Richtlinie nach § 75b SGB V über die Anforderungen zur Gewährleistung der IT-Sicherheit

Zum 1. Juli 2022 zu erfüllende Anforderungen samt Praxishinweisen

Anlage 2: Zusätzliche Anforderungen für mittlere Praxen

Hardware: Endgeräte und IT-Systeme

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
5	Endgeräte mit dem Betriebssystem Windows	Sichere zentrale Authentisierung in Windows-Netzen	In reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden.	In reinen Windows-Netzen sollte zur zentralen Authentisierung für Single Sign On (SSO) ausschließlich Kerberos eingesetzt werden. Eine Gruppenrichtlinie sollte die Verwendung älterer Protokolle verhindern. Der Schutz des Local Credential Store (LSA) sollte aktiviert werden (PPL, Protected Mode Light). Die Speicherung der LAN-Manager-Hashwerte bei Kennwortänderungen sollte per Gruppenrichtlinie deaktiviert werden. Die Überwachungseinstellungen sollten gemeinsam mit den Serverkomponenten von DirectAccess sorgfältig auf die Anforderungen des Informationsverbunds abgestimmt werden. Es sollte eine Protokollierung auf Clientseite sichergestellt werden.
6	Smartphone und Tablet	Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellen werden.	Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich auf der Webseite https://hub.kbv.de/site/its im Bereich *IT-Sicherheit in der Praxis* unter *Musterdokumente*. Diese sollte festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. Darin sollten auch die Themen Aufbewahrung und Verlustmeldung behandelt werden. Außerdem sollte verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten.
8	Mobiltelefon	Sicherheits-richtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich auf der Webseite https://hub.kbv.de/site/its im Bereich *IT-Sicherheit in der Praxis* unter *Musterdokumente.* Jedem Benutzer eines Mobiltelefons muss ein Exemplar der Sicherheitsrichtlinie ausgehändigt werden. Es muss regelmäßig überprüft werden, ob die Sicherheitsrichtlinie eingehalten wird. Die Sicherheitsleitlinie zur dienstlichen Nutzung von Mobiltelefonen sollte Bestandteil der Schulung zu Sicherheitsmaßnahmen sein.

Anlage 3: Zusätzliche Anforderungen für Großpraxen

Hardware: Endgeräte und IT-Systeme

Nr.	Zielobjekt	Anforderung	Erläuterung	Zusatzinformation
2	Smartphone und Tablet	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden. Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden.
8	Mobile Device Management (MDM)	Auswahl und Freigabe von Apps	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden.	Apps aus öffentlichen App-Stores sollten durch die Verantwortlichen geprüft und freigegeben werden. Dazu sollte ein Freigabeprozess entwickelt werden, in dem auch geeignete Bewertungskriterien definiert sind. Alle freigegebenen Apps sollten intern in einem Standardkatalog veröffentlicht werden und dort für die Benutzer verfügbar sein. Apps sollten gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden. Das MDM sollte die Installation, Deinstallation und Aktualisierung erzwingen, sobald eine Verbindung zum mobilen Endgerät besteht.