Sicherheitsarchitektur Dokument

***Online Ticketing System***

Frank Moritz, Ye Zhao, Jan Klominsky

Version 1.0, 2016-09-05

Management - Summary

Dokumenten-Historie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Bearbeiter | Änderung, Bemerkung |
| 1.0 | 01.06.15 | Frank Moritz, Ye Zhao, Jan Klominsky | Inital 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 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Inhaltsverzeichnis

[1 Schutzbedarfsanalyse (Aufgabe 1) 5](#_Toc460367226)

[1.1 Allgemeines 5](#_Toc460367227)

[1.2 Übersicht 5](#_Toc460367228)

[1.3 Erläuterungen 5](#_Toc460367229)

[2 Risikoanalyse (Aufgabe 2) 7](#_Toc460367230)

[2.1 Auswirkungen 7](#_Toc460367231)

[2.2 Darstellung der Risikoanalyse 8](#_Toc460367232)

[3 Sicherheitsanforderungen (Aufgabe 3) 9](#_Toc460367233)

[3.1 Abuse Case 9](#_Toc460367234)

[3.2 Sicherheitsanforderung 9](#_Toc460367235)

[4 Identity & Access Management (Aufgabe 4) 12](#_Toc460367236)

[4.1 Identitäten 12](#_Toc460367237)

[4.2 Speicherort der Identitäten 12](#_Toc460367238)

[4.3 Unterstützen einer Federation 12](#_Toc460367239)

[4.4 Welche Authentifizierungmethoden werden unterstützt? 12](#_Toc460367240)

[4.5 Initialer Zugang? 12](#_Toc460367241)

[4.6 Vergessene Auth-Mittel 13](#_Toc460367242)

[5 Netzwerksicherheit (Aufgabe 5) 14](#_Toc460367243)

# 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)

## Allgemeines

Grundsätzlich dürfen keine Passwörter im Klartext gespeichert sein. Die Kommunikation übers Netz ist immer verschlüsselt.

## 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 | DataTrans- Zugangsdaten |  |  |  |  |
| 4 | Logdateien |  |  |  |  |  |
| 5 | Bestelldaten | z.B. reservierte Plätze |  |  |  |  |
| 6 | Backups |  |  |  |  |  |
| 7 | Konfig-Dateien |  |  |  |  |  |

## Erläuterungen

### Personendaten

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

Jeder Kunde darf nur seine eigenen Daten sehen und ändern. Das Login-Passwort darf nur gehasht in der Datenbank gespeichert werden.

### 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.

### 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.

### Logdateien

Die Logdateien dürfen keine personenbezogenen Daten enthalten. Betreibersicht: Der Zugriff muss über Filepermissions geschützt werden.

### Bestelldaten

Es muss sichergestellt sein, dass die Bestelldaten nicht nachträglich vom Kunden geändert werden können. Nur Sachbearbeiter dürfen beispielsweise die Adresse korrigieren.

### 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.

### Konfigurationsdateien

Dürfen nicht über das Netz einsehbar sein.

# Risikoanalyse (Aufgabe 2)

In der Risikoanalyse werden die Möglichkeiten eines Angriffs aufgezeigt und die daraus folgenden Auswirkungen und Schäden. 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 | Vertraulichkeit,  Verfügbarkeit | - 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 |

## Auswirkungen

Todo

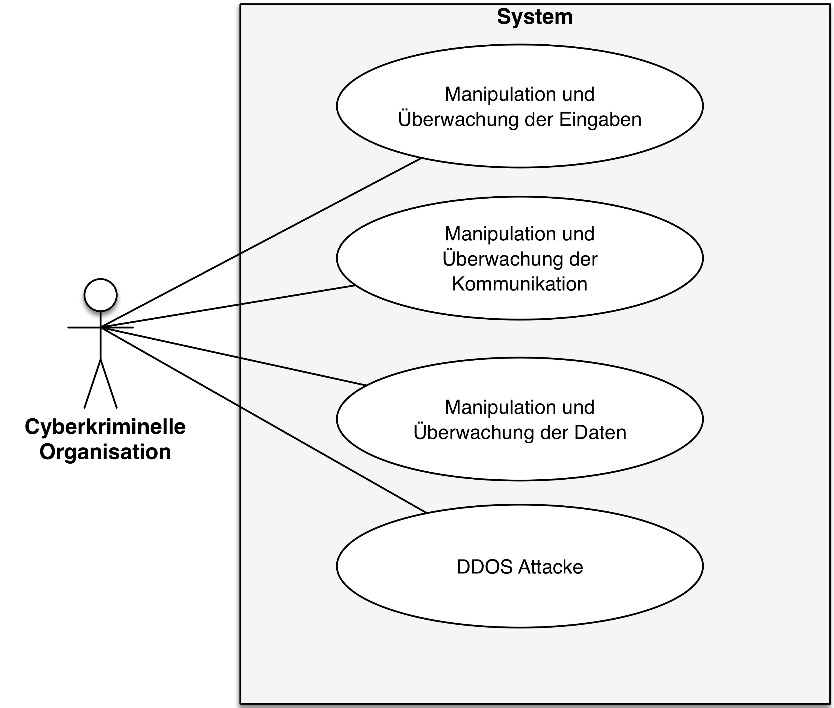
## Darstellung der Risikoanalyse

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **> 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 >** | | | |  |

# Sicherheitsanforderungen (Aufgabe 3)

## 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 | 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. | Autor | CSO |
| Quelle | Z-Group-Management |
| Prio | 1 |
| 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 |
| 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 |

# Identity & Access Management (Aufgabe 4)

## Identitäten

|  |  |
| --- | --- |
| System | Wer hat Zugriff ? |
| DB | * SysAdmin * Internen Admins * Onlineuser * Boxoffice-User * registrierte Onlinebenutzer |
| Filesystem | * Admin (Pflege der Anwendungen, Überwachung der Logdateien) |
| Umsysteme | * Systembenutzer für Payment-Schnittstelle * Systembenutzer für Exchange |

## Speicherort der Identitäten

**SysAdmin, interne Admins, Boxoffice-User, Webservice-User, Filesystem:**

* zentrale Benutzerverwaltung (ActiveDirectory)

**Registrierte Onlinebenutzer:**

* in der DB

**Umsystem:**

* in einer lokalen Config-Datei

## Unterstützen einer Federation

Für die internen Benutzer wird eine zentrale Benutzerverwaltung verwendet. Die Anmeldung an die DB erfolgt durch

Kerberos-Zertifikate

Vorteil: Benutzerfreudlich für die Endbenutzer, man muss sich nur einmal anmelden

Für die externen Benutzer steht nur Benutzername/Passwort zur Verfügung. Die Registrierung ist optional, daher lohnt sich die Implementierung nicht.

## Welche Authentifizierungmethoden werden unterstützt?

Für die externen Benutzer steht nur Benutzername/Passwort zur Verfügung. Die Registrierung ist optional, daher lohnt sich die Implementierung nicht.

## Initialer Zugang?

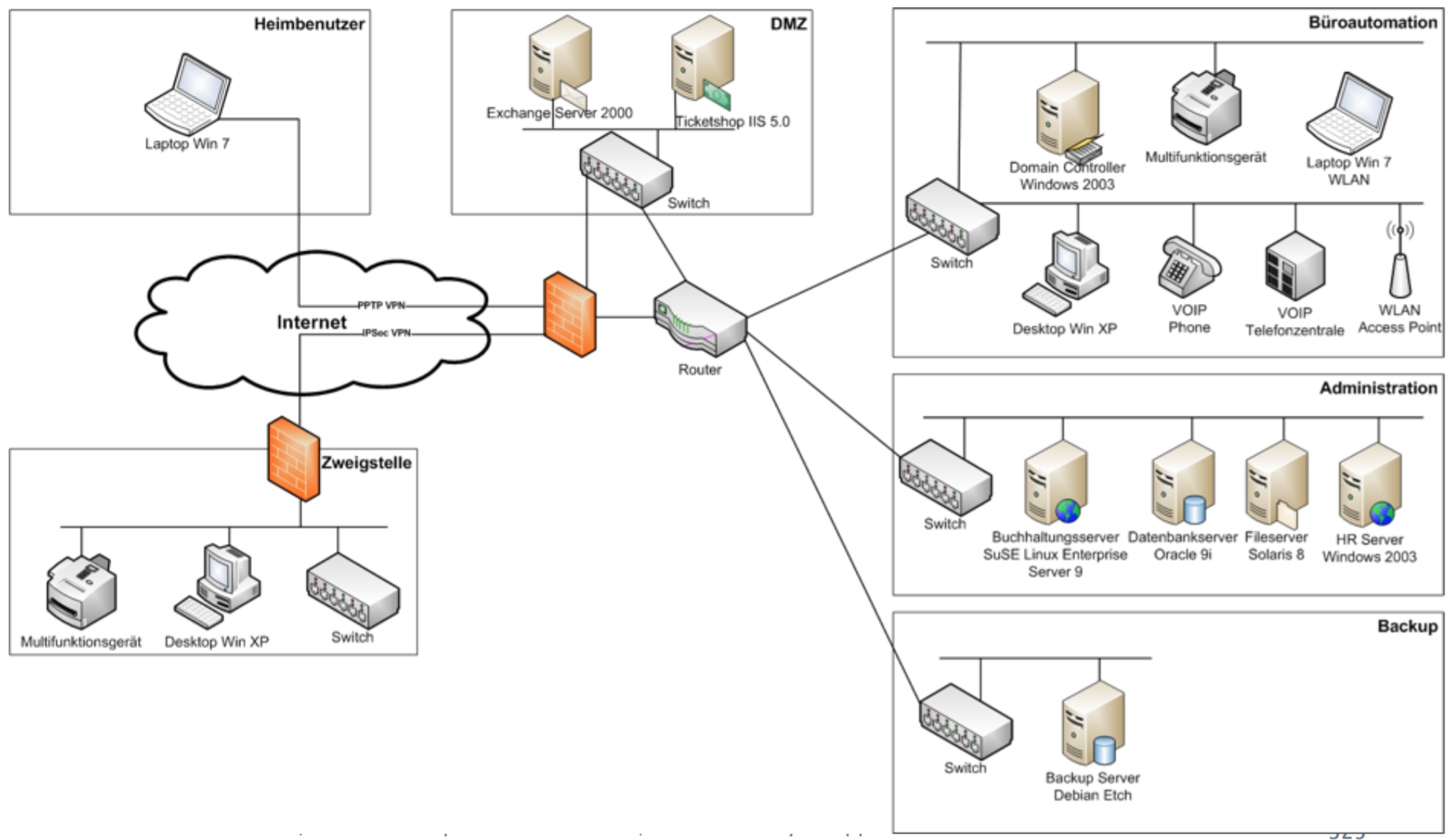
extern: E-mail zur Bestätigung senden

## Vergessene Auth-Mittel

extern: E-Mail mit Link schicken, damit das Passwort zurückgesetzt werden kann

# 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 | Veraltete Software und Betriebssysteme | Updateprozess definieren | 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 ersetzen durch IPSec | technisch |
| 5 | uneinheitliche Applikationslandschaft | Applikationen vor allem Betriebssysteme vereinheitlichen | technisch |
| 6 | Exchange Server in DMZ (nicht notwendig da Anwender sowieso im VPM sein müssen) | Exchange Server in das Firmennetz verschieben | technisch |
| 7 | Firewallregeln zu grosszügig eingerichtet | Firewallregeln prüfen | organisatorische |
| 8 | Zuviele 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 |  |  |  |