OJS-de.net

# Netzwerkworkshop

## der deutschsprachigen OJS-Dienstleister

**3./4. Dezember 2015, Berlin**

*DOKUMENTATION*

**DFG-Projekt *Nachhaltige OJS-Infrastruktur zur elektronischen Publikation wissenschaftlicher Zeitschriften***

DFG | Freie Universität Berlin | Universitäts-Bibliothek Heidelberg | Universität Konstanz | PKP Public Knowledge Project | open access

OJS-de.net

# Sicherheit & Datenschutz

## Praxisbeispiele CeDiS

**Božana Bokan**

Center für Digitale Systeme,
Freie Universität Berlin

DFG Freie Universität Berlin UNIVERSITÄTS-BIBLIOTHEK HEIDELBERG Universität Konstanz PKP PUBLIC KNOWLEDGE PROJECT open access

# Sicherheit

Auf verschiedenen Ebenen:

- Server- und Netzwerkinfrastruktur
- Software (Webserver, Datenbank, PHP, OJS)
- Nutzer/innen

Maßnahmen:

- Zugriffschutz und -kontrolle
- Rollentrennung
- Passwortschutz
- Wartung
- Datensicherung
- Protokollierung

# Server- und Netzwerkinfrastruktur

- Höchstwahrscheinlich die Aufgabe des Rechenzentrums
- Administrativen Zugriffe ausschließlich innerhalb des universitären Campusnetzes
- Zugriffe sind Verschlüsselt
- Kreis der Benutzer/innen beschränkt
- Firewall-Schutz
- Ein- und ausgehenden Zugriffe nur auf die erforderlichen Ports reduziert
- Regelmäßige Server- und Software-Patches und -Updates
- Regelmäßige Kontrolle von Protokolldateien

# Software

- Webserver, Datenbank, PHP, OJS
- Die einzelnen Bereiche sowie Zugriffe sind von einander getrennt
- Es können nur solche Aktionen durchgeführt werden, für die ausreichende Berechtigungen existieren
- Berechtigungen sind restriktiv und nach dem Minimalprinzip vergeben
- Regelmäßige Patches und -Updates
- Regelmäßige Kontrolle von Protokolldateien

Am Beispiel von OJS:

- Installation
- Konfiguration
- Software an sich
- Wartung
- Nutzung

# OJS-Installation

OJS-de.net

- Jede OJS-Mandanz hat eigenen Webserverbereich und Protokollierung
- SSL-Zertifikat
- Jede OJS-Mandanz hat eigene Datenbank, mit eigener Datenbankkennung
- Nur lokaler Zugriff auf die Datenbank
- Die Verzeichnisse für Programm und Dateien sind getrennt
- Dateienverzeichnis ist über die URL nicht erreichbar, d.h. außerhalb des Web-Verzeichnisses
- Dateien und Verzeichnisse werden mit entsprechenden Benutzerkennungen und Berechtigungen versehen
- Jede OJS-Mandanz hat eine eigene Administratorkennung
- SHA1 Passwortverschlüsselung

# OJS-Konfiguration

Datei config.ini.php:

- Jede OJS-Mandanz hat eigenen Salt für Passwortverschlüsselung
- SSL-Log-In
- CAPTCHA für Registrierung und Kommentierung
- Erlaubte HTML-Elemente in Webformularen
- Validieren der E-Mail-Adresse bevor Log-in möglich

Einstellungen der Website:

- Passwortlänge
- Installieren, Aktualisieren oder Löschen von Plug-Ins durch Zeitschriftenverwalter/innen

Datei php.ini:

- upload_max_filesize, post_max_size, max_execution_time, memory_limit
- error_reporting, log_errors, display_errors = Off
- session.hash_function = 1

# OJS-Software

Die Zuweisung von Rechten erfolgt auf der Grundlage von Benutzer-Rollen → sehr differenziertes OJS-internes Rollenmodel

Zugriffskontrolle berücksichtigt z. B.:

- Kontrolle aller beteiligten Ressourcen,
- Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen,
- Restriktive Dateisystemberechtigungen bei der Upload-Funktion

Zugriffe ausschließlich über die vorgesehenen, abgesicherten Kommunikationspfade (z. B. Zugang auf die Dateien nur über das System)

Kein Zugriff auf die Konfigurationsdatei

OJS-Benutzer/innen können nicht direkt auf die darunter liegende Systeme zugreifen

OJS-Passwörter werden verschlüsselt

SSL-Unterstützung

Kontrolle der Ein- und Ausgabedaten

# OJS-Wartung und -Nutzung

- Regelmäßige Patches und -Updates
- Regelmäßige Kontrolle von Protokolldateien
- Datensicherung
- Schulung der Nutzer/innen (Fehlbedienungen auf ein akzeptables Maß reduzieren)
- Regeln und Kontrollen innerhalb des Redaktionsteams und im Publikationsprozess
- Verantwortungsvoller und sicherer Umgang mit Passwörtern

# Datenschutz (1)

Umgang mit personenbeziehbaren Daten

Protokolldateien (z. B. Webserver-Log-Dateien):

- IP-Adressen anonymisieren, s. z. B. https://www.zendas.de/technik/sicherheit/apache/index.html

OJS-interne Speicherung von IP-Adressen in der Datenbank:

- anonymIP-Plug-In, s. https://github.com/ojsde/anonymIP

OJS-interne Statistiken, nach COUNTER:

- Datenschutz-Option:
  - Anonymisierung von IP-Adressen: kryptografisch, zufällig und täglich neu generierter Salt. Achtung: Salt-Datei aus den Backups auslassen!
  - Nutzer/innen informieren
  - Opt-out-Möglichkeit

Add This bzw. Social Media:

- Shariff-Plug-In, s. https://github.com/ojsde/shariff

# Datenschutz (2)

- Einbindung von JavaScript-Dateien („enable_cdn“ in der Datei config.inc.php)
- Problematische OJS-Plug-Ins, wie z. B. Google Analytics, Piwik
- OJS-Installation-ID an PKP für Statistikzwecke melden („enable_beacon“ in der Datei config.inc.php)

Offene Fragen:

- Log-In-As-Funktion
- Cookies-Information
- Datenschutzerklärung
- Nutzungsbedingungen
- Impressum

# Kontakt

www.OJS-de.net

kontakt@ojs-de.net

Bei Rückfragen zum Vortrag:

Božana Bokan

Freie Universität Berlin, Center für Digitale Systeme

E-Mail: bozana.bokan@cedis.fu-berlin.de