer positiven Rückmeldung stehen berechtigten Beschäftigten die Dienste zur Verfügung und sie können auf ihre Daten zugreifen. Solange die Informationen und Anwendungen im Intranet liegen, reicht hierzu ein im Unternehmensnetz gültiges Software-Token aus.

Möchte die/der Nutzer.in beispielweise Daten im Internet aufrufen, so erhält sie/er von einem weiteren Identity Provider nach Überprüfung des internen Software-Tokens ein weiteres Token, das sie/ihn berechtigt, ein Webportal oder einen Dienst zum Beispiel in der Cloud zu nutzen. Die spannende Frage aus Sicht eines Unternehmens ist: Wie mit Tokens umgehen, die durch einen Identity Provider des Partner-Unternehmens ausgestellt wurden? Das dazu erforderliche Verfahren wird *Identity Federation* genannt und unterscheidet sich vom *Single Sign On* dadurch, dass nicht nur selbst ausgestellte Tokens innerhalb eines Netzwerks zu akzeptieren sind, sondern eben auch Tokens anderer Identity Provider.

Ein weiteres Problem entsteht beim Zuordnen von Berechtigungen. Bisher war hier nur die Rede von Identifizierung und Authentifizierung, der nächste Schritt, die Autorisierung, bringt neue Probleme. Eines entsteht, wenn regulatorische Vorschriften beispielsweise untersagen, dass Bankkunden gleichzeitig Sachbearbeiter.in oder Administrator.in ihres/seines Bankkontos sein darf. Solange die Bank eigene Mitarbeiter.innen beschäftigt, ist das organisatorisch und technisch umsetzbar: Die/der Sachbearbeiter.in arbeitet in einer anderen Filiale, Administrator.innen, die Zugriff auf die Datenbanken haben, haben kein Bankkonto bei der eigenen Bank, oder jeder schreibende Zugriff auf das eigene Konto wird nicht nur geloggt, sondern auch sofort gemeldet, und es muss überprüft werden, ob es ein rechtmäßiger Zugriff war. Arbeitet die/der selbe Administrator.in für einen Cloudanbieter oder einen Drittanbieter des Cloud-Dienstleisters, wird es jedoch zur Herausforderung, festzustellen, ob die/der Mitarbeiter.in identisch mit dem Bankkunden ist. Das selbe Szenario lässt sich auf verschiedene Unternehmen transferieren, jedes größere Unternehmen muss den *Grundsätzen ordentlicher Buchführung* folgen und lückenlos den Nachweis erbringen, dass nur berechtigte Personen berechtigte Änderungen gemacht haben. Dazu gehört unter anderem auch, dass man in der Regel nicht seine eigenen Kunden- und Buchungsdaten bearbeiten soll, oder dass diese Zugriffe streng zu überwachen sind.

Authentisieren, aber wie mache ich es sicher?

In den letzten Jahrzehnten hat sich gezeigt, dass die Kombination ID/Passwort einen zu geringen Schutz darstellt. Gerade weil Mitarbeiter.innen nicht mehr an der Pforte ihren Ausweis zeigen, in einem festen Büro, an einem festen Arbeitsplatz, an einen vom Unternehmen selbst administrierten Desktop-Rechner sitzen, der mit einem Kabel mit dem Intranet verbunden ist, sondern sich irgendwo im Internet mit einem privaten Laptop, Smartphone oder Tablet in einem WLAN andocken und dennoch auf Unternehmensdaten zugreifen müssen.

Deshalb haben Unternehmen unter anderem die 2-Faktor Authentisierung eingeführt. Hierzu erhalten Mitarbeiter.innen zum Beispiel entweder ein Token oder eine Chipkarte, auf denen sich ein Zertifikat befindet, das sie mit einem Passwort bestätigen müssen. Man hat also zwei Credentials: Karte und Passwort. So muss ein Angreifer in Besitz des Token-/Chipkarten-Zertifikats sein (oder einer Kopie) und das Passwort kennen. Dieses Verfahren hat innerhalb von Unternehmen halbwegs funktioniert.

Wenn Beschäftigte keine Lust hatten, ständig die Chipkarte in der kurzen Kaffeepause abzuziehen und danach wieder reinzustecken und das Passwort einzugeben, meldeten sie die Karte einfach als verloren, um eine neue zu erhalten, damit sie wieder ins Gebäude kamen. Ihr Passwort mussten sie so nur noch nach der Mittagspause eingeben, da nach 20 Minuten der Bildschirmschoner anging.

Inzwischen haben sich die Geräte verändert. Smartphones und Tablets verfügen nicht über eine Schnittstelle für eine Chipkarte

Sylvia Johnigk

Sylvia Johnigk studierte Informatik an der TU Berlin und befasste sich schon im Studium mit Themen wie Datenschutz und Informationssicherheit. Sie arbeitete fünf Jahre in der Forschung und acht Jahre bei einem Finanzdienstleister. Seit 2009 ist sie selbständig und leitet ein kleines Unternehmen in München, das sich auf Beratung von Unternehmen zum Thema Informationssicherheitsmanagement mit dem Schwerpunkt Mitarbeitersensibilisierung spezialisiert hat.

und sind auch für das Token nur bedingt geeignet. Wenn es schon für *normale* Beschäftigte schwierig ist, eine allumfassende Lösung zu finden, dann erst recht für Manager.innen oder Vorstände eines Unternehmens. Vorstände möchten nicht ständig mit irgendwelchen Chipkarten, Token etc. hantieren. Sie wollen an die Information zu jeder Zeit, ohne irgendwelche Hürden, und sie wollen immer das neueste Gerät am Markt. So suchen Unternehmen ständig neue einfachere Lösungen, werden aber von keinem gängigen Verfahren oder Tool zufriedengestellt.

Fragt man junge Mitarbeiter.innen oder Kund.innen, so würden sie sich am liebsten mit *Social Login* (Facebook, Twitter, und Co) einmal anmelden und damit alle ihre Konten verknüpfen, um sich auch beim Energieversorger, beim Versicherer, etc. damit authentifizieren und ihren Geschäften nachgehen zu können.

Andere Lösungsansätze arbeiten mit Attributen, wie der Geräte-ID der Nutzer.in, Netzwerkkarten-ID, IP-Adresse, Arbeitszeiten oder biometrischen Daten. Nehmen wir an, Frau Müller benutzt immer ein bestimmtes Gerät, und die IP-Adresse befindet sich immer in Deutschland. Plötzlich meldet sich Frau Müller, gerade mal eine Stunde nach ihrem letzten Logout, mit einem neuen Gerät an, und die IP-Adresse ist in China gemeldet …?

Damit sind wir mitten in einer Diskussion, mit welchen Credentials ich welche Geschäfte machen kann. Fakt ist: User-ID und Passwort sind für die meisten geschäftlichen Prozesse zu schwach, einige Lösungsansätze funktionieren nur für bestimmte Geräte, andere sind nicht datenschutzgerecht, …

Wie kann ich selbst mit möglichst wenig Aufwand meine eigenen digitalen Identitäten im Netz benutzerfreundlich, sicher und datenschutzgerecht verwalten und einsetzen? Die kurze, vernichtende Antwort: Gar nicht. In Europa und den USA laufen seit mehr als 20 Jahren erfolglos Projekte, die das Problem erkannt, aber nicht gelöst haben. Während in Europa zentralistische Lösungen vorgezogen werden, sind es in den USA ökonomisch gesteuerte Lösungen.

Welche Rolle spielen automatisierte Softwareprozesse?

Wenn zukünftig das Auto selbständig seinen Tachostand meldet, Algorithmen den neuen Versicherungsbeitrag berechnen, die Rechnungen aus Textbausteinen zusammengesetzt und im Portal abgelegt werden, automatisch der neue Beitrag abgebucht wird, bleibt eine Frage. Wie stellt man sicher, dass alle Prozesse mit den richtigen Prozessen kommunizieren und zwar über Unternehmensgrenzen hinweg?

Beim Zertifikatsmanagement ist zu klären, wer autorisiert ist, die Zertifikate für die Software-Prozesse und Hardware herauszugeben und zu verteilen. Einige Unternehmen haben externe Zertifizierer beauftragt, andere betreiben eine interne Zertifizierungsstelle und geben ihre eigenen Zertifikate heraus. Aber wie stellt man Vertrauen über Unternehmensgrenzen her? Vertraue ich jedem externen Zertifizierer oder nur bestimmten? Wie stelle ich sicher, dass der interne Zertifizierer eines Partner-Unternehmens meinen internen und den gesetzlichen Anforderungen entspricht?

Dann ist sicherzustellen, dass man bei Problemen die Services wieder in Betrieb nehmen kann. Das lässt sich mit einem gut organisierten und strukturierten Assetmanagement lösen. Doch wie es in einer Cloud so ist, Server und Services verschwinden in einer Wolke, und die Frage eines Auditors, wo denn der Server *xyz* mit Service *abc* stehe, hat schon zu mancher Odyssee durch das Rechenzentrum geführt. Was bei einem ersten Audit (vor dem realen Betrieb) noch für leichte Heiterkeit sorgen kann, ist im Ernstfall, wenn ein wichtiger Service ausfällt, ganz und gar nicht mehr lustig.

Fazit

Obwohl das Überleben des Unternehmens in der Regel hochgradig vom Funktionieren der IT-Infrastruktur abhängt, gibt es nur einen Bruchteil an internen IT-Beschäftigten. Letztendlich tragen sie nur noch die Verantwortung, dass der Betrieb der IT in diversen Dienstleistungs-Unternehmen reibungslos läuft.

Diese ausgelagerte Arbeit wird bestenfalls in den Räumen der Partner, aber immer häufiger im *Home Office* erledigt. Hardware und Software werden nur noch geleast und nicht mehr in eigenen Rechenzentren administriert, sondern in der *Cloud*. Mehr und mehr Unternehmen stellen interaktive Angebote für ihre Kund.innen zur Verfügung und bieten damit einen direkten Zugriff auf Kundendaten via Internet.

Das Kernproblem sind die große Anzahl von digitalen Identitäten, die Zuordenbarkeit der Identitäten und damit verbundenen Credentials wie Passworte, Token oder Chipkarten, die jeder Einzelne hat. Diese sind nicht mehr handhabbar, weder für einen Einzelnen, und schon gar nicht in kommerziellen Unternehmen, deren Prozesse sicherstellen müssen, dass nur wirklich authentisierte Nutzer.innen Zugriff auf Daten erhalten.

Eine ganzheitliche Lösung des Problems gibt es nicht. Meine Lösung ist, meine mehr als 100 digitalen Identitäten/Passworte in einem digitalen Safe zu hüten und ständig für mein Empfinden zu viele Chipkarten und Token mit mir herumzuschleppen. Ich sehne mich nach ein wenig mehr Einfachheit.

Passerelle Léopold-Sédar-Senghor, Paris
Foto: Maya-Anaïs Yataghène CC BY 2.0