

Einsatz von digitalen Systemen im Arbeitnehmer:innenschutz



M•plus 930

Sicherheitsinformation
für Führungskräfte

Inhalt

1 Einleitung	4
2 Checkliste vor Einführung digitaler Systeme	6
3 Nutzen digitaler Systeme im Arbeitnehmer:innenschutz	7
4 Digitale Systeme und deren Einsatz	8
4.1 Digitale Analysesysteme	8
4.1.1 Wearables	8
4.1.2 Smarte persönliche Schutzausrüstung (PSA)	10
4.2 Extended Reality (XR): VR, AR und MR	12
4.3 Weitere digitale Tools (Drohnen, Online-Schulungsplattformen)	15
4.3.1 Drohnen	15
4.3.2 Online-Schulungsplattformen, E-Learnings, digitale Erhebungsinstrumente	16
5 Kriterien für die Beschaffung und den Einsatz digitaler Systeme	18
5.1 Datenschutz	18
5.2 Technik und Interoperabilität	19
5.3 Inhalt und Gebrauchstauglichkeit	20
6 Chancen und Risiken	21
6.1 Möglichkeiten oder Chancen digitaler Systeme	21
6.2 Herausforderungen oder Risiken digitaler Systeme	22



1 Einleitung

Die fortschreitende Digitalisierung verändert und beschleunigt unsere Arbeitswelt.

Digitale Systeme spielen zunehmend eine wichtige Rolle im Bereich des Arbeitnehmer:innenschutzes. Die Integration digitaler Tools in den Arbeitnehmer:innenschutz trägt wesentlich dazu bei, die Sicherheit und die Gesundheit der Arbeitnehmer:innen zu verbessern. Diese Tools ermöglichen eine schnelle Reaktion auf potenzielle Gefahren und bieten umfangreiche Schulungs- sowie Weiterbildungsmöglichkeiten. Digitale Technologien unterstützen Arbeitgeber:innen und Beschäftigte dabei, moderne Arbeitsumgebungen sicherer und effizienter zu gestalten. Dazu zählen auch Softwarelösungen für das Management der Arbeitssicherheit.

Der Einsatz digitaler Systeme bietet Chancen für die Verbesserung des Arbeitnehmer:innenschutzes am Arbeitsplatz bzw. im Betrieb. Daraus resultieren aber auch Herausforderungen und Risiken, die bei der Implementierung mitbedacht werden müssen. Diese sind z. B. hohe Anfangsinvestitionen, Datenschutzanforderungen oder auch der nötige Schulungsbedarf.

Das vorliegende Merkblatt soll Unternehmen, welche derartige Tools im Einsatz haben oder über den Einsatz derartiger Tools nachdenken, bei der Implementierung bzw. Gestaltung solcher Systeme unterstützen, um praxistaugliche Lösungen für mehr Arbeitssicherheit

zu finden. Des Weiteren geht es darum, Unternehmen und Anwender:innen auf die Chancen aufmerksam zu machen und für bestehende Risiken zu sensibilisieren.

Das Merkblatt hat digitale Systeme zum Thema, die im betrieblichen Kontext verwendet werden können – jeweils mit dem Fokus auf den Aspekt „Gesundheit bei der Arbeit“. Zu diesen digitalen Anwendungen zählen Apps, Wearables, Drohnen, Schulungsplattformen, der Einsatz von VR am Arbeitsplatz und smarte persönliche Schutzausrüstung.

Drohnen können beispielsweise die Begutachtung und Überwachung von schwer zugänglichen oder gefährlichen Arbeitsbereichen übernehmen. Bei Arbeiten auf Baustellen, in Industrieanlagen oder auf großen Industrieflächen kann es für Beschäftigte gefährlich oder auch zu zeitaufwendig sein, bestimmte Stellen manuell zu überprüfen – hierzu zählen etwa Dächer, Hochspannungsmasten, große Maschinen oder enge Schächte. Drohnen können eingesetzt werden, um diese Bereiche aus der Luft sicher zu inspizieren.

Im Gegenzug braucht es klare Regelungen, wie mit den erfassten Daten umgegangen wird. Der Einsatz digitaler Tools darf beispielsweise nicht zu einer ungewollten Überwachung der Mitarbeiter:innen führen. Hier geht es um Transparenz und die Schaffung von klaren und verbindlichen Regeln im Unternehmen.

Das Merkblatt richtet sich an:

- Sicherheitsfachkräfte (SFKs) im Beratungskontext
- Anwender:innen in Betrieben
- Betriebe und Organisationen, welche digitale Anwendungen einsetzen bzw. in naher Zukunft einsetzen möchten
- Präventivfachkräfte
- weitere für Arbeitssicherheit und Gesundheitsschutz zuständige Personen

Im Kontext des Arbeitnehmer:innenschutzes bezieht sich der Begriff „digitale Systeme“ auf Technologien und elektronische Systeme, die zur Unterstützung, Steuerung oder Automatisierung von Arbeitsprozessen verwendet werden, mit dem Ziel, die Sicherheit der

Beschäftigten zu erhöhen und Arbeitsunfälle zu vermeiden. Digitale Systeme im Arbeitnehmer:innenschutz können eine Vielzahl von Anwendungen umfassen.

In diesem Merkblatt werden verschiedene digitale Systeme vorgestellt und erklärt. Sie erfahren, in welchen Arbeitsbereichen sie eine Rolle spielen und welche Chancen sie für den Arbeitnehmer:innenschutz bieten, aber auch welche Herausforderungen sich aus ihrem Einsatz ergeben.



© Dejan – stock.adobe.com

2 Checkliste vor Einführung digitaler Systeme

Vor der Einführung digitaler Systeme im Betrieb bzw. im Arbeitsalltag sollten sich Arbeitgeber:innen, mit der Anschaffung betraute Beschäftigte, zuständige Präventivfachkräfte etc. folgende Fragen¹ stellen:

■ Welches Problem soll mit der Anschaffung eines digitalen Systems gelöst werden?
■ Was soll mithilfe des digitalen Systems erreicht werden?
■ Ist ein digitales System klar und eindeutig das Mittel der Wahl? ■ Gibt es eine weniger aufwendige Alternative?
■ Stehen für die Dauer des Einsatzes genügend finanzielle und personelle Ressourcen zur Verfügung?
■ Ist die Nutzung des digitalen Systems mit der betrieblichen Interessenvertretung abgestimmt?
■ Ist das digitale System mit dem IT-System des Unternehmens kompatibel?
■ Welche Daten werden erhoben? ■ Wer hat Zugang zu diesen Daten? ■ Wie wird der Schutz der Daten sichergestellt?
■ Wie wird der Einsatz des digitalen Systems allen Beteiligten bekannt gegeben?
■ Wann und wie wird sein Nutzen evaluiert?
■ Erfordert das System für die Nutzung eine zusätzliche Qualifizierung / Schulung der Beschäftigten? ■ Wenn ja, wie kann diese sichergestellt werden?

¹ Fragen erstellt in Anlehnung an den Fragenkatalog aus der „DGUV Information 206-058 – Digitale Anwendungen im Präventionsfeld „Gesundheit bei der Arbeit“ – eine Orientierungshilfe“, Seite 6 – zu finden unter publikationen.dguv.de (abgerufen am 13.02.2026)

3 Nutzen digitaler Systeme

im Arbeitnehmer:innenschutz

Frühzeitige Gefahren- und Risikowarnung

Digitale Systeme erfassen und analysieren Daten (z. B. Umweltbedingungen, Maschinenstatus, Mitarbeiter:innenstand) in Echtzeit. So können potenzielle Gefahren schneller erkannt und Unfälle vermieden werden.

Verbesserte Überwachung und Dokumentation

Digitale Tools ermöglichen eine lückenlose und transparente Dokumentation von Arbeitnehmer:innenschutzmaßnahmen, Vorfällen und Schulungen. Das verbessert die Einhaltung von Vorschriften und die Nachverfolgbarkeit bei Unregelmäßigkeiten.

Effiziente Kommunikation und Alarmierung

Bei Gefahrensituationen können digitale Systeme automatisch Warnungen an betroffene Personen senden oder Notfalldienste informieren – ohne Zeitverlust.

Individualisierte Schutzmaßnahmen

Durch die Auswertung von Daten zu Mitarbeiter:innengesundheit, Belastungen und Arbeitsumgebung können Schutzmaßnahmen individuell angepasst und optimiert werden.

Schulung und Sensibilisierung

Digitale Lernplattformen, Virtual Reality (VR) oder Augmented Reality (AR) ermöglichen praxisnahe und interaktive Schulungen, die die Aufmerksamkeit und das Verständnis für Arbeitssicherheit erhöhen.

Automatisierung gefährlicher Aufgaben

Risikoreiche Tätigkeiten werden von Robotern, Drohnen oder automatisierten Systemen ausgeführt, um Beschäftigte vor Gefährdungen zu schützen.

Datenbasierte Entscheidungen

Mithilfe von Big Data und KI können Unternehmen ihre Arbeitnehmer:innenschutzstrategien stetig verbessern, basierend auf konkreten Erkenntnissen aus der Praxis.



4 Digitale Systeme und deren Einsatz

4.1 Digitale Analysesysteme

Digitale Systeme wie beispielsweise Kameras und Sensoren werden zur Analyse und Bewertung von spezifischen Parametern auf Personen- und/oder Arbeits-

platzebene eingesetzt. So können Belastungen und Beanspruchungen frühzeitig erkannt werden.

4.1.1 Wearables

Merkmale

Wearables (englisch für „tragbare Geräte“) sind tragbare Systeme in Form von Kleidung, Accessoires oder Geräten, die auf digitalen Technologien beruhen. Sie sind oft mit Sensoren ausgestattet, die Daten sammeln und analysieren. Sie können verschiedene Funktionen haben wie z. B. Gesundheitsüberwachung, das

Übermitteln von Benachrichtigungen oder sogar die Steuerung anderer Geräte/Maschinen. Sie bieten den Nutzenden die Möglichkeit, Aktivitäten und Gesundheitsdaten in Echtzeit zu verfolgen und zu verwalten. Im privaten Gebrauch sind sie oft als Fitness-Tracker in Verwendung.

Einsatzmöglichkeiten im Arbeitnehmer:innenschutz

Smarte Armbänder

Wearables wie smarte Armbänder oder auch Brustgurte messen kontinuierlich Vitalparameter wie Herzfrequenz, Körpertemperatur oder Sauerstoffsättigung.

So können Stress, Überanstrengung oder gesundheitliche Probleme frühzeitig erkannt und dadurch bedingte Unfälle vermieden werden.

Standort- und Bewegungserfassung

(z. B. Smartwatches mit GPS-Tracking)

Wearables mit GPS oder Bewegungssensoren helfen dabei, die Position von Mitarbeitenden – besonders in gefährlichen oder nicht einsehbaren Arbeitsbereichen – zu überwachen. Einerseits können so Zusammenstöße vermieden, andererseits im Notfall Hilfe geschickt werden.

Erkennung von Stürzen und Unfällen

Intelligente Sensoren erkennen plötzliche Stürze oder ungewöhnliche Bewegungsmuster und lösen automatisch einen Notruf aus. Im Arbeitsalltag ist das besonders in Bereichen mit hohem Unfallrisiko wie Bau oder Produktion wichtig – sowie bei hohen Belastungen des menschlichen Organismus (wie zum Beispiel bei Feuerwehrleuten) relevant.

Schutz vor gefährlichen Umgebungen

(z. B. Gassensoren und Atmosphären-Warngeräte)

Manche Wearables erheben Umgebungsdaten wie die Konzentration giftiger Gase, Lärm oder Hitze und warnen die Träger:innen rechtzeitig, sodass sie sich in Sicherheit bringen können.

Haltungskorrektur und Alltags-Monitoring

Wearables können Haltung und Bewegungen analysieren und Feedback geben. Auf diese Weise werden Fehlhaltungen oder Überlastungen vermieden, was langfristig Muskel-Skelett-Erkrankungen vorbeugt.

Intelligente Helme

Intelligente Helme dienen der Erkennung gefährlicher Situationen: Sie können beispielsweise Erschütterungen oder Stöße registrieren und automatisch einen Alarm auslösen.

Vorteile

Im Arbeitnehmer:innenschutz bieten Wearables, also am Körper getragene Systeme wie Smartwatches, intelligente Helme oder spezielle Sensorkleidung, diverse Vorteile für Prävention, Intervention und die Gesundheitsförderung.

- **Standortbestimmung:** In Notfällen lässt sich die genaue Position eines:iner Mitarbeitenden, etwa in großen Industrieanlagen oder auf Baustellen, schnell ermitteln. Rettungskräfte gelangen rascher an den Einsatzort.
- **Automatische Notfallmeldung:** Bei einem Sturz, einem Unfall oder bei Bewusstlosigkeit senden Wearables automatisch eine Meldung an Rettungsdienste oder Kollegen:Kolleginnen, was die Reaktionszeit im Ernstfall erheblich verkürzt.

- **Datenaustausch mit Rettungsdiensten:** Bei einem Unfall werden Vitaldaten des:der Betroffenen an die Rettungsdienste übermittelt, um eine schnellere und gezieltere Behandlung zu ermöglichen.
- **Ergonomische Unterstützung:** Wearables können Haltung und Bewegungen analysieren und Feedback geben. Auf diese Weise werden Fehlhaltungen oder Überlastungen vermieden, was langfristig Muskel-Skelett-Erkrankungen vorbeugt.
- **Überwachung der Vitalwerte:** Wearables wie smarte Armbänder oder Brustgurte messen kontinuierlich Herzfrequenz, Körpertemperatur oder Sauerstoffsättigung. So können Stress, Überanstrengung oder gesundheitliche Probleme frühzeitig erkannt und dadurch bedingte Unfälle vermieden werden.

Nachteile

Auch wenn Wearables erhebliche Vorteile für den Arbeitnehmer:innenschutz bieten, ergeben sich durch sie eine Reihe von Nachteilen und Risiken, die Unternehmen wie auch die Mitarbeitenden berücksichtigen müssen. Diese reichen von ethischen Bedenken, Fragen zum Datenschutz über technische Probleme bis hin zu potenziellen Fehlinterpretationen von Daten.

- **Datenschutzverletzungen:** Wearables sammeln sensible persönliche Daten der Mitarbeitenden, einschließlich Gesundheitsdaten, Standort und Bewegungsmuster. Die Speicherung und Verarbeitung dieser Informationen birgt das Risiko von Datenschutzverletzungen und unbefugtem Zugriff.
- **Intransparente Algorithmen:** Die Algorithmen vieler Wearables sind nicht transparent, was die Bewertung der Qualität und Aussagekraft der erfassten Daten erschwert. Arbeitnehmer:innen erhalten unter Umständen Rückmeldungen, die auf fehlerhaften oder unverständlichen Berechnungen beruhen.

- **Gefahr der Diskriminierung:** Durch die Analyse der gesammelten Daten könnte es zu unbeabsichtigter Diskriminierung kommen, wenn beispielsweise Daten über den Gesundheitszustand oder die Aktivität zu falschen Rückschlüssen in Bezug auf die Leistungsfähigkeit eines:einer Mitarbeitenden führen.
- **Fehlendes Vertrauen:** Mitarbeitende könnten befürchten, dass Daten gegen sie verwendet werden, zum Beispiel bei der Besetzung von Stellen oder bei der Beurteilung ihrer Leistung.

4.1.2 Smarte persönliche Schutzausrüstung (PSA)

Merkmale

Smarte PSA ist eine innovative Form von Schutzausrüstung, die mit Technologien ausgestattet ist, um die Sicherheit und Effizienz von Nutzenden zu erhöhen. Diese Ausrüstung kann Sensoren, Kommunikationstechnologien und Datenanalysefunktionen enthalten, um Echtzeitinformationen über Umgebungsbedingungen, Gesundheitsdaten oder potenzielle Gefahren bereitzustellen. Als Beispiele wären Helme mit integrierten Kommunikationssystemen, Schutzanzüge mit Temperatur- oder Feuchtigkeitssensoren und Sicherheitswesten mit GPS-Tracking zu nennen. Smarte PSA verbessert nicht nur den Schutz, sondern auch die Entscheidungsfindung und die Reaktionsdauer in gefährlichen Situationen.

Im Gegensatz zu Wearables steht bei smarter PSA der Schutzcharakter der Arbeitnehmenden im Vordergrund.

Einsatzmöglichkeiten im Arbeitnehmer:innenschutz

Smarte Warnwesten

Smarte Warnwesten erhöhen als Weiterentwicklung klassischer Warnwesten (PSA) durch Sensorik, aktive Warnfunktion, hochreflektierende Materialien und Konnektivität den Personenschutz in gefährlichen Arbeits- und Verkehrsumgebungen deutlich. Sie werden u. a. auf Baustellen, in der Industrie, Logistik, im Straßenbau und bei Rettungsdiensten eingesetzt.

Smarte Schutzhelme

Smarte Schutzhelme – auch als intelligente oder vernetzte Helme bezeichnet – sind eine Weiterentwicklung klassischer Arbeitsschutzhelme. Sie schützen den Kopf nicht nur mechanisch, sondern bieten digitale Sicherheitsfunktionen wie z. B. GPS-Ortung, Sturzerkennung, Temperatur- oder Gaswarnsysteme oder Kamera-Integration (die Kamera erkennt Gefahren in Echtzeit, meldet diese und unterstützt den:die Träger:in). Einsatzgebiete sind Bau, Industrie, Bergbau, Rettungsdienste, Logistik und Sport (z. B. Fahrradfahren, Motorradfahren, Klettern).



Feuerwehrmann in smarter PSA mit gekennzeichneten Sensoren

Smarte Sicherheitsschuhe

Smarte Sicherheitsschuhe sind eine Weiterentwicklung klassischer Arbeitsschuhe. Sie kombinieren mechanischen Schutz (z. B. Stahlkappen, rutschfeste Sohlen) mit Sensorik und digitaler Intelligenz wie z. B. Drucksensoren oder Standorttracking, um Arbeitssicherheit, Gesundheit und Effizienz zu erhöhen. Sie werden vor allem am Bau, in Industrie, Lager, Logistik und Produktionsumgebungen eingesetzt.

Smarte Atemschutzmasken

Sie schützen nicht nur vor Schadstoffen, Staub oder Aerosolen, sondern überwachen aktive Atemfunktionen, Luftqualität und Umgebungsbedingungen, um Sicherheit und Gesundheit zu verbessern. Sie werden vor allem am Bau, in Industrie, Laboren, Gesundheitswesen, Chemie und bei Notfalleinsätzen verwendet.

Smarte Handschuhe

Smarte Handschuhe kombinieren mechanischen Schutz mit digitaler Intelligenz und Sensorik. Sie messen und unterstützen Handbewegungen, erkennen Gefahrensituationen und können in vernetzte Arbeitnehmerschutzsysteme integriert werden. Sie erhöhen die Sicherheit, Präzision, Ergonomie und Effizienz am Bau, in Industrie, Logistik, Medizin, Laboren und im Sport.

Vorteile

Smarte PSA bietet zahlreiche Vorteile, indem sie die Sicherheit in Echtzeit erhöht, präventive Maßnahmen ermöglicht und die Notfallreaktion optimiert. Durch Echtzeitüberwachung ist proaktive Gefahrenprävention möglich. Arbeitsbedingungen können verbessert, die Effizienz gesteigert werden.

- **Warnung vor unmittelbaren Gefahren:** Smarte PSA kann mit Sensoren ausgestattet sein, die gefährliche Zustände wie die Exposition gegenüber giftigen Gasen, übermäßiger Hitze, Lärm oder Strahlung sofort erkennen und Träger:innen sowie Vorgesetzte warnen. Beispielsweise können smarte Gehörschützer vor gesundheitsschädlichem Lärm warnen.
- **Gesundheitsmonitoring:** Sensoren in smarter Kleidung oder Helmen überwachen Vitalfunktionen wie Körpertemperatur, Herzfrequenz oder Blutsauerstoffsättigung und warnen vor Überhitzung, Stress oder Ermüdung. Dies ist besonders bei anstrengenden Arbeiten in heißen Umgebungen wichtig, um Hitzschläge zu vermeiden.
- **Lokalisierung und Zonenüberwachung:** Smarte PSA mit GPS oder RFID (radio frequency identification) kann den Standort von Arbeitnehmenden in weitläufigen oder unübersichtlichen Bereichen verfolgen.

Nachteile

Trotz aller Vorteile bringt die Nutzung von smarter persönlicher Schutzausrüstung auch eine Reihe von Nachteilen im Arbeitsalltag mit sich.

- **Ablenkung:** Integrierte Displays oder Benachrichtigungssysteme lenken Mitarbeitende ab und erhöhen so das Risiko von Unfällen.
- **Falsches Sicherheitsgefühl:** Mitarbeitende könnten sich durch die Nutzung smarter PSA in falscher Sicherheit wiegen und weniger vorsichtig agieren. Dadurch würde das Gefahrenbewusstsein in der realen Arbeitswelt sinken.

Kombinierte PSA-Systeme

Hierbei handelt es sich um vernetzte Systeme, bei denen Helm, Weste und Schuhe miteinander kommunizieren und Gefahren melden oder den Zustand des:der Trägers:Trägerin überwachen.

So lässt sich feststellen, ob sich jemand in einer Gefahrenzone aufhält oder vermisst wird.

- **Automatisierte Erkennung von Vorfällen:** Sensoren erkennen Stürze oder Stöße und lösen automatisch Alarm aus, was die Reaktionszeit im Notfall verkürzt.
- **Reduzierung menschlichen Versagens:** Da die smarten Systeme automatisch überprüfen, ob die richtige PSA getragen wird, wird die Gefahr menschlichen Versagens bei der Einhaltung von Sicherheitsvorschriften minimiert.
- **Besserer Tragekomfort:** Smarte PSA (wie etwa kühlende Westen) passt sich automatisch an die Umgebung an, was den Komfort erhöht und die Produktivität steigert.
- **Verringerte administrative Last:** Durch die automatisierte Datenerfassung und Bestandsverwaltung von PSA wird der Verwaltungsaufwand für Sicherheitsabteilungen reduziert.
- **Gezieltes Training:** Anhand der erhobenen Daten sind Unternehmen in der Lage, Schulungsprogramme gezielter auf die tatsächlichen Risiken am Arbeitsplatz auszurichten.

- **Fehlende Reparaturmöglichkeiten:** Modifizierte PSA oder nicht fachgerecht ausgeführte Reparaturen gefährden die Schutzfunktion. Bei smarter PSA fällt die Reparatur aufgrund der Elektronik komplexer aus.
- **Abhängigkeit von der Technologie:** Wenn die smarte PSA ausfällt, sind die Arbeitnehmenden plötzlich ungeschützt oder auf eine Notfalloption angewiesen.

4.2 Extended Reality (XR): VR, AR und MR¹

Ein XR-System ist eine computergestützte Erweiterung der Realitätswahrnehmung. Diese Information kann alle menschlichen Sinnesmodalitäten ansprechen. In XR-Systemen werden beispielsweise Umgebungen und

Tätigkeiten im Betrieb simuliert. Extended Reality (XR) ist der Überbegriff für Virtual, Augmented und Mixed Reality.

Merkmale

Virtual Reality (VR)

VR ist eine Technologie, die es ermöglicht, eine computergenerierte, interaktive 3D-Umgebung zu erleben. Mithilfe eines speziellen Headsets, das visuelle und oft auch akustische Eindrücke vermittelt, erleben die Nutzenden das Gefühl, in eine andere Welt einzutauchen. VR wird derzeit vor allem in den Bereichen Gaming, Simulation, Ausbildung und Medizin eingesetzt.

Augmented Reality (AR)

AR ist eine Technologie, die digitale Informationen wie Bilder, Videos oder 3D-Modelle in die reale Welt integriert. Dies geschieht oft über Smartphones, Tablets oder spezielle AR-Brillen. AR erweitert unsere Wahrnehmung der Realität, indem sie virtuelle Elemente in die uns bekannte Umgebung einfügt und interaktive und immersive Erlebnisse ermöglicht.

Mixed Reality (MR)

MR ist eine Technologie, die Elemente der VR und der AR kombiniert. Sie ermöglicht es, digitale Objekte in die reale Welt einzufügen und gleichzeitig mit ihnen zu interagieren, als wären sie Teil der physischen Umgebung. MR verwendet fortschrittliche Sensoren und Kameras, um die reale Welt zu erfassen und digitale Inhalte so darzustellen, dass sie realistisch in den Raum integriert werden. Ein Beispiel für MR ist Microsofts HoloLens, die es Nutzenden ermöglicht, holografische Objekte zu sehen und mit ihnen zu interagieren, während sie sich in ihrer realen Umgebung bewegen.

¹ Vertiefende Informationen zu den verschiedenen Einsatzmöglichkeiten von XR im Betrieb sind im AUVA-Merkblatt M.plus 931 „XR-Technologien am Arbeitsplatz“ unter auva.at/downloads zu finden.



Einsatzmöglichkeiten im Arbeitnehmer:innenschutz

Gefahrloses Sicherheitstraining im Betrieb

Risikofreies Üben: Trainings mit XR-Technologien ermöglichen es den Mitarbeitenden, in einer sicheren, simulierten Umgebung den Umgang mit gefährlichen Situationen wie Bränden, Gasaustritten, chemischen Lecks oder den Betrieb von schwerem Gerät zu üben.

Interaktion mit virtuellen Gefahren durch MR

Durch den Einsatz von MR-Technologien können virtuelle Gefahren (z. B. eine chemische Leckage) als Teil der realen Umgebung wahrgenommen werden, mit der die Lernenden interagieren können. Dies vertieft das Verständnis für die Risiken und die Handhabung der entsprechenden Schutzausrüstung.

Sicherheitstraining für Rettungskräfte

Einsatzkräfte und Beschäftigte im Rettungswesen können für Katastrophenszenarien, die in der Realität aufgrund des hohen Gefährdungspotenzials nicht geübt werden können (wie Gebäudebrände oder Chemieunfälle), ganz ohne Risiko trainieren.

Praxisnahe Notfallübungen mit MR-Unterstützung

Katastrophenszenarien wie Erdbeben oder Zug-

unglücke sind oft schwer zu inszenieren und können mithilfe von MR unter kontrollierten Bedingungen durchgeführt werden.

Begehung von Baustellen

VR-Simulationen können so konzipiert werden, dass sie die realen Arbeitsbedingungen genau abbilden. Entsprechend lassen sich z. B. das Begehen von Baustellen oder die Arbeit in engen und schwer zugänglichen Bereichen üben.

Feedback in Echtzeit

Bei interaktiven Schulungen mithilfe von AR erhalten Teilnehmende in Echtzeit Rückmeldung zu ihrer Leistung und können Fehler sofort korrigieren, was den Lernprozess beschleunigt.

Interaktive Anwendungen am Arbeitsplatz

Vor dem Hintergrund der Standardisierung von Anleitungen können AR-Anwendungen 3D-Anleitungen für Wartungs- und Sicherheitsverfahren direkt in das Sichtfeld der Arbeitskraft projizieren, um die korrekte Ausführung sicherzustellen.

Vorteile

Extended Reality (XR) bietet im Bereich des Arbeitnehmer:innenschutzes vielfältige Vorteile, da durch sie Schulungen, Risikobewertungen und die allgemeine Arbeitsumgebung sicherer und effektiver gestaltet werden.

- **Realistische Simulationen mit geringem Risiko:** XR kann realitätsnahe Umgebungen schaffen, in denen Mitarbeitende risikoreiche Situationen wie Brände, Chemikalienunfälle oder Störfälle an Maschinen sicher und ohne Konsequenzen trainieren können. Das Training in virtuellen Umgebungen eliminiert die Gefahr von Verletzungen oder Schäden an teurer Ausrüstung, die bei Übungen in der realen Welt auftreten können.
- **Fehler machen ohne Konsequenzen:** In der virtuellen Realität können Fehler gefahrlos gemacht und korrigiert werden, was den Lernprozess beschleunigt und die Behaltensquote erhöht.
- **Ganzheitliche Erfahrung:** Durch die hohe Immersivität vor allem von VR werden Gefahrenbewusstsein und Reaktion in einer Weise trainiert, die traditionelle Methoden nicht erreichen.
- **Wiederholbarkeit und Anpassung:** Die Mitarbeitenden können VR-Simulationen beliebig oft wiederholen, um ihre Fähigkeiten zu perfektionieren. Die Szenarien lassen sich auch an spezifische Arbeitsbedingungen anpassen.
- **Ausgeprägtes Gefahrenbewusstsein:** Das Training in XR erhöht das Bewusstsein für potenzielle Gefahren und ermöglicht es den Mitarbeitenden, Sicherheitsrisiken schneller zu erkennen und angemessen zu reagieren.
- **Höheres Engagement und besseres Behalten:** Interaktive AR-Lernszenarien wirken ansprechender als herkömmliche Methoden (z. B. Videos oder Präsentationen). Dies fördert die aktive Teilnahme und sorgt dafür, dass die Sicherheitsvorschriften besser im Gedächtnis bleiben.
- **Gesteigerte Motivation:** Der spielerische und immersive Charakter von VR-Trainings kann die Motivation der Mitarbeitenden steigern und das Lernen ansprechender gestalten.
- **Reduzierte Ausfallzeiten und Reisekosten:** Mit AR-Schulungen entfällt die Notwendigkeit, schweres Gerät für Übungszwecke zu transportieren oder Mitarbeitende an einen zentralen Trainingsort zu schicken.
- **Verbesserte Merkfähigkeit:** Interaktive Trainings, bei denen die Lernenden aktiv mit virtuellen Objekten interagieren müssen, führen zu einer rascheren Verhaltensänderung und unterstützen die Fähigkeit, sich das Gelernte langfristig zu merken.

Nachteile

Trotz der zahlreichen Vorteile birgt der Einsatz von Extended Reality (XR) im Arbeitnehmer:innenschutz auch Nachteile und Risiken, besonders in gesundheitlicher bzw. psychischer/kognitiver Hinsicht, die sorgfältig abgewogen werden müssen.

- **Motion Sickness:** Viele Nutzende klagen über Schwindel, Übelkeit oder Kopfschmerzen, ausgelöst durch die visuelle Wahrnehmung von Bewegung in einer statischen Position.
- **Augenbelastung:** Die Displays in VR-Headsets oder AR-Brillen befinden sich sehr nahe an den Augen. Längere Nutzung kann zu Augenermüdung, brennenden Augen und verschwommener Sicht führen.
- **Erhöhtes Unfallrisiko:** Bei AR-Anwendungen können eingeblendete Informationen die Sicht auf die reale Umgebung verfälschen bzw. beeinträchtigen und so die Stolper- oder Kollisionsgefahr begünstigen. Bei VR-Anwendungen steigt durch die Isolation von der realen Umgebung die Unfallwahrscheinlichkeit erheblich.
- **Körperliche Beschwerden:** Schwere VR-Brillen können Nacken- und Kopfschmerzen verursachen.
- **Kognitive Überlastung:** Die Fülle an Eindrücken in einer immersiven XR-Umgebung kann für einige Nutzende überwältigend sein und zu Überforderung führen.
- **Verändertes Gefahrenbewusstsein:** Es besteht die Gefahr, dass Arbeitnehmende Risiken in der realen Welt weniger ernst nehmen, weil sie an das „gefahrlose“, jedenfalls aber konsequenzlose Training in der virtuellen Welt gewöhnt sind.
- **Desorientierung:** Der intensive Einsatz von XR kann in einigen Fällen zu Desorientierung, Isolation und Konzentrationsschwierigkeiten führen.

4.3 Weitere digitale Tools (Drohnen, Online-Schulungsplattformen)

Es gibt eine Vielzahl weiterer digitaler Tools, die den Arbeitnehmer:innenschutz verbessern und dabei helfen, sowohl Gefährdungen zu erkennen als auch die Sicherheit und Gesundheit der Arbeitnehmenden

zu fördern. Im Folgenden werden einige zusätzliche digitale Werkzeuge vorgestellt, die im Arbeitnehmer:innenschutz eingesetzt werden.

4.3.1 Drohnen



Merkmale

Drohnen (auch unbemannte Fluggeräte oder UAVs – Unmanned Aerial Vehicles – genannt) sind Fluggeräte, die ohne Pilot:in an Bord betrieben werden. Sie werden entweder ferngesteuert oder autonom durch Computerprogramme und Sensoren gesteuert. Die Auswahl

an Modellen ist inzwischen sehr vielfältig. Es gibt kleine Drohnen, die nicht selten auch als „Spielzeug“ privat im Einsatz sind, wie auch sehr große Modelle. Drohnen können mit Kameras, GPS, Infrarotsensoren oder Laser ausgestattet sein.

Einsatzmöglichkeiten im Arbeitnehmer:innenschutz

Landwirtschaft

Drohnen haben sich in der Landwirtschaft als vielseitiges Werkzeug etabliert. Sie unterstützen Landwirte:Landwirtinnen dabei, effizienter, nachhaltiger und sicherer zu arbeiten (z. B. Überwachung von Feldern, Ausbringen von Pflanzenschutzmitteln).

Industrie- und Bauwesen

Drohnen sind im Industrie- und Bauwesen inzwischen ein essenzielles Werkzeug. Sie erhöhen Sicherheit, Effizienz und Transparenz, insbesondere dort, wo Arbeiten gefährlich, zeitaufwendig oder teuer sind (z. B. Inspektionen von Gebäuden, Vermessungen).

Rettung und Katastrophenschutz

Drohnen sind im Rettungswesen und Katastrophenschutz ein unverzichtbares Einsatzmittel geworden. Sie liefern schnell Lagebilder, erhöhen die Sicherheit der Einsatzkräfte und unterstützen die effiziente Rettung von Menschenleben – besonders dort, wo Zeit, Übersicht und Zugänglichkeit entscheidend sind (z. B. Suche nach Vermissten, Lageerkundung bei Bränden oder Überschwemmungen).

Militär

Drohnen sind heute ein zentrales Mittel moderner Streitkräfte. Ihr Einsatz reicht von Aufklärung über logistische Belange bis hin zu bewaffneten Operationen.

Vorteile

- **Erreichen schwer zugänglicher Orte:** Mit Drohnen lassen sich Dächer, hohe Bauwerke, Industrieanlagen, Brücken oder Gerüste inspizieren, ohne dass sich Mitarbeitende in Gefahr begeben müssen.
- **Reduzieren von Risiken für Menschen (z. B. bei gefährlichen Einsätzen):** Mithilfe von Drohnen kann man Risse, Korrosion, Lecks, Brandgefahren oder instabile Strukturen erkennen.
- **Schnelles und effizientes Arbeiten:** Große Areale werden schnell und sicher überwacht. Drohnen können gefährliche Zonen automatisch überwachen, ohne dass Mitarbeitende direkt eingreifen müssen.

Nachteile

- **Datenschutz und Privatsphäre:** Aufnahmen von Mitarbeitenden können die Privatsphäre verletzen.
- **Luftverkehrssicherheit:** Gesetze zur Datensicherheit und DSGVO müssen eingehalten werden.
- **Gesetzliche Regelungen (z. B. Flugverbotszonen):** Drohnenflüge erfordern Genehmigungen in bestimmten Zonen (Industriegelände, Baustellen, städtische Gebiete, Flughafennähe).

4.3.2 Online-Schulungsplattformen, E-Learnings, digitale Erhebungsinstrumente

Merkmale

Online-Plattformen und Apps gelten als digitale Tools, weil sie mithilfe digitaler Technologien gezielt Funktionen bereitstellen, mit denen Menschen Aufgaben erledigen, Prozesse steuern oder Informationen nutzen können. Entscheidend ist dabei nicht das Endgerät, sondern die digitale Funktionsweise. Online-Plattformen und Apps bieten zahlreiche Schulungs- und

Weiterbildungsmöglichkeiten für Betriebe, z. B. Sicherheitskurse, die den Umgang mit Maschinen und Gefahrstoffen lehren. Außerdem bieten E-Learnings die Möglichkeit, Mitarbeitende interaktiv über die Themen Datenschutz, Cybersecurity oder Compliance zu informieren.

Einsatzmöglichkeiten im Arbeitnehmer:innenschutz

Die AUVA hat bereits mehrere Online-Tools bzw. Apps (mit)entwickelt, die zur Unterstützung des Arbeitnehmer:innenschutzes eingesetzt werden können. Diese werden Betrieben bzw. Bildungseinrichtungen zur kostenlosen Nutzung angeboten. Darüber hinaus setzt das AUVA-Präventionsteam in der Beratung von Betrieben und im Rahmen von Veranstaltungen unterschiedliche digitale Analysesysteme und Extended-Reality-Anwendungen ein.

Auf auva.at/digitalesysteme gibt es eine Übersicht zu unterschiedlichen Anwendungen, z.B. Online-Tools und Apps, digitale Analysesysteme und Extended Reality.



Vorteile

- **Beschleunigte Berichterstattung:** Unfälle, Beinaheunfälle und gefährliche Situationen können direkt am Ort des Geschehens per App gemeldet werden. Fotos, Videos und detaillierte Beschreibungen werden unmittelbar hinzugefügt, was den Zeitverzug bei der Meldung reduziert, und die Genauigkeit erhöht.
- **Standardisierte Datenerfassung:** Apps und Online-Tools verwenden strukturierte Eingabefelder und Checklisten. Dadurch wird die Datenqualität verbessert, die Dateneingabe standardisiert und Fehler durch unleserliche handschriftliche Notizen vermieden.
- **Automatisierte Prozesse:** Routineaufgaben wie die Verwaltung von Unterweisungen oder die Erstellung von Berichten lassen sich automatisieren. Diese Vorgangsweise spart Verwaltungsaufwand und reduziert manuelle Fehler.
- **Digitales Dokumentenmanagement:** Dokumente, Berichte und Formulare können zentral in der Cloud gespeichert und verwaltet werden. Dies ermöglicht einen ortsunabhängigen Zugriff, gewährleistet eine revisionssichere Protokollierung und vereinfacht Audits.

Nachteile

Auch wenn Online-Tools und Apps im Arbeitnehmer:innenschutz viele Vorteile bieten, sind auch einige Nachteile zu beachten. Hier geht es vor allem um psychische und kognitive Herausforderungen sowie um das Fehlen persönlicher Kommunikation.

- **Informationsüberflutung:** Der ständige Zugang zu Informationen und Push-Benachrichtigungen führt mitunter zu einer Überlastung der Mitarbeitenden.
- **Ablenkung:** Benachrichtigungen und die Nutzung von Apps während der Arbeit können die Konzentration stören und das Unfallrisiko erhöhen.
- **Erhöhter Leistungsdruck:** Die ständige Verfügbarkeit von Leistungs- und Sicherheitsdaten kann den Druck, konstant perfekt zu arbeiten, erhöhen.
- **Fehlende soziale Komponente:** Digitale Tools können die persönliche Kommunikation ersetzen und dadurch Vertrauen und sozialen Zusammenhalt schwächen.
- **Nicht für alle Zwecke geeignet:** Bestimmte praktische oder soziale Aspekte des Arbeitnehmer:innenschutzes werden durch Online-Tools nicht vollständig abgebildet. So kann ein Online-Training z. B. keine praktische Unterweisung ersetzen.
- **Falsches Sicherheitsgefühl:** Eine übermäßige Fokussierung auf digitale Lösungen führt bisweilen dazu, dass die Mitarbeitenden ein falsches Sicherheitsgefühl entwickeln und grundlegende Sicherheitsregeln nicht ausreichend beachten.





5 Kriterien für die Beschaffung und den Einsatz digitaler Systeme

Bei der Anschaffung einer digitalen Anwendung ist bereits im Vorfeld deren sinnvolle Einbindung in bereits bestehende Unternehmensprozesse zu bedenken.

Im Hinblick auf Datenschutzanforderungen sollte der Zugang möglichst einfach sein.

Folgende Anforderungen gilt es bei der Einführung digitaler Systeme u.a. zu berücksichtigen.

5.1 Datenschutz

Die Datensicherheit ist ein zentrales Thema bei der Nutzung digitaler Systeme – insbesondere bei unterstützenden digitalen Tools, die in verschiedenen Bereichen eingesetzt werden (z. B. im Arbeitnehmer:innenschutz, in der Unternehmensorganisation oder im Gesundheitswesen). Diese Systeme verarbeiten oft sensible oder personenbezogene Daten, weshalb sie bestimmten Anforderungen an die Datensicherheit entsprechen müssen. Insbesondere in sensiblen Bereichen wie dem Gesundheitswesen oder der öffentlichen Verwaltung müssen hohe Standards für den Schutz vertraulicher Daten und die Systemsicherheit gewährleistet sein. Zudem sind gesetzliche Vorgaben einzuhalten. Im Folgenden werden die wichtigsten Anforderungen an die Datensicherheit für digitale Systeme und unterstützende Tools zusammengefasst:

- **Authentifizierung und Autorisierung:** sichere Methoden zur Identifizierung von Nutzenden
- **Verschlüsselung:** Schutz von Daten sowohl bei der Übertragung als auch bei der Speicherung (Ende-zu-Ende-Verschlüsselung, wo angebracht)
- **Integrität der Daten:** Sicherstellung, dass Daten nicht unbemerkt verändert wurden
- **Datensicherung und -wiederherstellung:** Mechanismen zur Sicherstellung der Verfügbarkeit von Daten im Notfall
- **Datenmanagement und -speicherung:** effiziente technische Lösungen für die Speicherung, Verwaltung und Archivierung von Daten, die gesetzlichen Anforderungen entsprechen

5.2 Technik und Interoperabilität

Technische Anforderungen an unterstützende digitale Systeme konzentrieren sich darauf, funktionale Anforderungen durch spezifische technische Spezifikationen zu gewährleisten. Es geht um Aspekte wie Systemarchitektur, Leistung (Performance), Interoperabilität, Sicherheit und Einhaltung spezifischer technischer Standards wie WCAG für Barrierefreiheit.

- **Systemarchitektur:** Die technische Struktur des Systems sollte modular, skalierbar und wartbar sein. Dies ermöglicht es, das System an eine wachsende Zahl von Nutzenden anzupassen und Updates effizient einzuspielen.
- **Performance und Verfügbarkeit:** Das System muss schnell reagieren (geringe Latenz) und eine hohe Verfügbarkeit aufweisen, d. h. zuverlässig und ohne häufige Ausfälle funktionieren.
- **Interoperabilität:** Die Fähigkeit, nahtlos Daten mit anderen Systemen auszutauschen, ist entscheidend. Dies erfordert die Nutzung offener, standardisierter Schnittstellen (APIs) und Datenformate (z. B. nach IEC 62056 oder spezifischen nationalen Standards im Gesundheitswesen).
- **Kompatibilität:** Das System muss auf verschiedenen Geräten und Betriebssystemen sowie mit assistierenden Technologien (wie Screenreadern) stabil laufen.
- **Wartbarkeit und Erweiterbarkeit:** Die Software sollte so entwickelt sein, dass sie leicht gewartet, dass Fehler behoben und neue Funktionen hinzugefügt werden können, ohne das Gesamtsystem zu destabilisieren.

Die Anwendung muss gegenüber externen Ereignissen sowie Fehlfunktionen und Fehlbedingungen robust und stabil betrieben werden können. Es muss möglich sein, die Anwendung jederzeit auf einen früher gespeicherten Zustand oder die Werkseinstellungen zurückzusetzen. Der Zeitpunkt der letzten Aktualisierung ist auf der Vertriebsplattform oder innerhalb der digitalen Anwendung ersichtlich. Die Anwendung wird regelmäßig aktualisiert und an sich ändernde Anforderungen angepasst. Die digitale Anwendung ist mit verschiedenen Betriebssystemen kompatibel.

Hardware: Es müssen geeignete Geräte wie Server, Computer, Netzwerke und andere technische Geräte vorhanden sein.

- **Server:** Server sind leistungsstarke Computer, die Daten verarbeiten und speichern. Sie sind das Rückgrat vieler digitaler Systeme, da sie Anwendungen, Datenbanken und andere Softwaredienste bereitstellen.

- **Datenzentren:** In vielen Fällen werden Server in spezialisierten Rechenzentren betrieben. Diese Einrichtungen sind mit leistungsstarker Klimaanlage, Notstromversorgung und Sicherheitsmechanismen ausgestattet, um den kontinuierlichen Betrieb sicherzustellen.
- **Endgeräte:** Computer, Tablets, Smartphones und andere Geräte, die von Benutzenden zum Zugriff auf digitale Systeme verwendet werden. Diese Geräte müssen ausreichend leistungsfähig sein, um Anwendungen und digitale Dienste ausführen zu können.
- **Netzwerkhardware:** Router, Switches, Firewalls und Netzwerkkarten sind notwendig, um Netzwerke zu verbinden, Daten zu übertragen und Sicherheitsmechanismen durchzusetzen.
- **Speicherlösungen:** Speicherhardware (z. B. Festplatten, SSDs, SANs – Storage Area Networks) sorgt für die dauerhafte Speicherung von Daten, auf die digitale Systeme zugreifen können.

Software: In diesem Zusammenhang geht es um notwendige Softwarelösungen, die das digitale System unterstützen (z. B. Betriebssysteme, Anwendungen, Sicherheitssoftware).

- **Betriebssysteme:** Software – wie Windows, Linux oder macOS – ermöglicht den Betrieb von Servern und Endgeräten. Sie verwaltet Ressourcen und bietet die grundlegenden Funktionen, die es für die Ausführung von Anwendungen braucht.
- **Datenbanken:** Digitale Systeme benötigen Datenbanken (z. B. MySQL, PostgreSQL, Oracle), um große Mengen an strukturierten Daten effizient zu speichern und darauf zuzugreifen.
- **Anwendungen und Dienste:** Spezifische Softwarelösungen unterstützen die Geschäftsprozesse (z. B. CRM-Software, Office-Anwendungen).

Cloud-Computing: Bei Bedarf sollte eine zuverlässige Cloud-Infrastruktur zur Verfügung stehen, um Ressourcen flexibel und skalierbar zu nutzen.

- **Cloud-Integration:** Viele digitale Systeme nutzen Cloud-Dienste, daher muss das Netzwerk eine stabile und schnelle Anbindung an die Cloud ermöglichen. Dies erfordert eine leistungsstarke Internetverbindung und gegebenenfalls VPNs oder dedizierte Verbindungen zu Cloud-Providern.
- **Zugriff von verschiedenen Geräten:** Netzwerke sollten den Zugriff auf digitale Systeme von verschiedenen Geräten (Laptops, Smartphones, Tablets) ermöglichen. Dies ist durch mobile Netzwerktechnologien und sichere, skalierbare Verbindungen zu gewährleisten.

5.3 Inhalt und Gebrauchstauglichkeit

Organisatorische Anforderungen an unterstützende digitale Systeme befassen sich mit den nicht technischen Rahmenbedingungen und Prozessen, die für die erfolgreiche Einführung, Nutzung und Aufrechterhaltung dieser Systeme in einer Organisation bzw. im Betrieb notwendig sind.

- **Strategische Verankerung:** Die Einführung und Nutzung der Systeme muss in die Gesamtstrategie der Organisation eingebettet sein. Es muss eine klare Vision und Zielsetzung geben, wie die Systeme die Unternehmensziele unterstützen sollen.
- **Top-Management-Unterstützung:** Das Projekt benötigt die Rückendeckung der Führungsebene, damit die notwendigen Ressourcen und die Autorität für Veränderungen bereitgestellt werden können.
- **Prozessanpassung und -integration:** Die bestehenden Arbeitsprozesse müssen oft angepasst oder neu gestaltet werden, damit die digitalen Systeme optimal integriert werden können. Die Systeme dürfen nicht als isolierte Insellösungen betrachtet werden, sondern müssen die Arbeitsabläufe sinnvoll unterstützen.
- **Benutzendenzentrierung und Akzeptanz:**
 - ◆ **Nutzendeneinbindung:** Die Endnutzenden sollten von Anfang an in den Auswahl- und Gestaltungsprozess einbezogen werden, um sicherzustellen, dass das System ihren Bedürfnissen entspricht und Akzeptanz findet.
 - ◆ **Kommunikation:** Offene und transparente Kommunikation über die Gründe, den Nutzen und die Auswirkungen des neuen Systems hilft, Ängste und Widerstände abzubauen.
- **Schulung und Support für Mitarbeitende:** Es muss sichergestellt werden, dass alle Nutzenden angemessen geschult werden und kontinuierlichen Support erhalten. Dies umfasst:
 - ◆ Initialschulungen zur Bedienung des Systems
 - ◆ laufende Helpdeskbetreuung oder Ansprechpartner:innen für Fragen und Probleme
 - ◆ regelmäßige Fortbildungen bei Systemaktualisierungen
- **Change Management (Veränderungsmanagement):** Die Einführung neuer Systeme bedeutet oft eine kulturelle Veränderung im Betrieb. Ein aktives Change Management ist erforderlich, um Akzeptanz zu schaffen, Widerstände abzubauen und die Mitarbeitenden von den Vorteilen der neuen Systeme zu überzeugen, damit diese sie auch nutzen.



© Gordenkoff – stock.adobe.com

6 Chancen und Risiken

Die Einführung und die Nutzung digitaler Systeme bringen neben allen Vorteilen auch Herausforderungen mit sich. Die Entscheidung, digitale Systeme einzuführen, muss sorgfältig überdacht werden, da die Auswirkungen

auf verschiedene Aspekte eines Unternehmens oder einer Organisation erheblich sein können. Im Folgenden werden die wesentlichen Vor- und Nachteile digitaler Systeme aufgeführt.

6.1 Möglichkeiten oder Chancen digitaler Systeme

Effizienzsteigerung und Automatisierung

Routineaufgaben werden automatisiert, wodurch menschliche Arbeitskraft für komplexe Tätigkeiten freigesetzt wird, und Fehler reduziert werden.

Beispiel Industrieroboter und Chatbots: In der Fertigung übernehmen Industrieroboter und automatisierte Logistiksysteme monotone Aufgaben, in der Verwaltung wickeln Chatbots erste Kunden-:Kundinnen-anfragen ab und nehmen E-Mail-Sortierungen vor.

Bessere Datenverarbeitung und -analyse

Digitale Systeme bieten leistungsstarke Tools zur Sammlung, Speicherung und Analyse von Daten. Unternehmen können so schneller fundierte Entscheidungen treffen, Trends erkennen und Prognosen erstellen.

Beispiel Medizin: Digitale Systeme in Laboren lesen automatisch Analyseergebnisse aus Messgeräten aus und übertragen sie direkt in Patienten-:Patientinnenakten. Dies verhindert Abschreibfehler bei der Dokumentation.

Zugänglichkeit und Flexibilität

Digitale Systeme (insbesondere Cloud-Dienste) bieten den Vorteil, von überall aus zugänglich zu sein. Das bedeutet, dass Mitarbeitende und Führungskräfte auch remote arbeiten oder auf Unternehmensressourcen zugreifen können.

Beispiel Remote Work (Heimarbeit): Mitarbeitende können dank Cloud-Technologien, VPN-Verbindungen und Kollaborationstools von nahezu jedem Ort der Welt aus arbeiten.

Kostenersparnis

Auf lange Sicht senken digitale Systeme die Betriebskosten, da viele manuelle Aufgaben automatisiert werden und dadurch weniger Personal erforderlich ist. Auch die Reduzierung von Papierverbrauch, Lagerräumen und physischen Archiven spart Geld.

Beispiel Predictive Maintenance (vorausschauende Wartung): Durch die Analyse von Sensordaten lässt sich der Wartungsbedarf von Maschinen genau vorhersagen. Wartungen finden nur dann statt, wenn sie notwendig sind.

Skalierbarkeit

Digitale Systeme, insbesondere Cloud-basierte Lösungen, ermöglichen eine schnelle Skalierung, wenn das Unternehmen wächst. Es ist einfach, die Ressourcen je nach Bedarf zu erweitern oder zu reduzieren, ohne dass erhebliche Investitionen in Hardware oder Infrastruktur erforderlich sind.

Beispiel Start-up: Ein Start-up beginnt mit minimalen IT-Kosten und skaliert die Infrastruktur parallel zum Wachstum der Nutzenden. Es muss keine hohen Anfangsinvestitionen in Hardware tätigen und zahlt nur für die Ressourcen, die es zum jeweiligen Zeitpunkt benötigt.

Verbesserte Kommunikation und Zusammenarbeit

Digitale Systeme verbessern die Kommunikation innerhalb von Teams und zwischen Abteilungen. Tools wie E-Mail, Instant Messaging, Videokonferenzen und Projektmanagement-Software erleichtern die Zusammenarbeit, speziell in globalen oder remote arbeitenden Teams.

Beispiel Krisenmanagement: Bei Notfällen übermitteln digitale Kommunikationssysteme Informationen in Echtzeit, um schnelle und koordinierte Entscheidungen von Rettungskräften oder Management-Teams zu ermöglichen.

Wettbewerbsvorteil

Unternehmen, die digitale Systeme effektiv nutzen, können einen technologischen Vorsprung gegenüber Mitbewerbern:Mitbewerberinnen erzielen. Sie sind in der Lage, schneller auf Marktveränderungen zu reagieren, innovative Produkte und Dienstleistungen anzubieten und eine bessere Kunden-:Kundinnenbindung aufzubauen.

Beispiel Einzelhandel: Durch die Analyse von Big Data erkennen Einzelhändler:innen Trends vor der Konkurrenz, sie verwalten Lagerbestände proaktiv und treffen strategische Preisentscheidungen.

6.2 Herausforderungen oder Risiken digitaler Systeme

Hohe Anfangsinvestitionen

Die Einführung digitaler Systeme kann mit hohen Kosten verbunden sein, sowohl in Bezug auf die Technologie (Software, Hardware) als auch auf die Schulung der Mitarbeitenden. Unternehmen müssen möglicherweise auch in Infrastruktur, IT-Support und Sicherheitslösungen investieren.

Beispiel Wartung und Updates: Die Kosten für die laufende Wartung, Sicherheits-Updates und Upgrades digitaler Systeme über viele Jahre hinweg werden oft nicht realistisch einkalkuliert.

Komplexität und Anpassungsbedarf

Die Implementierung neuer digitaler Systeme ist mitunter komplex und erfordert eine sorgfältige Planung. Oft müssen bestehende Prozesse angepasst oder neu strukturiert werden, was zusätzlichen Aufwand bedeutet.

Beispiel Vorbehalte, Bedenken der Mitarbeitenden (Change Management): Mitarbeitende sind oft an ihre alten, vertrauten Arbeitsweisen gewöhnt. Der Anpassungsbedarf an neue digitale Tools und Prozesse kann auf Widerstand stoßen, was die Akzeptanz und den Erfolg des Systems gefährdet.

Abhängigkeit von Technologie

Eine starke Abhängigkeit von digitalen Systemen kann gefährlich werden, insbesondere wenn Fehler auftreten oder es zu größeren Ausfällen kommt. Systemausfälle oder Softwareprobleme beeinträchtigen den Betrieb oft erheblich.

Beispiel veraltete Betriebssysteme: Organisationen, die weiterhin mit veralteten Betriebssystemen arbeiten (oft aus Kostengründen), sind anfälliger für Cyberangriffe, da keine Sicherheitsupdates mehr bereitgestellt werden.

Sicherheitsrisiken

Digitale Systeme sind anfällig für Cyberangriffe, Datenlecks und andere Sicherheitsrisiken. Hacker-, Malware- und Phishing-Angriffe können zu erheblichen Schäden führen, wenn die Sicherheitsinfrastruktur nicht ausreichend ist.

Beispiel laufende Aktualisierungen: Unternehmen müssen kontinuierlich in Sicherheitslösungen investieren, regelmäßige Updates durchführen und ihre Mitarbeitenden in Sicherheitsfragen schulen, um entsprechende Risiken zu minimieren.

Datenmanagement und Datenschutz

Die Verarbeitung großer Datenmengen erfordert eine sorgfältige Verwaltung, insbesondere in Bezug auf Datenschutz und Compliance. Unternehmen müssen sicherstellen, dass sie die rechtlichen Anforderungen erfüllen (z. B. DSGVO in der EU) und die Daten ihrer Kunden:Kundinnen und Mitarbeitenden angemessen schützen.

Eine unzureichende Datenstrategie kann zu Problemen bei der Qualität, Speicherung und Nutzung von Daten führen.

Beispiel Überwachung am Arbeitsplatz: Digitale Systeme ermöglichen es Arbeitgebenden, die Leistung und das Verhalten von Mitarbeitenden detailliert zu überwachen. Dies wirft Bedenken hinsichtlich der Privatsphäre und des Vertrauens auf.

Schulungsbedarf und Widerstand der Mitarbeitenden

Der Übergang zu digitalen Systemen erfordert oft umfangreiche Schulungen für Mitarbeitende. Sie müssen mit der neuen Technologie vertraut gemacht werden, was Zeit und Ressourcen in Anspruch nimmt. Es kann Widerstand gegen Veränderungen geben, insbesondere bei älteren Mitarbeitenden oder solchen, die nicht mit digitalen Tools vertraut sind. Dieser Widerstand erschwert die Implementierung.

Beispiel ältere Belegschaft in der Verwaltung: Diese benötigen möglicherweise mehr Geduld und intensivere Schulungen, um den Umgang mit digitalen Workflow-Systemen zu erlernen. Wenn diese Schulungen unzureichend sind, kann dies zu Frustration und Ineffizienz führen.

Verlust persönlicher Interaktion

Digitale Systeme können die persönliche Kommunikation in Unternehmen verringern, was unter Umständen zu einer Entfremdung von Mitarbeitenden oder zu einer Abnahme des Teamzusammenhalts führen würde. Besonders in kreativen oder kollaborativen Arbeitsumfeldern wären durch den Verlust von persönlichen Interaktionen die Innovationskraft und das Engagement beeinträchtigt.

Beispiel Home Office: Mitarbeitende, die überwiegend von zu Hause aus arbeiten, sehen ihre Kollegen:Kollegerinnen seltener. Der Verlust des informellen „Kaffeeküchen-Gesprächs“ kann zu Gefühlen der Isolation führen und die emotionale Bindung zum Unternehmen schwächen.

Veraltete Technologie

Die rasante Weiterentwicklung der Technologie bewirkt, dass digitale Systeme schnell veralten. Unternehmen müssen regelmäßig investieren, um mit den neuesten technologischen Entwicklungen Schritt zu halten und ihre Systeme zu aktualisieren. Dies verursacht nicht nur zusätzliche Kosten, sondern bringt auch die Notwendigkeit mit sich, bestehende Systeme zu migrieren oder neu zu integrieren.

Beispiel Datenmigration: Beim Versuch, Daten aus einem alten Datenbanksystem in ein neues, modernes ERP-System zu migrieren, können Inkompatibilitäten bei Datenformaten oder Schnittstellen zu erheblichem manuellem Aufwand, Datenverlust oder Projektverzögerungen führen.

Einsatz von digitalen Systemen im Arbeitnehmer:innenschutz

Bitte wenden Sie sich in allen Fragen des Gesundheitsschutzes und der Sicherheit bei der Arbeit an den Unfallverhütungsdienst der für Sie zuständigen AUVA-Landesstelle:

Oberösterreich:

UVD der Landesstelle Linz
Garnisonstraße 5, 4010 Linz
Telefon +43 5 93 93-32701

Salzburg, Tirol und Vorarlberg:

UVD der Landesstelle Salzburg
Dr.-Franz-Rehrl-Platz 5, 5010 Salzburg
Telefon +43 5 93 93-34701

UVD der Außenstelle Innsbruck
Ing.-Etzel-Straße 17, 6020 Innsbruck
Telefon +43 5 93 93-34837

UVD der Außenstelle Dornbirn
Eisengasse 12, 6850 Dornbirn
Telefon +43 5 93 93-34932

Steiermark und Kärnten:

UVD der Landesstelle Graz
Göstinger Straße 26, 8020 Graz
Telefon +43 5 93 93-33701

UVD der Außenstelle Klagenfurt am Wörthersee
Waidmannsdorfer Straße 42,
9020 Klagenfurt am Wörthersee
Telefon +43 5 93 93-33830

Wien, Niederösterreich und Burgenland:

UVD der Landesstelle Wien
Wienerbergstraße 11, 1100 Wien
Telefon +43 5 93 93-31701

UVD der Außenstelle St. Pölten
Kremser Landstraße 8, 3100 St. Pölten
Telefon +43 5 93 93-31828

UVD der Außenstelle Oberwart
Hauptplatz 11, 7400 Oberwart
Telefon +43 5 93 93-31901

Das barrierefreie PDF dieses Dokuments gemäß PDF/UA-Standard ist unter auva.at/downloads abrufbar.

Medieninhaber und Hersteller: Allgemeine Unfallversicherungsanstalt, Wienerbergstraße 11, 1100 Wien
Verlags- und Herstellungsort: Wien

HUB - M.plus 930 – 02/2025 – nom / htp

Titelbild: © Kannapat – stock.adobe.com

Fotos: stock.adobe.com; KI-generierte Bilder: Sora AI – Barbeitung: © AUVA / Attila Primus

Layout: Oanh Ho