Digitalisierung im Sicherheitsgewerbe

Von René Helbig

1. Die Digitalisierung – ein Megatrend in der Wirtschaft

Den wohl wichtigsten Trend in Technik und Wirtschaft setzt Anfang dieses Jahrhunderts die Digitalisierung der analogen Welt. Arbeit und Prozesse werden effizienter, zeitsparender und kostengünstiger. Die einzelnen Prozesskomponenten, Schnittstellen und Gewerke lassen sich durch Digitalisierung vernetzen. Das führt zu höherer Produktivität und mehr Transparenz. Das „Internet der Dinge" und „Industrie 4.0" sind gängige Schlagworte geworden. Zu Recht bezeichnet Michael Ziesemer, Präsident des ZVEI, die Digitalisierung als „die größte Veränderung und Herausforderung unserer Zeit", die dazu führt, dass sich Wertschöpfungsketten und Geschäftsmodelle verändern. Die Digitalisierung hat nicht nur industrielle Anlagen und Produktionsprozesse erfasst, sondern zunehmend auch Dienstleistungen. Georg Schütte, Staatssekretär im Bundesministerium für Bildung und Forschung (BMBF), wagte jüngst die Prognose, dass Dienstleistungsmärkte ohne Digitalisierung künftig nicht mehr möglich sein werden. Da Produktion und Dienstleistung immer stärker verknüpft würden, stärke die Digitalisierung die Wertschöpfung in beiden Bereichen.

2. Technik als Bestandteil der Sicherheitsdienstleistung

Das Sicherheitsgewerbe war vor noch nicht allzu langer Zeit fast ausschließlich von personeller Dienstleistung geprägt. Sowohl die rasante Entwicklung technologischer Innovationen wie der zunehmende Kostendruck infolge steigender Löhne und knapper Budgets der öffentlichen Hand und der Unternehmen mit Sicherheitsbedarf führten im Sicherheitsgewerbe zu einem Umdenken. Durch Integration moderner Sicherheitstechnik in das Leistungsspektrum wurde das Angebot effizienter, kreativer und kostengünstiger. In der mechanischen wie der elektronischen Sicherheitstechnik – vor allem bei der Gefahrendetektion und der Meldetechnik im Bereich Security wie im Safetysektor – wurden die Innovationszyklen immer kürzer. Sicherheitstechnik kann den Menschen und seine Leistungsfähigkeit niemals ersetzen, aber sie kann die personelle Leistung wesentlich unterstützen, den personellen Anteil wesentlich reduzieren und mindestens langfristig Kosten senken.

3. Auswirkungen der Digitalisierung auf Sicherheitsdienstleistungen

Das gilt erst recht für die Digitalisierung der analogen Technik. Sie verbessert, beschleunigt, erleichtert und reduziert personelle Sicherheitsdienstleistungen. Auch die Infrastruktur des Sicherheitsunternehmens kann besser genutzt werden. Für eine digitale Optimierung lassen sich viele Beispiele anführen:

- Durch intelligente Gefahrenmeldetechnik können vordefinierte Gefahrenelemente elektronisch erfasst und automatisch in eine Notrufzentrale gemeldet werden, so dass eine schnelle Intervention erfolgen kann.
- Multisensoren führen zur Brandfrüherkennung und schließen Fehlalarme durch die notwendige additive Reaktion der unterschiedlichen Sensoren weitestgehend aus.
- Algorithmische Software in Videokameras detektiert vordefinierte Verdachtsereignisse und löst in der Leitzentrale einen Voralarm oder Alarm in Echtzeit aus, so dass keine Zeit bis zur Intervention verloren geht. Diese Software wird immer intelligenter, so dass eine sich entwickelnde Gefahrensituation – etwa eine gewalttätige Auseinandersetzung auf einem Bahnsteig – automatisch erkannt und gemeldet werden kann.
- Die digitale Messung von Menschenströmen, zum Beispiel im Rahmen einer Großveranstaltung, kann zu automatisiert vorgeschlagenen (proaktiven) Umlenkungsmaßnahmen und Fluchtwegveränderungen führen.
- Netzartig verbundene Kameras decken einen weiten Überwachungsraum ab, dessen ständige Bewachung oder Bestreifung sich erübrigt; verdächtige Person werden von Kamerazone zu Kamerazone weiterverfolgt.
- Eine Vielzahl digitaler Funktionen werden im „Remote Video Solution"-System miteinander verknüpft. Dies ermöglicht Mehrfachanalysen, detektiert Manipulationsversuche an Kameras und lässt sich mit einem Audiosystem verbinden, über das erkannte Tatverdächtige aus der entfernten Leitstelle heraus live angesprochen werden können.
- Durch automatisierte Gefahrendetektion in Produktionsprozessen und Lagerbereichen lassen sich innerbetriebliche Streifengänge wesentlich reduzieren.

RENÉ HELBIG ist Mitglied der Geschäftsführung und Chief Technical Officer (CTO) der Securitas Holding GmbH.

- Die digitale Gefahrenanalyse kann mittels Software in Reaktionsvorschläge münden und so Reaktionsfehler und Verzögerungen verhindern.
- Die digitalisierte Zutritts- und Zufahrtskontrolle reduziert Zahl und Dauer personeller Kontrollen, und damit auch die Zahl der nötigen Kontrollkräfte.
- Sicherheitschips als Warenetiketten und Videoüberwachung erfassen Ladendiebstähle und senken die Zahl der einzusetzenden Warenhausdetektive.
- Die Möglichkeit einer verbesserten Notrufkommunikation zwischen Sicherheitsbegleitern im öffentlichen Personenverkehr (ÖPV), die bei Gefahren ohne Zeitverzug unterstützt werden können.
- Der komplexe digitale Schutz von Kunstwerken durch Erschütterungsmelder, elektronische Sicherheitsvorhänge und Videoüberwachung ermöglicht einen wesentlich geringeren Einsatz von Aufsichtspersonal.

4. Digitalisierung der Infrastruktur des Sicherheitsunternehmens

Ebenso wie die Sicherheitsdienstleistung durch Digitalisierung optimiert, erleichtert und beschleunigt wird, unterstützt sie auch die innerbetriebliche Organisation: zum Beispiel die Einsatzvor- und -nachbereitung, die Informationssammlung und -verarbeitung sowie den zügigen Datentransfer. Anzahl und Anforderungsprofil für den Einsatz der benötigten Kräfte sowie deren Zeit- und Dienstpläne lassen sich elektronisch erarbeiten, die Arbeitsmittel der Beschäftigten elektronisch verwalten. Digitalisierte Kalkulationsprogramme erleichtern die Angebotsabgabe in Ausschreibungs- und Vergabeverfahren. Projekt- und Einsatzplanung für eine zu sichernde Veranstaltung können über eine gemeinsame Plattform die Zusammenarbeit aller an dem Projekt beteiligten Unternehmensbereiche erleichtern und beschleunigen. Die Digitalisierung von Dokumenten, Daten und Informationen reduziert Papier und Schreibarbeit. Der Aufbau einer Datenbank, in der alle für die Betreuung und den Einsatz der Beschäftigten notwendigen Daten eingegeben werden, macht die Organisation transparenter. So können Schwachstellen aufgedeckt und eine optimale Auswahl der jeweils an einem Einsatz zu beteiligenden Kräfte getroffen werden – je nach Anforderungsprofil und Mobilitätsbedarf. In einer solcher Informations- und Datenbank sollten in einem größeren Sicherheitsunternehmen auch alle Informationen und Erfahrungen vorgehalten werden, die im dienstlichen Alltag schwer zugänglich sind. So könnten am Wissen Einzelner im Unternehmen alle Manager und operativ tätigen Mitarbeiter beteiligt werden, wichtige Erfahrungen gehen nicht verloren oder geraten in Vergessenheit. Auch die Einsatzdokumentation kann über eine solche Datenbank erfolgen. Innerhalb eines in mehreren Staaten tätigen Unternehmens, erst recht in einem weltumspannenden Sicherheitskonzern, könnten so die Erfahrungen der Landesgesellschaften umfassend und zeitnah genutzt werden – ein Wettbewerbsvorteil, der bisher noch nicht voll ausgeschöpft wird. Soweit Fakten und Daten aus geschäftlichen oder datenschutzrechtlichen Gründen nicht innerhalb des Unternehmens allgemein zugänglich sein dürfen, lassen sich geschützte Bereiche innerhalb des Informationssystems bilden.

5. Digitalisierung reduziert Personalmangel

Der hohe Sicherheitsbedarf insbesondere in der Wirtschaft, die gut laufende Konjunktur, vor allem in Deutschland, und der demographische Wandel führen zu einem regional unterschiedlich ausgeprägten, aber tendenziell wachsenden Personalmangel im Sicherheitsgewerbe. Allein bei den rund 900 Mitgliedsunternehmen des BDSW sind derzeit etwa 10.000 Stellen unbesetzt. Diese Knappheit an personellen Ressourcen wird durch die fortschreitende Digitalisierung und integrierte Sicherheitslösungen zwar noch nicht ausgeglichen, aber doch erheblich gemildert.

6. Digitalisierung verlangt Bewusstseinswandel und spezifische Qualifizierung

Wie stark das Potenzial einer digitalen Optimierung - von Sicherheitsdienstleistungen und der Infrastruktur eines Sicherheitsunternehmens - genutzt werden kann, hängt wesentlich davon ab, wie gut Beschäftigte und vor allem die Manager diese Technologie und ihre vielfältige Anwendung verstehen und dafür offen sind. Hier werden von der Unternehmensleitung ein nicht immer leicht zu verwirklichendes „Change Management" und Investitionen in die Qualifizierung des Personals gefordert. Die Unternehmenskultur muss die Digitalisierung als notwendiges Werkzeug integrieren.

Der Umgang mit den verschiedenen Anwendungsbereichen der Digitalisierung erfordert eine Erweiterung der Qualifizierung von Managern und Mitarbeitern. Sicherheitsunternehmen, die ihre Infrastruktur teilweise digitalisieren und im Leistungsangebot digitalisierte Prozesse und Produkte integrieren, benötigen IT-Experten. Im Studium des Sicherheitsmanagements werden Grundkenntnisse der Informationstechnologie und der IT-Sicherheit zunehmend eine größere Bedeutung gewinnen. Der Manager, der dem Kunden ein Lösungsangebot mit digitaler Technik unterbreitet, muss den Anwendungsbereich, die Möglichkeiten und Grenzen der Einsetzbarkeit, die Vorteile und Risiken verstehen und verkaufen können. Und trotz aller Technik sollte der Kundennutzen immer im Fokus und klar ersichtlich sein. Auch die Ausbildungsberufe im Sicherheitsgewerbe werden den Einsatz der Informationstechnologie im Unterricht stärker berücksichtigen müssen. Unternehmenseigene Akademien bieten schon heute entsprechende Seminare an.

Selbstverständlich wird die Sicherheitsdienstleistung auch künftig zu einem erheblichen Teil im Einsatz von Personal bestehen. Der personelle Einsatz ist der unverzichtbare Kern des Sicherheitsgewerbes. Auf den Menschen, seine Flexibilität und seine Urteilskraft kommt es an. Aber in einer immer mehr digital ausgeprägten Welt wird ein Sicherheitsdienstleister künftig nur dann erfolgreich arbeiten und im Markt erfolgreich bestehen, wenn er das Potenzial dieser Entwicklung in seinem Leistungsportfolio und in seiner eigenen Infrastruktur voll ausschöpft.