SchILDweb/SchILDapp Sicherheits-/Kommunikationskonzept

Serverseitiges Sicherheitskonzept

- Die Programmstruktur von SchILD*web (SchILDapp)* ermöglicht eine strikte Trennung zwischen Frontend, Backend und Datenbank. Alle Teile der Anwendung können auf physikalisch/virtuell getrennten Servern installiert und daher auch unterschiedlichen Firewall-Sicherheitszonen zugeteilt werden. Im Falle einer Installation auf einem einzigen Server (z.B. auf einem gehosteten Webspace) sind die Anwendungsteile nicht physikalisch getrennt.
- Das Frontend (und somit der SchILDweb/app-Nutzer) hat weder direkten Datenbankzugriff, noch einen direkten Zugriff auf das Backend (die Programmlogik) der Anwendung.
- Die Kommunikation zwischen Browser und/oder Smartphone und Webserver (Webspace) kann optional SSL verschlüsselt werden (ebenso wie die Kommunikation zwischen Frontend-Server und Backend-Server, im Falle einer Installation auf getrennten Servern). Voraussetzung hierfür die die Nutzung eines gültigen SSL-Zertifikats auf dem Webserver.
- Datenfluss je nach gewählter Installationsmethode: siehe angehängte Schaubilder.
- Kommandos/Befehle vom Frontend werden erst auf dem Applicationserver repektive im Backend in tatsächliche SQL-Befehle übersetzt. Die Kommunikation erfolgt über Ajax/im JSON-Format. Das Backend wandelt die von der Datenbank erhaltenen Daten wiederum in ein JSON-Format um und schickt diese an das Frontend und dieses dann zum Browser.
- Im Backend befindet sich die sicherheitsrelevante Programmlogik sowie die verschlüsselten SQL-Server-Verbindungsdaten. Hier erfolgt auch die Überprüfung der Anfragen (z.B. Userberechtigung, Geräteberechtigung, gültige Session, gültiges Passwort, generelle Prüfung der Abfrage/des Kommandos (respektive der JSON-Datei) (z.B. auf mögliche SQL-Injection, etc.) und Umwandlung der Abfrage in SQL-Befehle.
- Die Synchronisation zwischen SchILD-NRW und SchILDweb erfolgt manuell, über ein spezielles Synchronisationstool, der Datenabgleich erfolgt optional über eine verschlüsselte SSL-Verbindung. Voraussetzung hierfür die die Nutzung eines gültigen SSL-Zertifikats auf dem Webserver.
- Neben den für SchILDweb/SchILDapp essentiell benötigten Daten (Schülername, Klasse, Lehrkraft, Note, etc.) werden keine anderen personenbezogenen, datenschutzrechtlich relevanten Daten verfügbar gemacht.

Userseitiges Sicherheitskonzept: SchILDweb

- Die Anzahl der fehlerhaften Logins ist begrenzt (zentral einstellbar). Default ist 3, danach wird der Account gesperrt bzw. es muss vom Nutzer ein neues Passwort angefordert werden.
- Die Richtlinien für die Passwörter können zentral festgelegt werden. Standard ist: mind. 8 Zeichen, mind. 1 Großbuchstabe, mind. 1 Kleinbuchstabe, mind. 1 Ziffer, mind. 1 Sonderzeichen.
- Optional erhält der Anwender nach Abmeldung von SchILDweb eine E-Mail (mit Informationen über die letzte SchILDweb-Session)
- Dem Anwender wird nach dem Login die letzte Loginzeit sowie die Anzahl der Fehllogins angezeigt.
- Anmelden kann sich nur eine Lehrkraft die in SchILD dazu berechtigt wurde. Er muss zusätzlich eine gültige (dienstliche) E-Mailadresse hinterlegen.
- Bei der ersten Anmeldung (bei Anforderung eines neuen Kennwortes) wird die Gültigkeit der Lehrerkürzel/Schulnummern-Kombination, die Gültigkeit der angegeben E-Mailadresse (muss identisch mit der hinterlegten sein) sowie die allgemeine Berechtigung zum Zugriff auf SchILDweb geprüft.
  Bei erfolgreicher Prüfung wird ein Passwort an die hinterlegte E-Mailadresse gesendet. Dieses ist nur einmal gültig und muss während des Login-Vorgangs, bzw. vor der ersten Nutzung von SchILDweb zwingend geändert werden.

- Beim regulären Login wird die Lehrerkürzel/Schulnummer/Passwort-Kombination sowie die Berechtigung zur Nutzung von SchILDweb überprüft.
- SchILDweb wird nach einem vorgegebenen Zeitraum der Inaktivität (zentral einstellbar) automatisch beendet (automatisches Logout). Standardzeit bis zum Logout sind 3 min, die Vorwarnzeit beträgt 30 Sek (es erscheint ein entsprechendes Meldungsfenster).
- Alle nicht „gespeicherten" Daten werden automatisch bis zum nächsten Login in der Datenbank gesichert. Nur aktiv „gespeicherte" Daten werden endgültig in die SchILD-Datenbank geschrieben bzw. stehen zur Synchronisation zur Verfügung.
- Nach dem Logout bleiben keine temporären Daten, weder im Browser, noch im Frontend auf dem Webserver, zurück. Im Backend werden alle anfallenden temporären Daten (es werden von SchILDweb generell keine sicherheitsrelevanten Daten zwischengespeichert) nach ca. 20 min vom PHP-Garbage Collector gelöscht.

Userseitiges Sicherheitskonzept SchILDapp

- Der Start von SchILDapp ist nur mit einer benutzerspezifische PIN (6-16 Stellen) möglich. Auf diese Weise kann auch auf einem entsperrten Smartphone die App nicht unberechtigt gestartet werden.
- Die Anzahl der möglichen fehlerhaften Eingaben der PIN ist aktuell auf 10 begrenzt. Danach ist das Gerät für die Nutzung mit SchILDapp gesperrt und muss, bevor SchILDapp erneut genutzt werden kann, vom SchILDadministrator entsperrt bzw. erneut berechtigt werden.
- Vor jeder Datensynchronisation müssen die Zugangsdaten zum Webserver (Lehrerkürzel, Schulnummer, Passwort) eingegeben werden.
- Die Anzahl der fehlerhaften Logins zur Datensynchronisation ist begrenzt (zentral einstellbar). Default ist 3, danach wird der Zugang zur Datensynchronisation (respektive zum Webserver) gesperrt. Der Nutzer muss in diesem Fall ein neues Passwort anfordern.
- Die Richtlinien für die verwendeten Passwörter können zentral festgelegt werden. Standard ist: mind. 8 Zeichen, mind. 1 Großbuchstabe, mind. 1 Kleinbuchstabe, mind. 1 Ziffer, mind. 1 Sonderzeichen.
- Anmelden kann sich nur eine Lehrkraft die in SchILD dazu berechtigt wurde. Neben der generellen Nutzungsberechtigung muss eine gültige (dienstliche) E-Mailadresse sowie eine Geräteidentifikation (IMEI oder MAC-Adresse) für jedes mit SchILDapp genutzte Gerät hinterlegt sein.
- Bei der ersten Anmeldung (oder bei Anforderung eines neuen Kennwortes) wird die Gültigkeit der Lehrerkürzel/Schulnummern-Kombination, die Gültigkeit der angegeben E-Mailadresse (muss identisch mit der hinterlegten sein), die Geräteidentifikation sowie die allgemeine Berechtigung zur Nutzung von SchILDapp geprüft.
  Bei erfolgreicher Prüfung wird ein Passwort an die hinterlegte E-Mailadresse gesendet. Dieses ist nur einmal gültig und muss während des Login-Vorgangs, bzw. vor der ersten Datensynchronisation zwingend geändert werden.
- Beim regulären Login wird die Lehrerkürzel/Schulnummer/Passwort-Kombination, Geräteidentifikation sowie die Berechtigung zur Nutzung von SchILDapp überprüft.
- Alle von SchILDapp verwalteten Daten werden in einer verschlüsselten Datenbank im geschützten Systembereich des Smartphones abgelegt. Außerhalb der verschlüsselten Datenbank speichert SchILDapp keine Daten. Im geschützten Systembereich ist die Datenbank für andere auf dem System befindliche Anwendungen (z.B. Whatsapp) nicht erreichbar und wird auch nicht von automatischen (systeminternen) Backups erfasst.
- SchILDapp wird, sobald die App den „Fokus" verliert (bspw. bei Wechsel der Anwendung, oder bei Timeout des Bildschirms) automatisch gesperrt. Zur Weiternutzung muss erneut die benutzerspezifische PIN eingegeben werden.
- Nach dem Beenden bleiben keine temporären Daten auf dem Gerät oder dem Webserver zurück. Im Backend werden alle anfallenden temporären Daten (es werden generell keine sicherheitsrelevanten Daten zwischengespeichert) nach ca. 20 min vom PHP-Garbage Collector gelöscht.

SchILDweb/app Admin

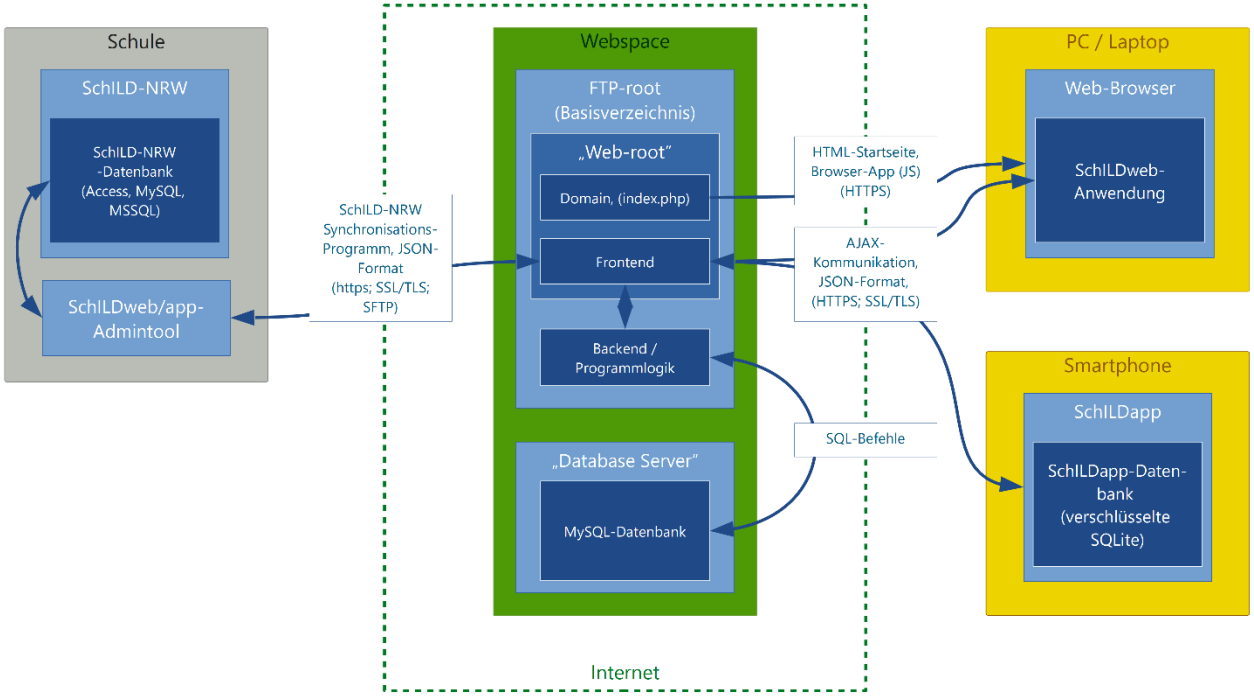
Alle Einstellungen für SchILDweb und SchILDapp werden nicht im SchILD-Hauptprogramm, sondern in einem separaten Administrations-Programm vorgenommen.

Das Admintool kann nur Als SchILD-Administrator unter Angabe von Benutzername und Passwort gestartet werden.

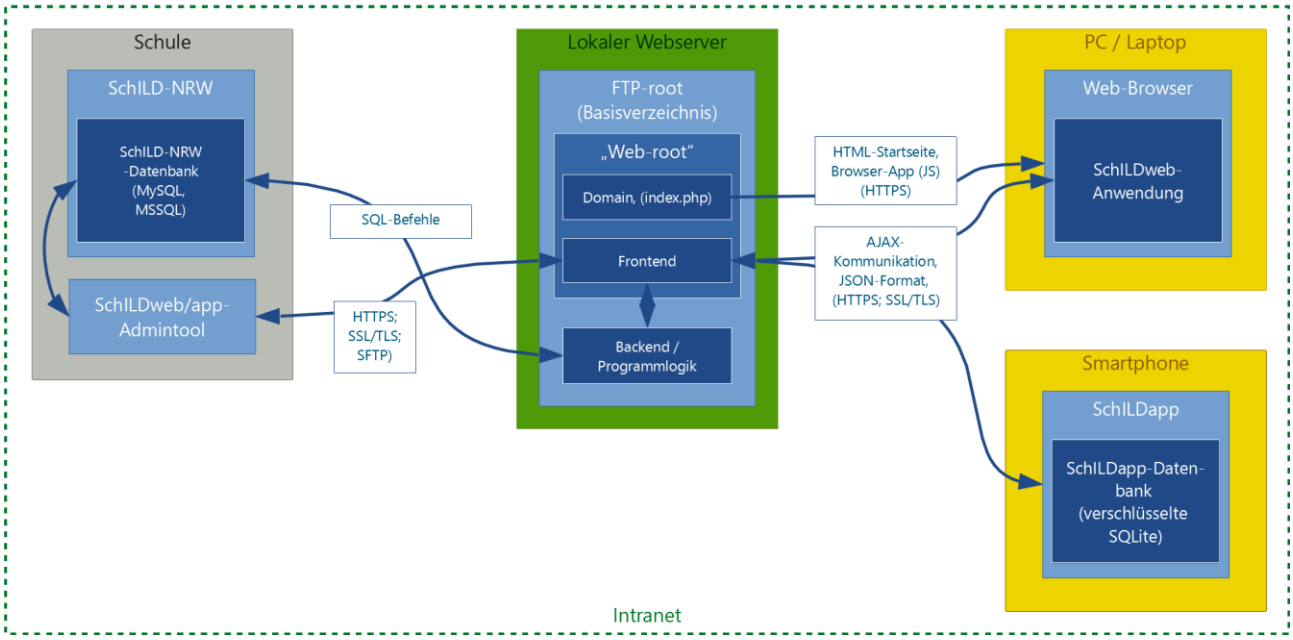
Neben den allgemeinen Verbindungseinstellungen werden hier schul-, klassen- und lehrerspezifische, sowie sicherheitstechnische Einstellungen und Einstellungen zur Datensynchronisation vorgenommen. Hier können bspw. SchILDweb/SchILDapp Nutzer für Funktionen berechtigt oder auch gesperrt und Einstellungen zu Eingabenfristen und Eingabe-Modi gesetzt werden. Weiterhin wird über das Admintool der Datentransfer (Synchronisation zwischen Webdatenbank und SchILD-Datenbank) angestoßen sowie eventuell notwendige Programmupdates (Webserver) durchgeführt.

Kommunikationskonzepte

SchILDweb/SchILDapp bei einem Webhosting Provider



SchILDweb/SchILDapp auf einem lokalen Webserver



SchILDweb/SchILDapp - Installation in einem Rechenzentrum