IT-Sicherheitsrichtlinie: Fristen und Vorgaben

Ab 1. April 2021

- In der Praxis werden aktuelle Virenschutzprogramme eingesetzt (Anlage 1 Nummer 15).
- Der Internet-Browser ist so eingestellt, dass in dem Browser keine vertraulichen Daten gespeichert werden (Anlage 1 Nummer 8).
- Es werden verschlüsselte Internetanwendungen genutzt (Anlage 1 Nummer 10).
- Apps werden nur aus den offiziellen App-Stores heruntergeladen und restlos gelöscht, wenn sie nicht mehr benötigt werden (Anlage 1 Nummer 1).
- Es werden keine vertraulichen Daten über Apps versendet (Anlage 1 Nummer 4).
- Smartphones und Tablets sind mit einem komplexen Gerätesperrcode geschützt (Anlage 1 Nummer 22).
- Nach der Nutzung eines Gerätes meldet sich die Person ab (Anlage 1 Nummer 13).
- Das interne Netzwerk ist anhand eines Netzplanes dokumentiert (Anlage 1 Nummer 33).
- App-Berechtigungen minimieren: Bevor eine App eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält; weitere müssen hinterfragt und gegebenenfalls unterbunden werden (vgl. Anlage 2 Nummer 1).

Ab 1. Januar 2022

- Bei der Bereitstellung und dem Betreiben von Internet-Anwendungen wie Praxis-Homepage oder Online-Terminkalender wird eine Firewall eingesetzt (Anlage 1 Nummer 9).
- Bei der Bereitstellung und dem Betreiben von Internet-Anwendungen wie Praxis-Homepage oder Online-Terminkalender werden keine automatisierten Zugriffe bzw. Aufrufe auf Webanwendungen eingerichtet oder zugelassen (Anlage 1 Nummer 11).
- Auf Endgeräten, z.B. einem Praxisrechner, erfolgt eine regelmäßige Datensicherung, wobei in einem Plan festgelegt ist, welche Daten wie oft gesichert werden sollen (Anlage 1 Nummer 14).
- Bei Verlust eines Mobiltelefons (Diensthandy) muss die darin verwendete SIM-Karte zeitnah gesperrt werden (Anlage 1 Nummer 25).
- Wechseldatenträger müssen bei jeder Verwendung mit einem aktuellen Schutzprogramm auf Schadsoftware überprüft werden (Anlage 1 Nummer 28).
- Es werden nur Apps genutzt, die Dokumente verschlüsselt und lokal abspeichern (Anlage 1 Nummer 3).
- Für die dezentralen Komponenten der Telematikinfrastruktur werden Updates zeitnah installiert (Anlage 5 Nummer 6).
- Für die dezentralen Komponenten der Telematikinfrastruktur werden die Administrationsdaten sicher aufbewahrt (Anlage 5 Nummer 7).
- Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden (vgl. Anlage 2 Nummer 8). Hierfür gibt es ein Musterdokument auf der Online-Plattform zur IT-Sicherheitsrichtlinie **