

Anlage 8: Sicherheit in Entwicklung und Betrieb

Diese Anlage beschreibt die Maßnahmen des Auftragsverarbeiters zur Sicherheit in Entwicklung und Betrieb der Plattform. Sie ergänzt Anlage 1 und beruht auf den internen Richtlinien zum Patch-Management und zum Change-Management.

1. Patch- und Schwachstellenmanagement

1.1 Geltungsbereich. Das Patch-Management erfasst verbindlich alle produktionsrelevanten Komponenten im Verantwortungsbereich des Auftragsverarbeiters, insbesondere Betriebssysteme, Container-Images, Base-Images, Container-Runtimes und Orchestrierungsplattformen, eigenentwickelte und eingesetzte Standardsoftware, eingesetzte Drittanbieter-Bibliotheken, Frameworks, Packages und Laufzeitabhängigkeiten, Datenbankserver und Engines, Infrastrukturkomponenten sowie Sicherheitskomponenten einschließlich Firewalls, Endpoint-Security, Identitäts- und Single-Sign-on-Komponenten, Scannern sowie Monitoring- und Security-Werkzeugen.

Bei vollständig durch externe Anbieter betriebenen Leistungen liegt das Patch-Management für die zugrunde liegende Plattform beim jeweiligen Anbieter. Der Auftragsverarbeiter bleibt zuständig für das Patchen eigener Konfigurationen und Workloads, die Aktualisierung eigener Anwendungen und Deployments, die Bewertung anbieterseitiger Sicherheitshinweise sowie die Risikobewertung und Nachverfolgung relevanter Sicherheitsupdates.

1.2 Identifikation. Sicherheits- und Funktionsupdates werden fortlaufend über Herstellerinformationen, Sicherheitshinweise, interne Erkenntnisse, Monitoring, Support-Fälle und sonstige technische Hinweise identifiziert.

1.3 Bewertung und Priorisierung. Jeder relevante Patch wird bewertet hinsichtlich der Kritikalität der Schwachstelle, der Betroffenheit der Plattform, der Auswirkungen auf Datenschutz und Informationssicherheit, der Betriebs- und Verfügbarkeitsrisiken sowie der Kompatibilität mit vorhandenen Komponenten. Die Priorisierung erfolgt durch die technische Leitung.

1.4 Umsetzungsfristen. Sicherheitsrelevante Updates werden nach Priorität innerhalb folgender Fristen umgesetzt:

Kategorie	Umsetzungsfrist
Kritische Sicherheitsupdates: unmittelbare erhebliche Gefahr für Vertraulichkeit, Integrität oder Verfügbarkeit oder aktive Ausnutzung	unverzüglich
Hohe Priorität: hohes Risiko, Missbrauch wahrscheinlich oder erhebliche Betriebsbeeinträchtigung möglich	innerhalb von 24 Stunden
Mittlere Priorität: relevantes, aber nicht unmittelbares Risiko	innerhalb von 2 Tagen
Niedrige Priorität: geringe sicherheitsseitige Relevanz	innerhalb von 3 Tagen, soweit sicherheitsseitig erforderlich, andernfalls im regulären Release-Zyklus

1.5 Freigabe. Die Freigabe produktiver Patch-Maßnahmen erfolgt durch die technische Leitung im Vier-Augen-Prinzip. Kritische Sicherheitsupdates können außerhalb regulärer Releasezyklen umgesetzt werden.

1.6 Fristüberschreitungen. Kann ein Patch nicht fristgerecht umgesetzt werden, entscheidet die technische Leitung über das weitere Vorgehen. Begründung und getroffene Kompensationsmaßnahmen werden nachvollziehbar dokumentiert. Als Kompensationsmaßnahmen kommen insbesondere Konfigurationsanpassungen, die Deaktivierung nicht erforderlicher Funktionen, Zugriffsbeschränkungen, zusätzliche Überwachungsmaßnahmen sowie organisatorische Einschränkungen bis zur Umsetzung des Patches in Betracht.

2. Sicherheit in der Entwicklung und Änderungsmanagement

2.1 Geltungsbereich. Erfasst sind alle produktionsrelevanten Änderungen, insbesondere an Backend- und Frontend-Komponenten, Infrastruktur- und Cloud-Komponenten, Datenbanken und Speicherkomponenten, Sicherheits- und Konfigurationskomponenten, Integrationen und Schnittstellen zu Drittsystemen sowie Deployments, Releases und Konfigurationsänderungen.

2.2 Grundsätze. Jede produktionsrelevante Änderung wird vor Umsetzung dokumentiert, versioniert und nach Umsetzung nachvollziehbar protokolliert. Änderungen werden vor Umsetzung hinsichtlich ihrer Auswirkungen auf Sicherheit, Datenschutz, Verfügbarkeit und

Funktionalität bewertet und vor Ausbringung in die Produktivumgebung geprüft. Entwicklungs-, Test- und Produktivumgebungen sind voneinander getrennt.

2.3 Versionierung und Dokumentation. Für die Code-Versionierung wird Git als verbindlicher Standard genutzt. Jede produktionsrelevante Änderung wird zentral dokumentiert mit Beschreibung und Ziel, betroffenen Systemen, Risikobetrachtung, Testvorgehen, Freigabe, Umsetzungszeitpunkt und gegebenenfalls Hinweisen zum Rollback.

2.4 Freigabe. Die Freigabe produktiver Änderungen erfolgt durch die technische Leitung im Vier-Augen-Prinzip.

2.5 Tests vor Produktivsetzung. Verpflichtend sind zwei manuelle Funktionstests, davon einer durch einen Entwickler und einer durch einen unabhängigen Tester, sowie automatisierte End-to-End-Tests für zentrale Prozesse, insbesondere Account-Erstellung, Anmeldung, Onboarding, Kalenderintegration und Account-Löschung. Bei kritischen oder produktionsrelevanten Änderungen erfolgen zusätzlich Smoke Tests der Kernfunktionen, eine gezielte Prüfung betroffener Komponenten und Schnittstellen, Regressionstests für bekannte kritische Funktionen sowie die Auswertung relevanter Protokolle und Monitoring-Meldungen nach dem Deployment.

2.6 Verifikation nach Produktivsetzung. Nach der Umsetzung wird geprüft, ob die betroffenen Funktionen ordnungsgemäß arbeiten, keine offensichtlichen Folgefehler auftreten, die Plattform stabil und erreichbar bleibt und keine sicherheits- oder datenschutzrelevanten Fehlwirkungen erkennbar sind.

2.7 Rollback. Für produktive Änderungen besteht die Möglichkeit, auf einen vorherigen stabilen Stand zurückzukehren. Sämtliche relevanten Artefakte werden vorgehalten; die Plattform wird containerbasiert betrieben.

2.8 Notfalländerungen. Für kritische Sicherheitsvorfälle, schwerwiegende Fehler oder akute Produktionsstörungen gilt ein beschleunigter Prozess außerhalb des regulären Releasezyklus. Auch in diesen Fällen gilt das Prinzip kontrollierter Umsetzung; die vollständige Dokumentation, die nachgelagerte Prüfung und die Freigabebestätigung erfolgen unverzüglich im Anschluss.

3. Nachweisführung und Aufbewahrung

Manuelle Prüfungen werden im jeweiligen Pull Request durch den verantwortlichen Tester dokumentiert; der Pull Request wird erst nach erfolgreicher Prüfung freigegeben und übernommen. Automatisierte Prüfungen werden in den Deployment-Pipelines dokumentiert und dort nachvollziehbar vorgehalten.

Die Dokumentation umfasst mindestens die betroffene Komponente, Anlass und Quelle, Priorität, Datum der Bewertung und der Umsetzung, die verantwortlichen Rollen, die Prüfergebnisse sowie etwaige Abweichungen und Kompensationsmaßnahmen.

Patch- und änderungsbezogene Artefakte und Nachweise werden mindestens ein Jahr aufbewahrt.

4. Sicherheitstests

Der Auftragsverarbeiter lässt die Plattform in regelmäßigen Abständen, mindestens jährlich, durch einen unabhängigen Dritten einem Penetrationstest unterziehen. Festgestellte Schwachstellen werden nach den Fristen gemäß Ziffer 1.4 behoben.

5. Regelmäßige Überprüfung

Die Prozesse zum Patch- und Change-Management werden regelmäßig auf Wirksamkeit, Aktualität und Angemessenheit überprüft und bei Bedarf angepasst. Dies gilt insbesondere bei Änderungen der Systemarchitektur, neuen regulatorischen Anforderungen oder geänderter Bedrohungslage.