Anforderungen Informationssicherheit für Informationstechnik, Kommunikationstechnik und Medizintechnik

Der vorliegende Katalog enthält die an Informationstechnik, Kommunikationstechnik und Medizintechnik gestellten funktionalen sowie nicht-funktionalen Informationssicherheitsmindestanforderungen. Der Katalog ist verbindlich für alle Anschaffungen aus den oben genannten Bereichen, die direkt oder indirekt die Patientenversorgung tangieren. Dieser Katalog gilt nicht für Anschaffungen, die ausschließlich für Forschung und Lehre beschafft werden. Mit Vertragsabschluss bestätigt der Auftragnehmer, dass das angebotene Produkt die hier geforderten Mindestanforderungen erfüllt. Sollten einzelne Anforderungen nicht erfüllt werden, ist eine Rücksprache mit dem UKB vor Vertragsabschluss nötig. Dieser Katalog soll sicherstellen, dass ein gesetzeskonformer und gleichzeitig wirtschaftlicher Betrieb des Produkts am UKB möglich ist.
Die Liste gliedert sich in verschiedene Bereiche. Diese sind nur zu prüfen, wenn Sie für das Gerät/System/Software zutreffen.

1. **Herstellersupport / LifeCycle**
   - 1.1. Der Hersteller muss noch mindestens vier Jahre nach Vertragsabschluss das Geräte/Software/System mit Sicherheitsupdates versorgen.
   - 1.2. Besondere Anforderungen an das Patch-Management müssen, falls vorhanden dokumentiert sein. Insbesondere, wenn eine Freigabe des Herstellers vorgesehen ist, bevor andere Software-Updates eingespielt werden.
   - 1.3. Der Hersteller muss das Support-Ende mindestens ein Jahr im Voraus ankündigen.
2. **Geräte/Systeme/Software mit Netzwerkfunktionalität**
   - 2.1. Kommunikationsbeziehungen müssen eindeutig mit Dienst/Port, Kommunikationspartner und Senderichtungen dokumentiert sein.
   - 2.2. Geräte/Systeme mit Netzwerkanschluss (LAN)
     - 2.2.1. Die Geräte/Systeme unterstützen den Standard IEEE 802.1x zur Authentifizierung am Netzwerk oder haben eine unveränderliche eindeutige MAC-Adresse.
   - 2.3. Geräte mit WLAN-Schnittstelle (WIFI)
     - 2.3.1. Der Client muss mindestens einen der Standards IEEE 802.11 g/n/a unterstützen.
     - 2.3.2. Das Gerät muss mind. WPA2-Enterprise mit TKIP oder AES Verschlüsselung unterstützen.
     - 2.3.3. Für die Authentifizierung ist mind. IEEE 802.1x mit EAP-PEAP MSCHAP V2 als Authentifizierungsmethode gefordert.
3. **Software**
   - 3.1. Software für Server muss kompatibel zum Betrieb in einer virtuellen Maschine basierend auf VMWare vSphere/ESXi sein.
   - 3.2. Die Anforderungen an das Betriebssystem müssen dokumentiert sein und insbesondere muss mindestens eine Betriebssystemversion unterstützt werden, die noch mindestens vier Jahre bei Server-Software bzw. 3 Jahre bei Desktop Software mit Sicherheitsupdates versorgt wird.
   - 3.3. Die Hardware-Anforderungen müssen eindeutige dokumentiert sein.
   - 3.4. Nötige Ausnahmen/Ausschlusslisten für Endpoint-Protection-Systeme müssen verbindlich dokumentiert sein.
   - 3.5. Dienste und Software die zusätzlich zur eigentlichen Software installiert und konfiguriert werden müssen, müssen verbindlich inklusive der nötigen Anforderungen der Konfiguration dokumentiert sein.
4. **Fernwartung**
   - 4.1. Sofern eine Fernwartung vorgesehen ist, muss diese entweder über einen VMware Horizon Windows-Terminalserver des UKB oder einen VPN-Tunnel möglich sein. Dabei sind die für die Fernwartung benötigten Dienste/Ports eindeutig zu benennen, damit die Fernwartung nach dem Least-Privilege-Prinzip eingerichtet werden kann.
   - 4.2. Wenn auf dem Produkt, das ferngewartet werden soll, personenbezogene Daten gespeichert werden, muss ein AV-Vertrag geschlossen werden.

Stand: 21.05.2021
Ansprechpartner: UK-IT Stabsstelle IT-Sicherheit
Klassifikation: OFFEN

5. Benutzerverwaltung

5.1. Die Benutzerverwaltung muss an Active Directory anbindbar sein. Dies kann über LDAPS oder ADFS erfolgen.

6. Medizinprodukte

6.1. Wenn Patientendaten im Medizinprodukt gespeichert werden, muss dies in der Dokumentation angegeben werden.

6.2. Wenn Patientendaten im Medizinprodukt gespeichert werden, muss eine protokollierte Löschung möglich sein.