## Risikoanalyse

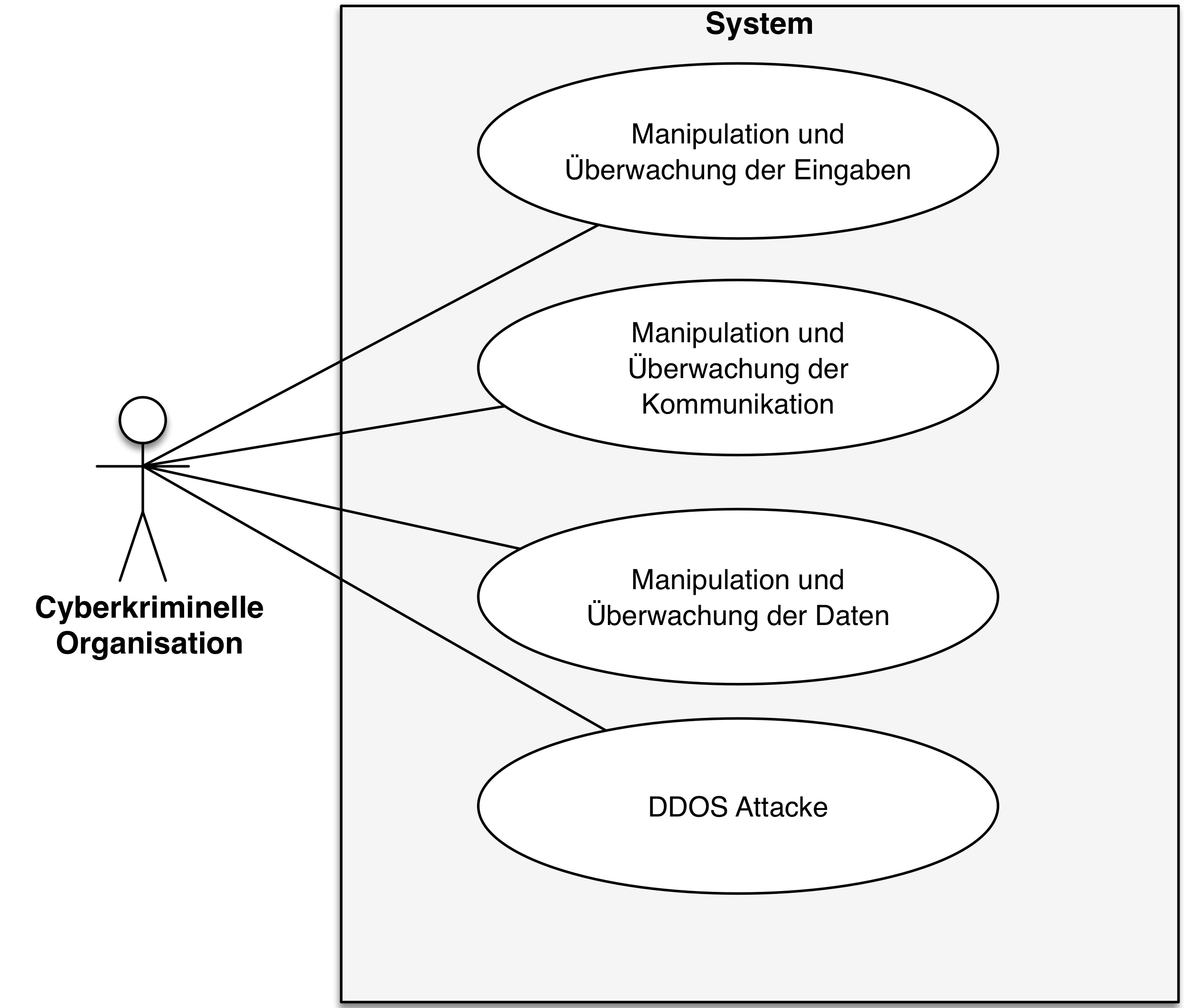
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Bezeichnung des Risikos | Wahrscheinlichkeit | Auswirkung | Bewertung | Begründung  (Schwachstellen / Bedrohung) | Auswirkung  auf | Schaden |
| R.01 | DDos Attacke | 3 | 4 | 12 | Der Server kann die die hohe Anzahl von Anfragen nicht mehr abarbeiten. | Verfügbarkeit | - Imageschaden  - wirtschaftlicher Verlust |
| R.02 | Unberechtigter Zugriff zum Admintool | 2 | 3 | 6 | Jemand hat unberechtigten Zugriff auf die Administratoren Seite  z.B. unzufriedener Mitarbeiter, Bestechung | Vertraulichkeit | - Imageschaden  - wirtschaftlicher Verlust (es können Tickets zum Schleuderpreis abgegeben werden) |
| R.03 | SQL-injection | 5 | 1 | 5 | Kontrolle über den Server | Vertraulichkeit,  Verfügbarkeit | - Imageschaden |
| R.04 | Geldströme werden vom und zum Paymentprovider umgeleitet | 3 | 2 | 6 | „man in the middle“ | Vertraulichkeit  Integrität | - Imageschaden  - wirtschaftlicher Verlust |
| R.05 | Cross-Site Scripting | 5 | 2 | 10 | Kundendaten werden gestohlen | Vertraulichkeit | - Imageschaden |

## Darstellung der Risikoanalyse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **> Wahrscheinlichkeit >** | **R.03** | **R.05** |  |  | häufig  (fast jeden Tag)  (Faktor 5) |
|  |  |  |  | wahrscheinlich  (alle 10 Tage)  (Faktor 4) |
|  | **R.04** |  | **R.01** | gelegentlich  (alle 100Tage)  (Faktor 3) |
|  |  | **R.02** |  | Selten  (alle1000 Tage)  (Faktor 2) |
|  |  |  |  | unwahrscheinlich  (alle 10000 Tage)  (Faktor 1) |
|  | niedrig  (<10kCHF)  (Faktor 1) | klein  (<100kCHF)  (Faktor 2) | hoch  (<1MCHF)  (Faktor 3) | Sehr hoch  (<1MCHF)  (Faktor 4) |  |
|  | **> Auswirkungen >** | | | |  |

## Abuse Case

In der folgenden Grafik soll gezeigt werden welche Szenarien für den Online Ticketshop der Z-Group gefährlich sein könnten, im Falle eines Angriffes von einer Cyberkriminellen Organisation.



## Sicherheitsanforderung

Im Dokument [SAD-OTS] Kapitel 11.2 Security werden einige Anmerkungen bezüglich Sicherheit gemacht. Dies soll mit den Sicherheitsanforderungen genauer spezifiziert werden.

|  |  |  |  |
| --- | --- | --- | --- |
| SA-10 | ***Manipulation und Überwachung der Eingaben*** *- Passwort* | Version | 1.0 |
| Passwörter MUSS Sonderzeichen und eine Mindestens 8 Zeichen enthalten. Das Passwort MUSS mittels SHA-256 verschlüsselt abgespeichert werden | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-20 | ***Manipulation und Überwachung der Eingaben*** *- Benutzereingaben* | Version | 1.0 |
| Alle Benutzereingaben MÜSSEN validiert werden. Prüfung des Datentyp, Maskierung Sonderzeichen. | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-30 | ***Manipulation und Überwachung der Eingaben*** *- Login* | Version | 1.0 |
| Alle Loginversuche (erfolgreich/nicht erfolgreich) MÜSSEN protokolliert werden.  Folgende Daten werden verschlüsselt protokolliert:   * Zeitpunkt * Benutzername * IP-Adresse * erfolgreich/nichterfolgreich | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-40 | ***Manipulation und Überwachung der Kommunikation*** *- Datenbankverbindung* | Version | 1.0 |
| Alle internen Benutzer MÜSSEN mittels Zertifikate eine Datenbankverbindung aufbauen. | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-50 | ***Manipulation und Überwachung der Kommunikation*** *- Webkommunikation* | Version | 1.0 |
| Web-Kommunikation MUSS HTTPS verschlüsselt sein. | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-60 | ***Manipulation und Überwachung der Daten -***  *Paymentdaten* | Version | 1.0 |
| Kreditkarten-Daten DÜRFEN nicht persistiert werden | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-70 | ***Manipulation und Überwachung der Daten*** *- Filesystem* | Version | 1.0 |
| Das Filesystem MUSS mit Filepermissions gesichert sein. (Configfiles, Logfiles) | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-80 | ***Manipulation und Überwachung der Kommunikation*** *– Configurations-Daten* | Version | 1.0 |
| Config-Files DÜRFEN keine Passwörter im Klartext enthalten. | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-90 | ***DDOS-Attacke*** *– Config-Daten* | Version | 1.0 |
| Die Verfügbarkeit der Webapplikation MUSS durch ein SLA gewährleistet werden. (Peak-Scenarien werden im Dokument Softwarearchitektur [SAD-OTS] berücksichtigt). | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |

|  |  |  |  |
| --- | --- | --- | --- |
| SA-100 | ***DDOS-Attacke*** *– Verfügbarkeit* | Version | 1.0 |
| Die Applikation MUSS redundant betrieben werden. | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| Ref | -- |
| Status | Ok |