Sicherstellung der technischen und organisatorischen Maßnahmen im Homeoffice zur Aufrechterhaltung des internen Kontrollsystems (IKS), der Sicherheit der Geschäftsprozesse und der grundlegenden IT-Sicherheit

Die Corona-Pandemie hat viele Unternehmen mit der Frage konfrontiert, wie die mobile Arbeitsfähigkeit ihrer Mitarbeiter auch im Homeoffice weiterhin sichergestellt werden kann und welche konkreten Maßnahmen dabei zum Erhalt der Datensicherheit getroffen werden können. Dieses führte oft zu neuen und bisher wenig oder gar nicht bekannten Situationen.

Strategien der letzten Monate

März

- Im März mussten Mitarbeiter vorrangig schnell „mobil“ werden.
- Cloud-Anwendungen wurden eingerichtet, VPN-Zugänge ermöglicht und es erfolgte eine pragmatische Datenmitnahme in das Homeoffice (USB-Sticks, Aktenordner etc.).

April

- Der April legte den Schwerpunkt auf das Thema Business Continuity.
- Es erfolgte eine breitere Unterstützung der Mitarbeiter im Homeoffice, erste Vorgaben und Richtlinien wurden angepasst, Collaboration Tools (Teams, Zoom, Skype etc.) zum persönlichen Austausch bereitgestellt und führten zu einer Gewöhnung an die neue Arbeitswelt.

Mai

- Im Mai waren erste Lockerungen zu verzeichnen.
- Teilweise kehrten Mitarbeiter zunächst tageweise zurück ins Office, später entwickelten sich daraus Hybrid-Modelle aus Home-Office- und Office-Anwendern.

Ausblick

Derzeit erfolgt eine Rückkehr zu einer neuen Arbeitswelt. Hybrid-Modelle werden zur Norm, die Digitalisierung von Prozessen wird weiter optimiert und vorangetrieben. Arbeit wird zunehmend als Tätigkeit definiert, nicht als Ort. Angepasste Strategien und proaktive Maßnahmen sollen zukünftig eine verlässliche Bereitschaft vor einer erneuten Krise sicherstellen. Dabei sind Risiken für Unternehmensdaten zu minimieren, die durch (un)absichtliches oder unsachgemäßes Fehlverhalten von Anwendern entstehen.

Hierzu sind klare und praxisorientierte Maßnahmen und Richtlinien für das klassische Homeoffice und die bleibenden Hybrid-Modelle abzuleiten und umzusetzen.

Die folgende Checkliste wurde in Anlehnung an die vom Bayerischen Landesamt für Datenschutzaufsicht am 18. Mai 2020 veröffentlichten „Best-Practice-Handreichungen zum Datenschutz“ (Quelle: https://www.lda.bayern.de) entwickelt und aus IT-Compliance und IKS-Gesichtspunkten ergänzt.

Zur gezielten Prävention von Sicherheitsrisiken und zur gesteigerten Sensibilisierung für dieses Thema empfiehlt es sich, die aufgeführten Prüfpunkte beispielsweise von Seiten der Geschäftsführung oder des IT-Sicherheitsbeauftragten im Sinne einer SOLL-IST-Überprüfung zu verwenden. Nicht bei allen Punkten ist es immer der Fall, dass diese im eigenen Unternehmen umgesetzt werden müssen - dann ist jedoch eine kurze kritische Hinterfragung des Grundes samt kurzer Dokumentation angeraten.

Gerne unterstützen wir Sie bei einer Kurzaufnahme und Beurteilung Ihrer Homeoffice-Strategie mit dem Aufzeigen von konkreten Verbesserungsmaßnahmen.

A - Arbeitsumgebung

Bei der Arbeit zu Hause soll die Umgebung so ausgestaltet sein, dass vom Grundsatz her die Vertraulichkeit und Verfügbarkeit der Daten wie im Büro sichergestellt ist.

- ☐ Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook oder in die Papierunterlagen werfen können.
- ☐ Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages.
- ☐ Papierunterlagen können in Dokumentenmappen oder Schränken verschlossen werden.
- ☐ Clean-Room-Policy für Videokonferenzen (z.B. keine sensiblen Informationen im Hintergrund sichtbar).
- ☐ Sperrung des Notebooks bei Verlassen des Arbeitsplatzes, falls ein anderer Zugriff (z.B. Kinder, Mitbewohner, Besucher) nicht ausgeschlossen ist.
- ☐ Es wird darauf geachtet, dass Telefongespräche und Videokonferenzen nicht von unbefugten Personen mitgehört werden, z.B. durch offenes Fenster, laufende andere Videokonferenzen, Lautsprecher mit virtuellen Sprachassistenten (Alexa, SONOS etc.) oder Videospielkonsolen (XBox, Playstation etc.).

B - Organisatorische Regelungen und Vermeidung von Schatten IT

Verlagern Mitarbeiter die Arbeit ins eigene Zuhause, können völlig neue Sicherheitsprobleme entstehen, die als Einfallstor für tiefgreifende Cyberangriffe fungieren können. Die Anbindung von Mitarbeitern im „Zu-Hause-Modus“ muss daher durchdacht und sicher ausgestaltet werden.

- ☐ Überblick über die Mitarbeiter im Homeoffice.
- ☐ Überblick über die Geräte der Mitarbeiter im Homeoffice (fortlaufend aktualisierte Inventarisierung).
- ☐ Es wird die Bereitstellung von dienstlichen Geräten empfohlen. Privatgeräte sollten nur in Ausnahmefällen eingesetzt werden.
    - Dienstliche Notebooks, Smartphone oder Softphones werden gestellt.
    - Dienstlich zur Verfügung gestellte Geräte werden - auch zu Hause - nicht für private Zwecke genutzt.
- ☐ Überblick über ausgeliehene Papierunterlagen oder Akten und Sicherstellung der Rückführung nach dem Homeoffice.
- ☐ Durchsicht und Aktualisierung der vorhandenen IT-Sicherheitsrichtlinie (Anpassung an neue Krisensituation).
- ☐ Schulung/Informationen für Mitarbeiter über die Homeoffice-Regelungen mit schriftlicher Verpflichtung zur Einhaltung.
- ☐ Sensibilisierung der Mitarbeiter für Social-Network-Hacking.
- ☐ Keine Nutzung unsicherer Messenger-Systeme zur Unternehmenskommunikation.
- ☐ Keine Weiterleitung von dienstlichen E-Mails an private E-Mail-Konten (keine Nutzung von privaten Mailadressen für dienstliche Zwecke).
- ☐ Keine Bearbeitung von Dokumenten auf Privatrechnern (u.a. auch Lizenzproblematik).
- ☐ Keine Privatnutzung von dienstlichen Notebooks (z.B. bei Kindern zur Einreichung oder dem Austausch von Schulunterlagen, Schul- oder privaten Videokonferenzen).

C - Umgang mit Papierdokumenten

Noch nicht alle Arbeitsabläufe sind komplett digital nutzbar. Beim Umgang mit Papierdokumenten entstehen Risiken, die in den Räumlichkeiten des Büros so nicht auftreten.

- Papierunterlagen werden in geeigneten Mappen (mit Namen des Unternehmens im Falle eines Verlusts) mit nach Hause genommen. Hierzu ist im Unternehmen zu dokumentieren, wo sich diese Unterlagen befinden und ob sie wieder an ihren Ursprungsort zurückgebracht wurden.
- Regelungen, dass Papierunterlagen beim Transport nach/von zu Hause nicht erhöhten Risikosituationen (z.B. Rücksitz beim Einkaufen, Tasche im Restaurant etc.) ausgesetzt werden sollen.
- Entsorgung von Papierunterlagen sollte nicht über den Hausmüll oder das Altpapier entsorgt werden, sondern entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 5 (nach DIN 66399).
- Es wurde über die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) sensibilisiert.

D – Internes Kontroll-System (IKS): Analyse, Neubewertung und Ausrichtung

Viele Prozesse, Workflows und Systemberechtigungen wurden zur schnellen Sicherstellung der Betriebsbereitschaft vorrübergehend angepasst und führten teilweise zur Aufweichung oder Aussetzung interner Kontrollverfahren. Auch zukünftige Hybrid-Arbeitsmodelle erfordern eine einheitliche Umsetzung interner Kontrollen.

- Homeoffice-Potenzial der Geschäftsprozesse bestimmen, notwendige Kontrollanpassungen und alternative Freigabeprozesse ermitteln (Einhaltung Vier-Augen-Prinzip).
- Bestimmung geschäftskritischer Kontrollen.
- Festlegung von klaren Vertretungsregelungen (Kompensation Vier-Augen-Prinzip).
- Kurzfristige Anpassung von Rollen- und Berechtigungskonzepten, Einrichtung einer entsprechenden Überwachung (insbesondere von Zugangsberechtigungen bei VPN-Zugang und Finanzabwicklungen zu überprüfen).
- Temporär erweitertes Rollen- und Berechtigungskonzept ist nach der Krise zeitnah wieder auf den Soll-Zustand zurückzuführen.
- Anpassung veralteter Richtlinien zur Sicherstellung der Prozesstreue.
- Periodisches Überprüfen der Prozesse und Homeoffice-Regelungen, regelmäßige Sensibilisierung der Mitarbeiter.

E – IT Sicherheit

Das Homeoffice ist das virtuelle Büro – die Sicherheitsrisiken erhöhen sich durch die Anbindung an das Internet. Die Zusammenarbeit im Team über das Homeoffice setzt häufig geeignete Softwarewerkzeuge, sog. Collaboration-Tools, voraus.

- Anbindung an das Firmennetz ausschließlich mit verschlüsselten Verbindungen nach Stand der Technik (z.B. VPN-Verbindung).
- Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung nebst PIN/Passwort (z. B. Hardwaretoken oder (Software-)Zertifikate) bei VPN-Verbindungen.
- Nutzung vom heimischen Wi-Fi mit starken Passwörtern.
- Nutzung öffentlicher Wi-Fi-Hotspots nur bei durchgängiger Absicherung sämtlicher Kommunikation durch VPN-Anbindung.
- Zugriff nur auf für das Homeoffice erforderliche Server, Dateiablagen und Anwendungen durch die VPN-Verbindung.
- Speicherung von Daten auf über die VPN-Verbindung erreichbare Netzlaufwerke im Unternehmen.
- Regelmäßiges Patch Management erfolgt auch auf dem Homeoffice-Notebook durch den Einsatz von geeigneten Tools und Maßnahmen
    - zur automatischen Verteilung von Sicherheitsupdates (Policy-Patching),
    - zum Gerätemonitoring und
    - zum Notfallplan (für unsicher bewertete Geräte Maßnahmen definieren, z.B. Quarantäne oder Sperrung).
- Täglich Updates der Virendefinitionen/-signaturen auf den Homeoffice-Notebooks.
- Regelungen zum Umgang mit USB-Ports (z. B. Deaktivierung oder Verbot des Anschlusses privater Sticks) wurden getroffen.
- Bei vertraulichen Dokumenten verhindern Regelungen zum Ausdruck von Dokumenten auf den Druckern im Büro/im Homeoffice die Einsicht durch andere Mitarbeiter/Personen.
- Festplattenvollverschlüsselung bei Notebooks; zentrale Aufbewahrung der Schlüssel im Unternehmen.
- Vollverschlüsselung bei dienstlichen Smartphones.
- PIN-Sperre bei dienstlichen Smartphones.
- Regelungen und Verfahren im Verlustfall bei mobilen Endgeräten (z.B. Remote-Wipe bei Smartphones, Sperrung von Hardware-Token) sind getroffen.
- Einsatz geeigneter, sicherer Softwarewerkzeuge zur Zusammenarbeit im Team über das Homeoffice (Collaboration-Tools, Nutzung von Cloud-Diensten).
- Sensibilisierung der Mitarbeiter für Risiken von Phishing-Attacken auf Cloud-Konten
- Bereitstellung geeigneter Plattformen zum Datenaustausch; Vermeidung unsicherer (privater) Cloud-Speicher wie OneDrive, iCloud oder DropBox.
- Überprüfung der elektronischen Datenübermittlung auf den aktuellen Stand der Technik (auch bei ERP-Systemen).
- Authentifizierungsmethoden bei IT Supportfällen (z.B. Remote-Unterstützung, Kennwortzurücksetzung) und mobilen Anfragen (z.B. Auswertungen, Listen, Anweisungen).