# Intelligente Automation schützt Unternehmen und Beschäftigte

**Mit fortschreitender Digitalisierung und der Möglichkeit, jede Eingangstür und jede Wartungsklappe einer Fertigungsmaschine ins Netzwerk zu bringen, werden wirkungsvolle Zugangsbeschränkungen durch eine sichere Berechtigungsstruktur zunehmend wichtiger. Durch intelligente, zentrale Verknüpfung vorhandener Technik und bestehender Daten aus Zeitwirtschaft und Produktion mit neuen Komponenten ist es möglich, das Risiko von Schäden durch unberechtigten Zutritt zu minimieren und zugleich die gesamte Administration über eine einheitliche Oberfläche zugänglich zu machen. MELANIE HABERER, Vertriebsleiterin bei der Drakos GmbH, erklärt wie.**

*Melanie Haberer, Vertriebsleiterin bei der Drakos GmbH*

Ob Terroristen, Diebe, Spione oder ein widriger Mitbewerber – sie alle könnten ein Interesse haben, sich Zugang zu Ihrem Unternehmen zu verschaffen und entsprechenden Schaden anzurichten. Verlust und Zerstörung von materiellen Gütern, Datendiebstahl, Manipulation einzelner Computer oder ganzer Netzwerke können die Folge sein – mit schwerwiegenden Auswirkungen auf Wirtschaftskraft und Reputation des Unternehmens.

Eine Studie des Arbeitskreises für Unternehmenssicherheit in Berlin-Brandenburg aus dem Jahr 2009 kommt zu dem Schluss, dass 85 Prozent aller Wirtschaftsdelikte von unternehmensfremden Personen begangen wurden. Dabei haben die Täter oft leichtes Spiel: durch ungenügend gesicherte Zugänge oder veraltete Kontrollmechanismen gelangen sie sogar während der normalen Betriebszeiten an ihr Ziel. So könnte etwa ein Pförtner einen bereits gekündigten Mitarbeiter noch auf das Gelände lassen, nur weil er sich an sein Gesicht erinnert.

Doch auch innerhalb des Betriebs sind offene Türen und unbeschränkte Zugänge ein Risiko – und erschweren möglicherweise sogar den weltweiten Warenverkehr des Unternehmens: Wer etwa im Luftfrachtverkehr nicht bestimmte, durch die Europäische Kommission festgelegte Sicherheitsmaßnahmen als so genannter Bekannter Versender oder Geschäftlicher Versender erfüllt, muss mit verzögerter Abfertigung und höheren Kosten rechnen. Daneben fordern auch Versicherungen in ihren Policen wirkungsvolle Präventivmaßnahmen. Daher ist es ratsam, den Zutritt für Mitarbeiter auf die notwendigen Bereiche zu beschränken, sei es zu ihrem eigenen Schutz oder um Diebstahl zu verhindern, Produktionsabläufe nicht zu stören, Betriebsgeheimnisse zu wahren oder Daten zu schützen.

In der Fertigung beispielsweise kann es erforderlich sein, Maschinen nur von qualifizierten und autorisierten Personen bedienen zu lassen und Prozesse nur zu starten, wenn bestimmte zusätzliche Kriterien erfüllt sind. So könnte etwa der Zugang zu einem gefährlichen Bereich einer Maschine oder bestimmte Funktionen nur freigegeben werden, wenn sich eine Person als qualifizierter Techniker authentifiziert. Und – noch weiter gedacht – was geschieht eigentlich im Katastrophenfall? Wissen Sie jederzeit, wie viele Mitarbeiter sich in welchen Bereichen aufhalten?

### *Zentrale Verwaltung über SAP HCM*

Wie wird man nun all diesen Anforderungen gerecht, ohne zusätzliche Systeme zu errichten, die separat verwaltet werden müssen? Der Schlüssel liegt in der Erweiterung und zentralen Nutzung von SAP HCM. Die Personaladministration beinhaltet bereits alle notwendigen Informationen, um unternehmensweit Zutritts- und Zugangsberechtigungen ableiten zu können:

- *Personal:* Geschäftsbereich, Personalbereich, Kostenstelle, Abrechnungskreis
- *Organisationsmanagement:* Organisationseinheit, Planstelle, Person
- *Zeit:* Arbeitszeitmodell, Feiertage (überregional), Betriebsferien
- *Gebäudemanagement:* Videoüberwachung, Brandmeldeanlage, Alarmsicherung

Nun gilt es, das reibungslose Zusammenspiel der Zeit- und Betriebsdatenerfassung mit den Zutrittslesern und digitalen Türschlössern herzustellen. Bereits vorhandene Hardware ist so zu integrieren, zu erweitern oder zu ersetzen, dass die angestrebte Sicherheit gewährleistet und Datenredundanz vermieden wird. Durch Einsatz eines speziellen, in SAP integrierten Moduls ist es möglich, alle relevanten Daten zentral zu verknüpfen und, falls erforderlich, zu individualisieren. Auf diese Weise lassen sich orts- oder personenbezogen fein abgestufte Zutrittsberechtigungen vergeben und mit weiteren Informationen wie Zeiträumen oder Auftragsdaten verknüpfen. Der Datenaustausch mit den Terminals erfolgt zeitnah und automatisch – ein manueller Abgleich entfällt.

Ein so konzipiertes Zutrittsmanagement ist höchst flexibel und sehr effizient. Die grundlegenden Zutrittsrechte eines neuen Mitarbeiters werden bereits beim Anlegen seines Stammsatzes automatisiert und sicher, also nicht aufgrund persönlicher Einschätzungen generiert. Diese Rechte lassen sich bei Bedarf mithilfe eines eigenen SAP-Infotypen noch erweitern oder einschränken. Und weil alle Informationen über die gewohnte Bedienoberfläche unter SAP zugänglich sind, ist praktisch keine Einarbeitungszeit notwendig.

Darüber hinaus beinhaltet eine professionelle Lösung für die Zutrittskontrolle auch die Dokumentation aller Vorgänge mit der Möglichkeit der Auswertung. Auf diese Weise haben Verantwortliche beispielsweise im Notfall schnell eine Übersicht über alle betroffenen Personen zur Hand. Das kann lebensrettend sein und ist in manchen Industrien Pflicht. Auswertungen erlauben es zudem, jederzeit nachvollziehen zu können, wer wann wo angemeldet war oder sich Zutritt zu verschaffen versucht hat:

- *Ortsbezogen:* Wo hat wer Zugang?
- *Personenbezogen:* Wer hat wo Zugang?
- *Ereignisbezogen:* Alle Ereignisse, nach Personen, nach Terminals, unberechtigte Anmeldeversuche

Dank der SAP-Integration bleiben alle Daten auch über längere Zeiträume revisionssicher verfügbar und vor fremdem Zugriff geschützt.

Wer SAP HCM oder das SAP-Organisationsmanagement (oder zukünftig Success Factors) einsetzen möchte oder bereits nutzt und ein Zutrittsmanagement neu einrichtet oder erweitert, kann die Gelegenheit nutzen, eine integrierte Lösung anzustreben, die mehr Sicherheit für Unternehmen und Beschäftigte ermöglicht, vorhandene und neue Technik integriert und leicht zu handhaben ist – und die sich auch später jederzeit problemlos ergänzen und an neue Technologien anpassen lässt.

**Die Autorin**

***Melanie Haberer*** *startete 2011 als Vertriebsleiterin bei der Drakos GmbH, nachdem sie 20 Jahre lang in einem weltweit agierenden Unternehmen für Terminal-Hardware im In- und Ausland tätig war. Mit ihrer Expertise speziell im Hardware-Bereich ist sie die ideale Ergänzung zu Drakos-Geschäftsführer Andreas G. Dietrich, der 1991 an der Standardisierung der ersten SAP-Schnittstellen beteiligt war. Heute ist Drakos auf die Entwicklung von SAP-Lösungen spezialisiert und bietet mit Janitor die erste herstellerunabhängige und integrierte Zutrittskontrolle in SAP an.*