Sicherheitskonzept efaCloud

Sicherheitskonzept für die Anwendung efaCloud für den Verein -
Stand: 17.01.2022
efaCloud Server 2.3.1_05

Basisdaten

Verein: -
Verantwortlich für den Betrieb des efaCloud Servers: -
Betreiber des Web-Servers: -
URL der efaCloud-Anwendung: localhost
Datum der AVV mit dem Betreiber des Web-Servers: -
efaCloud Version: 2.3.1_05
PHP-Version: 8.0.14
PHP-Erweiterungen: Core, date, libxml, openssl, pcre, zlib, filter, hash, json, Reflection, SPL, session, standard, sodium, cgi-fcgi, mysqlnd, PDO, calendar, ctype, mbstring, FFI, fileinfo, ftp, gettext, iconv, imagick, exif, mysqli, pdo_mysql, Phar, posix, readline, shmop, sockets, sysvmsg, sysvsem, sysvshm, tokenizer, zip, Zend OPcache,
Datenbank Version: Client info = mysqlnd 8.0.14, Server info = 8.0.27-0ubuntu0.20.04.1, Server version = 80027
Datenbankuser Kennwortlänge: 8
Backup-Strategie: Tägliche Sicherung aller Tabellendaten für 10 Tage, alle 10 Tage Sicherung der ältesten täglichen Sicherung für 100 Tage
Nutzerkennwort-Sicherheit: 8 – 32 Zeichen aus drei Gruppen der folgenden vier Gruppen enthalten sein: Ziffern, Kleinbuchstaben, Großbuchstaben, Sonderzeichen. Zulässige Sonderzeichen sind !"#$%&'*+,-./:;<=>?@[\]^_`{|}~

Technische Sicherheit

Technischer Aufbau

Die Anwendung besteht aus einem ausführbaren PHP-Skript, welches auf eine MySQL Datenbank zugreift und einem Dateisystem für die Code-Ablage, Konfiguration und Überwachung.

Das Dateisystem ist bis auf ausgewählte Verzeichnisse nicht von außen lesbar. Lesbar sind ausschließlich die Verzeichnisse, auf die unmittelbar über Browser oder API zugegriffen wird: api, forms, js, license, pages, public, resources.

Sämtliche anderen Verzeichnisse sind sowohl durch Berechtigungsvergabe, als auch durch Hinterlegung einer .htaccess Datei für den Zugriff von außen gesperrt.

Die Anwendung verwendet außer den Standardmodulen von PHP kein Framework.

Datenbanksicherheit

Der technische Nutzer, der für den Zugriff der Anwendung auf die Datenbank verwendet wird, ist in der Konfiguration hinterlegt. Diese Konfiguration befindet sich im nicht zugänglichen Bereich des Dateiverzeichnisses und ist nicht im Klartext abgelegt, sondern zusätzlich „versteckt“ durch einfache symmetrische Verwürfelung und anschließende base64 Kodierung. Das schützt zwar nicht vor echten Hackern, erfordert aber einen Zugang zum geschützten Server-Bereich und ist dadurch abgesichert.

Lastbegrenzung

Die Anwendung hat einen eingebauten Lastbegrenzer, der maximal 3000 Zugriffe bzw. API-Container und maximal 100 Fehler pro Stunde auf sowohl die PHP Anwendung als auch die API zulässt. Danach wird jeder Zugriff bzw. API-Container abgelehnt.

Anwenderzugriff

Die API und die PHP-Anwendung kapseln alle Datenbankzugriffe, so dass direkte SQL-Statements durch den Anwender nicht möglich sind. Auf der API werden bis zu zehn Transaktionen in einem Container gebündelt, z. B. bei Synchronisation von mehreren Datensätzen.

Der Nutzer wird in der API für jeden Container autorisiert. Bei Verwendung des Browsers wird durch den erfolgreichen Login eine Sitzung aufgebaut, die bei Inaktivität nach 10 Minuten geschlossen wird.

Die Kommunikation erfolgt ausschließlich über HTTPS, um die Daten vor Mitlesen, Verlust und Manipulation zu schützen. Nutzung per HTTP wird in der Servereinstellung blockiert.

efaCloud Server-Anwendung

Menschliche Anwender greifen grundsätzlich über PHP-Formulare oder Seiten auf die Daten zu. Technische Nutzer, wie zum Beispiel ein Bootshaus-PC, können über eine API zugreifen.

Sie autorisieren sich dafür mit einem Kennwort, welches im User-Datensatz als Hash hinterlegt ist. Dazu wird der in PHP

mitgelieferte Hashalgorithmus in Standardeinstellung verwendet.

efaWeb

efaWeb stellt eine Javascript Anwendung innerhalb des efaCloud-Server-Angebotes dar. Sie wird über die Seite pages/bths.php aufgerufen. Die Javascript Anteile liegen komplett im Verzeichis js (s.o.).

efaWeb greift über nicht direkt, sondern über die API auf die Daten zu, so wie es auch der Bootshaus-PC macht. Es gibt keinen direkten Zugriff aus der efaWeb Fahrtenbuchanwendung auf die Datenbank.

Nutzer von efaWeb werden über die API identifiziert und autorisiert, dabei liefert die Seite bths.php, wenn eine Sitzung offen ist, den aktuellen Nutzer an efaWeb, der sich dann nicht mehr autorisieren muss.

Berechtigungskonzept

Die Anwendung efaCloud unterscheidet sechs Rollen, die mit * gekennzeichneten sind privilegierte Rollen, zu denen die Berechtigungen weiter unten namentlich aufgeführt sind. Jede Rolle hat grundsätzlich alle Berechtigungen der zuvor aufgeführten Rolle:

- **anonymous**: der nicht angemeldete Nutzer.
- **guest**: Gastzugriff für Testzwecke
- **member**: Vereinsmitglieder, Zugriff zum eigenen Profil zur Prüfung der im Verein hinterlegten Daten.
- ***bths**: Bootshaus PC zum Eintrage von Fahrten, Schadensmeldungen, Nachrichten an Admin etc.
- ***board**: Vorstandsfunktionen
- ***admin**: Verwalter der Anwendung

Die Berechtigungen im Web sind:

- **anonymous**: Startseite
- **guest**: nicht verwendet.
- **member**: Mein Profil, Startseite, Profil anzeigen, Profil ändern, Abmelden, Bearbeiten, Schadensmeldungen, Nachrichten, Datensatz anzeigen
- **bths**: nicht verwendet.
- **board**: Fahrten, Reservierungen, Fahrtenbuch, Datensatz finden, Datensatz ändern, Datensatz Versionen, API Test, efa Tabelle ausgeben, efaWeb, Verwalten, Nutzer finden, Nutzer anzeigen, Liste ausgeben, Datenstruktur
- **admin**: Tabelle importieren, Fahrtenbücher korrigieren, Nutzer ändern, Workflows/Concessions ändern, Nutzer anlegen, Partner neu/ändern, Sammeltransaktionen, Login token versenden, Konfigurieren, Einstellungen ändern, Farbschema ändern, Datenbank neu aufsetzen, Überwachen, Alle Berechtigungen, Aktivitäten anzeigen, Datenänderungen, Logs und Grafiken, Zugriffsstatistik, efa logs zeigen, efaCloud Datenbank auditieren, efaCloud Sicherheitskonzept, Support / Upgrade, Service / Feedback, efaCloud Hilfe, Versionsupgrade

Die Berechtigungen auf der API-Schnittstelle sind:

- **anonymous**: Fehler melden
- **guest**: Schnittstelle testen, Information abfragen
- **member**: nicht verwendet.
- **bths**: Datensatz anlegen, Datensatz aktualisieren, Datensatz löschen, Datensatz korrigieren, Datensätze lesen, Datensätze lesen, Datensätze lesen, Nutzerkennwort verifizieren, Backup anstoßen, Cronjobs anstoßen, Statistik upload
- **board**: nicht verwendet.
- **admin**: Tabelle anlegen, Tabelle konfigurieren, Tabelle konfigurieren, Tabelle konfigurieren

Die in efa verwendeten Admin-Berechtigungsprofile sind in efaCloud abgelegt um Konsistenz über alle Clients durch eine zentrale Verwaltung sicherzustellen, aber ohne Wirkung. Ein Admin-Zugriff wird immer online geprüft, d.h. ein Bootshaus-PC der offline ist, kann nur durch den lokalen efa-Superadmin verwaltet werden.

Überwachung

Die Anwendung enthält eine umfangreiche Überwachungslogik sowie die Möglichkeit der Auditierung.

Logs

Jede Transaktion auf der API, jeder Login, jeder Fehler und jede Datenänderung und jede Bereitstellung von Listen wird mitgeschrieben. Die entsprechenden Logs sind allerdings nur Nutzern in der Rolle ‚admin' zugänglich, da sie insbesondere im Datenänderungslog auch echte Daten enthält.

Nutzer mit einer Verwaltungsberechtigung müssen darauf hingewiesen werden, dass ihre Aktivität mitgeschrieben und zugeordnet werden kann.

Audit, Cronjobs

Die Anwendung führt regelmäßig „Audits" durch, bei denen die Berechtigungstruktur im Dateiverzeichnis geprüft und ggf. korrigiert wird.

Cron-Jobs dienen zur Datenbank-Kontrolle und erlauben den Versand von Fahrtenbüchern an Mitglieder.

Schnittstellen, Export und Import von Daten

Sämtliche Zugriffe werden per HTTPS ausgeführt. Nur bei der Erst-Installation ist einmalig ein sftp-Zugang erforderlich, um die Installationsdatei im Wurzelverzeichnis zu hinterlegen. Upgrades nutzen auch den Zugang zum efaCloud-Server per HTTPS.

Daten können sowohl über die API als auch über die Benutzeranwendung als Listen exportiert werden. Der Export über die API ist erforderlich für die Synchronisation der Bootshaus-PCs mit dem Server. Der Export als Liste in der Serveranwendung dient Verwaltungszwecken – er wird mit Angabe des exportierenden Nutzers mitgeschrieben und erfordert die Berechtigungsstufe „board".

Daten können sowohl über die API als auch über die Benutzeranwendung als Listen importiert werden. Der Import über die API ist erforderlich für die Synchronisation der Bootshaus-PCs mit dem Server. Der Export als Liste in der Serveranwendung wird für die Wiederherstellung von Backups verwendet und erfordern ‚admin' Rechte.

Verfahren

Um den Datenschutz angemessen sicherstellen zu können, werden die folgenden Verfahren zur Berechtigungsvergabe und Prüfung vereinbart.

Berechtigungsvergabe

Die Vergabe von Berechtigungen erfolgt durch einen Nutzer mit der Berechtigung „admin" nach Prüfung der Funktion des Nutzers im Verein. Die Berechtigung „board" wird dabei nur Funktionsträgern im Verein zugeordnet.

Berechtigungsentzug

Die Berechtigung „board" oder „admin" wird bei Wegfall der Vereinsfunktion vom durch einen Nutzer mit der Berechtigung „admin" auf „member" gesetzt. Der Nutzer wird bei Austritt aus dem Verein in die Berechtigungsstufe „anonymous" gesetzt.

Berechtigungskontrolle

Einmal jährlich werden die Berechtigungen durch den Betreiber der Anwendung überprüft.

Löschkonzept

Eine automatisierte Löschung oder Anonymisierung der Daten findet nicht statt.

Prozesskontrolle

Einmal jährlich wird dieses Sicherheitskonzept aktualisiert und dem Vereinsvorstand zur Kenntnisnahme und Kontrolle auf angemessene Umsetzung vom Betreiber der Anwendung vorgelegt.

Audit

Im Folgenden wird eine Zusammenfassung des aktuellen Zugriffsstatus und das aktuelle Auditergebnis angegeben. Veränderliche Angaben beziehen sich dabei immer auf die letzten 14 Tage, stellen also nur eine Stichprobe dar.

Bei den Datenmengen ist zu beachten, dass versionierte Tabellen (efa2boats, efa2destinations, efa2groups, efa2persons) in der Regel mehr Datensätze als Objekte enthalten, weil ein Objekt wie beispielsweise die Person mehrere Datensätze mit unterschiedlicher zeitlicher Gültigkeit hat.

Dem Verwalter steht diese Überwachungsinformation ebenfalls online zur Verfügung.

Zugriffsstatistik

Zugriffe der letzten 14 Tage über das Web

Als Zugriffsart wird login, init (= Seitenaufrufe), und error (erzeugte Umleitungen auf die Fehlerseite error.php) unterschieden.

Datum	err	login	init
2022-01-16	6	10	222
2022-01-15		2	43
2022-01-14		4	47
2022-01-08	6	8	220
2022-01-07	1	3	101
2022-01-05	1	11	103
2022-01-04	2	2	27
Summe 14 Tage	16	40	763

Zugriffe der letzten 14 Tage über die API

Alex Adminis (#1142, admin), letzte Aktivität: 2022-01-06 19:09:58

Date	requests	requSize	respSize
2022-01-04	207	20240	13419816
2022-01-05	527	56532	36196620
2022-01-06	930	181529	64002917
2022-01-16	196	26128	11964316

Bootshaus am Rhein (#6000, bths), letzte Aktivität: 2021-12-19 22:47:39

Date	requests	requSize	respSize
2022-01-15	9	712	203604

Datenänderungen der letzten 14 Tage

Autor	Modifikationstyp: Anzahl Transaktionen
1142	inserted: 1693, updated: 98, deleted: 4,
6000	updated: 210, inserted: 5,

Namentlich benannte Nutzer

Nutzer mit besonderen Rechten werden mit Namen hier aufgeführt für die Kontrolle des Sicherheitskonzeptes durch den Vereinsvorstand.

Privilegierte Nutzer

Die Nutzer mit privilegierten Rollen sind:

admin: (1142) Alex Adminis
bths: (6000) Bootshaus am Rhein

Nutzer mit efa-Admin Rechten

Die Nutzer mit efa-Admin Rechten sind:

(1142) Alex Adminis: **Workflows** Admins verwalten, Projekte und Fahrtenbücher administrieren, Fahrtenbuch bearbeiten, **Concessions**

Konfigurationsübersicht

Etwas weniger technisch als der Audit Log ist die Zusammenstellung der Parameter, die vom Verwalter konfiguriert werden.

Der zeitliche Abstand zwischen zwei automatischen Download-Synchronisationen in Sekunden. Standard ist 3600 Sekunden.: *3600*
Der zeitliche Abstand zwischen zwei automatischen Änderungschecks in Sekunden. Standard ist 60 Sekunden. Um automatische Änderungschecks abzuschalten bitte 0 eingeben.: *60*
Unterschrift unter Mails, die vom System erzeugt werden: *<p>Dein efacloud-Server.<p>*
Fußzeile unter Mails, die vom System erzeugt werden: *<hr><small>efaCloud © www.nmichael.de</small>*
'no-reply'-Absender der Mails, die vom System erzeugt werden: *efacloud-noreply<noreply@default.efacloud.org>*
Mail-Adresse für den Kopie-Empfänger der Workflowbenachrichtigungen.: *kontakt@default.efacloud.org*
Die Abkürzung, die für Euren Verein verwendet werden soll gegenüber Partnervereinen und für Mail-Kommunikation, kann leer bleiben.: *???*
Wann startet das Fahrtenbuchjahr?: *1*
Information über Boote auf dem Wasser ohne login sichtbar: *on*
Information über nicht verfügbare Boote ohne login sichtbar:
Information über Boote mit Bootsschaden ohne login sichtbar:
Information über Bootsreservierungen ohne login sichtbar:
Fahrten können an Partnervereine weitergegeben werden:
Debug-Informationen mitschreiben für Supportzwecke:
Automatische Abläufe, die als 'cronjobs' angestoßen werden. Ein Job pro Zeile, als 'Tagangabe Typ' z.B. 'M31 persLogbook'.:
W1 monitoring
M31 persLogbook
Bezeichnung des Vereins:
Names dessen, der betriebsverantwortlich ist:
Unternehmen, das die Site betriebt (Hoster):
Datum der AVV Mit diesem Unternehmen (Hoster):

Aktuelles Tagesaudit

Täglich erfasst efaCloud den Zustand in Form eines Audits. Bei Erzeugung des Konzepts wurde ein Audit durchgeführt, dessen Ergebnis hier mit abgedruckt ist.

Auditing 'efaCloud' at 'http://localhost/forms/login.php?fseq=plZLu1', version '2.3.1_05'
Starting audit at: 2022-01-17 19:43:45
Forbidden directories access check ...
  file permissons for all_mails_localhost: drwxrwxrwx.
  file permissons for classes: drwxrwxrwx.
  file permissons for config: drwxrwxrwx.
  file permissons for config/access: drwxrwxrwx.
  file permissons for install: drwxrwxrwx.
  file permissons for log: drwxrwxrwx.
  file permissons for log/backup: drwxrwxrwx.
  file permissons for log/contentsize: drwxrwxrwx.
  file permissons for log/sessions: drwxrwxrwx.
  file permissons for log/uploads: drwxrwxrwx.
  file permissons for pdfs: drwxrwxrwx.
  file permissons for tasks_queue: drwxrwxrwx.
  file permissons for tcpdf: drwxrwxr-x.
  file permissons for templates: drwxrwxrwx.
  file permissons for uploads: drwxrwxrwx.
.htaccess files ok.
Publicly available directories access check ...
  file permissons for api: drwxrwxrwx.
  file permissons for forms: drwxrwxrwx.
  file permissons for js: drwxrwxrwx.
  file permissons for license: drwxrwxrwx.
  file permissons for pages: drwxrwxrwx.

    file permissons for public: drwxrwxrwx.
    file permissons for resources: drwxrwxrwx.
.htaccess files ok.
Framework configuration check ...
users:
    action_links = ["admin: <a href='..\/pages\/nutzer_profil.php?id={#ID}'> - anzeigen<\/a>","admin: <a
href='..\/forms\/nutzer_aendern.php?id={#ID}'> - Profil \u00e4ndern<\/a>","admin:
<a
href='..\/forms\/workflows_aendern.php?id={#ID}&conc=0'> - efa-Berechtigungen \u00e4ndern (Workflows)<\/a>","admin: <a
href='..\/forms\/workflows_aendern.php?id={#ID}&conc=1'> - efa-Berechtigungen \u00e4ndern (Concessions)<\/a>","admin:

<a href='..\/pages\/logintoken_versenden.php?id={#ID}'> - Login Token versenden<\/a>"]
    user_table_name = efaCloudUsers
    user_id_field_name = efaCloudUserID
    user_archive_table_name =
    user_firstname_field_name = Vorname
    user_lastname_field_name = Nachname
    user_subscriptions = false
    user_workflows = true
    user_concessions = true
config:
    app_name = efaCloud
    app_url = https://www.efacloud.org
    changelog_name = efaCloudLog
    parameter_table_name = efaCloudConfig
    forbidden_dirs = all_mails_localhost,classes,config,config/access,install,log,log/backup,log/contentsize,log/sessions,log/uploa
ds,pdfs,tasks_queue,tcpdf,templates,uploads
    public_dirs = api,forms,js,license,pages,public,resources
init:
    max_inits_per_hour = 3000
    max_errors_per_hour = 100
    max_concurrent_sessions = 25
    max_session_duration = 600
history:
    efa2boatdamages = ecrhis
    efa2boatreservations = ecrhis
    efa2boats = ecrhis
    efa2clubwork = ecrhis
    efa2fahrtenabzeichen = ecrhis
    efa2logbook = ecrhis
    efa2persons = ecrhis
    efa2sessiongroups = ecrhis
    efaCloudPartners = ecrhis
    efaCloudUsers = ecrhis
maxversions:
    efa2boatdamages = 20
    efa2boatreservations = 20
    efa2boats = 20
    efa2clubwork = 20
    efa2fahrtenabzeichen = 20
    efa2logbook = 20
    efa2persons = 20
    efa2sessiongroups = 20
    efaCloudPartners = 20
    efaCloudUsers = 20
Configuration:
    db_host = "127.0.0.1"
    db_name = "efaCloud"
    db_user = 4 characters long.
    db_up = 8 characters long.
    synch_period = 3600
    synch_check_period = 60
    mail_subscript = "<p>Dein efacloud-Server.<p>"
    mail_footer = "<hr><small>efaCloud \u00a9 www.nmichael.de<\/small>"
    system_mail_sender = "efacloud-noreply<noreply@default.efacloud.org>"
    mail_schriftwart = "kontakt@default.efacloud.org"
    partners_enabled = ""
    acronym = "???"
    public_onthewater = "on"

public_notavailable = ""
public_notusable = ""
public_reserved = ""
configured_jobs = "W1 monitoring\r\nM31 persLogbook"
db_layout = 3
debug_support = ""
sports_year_start = 1
Verein = ""
Betriebsverantwortlich = ""
Hoster = ""
AVVdatum = ""
Table configuration check ...
efa2autoincrement [3*7],
efa2boatdamages [400*24, hist:ecrhis.20],
efa2boatreservations [15*22, hist:ecrhis.20],
efa2boats [201*45, hist:ecrhis.20],
efa2boatstatus [199*15],
efa2clubwork [1*18, hist:ecrhis.20],
efa2crews [0*33],
efa2destinations [44*20],
efa2fahrtenabzeichen [159*26, hist:ecrhis.20],
efa2groups [0*13],
efa2logbook [2118*80, hist:ecrhis.20],
efa2messages [580*16],
efa2persons [3032*40, hist:ecrhis.20],
efa2sessiongroups [117*14, hist:ecrhis.20],
efa2statistics [6*79],
efa2status [8*12],
efa2waters [215*9],
efaCloudLog [2010*7],
efaCloudPartners [0*9, hist:ecrhis.20],
efaCloudUsers [3*12, hist:ecrhis.20],
in total [9111*501] records * columns in 20 tables.
Users and access rights check ...
Count of privileged roles: bths - 1; board - 0; admin - 1;
Count of non-privileged roles: anonymous - 1; guest - 0; member - 0;
Workflows: @1: Admins verwalten - 1; @4: Projekte und Fahrtenbücher administrieren - 1; @16: Fahrtenbuch bearbeiten - 1;
Concessions:

Backup check...
22 backup files with a total size of 13.5 MByte
Audit completed.