Eskalationsprotokoll für Sicherheitsvorfälle

1. Zweck

Dieses Eskalationsprotokoll definiert die Verfahren und Verantwortlichkeiten für die Eskalation von Sicherheitsvorfällen in unserem Unternehmen, um eine schnelle und effektive Reaktion zu gewährleisten.

2. Vorfallskategorien

Vorfälle werden in folgende Kategorien eingeteilt:

- Kritisch (K): Unmittelbare, schwerwiegende Auswirkungen auf Geschäftsbetrieb oder sensible Kundendaten (z.B. Aufzeichnungen von Kundengesprächen, Transkripte, E-Mails oder Namen der Kundenkunden)
- Hoch (H): Erhebliche Auswirkungen auf Cloud-Dienste oder Datenschutz, aber kein vollständiger Systemausfall
- Mittel (M): Begrenzte Auswirkungen auf nicht-kritische Systeme, die behoben werden müssen
- Niedrig (N): Minimale Auswirkungen, keine unmittelbare Gefahr für sensible Daten oder Systeme

3. Eskalationsstufen

- Stufe 1: Entwicklerteam (Erstreaktion)
- Stufe 2: CTO / Datenschutzbeauftragter
- Stufe 3: Geschäftsführung
- Stufe 4: Externe Parteien (Kunden, Behörden)

4. Eskalationsmatrix

Vorfallskategorie	Initiale Eskalation	Zeit bis zur Eskalation	Benachrichtigung des Kunden
Kritisch (K)	Stufe 2	Sofort	Innerhalb von 4 Stunden
Hoch (H)	Stufe 1	Innerhalb von 1 Stunde	Innerhalb von 24 Stunden

Mittel (M)	Stufe 1	Innerhalb von 4 Stunden	Innerhalb von 48 Stunden
Niedrig (N)	Stufe 1	Innerhalb von 24 Stunden	Nach Ermessen

5. Eskalationsverfahren

1. Vorfallserkennung und -meldung
    - Mitarbeiter meldet Vorfall an das Entwicklerteam
    - Entwicklerteam kategorisiert den Vorfall
2. Initiale Bewertung und Eskalation
    - Entwicklerteam eskaliert gemäß Matrix
    - Bei Unsicherheit immer zur höheren Stufe (CTO) eskalieren
3. Untersuchung und Behandlung
    - Zuständige Stufe untersucht und behandelt den Vorfall
    - Regelmäßige Updates an CTO
4. Weitere Eskalation (falls erforderlich)
    - Bei Überschreitung definierter Schwellenwerte oder Zeitrahmen
    - Bei Erkennung größerer Auswirkungen als initial angenommen
5. Kundenbenachrichtigung
    - Gemäß Matrix und unter Berücksichtigung der DSGVO
    - Durch CTO oder designierten Kommunikationsverantwortlichen
6. Abschluss und Nachbereitung
    - Dokumentation des Vorfalls und der ergriffenen Maßnahmen
    - Lessons Learned und Aktualisierung des Eskalationsprotokolls bei Bedarf

6. Kontaktinformationen

- Entwicklerteam: dev-admin@kickscale.com
- CTO / Datenschutzbeauftragter: fabian.riedlsperger@kickscale.com
- Geschäftsführung: gerald.zankl@kickscale.com

7. Spezifische Richtlinien

- Cloud-Dienste: Bei Vorfällen, die Google Cloud-Dienste betreffen, ist der CTO unverzüglich zu informieren.
- DSGVO-Konformität: Alle Maßnahmen müssen DSGVO-konform sein. Bei Datenschutzverletzungen ist der Datenschutzbeauftragte (CTO) sofort einzubeziehen.
- Sensible Daten: Besondere Vorsicht bei Vorfällen, die Aufzeichnungen von Kundengesprächen, Transkripte, E-Mails oder Namen der Kundenkunden betreffen.

8. Aktualisierung und Überprüfung

Dieses Protokoll wird vierteljährlich vom CTO überprüft und bei Bedarf aktualisiert.

Letzte Aktualisierung: 22.07.2024