



Informationssicherheitsanforderungen für den Betrieb von Geräten

Cyber-Sicherheitsanforderungen an Geräte und Systeme für den Betrieb in den Einrichtungen der Barmherzigen Brüder Träger GmbH

Datum:
Name des Herstellers:
Gerät und Typ:
Ansprechpartner (Hersteller):
zuständiger Mitarbeiter der Einrichtung:

Fragen an den Hersteller:

1.	Nachweise, Zertifizierungen	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
1.1.	Gibt es ein freiwilliges Sicherheitskennzeichen (für das Produkt)?	sollte			
1.2.	Ist das Produkt zertifiziert nach CE, ISO oder anderweitig?	muss			

2.	Entwicklung	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
2.1.	Sind bei Softwarekomponenten– sofern technisch möglich – automatisierte Codeanalysen fester Bestandteil des Entwicklungszyklus?	sollte			

2.2.	Wird bei Softwarekomponenten während des Entwicklungsprozesses gezielt nach bekannten Schwachstellen wie buffer overflows und unhandled exceptions gesucht?	sollte			
2.3.	Werden flankierende Maßnahmen eingebaut, die verhindern, dass innerhalb von Speicherbereichen, die nicht dafür vorgesehen sind, Code ausgeführt wird?	sollte			
2.4.	Werden Produkte einer technischen Sicherheitsanalyse (Penetrationstests) unterzogen?	sollte			
2.5.	Wird beispielsweise auf bisher unbekannte Verwundbarkeiten (z. B. durch Fuzzing-Tests) oder alternative Zugriffsmöglichkeiten (beispielsweise durch Auslesen von versteckten Dateien, Konfigurationen, Datenströmen oder Hardwareregistern) geprüft?	sollte			
2.6.	Wird dem Betreiber eine vollständige technische Dokumentation übermittelt, die ihnen verständlich dokumentiert, wie das Gerät technisch sicher zu betreiben ist?	muss			
2.7.	Ist das System gehärtet?	muss			
2.8.	Ist das System nach dem "Stand der Technik" ausgestattet?	muss			

3.	Informationspflicht	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
3.1.	Werden Meldungen und Auswirkungen von bekannten Schwachstellen oder IT-Sicherheitslücken beim Hersteller bei Bekanntwerden an den Betreiber gemeldet?	muss			Verfahren beschreiben
3.2.	Wird geprüft, ob die notwendigen Maßnahmen zur Schwachstellenbeseitigung durchgeführt wurden?	muss			Verfahren beschreiben

4.	Schwachstellen	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
4.1.	Ist eine Regelung zum Umgang mit Schwachstellen vorhanden?	muss			Verfahren beschreiben
4.2.	Werden Produkte über einen hinreichend langen Zeitraum möglichst zeitnah mit Patches und Updates bzw. Workarounds versorgt, um entdeckte Schwachstellen zu beheben oder zumindest zu deren Wirkung abzuschwächen?	muss			Zyklus angeben
4.3.	Ist die Auslieferungskette für Updates, Patches oder für eventuell für den Betrieb benötigte Software ausreichend gesichert?	muss			Verfahren beschreiben
4.4.	Ist eine Erkennung und ein Schutz gegen Schadprogramme eingerichtet?	sollte			

5.	Konfiguration	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
5.1.	Kann die Konfiguration nur nach vorheriger Authentifizierung modifiziert werden?	muss			
5.2.	Erfolgt die Auslieferung in einer sicheren Standardkonfiguration („Secure by Default“)?	muss			
5.3.	Sind die Passwörter, Zertifikate usw. für sämtliche Dienste austauschbar?	sollte			
5.4.	Gibt es einen automatischen Logoff-Prozess, der verhindert, dass unberechtigte Personen nach einer vergessenen Abmeldung in der Lage sind, Konfigurationsänderungen vorzunehmen?	sollte			
5.5.	Sind alle Schnittstellen, die für Servicezwecke verwendet werden, gegen den Zugriff durch Unberechtigte geschützt? (z.B. Passwortabfrage)	muss			
5.6.	Sind Update-Mechanismen (z. B. für Firmware-Updates), insbesondere die über ein Netzwerk erfolgen, hinreichend abgesichert?	muss			Verfahren beschreiben

5.7.	Gibt es eine Zugriffskontrolle (Login/Authentifizierung)?	sollte			
------	---	--------	--	--	--

6.	Fernwartung	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
6.1.	Wenn eine Fernwartung durchgeführt wird, ist gesichert, dass die dafür eingerichteten Komponenten den eigentlichen Betrieb in keinsten Weise beeinträchtigen?	sollte			
6.2.	Kann eine Fernwartung bzw. ein Schreibzugriff auf ein Produkt oder eine Komponente nur dann erfolgen, wenn diese explizit aktiviert wird, mit zeitlicher Beschränkung (Beispielsweise durch einen Bestätigungsdialog, Freischaltung)?	muss			
6.3.	Wird verhindert, dass über Logdaten ungeschützt auf kritische oder vertrauliche Informationen (z. B. Login- oder Patientendaten) zugegriffen werden kann?	sollte			
6.4.	Bei einer Fernwartung: Gibt es eine Möglichkeit zur automatischen Alarmierung im Falle von kritischen Systemereignissen oder -zuständen?	sollte			

7.	IT-Sicherheitskonzept	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
7.1.	Sind sämtliche Schnittstellen, Zugänge und Funktionen dokumentiert?	muss			
7.2.	Werden die Cyber-Sicherheitseigenschaften bzw. -funktionen der Komponente beschrieben?	sollte			
7.3.	Wird dargestellt, welche Risiken / Bedrohungen durch die Komponente selbst abgedeckt werden?	sollte			

7.4.	Ist dokumentiert, welche Dienste (mit den im Produkt integrierten Mechanismen) nicht abgesichert werden können und daher ergänzende technische oder organisatorische Cyber-Sicherheitsmaßnahmen erfordern?	sollte			
7.5.	Werden alle ggf. kritischen Aktionen in Logdateien vermerkt wie z. B. die Änderung der Konfiguration, fehlgeschlagene Login-Versuche, das Entfernen oder der Austausch von Speichermedien oder das Anschließen eines USB-Geräts?	sollte			

8.	Integration ins Netzwerk	Anforderung Informationssicherheit	erfüllt (ja/nein)	Anmerkungen des Herstellers (ggf. Beiblatt ausfüllen)	Anmerkungen des Betreibers
8.1.	Können nicht notwendige Dienste deaktiviert werden?	muss			
8.2.	Ist eine Netzwerkidentifikation mit Zertifikaten möglich?	sollte			
8.3.	Erfolgen Übertragungen verschlüsselt (https), kein ftp/http, kein SMB V1?	sollte			
8.4.	Ist es möglich mobile Geräte in einem zentralen Managementsystem zu verwalten (z. B. MobileIron)?	sollte			