Zusammenfassung der Untersuchung von QIS-POS durch ZENDAS

Im Auftrag der HIS GmbH hat ZENDAS, die Zentrale Datenschutzstelle der baden-württembergischen Universitäten, das Produkt QIS-POS unter sicherheitstechnischen Aspekten untersucht.

QIS-POS ermöglicht es Hochschulen, ihren Mitgliedern einen Zugriff auf das Prüfungsverwaltungssystem POS über das Internet einzuräumen. Studierende können ihre Prüfungen anmelden und Prüfungsleistungen einsehen. Prüferinnen und Prüfer sind mittels der Web-Schnittstelle in der Lage, Prüfungsleistungen zu verbuchen.

QIS-POS ist eine in Java geschriebene Anwendung, die auf dem Tomcat-Applikationsserver aufsetzt. Zur Steigerung der Performance kann ein Apache-WWW-Server vorgeschaltet werden, der die HTTPS-Verarbeitung übernimmt und statische Inhalte (Bilder) bereitstellt.

QIS-POS greift direkt auf die Produktionsdatenbank der Prüfungsverwaltung zu. Dies ist ein Novum, da bislang in solchen Situationen der Einsatz einer Schattendatenbank empfohlen wurde. Wegen der von QIS-POS angebotenen Funktionen (Prüfungsanmeldung und Notenverbuchung) erfordert die Anwendung aber direkt oder indirekt Schreibzugriff auf die Datenbank der Prüfungsverwaltung. Der Einsatz einer Schattendatenbank würde daher ein komplexes Replikationsprotokoll erfordern, welches parallele Änderungen an beiden Datenbanken zusammenführen kann und potentielle Konflikte auflöst.

Außerdem müsste auch die Schattendatenbank besonders gegen unberechtigten Zugriff geschützt werden, da sie für die Prüfung der Vorleistungen in erheblichem Umfang personenbezogene Daten der Studierenden enthielte. Diese Problematik ließe sich nur dadurch vermeiden, dass die Überprüfung der Prüfungsvoraussetzungen komplett unter völlig neuen Gesichtspunkten reimplementiert würde. Bezüglich der Komplexität des Replikationsprotokolls wäre damit allerdings kein Vorteil erlangt.

ZENDAS – Zentrale Datenschutzstelle der baden-württembergischen Universitäten
70174 Stuttgart – Breitscheidstr. 2
Tel. 0711/121-3690
Fax: 0711/121-3688
E-Mail: info@zendas.de
Internet: www.zendas.de

Vor diesem Hintergrund erscheint es vertretbar, für die QIS-POS-Anwendung auf den Einsatz einer Schattendatenbank zu verzichten. Das Augenmerk sollte sich ganz auf die Sicherung der QIS-POS-Anwendung selbst und ihres Betriebes konzentrieren. Insofern sieht ZENDAS QIS-POS nicht als Sicherheitsrisiko für die Prüfungsdatenbank, sondern als Firewall-Komponente und Application Level Gateway für den Zugriff auf die Datenbank im geschützten Verwaltungsnetz aus dem Internet.

Aus diesem Grund entwickelte ZENDAS für den Einsatz von QIS-POS ein Bedrohungsmodell, das als Grundlage weiterer Untersuchungen diente. Typische Angriffsverfahren auf Web-Anwendungen werden beschrieben und daraus Gegenmaßnahmen entwickelt.

Da die QIS-POS-Anwendung in vielen Fällen auf drei getrennten Rechnersystemen (Apache-Server, Tomcat-Server, Datenbank-Server) läuft, beschreibt ZENDAS Maßnahmen, um die Kommunikation der Systeme untereinander zu sichern und so einen verteilten Einsatz zu ermöglichen. Ebenso werden praktische Empfehlungen ausgesprochen, um im Rahmen üblicher Administrationskonzepte die Sicherheit der Betriebssysteme und Basisanwendungen der einzelnen Komponenten zu erhöhen.

Eine Untersuchung der QIS-POS-Softwarearchitektur wurde durchgeführt, um mögliche Problemstellen zu identifizieren und HIS die Möglichkeit einzuräumen, durch defensive Programmierung Risiken zu vermeiden. Bei den Untersuchungen wurden in freigegebenen, für den Produktionseinsatz vorgesehenen Anwendungsteilen keine Schwachstellen entdeckt, die so gravierend waren, dass sie aus der Sicht von ZENDAS einen Einsatz verhindern. In nicht für den Produktionseinsatz bestimmten Komponenten sowie in einigen noch nicht freigegebenen Anwendungsteilen wurden jedoch Fehler entdeckt. Die Analysen beschränkten sich ausschließlich auf QIS-POS, so dass diese Aussagen nicht auf andere QIS-Anwendungen übertragbar sind.

Konkret identifizierte Schwächen in QIS-POS wurden von der HIS GmbH umgehend behoben. Eine Berücksichtigung der ZENDAS-Empfehlungen, die zwar nicht unmittelbar Sicherheitsprobleme verhindern, aber den Umfang des sicherheitskritischen Kerns von QIS-POS verkleinern und ganz allgemein die Wartbarkeit erhöhen, wird von HIS geprüft. Ferner ergänzte die HIS GmbH ihre interne Entwicklerdokumentation, um ihre Programmierer ausdrücklich auf weitere Sicherheitsrisiken hinzuweisen, die bislang wegen sorgfältiger Programmierung zwar noch nicht auftraten, die aber zwangsläufig mit der Servlet-basierten Softwarearchitektur verknüpft sind. So wird sichergestellt, dass die aus der ZENDAS-Untersuchung gewonnenen Erkenntnisse auch langfristig umgesetzt werden.

ZENDAS geht nach den Untersuchungen und aufgrund der positiven Zusammenarbeit mit der HIS GmbH davon aus, dass QIS-POS dem gesteckten Ziel als Firewall-Komponente gerecht wird. Obgleich die ZENDAS-Analysen nicht die notwendige Tiefe hatten, um das Fehlen von Sicherheitsproblemen nachweisen zu können, zeigte sich dennoch, dass die HIS GmbH in Sicherheitsfragen weitaus sorgfältiger vorgeht als die meisten Entwickler vergleichbarer Web-Anwendungen, sowohl im Hochschulumfeld als auch für Web-basierte Anwendungen im Dienstleistungssektor.

Aus sicherheitstechnischer Sicht hat ZENDAS daher keine Bedenken, was den Einsatz von QIS-POS in einer sorgfältig gewarteten Umgebung angeht, insbesondere wenn die Firma HIS den eingeschlagenen Weg weiter verfolgt.