personal manager

Zeitschrift für Human Resources

12,50 Euro

1 Jänner / Februar 2017

www.personal-manager.at

Personalarbeit in unsicheren Zeiten

- **Terroranschläge, Cyberattacken, Wirtschaftskriminalität: HR-Management in der Krise**
- **Die Angst vor dem Jobverlust: Vom Mensch in der digitalen Fabrik**

Wolfgang Mazal
Arbeitsrechtler und Familienforscher

Karriere mit Familie

Wolfgang Mazal beschreibt im aktuellen Interview, warum sich Familienfreundlichkeit auszahlt

Die Richtigen finden

Cultural Fit: Lässt sich kulturelle Passung messen?

Zukunft des Lernens

Quantified Self – Gamification – Kollaboration

9 190001 012506 01

ISSN 1612-2836
Verlagsort 1230 Wien
P.b.b. 10Z038386M

www.hrm.at/profiles/
bettina-geuenich

Liebe Leserinnen und Leser,

ging es Ihnen auch so? In den vergangenen Monaten mochte ich die Zeitung teilweise nicht mehr aufschlagen angesichts der vielen Krisen und Katastrophen, die mir dort entgegenschlugen. Die Kriege außerhalb Europas, die Flüchtlingsschicksale, die daraus folgten, die Terroranschläge, die politischen Spaltungen des Kontinents und die steigenden Arbeitslosenzahlen ergaben eine Melange aus Trauer, Bedrohung und Angst, die das Stimmungsbild beherrschte.

Auch die Veränderungen in der Arbeitswelt lösen bei vielen Menschen das Gefühl aus, in unsicheren Zeiten zu leben und latent bedroht zu sein. Die Angst, dass Roboter uns die Arbeit wegnehmen; die Befürchtung, abgehängt zu werden in einer komplexer werdenden Welt, ist allgegenwärtig.

Kein Wunder also, dass viele Österreicherinnen und Österreicher mit Skepsis oder Sorge in die Zukunft blicken, wie eine repräsentative IMAS-Studie vom September zeigt. Nur 23 Prozent äußerten sich in der Befragung zuversichtlich. „Die Sorgenfalten sitzen tief: It's the Abstiegsangst, stupid", betitelte das Institut seinen Bericht.

Was heißt das alles für HR? In dieser Ausgabe beschäftigen wir uns im Titelthema „Personalarbeit in unsicheren Zeiten" mit den realen und herbeigeredeten Bedrohungen, die unsere Lebens- und Arbeitswelt aktuell prägen. Wir gehen der Frage nach, welchen Einfluss die aktuelle geopolitische Lage auf Wirtschaft und Personalmanagement hat und mit welchen Krisenszenarien Unternehmen wirklich rechnen sollten (S. 12). Dabei gehen wir unter anderem auf die Gefahren durch Cyberattacken und Datenklau im Personalbereich ein und geben Tipps für die Prävention (S. 17). Wie Arbeitgeber Notfallpläne entwickeln (S. 14), Krisenmanager schulen und im Ernstfall gekonnt kommunizieren (S. 20), sind Themen weiterer Beiträge.

Außerdem befassen wir uns mit den Auswirkungen der Automatisierung auf den Menschen (S. 23) und beschreiben, welche Trends die Arbeitswelt von morgen verändern (S. 26).

Eine spannende Lektüre wünscht Ihnen

Ihre

Bettina Geuenich

Drei Fragen an ...

Foto: Aziz-Trebesiner

Yasmin Aziz-Trebesiner,
Leitung Personalentwicklung/Recruiting,
Österreichisches Verkehrsbüro AG

Beim Verkehrsbüro kann man sich seit einiger Zeit in 140 Zeichen bewerben. Wie wird die Quick-Bewerbung genutzt?
Die Suche nach attraktiven Arbeitgebern erfolgt längst nicht mehr nur zu Hause, sondern auch im Zug, beim Warten auf den Bus oder in der Warteschlange beim Einkaufen. Aus diesem Grund haben wir eine mobile Plattform entworfen, auf der sich interessierte User per Smartphone einen schnellen Überblick über die Karrieremöglichkeiten des Unternehmens verschaffen können. Als besonderes Feature haben wir darin auch die Möglichkeit zur Quickbewerbung integriert. Damit haben User die Möglichkeit, sich einfach und schnell bei der Verkehrsbüro Group mit 140 Zeichen zu bewerben. Wir nehmen anschließend Kontakt mit den Bewerbern auf und gehen aktiv auf Bewerber zu.

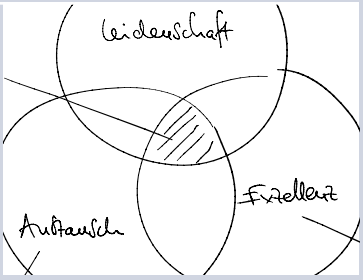
Wie gut ist die Qualität der Bewerbungen, die per Kurznachricht reinkommen?
Die Qualität ist durchwachsen – und abhängig von der Position. Wir bekommen aber durchaus interessante und vor allem kreative Bewerbungen. Die Bewerber freuen sich, dass das Unternehmen Kontakt aufnimmt und nicht immer die Bewerber alle Unterlagen zusenden müssen.

Welche weiteren Kanäle/Methoden nutzen Sie, um gute Bewerber zu finden?
Die Verkehrsbüro Group ist auf den meisten Social-Media-Kanälen vertreten, wir suchen den direkten Kontakt zu Schulen und veranstalten Exkursionen mit Schulklassen, zum Beispiel mit Besichtigung von Hotels.

© currycom

10

Bei currycom communications in Wien ist nicht nur der Kunde, sondern auch der Mitarbeiter König. Die Kommunikationsagentur mit 25 Beschäftigten leistet sich eine HR-Stabsstelle und legt Wert auf einen wertschätzenden Umgang mit den Mitarbeitern. Wie das in der Praxis aussieht, beschreiben Geschäftsführer Christian Krpoun und HR-Verantwortliche Barbara Goldschmidt.



© Fink

30

Worin besteht der Sinn unserer Arbeit und unseres Unternehmens? Der zweite Teil der Serie „Zukunft der Organisation" beleuchtet das Prinzip der „purpose-driven organisation" am Beispiel der Unternehmen Airbnb und Zappos.

48

Passende Lehrlinge zu finden ist nicht einfach. Daher gehen immer mehr Unternehmen dazu über, ihre Lehrlingskommunikation individuell auf bestimmte Zielgruppen abzustimmen. Wie das funktioniert, zeigen die Beispiele dm und Lidl Österreich.

58

Auf dem E-Learning-Markt ist einiges in Bewegung. Wir beschreiben Anwendungsbeispiele aus der Praxis, die repräsentativ für drei Trends im E-Learning stehen: Quantified Self, Gamification und Kollaboration. Außerdem stellen wir Softwareanbieter und ihre E-Learning-Lösungen im Überblick vor.

Liebe Leserinnen und Leser, in unseren Artikeln verwenden wir das generische Maskulinum. Damit sprechen wir sowohl Frauen als auch Männer an.

Titelbild: © ra2 studio - Fotolia.com | Titelporträtbild: Mazal

Foto: Deloitte

Autor
Gilbert Wondracek
Manager im Bereich Risk Advisory,
Deloitte Österreich

Personaldaten im Visier
Wie sich Unternehmen vor Cyberkriminalität schützen

Viele Unternehmen unterschätzen die Gefahren, die von Cybercrime ausgehen, obwohl ein Datendiebstahl weitreichende Folgen haben kann. Gerade sensible Personaldaten sind für Internetkriminelle ein interessantes Angriffsziel. Unternehmen und ihre HR-Abteilungen sind daher gut beraten, das Thema ernst zu nehmen und besser heute als morgen, entsprechend ihren individuellen Bedürfnissen, vorzubeugen.

Cybercrime ist seit einiger Zeit verstärkt ins öffentliche Bewusstsein getreten, denn die wirtschaftlichen, politischen und gesellschaftlichen Auswirkungen der Internetkriminalität sind zunehmend sichtbar. Gigantische Online-Diebstähle von mehreren Hundert Millionen Datensätzen oder betrügerische Aktivitäten durch Cyberangriffe, wie etwa bei der Deutschen Telekom, deren Kundendaten im Netz zum Verkauf angeboten wurden, verdeutlichen den Aufwand, den Datendiebe und Hacker betreiben. Das wirtschaftliche Interesse, Zugang zu vertraulichen und oft auch personenbezogenen Daten für kriminelle Zwecke (zum Beispiel Erpressung oder Weiterverkauf) zu erlangen, ist in den letzten Jahren enorm gestiegen. Das amerikanische Wirtschaftsmagazin Forbes schätzt den weltweiten Gesamtschaden für Unternehmen auf mehrere Hundert Milliarden Dollar pro Jahr. Die Internetkriminalität hat nach Angaben von Europol sogar schon den internationalen Drogenhandel an Profitabilität überholt und ist ein hochprofessionelles globales Business.

Auch in Österreich sind verstärkt Cyberangriffe zu beobachten. Dieser Trend wird sich in Zukunft durch die Digitalisierung weiter beschleunigen. Dabei sind die aus den Medien bekannten Fälle, wie etwa der Angriff auf die Telekom Austria, bei dem Angreifer mit erpresserischen Absichten das mobile Datennetz gezielt überlasteten und zum Erliegen brachten, nur die Spitze des Eisbergs. Experten gehen von einer hohen Dunkelziffer bei Cyberangriffen gegen Unternehmen und deren Mitarbeiter aus – entweder weil Unternehmen die Attacken nicht öffentlich machen oder weil sie diese schlicht nicht entdecken. Dass ein Angriff auf ein Computernetzwerk eines Unternehmens monatelang unbemerkt bleibt, ist kein Einzelfall.

Kein Unternehmen ist sicher

Kein Unternehmen kann sich entspannt zurücklehnen und darauf hoffen, zufällig nicht ins Visier der Cyberkriminellen zu geraten. Dazu sind die Vorgehensweisen der Datendiebe zu strukturiert und systematisch. Gezielt richten sie ihre Angriffe gegen einzelne Branchen und operieren dabei mit weitreichenden Spezialkenntnissen. Besonders beunruhigend sind dabei der zunehmende Spezialisierungsgrad sowie die Dynamik der Angriffsmethoden. Noch vor einigen Jahren waren eher technisch orientierte oder wenig spezifische Angriffe in der Überzahl. Ein Beispiel dafür sind die klassischen Phishing-

mails, die an eine Vielzahl von Empfängern verschickt werden und mit fadenscheinigen Begründungen zur Preisgabe von Passwörtern oder zum Öffnen von Schadsoftware auffordern. Solche betrügerischen E-Mails sind oft an den zahlreichen Rechtschreibfehlern oder dem offensichtlich falschen Namen des Adressaten leicht zu erkennen.

Die Methoden haben sich heute deutlich verändert: Die Angriffe werden gezielter und richten sich konkret gegen kleine Gruppen oder einzelne Mitarbeiter eines Unternehmens, über die sie gezielt an Informationen kommen wollen. Der Fokus liegt dabei vor allem auf kritischen Abteilungen oder Bereichen, wie etwa HR oder Rechnungswesen, da diese den Zugriff auf umfassende Daten über Mitarbeiter oder Zahlungsvorgänge haben.

Angriffsziel Personalmanagement

Personalabteilungen sind ein besonders interessantes Ziel für Angreifer. Das Vorhandensein von sensiblen Daten wie etwa Mitarbeiter- oder Gehaltslisten und ein oft privilegierter Zugang der HR-Mitarbeiter zu diesen Ressourcen im Unternehmen sind eine verlockende Kombination für Cyberkriminelle. Die Palette der Missbrauchsszenarien reicht dabei von der direkten Verwertung der Mitarbeiterdaten, wie etwa dem Weiterverkauf, über die betrügerische Veränderung der Stammdaten, um beispielsweise Gehaltszahlungen auf fremde Konten umzuleiten, bis hin zur Ermöglichung weiterführender Angriffe durch gestohlene Zugangsdaten oder der Erpressung durch angedrohte Veröffentlichung der Daten.

HR-Systeme stellen meist die Schnittstelle für das Zusammenspiel zwischen Identitäten („Wer?"), also Mitarbeitern, und Unternehmensressourcen („Was?") dar. Typischerweise vergibt die HR-Abteilung Zugriffsrechte auf Anwendungen und Datenspeicher und ermöglicht den Zutritt zu Gebäuden. Das ist beispielsweise der Fall beim Ein- oder Austritt von Mitarbeitern oder auch beim Wechsel der Abteilung oder des Aufgabengebiets.

Im schlimmsten Fall erfolgen die Freigaben uneinheitlich auf Basis von Ad-hoc-Veränderungen, also quasi auf „Zuruf", oder sie sind nicht ausreichend organisatorisch abgesichert, zum Beispiel dadurch, dass zwei Personen ihnen zustimmen müssen. Ein Beispiel: Zugriffsrechte werden „dringend" mündlich bei einem Kollegen angefordert, der die administrativen Rechte hat und dies ohne Dokumentation oder Rücksprache im System umsetzt. Das ist besonders gefährlich. Denn wenn Betrüger solche Zugänge mit umfassenden Zugriffsrechten knacken, haben sie die Möglichkeit, andere sensible Informationen zu erlangen, finanzielle Transaktionen zulasten des angegriffenen Unternehmens durchzuführen oder weiter reichende Angriffe zu starten. Besonders wenn die umliegenden Prozess- und Kontrolllandschaften historisch gewachsen sind oder ausschließlich vor „traditionellem" Betrug schützen sollen, ist Gefahr im Verzug. Sind die Mitarbeiter dann auch noch unzureichend über aktuelle Angriffsmuster oder Vorgangsweisen von Kriminellen aufgeklärt, ist früher oder später mit einem Schaden für das Unternehmen zu rechnen.

Typische Risiken

Welchen Bedrohungen ein Unternehmen ausgesetzt ist und wie es vorbeugen und reagieren kann, lässt sich nur durch einen strukturierten Prozess auf Risikobasis ermitteln. Einige typische Fallstricke und Schwachstellen gibt es jedoch bei fast jedem Unternehmen.

1. Mangelndes Bewusstsein

Die Erfahrung zeigt, dass der Bereich Cybersicherheit traditionell in der IT-Abteilung oder bei dem Verantwortlichen für Informationssicherheit angesiedelt ist. Die Übertragung der Verantwortung auf diese kleinen Bereiche erweist sich jedoch meist als zu eingeschränkt. Dadurch werden nämlich wesentliche Risiken nicht erkannt und logischerweise auch nicht abgedeckt. Die Angriffe, die aktuell zu beobachten sind, kombinieren Schritte gegen Mitarbeiter und Technik und erfolgen mit dem Wissen über typische Abläufe in den Unternehmen. Zum Beispiel werden zunächst Mitarbeiter angerufen und unter einem Vorwand („Hier spricht Ihre IT-Security, wir müssen etwas testen") angehalten, eine Datei herunterzuladen und Alarme zu ignorieren. In solchen Fällen gilt dann das Prinzip des schwächsten Glieds der Kette. Wenn über organisatorische Grenzen hinweg kein einheitliches Sicherheitsbewusstsein herrscht, wenn Schnittstellen unklar definiert sind oder eine „Helikopterperspektive" bei der Planung von Sicherheitsvorkehrungen fehlt, ist das Risiko groß, dass Angreifer diese Schwachstellen gezielt ausnutzen.

Die IT-Abteilung kann im HR-Bereich hervorragend unterstützen, aber die Mitwirkung der betroffenen Mitarbeiter lässt sich dadurch nicht ersetzen. So gilt es, zunächst gemeinsam mit den Sicherheitsspezialisten die Cyberrisikolandschaft des Unternehmens mit aktuellen Angriffsmustern zu vergleichen, um dann geeignete Schutzvorkehrungen zu treffen. So identifizieren Unternehmen zuerst die wertvollsten Daten oder Anwendungen aus Sicht des Angreifers, um diesen dann aktuelle Angriffsmethoden gegenüberzustellen. Ein Beispiel ist der „Fake President", bei dem sich ein Angreifer als Vorstand ausgibt und schnell eine Überweisung für einen angeblichen Zukauf einfordert.

Checkliste zum Schutz vor Cyberangriffen auf HR

- Sind Risiken im Zusammenhang mit Cybercrime und Personal im Unternehmen identifiziert und an die Mitarbeiter kommuniziert?
- Ist klar, welche Daten das Unternehmen überhaupt speichert und welchen „Wert" diese aus Perspektive eines Angreifers haben?
- Gibt es ein klares Berechtigungskonzept für die Anwendungen und Systeme im HR-Bereich?
- Gibt es einen Austausch zwischen Fachbereich, Informationssicherheit und IT?
- Unterstützt die eingesetzte Software die Sicherheitsanforderungen?
- Werden Vorgaben wirklich eingehalten oder gibt es Ausnahmen für die HR?
- Werden auch im HR-Bereich kombinierte Angriffe gegen Mitarbeiter, Technik und Prozesse simuliert und bewertet?

Durch zielgerichtete Schulungen können Arbeitgeber die HR-Mitarbeiter dann für die konkreten Bedrohungen sensibilisieren und ihr Wissen über Prozesse sowie sinnvolle Vorkehrungen effektiv einbringen.

2. Unsichere Berechtigungen

Viele Anwendungen oder IT-Systeme im Bereich des Personalmanagements sind zwar up to date, wenn es um rechtliche oder regulatorische Funktionalität geht. Effektive Sicherheitsvorkehrungen sind aber oft nur rudimentär vorhanden oder werden in der Praxis einfach nicht genutzt. Nicht selten sind HR-Systeme nicht unter denselben strengen Vorgaben wie andere Informationssysteme in die IT-Landschaft des Unternehmens eingegliedert. So gehören unzureichend eingeschränkte Rechte und eine unklare Benutzerrollenstruktur zum typischen Bild. Besonders bei kleinen Unternehmen, aber auch in größeren Abteilungen sind wesentliche Berechtigungen, wie das Verändern von Stammdaten, auf einen großen Personenkreis verteilt oder eine Funktionstrennung unzureichend ausgestaltet. Das kann beispielsweise Administrationszugänge innerhalb der Anwendungen (Bereichs- oder Abteilungsleiter sind per se höchstberechtigt) oder auch gefährliche Kombinationen von Benutzerrollen betreffen. Wenn dann auch noch Sammelkonten zum Einsatz kommen, die mehreren Personen mit denselben Zugangsdaten die gleichen Zugriffsrechte auf vertrauliche Daten geben und häufig vermeintlich durch die Notwendigkeit von Vertretungsregelungen legitimiert sind, wird es schwer bis unmöglich, Änderungen im Nachhinein nachzuvollziehen. Protokollierte Aktivitäten lassen sich dann nicht mehr den jeweiligen Anwendern zuordnen, wodurch Unternehmen Sicherheitsvorfälle nur schwer erkennen und aufklären können. Natürlich ist dazu ohnehin ein Aktivitätsprotokoll notwendig, das Datenänderungen und andere durchgeführte Schritte automatisch speichert („Logging"). Häufig gibt es eine derartige Funktionalität jedoch nicht oder sie ist nicht aktiviert beziehungsweise speichert die Aktivitäten nur über einen zu kurzen Zeitraum.

Unternehmen sollten Anforderungen aus dem Personalmanagement prinzipiell dokumentieren und mit einheitlichen Regeln standardisieren. Dazu zählt auch der Freigabeprozess, also die Vergabe einer bestimmten Benutzerrolle, einer Sammlung von Einzelrechten im IT-System oder einer Software an einen Mitarbeiter auf der Basis von dessen Tätigkeitsbeschreibung. Leider ist es jedoch oft noch Standard, dass Betriebe solche Freigaben per Mail oder außerhalb von Workflowsystemen geben. Einen IT-gesteuerten Workflow erst im Anschluss an eine Anfrage zu starten ist nicht ausreichend. Vielmehr braucht es elektronische Workflowsysteme, in denen Unternehmen alle zusammengehörigen Nachrichten speichern, zum Beispiel über Ticketsysteme.

3. Schwache Authentifizierung

Trotz der erhöhten Sicherheitsanforderungen an Personalsysteme legitimieren sich die Mitarbeiter in vielen Unternehmen häufig noch mit Username und Passwort im System. Das erscheint unverständlich angesichts der viel sichereren Methoden, die man in vielen anderen Bereichen längst einsetzt, wie etwa mit zusätzlicher PIN am Handy oder via Token. In vielen gängigen Anwendungen ist zudem ein Rollenwechsel zwischen Funktionen wie „Mitarbeiter" oder „Administrator" mit einem einzigen Klick möglich. Ist der Account eines Mitarbeiters dann beispielsweise per Phishing übernommen worden, stehen dem Angreifer alle in der Benutzerrolle gesammelten Berechtigungen zur Verfügung. Auch für die Kommunikation zwischen dem Personalmanagement und anderen Fachbereichen oder Mitarbeitern sollten hohe Sicherheitsanforderungen gelten. Die Identität des Gegenübers muss mit sicheren Methoden, beispielsweise über zusätzliche Verifikation mit Zertifikaten („digitaler Fingerabdruck"), nachvollziehbar sein.

Unternehmen sollten die Wahrscheinlichkeit, zur Zielscheibe eines Cyberangriffs zu werden, nicht unterschätzen. Vor allem HR-Systeme mit ihren sensiblen Daten sowie der Verwaltung und Organisation der Zugriffsrechte geraten zunehmend ins Visier der Täter. Typische Schwachstellen wie Berechtigungs- und Authentifizierungskonzepte sollten daher in jedem Unternehmen auf den Prüfstand. Wirksame Schutzvorkehrungen sind nur im Zusammenspiel von IT-Technik und Awareness der Mitarbeiter möglich und müssen unternehmensübergreifend gesetzt werden.

Nehmen uns die Roboter die Arbeit weg?
Vom Menschen in der digitalen Fabrik

Sie geht wieder um, die Angst vor der Massenarbeitslosigkeit, die Befürchtung, dass Maschinen uns die Arbeit wegnehmen. Zuletzt warnte der amerikanische Sachbuchautor Martin Ford („Aufstieg der Roboter“) bei einer Podiumsdiskussion in Wien davor, dass mittelfristig die Hälfte aller Jobs durch Digitalisierung und Automatisierung verschwinden könnte. Er gehört zu einer ganzen Reihe von Kommentatoren, die massenhafte Jobverluste durch Digitalisierung und Automatisierung prognostizieren. Wie berechtigt sind solche Szenarien? Welche Risiken birgt die Entwicklung in Richtung Industrie 4.0?

Einer, der radikale Veränderungen erwartet, ist Jens-Uwe Meyer. Der Managementberater, Autor, Dozent und Geschäftsführer eines Softwareunternehmens hat zahlreiche Studien über die Auswirkungen des digitalen Fortschritts auf das Arbeitsangebot analysiert und die Ergebnisse in seinem jüngsten Buch „Digitale Disruption“ aufgeschrieben. Bis zu 40 Prozent der Jobs werden demnach durch Technik ersetzt.

„Bestimmte Tätigkeitsprofile werden entfallen“, erklärt Meyer. Dazu gehörten vor allem leicht zu standardisierende Arbeiten wie das Prüfen eines Vorgangs nach bestimmten Regeln – Tätigkeiten also, in denen Computer besonders gut sind. Der Job des Steuerberaters sei so ein Fall, den zu 95 Prozent Algorithmen erledigen könnten.

Da standardisierte Aufgaben in vielen Jobs eine Rolle spielen, klingt das zunächst einmal bedrohlich. Da lohnt sich vielleicht der Blick auf eine Webseite der Süddeutschen Zeitung. „Wie wahrscheinlich ist es, dass ich durch einen Computer ersetzt werde?“, fragt mich die Headline. Wenn ich dort meine Berufsbezeichnung eingebe, berechnet das Tool die Wahrscheinlichkeit, mit der mein Job mittelfristig verschwinden wird. Bei Personalmanagern liegt diese Wahrscheinlichkeit bei beruhigend niedrigen 0,6 Prozent. Redakteure verlieren mit einer immerhin 5,5-prozentigen Wahrscheinlichkeit ihre Arbeit. Doch in vielen Sparten sehen die Zahlen laut Onlineberechnung deutlich dramatischer aus. Das liest sich nicht nur auf SZ Online so. Auch die WirtschaftsWoche listet reihenweise Jobs auf, die sich besonders einfach von Computern erledigen lassen – vom Konditor bis zum Chemiker. Der Spiegel machte im vergangenen September die Angst vor Arbeitsplatzverlusten sogar zum Titelthema. Unter der Headline „Sie sind entlassen! Wie uns Computer und Roboter die Arbeit wegnehmen“ greift die Hand eines Roboters nach einem Mann im Anzug, um ihn vor die Tür zu befördern.

Angst vor Jobabbau hat Tradition

Neu sind diese Bedrohungsszenarien allerdings nicht. Schon im März 1965 (!)

veranstaltete die IG Metall im deutschen Oberhausen eine internationale Tagung zu den Chancen und Risiken der Automatisierung. Die Angst vor einer umfassenden Freisetzung von Arbeitnehmern durch den technologischen Fortschritt war auf dieser Veranstaltung vor rund 50 Jahren ein zentrales Thema. Das war ganze 17 Jahre bevor das Time Magazine den Computer als neues Leitmedium zur „Maschine des Jahres" kürte. Im selben Jahr – 1982 – warnte der „Club of Rome" in seinem Bericht zu „Chancen und Gefahren der Mikroelektronik" vor Massenarbeitslosigkeit durch Computertechnik.


Foto: Riemensperger

Frank Riemensperger,
Accenture, Bitkom

Jetzt scheint sie wieder aktueller denn je zu sein, die Angst vor dem Jobabbau. Doch es gibt auch Gegenstimmen, die ebenfalls statistische Belege heranziehen. So wendet sich Frank Riemensperger, Vorsitzender der Accenture-Ländergruppe Deutschland, Österreich und der Schweiz sowie Hauptvorstandsmitglied des IT-Branchenverbands Bitkom gegen Angstmache in Sachen Jobabbau. „Alle Studien, die uns vorliegen, sagen ganz klar: Es droht kein massenhafter Verlust von Arbeitsplätzen".

Eine dieser Studien ist ein Gutachten des Instituts der deutschen Wirtschaft Köln (IW) im Auftrag der Initiative Neue Soziale Marktwirtschaft (INSM). In dem Papier, das vergangenen Sommer herauskam, heißt es: „Die Möglichkeit negativer Beschäftigungseffekte wird zwar immer wieder politisch thematisiert und diskutiert, wissenschaftlich lassen sich aber keine Belege für diese Vermutung finden." Schließlich sei die Digitalisierung ja bereits seit Jahren in vollem Gange. Und während sie einige Jobs verändert oder vielleicht auch vernichtet hat, sind andere entstanden. Wer hätte schließlich vor 15 Jahren vermutet, dass es irgendwann den Beruf des App-Entwicklers geben wird? In manchen Branchen ist die Produktion sogar schon nahezu vollständig digitalisiert – ohne die befürchteten massenhaften Jobverluste.

Strukturwandel in der Automobilindustrie

Beispiel Automobilindustrie: Wo früher Scharen von Facharbeitern Türen lackierten und Windschutzscheiben montierten, sind heute zu einem hohen Prozentsatz Roboter am Werk. Dennoch konnte die Branche in Deutschland ihre Beschäftigtenzahlen in den vergangenen zehn Jahren steigern. In Österreich befindet sich Branchengröße Magna Steyr gerade mitten in einem Mammut-Rekrutierungsprojekt. In den nächsten zwei Jahren will der Autobauer 3.000 Mitarbeiter einstellen, um die Großaufträge von Kunden wie BMW und Jaguar/Land Rover und Daimler erledigen zu können. Darunter sind Montage-, Karosseriebau- und Logistikplaner, Qualitätsmanager, Facharbeiter und Mitarbeiter für die Produktion.


Foto: Tutner

Hansjörg Tutner,
Magna Steyr

„Wir suchen insbesondere im Bereich der Instandhaltung Hundertschaften von Leuten", erzählt Personalchef Hansjörg Tutner. Gemeinsam mit dem AMS führt das Unternehmen in der gesamten Steiermark Veranstaltungen durch, um Arbeitskräfte zu gewinnen. Auch im nahen Slowenien wird rekrutiert. „Wir rechnen damit, dass wir rund 40.000 Bewerbungen benötigen, um 3.000 passende Leute zu finden", erläutert Tutner. In den Jahren 2017 und 2018 will die – personell verstärkte – HR-Abteilung des Unternehmens an die 10.000 Vorstellungsgespräche führen.

100 Bewerber will Magna an einem einzigen Tag kennenlernen. Dafür hat das HR-Management einen „Job Day" konzipiert, an dem es in acht Stunden 100 Bewerber testet, mit ihnen Gespräche führt und die Arbeitsplätze vorstellt. Zu einer Spitzenzeit im Juli 2017 muss HR in einer Woche 400 Leute neu aufnehmen. Das klingt nicht nach Jobbabbau, auch wenn Personalchef Tutner einschränkt: „Vor 20 Jahren hätten wir für diese Projekte natürlich noch viel mehr Menschen benötigt."

Denn Magna hat seine Produktion, wie andere Autorbauer auch, längst weitgehend automatisiert. Die Karosserien werden zu 98 Prozent von Robotern zusammengeschweißt. Und die Entwicklung geht weiter. Das Unternehmen setzt die Idee der „Smart Factory", der digital vernetzten Produktion, am Standort Graz zunehmend um. „Die Stückzahlen, die wir heute bauen, mit all ihren individuellen Ausfertigungen, können wir nicht mehr manuell herstellen. Das wäre völlig unwirtschaftlich", betont Tutner. „Wenn ich heute anfangen würde, personalintensiv zu produzieren, könnten wir unsere Autos bald nicht mehr in Österreich bauen." Heute überwachen die Mitarbeiter die Maschinen, warten sie, planen die Prozesse. Dafür sei in der Produktion ein höherer Ausbildungsstand notwendig als noch vor 20 Jahren. „Klassische Hilfstätigkeiten gibt es nicht mehr. Die Menschen sind für hochautomatisierte und sündteure Anlagen zuständig, die Eigenverantwortung steigt", sagt Tutner. Um genügend qualifiziertes Fachpersonal zu haben, bildet Magna derzeit 300 Nachwuchskräfte als Mechatroniker oder Kfz-Techniker aus, die im Frühjahr 2017 ihre Lehre abschließen und in den Beruf einsteigen sollen.

Die menschenleere Fabrik wird nicht kommen

Wie sich die Arbeit in der vernetzten Produktion verändert und wie sich die Digitalisierung auf den Arbeitskräftebedarf auswirkt, untersucht aktuell eine Arbeitsgruppe des Vereins „Industrie 4.0 Österreich – die Plattform für intelligente Produktion". Der Verein wurde 2015 gegründet, um Akteure und Anbieter zu vernetzen und das Thema digitalisierte Produktion in Österreich zu fördern.


Foto: Sommer

Roland Sommer,
Plattform „Industrie 4.0 Österreich"

„Die menschenleere Produktionshalle wird es nie geben", nennt Roland Sommer, Geschäftsführer des Vereins, ein Ergebnis der Arbeitsgruppe „Mensch in der digitalen Fabrik". „Es gibt sogar schon erste Beispiele von Unternehmen, die wieder verstärkt Personal in die Produktion einbinden, weil durch eine zu starke Digitalisierung der kontinuierliche

Verbesserungsprozess stockt". Unternehmen brauchten eben nach wie vor Menschen, die auf Probleme hinweisen und um die Ecke denken könnten.

Da die Komplexität der Prozesse laufend zunehme, steige allerdings der Qualifizierungsbedarf – zum Beispiel im Hinblick auf das Prozesswissen: „Einige Unternehmen versuchen, den Mitarbeitern ein Verständnis für die gesamten Prozesse zu vermitteln, andere teilen komplexe Prozessketten in kleine auf und definieren klare Verantwortlichkeiten. Das hängt stark von der Unternehmenskultur ab", erläutert Sommer. Neben Prozess- und Fachwissen werde ein gekonnter Umgang mit Daten immer wichtiger. Dazu gehöre das Verarbeiten großer Datenmengen ebenso wie Kenntnisse im Datenschutz.

Hinzu komme der große Bereich der Selbstkompetenzen. In vielen Jobs seien Flexibilität, Selbstmotivation und Problemlösungskompetenzen zentral. „Ein wichtiger Punkt ist die Eigenverantwortung", beobachtet der Geschäftsführer. „Einige Unternehmen berichten, dass sie immer größere Probleme haben, Mitarbeiter zu finden, die bereit sind, Managementverantwortung in der Produktion zu übernehmen, weil die Verantwortung für mehrere Maschinen oft schon eine recht große ist." Wer jahrelang in einer Facharbeiterposition unter eng definierten Hierarchiegrenzen gearbeitet hat, will diesen Schritt unter Umständen nicht gehen. Andere bringen das notwendige Know-how erst gar nicht mit.

Arbeit der Personalisten wird wichtiger

Die Unternehmen und vor allem die Personalabteilungen sind somit stark gefordert, Mitarbeiter ins Boot zu holen, zu entwickeln und zu qualifizieren.


Foto: Zierler

Clemens Zierler,
JKU Linz

„Die Arbeit der Personalisten wird immer wichtiger und notwendiger", sagt Clemens Zierler, Geschäftsführer des Instituts für Arbeitsforschung und Arbeitspolitik an der Johannes Kepler Universität Linz. Zierler forscht zum Thema Industrie 4.0 und hat eine Reihe von Unternehmen in dieser Hinsicht begleitet. Dabei hat er festgestellt, dass die „gesamte Diskussion um Automatisierung und Digitalisierung sehr technikgetrieben ist. Da werden sehr oft die Anforderungen der Menschen und der sozialen Systeme vergessen". Die Gefahr dabei sei, dass Arbeitgeber Mitarbeiter überforderten – einerseits, weil diesen die notwendigen Qualifikationen fehlen, andererseits aber auch, weil sie beim Tempo und der Komplexität der Produktionsprozesse nicht mehr mitkämen. Organisationen sollten auch nicht unterschätzen, wie sich die sozialen Systeme ändern, wenn sich Produktionsprozesse wandeln. Welche Auswirkungen auf das soziale Miteinander hat es, wenn Maschinen plötzlich die Rolle von Führungskräften einnehmen und den Menschen Anweisungen geben? Wie fühlt sich das an, wenn gewohnte Teamstrukturen oder bekannte Hierarchien verschwinden? Auch hier seien Personalverantwortliche gefragt, Veränderungsprozesse in der Organisationsentwicklung zu begleiten.

Die Art und Weise, wie Unternehmen Mitarbeiter auf neue Herausforderungen in der betrieblichen Weiterbildung vorbereiten, verändert sich gerade massiv, beobachtet Frank Riemensperger. „Der Arbeitsort wird zunehmend zum Trainingsort, der Trainer ist nicht mehr der Kursleiter, sondern der Kollege." Auch die Art, wie gelernt werde, sei einem zunehmenden Wandel unterworfen. Gelernt wird nicht mehr „auf Vorrat", sondern in kleinen Micro-Trainingseinheiten.

Aus- und Weiterbildung gefragt

Doch nicht nur die bestehenden Mitarbeiter müssen qualifiziert werden, auch Nachwuchs ist notwendig. Hier gibt es gerade in Schlüsselbereichen wie der Mechatronik deutliche Engpässe. Wie finden Unternehmen die Facharbeiter von morgen – und wie gewährleisten sie eine exzellente Ausbildung? Möglicherweise liegt die Lösung in der Kooperation. Zehn Industriebetriebe aus dem Waldviertel sind diesen Weg gegangen. Sie haben vor zwei Jahren die Weinviertler Mechatronik Akademie (WMA) gegründet. In Kooperation mit dem AMS und dem bfi bilden sie am Standort Wolkersdorf aktuell 28 Jugendliche zu Mechatronikern aus.


Foto: Körbisser

Dieter Körbisser,
Weinviertler Mechatronik Akademie (WMA)

„Dabei wenden wir uns an orientierungslose Jugendliche, die noch keine Lehrstelle haben", erklärt Geschäftsführer Dieter Körbisser. Einige von ihnen kommen aus schwierigen Sozialmilieus, haben Gewalt- und Drogenerfahrungen hinter sich. Entsprechend wichtig war Körbisser bei der Auswahl der Ausbildner darauf zu schauen, dass neben den fachlichen Skills die persönlichen Fähigkeiten passen. Unterstützung erhalten die Lehrlingsausbilder durch Psychologen des bfi. In der WMA erhalten die Jugendlichen eine Chance. Für die beteiligten Unternehmen verbindet sich soziales Engagement mit einem realen Bedarf. Entsprechend praxisnah ist die Ausbildung: „Wir erhalten aus unserem Kooperationskreis konkrete Aufträge", erzählt Körbisser. „Zuletzt haben unsere Lehrlinge eine computergesteuerte Löteinrichtung gebaut, die auch wirklich zum Einsatz kam." Der Geschäftsführer hofft, dass die beteiligten Unternehmen nach der vierjährigen Lehre möglichst viele Jugendlichen übernehmen. Die ersten Praktika verliefen jedenfalls erfolgreich.

Aus- und Weiterbildung ist eben das Um und Auf für die Arbeitsplatzsicherheit – da sind sich alle Interviewpartner einig. Nur mit Qualifizierung lässt sich der Sorge begegnen, im Beruf nicht mehr mitzukommen. Vielleicht sollten Führungskräfte und HR ihre Mitarbeiter auch zuweilen ermutigen, auf ihre Ressourcen zu vertrauen. „Wir alle sind in den letzten zehn Jahren im Privaten Profis darin geworden, wie man ein Smartphone mit Hunderten von Apps bedient", kommentiert Frank Riemensperger. „Wir haben sogar positive Erfahrungen damit gemacht. Das können wir auch im Arbeitsleben."

Bettina Geuenich

Webtipp

Ausführliche Interviews zum Thema „Industrie 4.0" mit den Ansprechpartnern aus diesem Artikel finden Sie auf dem Portal HRM.at.