IEC 62443-4-1:2018 Sicherer Entwicklungsprozess für Produkte der industriellen Automatisierung

Sicherer Entwicklungslebenszyklus, acht Praktiken

47 Anforderungen. Diese Norm ist akkreditiert zertifizierbar. Stand 07/2026.

IEC 62443-4-1 ist zertifizierbar, aber der Gegenstand ist ungewöhnlich: zertifiziert wird der Entwicklungsprozess einer benannten Entwicklungsorganisation, also eine konkrete dokumentierte Fassung des sicheren Lebenszyklus. Nicht zertifiziert werden ein Produkt oder eine Person. Wege sind ISASecure SDLA und das IECEE CB Scheme. Ein solches Zertifikat begründet nach heutigem Stand keine Konformitätsvermutung zum EU Cyber Resilience Act. Nicht verwechseln mit IEC 62443-4-2, die Anforderungen an die Komponente selbst stellt. Diese Liste ist eine Arbeitshilfe für den Selbstcheck, kein Nachweis.

Betrieb	Datum	Bearbeiter

5 Praktik 1: Sicherheitsmanagement (SM) 13

SM-1 **Es existiert ein beschriebener Entwicklungsablauf, der Sicherheit über alle Phasen hinweg mitführt, von der ersten Idee bis zur Ausserbetriebnahme des Produkts, und dieser Ablauf ist derjenige, nach dem tatsächlich gearbeitet wird.** Dokument

Woran man es festmacht: Prozessbeschreibung oder Verfahrensanweisung mit Phasen, Ergebnissen je Phase und Übergabepunkten, dazu Belege aus einem laufenden Vorhaben, die zeigen, dass die Phasen wirklich durchlaufen wurden. Ein kleiner Betrieb kommt mit einer Seite pro Phase plus Checkliste im Ticketsystem aus, wichtig ist nur, dass Plan und gelebte Praxis zusammenpassen.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-2 **Für jede Aufgabe im sicheren Entwicklungsablauf ist festgelegt, wer sie verantwortet, und diese Zuordnung ist den Beteiligten bekannt.** Dokument

Woran man es festmacht: Rollen- und Aufgabenmatrix, in der jeder Prozessschritt einer benannten Rolle zugeordnet ist, ergänzt um die aktuelle Besetzung der Rollen. Bei wenigen Köpfen reicht eine Tabelle mit Rolle, Aufgabe und Person, wichtig ist die Vertretungsregelung für Urlaub und Krankheit.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-3 **Es ist nachvollziehbar bestimmt, welche Produkte, Varianten, Releases und Komponenten unter den sicheren Entwicklungsablauf fallen und welche nicht.** Dokument

Woran man es festmacht: Liste der betroffenen Produkte und Versionsstände mit Begründung für Ein- und Ausschlüsse, gepflegt bei jedem neuen Release. Praktisch ist eine Spalte in der Produktübersicht, die je Zeile Ja oder Nein und einen Satz zur Begründung trägt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-4 **Die Personen, die Sicherheitsaufgaben übernehmen, verfügen über die dafür nötige Fachkenntnis, und diese Kenntnis wird gezielt aufgebaut und aufgefrischt.**

Woran man es festmacht: Kompetenzprofil je Sicherheitsrolle, Qualifikationsnachweise, Schulungsplan und Teilnahmebelege, ergänzt um eine Lücken-Übersicht. Kleine Betriebe belegen das über Zertifikate, Konferenz- oder Webinarteilnahmen und einen kurzen jährlichen Abgleich, wer welche Lücke bis wann schliesst, notfalls ergänzt durch eingekaufte Expertise.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SM-5 **Der Geltungsbereich des sicheren Entwicklungsablaufs ist abgegrenzt und benennt die beteiligten Standorte, Organisationseinheiten, Zulieferbeiträge und Entwicklungsumgebungen samt der Grenzen dieses Bereichs.** Dokument

Woran man es festmacht: Geltungsbereichsbeschreibung mit Standorten, Teams, ausgelagerten Anteilen und Systemen, dazu eine Skizze der Schnittstellen nach aussen. Wer nur an einem Standort entwickelt, hält das in wenigen Sätzen fest und benennt ausdrücklich, was ausserhalb liegt, etwa fremdentwickelte Baugruppen oder Hosting durch Dritte.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-6 **Für alle an Anwender ausgelieferten Bestandteile, Software, Firmware, Konfigurationen und begleitende Dateien, ist eine Prüfung der Unversehrtheit möglich, sodass Empfänger unbemerkte Veränderungen erkennen können.**

Woran man es festmacht: Signaturen oder veröffentlichte Prüfsummen je Auslieferungspaket, Beschreibung des Verfahrens und ein Beispiel aus einem realen Release samt Anleitung für den Kunden, wie er die Prüfung durchführt. Für kleine Teams genügt eine signierte Prüfsummendatei neben dem Download plus ein Absatz in der Release-Notiz.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-7 **Die Umgebungen, in denen entwickelt, gebaut und getestet wird, sind gegen unbefugten Zugriff und gegen Manipulation an Quellcode, Build-Werkzeugen und Artefakten geschützt.**

Woran man es festmacht: Berechtigungskonzept für Repository, Build-Server und Testsysteme, Zugriffslisten mit letztem Prüfdatum, Protokolle sicherheitsrelevanter Änderungen und Nachweis der Trennung von Produktiv- und Entwicklungszugängen. Ohne eigene IT-Abteilung reichen Zwei-Faktor-Anmeldung, geschützter Hauptzweig mit Pflichtreview und eine halbjährliche Sichtung, wer noch Zugriff hat.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-8 **Private Schlüssel, mit denen Auslieferungen signiert werden, sind gegen Offenlegung und Missbrauch abgesichert, ihr Einsatz ist auf berechtigte Personen und Systeme begrenzt.**

Woran man es festmacht: Beschreibung von Aufbewahrung, Zugriff, Erneuerung und Sperrung der Schlüssel, Nachweis der geschützten Ablage, etwa Hardware-Token oder Schlüsseldienst, sowie Aufzeichnungen über Signiervorgänge. Ein kleiner Betrieb legt den Signaturschlüssel auf einen Hardware-Token, dokumentiert die zwei Personen mit Zugriff und hält einen Ablauf für den Verlustfall bereit.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-9 **Für zugekaufte oder übernommene Bestandteile, einschliesslich quelloffener Software, sind die sicherheitsbezogenen Erwartungen an den Lieferanten festgelegt und werden bei der Auswahl herangezogen.** Dokument

Woran man es festmacht: Sicherheitsanforderungen in Lieferantenvorgaben oder Verträgen, Auswahlkriterien für Fremdbestandteile, Bestandsliste aller Fremdbestandteile mit Version und Bezugsquelle sowie die Bewertung, ob der Lieferant die Erwartungen erfüllt. Ohne Einkaufsabteilung reicht eine gepflegte Komponentenliste mit einer Spalte, ob Sicherheitsupdates und Meldewege des Lieferanten geprüft wurden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-10 **Bestandteile, die ein Dritter im Auftrag eigens entwickelt, unterliegen denselben sicherheitsbezogenen Anforderungen wie die Eigenentwicklung, und die Einhaltung wird überprüft.**

Woran man es festmacht: Auftrags- oder Vertragsunterlagen mit den geforderten Sicherheitspflichten, Nachweise des Dienstleisters über die angewandten Praktiken, Abnahmeprotokolle und Ergebnisse eigener Prüfungen an der gelieferten Arbeit. Ohne eigenes Auditbudget genügen eine vertragliche Zusicherung, die Vorlage der Testergebnisse des Dienstleisters und eine eigene Stichprobe vor der Abnahme.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-11 **Sicherheitsbezogene Feststellungen aus allen Quellen, Tests, Reviews, Meldungen von Anwendern und Hinweisen Dritter, werden erfasst, in ihrer Tragweite eingeschätzt, mit Verantwortlichem und Frist versehen und bis zum Abschluss verfolgt.** Dokument

Woran man es festmacht: Fehler- oder Ticketsystem mit einer eigenen Kennzeichnung für Sicherheitsthemen, je Eintrag die Einschätzung der Tragweite, der Verantwortliche, die Frist und der Abschlussvermerk, dazu eine Auswertung offener Punkte. Ein kleines Team nutzt dafür ein Label im vorhandenen Ticketsystem und einen festen Tagesordnungspunkt in der Wochenrunde.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-12 **Vor der Freigabe eines Produkts ist geprüft und belegt, dass die vorgesehenen Schritte des sicheren Entwicklungsablaufs tatsächlich durchgeführt und die zugehörigen Nachweise erzeugt wurden.** Dokument

Woran man es festmacht: Freigabeprüfung je Release mit Abgleich gegen die Prozessschritte, Verweis auf die jeweiligen Nachweise und eine dokumentierte Freigabeentscheidung mit Datum und Unterschrift. Praktisch ist eine Freigabecheckliste, die ohne vollständige Haken keine Auslieferung zulässt, offene Punkte werden begründet und terminiert.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SM-13 **Der sichere Entwicklungsablauf selbst wird regelmässig hinterfragt und weiterentwickelt, wobei Erkenntnisse aus Vorfällen, Prüfergebnissen, Kundenrückmeldungen und der Bedrohungslage einfliessen.**

Woran man es festmacht: Aufzeichnungen der Prozessbewertung, etwa Managementbewertung oder Retrospektive, mit den ausgelösten Prozessänderungen, deren Umsetzungsstand und einem Verweis auf die Ursache. Wer die Reifegrade der Norm nutzt, hält je Praktik den heutigen Stand und das Ziel fest, Maturity Level 4 verlangt genau diesen Nachweis fortlaufender Verbesserung. Für einen kleinen Betrieb reicht ein Termin pro Jahr mit Protokoll und drei konkreten Verbesserungen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

6 Praktik 2: Festlegung der Sicherheitsanforderungen (SR) 5

SR-1 **Der vorgesehene Einsatzrahmen des Produkts ist beschrieben: erwartete Einsatzumgebung, unterstellte Schutzmaßnahmen der Umgebung, vorgesehene Nutzergruppen und Rollen, angenommene Vertrauensgrenzen sowie die Fälle, für die das Produkt ausdrücklich nicht gedacht ist.** Dokument

Woran man es festmacht: Beschreibung des Einsatzrahmens als eigenes Dokument oder als fester Abschnitt der Produktspezifikation, mit Netzumgebung, angenommenen externen Schutzmaßnahmen wie Firewall oder physischer Zutrittsschutz, Rollenliste und einer ausdrücklichen Negativliste. Ein kleiner Betrieb hält das auf zwei Seiten fest, ergänzt um eine einfache Skizze der Anlagenumgebung, und lässt sie vom Produktverantwortlichen datieren und freigeben.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR-2 **Für das Produkt liegt eine Bedrohungsbetrachtung vor, die Datenflüsse, Schnittstellen, Vertrauensgrenzen und Angriffswege abbildet, die daraus abgeleiteten Bedrohungen und ihre möglichen Auswirkungen benennt und Gegenmaßnahmen zuordnet. Sie wird bei relevanten Änderungen und mindestens einmal je Produktversion überprüft und aktualisiert, offene Punkte werden bis zur Klärung verfolgt.** Dokument

Woran man es festmacht: Bedrohungsmodell mit Datenflussdiagramm, Bedrohungsliste je Schnittstelle, zugeordneten Gegenmaßnahmen und Status der offenen Punkte, dazu die Änderungshistorie mit Datum und Autor. Ein kleiner Betrieb kommt mit einer Tabelle je Schnittstelle aus, Spalten: Was kann dort passieren, wie schlimm wäre es, was tun wir dagegen, wer prüft es.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SR-3 **Die Sicherheitsanforderungen an das Produkt sind festgelegt und dokumentiert. Sie decken die Ergebnisse der Bedrohungsbetrachtung, den beschriebenen Einsatzrahmen, geltende gesetzliche und vertragliche Vorgaben sowie das angestrebte Schutzniveau ab und beziehen die Sicherheitsfunktionen ein, die das Produkt selbst bereitstellen muss.** Dokument

Woran man es festmacht: Anforderungsliste oder Anforderungsverwaltung mit eindeutiger Nummerierung je Anforderung, Quellenangabe je Eintrag, etwa Bedrohung, Kundenvertrag oder Gesetz, und Angabe des angestrebten Schutzniveaus. Ein kleiner Betrieb führt das als eine Tabelle mit fester ID-Spalte, an der Verifikation und Test später andocken.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR-4 **Jede einzelne Sicherheitsanforderung ist so formuliert, dass sie eindeutig, widerspruchsfrei, prüfbar und einer konkreten Produktfunktion oder Schnittstelle zuordenbar ist, und sie enthält die Angaben, die eine spätere Prüfung ohne Rückfrage möglich machen.**

Woran man es festmacht: Stichprobe aus der Anforderungsliste, an der sich zu jeder Anforderung ein messbares Abnahmekriterium und die betroffene Funktion oder Schnittstelle ablesen lässt, sowie die Zuordnung Anforderung zu Testfall. Ein kleiner Betrieb prüft das mit einer festen Formulierungsvorlage und der Kontrollfrage, ob sich aus der Anforderung ohne Nachfrage ein Testfall schreiben lässt.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SR-5 **Die Sicherheitsanforderungen werden vor ihrer Verwendung in Entwurf und Umsetzung geprüft, und zwar unter Beteiligung der betroffenen Seiten wie Entwicklung, Test, Produktverantwortung und, wo sinnvoll, Vertrieb oder Kunde. Geprüft wird auf Vollständigkeit gegenüber Bedrohungsbetrachtung und Einsatzrahmen, auf Korrektheit und auf Prüfbarkeit. Befunde werden erfasst und bis zum Abschluss nachverfolgt.**

Woran man es festmacht: Prüfprotokoll mit Datum, Teilnehmern und ihren Rollen, geprüfter Fassung der Anforderungen, Liste der Befunde mit Verantwortlichem und Erledigungsstand sowie Freigabevermerk. Ein kleiner Betrieb löst das als Vier-Augen-Prüfung zwischen Entwicklung und Test mit einem kurzen Protokoll und einer Freigabezeile in der Anforderungsliste.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

7 Praktik 3: Sicherer Entwurf (SD) 4

SD-1 **Für jedes Produkt existiert eine Entwurfsbeschreibung, die die sicherheitsrelevanten Aspekte der Architektur festhält: welche Bausteine es gibt, wie sie miteinander sprechen, wo die Vertrauensgrenzen verlaufen, welche externen Schnittstellen nach aussen offen sind und mit welchen Mechanismen die zuvor festgelegten Sicherheitsanforderungen im Entwurf umgesetzt werden.** Dokument

Woran man es festmacht: Architekturdokument oder Entwurfsspezifikation mit einem Diagramm, das Komponenten, Datenflüsse und Vertrauensgrenzen zeigt, plus einer Zuordnungstabelle von Sicherheitsanforderung zu umsetzendem Entwurfselement. Ein kleiner Betrieb kommt mit einem gepflegten Diagramm plus zwei bis drei Seiten Erläuterung aus, wichtig ist nur, dass es versioniert im Repository liegt und bei Architekturänderungen mitgezogen wird.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SD-2 **Der Entwurf wird systematisch auf Bedrohungen untersucht. Die Analyse benennt Angreiferziele, betroffene Vertrauensgrenzen und Schnittstellen, die daraus folgenden Bedrohungen samt ihrer Einstufung sowie die Gegenmaßnahmen im Entwurf. Sie wird bei relevanten Änderungen an Architektur oder Umfeld erneut durchlaufen, und die identifizierten Bedrohungen werden bis zu einer Entscheidung nachverfolgt.** Dokument

Woran man es festmacht: Bedrohungsmodell je Produkt oder je grösserem Release, zum Beispiel als Tabelle mit Spalten für Bedrohung, betroffene Schnittstelle, Einstufung, Gegenmaßnahme und Status, dazu das Protokoll der Modellierungssitzung mit Teilnehmern und Datum. Ein kleines Team modelliert pragmatisch in einem Workshop von zwei bis drei Stunden entlang des Architekturdiagramms und hält die offenen Punkte als Tickets fest, damit der Nachweis der Nachverfolgung ohne Extraaufwand entsteht.

○ Offen ○ In Arbeit ○ Erfüllt ○ Nicht anwendbar

Nachweis / Begründung

SD-3 **Der Entwurf folgt nachvollziehbar anerkannten Gestaltungsprinzipien für Sicherheit, unter anderem geringstmögliche Rechte, sparsame Angriffsfläche, gestaffelte Verteidigung, sichere Voreinstellungen, sicheres Verhalten im Fehlerfall und möglichst einfache, prüfbare Sicherheitsmechanismen. Die Anwendung dieser Prinzipien ist im Entwurf erkennbar und begründet.**

Woran man es festmacht: Abschnitt in der Entwurfsbeschreibung oder eine hausinterne Entwurfsrichtlinie, die die Prinzipien benennt, dazu je Prinzip ein konkreter Beleg im Produkt, etwa die Rechtematrix der Dienste, die Liste der offenen Ports mit Begründung, die Auslieferungsvoreinstellungen oder die dokumentierte Fehlerreaktion. Ein kleiner Betrieb nutzt eine kurze Checkliste dieser Prinzipien als festen Punkt im Entwurfsreview und legt das ausgefüllte Blatt zum Entwurf.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SD-4 **Der Entwurf wird vor der Umsetzung fachlich gegengelesen. Die Prüfung deckt die Vollständigkeit gegenüber den Sicherheitsanforderungen, die Richtigkeit und Wirksamkeit der Sicherheitsmechanismen sowie die Ergebnisse der Bedrohungsanalyse ab. Beteiligt sind Personen mit ausreichender Sicherheitskompetenz, Befunde werden festgehalten und bis zur Erledigung verfolgt.** Dokument

Woran man es festmacht: Reviewprotokoll mit Datum, Prüfgegenstand samt Version, Teilnehmern und deren Rolle, Befundliste mit Status und der Freigabeentscheidung. Ein kleines Team hängt das Review an den Pull Request der Entwurfsdokumente und lässt die Befunde als Kommentare mit Erledigungsvermerk stehen, dann ist die Nachverfolgung ohne zusätzliches Werkzeug belegt. Fehlt intern die Sicherheitskompetenz, ist ein externer Gutachter auf Stundenbasis für die kritischen Entwürfe der pragmatische Weg.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

8 Praktik 4: Sichere Umsetzung (SI) 2

SI-1 **Es besteht ein festgelegtes Vorgehen, mit dem die tatsächliche Umsetzung gegen das sichere Design geprüft wird: geprüft wird, ob die im Entwurf vorgesehenen Schutzmaßnahmen im Code wirklich vorhanden und wirksam sind, ob die Verteidigungstiefe erhalten bleibt und ob bei der Umsetzung neue Schwachstellen entstanden sind. Die Prüfung wird durch fachlich geeignete Personen durchgeführt, gefundene Abweichungen werden erfasst und bis zur Klärung verfolgt.**

Woran man es festmacht: Verfahrensbeschreibung zur Umsetzungsprüfung sowie Prüfaufzeichnungen je Komponente oder Release: geprüftes Modul, Bezug zum Designdokument, Datum, prüfende Person, Befunde und deren Abarbeitungsstand. Als Beleg eignen sich Pull Request Reviews mit einer verbindlichen Sicherheits Checkliste, Ergebnisse statischer Codeanalyse mit dokumentierter Bewertung der Treffer sowie Protokolle von Review Runden. Ein kleines Team löst das mit dem Vier Augen Prinzip, einem Review Template im Repository, in dem jede Designmaßnahme einzeln abgehakt wird, und einem Ticket je offenem Befund. Wichtig ist, dass der Ersteller des Codes nicht sein eigener Prüfer ist.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SI-2 **Für alle sicherheitsrelevanten Entwicklungsarbeiten gelten verbindliche Programmierregeln, die mindestens die Vermeidung bekannter unsicherer Konstrukte und Funktionen, die Behandlung von Eingaben und Fehlern, den Umgang mit Speicher und Ressourcen sowie die Nutzung geprüften statt selbst entwickelten Sicherheitscodes abdecken. Die Regeln gelten je eingesetzter Programmiersprache, sind allen Entwickelnden bekannt und werden bei Bedarf, etwa bei neuen Angriffsmustern oder neuen Werkzeugen, aktualisiert.** Dokument

Woran man es festmacht: Freigegebene Programmierrichtlinie mit Versionsstand, Geltungsbereich je Sprache und Freigabedatum, ergänzt um den Nachweis, dass sie im Alltag greift: Konfiguration der Linter und Analysewerkzeuge im Repository, eine Build Regel, die Verstösse sichtbar macht, und die Teilnahmeliste der Einweisung. Kleine Betriebe schreiben keine eigene Richtlinie von Grund auf, sondern erklären einen etablierten öffentlichen Regelsatz für verbindlich, ergänzen ihn um eine kurze Liste eigener Zusatzregeln und verankern die Prüfung in der Pipeline, sodass die Einhaltung automatisch belegt wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

9 Praktik 5: Prüfen und Nachweisen der Sicherheit im fertigen Produkt (SVV) 5

SVV-1 Dokument

Zu jeder sicherheitsbezogenen Produktanforderung existiert mindestens ein zugeordneter Testfall, der belegt, dass die Schutzfunktion im vorgesehenen Betrieb wirkt, dass sie sich bei ungültigen Eingaben und Fehlbedienung wie festgelegt verhält und dass die ausgelieferten Standardeinstellungen dem sicheren Zustand entsprechen. Die Durchführung und das Ergebnis sind je geprüftem Softwarestand aufgezeichnet.

Woran man es festmacht: Zuordnungstabelle Anforderung zu Testfall zu Ergebnis, dazu Testprotokolle mit Datum, geprüftem Versions- oder Buildstand und Name der prüfenden Person. Ein kleiner Betrieb ergänzt in seiner Anforderungsliste einfach eine Spalte mit der Testfall-ID und archiviert den Ausgabe-Log des automatisierten Testlaufs aus der Build-Pipeline als Datei zur jeweiligen Version.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-2

Die Gegenmaßnahmen, die aus der Bedrohungsanalyse hervorgegangen sind, werden gezielt daraufhin geprüft, ob sie den unterstellten Angriffsweg tatsächlich schliessen. Geprüft wird gegen die identifizierten Bedrohungen, nicht nur gegen die gute Bedienung, und offene Punkte gehen in die Fehlerbehandlung ein.

Woran man es festmacht: Testfälle, die direkt auf die Einträge des Bedrohungsmodells verweisen, zum Beispiel je Bedrohungs-ID ein Missbrauchsszenario mit erwartetem Abwehrverhalten, sowie die Protokolle dieser Läufe. Ohne grossen Apparat genügt eine Spalte im Bedrohungsmodell mit Verweis auf den Testfall und dem Datum der letzten erfolgreichen Prüfung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-3 Dokument

Das Produkt wird vor der Freigabe systematisch auf Schwachstellen untersucht. Der Umfang deckt mindestens ab: Untersuchung der von aussen erreichbaren Schnittstellen und Dienste, Prüfung mit fehlerhaften und zufällig verfremdeten Eingaben, Abgleich der eingesetzten Fremdbestandteile gegen bekannte gemeldete Schwachstellen sowie Prüfung auf bekannte Fehlerklassen im eigenen Code. Die Funde sind mit Bewertung festgehalten.

Woran man es festmacht: Berichte der eingesetzten Werkzeuge mit Angabe von Werkzeugname, Version und Datenstand der Schwachstellendatenbank, Fuzzing-Protokolle, Liste der Fremdbestandteile mit Abgleichdatum und die Fundliste mit Bewertung und Entscheidung. Ein kleiner Betrieb kombiniert kostenfreie Standardwerkzeuge, einen Abhängigkeits-Scan und einen Port- und Dienste-Scan gegen das installierte Produkt und legt die Ausgaben je Release in einem Ordner ab.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-4

Am freigabereifen Produkt wird ein Angriffsversuch unter realistischen Bedingungen durchgeführt, der die Schutzmechanismen aktiv zu umgehen versucht, statt sie nur abzufragen. Umfang, Rahmenbedingungen und Grenzen der Prüfung sind vorab festgelegt, und die dabei gefundenen Schwächen werden wie Fehler behandelt und nachverfolgt.

Woran man es festmacht: Beauftragung oder Prüfauftrag mit Umfang und Testumgebung, Bericht mit Vorgehen, ausgenutzten Schwächen und Bewertung, dazu die Einträge im Fehler- oder Ticketsystem mit Nachweis der Behebung oder der begründeten Risikoannahme. Kleine Anbieter kaufen diese Prüfung typischerweise als abgegrenztes Zeitkontingent extern ein oder lassen sie von einer Person durchführen, die nicht am Produkt entwickelt hat.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SVV-5

Die Unabhängigkeit der prüfenden Personen ist geregelt und dem angestrebten Reifegrad angemessen. Wer einen Bestandteil selbst entwickelt hat, prüft ihn nicht in eigener Verantwortung frei, und mit steigendem Reifegrad wird die Prüfung von einer organisatorisch getrennten Stelle oder einer externen Partei verantwortet. Die tatsächliche Zuordnung ist je Prüfung nachvollziehbar.

Woran man es festmacht: Rollenfestlegung im Entwicklungsprozess, aus der die Trennung von Erstellung und Prüfung hervorgeht, sowie je Testlauf oder Prüfbericht der namentliche Eintrag der prüfenden Person und ihrer Rolle. Ein Zweipersonenbetrieb löst dies über gegenseitiges Prüfen mit dokumentiertem Vier-Augen-Vermerk und zieht für die tiefe Sicherheitsprüfung eine externe Person hinzu.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

10 Praktik 6: Umgang mit Sicherheitsmängeln (DM) 6

DM-1 **Es besteht ein festgelegter Weg, auf dem Hinweise auf Sicherheitsschwächen im Produkt aus allen Richtungen eingehen und erfasst werden: aus dem eigenen Team, aus Tests und Reviews, von Kunden und Integratoren, von externen Meldern sowie aus Hinweisen zu eingesetzten Fremd- und Open-Source-Bestandteilen. Der Meldeweg ist für Externe auffindbar und jede Meldung wird mit Eingangsdatum und Quelle festgehalten.** Dokument

Woran man es festmacht: Beschreibung des Meldewegs, die öffentlich erreichbare Kontaktstelle (Security-Seite, security.txt oder eine Mailadresse wie security@) und das Eingangsregister mit Datum, Quelle und Kurzbeschreibung je Meldung. Ein kleiner Betrieb kommt mit einem geteilten Postfach und einer einzigen Tabelle oder einem Ticket-Label aus, solange jede Meldung dort landet, auch die aus dem eigenen Entwicklerchat.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

DM-2 **Jede eingegangene Meldung wird gesichtet und darauf geprüft, ob sie sicherheitsrelevant ist und welche Produkte, Versionen und Bestandteile sie betrifft. Auch Meldungen, die sich als nicht sicherheitsrelevant oder als nicht zutreffend erweisen, werden mit Begründung abgeschlossen und nicht stillschweigend verworfen.**

Woran man es festmacht: Sichtungsvermerk je Meldung mit Ergebnis (sicherheitsrelevant ja oder nein), betroffenen Versionen und Begründung bei Ablehnung, sichtbar im Ticket oder in der Meldeliste. Wer wenige Meldungen hat, führt die Sichtung in einer wiederkehrenden kurzen Runde durch und hält das Ergebnis in zwei Sätzen je Eintrag fest.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

DM-3 **Bestätigte Sicherheitsmängel werden nach einem einheitlichen Verfahren bewertet: Ursache, betroffene Versionen und Konfigurationen, mögliche Auswirkung auf Betrieb und Sicherheit, Ausnutzbarkeit sowie der Schweregrad nach einem festgelegten Massstab. Das Bewertungsergebnis ist aufgezeichnet und nachvollziehbar.** Dokument

Woran man es festmacht: Bewertungsbogen oder Ticketfelder je Mangel mit Ursache, Schweregrad und dem verwendeten Massstab (zum Beispiel eine gängige Bewertungssystematik mit dokumentiertem Vektor), dazu die Liste der betroffenen Versionen. Für kleine Teams reicht eine feste Feldvorlage im Ticketsystem plus eine halbe Seite, die den Massstab und die Schwellen für sofortiges Handeln beschreibt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

DM-4 **Für bewertete Sicherheitsmängel ist entschieden, wie damit umgegangen wird: Behebung, Ausgleichsmaßnahme oder begründete Annahme des Risikos. Die Entscheidung richtet sich nach dem Schweregrad, sie ist einer verantwortlichen Person und einem Termin zugeordnet und der Mangel wird bis zum Abschluss verfolgt.** Dokument

Woran man es festmacht: Maßnahmenliste oder Ticketstatus mit Verantwortlichem, Zieltermin, Art der Maßnahme und Abschlussvermerk, verknüpft mit dem Codestand oder der Version, in der die Behebung wirksam wird. Angenommene Restrisiken brauchen eine kurze schriftliche Begründung mit Freigabe durch die Produktverantwortung. Ein kleiner Betrieb bildet das in einem Ticketboard mit Fälligkeitsdatum ab, ohne zusätzliches Werkzeug.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

DM-5 **Betroffene Nutzer, Integratoren und weitere Beteiligte werden über Sicherheitsmängel informiert, sobald die Bewertung dies erfordert, mit Angabe der betroffenen Versionen, der Auswirkung, der verfügbaren Behebung oder Ausgleichsmaßnahme. Fristen und Empfängerkreis der Bekanntgabe sind vorab festgelegt, ebenso das Vorgehen bei Meldungen Dritter, die eine eigene Veröffentlichungsfrist mitbringen.**

Woran man es festmacht: Veröffentlichte Sicherheitshinweise oder Advisories mit Datum und Versionsbezug, der Verteiler oder Abonnentenkanal sowie die schriftliche Regel zu Fristen und koordinierter Veröffentlichung. Wer wenige Kunden hat, nutzt eine Sammelmail an eine gepflegte Kundenliste und eine datierte Hinweisseite, deren Änderungen versioniert sind.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

DM-6 **Der Umgang mit Sicherheitsmängeln wird in festen Abständen überprüft. Betrachtet werden dabei offene und überfällige Fälle, die Zeiten von der Meldung bis zur Behebung, wiederkehrende Ursachen sowie die Wirksamkeit der eingeleiteten Maßnahmen. Aus der Überprüfung abgeleitete Verbesserungen am Vorgehen werden umgesetzt und ihre Umsetzung verfolgt.**

Dokument

Woran man es festmacht: Protokoll der wiederkehrenden Überprüfung mit Datum, Teilnehmern, Kennzahlen zu offenen und überfälligen Fällen sowie einer Liste beschlossener Verbesserungen mit Verantwortlichem und Termin. Ein kleiner Betrieb hängt diesen Punkt an eine bestehende Quartalsrunde und hält Kennzahlen und Beschlüsse auf einer Seite fest.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

11 Praktik 7: Verwaltung von Sicherheitsaktualisierungen (SUM) 5

SUM-1 **Jede Sicherheitsaktualisierung für das Produkt wird vor der Freigabe an Kunden gegen die unterstützten Produktversionen und Betriebsumgebungen geprüft, und es liegt eine Aufzeichnung darüber vor, dass die Aktualisierung die Schwachstelle schliesst, ohne die bestimmungsgemässe Funktion zu stören.**

Dokument

Woran man es festmacht: Testprotokoll je Patch mit getesteter Produktversion, Plattform, Testfällen (Wirksamkeit gegen die Schwachstelle plus Regression der Kernfunktionen) und Freigabevermerk. Ein kleiner Betrieb kommt mit einer Patch-Freigabeliste im Ticket aus: Ticket-ID, geprüft von, geprüft am, Ergebnis, plus dem Log des automatisierten Testlaufs als Anhang.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-2 **Für alle Bestandteile des Produkts, die nicht selbst entwickelt wurden (Fremdbibliotheken, Betriebssystem, Laufzeitumgebungen), ist geregelt und belegt, wie deren Sicherheitsaktualisierungen bewertet, in das eigene Produkt übernommen oder mit einer Begründung verworfen werden.**

Dokument

Woran man es festmacht: Komponenteninventar der Fremdanteile mit Version und Bezugsquelle, dazu je gemeldeter Fremd-Schwachstelle ein Bewertungseintrag mit Entscheidung (übernehmen, nicht betroffen, mit Ausgleichsmaßnahme belegen) und Begründung. Kleine Teams nutzen dafür einen automatisierten Abhängigkeits-Scan im Build und pflegen die Entscheidungen direkt als Kommentar im Scan-Ergebnis oder in einer schlanken Ausnahmeliste.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-3 **Zu jeder ausgelieferten Sicherheitsaktualisierung erhalten die Anwender eine verständliche Begleitinformation: welche Produktversionen betroffen sind, welche Schwachstelle behoben wird, wie schwerwiegend sie ist, ob Nebenwirkungen oder Ausgleichsmaßnahmen zu beachten sind und wie die Aktualisierung eingespielt wird.**

Dokument

Woran man es festmacht: Veröffentlichte Sicherheitshinweise oder Release Notes mit Kennung der Schwachstelle, betroffenen Versionen, Einstufung der Schwere, Installationsschritten und Hinweisen zum Rückfall auf den vorherigen Stand. Kleine Anbieter führen eine einzige öffentliche Seite mit chronologischer Liste der Sicherheitshinweise und verlinken sie aus dem Produkt heraus.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-4 **Es gibt einen definierten und gegen Manipulation geschützten Weg, auf dem Anwender Sicherheitsaktualisierungen beziehen, und die Echtheit und Unversehrtheit einer Aktualisierung lässt sich auf Anwenderseite prüfen, bevor sie eingespielt wird.**

Woran man es festmacht: Beschreibung des Auslieferungskanals (Downloadbereich, Update-Server, Datenträger) samt Schutzmaßnahmen, dazu die digitale Signatur oder Prüfsumme je Paket und die Anleitung, wie der Anwender sie verifiziert. Kleine Betriebe erreichen das mit Signatur über den Build-Server, veröffentlichter Prüfsumme neben dem Download und einem klar benannten Ort, an dem der öffentliche Schlüssel liegt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SUM-5 **Für die Bereitstellung von Sicherheitsaktualisierungen bestehen festgelegte Zeitziele, die sich an der Schwere der Schwachstelle orientieren, die tatsächlich erreichten Zeiten werden nachgehalten, und Überschreitungen sind begründet und mit einer Zwischenmaßnahme für die Anwender hinterlegt.** Dokument

Woran man es festmacht: Interne Vorgabe mit Zeitfenstern je Schwerekategorie (zum Beispiel kritisch <= 30 Tage, hoch <= 90 Tage) und eine Auswertung je Schwachstelle: Meldedatum, Freigabedatum des Patches, verstrichene Tage, Abweichungsgrund. Kleine Betriebe pflegen das als zwei Datumsfelder im Schwachstellen-Ticket und schauen die Liste einmal im Quartal durch, statt ein eigenes Kennzahlensystem aufzusetzen.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

12 Praktik 8: Sicherheitsleitfäden für Einsatz und Betrieb des Produkts (SG) 7

SG-1 **Für jedes Produkt liegt eine Beschreibung der gestaffelten Schutzwirkung vor: sie benennt die im Produkt selbst verbauten Schutzebenen, ordnet ihnen die Bedrohungen zu, gegen die sie wirken, und macht sichtbar, welche Schutzwirkung erst durch das Zusammenspiel mehrerer Ebenen entsteht.** Dokument

Woran man es festmacht: Ein Abschnitt in der ausgelieferten Produktdokumentation oder ein eigenes Schutzkonzept, das je Schutzebene den Mechanismus, die abgedeckte Bedrohung und die Grenzen der Wirkung nennt. Ein kleiner Betrieb hält das als zweiseitige Tabelle: Spalte Schutzebene, Spalte Bedrohung aus der eigenen Bedrohungsanalyse, Spalte Restrisiko. Der Verweis auf die Bedrohungsanalyse aus SR-2 genügt, die Inhalte müssen nicht doppelt gepflegt werden.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SG-2 **Die Dokumentation benennt die Schutzmaßnahmen, die das Produkt nicht selbst mitbringt, sondern von der Einsatzumgebung erwartet, zum Beispiel Netzsegmentierung, vorgelagerte Firewalls, physischer Zugangsschutz oder ein externer Zeitdienst, und macht deutlich, dass die zugesicherte Sicherheit ohne diese Maßnahmen nicht erreicht wird.** Dokument

Woran man es festmacht: Kapitel Einsatzvoraussetzungen im Handbuch oder ein Referenzarchitektur-Bild mit Zonen und Übergängen, in dem die vom Betreiber zu stellenden Maßnahmen ausdrücklich markiert sind. Praktisch bewährt hat sich eine Liste der Annahmen über die Umgebung, die direkt aus dem Sicherheitskontext des Produkts abgeleitet und bei jeder Produktversion gegengelesen wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SG-3 **Es existiert eine Anleitung zur sicheren Grundkonfiguration, die alle sicherheitsrelevanten Einstellungen, Dienste, Ports und Schnittstellen aufführt, den empfohlenen Auslieferungszustand angibt und die Auswirkungen einer Abweichung von dieser Empfehlung beschreibt.** Dokument

Woran man es festmacht: Härtungsleitfaden mit Einstellungstabelle: Parameter, empfohlener Wert, Wirkung, Nebenwirkung beim Abweichen. Dazu die Liste der ab Werk aktiven Dienste und Ports mit Begründung, warum sie aktiv bleiben. Ein kleines Team pflegt diese Tabelle direkt neben der Konfigurationsdatei im Repository und exportiert sie in die Auslieferungsdokumentation, so bleibt sie mit dem Produkt in Deckung.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SG-4 **Für den laufenden Betrieb liegt eine Anleitung vor, die beschreibt, wie das Produkt sicher betrieben, überwacht und im Sicherheitszustand gehalten wird, einschliesslich Sicherung und Wiederherstellung, Protokollierung und Umgang mit sicherheitsrelevanten Ereignismeldungen.** Dokument

Woran man es festmacht: Betriebsanleitung mit Abschnitten zu Protokollierung, Sicherungen, Wiederanlauf und Ereignismeldungen. Als Nachweis eignet sich zusätzlich die Liste der sicherheitsrelevanten Meldungen, die das Produkt ausgibt, mit einer kurzen Handlungsempfehlung je Meldung, damit der Betreiber sie nicht selbst deuten muss.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SG-5 **Die Dokumentation erklärt, wie Benutzerkonten, Rollen und Berechtigungen des Produkts eingerichtet und gepflegt werden, insbesondere die Trennung von Rollen, das Ändern voreingestellter Zugangsdaten und das Entfernen nicht mehr benötigter Konten.** Dokument

Woran man es festmacht: Kapitel Kontenverwaltung mit Rollenübersicht und der Zuordnung von Rechten je Rolle, dazu ein ausdrücklicher Hinweis auf voreingestellte Zugangsdaten und deren Änderung bei Inbetriebnahme. Praktisch tauglich ist eine kurze Inbetriebnahme-Checkliste im Handbuch, die der Betreiber abhaken und ablegen kann.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SG-6 **Es liegt eine Anleitung für die sichere Ausserbetriebnahme vor, die das vollständige Entfernen sensibler Daten aus dem Produkt beschreibt, etwa Zugangsdaten, Schlüssel, Konfigurationsdaten und Protokolle, bevor das Gerät weitergegeben, wiederverwendet oder entsorgt wird.** Dokument

Woran man es festmacht: Abschnitt Ausserbetriebnahme mit Aufzählung aller Speicherorte sensibler Daten im Produkt und dem jeweiligen Löschverfahren, inklusive der Fälle, in denen ein Löschen technisch nicht möglich ist und die Hardware physisch zu vernichten ist. Hilfreich ist eine Liste der persistenten Speicher aus der Architekturbeschreibung, sie verhindert, dass ein Speicherort vergessen wird.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung

SG-7 **Die an Anwender ausgelieferte Sicherheitsdokumentation wird vor Freigabe geprüft: sie ist fachlich richtig, mit der ausgelieferten Produktversion konsistent, vollständig gegenüber den vorgesehenen Inhalten und für die vorgesehene Zielgruppe verständlich, und sie wird nachgezogen, wenn sich das Produkt ändert.**

Woran man es festmacht: Prüfaufzeichnung je Dokument und Produktversion mit Prüfer, Datum, Befunden und deren Erledigung, verknüpft mit der Release-Freigabe. Ein kleiner Betrieb löst das über ein Vier-Augen-Prinzip im Pull-Request der Dokumentation: ein Entwickler prüft die Technik, eine zweite Person die Verständlichkeit, die Freigabe wird im Ticket festgehalten. Auslieferbar ist eine Version erst, wenn die Prüfung dokumentiert vorliegt.

◯ Offen ◯ In Arbeit ◯ Erfüllt ◯ Nicht anwendbar

Nachweis / Begründung