

Anforderungen IT-Security

Content Management System - 250210



**Kaufmännische Krankenkasse - KKH
Karl-Wiechert-Allee 61
30625 Hannover**

Einleitung

Dieses Dokument dient als Ergänzung der Allgemeinen Rahmenbedingungen IT- Service Management.

Es enthält die IT-Security-spezifische Anforderungen im Rahmen der Beschaffung von IT-Produkten.

Die Kapitel-Angaben beziehen sich auf die Allgemeinen Rahmenbedingungen ITSM und sind in diesem Zusammenhang zu verstehen.

Anforderungen

Für den beschriebenen Service sind folgende IT-Security-spezifische Anforderungen zu erfüllen:

1. **(1.2) Gültigkeit der ITSM-Anforderungen in Abhängigkeit vom Betriebsmodell:**
Bei höheren Schutzbedarfen haben die strengereren Anforderungen aus B3S-GKV/PV, BSIG, SGB V/X sowie dem KKH Security-Guide Vorrang vor den vereinbarten IT-Service-Management-Prozessen.
2. **(2.1) Kollaboration:**
Das eingesetzte Personal des AN absolviert regelmäßig Informationssicherheits-, Datenschutz-/Sozialdatenschutz- und bei KI-Einsatz AI-Kompetenz Schulungen.
3. **(2.1) Kollaboration:**
Der AN garantiert für Administratoren und Supportpersonal personenbezogene Accounts, MFA, Least Privilege, die Protokollierung privilegierter Zugriffe und geregelte Vertretungen.
4. **(2.2.1) Servicezeiten:**
Der AN kann für P1/P2- und Security-Incidents eine 24x7-Ruf- und Reaktionsbereitschaft anbieten. Die Kosten für diese Leistungen sind separat auszuweisen.
5. **(2.4) Service Meetings:**
Security- und Compliance-Themen sind fester Bestandteil der Service Reviews, insbesondere Risiken, Schwachstellen, Incidents, Audit-Findings und Maßnahmenstatus.
6. **(2.5) Service Level Management:**
P1 und P2 können für vollständigen Serviceausfall, Cyberangriffe, Kompromittierung oder erhebliche Datenschutz-/Sozialdatenschutzereignisse genutzt werden.
7. **(2.7.1) Incident-Management:**
Der AN muss einen eigenständigen, dokumentierten und verbindlichen Prozess zur Behandlung von Informationssicherheitsvorfällen (Security Incident Management) implementieren und während der gesamten Vertragslaufzeit aufrechterhalten. Dieser Prozess muss in das allgemeine Incident Management integriert sein und eine eindeutige Abgrenzung zwischen betrieblichen Störungen und sicherheitsrelevanten

Ereignissen ermöglichen.

Der Prozess muss mindestens die Erkennung (Detection), Erstbewertung und Priorisierung (Triage), Eindämmung (Containment), Ursachen- und Schadensbeseitigung (Eradication), Wiederherstellung des regulären Betriebs (Recovery), forensische Untersuchung sowie die systematische Nachbereitung (Lessons Learned) umfassen.

Für jede Prozessphase sind Verantwortlichkeiten, Eskalationswege, Entscheidungskompetenzen und Dokumentationspflichten verbindlich festzulegen, spätestens mit Abschluss des Vertrages. Sicherheitsvorfälle müssen anhand definierter Kriterien hinsichtlich ihrer Kritikalität, ihrer Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit sowie möglicher regulatorischer Meldepflichten bewertet und klassifiziert werden.

Der AN muss sicherstellen, dass sicherheitsrelevante Ereignisse und durchgeführte Maßnahmen nachvollziehbar und revisionssicher dokumentiert werden. Bei der Sicherung und Auswertung digitaler Beweismittel sind deren Integrität, Authentizität und Nachvollziehbarkeit durch geeignete organisatorische und technische Maßnahmen sicherzustellen. Hierzu gehört insbesondere eine dokumentierte Beweismittelkette (Chain of Custody).

Für kritische Sicherheitsvorfälle sind unverzügliche Eskalations- und Informationsverfahren gegenüber dem Auftraggeber vorzusehen. Die konkreten Meldewege, Meldefristen und Mitwirkungspflichten sind verbindlich, spätestens mit Abschluss des Vertrages, zu vereinbaren.

Nach Abschluss eines Sicherheitsvorfalls muss eine dokumentierte Ursachenanalyse erfolgen. Identifizierte Schwachstellen und erforderliche Korrekturmaßnahmen sind zu erfassen, hinsichtlich ihrer Umsetzung zu verfolgen und auf ihre Wirksamkeit zu überprüfen.

8. (2.7.1) Incident-Management und (2.7.4) Availability Management

Der AN muss eine kontinuierliche, risikoorientierte Überwachung sicherheitsrelevanter Ereignisse für sämtliche im Leistungsumfang enthaltenen Systeme, Anwendungen, Schnittstellen und Infrastrukturkomponenten gewährleisten. Hierzu sind geeignete technische und organisatorische Maßnahmen zur zentralen Erfassung, Korrelation, Analyse und Bewertung sicherheitsrelevanter Protokoll- und Ereignisdaten vorzusehen. Die Überwachung muss die zeitnahe Erkennung potenzieller Sicherheitsvorfälle, unberechtigter Zugriffe, auffälliger Systemaktivitäten, sicherheitsrelevanter Konfigurationsänderungen und möglicher Beeinträchtigungen der Verfügbarkeit unterstützen.

Der AN muss die Anbindung an eine zentrale Sicherheitsüberwachungsinfrastruktur des AG oder eines durch diesen benannten Security Operations Centers (SOC) ermöglichen. Hierfür sind standardisierte, dokumentierte und sicher abgesicherte Schnittstellen zur Übermittlung sicherheitsrelevanter Ereignis- und Protokolldaten bereitzustellen. Die Anbindung muss eine automatisierte Weiterverarbeitung und Korrelation der Ereignisdaten innerhalb einer zentralen Sicherheitsinformations- und Ereignismanagementumgebung (SIEM) ermöglichen. Die Auswahl der hierfür eingesetzten technischen Lösungen bleibt dem AN überlassen, sofern die geforderten funktionalen, sicherheitstechnischen und betrieblichen Anforderungen erfüllt werden.

Für sicherheitskritische Ereignisse muss eine automatisierte, prioritätsabhängige Alarmierung eingerichtet werden. Die Alarmierung muss definierte Schweregrade, Eskalationsschwellen, Zuständigkeiten und Reaktionszeiten berücksichtigen.

Kritische Sicherheitsereignisse müssen unverzüglich an die vereinbarten Ansprechpartner beziehungsweise die zuständige Sicherheitsüberwachungsinstanz

übermittelt werden.

Die Integrität, Vollständigkeit und Verfügbarkeit sicherheitsrelevanter Protokolldaten sind durch geeignete Schutzmaßnahmen sicherzustellen. Insbesondere müssen unberechtigte Veränderungen, Manipulationen und Löschungen verhindert beziehungsweise zuverlässig erkannt werden können. Zugriffsberechtigungen auf Protokolldaten sind nach dem Erforderlichkeitsprinzip zu vergeben. Aufbewahrungs- und Löschfristen sind unter Berücksichtigung vertraglicher, gesetzlicher und regulatorischer Anforderungen verbindlich festzulegen.

Sämtliche für die Sicherheitsüberwachung relevanten Systeme und Komponenten müssen über eine einheitliche, synchronisierte und nachvollziehbare Systemzeit verfügen. Die Zeitsynchronisation muss über geeignete, vertrauenswürdige Zeitquellen erfolgen. Zeitstempel müssen eine systemübergreifende Korrelation von Ereignissen sowie die Rekonstruktion sicherheitsrelevanter Abläufe im Rahmen von Incident Response und IT-Forensik ermöglichen.

Der AN muss die Funktionsfähigkeit der Sicherheitsüberwachung, der Protokolldatenerfassung, der zentralen Anbindung und der Alarmierungswege regelmäßig überprüfen. Ausfälle oder Einschränkungen dieser Funktionen müssen erkannt, dokumentiert und entsprechend ihrer Kritikalität eskaliert werden.

Die Umsetzung der genannten Anforderungen ist durch geeignete Prozessdokumentationen, technische Konzepte, Schnittstellenbeschreibungen und prüffähige Nachweise gegenüber dem Auftraggeber zu belegen.

9. **(2.7.1) Incident-Management:**

Vulnerability Management: Regelmäßige Schwachstellenscans, CVE-Bewertung, definierte Patchfristen nach Kritikalität, Emergency Patching und EOL/EOS-Management werden durchgeführt.

10. **(2.7.3) Change-Management & Enablement:**

Für Changes ist eine Security-Impact- und Risikoanalyse sowie für Emergency Changes eine nachgelagerte Prüfung und Dokumentation verpflichtend.

11. **(2.7.5) Release Management, Qualitätssicherung:**

Vor Releases sind Security-Tests, Vulnerability Scans und Freigabekriterien verpflichtend.

12. **(2.7.3) Change-Management & Enablement und (2.7.5) Release Management:**

Die Anforderungen gelten analog für Änderungen an Unterauftragnehmern, Hosting-Standorten, Sicherheitskomponenten und wesentlichen Cloud-Services.

13. **(2.7.6) IT Service Continuity Management:**

Der AN hat in seinen Systemen BCM/Disaster Recovery, RTO/RPO, Backup/Restore, Failover und regelmäßige Wiederherstellungstests implementiert.

14. **(2.8) Reporting:**

Der AN verpflichtet sich Reports von Security Incidents, offenen Schwachstellen, Patchstatus, Backup-/Restore Ergebnissen, Verfügbarkeit, Major Incidents und SLA Verletzungen monatlich zur Verfügung zu stellen.

Kritische Abweichungen von üblichen operativen Security Kennzahlen müssen unverzüglich an den AG gemeldet werden.