Security Baseline Assessment – Beispiel Software GmbH

BEISPIELBERICHT · Beispieldaten · Version 1.0
Pommer Cyber Advisory · Benjamin Pommer

Aufbau: 1 Management Summary, 2 Scope und Vorgehen, 3 Von den Scan-Ergebnissen zum Bericht, 4 Befunde, 5 Remediation-Roadmap, 6 NIS-2-Orientierung, 7 Limitationen, 8 Nachprüfung nach 6 Wochen (auf Wunsch). Anhang: A Befundliste, B Akzeptierte Risiken, C Glossar.

Ausgangslage: Die Beispiel Software GmbH entwickelt eine B2B-Software für Tourenplanung (50 Beschäftigte, davon 12 in der Entwicklung). Sie betreibt drei AWS-Accounts (Produktion, Staging, Shared Services) in `eu-central-1` und `eu-west-1`: einen EKS-Cluster mit Microservices, EC2-Instanzen für Batch-Läufe und einen Zugangsrechner, rund 60 Lambda-Funktionen, Step Functions für die Abrechnung, RDS PostgreSQL, S3, API Gateway mit CloudFront und WAF. Gebaut und ausgerollt wird mit Terraform und GitHub Actions (vier Repositories).

1. Management Summary

Gesamtbild: Solide Basis mit gefährlichen Einzelfällen. Von 3.412 automatisch bewerteten Prüfungen sind 2.890 bestanden (84,7 %), 522 nicht: **3 kritisch, 41 hoch, 297 mittel, 181 niedrig**. 64 Prüfungen lassen sich nur manuell bewerten.

Schwere	Anzahl nicht bestandener Prüfungen
Kritisch	3
Hoch	41
Mittel	297
Niedrig	181

- **Drei kritische Befunde, alle über Nacht behebbar:** ein öffentlich lesbarer S3-Bucket mit Kundenexporten (F-01), ein Root-Konto ohne MFA (F-02) und eine öffentlich erreichbare Staging-Datenbank (F-03). Dazu in den Repositories ein aktiver Zugriffsschlüssel in einer Konfigurationsdatei (F-09).
- **Hauptthema Identitäten und Angriffsfläche:** zu weite Rollen, fehlender zweiter Faktor, öffentliche Endpunkte (Kubernetes-API, SSH, Function-URLs). Erkennung und Protokollierung sind lückenhaft (GuardDuty in drei Account-/Regionskombinationen nicht aktiv, fehlende Flow Logs und Log-Aufbewahrung).

- **Quick Wins (unter 1 Tag je Punkt):** Block Public Access aktivieren · Root-MFA einrichten · Staging-Datenbank privat schalten · Schlüssel im Repository widerrufen · SSH aus dem Internet schließen · IMDSv2 erzwingen.
- **Orientierung NIS-2:** siehe Kapitel 6 (Zuordnung, keine Rechtsbewertung).

2. Scope und Vorgehen

- **Geprüft:** 3 AWS-Accounts (Kennungen im Kundenbericht, hier nicht dargestellt), Regionen `eu-central-1` und `eu-west-1`; 4 Repositories (Terraform, Helm-Charts, Dockerfiles, GitHub-Actions-Workflows; 311 Dateien).
- **Vorgehen:** automatisierte Prüfung der Cloud-Konfiguration (anerkannte Härtungsempfehlungen, CIS, ISO 27001, NIS-2-Zuordnung) und der Repositories (Fehlkonfigurationen, Schwachstellen, Secrets im Arbeitsbaum). Danach manuelle Auswertung und Gegenprobe an den Stellen, die automatische Prüfungen schlecht sehen: Root-Konto, Admin-Rollen, Vertrauensbeziehungen, Netzwerkfreigaben, CI/CD-Rechte (Kapitel 3).
- **Zugriff:** lesend (AWS-Managed-Policies SecurityAudit und ViewOnlyAccess, Lesetoken für die Repositories), kein Zugriff auf Dateninhalte, zeitlich befristet.
- **Ablauf:** Tag 0 Onboarding und Zugang, Tag 1 automatisierte Läufe (rund 38 Minuten für 3 Accounts in 2 Regionen, 4 Minuten für die Repositories), Tag 2 bis 3 Auswertung, Tag 4 Bericht, Tag 5 Debriefing von 60 Minuten mit Geschäftsführung und technischer Leitung.
- **Einordnung:** Automatisierte Prüfungen sind ein Raster, kein Urteil. Jeder Befund wurde auf Relevanz für die Umgebung eingeordnet.

3. Von den Scan-Ergebnissen zum Bericht

Einen Scan kann jeder starten, er liefert Tausende Zeilen. Dieser Bericht beantwortet, was davon zählt, in welcher Reihenfolge es behoben wird und mit welchem Aufwand. Aus **522 Einzeltreffern** in der Cloud-Konfiguration und **102** in den Repositories wurden **10 Befunde** und **8 Maßnahmen**.

Schritt	Scan-Ausgabe	Ergebnis im Bericht
Bündeln	522 Einzeltreffer, je Ressource eine Zeile	10 Befunde mit Anzahl als Beleg, z. B. „17 S3-Buckets ohne Zugriffsprotokoll“ ist ein Befund
Einordnen	Schwere nach Werkzeug, ohne Kenntnis der Umgebung	Gewichtung nach Inhalt und Erreichbarkeit: die Staging-Datenbank enthält eine Produktionskopie und bleibt kritisch, derselbe Treffer bei einer leeren Test-Datenbank wäre nachrangig; 2 Test-Buckets ohne Daten sind nicht priorisiert; 6 bewusste Ausnahmen mit dem Kunden geklärt (Anhang B)

Schritt	Scan-Ausgabe	Ergebnis im Bericht
Gegenprobe von Hand	nicht enthalten	4 Punkte, die die automatische Prüfung nicht meldet: `pull_request_target` mit Code aus Pull Requests, Runner mit Administrator-Rolle, fehlender Branch-Schutz, Vertrauensbeziehung zweier Rollen zu einem fremden Account ohne Bedingung (F-06, F-09)
Zusammenhänge	jeder Treffer einzeln	Angriffspfad: öffentliche Function-URL (F-07), Rolle mit Rechteausweitung (F-06) und Instanzrolle über IMDSv1 (F-05) ergeben zusammen einen Weg vom Internet zum Administrator; Priorität 1 folgt der Wirkung, nicht der Schwere des Einzeltreffers
Aufwand und Reihenfolge	keine Angabe	8 Maßnahmen mit Aufwand (0,5 bis 6 Tage) und Zeitrahmen, Quick Wins zuerst (Kapitel 5)
Übersetzen	Tabellen und Prüfnummern	Management Summary für die Geschäftsleitung, NIS-2-Zuordnung (Kapitel 6), Debriefing von 60 Minuten mit Fragen und Entscheidungen

4. Befunde

F-01 · Öffentlich lesbarer S3-Bucket mit Kundenexporten · Schwere: kritisch

- **Betroffen:** 1 Bucket in der Produktion, 2 Accounts ohne Block Public Access auf Kontoebene.
- **Einordnung:** Kritisch, weil die Dateien Kundendaten enthalten und der Bucket ohne Anmeldung lesbar ist. Derselbe Treffer bei einem Bucket mit öffentlichen Webseiten-Dateien wäre unkritisch.
- **Auswirkung:** Exportdateien mit Kundendaten sind ohne Anmeldung abrufbar. Ob Zugriffe stattgefunden haben, lässt sich nur über Zugriffsprotokolle klären.
- **Empfehlung:** Block Public Access auf Konto- und Bucket-Ebene, Zugriff nur noch über signierte, kurzlebige Links; Zugriffe der letzten 90 Tage über CloudTrail-Datenereignisse und S3-Protokolle auswerten. Die rechtliche Prüfung einer Meldepflicht ist nicht Teil dieser Prüfung und liegt beim Verantwortlichen.
- **Aufwand:** 0,5 Tage, sofort.

F-02 · Identitäten: Root ohne MFA, Benutzer ohne zweiten Faktor, alte Schlüssel · Schwere: kritisch

- **Betroffen:** Root-Konto im Shared-Services-Account ohne MFA; 4 Benutzer ohne MFA für die Konsole; 5 Zugriffsschlüssel älter als 90 Tage und 4 länger als 45 Tage ungenutzt; Passwortrichtlinie in 2 Accounts unter 14 Zeichen.
- **Auswirkung:** Ein gestohlenes Passwort oder ein alter Schlüssel genügt für Zugriff auf das Konto; beim Root-Konto gibt es keine Einschränkung.
- **Empfehlung:** MFA für Root und alle Benutzer, Schlüssel rotieren oder entfernen, mittelfristig Anmeldung über IAM Identity Center statt dauerhafter Benutzer.

- **Aufwand:** 1 Tag.

F-03 · Staging-Datenbank öffentlich erreichbar · Schwere: kritisch

- **Betroffen:** 1 RDS-Instanz im Staging-Account, nach Aussage des Teams mit einer Kopie von Produktionsdaten befüllt.
- **Auswirkung:** Die Datenbank ist aus dem Internet erreichbar; ein schwaches Passwort oder eine Lücke genügt für einen Datenabfluss.
- **Empfehlung:** Öffentlichen Zugriff abschalten, Zugriff nur über Bastion oder SSM-Tunnel, Testdaten maskieren oder synthetisch erzeugen.
- **Aufwand:** 0,5 Tage plus Konzept für Testdaten.

F-04 · EKS: öffentlicher API-Endpunkt, unvollständiges Logging, Secrets ohne KMS-Verschlüsselung · Schwere: hoch

- **Betroffen:** 2 Cluster-Endpunkte offen für `0.0.0.0/0`; Control-Plane-Logging nicht für alle Typen aktiv (2 Cluster); Kubernetes-Secrets nicht mit einem KMS-Schlüssel verschlüsselt (2 Cluster).
- **Auswirkung:** Die Verwaltungsschnittstelle des Clusters ist aus dem Internet erreichbar; Audit-Spuren fehlen.
- **Empfehlung:** Endpunkt auf eigene Netze oder privat beschränken, alle Log-Typen aktivieren, Secrets-Verschlüsselung mit KMS. Die Konfiguration **innerhalb** des Clusters (RBAC, Pod-Sicherheit, Netzwerkrichtlinien) ist nicht Teil des Festpreis-Umfangs (siehe Kapitel 7).
- **Aufwand:** 1,5 Tage.

F-05 · EC2: SSH aus dem Internet, IMDSv1, unverschlüsselte Volumes, Patching · Schwere: hoch

- **Betroffen:** 2 Security Groups mit SSH für `0.0.0.0/0`; 14 Instanzen akzeptieren IMDSv1; 6 unverschlüsselte EBS-Volumes; 3 Instanzen nicht patch-konform und 6 nicht per Systems Manager verwaltet; 5 Instanzen mit öffentlicher IP, 11 älter als das festgelegte Höchstalter.
- **Auswirkung:** IMDSv1 erleichtert den Diebstahl von Instanz-Rollen über Anwendungslücken (SSRF); offener SSH-Zugang ist ein Dauerziel.
- **Empfehlung:** SSH schließen und durch Systems Manager Session Manager ersetzen, IMDSv2 erzwingen (Launch-Template), EBS-Standardverschlüsselung aktivieren, Patch-Baselines verbindlich machen.
- **Aufwand:** 2,5 Tage.

F-06 · IAM: Rechteausweitung, zu weite Rollen, offene Vertrauensbeziehungen · Schwere: hoch

- **Betroffen:** 3 kundenverwaltete Richtlinien erlauben Rechteausweitung, darunter die Rollen mehrerer Lambda-Funktionen und der Step-Functions-Abrechnung; 3 Benutzer mit direkt angehängten Richtlinien; IAM Access Analyzer in 6 Account-/Regionskombinationen nicht aktiv. **Bei der manuellen Gegenprobe zusätzlich:** 2 Rollen vertrauen einem fremden Account ohne Bedingung (ohne External ID).
- **Auswirkung:** Wer eine dieser Funktionen kompromittiert, kann sich weitere Rechte verschaffen (Richtlinien anhängen, Rollen übernehmen) und Daten abgreifen oder Protokolle verändern.

- **Empfehlung:** Wildcards in `Action` und `Resource` entfernen, `iam:PassRole` auf konkrete Rollen und Dienste begrenzen, Permission Boundaries für alle von der Pipeline erzeugten Rollen, Vertrauensrichtlinien mit External ID, Access Analyzer aktivieren.
- **Aufwand:** 3 Tage.

F-07 · Lambda: öffentliche Function-URLs und veraltete Laufzeiten · Schwere: hoch

- **Betroffen:** 2 Funktionen mit öffentlicher Function-URL, 9 Funktionen mit nicht mehr unterstützter Laufzeit.
- **Auswirkung:** Öffentliche URLs sind ohne Authentifizierung aufrufbar; veraltete Laufzeiten erhalten keine Sicherheitsupdates.
- **Empfehlung:** Authentifizierung (IAM oder API Gateway mit Autorisierung) verlangen, Laufzeiten aktualisieren und in die Pipeline eine Versionsprüfung aufnehmen.
- **Aufwand:** 2 Tage.

F-08 · Erkennung und Protokollierung (NIS-2-relevant) · Schwere: mittel, teils hoch

- **Betroffen:** GuardDuty in 3 Account-/Regionskombinationen nicht aktiv (hoch); CloudTrail ohne Prüfsummen (2); AWS Config unvollständig (4); Step-Functions-Logging fehlt (7 Zustandsmaschinen); VPC-Flow-Logs fehlen (8); Zugriffsprotokolle fehlen bei 17 S3-Buckets, 3 CloudFront-Distributionen, 2 WAF-ACLs, 3 API-Gateway-Stages, 4 Load Balancern; 36 CloudWatch-Log-Gruppen ohne Aufbewahrungsfrist.
- **Auswirkung:** Fehlende Spuren erschweren Angriffserkennung, Forensik und Nachweispflichten; Meldefristen (24 Stunden, 72 Stunden) sind ohne belastbare Protokolle schwer einzuhalten.
- **Empfehlung:** GuardDuty und Config in allen genutzten Regionen, zentrales Log-Archiv in einem eigenen Account mit Objektsperre, Aufbewahrung festlegen (z. B. 12 Monate), Alarme auf Auffälligkeiten.
- **Aufwand:** 2 Tage.

F-09 · CI/CD, Repositories und Container · Schwere: hoch

- **Betroffen (automatische Prüfung, 4 Repositories, 311 Dateien):** 1 aktiver AWS-Zugriffsschlüssel in `charts/platform/values-staging.yaml` (kritisch, im Arbeitsbaum), 12 Fehlkonfigurationen mit hoher Schwere (u. a. Container als Root, ungesetzte Ressourcenlimits), 31 mittel, 58 niedrig. **Manuelle Gegenprobe:** 31 GitHub-Actions-Verwendungen ohne feste Version, 1 Workflow mit `pull_request_target`, der Code aus Pull Requests auscheckt, ein selbst gehosteter Runner mit Administrator-Rolle, fehlender Branch-Schutz in 2 Repositories. **Container-Registry:** 12 Repositories mit bekannten Schwachstellen im neuesten Image, 11 ohne Lifecycle-Regel.
- **Auswirkung:** Ein Schlüssel im Repository ist für jeden mit Lesezugriff nutzbar; `pull_request_target` mit Code-Checkout ermöglicht Fremdcode im Kontext der Pipeline; ein Runner mit Administrator-Rolle macht jeden Workflow zum Admin.
- **Empfehlung:** Schlüssel sofort widerrufen und durch OIDC-Rollen ersetzen (Secret-Scanning und Push-Schutz aktivieren, den Verlauf des Repositories gesondert prüfen), Actions auf Commit-Hashes

festlegen, `pull_request_target` entfernen oder isolieren, Runner-Rechte begrenzen, Branch-Schutz mit Pflicht-Reviews, Basis-Images aktualisieren.

- **Aufwand:** 3 Tage.

F-10 · Weitere Härtung nach Schutzbedarf · Schwere: mittel und niedrig

- **Betroffen (Auswahl, Details in Anhang A):** 64 CloudWatch-Log-Gruppen ohne KMS-Verschlüsselung und 21 S3-Buckets nur mit SSE-S3; 19 S3-Buckets ohne MFA-Delete, 14 ohne Transportverschlüsselungs-Pflicht; 9 SQS-Warteschlangen ohne serverseitige Verschlüsselung, 9 DynamoDB-Tabellen ohne Point-in-Time-Recovery und 1 RDS-Instanz ohne Backup; 4 Web-Endpunkte ohne WAF; 52 Lambda-Funktionen außerhalb eines VPC; 19 EC2-Instanzen ohne detaillierte Überwachung; 15 ungenutzte Security Groups, 6 ungenutzte Netzwerk-ACLs.
- **Einordnung:** Nicht bei jeder Umgebung sinnvoll. Für personenbezogene Daten und Kundenexporte kundenverwaltete Schlüssel erwägen; für Logs und unkritische Daten reichen AWS-verwaltete. Entscheidung nach Schutzbedarf und Kosten (siehe Anhang B für akzeptierte Punkte).
- **Aufwand:** 4 bis 6 Tage je nach Schutzbedarfsklassifizierung.

5. Remediation-Roadmap

Prio	Maßnahme	Befunde	Aufwand	Zeitrahmen
1	Öffentliche Exponierung beenden: S3-Bucket, Staging-Datenbank, EKS-API, SSH, Function-URLs	F-01, F-03, F-04, F-05, F-07	2 Tage	unter 1 Woche
2	Identitäten sichern: Root-MFA, Benutzer-MFA, Schlüssel rotieren, Schlüssel im Repository widerrufen	F-02, F-09	1 Tag	unter 1 Woche
3	Rechte straffen: Eskalationspfade, Lambda- und Step-Functions-Rollen, Permission Boundaries	F-06	3 Tage	unter 30 Tagen
4	EC2 und EKS härten: IMDSv2, EBS-Verschlüsselung, Patching, EKS-Logging	F-04, F-05	2,5 Tage	unter 30 Tagen
5	Erkennung und Protokollierung: GuardDuty, Config, Flow Logs, zentrales Archiv, Alarme	F-08	2 Tage	unter 30 Tagen
6	CI/CD härten: Actions pinnen, `pull_request_target`, Runner-Rechte, Branch-Schutz	F-09	3 Tage	unter 30 Tagen
7	Laufzeiten und Abhängigkeiten aktualisieren, Container-Images neu bauen	F-07, F-09	3 Tage	unter 60 Tagen
8	Schlüsselhoheit, Backup und weitere Härtung nach Schutzbedarf	F-10	4 bis 6 Tage	unter 90 Tagen

6. NIS-2-Orientierung nach § 30 Abs. 2 BSIG

Orientierung, keine Rechtsberatung oder Zertifizierung. Die Tabelle ordnet die technischen Befunde den zehn Mindestbereichen für Risikomanagementmaßnahmen zu (§ 30 Abs. 2 BSIG, NIS-2 Art. 21). Sie zeigt, wo dieser Bericht technische Belege liefert und wo nicht. Organisation, Richtlinien und Schulung sind nicht Gegenstand der Prüfung.

Nr.	Bereich nach § 30 Abs. 2 BSIG	Technische Befunde	Abdeckung durch diese Prüfung
1	Risikoanalyse und Sicherheitskonzepte	–	nicht bewertet (organisatorisch)
2	Bewältigung von Sicherheitsvorfällen	F-08 (Protokollierung, Erkennung)	teilweise (nur technische Voraussetzungen)
3	Betriebskontinuität: Backup, Notfallwiederherstellung	F-10 (Backup, Versionierung)	teilweise (nur technische Voraussetzungen)
4	Sicherheit der Lieferkette	F-09 (Abhängigkeiten, Images, Pipelines)	teilweise (nur technische Lieferkette im Scope)
5	Sicherheit bei Erwerb, Entwicklung und Wartung, Umgang mit Schwachstellen	F-07, F-09	technisch geprüft im Scope
6	Bewertung der Wirksamkeit der Maßnahmen	–	nicht bewertet (Momentaufnahme)
7	Cyberhygiene und Schulungen	–	nicht bewertet (Schulung nicht Gegenstand)
8	Konzepte und Verfahren für Kryptografie	F-04, F-10 (Verschlüsselung)	technisch geprüft im Scope
9	Personalsicherheit, Zugriffskontrolle, Verwaltung von IT-Systemen	F-02, F-06	technisch geprüft im Scope
10	Mehr-Faktor-Authentifizierung und gesicherte Kommunikation	F-02, F-03	technisch geprüft im Scope

„Technisch geprüft“ heißt nur, dass der vereinbarte Scope auf dieses Thema untersucht wurde. Es ist keine Aussage darüber, ob eine gesetzliche Pflicht erfüllt ist.

7. Limitationen

- Die Analyse ist eine Momentaufnahme zum Prüfzeitpunkt, sie ist nicht vollständig und schließt weitere Schwachstellen nicht aus.

- Geprüft wurde ausschließlich der vereinbarte Scope (3 Accounts, 4 Repositories) mit lesendem Zugriff; 64 Prüfungen lassen sich nur manuell bewerten.
- **Nicht Teil des Festpreis-Umfangs:** die Konfiguration innerhalb der Kubernetes-Cluster (RBAC, Pod-Sicherheit, Netzwerkrichtlinien), Penetrationstests, eine Bewertung der Anwendungen selbst und organisatorische Maßnahmen. Diese lassen sich als Zusatzleistung vereinbaren.

8. Nachprüfung nach 6 Wochen (auf Wunsch)

Eine Nachprüfung sechs Wochen nach dem Bericht ist **auf Wunsch** möglich und nicht im Festpreis enthalten. Sie wiederholt dieselben Läufe im selben Scope und vergleicht mit dem Bericht.

8.1 Ergebnis

- **Gesamtbild:** Von 3.398 automatisch bewerteten Prüfungen sind 3.187 bestanden (93,8 %), 211 nicht: **0 kritisch, 4 hoch, 96 mittel, 111 niedrig** (vorher 84,7 % und 522). Die Zahl der bewerteten Prüfungen ist gesunken, weil Ressourcen stillgelegt wurden (u. a. ungenutzte Security Groups, zwei Test-Buckets).
- **Alle drei kritischen Befunde und der Schlüssel im Repository sind behoben.** Der Bucket ist nicht mehr öffentlich, das Root-Konto hat MFA, die Staging-Datenbank ist nur noch privat erreichbar, der Schlüssel wurde widerrufen und durch eine OIDC-Rolle ersetzt.
- **Offene hohe Befunde (4):** 3 sind mit Begründung als akzeptiert dokumentiert (Anhang B), 1 ist in Umsetzung (Patch-Konformität einer Altinstanz, Frist in 4 Wochen).
- **Repositories:** 0 kritisch, 3 hoch, 19 mittel, 52 niedrig (vorher 1, 12, 31, 58).

Schwere	Bericht	Nachprüfung
Kritisch	3	0
Hoch	41	4
Mittel	297	96
Niedrig	181	111
Bestanden	84,7 %	93,8 %

8.2 Status der Roadmap

Prio	Maßnahme	Status	Anmerkung
1	Öffentliche Exponierung beenden	erledigt	alle fünf Punkte geschlossen
2	Identitäten sichern	erledigt	Root-MFA, Benutzer-MFA, Schlüsselrotation; Schlüssel im Repository ersetzt

Prio	Maßnahme	Status	Anmerkung
3	Rechte straffen	teilweise	2 von 3 Richtlinien bereinigt; 1 akzeptiert (Anhang B, B-1)
4	EC2 und EKS härten	teilweise	EBS, EKS und SSH erledigt; 2 Altinstanzen mit IMDSv1 akzeptiert (B-2); Patching in Umsetzung
5	Erkennung und Protokollierung	teilweise	GuardDuty, Config, zentrales Log-Archiv mit Objektsperre und Alarme erledigt; Zugriffsprotokolle bei 4 Buckets und Flow Logs in 2 VPCs offen
6	CI/CD härten	erledigt	Actions auf Commit-Hashes, Runner-Rechte begrenzt, Branch-Schutz aktiv
7	Laufzeiten und Abhängigkeiten	teilweise	6 von 9 Laufzeiten aktualisiert, 7 Images mit bekannten Schwachstellen offen
8	Weitere Härtung nach Schutzbedarf	offen	Entscheidung zur Schlüsselhoheit steht aus

8.3 Offene Punkte

- Patch-Konformität der Altinstanz (Frist in 4 Wochen) und Ablösung der zwei Batch-Instanzen mit IMDSv1 (Frist in 2 Monaten).
- Entscheidung zu kundenverwalteten Schlüsseln für Kundenexporte und Datenbanken (Schutzbedarf klassifizieren).
- Bei Bedarf: Prüfung der Konfiguration innerhalb des Clusters (nicht im Festpreis enthalten) und eine weitere Nachprüfung nach Umsetzung der Punkte aus Anhang B.

Anhang

A. Befundliste (aggregiert)

Alle nicht bestandenen automatischen Prüfungen der Cloud-Konfiguration, nach Schwere sortiert. „Bericht“ und „Nach“ (Nachprüfung) = betroffene Ressourcen im Bericht und nach 6 Wochen. Die Einzelliste je Ressource (CSV) wird im Kundenbericht gesondert und verschlüsselt übergeben.

Schwere	Prüfung	Bericht	Nach	Befund
kritisch	Root-Konto ohne MFA	1	0	F-02
kritisch	Datenbank-Instanz aus dem Internet erreichbar	1	0	F-03
kritisch	S3-Bucket öffentlich lesbar	1	0	F-01
hoch	EC2-Instanz erlaubt noch IMDSv1	14	2	F-05
hoch	EBS-Volume nicht verschlüsselt	6	0	F-05
hoch	Benutzer mit Konsolenzugang ohne MFA	4	0	F-02
hoch	GuardDuty nicht aktiv	3	0	F-08
hoch	Richtlinie ermöglicht Rechteausweitung	3	1	F-06
hoch	Instanz nicht patch-konform	3	1	F-05
hoch	Lambda-Function-URL öffentlich erreichbar	2	0	F-07
hoch	SSH (Port 22) aus dem Internet erlaubt	2	0	F-05
hoch	Kubernetes-API-Endpunkt öffentlich	2	0	F-04
hoch	Block Public Access auf Kontoebene fehlt	2	0	F-01
mittel	Log-Gruppe ohne KMS-Verschlüsselung	64	30	F-10
mittel	Log-Gruppe ohne Aufbewahrungsfrist	36	0	F-08
mittel	S3-Bucket nur mit SSE-S3 statt KMS verschlüsselt	21	21	F-10
mittel	S3-Bucket ohne MFA-Delete	19	19	F-10
mittel	S3-Bucket ohne Zugriffsprotokoll	17	4	F-08
mittel	S3-Bucket erlaubt unverschlüsselten Transport	14	3	F-10

Schwere	Prüfung	Bericht	Nach	Befund
mittel	Container-Image mit bekannten Schwachstellen	12	7	F-09
mittel	EC2-Instanz älter als das festgelegte Höchstalter	11	3	F-05
mittel	Lambda-Funktion mit nicht mehr unterstützter Laufzeit	9	3	F-07
mittel	DynamoDB-Tabelle ohne Point-in-Time-Recovery	9	1	F-10
mittel	SQS-Warteschlange ohne Verschlüsselung	9	0	F-10
mittel	VPC ohne Flow Logs	8	2	F-08
mittel	Step-Functions-Zustandsmaschine ohne Logging	7	0	F-08
mittel	EC2-Instanz nicht über Systems Manager verwaltet	6	0	F-05
mittel	S3-Bucket ohne Versionierung	6	0	F-10
mittel	EC2-Instanz mit öffentlicher IP-Adresse	5	0	F-05
mittel	Zugriffsschlüssel älter als 90 Tage	5	0	F-02
mittel	AWS Config nicht vollständig aktiv	4	0	F-08
mittel	Load Balancer ohne Zugriffsprotokoll	4	0	F-08
mittel	Zugriffsschlüssel seit über 45 Tagen ungenutzt	4	0	F-02
mittel	Kontaktdaten des Accounts nicht aktuell	3	2	F-10
mittel	API-Gateway-Stage ohne Logging	3	0	F-08
mittel	CloudFront-Distribution ohne Logging	3	0	F-08
mittel	API-Gateway-Stage ohne WAF	2	0	F-10
mittel	CloudTrail ohne Prüfsummen der Logdateien	2	0	F-08
mittel	Kubernetes-Secrets nicht mit KMS verschlüsselt	2	0	F-04
mittel	Kubernetes-Control-Plane-Logging unvollständig	2	0	F-04
mittel	Load Balancer mit veralteter TLS-Richtlinie	2	0	F-10
mittel	Load Balancer ohne WAF	2	0	F-10
mittel	Passwortrichtlinie unter 14 Zeichen	2	0	F-02

Schwere	Prüfung	Bericht	Nach	Befund
mittel	WAF ohne Logging	2	0	F-08
mittel	Datenbank-Instanz ohne Backup	1	0	F-10
mittel	Datenbank-Instanz ohne Multi-AZ	1	1	F-10
niedrig	Lambda-Funktion außerhalb eines VPC	52	52	F-10
niedrig	Lambda-Aufrufe nicht in CloudTrail protokolliert	52	13	F-10
niedrig	EC2-Instanz ohne detaillierte Überwachung	19	19	F-10
niedrig	Ungenutzte Security Group	15	6	F-10
niedrig	Container-Registry ohne Lifecycle-Regel	11	0	F-09
niedrig	IAM Access Analyzer nicht aktiv	6	0	F-06
niedrig	Ungenutzte Netzwerk-ACL	6	6	F-10
niedrig	CloudFront ohne Verschlüsselung auf Feldebene	3	3	F-10
niedrig	CloudTrail ohne Insights	3	3	F-08
niedrig	CloudTrail ohne Lese-Ereignisse für S3-Objekte	3	3	F-08
niedrig	Kein SAML-Anbieter für zentrale Anmeldung	3	3	F-10
niedrig	Benutzer mit direkt angehängter Richtlinie	3	0	F-06
niedrig	Keine Rolle für den AWS-Support	3	3	F-10
niedrig	Kein zentraler Backup-Plan	2	0	F-10
Summe		**522**	**211**	

B. Akzeptierte Risiken und Abweichungen

Einträge der Nachprüfung. Im Kundenbericht dokumentiert diese Tabelle die mit dem Kunden abgestimmten Ausnahmen inklusive Entscheider und Datum.

Nr.	Befund	Entscheidung	Begründung und Kompensation	Überprüfung
B-1	F-06 · Richtlinie ermöglicht Rechteausweitung (1)	akzeptiert	Deploy-Rolle der Pipeline benötigt IAM-Rechte; Kompensation: OIDC nur vom geschützten Hauptzweig, MFA für Menschen, Alarm bei Richtlinienänderungen, Permission Boundary geplant	in 3 Monaten
B-2	F-05 · EC2-Instanz erlaubt noch IMDSv1 (2)	akzeptiert	Zwei Altinstanzen des Batch-Betriebs benötigen IMDSv1 bis zur Ablösung; keine Internet-Erreichbarkeit, minimale Instanzrolle	in 2 Monaten
B-3	F-10 · Datenbank-Instanz ohne Multi-AZ (1)	akzeptiert	Staging bewusst ohne Multi-AZ (Kosten)	jährlich
B-4	F-10 · S3-Bucket ohne MFA-Delete (19)	akzeptiert	Versionierung und Objektsperre genügen; MFA-Delete erfordert Root-Zugang	jährlich
B-5	F-10 · S3-Bucket nur mit SSE-S3 statt KMS verschlüsselt (21)	akzeptiert	SSE-S3 für Buckets ohne personenbezogene Daten; Kundenexporte folgen mit Schlüsselentscheidung	bei Entscheidung
B-6	F-10 · Lambda-Funktion außerhalb eines VPC (52)	akzeptiert	Funktionen ohne Zugriff auf VPC-Ressourcen; Kompensation: eng gefasste Rollen	bei Architekturänderung

C. Glossar

- **IAM** – Identity and Access Management: Benutzer, Rollen und Berechtigungen in der Cloud.
- **MFA** – Zweiter Faktor bei der Anmeldung; schützt vor Passwortdiebstahl.
- **IMDSv2** – Gesicherte Abfrage der Instanz-Metadaten (und damit der Instanz-Rolle) auf EC2; IMDSv1 ist bei Anwendungslücken (SSRF) leichter auszunutzen.
- **EKS** – Verwaltetes Kubernetes in AWS; geprüft wird die AWS-Seite (Endpunkt, Logging, Verschlüsselung), nicht der Inhalt des Clusters.
- **Privilegien-Eskalation** – Ein Konto mit begrenzten Rechten verschafft sich höhere Rechte (z. B. über `iam:PassRole` oder das Ändern von Richtlinien).
- **Least Privilege / Permission Boundary** – Jedes Konto bekommt nur die nötigen Rechte; Boundaries setzen Obergrenzen.

- **KMS / Customer-Managed Key** – Schlüsseldienst für Verschlüsselung; bei eigenen Schlüsseln liegen Rotation, Zugriff und Widerruf beim Kunden.
- **GuardDuty / CloudTrail / Config** – Erkennung von Auffälligkeiten, Protokoll der API-Aufrufe und Aufzeichnung der Konfiguration.
- **WAF** – Web Application Firewall: filtert und begrenzt Anfragen an Webanwendungen.
- **OIDC (GitHub Actions)** – Anmeldung der Pipeline mit kurzlebigen Rollen statt dauerhaften Zugriffsschlüsseln.
- **IaC (Terraform)** – Infrastruktur als Code: Cloud-Ressourcen werden per Code beschrieben und versioniert.
- **CIS Benchmarks** – Anerkannte Härtungsempfehlungen des Center for Internet Security.
- **NIS-2** – EU-Richtlinie zur Cybersicherheit; verlangt u. a. Risikomanagement, Protokollierung und Meldeprozesse.
- **Momentaufnahme** – Der Bericht beschreibt den Zustand zum Prüfzeitpunkt; spätere Änderungen sind nicht erfasst.