EBC-Marburg
Dokumentation der technischen und organisatorischen Maßnahmen (TOMs)

Anmerkung: als Einzelunternehmer verweise ich auf die DSGVO, in der auf das Prinzip der Verhältnismäßigkeit hingewiesen wird. In meinen Büroräumen werden z.B. keine, über das Normale hinausgehenden Maßnahmen, zur Zutrittskontrolle (Codeschlösser und Alarmanlagen, etc.) ergriffen.

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1 Zutrittskontrolle, Zugangskontrolle und Zugriffskontrolle

Meine Werkstatt wird außerhalb der Geschäftszeiten video-überwacht. Ein Bewegungssensor startet die Aufzeichnung. Die Videos werden bis zur manuellen Löschung aufbewahrt oder bis der Speicherplatz voll ist.

Für die von mir genutzten EDV-Systeme (sowohl stationär als auch mobil) gilt:

- es werden personalisierte Benutzernamen und Kennworte vergeben. Sie entsprechen den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

- es werden die windows-internen Firewalls und kommerzielle Antiviren-Systeme eingesetzt

- außer mir haben meine Mitarbeiter David Müller und Tim Schuhmacher Administrationsrechte für meine EDV-Systeme

- neben Standard-Software (MS Office, Rechnungswesen, etc.) setze ich alle gängigen Tools, die für meine Arbeit nötig sind, ein (Content Management Systeme, Datenrettungs-Tools, VPN-Software). Individuell für mich programmierte Software setze ich nicht ein

- zur Speicherung von EDV-Dokumentationen und Kennworten nutze ich die Verschlüsselungssoftware Boxcryptor[1] und den Passworttresor Keepass[2]

- sobald das entsprechende Gerät verlassen wird, werden die Geräte entweder manuell gesperrt oder die Systeme werden nach einer bestimmten Zeit der Inaktivität automatisch gesperrt

- die für die Mitarbeiter zur Verfügung stehenden Mobilgeräte, werden nur im Rahmen der Tätigkeit bei EBC-Computer genutzt. Eine private Nutzung ist untersagt

- für Fernwartungsaufgaben setze ich Anydesk[3] der Firma „philandro Software GmbH“ ein

---

[1] Boxcryptor: Infos zum Programm (https://www.boxcryptor.com/de/technical-overview/) und zum Verschlüsselungsverfahren (https://www.boxcryptor.com/de/technical-overview/)
[2] Keepass: Infos zum Programm (https://keepass.info/index.html) und zum Verschlüsselungsverfahren (https://keepass.info/help/base/security.html)
[3] Anydesk: Infos zum Programm (https://anydesk.de) und zum Verschlüsselungsverfahren (https://anydesk.de/features)

- besteht zum Endkunden eine VPN-Verbindung, kann die Fernwartung auch über diesen verschlüsselten Verbindungsweg per windows-internen Zugriffsmöglichkeiten (Remote Desktop Protokoll, RDP) anstatt über Fernwartungssoftware erfolgen.

2. Maßnahmen zur Gewährleistung der Verfügbarkeit

Alle von mir verarbeiteten Daten, werden regelmäßig auf externe Datenträger (NAS-Laufwerke), die sich in meinen Büroräumen befinden, gesichert. Es werden zyklisch Vollsicherungen (normalerweise wöchentlich) und inkrementelle oder differentielle Sicherungen (normalerweise täglich) angelegt. Kundendaten werden verschlüsselt (siehe 1.) auf die entsprechenden Datenträger gesichert.

Darüber hinaus lagert eine Datensicherung meiner Geschäftsdaten[4] (keine Kundendaten) in einem Bankschließfach. Die Aktualisierung der Datensicherung erfolgt wöchentlich.

[4] Dies beinhaltet nur Daten, die ich für die Kommunikation mit meinen Kunden, zur Abrechnung geleisteter Tätigkeiten oder zur Erfüllung meiner Aufträge benötige. Personenbezogene Daten von dritten (z.B. Auftraggeber, Patienten meiner Kunden, etc.) werden nicht extern gelagert