Fragen der IT-Sicherheit in der „Arbeitswelt 4.0“

Im Rahmen eines Projektes der Offensive Gutes Bauen und der Offensive Mittelstand entstanden.

1. Information

Was ist unter „Fragen der IT-Sicherheit in der ‚Arbeitswelt 4.0‘“ zu verstehen?

Der Umbau der Arbeitswelt hin zu „Arbeit 4.0“ verlängert bzw. unterstreicht zahlreiche Eckpunkte aus den letzten zwanzig Jahren der Digitalisierung der Wirtschaft und fügt zudem neue Aspekte hinzu. Grundsätzlich lassen sich die Fragen der IT-Sicherheit in zwei große Blöcke aufteilen:

- Es gibt die **technischen** und
- die **nicht technischen Bereiche**.

Diese beiden Bereiche enthalten jeweils die Themen:

- **Datensicherheit** und
- **Datenschutz**.

Datensicherheit und Datenschutz bedingen einander und fußen wiederum auf technischen und nichttechnischen Bereichen.

Zu den technischen Eckpunkten von Datensicherheit und Datenschutz gehören die Grundwerte:

- Vertraulichkeit (Schutz vertraulicher Informationen vor unbefugter Preisgabe),
- Verfügbarkeit (Verlässlichkeit, Zugänglichkeit, Anwender/innen stehen Daten zum geforderten Zeitpunkt zur Verfügung),
- Integrität (Daten sind vollständig und unverändert).

Technisch gesprochen bedeutet dies: Datensicherheit umfasst die sichere Übermittlung, die sichere Speicherung sowie die Sicherheit, dass keine unbefugte Person Zugang zu den Daten erhält und somit niemand den Zustand der Daten (Integrität) unbefugt verändern, beschädigen oder löschen kann. Zur Verfügbarkeit gehört einerseits die Sicherheit der dauernden technischen Bereitstellung (etwa bei Cloud-Lösungen) wie andererseits die Stabilität der Zugangsleitungen (Breitband).

Zu den nicht technischen Eckpunkten von Datensicherheit und Datenschutz gehören:

- rechtliche Rahmenbedingungen (Recht auf informationelle Selbstbestimmung),
- organisatorische Vereinbarungen und Regelungen (Betriebsvereinbarungen, IT-Sicherheitskonzepte),
- Kenntnisse in der Verwendung von Anonymisierungs- oder Pseudonymisierungstechniken sowie von Verschlüsselungen (Elektronische Signaturen),
- sowie eine qualifizierte und hohe Anwendungskultur (Anwenderverhalten).

Zu den rechtlichen Rahmenbedingungen zählt unter anderem das Bundesdatenschutzgesetz. Darin werden zum Beispiel in § 9 unter anderem organisatorische Maßnahmen festgelegt wie Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und getrennte Verarbeitungsmöglichkeit. Zu den organisatorischen und rechtsverbindlichen Maßnahmen gehören zudem Betriebs- oder Dienstvereinbarungen, die insbesondere den Arbeitnehmerdatenschutz verbessern.

Wie wirkt sich der Wandel auf den eigenen Betrieb und die Arbeit aus?

Der Wandel hin zu „Arbeit 4.0“ erfordert von allen Beteiligten im Betrieb, aber auch von Selbstständigen eine deutlich höhere Sensibilität und ein geschärftes Bewusstsein für Belange des Datenschutzes und der Datensicherheit. Technisch sind die Möglichkeiten gegeben, ein hohes Sicherheitsniveau zu schaffen. Dies setzt Kenntnisse, den Willen und Ressourcen voraus. Lücken im betrieblichen Datenschutz (Identitätsdiebstahl, Kundendaten erscheinen plötzlich in Social Media-Plattformen etc.) oder Lücken in der Datensicherheit (Produktdatendiebstahl, Sabotage etc.) können eine Firma an den Rand ihrer Existenz führen. In der Welt von „VierNull“ müssen Datensicherheit und Datenschutz als Top-Themen der Geschäftsleitung und der Belegschaft verstanden sowie im Unternehmen aktiv gelebt werden. Die angepasste Verteidigung und Bewahrung von Privatheit (Privacy-by-design) gehört zu den Eckpunkten digitalen Kommunikationsverhaltens.

Welche Herausforderungen stellen sich?

Die Erfahrungen der zurückliegenden Jahre aus der digitalen Wirtschaft zeigen, dass die größten Herausforderungen für die Betriebe im Bereich Datensicherheit und Datenschutz (Kundendaten, Mitarbeiterdaten etc.) vor allem aus zwei Zusammenhängen kommen:

- Es ist die Anwender- und Nutzungskultur, das Anwenderverhalten (fehlerhafter, lässiger oder unzulässiger Umgang mit personenbezogenen Daten).
- Es ist die deutlich ansteigende Zahl äußerer technischer ungezielter Angriffe mit Hilfe von gefährlicher Software (Viren, Malware, Bots etc.) oder bewusst gezielten Angriffen (Datendiebstahl, Lahmlegung der Systeme, Wissensdiebstahl, Sabotage etc.).

Welche neuen Potenziale erwachsen für Mittelstand und Handwerk?

Für Betriebe, die in der digital-virtuellen Geschäfts- und Arbeitswelt unterwegs sind, stellt die aktive Kultur eines bewusst gelebten Datenschutzes und einer solide gebauten Datensicherheit ein wesentliches zukunftsträchtiges Qualitäts- und Unterscheidungsmerkmal dar. Diese Qualität bildet einen positiven Wettbewerbsfaktor. Es lohnt eine Zertifizierung.

2. Entscheidungsmöglichkeiten

Wie kann sich der Betrieb dem Thema öffnen?

Der Betrieb, die Geschäftsleitung und die Belegschaft benötigen Orientierungswissen über Datensicherheit und Datenschutz. Bevor im Betrieb technische Maßnahmen in Angriff genommen werden, sollte der Betrieb eigene Basis-Kompetenz aufbauen, um die verschiedenen Handlungsebenen von Datensicherheit, Datenschutz und digitaler Souveränität überblicken zu können.

Wo gibt es Informationen und Rat?

Informationen und Rat werden von vielen landesweiten Innovationsnetzwerken bereitgestellt, die zumeist unter der Schirmherrschaft von Landesministerien stehen wie etwa beispielhaft das Technologie-Netzwerk „Intelligente Technische Systeme OstWestfalenLippe“ in Nordrhein-Westfalen oder die „Allianz Industrie 4.0 Baden-Württemberg“. Zudem bieten das Beraternetzwerk der „Offensive Mittelstand“ (OM) und das Beraternetzwerk der „Offensive Gutes Bauen“ (OGB) auf Landesebene begleitende Hilfen an. Ebenso geben Kammern und Gewerkschaften Orientierungshilfen.

Welche Beispiele für vorhandene Umsetzungen gibt es?

Wer spezielles Fachwissen sucht, kann dies bei zwei neuen Großvorhaben finden: Das Bundesministerium für Bildung und Forschung (BMBF) stellt die Forschung im Bereich Big Data und IT-Sicherheit in Deutschland neu auf. Dazu werden zwei Big Data-Kompetenzzentren in Berlin und Dresden eingerichtet. Unter der Leitung der TU Berlin entsteht das Berlin Big Data Center (BBDC) und unter der Leitung der TU Dresden das Competence Center for Scalable Data Services and Solutions (ScaDS).

Wer Fallbeispiele kennenlernen will, kann diese in den Netzwerken der Cloud-Anwendungen entdecken. Laienverständliches Orientierungswissen liefern auch rechtliche Blogs.

3. Welche Schritte eignen sich als Einstieg?

An welchen Stellen im Betrieb könnte ich ansetzen?

Der Betrieb könnte beschreiben, wo überall im alltäglichen Ablauf sensible Daten eingegeben, abgerufen, verarbeitet, mobil verwendet oder gespeichert werden. Wer hat wozu Zugriff? Wer hat Lese- und Schreibrecht? Wie wurde bisher Datenschutz und Datensicherheit gehandhabt? – Die Ergebnisse dieser Zusammenstellungen sollten dann verglichen werden mit den in Richtung Cloud oder „Arbeit 4.0“ umgebauten Abläufen. Wo sind neue Sicherheitslücken oder Datenschutzlöcher erkennbar? – Daraus lässt sich ein IT-Sicherheits- und IT-Schutzkonzept erarbeiten. Eine Zertifizierung kann erwogen werden und alles zusammen lässt sich als neues Qualitätsmerkmal des Betriebes gegenüber Kunden offensiv darstellen.

Welche Techniken werden gebraucht?

Hier wird ein ganzes Bündel von Aktivitäten möglich. Sicherlich sollten die Anwendungen von Verschlüsselungs- und Anonymisierungstechniken eine wichtige Basis bilden.

Checkliste „Fragen der IT-Sicherheit in der ‚Arbeitswelt 4.0‘“

Entscheidungscheckliste des Handelns (inkl. einer Liste von Fragen nach Einbindung des eigenen betrieblichen Teams, nach Hinzuziehung von externer Beratung und Kompetenz)

		Ja	Nein
1.	Starten Sie eine Sensibilisierungsoffensive in der Geschäftsleitung und in der Belegschaft.	☐	☐
2.	Machen Sie Datensicherheit und Datenschutz zu einem wesentlichen Zukunftsthema des Betriebes.	☐	☐
3.	Bieten Sie Schulungen für alle betrieblich Beteiligten an – gerade auch im Bereich mobiler Nutzungen (Apps, Social Media etc.).	☐	☐
4.	Analysieren und beschreiben Sie die bisherige Verarbeitung sensibler und personenbezogener Daten.	☐	☐
5.	Analysieren und beschreiben Sie die technisch neu gestaltete Verarbeitung sensibler und personenbezogener Daten (zum Beispiel in der Cloud).	☐	☐
6.	Beseitigen Sie offensiv Sicherheits- und Schutzlücken.	☐	☐
7.	Vereinbaren Sie mit der Belegschaft einvernehmliche verbindliche Regelungen (zum Beispiel Betriebsvereinbarungen mit dem Betriebsrat).	☐	☐
8.	Prüfen Sie eine Zertifizierung.	☐	☐
9.	Werben Sie bei Ihren Kunden für Ihre hohe Qualität im sicheren und vertrauensvollen Umgang mit Kunden- und Mitarbeiterdaten (Kundendatenschutz, Arbeitnehmerdatenschutz).	☐	☐
10.	Machen Sie hohe Datensicherheit und hohen Datenschutz zu einem aktiven Wettbewerbsfaktor.	☐	☐

4. Weitere Hinweise

Dokumente

Siehe dazu auch die vertiefenden Entscheidungshilfen zu

- Einstiege in die digital-integrierte Wirtschaft – Potenziale der „Arbeitswelt 4.0“ für Mittelstand und Handwerk
- Bedeutung von Cyber Physical Systems (CPS) für KMU
- „Arbeitswelt 4.0“: Herausforderung Qualifizierung
- Gutes Arbeiten mit der Crowd – Qualität und Standards
- „Prävention 4.0“
- Führungs- und Kommunikationskompetenz für die „Arbeitswelt 4.0“
- Rechtliche Aspekte der Nutzung von Cloud-Lösungen

Links

- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (http://www.bfdi.bund.de/DE/Home/home_node.html)
- Netzwerk Trusted Cloud (http://www.trusted-cloud.de/)
- Bundesamt für Sicherheit in der Informationstechnik (BSI) (https://www.bsi.bund.de/DE/Home/home_node.html)
- Forum Privatheit (https://www.forum-privatheit.de/forum-privatheit-de/index.php)
- Fraunhofer-Initiative für sicheren Datenraum startet (http://www.isst.fraunhofer.de/de/publikationen/presse/2015/PI-28-09-2015-Industrial_Data_Space.html)
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (https://www.datenschutzzentrum.de/)
- Recht 2.0 – Das IT-Rechtsblog von Dr. Carsten Ulbricht (www.rechtzweinull.de)
- Virtual Fort Knox – Plattform für produzierende Unternehmen (https://www.virtualfortknox.de/)

Beraternetze

- Beraternetzwerk der „Offensive Mittelstand“ (OM) (http://www.offensive-mittelstand.de/)
- Beraternetzwerk der „Offensive Gutes Bauen“ (OGB) (http://www.offensive-gutes-bauen.de/)

Gefördert durch:

Bundesministerium für Arbeit und Soziales

aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der:

INITIATIVE NEUE QUALITÄT DER ARBEIT

Impressum:

Diese Entscheidungshilfe ist im Rahmen des Projektes AKTIV der Offensive Gutes Bauen und der Offensive Mittelstand entstanden, gefördert durch das Bundesministerium für Arbeit und Soziales (BMAS) im Rahmen der Initiative Neue Qualität der Arbeit.

Offensive Mittelstand, Theodor-Heuss-Str. 160, 30853 Langenhagen, E-Mail: info@offensive-mittelstand.de – Offensive Gutes Bauen, Kaiser-Friedrich-Ring 53, 65185 Wiesbaden, E-Mail: info@offensive-gutes-bauen.de – Konzept und Text: Welf Schröter, Irene Scherer (Forum Soziale Technikgestaltung) – Stand: November 2015