Sicherheit

**Backup:**

Um das Risiko eines Ausfalls (und somit Datenverlust) zu minimieren, soll es ein Backup-System geben. Dieses Backup-System soll innerhalb von 2 Minuten, nach dem Ausfall des Hauptservers verfügbar sein und alle Daten des Hauptservers (vor dem Ausfall) beinhalten.

Umgesetzt wird dies, durch sogenannte Hochverfügbarkeitscluster bei denen der Hauptserver dauerhaft gespiegelt wird. Trifft auf einem Knoten des Clusters ein Fehler auf, werden die auf diesem Knoten laufenden Dienste auf einen anderen Knoten migriert. Dieses Verfahren entspricht heute dem Standard und wird von jeder Webseite genutzt. Die Arbeit wird hier von dem jeweiligen Hoster übernommen (da dies privat schwierig zum umsetzten ist) und passiert automatisch, sollte ein Server ausfallen. Allerdings hat man keinen direkten Zugriff auf die Server des Hoster und kann somit keine Server ausschalten/ausfallen lassen.

Ein veraltetest und unsicheres Verfahren, wäre das manuelle Übertragen von Daten, an einen zweien Server (der DNS-Server würde sich um die richtige Zuordnung kümmern). Bei diesem Verfahren hat meine eine viel höhere Fehleranfälligkeit und hat maximal einen Ersatz Server. Dazu kommt, dass die Daten, bei der Übertragung zum zweien Server manipuliert werden könne, was ein hohes Sicherheitsrisiko ist. Beim Hochverfügbarkeitscluster, greifen alle Cluster auf denselben Datensatz zu, und somit ist dieser für jeden gleich und unverfälscht.

**Import der Liste mit Wählern/Parteien/Kandidaten:**

Damit eine Wahl vollständig ist, braucht sie eine Liste mit berechtigten Wähler. Diese Liste wird von den jeweiligen Wahlkreisen erstellt und als Datei zum Verantwortlichen der Wahl gesendet (Ersteller der Online Wahl).

Die Datei/Liste muss den Wahlkreis und ihre berechtigten Wähler beinhalten.

Bei den jeweiligen Wählern muss als Information sein Vor-/Nachname sowie der Hash-Wert des RFID-Tag angegeben sein (Wahlkreis wird dadurch angeben, dass die ganze Datei/Liste nur Wähler eines Wahlkreises beinhalten).

Nach dem gleichen Prinzip werden auch die Listen für die Kandidaten/Parteien erstellt.

Auch hier muss der jeweilige Wahlkreis eine Datei/Liste erstellen mit seinen wählbaren Parteien/Kandidaten und diese zum Verantwortlichen der Wahl senden (Ersteller der Online Wahl).

Ein Import geht immer nur im Ganzen und kann auch nur im Ganzen gelöscht werden.

Das heißt, eine Liste wird genauso importiert wie ein Wahlkreis sie erstellt. Einzelne Einträge sind nicht von der Software veränderbar. Hat man doch einen Fehler gemacht, in dem z.B. ein Eintrag falsch ist oder fehlt, muss die Liste neu importiert werden und die alten Einträge werden entfernt.

Um die Korruption dieser Listen/Dateien zu vermeiden, werden diese Dateien verschlüsselt (wenn die Anforderung besteht mit einem Passwort versehen) und die Checksum berechnet.

Checksum (sowie Passwort) müssen separat versendet werden. Dazu werden die CSV Dateien in einem ZIP-Archiv mit Passwort gepackt, welches verschlüsselt wird. Dieses ZIP-Archiv muss vor dem importieren mit besagten Passwort entschlüsselt werden. Dies muss für eine erhöhte Sicherheit manuell und vor dem Import der einzelnen CSV-Dateien passieren.

Dazu sollte man, manuell von der angekommenen Datei eine Checksum berechnen und diese mit der gesendeten Checksum vergleichen. Ebenfalls besteht die Möglichkeit, diese Schritte von der Webseite zu übernehmen (Validierung der Checksum). Erst wenn alle diese Schritte geglückt sind, wird die Datei als akzeptable gewertet und kann in die Datenbank gespeichert werden. Allerdings kann die Webseite nicht zwischen einer Falschen oder richtigen Wählerliste unterscheiden, solange das Format eingehalten wurde und die anderen Schritte geglückt sind, ist die Liste/Datei für die Webseite.

Als Verfahren für die Berechnung der Checksum, wird der CRC32 Hash-Algorithmus verwendet.

**Frontend Passwörter:**

Alle Passwörter werden auf der Webseite mit Punkten/Sternen bei der Angabe angezeigt. Dies soll verhindern, dass Passwörter bei der Eingabe, von anderen Person im Raum, einfach vom Bildschirm abgelesen werden können.

**RFID-Reader/Login:**

Möchte ein/eine WählerIn seine Wahl Online absolvieren, muss er/sie dies anmelden. Dazu geht er/sie zu einer Beauftragten Stelle (Beispiel: Rathaus, Bürger Büro) und zeigt dort seinen/ihren Personalausweis vor. Danach erhält er/sie (wenn er/sie berechtig ist zum Wählen) einen RFID-Tag/-Chip. Zusätzlich dazu, wird dem/der WählerIn ein Passwort per Post verschickt.

Möchte man sich nun anmelden, muss man den RFID Reader per USB mit dem PC verbinden. Legt man nun den RFID-Tag/-Chip auf das Gerät piepst dieses einmal, wenn es den Chip lesen konnte. Zusätzlich muss dann man noch das Passwort, welches man per Post erhalten hat, eingeben. Diese Kombination aus Passwort und RFID-Chip, macht das „Knacken“ des Zugangs per Brute Force Attacke so gut wie unmöglich. Dazu kommt eine Zwei Faktor Authentifizierung, da einmal ein RFID-Chip benötigt wird, welchen man nur von offiziellen Stattlichen Behörden erhält und einem Passwort, welches man per Post erhält.