Physik Online

Administration
Sven Köppel <koeppel@th.physik.uni-frankfurt.de>
Mirko Pohland <pohland@stud.uni-frankfurt.de>

CHECKLISTE FÜR DIE VORABKONTROLLE
NACH §7 ABS. 6 HDSG

für die neue Physik Online-Plattform
https://elearning.physik.uni-frankfurt.de
Revision 2, 26.09.2011

GRUNDANGABEN

- zur datenverarbeitenden Stelle (Nr. 1)

  Physik eLearning-Team, zentraler eLearning-Server, elearning.physik.uni-frankfurt.de

- zur Zweckbestimmung (Nr. 2.1)

  Lernplattform „Physik Online“ für den Fachbereich 13 (Physik).

- zur Rechtsgrundlage (Nr 2.3)

  unbekannt

- Zur Art der gespeicherten Daten (Nr. 3)

  Die auf dem Server gespeicherten Daten gliedern sich in 6 Typen (lfd. Nr.):
  1. *öffentlicher eindeutiger Benutzer-Identifikationsname*: HRZ-Benutzername.
  2. *Intentitätsstiftende Stammdaten*: Echter Name und Vorname (freiwillige Angabe)
  3. *Private Stammdaten*: E-Mail-Adresse, sonstige freiwillige Profildaten
  4. *Mit Benutzerdaten unkorrelierte Webserver-Logfiles*: IP-Adresse, Referer, Browser-Kennung, …
  5. *Von der Lernplattform erstellte Daten (nur für den Benutzer)*: Anwesenheit, Nutzungsstatistik
  6. *Von der Lernplattform lernmodulspezifisch erstellte Daten (nur für den Benutzer)*: Lernfortschritt, persönliche Kommentare, ...

  Für Details siehe Anhang mit Zugriffsrechtematrix.

- Zur Schutzbedürftigkeit der Daten, insbesondere bei sensitiven Daten im Sinne von §7 Abs. 4 HDSG oder sonst besonders schutzbedürftigen Daten

  Von Nr. 3 sind alle Daten 1,2,3,4,5,6 schutzbedürftig. Lediglich Daten 1 und 2 sind dem Benutzerkreis der Dozenten zugänglich, wenn Studenten in ihren Veranstaltungen angemeldet sind.

- Zum Kreis der Betroffenen (Nr 4)

  Betroffen sind alle Benutzer des Systems: Studenten des Fachbereich 13, Nebenfächler anderer Fachbereiche sowie Dozenten und Mitarbeiter in der Lehre.

- Zu den zugriffsberechtigten Personengruppen (Nr. 6)

  Die Betroffenen (Nr. 4) gliedern sich in vier Gruppen unterschiedlicher Rechte:
  1. Studenten der Uni Frankfurt (Leserecht, Anmeldung in Kurse)
  2. Dozenten: Verwaltung eigener Kurse, Einsicht in Mitgliedslisten.
  3. Mitarbeiter von Physik Online (ca. 6 Personen): Einsicht in alle Lernmaterialien.
  4. Administratoren von Physik Online (< 6 Personen)

- Zu den Fristen für die Löschung (Nr. 9)

  Vom Webserver erhobene Logdaten (lfd. Nr. 4) werden innerhalb der gesetzlichen Frist anonymisiert bzw. gelöscht.

PRÜFUNG GEGEN RECHTSGRUNDLAGE

- Art der gespeicherten Daten (Nr. 3): Sind von der Rechtsgrundlage gedeckt. IP-Adressen (lfd. Nr. 4) müssen laut Datenschutzgesetzt binnen 3 Tagen nicht rekonstruierbar anonymisiert werden, dies wird technisch umgesetzt.
- Übermittlungen (Nr. 5 und 10): Komplett SSL-verschlüsselt
- Eingrenzung der Zugriffsberechtigten (Nr. 6): Administrationszugriff hat nur eine kleine Gruppe (lfd. Nr. 4).
- Löschfristen (Nr. 9): Siehe oben.

PRÜFUNG DER RECHTE DER BETROFFENEN

- Können Auskünfte, Berechtigungen, Sperrungen und Löschungen durchgeführt werden?

  Benutzer können durch Administratoren aus dem System gelöscht werden. Benutzer können durch Gruppenzugehörigkeit aus dem System gesperrt werden. Es kann jederzeit eine Auskunft über alle gespeicherten Benutzernamen gegeben werden. § 8 Abs. 2 HDSG ist nicht verletzt.

RISIKOFAKTOREN FÜR MISSBRAUCH DER DATEN

Wenn der verwendete Server komprommitiert wurde, befinden sich die Daten im Zugriff. Backups werden auf die gleiche NAS-Speicherinfrastruktur geladen und unterliegen dementsprechend der gleichen Sicherheitsstufe.

BEURTEILUNG DER MÖGLICHEN FOLGEN BEI MISSBRÄUCHLICHER VERWENDUNG DER DATEN

Da wir keine HRZ-Passwörter speichern, ist das Missbrauchspotential beschränkt. Die reinen eLearning-Daten sind für Außenstehende wenig interessant. Die Angabe jeglicher Stammdaten haben wir auf ein Minimum reduziert und auf freiwilliger Basis gestaltet.

ANGABEN ZU DER TECHNIK DES VERFAHRENS

- Zentraler Server elearning.physik.uni-frankfurt.de (IP: 141.2.246.155), mit klassischem LAMP-Stack:

  Ubuntu Server LTS
  Apache-Webserver 2.2
  PHP
  MySQL-Datenbank

  auf dieser Plattform läuft die

  Lernplattform ILIAS (www.ilias.de)

- Jede Kommunikation zu Clienten erfolgt SSL-Verschlüsselt. Die Authentifikation zum HRZ erfolgt entweder über ein noch nicht näher spezifiziertes geeignetes Protokoll (z.B. Kerberos).

ABGLEICH DER RISIKOFAKTOREN

- *Zum HRZ-Account*: In Anbetracht des Mehrwertes für den Benutzer, sich mit seinen gewohnten Daten anmelden zu können, ist das Risiko so groß wie bei jeder anderen Lernplattform, dass mit den im Angriffsfalle gewonnen Daten Missbrauch gestaltet werden kann.
  Die Alternative lautet, auf HRZ-Login zu verzichten, was neben Bequemlichkeitsverlust erfordert, neue Benutzer- und diesmal auch Passwörter zu speichern.

- *Zur Lernplattform:* Der Nutzen einer eigenen Lernplattform wiegt die Risiken der darin gespeicherten Daten auf.