ANLAGE 2: ZUSÄTZLICHE ANFORDERUNGEN FÜR MITTLERE PRAXEN

SOFTWARE: RECHNER-PROGRAMME, MOBILE APPS UND INTERNET-ANWENDUNGEN

NR.	ZIELOBJEKT	ANFORDERUNG	ERLÄUTERUNG	GELTUNG AB	WEITERE HINWEISE ETC.
1.	Mobile Anwendungen (Apps)	Minimierung und Kontrolle von App-Berechtigungen	Minimierung der App-Berechtigungen.	01.04.2021	– Bevor eine App in einer Institution eingeführt wird, muss sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen müssen hinterfragt und gegebenenfalls unterbunden werden. – Sicherheitsrelevante Berechtigungseinstellungen müssen so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können. – Wo dies technisch nicht möglich ist, müssen die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.
2.	Internet-Anwendungen	Zugriffskontrolle bei Webanwendungen	Sicherstellung von Berechtigungen.	01.01.2022	– Es muss durch die Entwickler einer Internet-Anwendung mittels einer Autorisierungskomponente sichergestellt werden, dass Benutzer nur Aktionen durchführen können, zu denen sie berechtigt sind. – Jeder Zugriff auf geschützte Inhalte und Funktionen muss kontrolliert werden, bevor er ausgeführt wird. – Sollte es nicht möglich sein, Zugriffsrechte zuzuweisen, muss dafür ein zusätzliches Sicherheitsprodukt eingesetzt werden.

JETZT KOMMENTIEREN

HARDWARE: ENDGERÄTE UND IT-SYSTEME

NR.	ZIELOBJEKT	ANFORDERUNG	ERLÄUTERUNG	GELTUNG AB	WEITERE HINWEISE ETC.
3.	Endgeräte	Nutzung von TLS	Benutzer sollten darauf achten, dass zur Verschlüsselung von Webseiten TLS verwendet wird.	01.01.2022	– vgl. Anlage 1 - Anforderung Nr. 10 – Auf https achten, Plug-In/ Erweiterung wie HTTPS Everywhere verwenden
4.	Endgeräte	Restriktive Rechtevergabe	Restriktive Rechtevergabe.	01.01.2022	– Der verfügbare Funktionsumfang des IT-Systems sollte für einzelne Benutzer oder Benutzergruppen so eingeschränkt werden, dass sie nur genau die Rechte besitzen und nur auf die Funktionen zugreifen können, die sie für ihre Aufgabenwahrnehmung benötigen („Need-to-know-Prinzip"). – Zugriffsberechtigungen sollten hierfür möglichst restriktiv vergeben werden. – Es sollte regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der Sicherheitsrichtlinie entsprechen. – Auf Systemdateien sollten möglichst nur die Systemadministratoren zugreifen können. – Der Kreis der zugriffsberechtigten Administratoren sollte möglichst klein gehalten werden. – Auch System-Verzeichnisse sollten nur die notwendigen Privilegien für die Benutzer zur Verfügung stellen.
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.	01.07.2022	– 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 erstellt werden.	01.07.2022	– Es sollte eine verbindliche Richtlinie für Mitarbeiter zur Benutzung von mobilen Geräten erstellt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich im Bereich Musterdokumente. – Diese sollte festlegen, wie mobile Geräte genutzt und gepflegt werden sollen. – Darin sollten die Themen Aufbewahrung und Verlustmeldung behandelt werden. – Außerdem sollte verboten werden, Verwaltungssoftware zu deinstallieren oder das Gerät zu rooten.
7.	Smartphone und Tablet	Verwendung von Sprachassistenten	Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind.	01.01.2022	– Sprachassistenten sollten nur eingesetzt werden, wenn sie zwingend notwendig sind. Andernfalls sollten sie deaktiviert werden. – Generell sollte ein Sprachassistent nicht genutzt werden können, wenn das Gerät gesperrt ist.
8.	Mobiltelefon	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden.	01.07.2022	– Werden Mobiltelefone für dienstliche Zwecke verwendet, muss eine Nutzungs- und Sicherheitsrichtlinie erstellt werden. Ein Beispiel in Form einer Muster-Richtlinie befindet sich im Bereich 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.
9.	Mobiltelefon	Sichere Datenübertragung über Mobiltelefone	Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. Diese sind zu verschlüsseln.	01.01.2022	– Es sollte geregelt sein, welche Daten über Mobiltelefone übertragen werden dürfen. – Die dafür erlaubten Schnittstellen sollten festgelegt werden. – Außerdem sollte beschlossen werden, wie die Daten bei Bedarf zu verschlüsseln sind.
10.	Wechseldatenträger / Speichermedien	Regelung zur Mitnahme von Wechseldatenträgern	Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen.	01.01.2022	– Es sollte klare schriftliche Regeln dazu geben, ob, wie und zu welchen Anlässen Wechseldatenträger mitgenommen werden dürfen. – Darin sollte festgelegt sein, welche Datenträger von wem außer Haus transportiert werden dürfen und welche Sicherheitsmaßnahmen dabei zu beachten sind. – Ein Beispiel in Form einer Muster-Richtlinie befindet sich im Bereich Musterdokumente.

11.	Netzwerksicherheit	Umfassende Protokollierung, Alarmierung und Logging von Ereignissen	Wichtige Ereignisse auf Netzkomponenten und auf den Netzmanagement-Werkzeugen sollten automatisch an ein zentrales Management-System übermittelt und dort protokolliert werden.	01.01.2022	– Es sollten mindestens folgende Komponenten und Ereignisse auf einem zentralen Protokoll-Server protokolliert werden:
					  – Active Directory:
					  – unautorisierte Zugriffe bzw. Zugriffsversuche,
					  – Firewall:
					  – Ereignisse wie erlaubte und unterbundene Zugriffe
					  – Virenscanner:
					  – Start, Stop, Fehler bei Scannen
					  – Erkannte Malware
					  – PVS:
					  – Anmeldungen, Verfügbarkeit, etc.
					Wenn der Durchsatz und die Erreichbarkeit der Netzwerkkomponenten und Dienste überwacht werden soll, kann dies mit open source Tools wie Icinga erfolgen.

JETZT KOMMENTIEREN

Ein Service der Kassenärztlichen Bundesvereinigung (KBV)
Dezernat Digitalisierung und IT

Ansprechpartner
Telefon: 030 40 05 - 21 21
E-Mail: servicedesk@kbv.de

Weitere Informationen
Nutzungsbedingungen
Datenschutz
Impressum