Physik Online

Administration
Sven Köppel, 19.09.2011

CHECKLISTE FÜR DIE VORABKONTROLLE NACH §7 ABS. 6 HDSG

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

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 Studenten des Fachbereich 13 (Physik) und Nebenfächler

- zur Rechtsgrundlage (Nr 2.3)

  zum Login werden HRZ-Benutzername und Passwort abgefragt. Die Motivation dafür ist die Authentifikation der Besucher als Studenten und Mitarbeiter der Uni Frankfurt.

- Zur Art der gespeicherten Daten (Nr. 3)

  Der Benutzername (HRZ-Name) wird zur weitergehenden Identifikation in einer lokalen MySQL-Datenbank gespeichert.
  Ferner werden Zugriffe auf den Webserver in Form von anonymisierten Logdateien gespeichert. Letztere dienen aber nur der Fehleranalyse und sind keine Nutzdaten des Systems.

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

  Insbesondere das HRZ-Benutzerpasswort ist schutzbedürftig. Selbiges wird auf dem Physik eLearning-Serverbetrieb nicht zwischengespeichert, sondern komplett verschlüsselt an die zentralen Authentifikationsmechanismen des HRZ weitergereicht.

- Zum Kreis der Betroffenen (Nr 4)

  Betroffen sind die Benutzer des Systems, die sich per HRZ-Account einloggen. Dies sind im Allgemein Studenten und Mitarbeiter der Uni Frankfurt.

- Zu den zugriffsberechtigten Personengruppen (Nr. 6)

Durch Authentifikation via HRZ-Account erhalten diese Personengruppen Lesezugriff zu den Materialien der Plattform. Lehrenden werden weitergehende Rechte zur Verwaltung von Lernressourcen gewährt.

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

  Die erhobenen Logdaten des Webservers werden innerhalb von 8 Wochen gelöscht. Sie sind mit den HRZ-Benutzerdaten nicht gekopppelt.

PRÜFUNG GEGEN RECHTSGRUNDLAGE

- Art der gespeicherten Daten (Nr. 3): HRZ-Benutzername, Logfiles
- Übermittlungen (Nr. 5 und 10): Komplett SSL-verschlüsselt
- Eingrenzung der Zugriffsberechtigten (Nr. 6): Physik Online-Team
- Löschfristen (Nr. 9): Keine Fristen für HRZ-Benutzernamen, Logfiles binnen 8 Wochen

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

Folgende Worst-Case-Szenarien in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit sind vorstellbar:

- **Totalkompromittierung des Servers**. In diesem Fall liegt ggf. der für HTTPS verwendete SSL-Private Key dem Angreifer offen und jeglicher Datenverkehr kann mitgeschnitten werden. Auf diese Weise werden die Sicherheitsmaßnahmen des Systems unterhöhlt und der Angreifer kommt in den Besitz aller sich zum Zeitpunkt der Kompromittierung anmeldenden HRZ-Benutzerdaten (Benutzername und Passwort), sofern sie sich zu diesem Zeitpunkt neu per Passwort anmelden und nicht bestehende Anmeldecredentials (Cookie-Authentifikation) nutzen.

Dieses Angriffsszenario ist für jedes Computersystem denkbar und gehört zu dem Risiko, was bei der Nutzung von elektronischen Authentifikationssystemen in Kauf genommen wird.

BEURTEILUNG DER MÖGLICHEN FOLGEN BEI MISSBRÄUCHLICHER VERWENDUNG DER DATEN

Gemäß obigem Szenario würde ein Angreifer eine Liste mit Zuordnung von HRZ-Benutzernamen zu HRZ-Benutzerpasswörtern erhalten. Anhand dieser Daten kann er sich im Namen der betroffenen Studenten bei jedem Universitätsdienst anmelden, der HRZ-Authentifikation erlaubt, also etwa QIS/HLS, andere Lernplattformen, etc.

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 Anmeldung zum HRZ erfolgt über LDAP.

ABGLEICH DER RISIKOFAKTOREN

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.