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, Video-Überwachung, Alarmanlagen, etc.) ergriffen.

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

1.1 Zugangskontrolle und Zugriffskontrolle

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 hat niemand 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 ich das entsprechende Gerät verlasse, werden die Geräte entweder manuell gesperrt oder die Systeme werden nach einer bestimmten Zeit der Inaktivität automatisch gesperrt

- für das von mir genutzte Notebook gilt darüber hinaus, dass dieses Gerät nur beruflich genutzt wird

- für Fernwartungsaufgaben wird zum einen Anydesk[3] der Firma „philandro Software GmbH“ sowie Teamviewer[4] der Firma „TeamViewer GmbH“ verwendet.

[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)
[4] Teamviewer: Infos zum Programm (https://www.teamviewer.com/de/) und zum Verschlüsselungsverfahren (https://www.teamviewer.com/de/security/)

- 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.

- für die Kommunikation per Mail nutze ich ein E-Mail-Zertifikat von Comodo (https://www.comodo.com/home/email-security/free-email-certificate.php) mit dem ich ausgehende Mails standardmäßig signiere. Auf Wunsch versende ich E-Mails auch verschlüsselt (S/MIME)

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.