

VDGH-WHITEPAPER

IT-Product Security Whitepaper Template

Inhalt

Vorwort	3
Nutzung des Whitepapers	3
Entwicklung und Redaktion	4
Disclaimer und Feedback	4

Aus Gründen der besseren Lesbarkeit wird im Folgenden auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die gewählte Sprachform hat rein redaktionelle Gründe und beinhaltet keine Wertung.

Vorwort

Die IT-Sicherheit von Medizinprodukten, auch unter dem Begriff „Produktsicherheit“ abgekürzt, ist ein wesentlicher Bestandteil der Funktionalität von Medizinprodukten. Sie ist für den sicheren Betrieb unerlässlich und gewährleistet:

- Vertraulichkeit der Patientendaten
- Integrität des Medizinprodukts, d. h. das Produkt funktioniert wie vorgesehen.
- Verfügbarkeit des Medizinprodukts

Um die Produktsicherheit zu erreichen, muss ein Medizinprodukt ordnungsgemäß entwickelt, implementiert und getestet sein. Ferner muss es bestimmungsgemäß installiert, konfiguriert, gewartet und betrieben werden. Die Nichtbeachtung eines dieser Aspekte kann schnell die Produktsicherheit des Medizinprodukts beeinträchtigen, was schwerwiegende Folgen für die Produktsicherheit haben kann.

Das Ziel des IT-Product Security Whitepaper Templates ist es, den für die Installation, Wartung und den Betrieb von Medizinprodukten Verantwortlichen alle notwendigen Informationen zur Verfügung zu stellen, damit sie ihre Arbeit gemäß den erforderlichen Standards ausführen können:

- Bereitstellung von Informationen zu allen relevanten Aspekten der Produktsicherheit für Kunden und Servicepersonal.
- Sicherstellung der Verfügbarkeit aller Daten und Anleitungen, die für die sichere Installation, Konfiguration, Wartung und den Betrieb des Systems erforderlich sind.

Das IT-Product Security Whitepaper soll darüber hinaus alle Informationen bereitstellen, die während des Beschaffungs- und Auswahlprozesses für ein Medizinprodukt erforderlich sein können, sodass keine kundenspezifischen Fragebögen mehr erforderlich sind.

Nutzung des IT-Product Security Whitepaper Template

Das Whitepaper kann als Vorlage mit allen relevanten Informationen zum Produkt ausgefüllt werden. Zunächst sind allgemeine Informationen zum System anzugeben, darunter Hardware, Software und Betriebssystem mit Angaben zur Version, zum Patch-Status und zur Netzwerkkonfiguration. Im nächsten Abschnitt sind die Grundprinzipien und wichtigsten Sicherheitsmaßnahmen für das Produkt zu beschreiben. Dazu gehören Schutzmechanismen gegen Malware und Schwachstellen, Netzwerksicherheit, Umgang mit Vorfällen und Schwachstellen sowie Vorschriften für den Fernzugriff. Auch die Themen Authentifizierung und Autorisierung sollten ausführlich behandelt werden. Dazu gehören die Verwaltung von Benutzerkonten, rollenbasierte Zugriffskontrolle, spezielle Mechanismen wie das „Break-the-Glass“-Konzept und die organisatorische Datentrennung.

Das ausgefüllte Whitepaper sollte auch klare Vorgaben zum Datenschutz für übermittelte, gespeicherte und exportierte Daten enthalten. Außerdem sollte der datenschutzkonforme Umgang mit Informationen während des gesamten Produktlebenszyklus dargelegt wer-

den. Wichtige Aspekte wie physische Sicherheit, Überwachung sicherheitsrelevanter Vorfälle durch Ereignis- und Auditprotokollierung, Disaster Recovery, Einhaltung von Richtlinien und Zertifizierungen sowie Best Practices für eine sichere Systemkonfiguration sind ebenfalls Teil des Whitepapers und sollten berücksichtigt werden. Das Whitepaper kann durch ein Netzwerk- oder Systemdiagramm, in das das Produkt integriert ist, und ein standardisiertes MDS²-Formular mit weiteren Sicherheitsinformationen sinnvoll ergänzt werden. Das Whitepaper sollte außerdem einen rechtlichen Hinweis zu Haftungsfragen des Herstellers enthalten.

Ausgefüllt ergibt sich eine umfassende, praxisorientierte Darstellung der wichtigsten sicherheitskritischen Bereiche eines IT-Produkts, die branchenübergreifend im Gesundheitswesen eingesetzt werden kann.

Entwicklung und Redaktion

Das IT-Product Security Whitepaper Template wurde von der AG IT-Security des VDPGH (Verband der Diagnostica-Industrie e.V.) entwickelt, um einheitliche Leitlinien für die Dokumentation der Produktsicherheit in der Diagnostica-Industrie bereitzustellen. Die AG IT-Security setzt sich aus Branchenexperten und IT-Security-Experten zusammen. Ziel der Arbeitsgruppe ist es, Best Practices zu etablieren und die Mitgliedsunternehmen des VDPGH bei der Umsetzung umfassender Sicherheitsmaßnahmen für ihre Produkte zu unterstützen.

Disclaimer und Feedback

Das IT-Product Security Whitepaper Template dient als allgemeine Vorlage und kann als Referenz verwendet werden. Der Hersteller des IT-Produkts ist allein verantwortlich für die Implementierung, Wartung und Gewährleistung der Korrektheit aller darin beschriebenen Sicherheitsmaßnahmen. Es ist zu beachten, dass das Whitepaper nicht abschließend ist und dass nicht alle Abschnitte der Vorlage ausgefüllt werden müssen, wenn sie für das Produkt nicht zutreffend sind.

Der VDPGH nimmt Anregungen und Feedback zur Verbesserung der Vorlage gerne entgegen – bitte kontaktieren Sie uns mit Ihren Empfehlungen oder Fragen, damit wir die Vorlage für die Diagnostik-Community weiter verbessern können.

Impressum

Herausgeber

VDGH · Verband der Diagnostica-Industrie e. V.

Dr. Martin Walger, verantwortlich

Neustädtische Kirchstraße 8

10117 Berlin

Telefon +49 30 2005 99 -40

vdgh@vdgh.de

www.vdgh.de

Referat Digitales

Benedikt Beyer

Telefon +49 30 2005 99 -52

beyer@vdgh.de

Gestaltung

FGS Kommunikation, Berlin

Berlin, November 2025



www.vdgh.de/productsecurity