Feedback und Maßnahmen

# Feedback TÜV Süd

Die meiner Meinung nach wichtigen Fragen/Anmerkungen habe ich rot gekennzeichnet. Fragen zur Usability grün. Anregungen sind in blau. Nicht hervorgehobene Punkte (nur wenige) halte ich für inkorrekt.

|  |  |  |  |
| --- | --- | --- | --- |
| **Sektion** | **Aussage** | **Kommentar TÜV** | **Status oder Anmerkung CJ** |
| C) 2. a) i) | "Der Hersteller hat die Sicherheitsrelevanz aller Funktionen analysiert."  "Der Hersteller hat die Auswirkungen sicherheitsrelevanter Funktionen im Risikomanagement dokumentiert." | --> Meines Erachtens ist dieser Ansatz unvollständig: Es können auch von nicht sicherheitsrelevanten Funktionen hohe Risiken ausgehen. | Brauche Hilfe. Wenn hohe Risiken von einer Funktion ausgehen, ist sie dann nicht sicherheitsrelevant? |
|  | "Der Hersteller hat für jedes Benutzungsszenario oder für jede zusammengehörende Gruppe an UI-Elementen (z.B. Bildschirmseiten, Panels) eine Liste an Funktionen spezifiziert, die im Rahmen dieses Benutzungsszenarios oder über diese Gruppe an UI-Elementen angeboten werden." | --> Mehrwert? | Kritik gerechtfertigt: Es ist so unvollständig. Es muss untersucht werden ob die Benutzungsszenarien sicherheitsrelevant sind. Das fehlte.  Mehrwert: 1. Forderung IEC 62366-1, 2. Wir müssen Ursachenkette von UI bis zum Patient verstehen, um Risiken zu beurteilen.  Maßnahme: Korrigiert und kommentiert |
|  | "Der Hersteller hat im Risikomanagement die Auswirkungen für die Patientensicherheit analysiert, wenn eine Person nicht auf Patientendaten zugreifen kann (z.B. keine Berechtigung, Passwort vergessen), und entsprechende Maßnahmen definiert." | --> Ich würde es allgemeiner formulieren: Patientensicherheit, wenn Patientendaten nicht verfügbar (unabhängig davon, ob Person oder System Daten abruft, und unabhängig davon, warum Daten nicht verfügbar sind (Passwort vergessen, Unterbrechung der Netzwerkkommunikation, Angriff von Hacker)) | Mir war der Punkt wichtig, weil ich trennen wollte, die Nicht-Verfügbarkeit von Daten, weil sich das System nicht spezifikationsgemäß verhält, und die Nicht-Verfügbarkeit von Daten, weil sich das System spezifikationsgemäß verhält. Den letzten Punkt übersehen viele. Es geht also nicht um Risiken durch mangelnde IT-Sicherheit, sondern um Risiken, die aus Maßnahmen zur Erhöhung der IT-Sicherheit folgen.  Maßnahme: Diesen Hinweise ergänzt. |
| C) 2. a) ii) | "Das Produkt erlaubt eine Authentifizierung mit Passwort nur, wenn dieses Passwort eine Länge von 6 Zeichen hat von denen mindestens eines ein nicht alphanumerisches Zeichen ist und das mindestens einen Groß- und einen Kleinbuchstaben enthält [^C2a-02].  [^C2a-02]: Idealerweise müssten auch Passwörter ausgeschlossen werden, die über Wörterbuch-Angriffe erraten werden können." | --> Warum 6 Zeichen? brute force immer noch trivial, falls keine weiteren Maßnahmen vorhanden, unabhängig von Komplexität. Nicht alphanumerisch nicht immer möglich. | Kritik gerechtfertigt.  Maßnahme: Das nur noch als Beispiel und erwähnt, dass wegen Brute-Force diese Vorgabe nicht ausreicht kann. Ebenso ergänzt, dass nicht-alphanumerische Zeichen manchmal unmöglich sind, was sich auf die Länge des Passworts auswirken wird. |
|  | "Das Produkt sperrt Benutzer und Nachbarsysteme nach n Versuchen für m Minuten aus, wobei der Hersteller n und m Werte oder Untergrenzen festlegt." | leider ideal für DoS! Safety-Bedenken | Stimmt.  Maßnahme: Ergänzt, dass wir ein „Breaking-the-glass“ benötigen. |
|  | "Das Produkt erlaubt berechtigten Benutzern, andere Benutzer und Nachbarsysteme zu sperren."  "Das Produkt erlaubt berechtigten Benutzern, andere Benutzer und Nachbarsysteme zu löschen." | --> kann im laufenden Betrieb kritisch sein (Safety?). Vorschlag: auf Wartungsmodus beschränken? | Wichtiger Hinweis.  Maßnahme: Hinweis ergänzt, der genau das aussagt. |
|  | "Das Produkt erlaubt berechtigten Benutzern, die Passwörter anderer Benutzer und Nachbarsysteme zurückzusetzen." | --> alle Elemente der Authentifizierungen müssen ersetzt werden können, also insbesondere auch kryptographische Schlüssel und Zertifikate. | Stimmt.  Maßnahme: Geändert |
|  | "Das Produkt erlaubt es, Berechtigungen auszuhebeln ("Breaking the glas"), und identifiziert / dokumentiert die Person und die Gründe." | --> Beispiele zu meinem Verständnis? | Maßnahme: Beispiele ergänzt |
|  | "In einer Client-Server Architektur werden alle Cyber-Sicherungsmaßnahmen serverseitig berechnet und geprüft."  "In einer Client-Server Architektur werden alle Eingaben des Clients serverseitig geprüft." | --> Cyber-Sicherungsmaßnahmen und Eingaben sollten beidseitig jeweils von der anderen Seite geprüft werden, genauso wie Authentifizierung möglichst beidseitig stattfinden sollte. | Einverstanden.  Maßnahme: Entsprechend umformuliert, dass die Prüfung immer **auch** serverseitig erfolgen muss. |
| C) 2. b) i) | "Der Hersteller hat eine Liste aller vom System verwalteten Daten [^C2b-01] erstellt."  "[^C2b-01]: Beispiele für solche Daten sind Patientendaten (z.B. demographische Daten, Anamnesen, Diagnosen), Untersuchungsdaten (z.B. Laborwerte, radiologische und pathologische Bilder) und Behandlungsdaten (Verschreibungen, Einstellungen von Medizingeräten), Konfigurationsdaten der Produkte, Daten der Anwender (insbesondere Zugangsdaten), Keys, Software Zertifikate, Programm-Code (inklusive SOUP/OTS)." | --> bei OS wie Windows und Linux nicht zu bewältigen und auch nicht zielführend | Verstehe ich nicht ganz. Es ginge hier nicht um die einzelnen dlls, sondern um das Betriebssystem als Ganzes?  Noch keine Maßnahme. |
|  | "Der Hersteller hat im Risikomanagement die Folgen einer Überlastung des Systems durch zu viele Anfragen (z.B. DoS) oder Anfragen mit zu großen Daten-Volumina untersucht und falls notwendig Maßnahmen definiert." | --> Überlastung kann auch andere Ursachen haben, diese sind aber hier nebensächlich. Der Fokus liegt auf die zu ergreifenden Maßnahmen für einen geeigneten Umgang mit der Situation. | Stimme der Aussage zu, weiß aber nicht, was ich ändern soll |
| C) 2. b) ii) | "Das gilt insbesondere für sicherheitsrelevante Daten wie die unter [^C2b-02] genannten." | --> eher [^C2b-01], oder? | Absolut  Maßnahme: Korrigiert |
|  | "Das Produkt speichert Passwörter und personenidentifizierende Merkmale nur verschlüsselt." | --> Passwörter werden üblicherweise gehasht und gesalzen gespeichert, nicht verschlüsselt. Wie sieht es mit dem Schlüssel- bzw. Zertifikatsmanagement aus, insbesondere mit der Anforderung, dass jedes Gerät einen anderen Schlüssel erhält? | Absolut zutreffend.  Maßnahme: korrigiert und Anforderungen ergänzt |
| C) 2. c) ii) | "Das Produkt prüft geänderten Programm-Code (Patches) vor dessen ersten Ausführung auf Integrität." | -> Wie soll das funktionieren bzw. warum nur bei der ersten Ausführung? Wenn schon eine solche Funktionalität implementiert wird, sollte man sie in Richtung secure boot nutzen, sprich bei jedem Neustart des Geräts die Integrität der Firmware/Software prüfen. | Was missverständlich formuliert. Mit „erste Ausführung“ war jeder Neustart gemeint.  Der Secure Boot ist genau eine Möglichkeit dies zu implementieren.  Maßnahme: umformuliert. |
|  | "Das Produkt aktualisiert sich selbständig." | --> Halte ich gerade im medizinischen Umfeld für potentiell problematisch: Patching im laufenden Betrieb risikoreich; Neustart erforderlich, obwohl Gerät gerade für Behandlung benötigt wird; setzt nach meinem Verständnis außerdem meist eine Internetverbindung voraus, was die Angriffsfläche vergrößert und somit eher zu vermeiden ist | Einverstanden.  Maßnahme: Forderung gelöscht |
| C) 2. d) | "Das Produkt erkennt einen Einbruch oder Angriff [^C3d-02] und reagiert darauf [^C3d-03]" | --> halte ich bei Medizingeräten für unrealistisch, das bekommen ja selbst die besten IDS/IPS nicht konsequent bzw. vollständig hin | Einverstanden.  Ganz entfernt werden kann es nicht: Ist eine Forderung der FDA.  Maßnahme: Level hochgesetzt, Absolutheit der Anforderungen reduziert. |
| C) 3. i) | "Der Hersteller, die OTS-Betriebssysteme einsetzen, haben einer Liste aller Dienste [^C3-01] erstellt, die das Betriebssystem nach "außen" anbietet bzw. nutzt." | --> warum auf OTS und OS beschränkt? system hardening sollte immer durchgeführt werden, unabhängig von Softwaretyp (OS oder Anwendung) und -ursprung (OTS oder proprietär) | Einverstanden  Maßnahme: Umformuliert |
|  | "Wenn das Produkt eine USB-Schnittstelle anbietet, hat der Hersteller im Risikomanagement beschrieben, wie Angriffe über diese Schnittstelle beherrscht werden." | --> warum nur USB? sollte auf alle Schnittstellen zutreffen | Einverstanden  Maßnahme: Umformuliert |
|  | "Der Hersteller hat für jede Funktion (siehe oben) den Prozess identifiziert, der diese Funktion anbietet / realisiert." | --> siehe wo oben? sind die Dienste gemeint? Vorteil dieser Maßnahme Schutz vor Backdoors? | Einverstanden  Hier geht es ums Threat-Modeling  Maßnahme: Umformuliert |
|  | "Der Hersteller hat für jeden Prozess den Nutzer (auf Betriebssystemebene) identifiziert und begründet, wenn dieser mit maximalen Rechten (als Root) läuft." | --> ich wüsste nicht, dass man z. B. bei Windows beeinflussen kann, mit welchen Rechten OS Dienste laufen. Außerdem sind nicht nur maximale Rechte gefährlich. Idealerweise sollte alles mit minimalen Rechten laufen. | Verstehe  Maßnahme: Umformuliert, dass alles mit minimalen Rechten laufen muss |
|  | "Der Hersteller hat für alle Software-Komponenten [^C3-02], Dienste bzw. Prozesse, Daten und internen Funktionen analysiert, welche Risiken entstehen, wenn diese sich aufgrund eines Problems mit der IT-Sicherheit nicht spezifikationsgemäß verhalten." | --> ist mit Funktionen Funktionalität gemeint oder Funktionen beim Programmieren? Sollten die Funktionen im Code gemeint sein, dann ist diese Prüfung vom Aufwand her kaum zu bewältigen und wahrscheinlich auch nicht zielführend | Einverstanden, ist unklar. Es ging in der Tat nicht um einzelne Methoden.  Maßnahme: Umformuliert 🡪 Software-Komponenten |
| C) 3. ii) | "Die Software ist vor Malware (Viren, Würmern usw.) geschützt." | --> ist das tatsächlich bei allen Medizingeräten umsetzbar? Virenscanner halte ich für schwierig, whitelisting eher machbar | Den Schutz vor Malware müssen wir schon fordern. Das tun auch die FDA und andere.  Virenscanner sind nur eine Möglichkeit.  Noch keine Maßnahme, brauche Input. |
|  | "Die Software basiert auf den aktuellsten Versionen der SOUP-/OTS-Komponenten." | --> neuste Version kann bekannte Schwachstelle enthalten, die in vorherigen Versionen nicht vorhanden war, und somit unsicherer sein; kann zu Kompatibilitätsproblemen führen; kann sehr aufwendig sein und nicht unbedingt notwendig, wenn nicht security relevant | Einverstanden  Maßnahme: komplett umformuliert |
| C) 4. | "Der Hersteller spielt nur Code auf, der vor Reverse-Engineering und Auslesen des RAMs geschützt ist [^C4-02]."  "[^C4-02]: Beispiele wären ein physischer Zugriffsschutz, Obfuscation von Code, Betriebssystem mit Address Space Layout Randomization" | --> wie sollen gängige OS wie Windows und Linux vor RE geschützt werden? ASLR schützt nicht vor Auslesen des RAMs | ASLR erschwert das Auslesen des RAM, verhindert das aber nicht.  Die Anforderung ist nur für Stufe 3!  Maßnahme: Umformuliert, dass es nur um Schutz vor inakzeptablen Risiken geht |
| C) 5. | "Der Hersteller verlangt Code-Reviews für alle Komponenten, die (IT-)sicherheitsrelevanten Funktionen abbilden." | --> Unabhängigkeit und Eignung der Personen, die Reviews durchführen? Vier-Augen-Prinzip und Training | Absolut!  Maßnahme: Dies ergänzt |
|  | "Der Hersteller hat für alle SOUP- bzw. OTS-Komponenten beschrieben, wie diese zu verifizieren sind" | --> OS wie Windows und Linux können vom Umfang her nicht verifiziert werden | Das stimmt. Die Aussage können wir nicht fallen lassen, das gibt uns die IEC 62304 vor. Es heißt ja nur, dass festgelegt werden muss, wie diese zu verifizieren sind, nicht dass diese zu 100% zu verifizieren sind. |
| C) 6. | "Der Hersteller sieht im Testplan [^9] Portscans an allen relevanten Datenschnittstellen vor und führt diese auch durch." | --> Netzwerkschnittstellen statt Datenschnittstellen? | Einverstanden  Maßnahme: Korrigiert |
|  | "Der Hersteller sieht im Testplan Penetrationstests an allen relevanten Datenschnittstellen und/oder für alle bekannten Schwachstellen der eingesetzten OTS-Komponenten [^10] vor und führt diese auch durch." | --> Falls mit Pentest das Testen von Angriffen basierend auf alle bekannten Schwachstellen gemeint ist, dann ist dies kaum zu bewältigen. Sinnvoller ist der Einsatz von vulnerability Scanner wie z. B. Nessus, Qualys oder OpenVAS. | Das war nicht gemeint. Der Einsatz der genannten Scanner wäre genau die Möglichkeit, dies umzusetzen.  Maßnahme: Kommentar ergänzt, der diese Scanner vorschlägt und sagt, dass i.d.R. nicht alle Schwachstellen geprüft werden können und müssen |
|  | "Der Hersteller sieht im Testplan Fuzz-Tests an allen relevanten Datenschnittstellen mit mindestens einem Werkzeug vor und führt diese auch durch." | --> Die Anzahl der Werkzeuge sagt erst einmal wenig über die Qualität (= Codeabdeckung) der Tests aus. Außerdem sind Fuzz-Tests bei OTS wie Windows und Linux wenig sinnvoll. | Das stimmt.  Maßnahme: Kommentar ergänzt, dass es v.a. um den eigenen Code geht. |
|  | "Der Hersteller sieht im Testplan eine Simulation der üblichen Angriffsvektoren vor [^11]" | --> Was ist mit Simulation gemeint? Wie soll z. B. eine Simulation von privilege escalation aussehen? | Das war missverständlich formuliert  Maßnahme: Geschrieben, dass man diese Angriffe durchführen und prüfen soll, ob das System damit umgehen kann |
| C) 7. | "Die Begleitmaterialien beschreiben, wie mit verlorengegangenen oder gestohlenen Produkten Tokens (z.B. Karten) sowie mit vergessenen Passwörtern umgegangen werden soll." | --> alle Elemente der Authentifizierungen können verloren gehen, ablaufen, gestohlen oder kompromittiert werden. Also muss für alle ein Prozess beschrieben werden, insbesondere für kryptographische Schlüssel- und Zertifikate. | Absolut zutreffend  Maßnahme: Umformuliert |
|  | "Die Begleitmaterialien beschreiben, welche Anti-Malware-Software für das Produkt zugelassen und von wo (z.B. Link) diese zu beziehen ist." | --> Es gibt Dutzende Antivirenprogramme für Windows... | Das stimmt. Die Aussage war nur, dass der Hersteller ein „Whitelisting“ machen soll.  Noch keine Maßnahme. Brauche Input. |
| D) 2. | "[^D2-05]: Die Frequenz müsste mindestens jährlich, bei kritischen Komponenten häufiger als monatlich erfolgen. Die UL 2900-2-1 spricht von Update-Zyklen von zwei Wochen." | --> selbst bei unkritischen Komponenten sollten security Patches zeitnah den Betreibern zur Verfügung gestellt werden, deshalb sollten die Zyklen nicht 2-4 Wochen übersteigen. | Dem stimme ich absolut zu. Die Forderung kann nur schnell zu einer Überforderung führen. In der Anmerkung heißt es, dass es bei den sicherheitskritischen Komponenten häufiger als monatlich sein muss.  Noch keine Maßnahme, brauche Input. |
| D) 3. | "wie der Hersteller die Patches zum Kunden bringt und dort deren Installation sichergestellt," | --> der Hersteller ist meines Erachtens für die Installation nicht zuständig oder verantwortlich (außer bei auto-update), sondern der Betreiber. | Absolut.  Maßnahme: Umformuliert |
| E) | "Stufe 3 ("Experten-Niveau"): Dieses Niveau erreichen hauptberufliche IT-Security-Experten. Es geht über das hinaus, was ein Auditor in der Regel bei Medizinprodukten erwarten darf. Auf diesem Niveau werden beispielsweise Schwachstellen beherrscht, die allgemein nicht bekannt sind. Energieversorger, Geheimdienste und das Militär müssten auf diesem Niveau agieren." | --> inkonsistent: die wenigsten security-Experten entdecken 0-days und Energieversorger sind nach meiner bisherigen Erfahrung auch nicht dagegen gewappnet. | Stimmt  Maßnahme: Satz mit 0-day gelöscht |

# Feedback „GHS“

|  |  |  |  |
| --- | --- | --- | --- |
| **Sektion** | **Aussage** | **Kommentar TÜV** | **Status oder Anmerkung CJ** |
| C) 2. a) i) | Interoperabilitätsebenen | GHS: und die organisatorische Ebene. ? STandards?? | Stimmt  Maßnahme: Organisatorische Ebene ergänzt |
| 4 | Der Hersteller spielt nur Code auf, der vor Reverse-Engineering und Auslesen des RAMs geschützt ist. | GHS: Datenspeicher ? Programmspeicher ? Macht das nichtt ehr die Plattform?) | Absolut  Maßnahme: In Kommentar ergänzt, dass das die Plattform üblicherweise übernimmt |