

Schutzbedarfsanalyse Kino-Projekt (initial)

(sollte nach der nächsten Entwicklungsphase erneut durchgeführt werden da Daten und Funktionen noch nicht genau definiert sind)

Schadensszenario	Schutzbedarf	Begründung & Einschätzung
Beeinträchtigung der persönlichen Unversehrtheit	Normal	<p>Begründung: Ein Ausfall oder Hack der Website führt nicht direkt zu physischen Personenschäden.</p> <p>Einschätzung: Anders als bei Steuerungssystemen in der Medizintechnik oder bei vernetzten Brandmeldeanlagen, hat die Kino-Webseite keinen direkten Einfluss auf Leib und Leben. Der Schutzbedarf ist hier als niedrig oder normal anzusehen (Standardmaßnahmen genügen, besonders Verarbeitung personenbezogener/transaktionsbezogener Daten sollten höher gewichtet sein).</p>
Verstöße gegen Gesetze, Vorschriften oder Verträge	Sehr Hoch	<p>Begründung: Die Anwendung verarbeitet personenbezogene Daten (DSGVO) und führt Transaktionen durch, durch die vertragsrechtlicher/juristischer Schaden entstehen kann.</p> <p>Einschätzung (nach Sachverhalt):</p> <ol style="list-style-type: none"> 1. DSGVO: Bei der Buchung (/bookings und /account) und Account-Erstellung fallen Namen, E-Mails und ggf. Adressdaten an. Ein Datenleck zieht hohe Bußgelder nach sich. Und sollte unbedingt verhindert werden. 2. Zahlungen (PCI?): Da Tickets bezahlt werden, müssen Kreditkartenstandards (auch bei Einbindung von Drittanbietern) beachtet werden. Verbindungen sind besonders zu 3. Vertragsrecht: Ein verkauftes Ticket ist ein Vertrag. Systemfehler (Doppelbuchungen) führen zu Vertragsbrüchen und damit zu potenziell hohen Kosten.
Beeinträchtigung des informationellen Selbstbestimmungsrechts	Hoch	<p>Begründung: Die Ansammlung von Nutzerprofilen erlaubt Rückschlüsse auf persönliche Vorlieben und Gewohnheiten.</p> <p>Einschätzung: Ein Nutzer hat das Recht, dass seine Daten (welche Filme er wann sieht, Zahlungsdaten) vertraulich bleiben. Ein Leak der Datenbank ("Wer schaut welchen Film?") könnte für Einzelpersonen peinlich sein oder für Phishing missbraucht werden. Da du Vercel Analytics verwendest, findet zudem Tracking statt, was die Privatsphäre tangiert.</p>
Beeinträchtigung der Aufgabenerfüllung	Sehr Hoch	<p>Begründung: Der Ticketverkauf über das Web ist heutzutage der primäre Vertriebskanal eines Kinos. Falls diese sein</p> <p>Einschätzung: Wenn der Container ausfällt, können keine Tickets verkauft werden. Dies bedeutet direkten finanziellen Verlust pro Minute Ausfallzeit und weiter entstehende Kosten. Da es sich um ein Kerngeschäft handelt, ist die Toleranz für Ausfallzeiten sehr gering.</p>
Negative Außenwirkung	Hoch	<p>Begründung: Vertrauensverlust bei Kunden führt zu langfristigen Umsatzeinbußen. Bei Ausfall oder Zugriff von Angreifern könnte auch zu Vertragsbrüchen/verlusten führen.</p> <p>Einschätzung: Ein Hack, bei dem auf der Startseite ("Fresh in Cinema") manipulierte Inhalte angezeigt werden oder Kundendaten im Darknet landen, würde den Ruf des Kinos massiv schädigen. Kunden würden zögern, erneut online zu buchen.</p>

A. Zielobjekt: Daten (Schutzbedarf: Hoch)

Hier geht es um Benutzerdaten, Buchungshistorie und Zahlungsdaten. Die auf der Website genutzt werden müssen.

- **Datenminimierung:** Nur die Daten speichern, die zwingend nötig sind. Zahlungsdaten (Kreditkartennummern) nicht selbst in der Datenbank speichern, sondern Token von Payment-Providern (Stripe/PayPal oder ähnliches) nutzen falls vorhanden.
- **Verschlüsselung (At Rest & In Transit):**
 - **In Transit:**? Für die Produktion ein Reverse Proxy (z.B. Nginx oder Traefik) mit SSL-Zertifikaten (Let's Encrypt) davor?
 - **At Rest:** Passwörter müssen gehasht und gesalzt werden
- **Validierung**

B. Zielobjekt: Anwendungen & Prozesse (Schutzbedarf: Hoch)

Hier geht es um den Next.js Server und den Container.

- **Container-Härtung (Docker)**
- **Strategie:** Implementierung einer robusten Lösung wie **NextAuth.js**.
- **Abwehr von Bot-Traffic**

C. Zielobjekt: Kommunikationsverbindungen (Schutzbedarf: Hoch)

**Wollte ich mir angucken*

- **Netzwerk-Segregation**
- **Sicherheits-Header**