Sicherheitsarchitektur Dokument

Online Ticketing System

Frank Moritz, Ye Zhao, Jan Klominsky

Version 1.0, 2016-09-05

Management - Summary

Über das Online Ticketing System (OTS) der Firma Z-Group werden Tickets verkauft. Wie jede Web-Anwendung, besonders Kommerzielle, steht sie im Fokus von Cyberkriminellen die der Firma Schaden zufügen oder sich durch Erpressungsversuche bereichern wollen.

In diesem Dokument wird analysiert, welche Komponenten von OTS besonderen Schutz benötigen, welche Angriffsszenarien für OTS bestehen und welche Massnahmen im technischen wie auch im organisatorischen Bereich getroffen werden können.

Dokumenten-Historie

Version	Datum	Bearbeiter	Änderung, Bemerkung
1.0	05.09.16	Frank Moritz, Ye Zhao, Jan Klominsky	Initial Dokument

Basis Dokumente

Referenz	Dokument	Beschreibung	Version
1.0	SAD-OTS	Software Architektur Dokument des Online Ticketing System	V1.0, 2016

Glossar, Abkürzungen, Begriffe

Begriff	Definition
OTS	Online Ticketing-System der Firma Z-Group
SSL	Secure Sockets Layer, Verschlüsselungsprotokoll
CSO	Chief Security Officer
SAD	Software Architektur Dokument
SLA	Service Level Agreement
DDOS	Distributed Denial of Service
Active Directory	Verzeichnisdienst von Microsoft Windows Server
Google Authentifizierung	Google Einmalpasswort
PPTP	Point-to-Point Tunneling Protocol
IPSec	Internet Protocol Security
DMZ	Demilitarized Zone

Inhaltsverzeichnis

1 Schutzbedarfsanalyse (Aufgabe 1)

OTS enthält wichtige Geschäftsinformationen die nur berechtigten Personen zugänglich sein dürfen. Der Zugriff auf die Daten muss daher geschützt sein. Eine hohe Verfügbarkeit der Anwendung muss gewährleistet sein. (siehe Anforderungen)

1.1 Allgemeines

Grundsätzlich dürfen keine Passwörter im Klartext gespeichert sein. Die Kommunikation übers Netz erfolgt immer verschlüsselt.
Für den Datenbankzugriff wird ein Rollenkonzept erstellt, da nicht jeder Benutzer alle Daten sehen bzw. ändern darf.

1.2 Übersicht

Im Projekt müssen die in der Tabelle angegeben Punkte berücksichtigt werden. Für die Bewertung werden 1, 2 oder 3 Punkte vergeben, wobei: 1 geringer Schutzbedarf und 3 sehr hohen Schutzbedarf bedeutet.

Nummer	Bezeichnung	Bemerkung	Vertraulichkeit	Integrität	Verfügbarkeit	Nachvoll-ziehbarkeit
1	Personendaten	Kontaktdaten, Adresse, Anmeldedaten	2	1	2	1
2	DB-Verbindung		3	1	2	1
3	Payment-Schnittstelle	Data-Transfer- Zugangsdaten	3	2	3	3
4	Logdateien		1	1	1	2
5	Bestelldaten	z.B. reservierte Plätze	2	2	3	2
6	Backups		1	2	1	1
7	Konfigurations-Dateien		1	1	1	2

Tabelle 1:Schützenswerte Daten

1.3 Erläuterungen

1.3.1 Personendaten

Es muss sichergestellt werden, dass nur berechtigte Sachbearbeiter die Kundendaten sehen und ändern können.

Jeder Kunde darf nur seine eigenen Daten sehen und ändern. Das Login-Passwort darf nur «gehasht und gesalzen» in der Datenbank gespeichert werden. D.h. für das Passwort wird mittels einer Einwegverschlüsselung in der Datenbank gespeichert.
Die Abwicklung der Zahlung erfolgt über die Payment-Schnittstelle, daher werden keine Kreditkarten-Daten gespeichert. Stattdessen werden nur die Transaktions-ID und der Betrag gespeichert.

Zu den Personendaten gehören Anrede, Name, Vorname, Geburtsdatum und die Adresse. Diese Daten sind notwendig, damit die Tickets zugestellt werden können. Eine Registrierung ist nicht notwendig. Wenn sich der Benutzer registrieren möchte, wird zusätzlich die E-Mailadresse gespeichert.

1.3.2 DB-Verbindung

Auf die Datenbank darf nicht über das Internet direkt zugegriffen werden können. Der Zugang erfolgt entweder über die Web-Applikation oder über das interne Admin-Tool. Der interne Zugriff auf die DB erfolgt mittels Zertifikaten und nicht über Benutzer/Passwort.
Es werden verschiedene Rollen definiert. Nur Admins dürfen die Saalkonfiguration und Preiskategorien ändern.
Für die Web-Applikation wird ein eigener DB-User erstellt. Die Rechte des DB-Users müssen möglichst strikt eingeschränkt werden.

1.3.3 Payment-Schnittstelle

Der Zahlungsvorgang wird durch einen externen Anbieter durchgeführt. Daher werden keine Kreditkartennummer oder ähnliche Daten in der Datenbank gespeichert. Die Übertragung der Daten muss mittels SSL gesichert werden. Die Zugangsdaten zum externen Anbieter müssen verschlüsselt abgelegt werden.

Es muss sichergestellt sein, dass getätigte Zahlungen nicht verändert werden können. Eine Archivierung der Zahlungsdaten ist nicht notwendig.

1.3.4 Logdateien

Die Logdateien dürfen keine personenbezogenen Daten enthalten. Betreibersicht: Der Zugriff auf die Dateien muss über Zugriffberechtigungen geschützt und geregelt werden.

1.3.5 Bestelldaten

Es muss sichergestellt sein, dass die Bestelldaten nicht nachträglich vom Kunden geändert werden können. Nur Sachbearbeiter dürfen beispielsweise die Adresse korrigieren. In der Datenbank muss ersichtlich sein, wann und vom wem die Bestelldaten geändert wurden.

1.3.6 Backups & Archivierung

Es müssen in regelmässigen Abständen Backups erstellt werden, damit nach einem Ausfall der Datenbank nicht zu viele Daten verloren gehen.
Eine Archivierung der Daten ist nicht notwendig, für spätere Auswertungen aber wünschenswert.

1.3.7 Konfigurationsdateien

Die Konfigurationsdateien dürfen nicht über das Netz einsehbar sein, sondern müssen wie die Logdateien über Zugriffberechtigungen geschützt werden.

2 Risikoanalyse (Aufgabe 2)

In der Risikoanalyse werden die Möglichkeiten eines Angriffs sowie die daraus folgenden Auswirkungen und Schäden aufgezeigt. Die Bewertung des Risikos ist das Produkt aus der Eintrittswahrscheinlichkeit und der Auswirkung. Je höher diese Bewertung ist, desto höher das Risiko. Als Grundlage für die Risikoanalyse dient die Abbildung 3 (Bausteinsicht Ebene2) des SAD-OTS Dokumentes.

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 Admininterface	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	2	10	Kontrolle über den Server, Manipulation der Daten	Vertraulichkeit, Verfügbarkeit, Integrität	- Datenverlust - Imageschaden
R.04	Geldströme werden vom und zum Paymentsystem umgeleitet	3	2	6	„man in the middle“	Vertraulichkeit Integrität	- Imageschaden - wirtschaftlicher Verlust
R.05	Cross-Site Scripting	5	3	15	Kundendaten werden gestohlen	Vertraulichkeit	- Imageschaden

Tabelle 2: Übersicht Risiken

2.1 Auswirkungen

Mit dem Management der Z-Group wurde die Auswirkungen bei welchem Schadensszenario quantifiziert:

Auswirkung	Mögliches Schadensszenario
< 10kCHF	- Verlust einzelner Tickets - Falschbuchung
< 100kCHF	- Passwörter werden geklaut
< 1MCHF	- Ausfall einer Show - Kunden können nicht buchen - Interne Daten werden öffentlich - Tickets werden zu einem niedrigen Preis angeboten
> 1MCHF	- Imageschaden - Schlechte Presse wegen IT - Interne Daten werden öffentlich

2.2 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 >				

Tabelle 3: Einordnung der wichtigsten Risiken

Daraus folgt, dass für die Risiken R.01 (DDOS-Attacke), R.03 (SQL-Injection) und R.05 (Cross-Site Scripting) dringend Massnahmen ergriffen werden müssen.

3 Sicherheitsanforderungen (Aufgabe 3)

3.1 Abuse Case

Die folgende Grafik zeigt, welche Szenarien für den Online Ticketshop der Z-Group im Falle eines Cyber-Angriffes am gefährlichsten sind und leitet nachfolgend die Sicherheitsanforderungen ab.

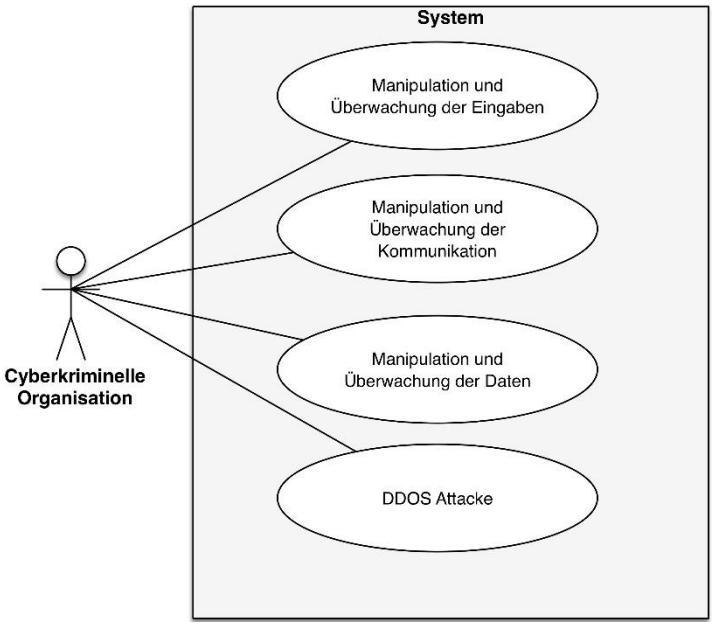


Abbildung 1: Abuse Case

3.2 Sicherheitsanforderung

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

Erläuterung zu den Anforderungen

SA-##	SA Sicherheitsanforderung mit einer eindeutigen Nummer
Version	Aktuelle Versionsnummer der Anforderung
Author	Wer hat die Anforderung erfasst?
Quelle	Wer stellt die Anforderung?
Ref	Die Referenz bezieht sich auf die Tabelle 2.
Status	init Ungeprüft nok Abgelehnt OK Angenommen

SA-10	***Manipulation und Überwachung der Eingaben*** *- Passwort*	Version	1.0
	Passwörter MÜSSEN Sonderzeichen und mindestens 8 Zeichen enthalten. Das Passwort MUSS zusammen mit einem individuellen Salt-Wert als SHA-256-Hashwert abgespeichert werden.	Autor	CSO
		Quelle	Z-Group-Management
		Ref	R.02
		Status	Ok

SA-20	***Manipulation und Überwachung der Eingaben*** *- Benutzereingaben*	Version	1.0
	Alle Benutzereingaben MÜSSEN validiert werden (Prüfung des Datentyp, Maskierung Sonderzeichen) Zu den Benutzereingaben zählen nicht nur die Textfelder sondern beispielsweise auch die URL-Parameter. Die Prüfung erfolgt immer serverseitig, optional ist eine zusätzlich Prüfung auf dem Client möglich.	Autor	CSO
		Quelle	Z-Group-Management
		Ref	R.03 und R.05
		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
		Ref	R.03 und R.05
		Status	Ok

SA-40	***Manipulation und Überwachung der Kommunikation*** *- Datenbankverbindung*	Version	1.0
	Alle internen Benutzer MÜSSEN mittels Zertifikate eine Datenbankverbindung aufbauen. (und nicht über Benutzername/Passwort)	Autor	CSO
		Quelle	Z-Group-Management
		Ref	R.02
		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
		Ref	R.04
		Status	Ok

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

SA-70	***Manipulation und Überwachung der Daten*** *- Filesystem*	Version	1.0
	Das Dateisystem MUSS mit Zugriffsberechtigungen gesichert sein. Das gilt für Konfigurationsdateien sowie für Log-Dateien.	Autor	CSO
		Quelle	Z-Group-Management
		Ref	--
		Status	Ok

SA-80	***Manipulation und Überwachung der Daten*** *- Nachvollziehbarkeit*	Version	1.0
	Es MUSS in der Datenbank ersichtlich sein, wann und vom wem die Daten geändert wurden.	Autor	CSO
		Quelle	Z-Group-Management
		Ref	R.01
		Status	Ok

SA-90	***Manipulation und Überwachung der Kommunikation –*** *Konfigurations-Daten*	Version	1.0
	Konfigurationsdateien DÜRFEN keine Passwörter im Klartext enthalten.	Autor	CSO
		Quelle	Z-Group-Management
		Ref	R.02
		Status	Ok

SA-100	***DDOS-Attacke*** *– Verfügbarkeit*	Version	1.0
	- Die Verfügbarkeit der Webapplikation MUSS durch ein SLA gewährleistet werden. (Peak-Szenarien werden im Dokument Softwarearchitektur [SAD-OTS] berücksichtigt). - Die Applikation MUSS redundant betrieben werden, damit interne Benutzer auch im Falle einer DOS-Attacke weiterarbeiten können. - Es muss ein Notfallkonzept erarbeitet werden, damit IP-Adressen gefiltert werden können	Autor	CSO
		Quelle	Z-Group-Management
		Ref	R.01
		Status	Ok

4 Identity & Access Management (Aufgabe 4)

4.1 Identitäten

System	Wer hat Zugriff ?
DB	- System-Administrator - Interner Administrator - Webservice-User - Boxoffice-User
Web-Applikation	- anonyme Webbenutzer - registrierte Onlinebenutzer - Boxoffice-User
Filesystem	- Admin (Pflege der Anwendungen, Überwachung der Logdateien)
Umsysteme	- Systembenutzer für Payment-Schnittstelle - Systembenutzer für Exchange

4.2 Speicherort der Identitäten

System Administrator, interne Administrator, Boxoffice-User, Webservice-User, Filesystem:

➔ zentrale Benutzerverwaltung (Active Directory)

Registrierte Onlinebenutzer:

➔ in der DB

Umsystem:

➔ in einer lokalen Konfigurations-Datei

4.3 Unterstützen einer Federation

Aus Anwendersicht hat einer Federation den Vorteil, dass man sich nicht einen weiteren Account merken muss und die Accounts zentral verwaltet werden, zum Beispiel bei Google. Für OTS hätte es den Vorteil, dass die Authentifizierung extern (also beispielsweise von Google) erfolgen würde. Allerdings würden wir uns dann von Google abhängig machen.

Da die Registrierung optional ist, ist der Vorteil der Federation fürs OTS recht gering. In der Realisierungsphase sollte trotzdem untersucht werden, wie aufwendig die Integration von Google Authentifizierung ist. Wenn es sich einfach integrieren lässt, sollte sowohl die Registrierung mittels Benutzername/Passwort als auch Google Authentifizierung möglich sein, um dadurch die Benutzerfreundlichkeit zu erhöhen.

4.4 Welche Authentifizierungmethoden werden unterstützt?

Für die Web-Applikation stehen Benutzername/Passwort und Google Authentifizierung zur Verfügung.

Für die internen Benutzer wird ausschliesslich das «Active Directory» verwendet.

4.5 Initialer Zugang zum OTS

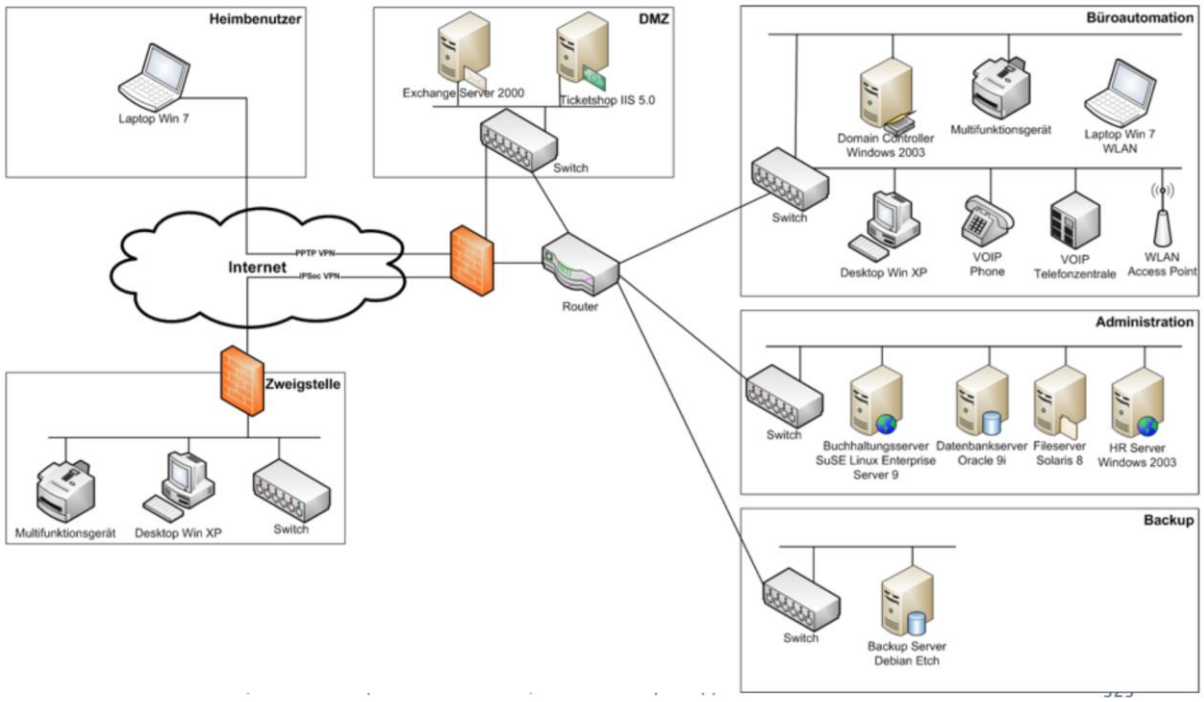
Der Benutzer erhält nach der Registrierung eine E-Mail zur Bestätigung. Erst danach wird der Account aktiviert.

4.6 Vergessene Authentifizierungs-Mittel

Fall der Benutzer/Kunde sein Benutzername oder Passwort vergessen hat, kann der diese beim OTS-Administrator anfordern. Der schickt dem Benutzer eine E-Mail mit einem Link zum Bestätigen, damit wird das Passwort zurückgesetzt.

5 Netzwerksicherheit (Aufgabe 5)

Abbildung der Netzwerk- und Systemumgebung des OTS



Nummer	Risiko	Massnahme	Art der Massnahme
1	Veraltete Software und Betriebssysteme	Update auf neue Softwareversion	technisch
2	neue Sicherheitslücken	regelmässige Überprüfung der Netzwerkarchitektur	organisatorisch
3	keine Firewall zwischen DMZ und internem Netz	Firewall zwischen DMZ und internem Netz einrichten	technisch
4	PPTP Protokoll für Heimnutzer wird verwendet (PPTP ist veraltet)	PPTP durch IPSec ersetzen	technisch
5	uneinheitliche Applikationslandschaft	Betriebssysteme vereinheitlichen	technisch
6	Exchange Server in DMZ (nicht notwendig da der Anwender sich über VPN mit dem Netzwerk verbindet)	Exchange Server in das interne Firmennetz verschieben	technisch
7	Die Firewall-Regeln sind zu grosszügig eingerichtet	Firewall-Regeln prüfen	organisatorische

8	Zu viele Zugriffe theoretisch auf DB Server möglich	DB Server mit einer DB Firewall abgrenzen	technisch
9	Eventuell veralte WLAN WEP-Verschlüsselung	durch moderne Verschlüsselung WPA ersetzen	technisch
10	Ausspähversuche	Logdateien auf mögliche Ausspähversuche hin untersuchen	organisatorisch
11	Notfallkonzept greift nicht	Erstellung und testen des Notfallkonzeptes (Restore Datenbank, Umzug Server, Filterung IP-Adressen usw.)	organisatorisch
12	Unsicherer Code	Schulung der Entwickler, damit der aktuelle Stand der Technik berücksichtigt wird	organisatorisch

6 Anwendungssicherheit (Aufgabe 6)

Aus den OWASP Top 10 werden die A1 (Injection) und die A5 (Security Misconfiguration) als grösste Bedrohung für das OTS angesehen. Dies folgt aus der Risikoanalyse R.03 (SQL-Injection) und R.02 (Unberechtigter Zugriff zum Administratoren-Interface).

OWASP A1 Injection	
Grund:	Die Manipulation der Daten wird als Risiko angesehen
Technische Massnahmen	Validierung der Eingaben: - Maskierung der Sonderzeichen - Parameter für SQL-Abfragen - Nur allgemeine Fehlermeldungen zurückgeben die keine Rückschlüsse auf die interne Umsetzung geben
Organisatorische Massnahmen	- Regelmässige Codereviews - «Penetrationtests» durch externe Firmen

OWASP A5 Security Misconfiguration	
Grund:	- Unberechtigter Zutritt zur Datenbank - Verlust von vertraulichen Daten, wie Personendaten, Preiskategorien, Auslastung der Shows
Technische Massnahmen	- Automatisierung der Konfiguration - Verschlüsselung der Passwörter - Regelung der Zutrittsberechtigungen und Einschränkungen vornehmen, nur so viel Rechte wie nötig - Firewallregeln einschränken - Softwarekomponenten auf dem neusten Stand
Organisatorische Massnahmen	- Checklisten und interne Richtlinien (siehe Kap. 3 Sicherheitsanforderungen) - Backup dürfen vom Web nicht erreichbar sein - Backup muss regelmässig gemacht werden - Regelmässige Audits/Reviews - Regelmässige Sicherheitsupdates machen