MKK Mühlenkreiskliniken

IT-RICHTLINIE FÜR DEN BETRIEB VON HARD- UND SOFTWARE IN DER NETZWERKINFRASTRUKTUR DER MÜHLENKREISKLINIKEN

TECHNISCHE UND ORGANISATORISCHE VORAUSSETZUNG FÜR DIE INBETRIEBNAHME VON ENDGERÄTEN AN DER NETZWERKINFRASTRUKTUR DER MÜHLENKREISKLINIKEN

VERSION 7.0

INHALTSVERZEICHNIS

1 EINLEITUNG

Um eine optimale und funktionsfähige Patientenversorgung und Unternehmensführung, sowie Forschung und Lehre in Kooperation mit der Ruhr Universität Bochum und der Ausbildungsakademie gewährleisten zu können, sind die Mühlenkreiskliniken (MKK) auf eine funktionsfähige und sichere Informationstechnologie (IT) angewiesen. Um dieses zu gewährleisten, betreiben die MKK eine komplexe IT-Infrastruktur in der viele der mittlerweile IT-gestützten Prozesse abgebildet sind.

Zum Schutz der IT-Infrastruktur sind Regeln bei der Auswahl und Inbetriebnahme von Endgeräten einzuhalten. Diese werden in dieser Richtlinie beschrieben zu deren Einhaltung der Mitarbeiter bzw. der Vertragspartner der MKK sich verpflichtet.

2 GELTUNGSBEREICH

Diese IT-Nutzungsrichtlinie gilt für alle Beschäftigte und Geschäftspartner des Unternehmens und Ihrer Tochterunternehmen, die einen Betrieb eines Endgerätes an der IT-Infrastruktur der MKK betreiben, betreiben wollen oder beschaffen möchten.

Beschäftigte der MKK und Geschäftspartner sind verpflichtet, sich an diese Richtlinie zu halten.

3 ZUWIDERHANDLUNGEN

Eine Zuwiderhandlung / ein Verstoß kann arbeits- oder dienstrechtliche Konsequenzen nach sich ziehen. Im Falle des Vorliegens von grober Fahrlässigkeit oder Vorsatzes können dem Unternehmen entstandene Schäden gegenüber dem Mitarbeiter ganz oder teilweise geltend gemacht werden.

Als Verstöße werden Handlungen gegen das Regelwerk der IT-Sicherheit verstanden. Dazu zählen insbesondere die aus der vom Nutzer zu verantwortender Beeinträchtigung der Funktionalität der MIT-Systeme hervorgerufene negative Auswirkungen auf die IT-Sicherheit.

Im Falle externer Personen, Systemanbieter und Dienstleister kann eine Zuwiderhandlung / ein Verstoß vertragliche Konsequenzen und Strafzahlungen nach sich ziehen. Im Falle des Vorliegens von grober Fahrlässigkeit oder Vorsatzes können dem Unternehmen entstandene Schäden gegenüber dem externen Partner ganz oder teilweise geltend gemacht werden.

4 Allgemeine Voraussetzungen

- MDM[1]-fähig – im speziellen Workspace One und Softwarekomponente Workspace One HUB
- Im DEP[2]-Programm der MKK eingebunden (bei Apple iOS-Endgeräten)
- Eingesetzte Software muss als APK-Datei bereitstehen (bei Android basierten Endgeräten)
- Datenspeicher, wie z.B. Festplatten / SSD und Speicherkarten sind zu verschlüsseln
- UML-Sequenzdiagramm zur Darstellung der Kommunikation in einem editbaren Format (VSDX)
- Rollen- und Rechtekonzept muss beschrieben sein

5 Voraussetzungen / Anforderungen an das eingesetzte Betriebssystem

Nachfolgende Versionen werden je nach Betriebssystem für den Betrieb in der Netzwerkinfrastruktur der MKK vorausgesetzt.

Windows-Betriebssysteme

Die von Microsoft veröffentlichten Produktlebenszyklen für Windows sind einzuhalten.

Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen.

Das Betriebssystem ist im Server- und Clientbereich als Enterprise-Edition zu betreiben.

[1] Mobile Device Management (MDM): Mobilgeräteverwaltung
[2] Device Enrollment Program (DEP): Programm zur Geräteregistrierung bei Apple

LINUX-/UNIX-DISTRIBUTIONEN

Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen.

Die Distributoren haben dazu die Produktlebenszyklus im Internet veröffentlicht.

APPLE IOS

Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen.

ANDROID OS

Es ist immer das am längsten unter Support stehende und vom Servicepartner unterstützte Betriebssystem im aktuellen Versions- und Patchstand einzusetzen. Endgeräte müssen Android Enterprise fähig sein.

6 PATCHMANAGEMENT DES BETRIEBSSYSTEMS

Die in Ziffer 5 benannten Betriebssysteme sind immer auf der aktuellen Version und Patchstand zu halten. Die Einbindung Active Directory fähiger Betriebssysteme und dem in der Domäne der MKK vorgegebenen Update- und Patchmanagement ist im Grundsatz vorgegeben.

Apple iOS und Android basierte Endgeräte werden im Grundsatz über die MKK MDM-Plattform Workspace One verwaltet.

Die Einbindung von Endgeräten ohne Anbindung in das Active Directory der MKK und/oder dem Management über die MKK MDM-Plattform ist nur dann gestattet, wenn der Hersteller / Lieferant schriftlich zusichert, dass das Endgerät immer auf dem aktuellen Versionsstand und Patchstand gehalten wird. Eine Überprüfung des Versionsstandes und des Patchlevels kann durch die MIT-Abteilung jederzeit erfolgen. Für die Prüfung ist der aktuelle Einsatzort des Geräts der MIT-Abteilung jederzeit zu nennen.
Bei Verwendung eines eigenen Updatemanagement ist vorab die technische Umsetzung darzustellen.

7 SCHUTZ VOR SCHADSOFTWARE

Endgeräte können nur dann in der Netzwerkinfrastruktur der MKK betrieben werden, wenn diese regelmäßige Aktualisierung der eingesetzten Sicherheits-

Software Microsoft Defender mit Firewall und dem Einspielen von Updates bzw. Patches unmittelbar nach deren Erscheinen gewährleisten.

Abweichungen hiervon bedarfen einer individuellen Freigabe.

8 Härtung des Betriebssystems und der Anwendungen / Services

Im Grundsatz ist eine Härtung des Betriebssystems, der Anwendungen und der Services durch den Hersteller durchzuführen.

Administrative Kennwörter und Accounts sind nicht für den Betrieb und die Bereitstellung von Betriebssystemen, Anwendungen und Services zu benutzen.

Zugriffsmöglichkeiten auf das Betriebssystem, die Anwendungen und die Services sind auf ein für den Betrieb notwendiges Minimum zu beschränken und zu sichern (z.B. Netzwerkports, Konsolen, Tools, Treiber, Dienste). Alle nicht benötigten Softwarebestandteile/Anwendungsprogramme und Funktionen sind zu entfernen.

Für Windows-Systeme ist der IT-Grundschutz-Baustein SYS.1.2.3 Windows Server des BSI in der aktuellen Fassung anzuwenden.

Für Linux-Systeme ist der IT-Grundschutz-Baustein SYS.1.3 Server unter Linux und Unix des BSI in der aktuellen Fassung anzuwenden.

Eine Überprüfung der Härtung des Betriebssystems und der Anwendung kann durch die MIT-Abteilung jederzeit erfolgen. Für die Prüfung ist der aktuelle Einsatzort des Geräts der MIT-Abteilung jederzeit zu nennen.

9 Anbindung per Wireless LAN

Die eingesetzten Endgeräte unterstützen den 2,4 und 5 GHz Wireless-Standard und sind in der Lage nach WPA2-802.1x mit Zertifikaten zu verschlüsseln und zu authentifizieren.

Unabhängig von der Anbindung direkt an die MKK-Infrastruktur ist ein Betrieb fremder WLAN-Netzwerktechnik (nicht MKK-Infrastruktur) zum Aufbau eigener Strukturen nicht zulässig.

10 Datenspeicher und Medienanschlüsse

Die zulässigen Datenspeicher sind in der IT-Speicherklassenrichtlinie beschrieben. Betriebsbedingte Ausnahmen sind durch MIT, ISM und Datenschutz freizugeben. Medienanschlüsse, wie z.B. USB sind auf ein für den Betrieb notwendiges Minimum zu beschränken und zu sichern. Ungenutzte Anschlüsse sind zu deaktivieren.

11 Lebensdauer Betriebssysteme und Anwendungen

Die Produktlebenszyklen der Produkte und Hersteller sind einzuhalten.

Ein Betrieb des Endgerätes ist ausschließlich nur dann gestattet, wenn alle Soft- und Hardwareprodukte vom Hersteller noch nicht abgekündigt sind und ein Produktsupport (bei Software mit Updatesupport) besteht.

12 Voraussetzungen / Anforderungen an Softwarekomponenten

Java JRE/JDK

Java ist grundsätzlich in einer lizenzkostenfreien Version einzusetzen und ausschließlich im aktuellen Versions- und Patchstand zu betreiben.

Ist eine Nutzung einer lizenzpflichtigen Java-Version erforderlich, so ist die Lizenz durch den Hersteller/Anbieter zu stellen.

Websocket

Die Nutzung von Websockets ist in den Mühlenkreiskliniken untersagt.

Microsoft SQL-Server und -Datenbanken

Im Grundsatz ist für MS SQL-Datenbanken der zentrale MS SQL-Cluster der MKK zu nutzen. Abweichungen hiervon bedarf einer individuellen Freigabe.

Für den Betrieb der Datenbanken werden ausschließlich administrative Rechte auf der Datenbank selbst zur Verfügung gestellt. Sogenannte administrative Instanz- oder SA-Rechte werden nicht vergeben (auch nicht temporär).

DATEIFREIGABEN

Im Grundsatz sind keinerlei Dateifreigaben oder s.g. Shares für die Bereitstellung der Softwareanwendung oder Daten gestattet. Insbesondere Freigaben mit Jeder/Erveryone Berechtigungen sind ausnahmslos nicht gestattet.

INTERNET

Wird eine Kommunikation in das Internet benötigt, müssen vollständig mit Quelle, Port, Ziel und Protokoll angegeben werden. Angaben wie *.hersteller.de (sog. Wildcards) werden im Grundsatz nicht akzeptiert.
Die Kommunikation muss nach den technischen Richtlinien des BSI „TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ erfolgen.

IPSEC-TUNNEL

Die Kommunikation muss nach den technischen Richtlinien des BSI „TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ erfolgen.

MAILRELAY

Ein sog. Mail-Relay auf die Mailserver der MKK ist aussschließlich aus den internen Netzwerkbereichen der MKK und nur als internes Relay gestattet.

13 FERNWARTUNG

Zur Fernwartung von Endgeräten in der IT-Infrastruktur der MKK wird der Einsatz des Fernwartungstools Bomgar vorausgesetzt (siehe „IT-Nutzungsrichtlinie zur Fernwartung von MIT-Systemen der Mühlenkreiskliniken“).

Abweichungen hiervon bedarfen einer individuellen Freigabe.

14 BSI-MELDEPFLICHT

Die MKK betreibt eine kritische Infrastruktur gem. BSI-Gesetz und ist verpflichtet Meldung vom BSI über Schwachstellen, Gefährdungen, Vorfälle etc. entgegenzunehmen und zeitnahe zu behandeln. Sofern Produkte des Auftragnehmers im Rahmen von BSI-Meldungen thematisiert werden, behält sich die MKK vor eine Stellungnahme zu der entsprechenden BSI-Meldung von dem Auftragnehmer einzuholen. Die Stellungnahme muss u.a. eine Risikoabschätzung seitens des Auftragnehmers, einen Maßnahmenplan zur Behandlung inkl. verbindlicher zeitlicher Planung zum weiteren Vorgehen enthalten. Die Stellungnahme muss zeitnah, unter Berücksichtigung der gesetzlichen Fristen für Datenschutzvorfälle gemäß DSGVO bzw. Informationssicherheitsvorfälle, bei den MKK eingehen.