zentraler informatik dienst

universität wien

Policy

Web Single Sign-on

Genehmigt durch: Ulf Busch, CIO

Gültig ab: 01.02.2012

Version: 1.0

1. Zweck

Zweck ist die Standardisierung des Anmeldens und Abmeldens an/von Web-Applikationen bzw. geschützten Web-Services. Diese Policy soll bei der Einführung von web-basierten Anwendungen durch den Zentralen Informatikdienst und möglichst auch von anderen Einrichtungen berücksichtigt werden bzw. als Kriterium in Pflichtenhefte/Leistungskataloge aufgenommen werden.

2. Anwendungsbereich

Anmelden und Abmelden an/von Web-Applikationen bzw. geschützten Web-Services.

3. Policy

Als Ziel soll langfristig angestrebt werden, dass alle Web-Applikationen bzw. geschützten Web-Services des ZID die Anmeldung über SAML V2.0 (oder höher) vornehmen. Es werden andere Einrichtungen der Universität angehalten, sich diesem System anzuschließen.

Begründung

Mit SAML ist u. a. standardbasiertes Web Single Sign-on möglich. Damit kommen wir einem oft gehegtem Wunsch nach. Wichtiger ist jedoch die Vorbeugung vor Phishing-Angriffen. Derzeit gibt es an der Universität Wien eine Vielzahl von Login-Seiten mit unterschiedlichem Aussehen. So ist es schwer zwischen original Login-Seiten der Universität Wien und Phishing-Seiten zu unterscheiden. Hinzu kommt, dass bei jedem Service mit eigenem Login im Fall eines Einbruchs Passwörter erlangt werden können, während sich bei SAML die Angriffsfläche auf nur einen einzigen Server reduziert.

Bei Web-Applikationen bzw. geschützten Web-Services, die die Anmeldung über SAML vornehmen, soll gänzlich auf Logout/Abmelden-Links verzichtet werden, sofern dies technisch möglich ist. Stattdessen soll der Hinweis „Um sich sicher von den Anwendungen der Universität Wien abzumelden, schließen Sie bitte Ihren Webbrowser“ o. ä. an prominenter Stelle platziert werden. Hintergrundinformationen und verwandte Tipps dazu werden in den ZID-Webspace aufgenommen.

Begründung

Das Verhalten eines Logout-Links in einem Web Single Sign-on System müsste eindeutig und für die Benutzer leicht verständlich sein. Dies ist fast nicht zu gewährleisten. Eine in allen Fällen funktionierende Single-Logout-Lösung ist nicht realisierbar. Der Verzicht auf Logout/Abmelden-Links sowie das Schließen des Webbrowsers nach Beendigung der Arbeit ist jedoch eindeutig und vermittelbar.

Für Supportleistungen ist oft ein Wechsel der Identität notwendig. Dies ist in einer solchen Single Sign-on-Umgebung ohne Logout-Buttons schwierig. Für diese Aufgabe sollen in den Applikationen, so weit wie möglich, Hilfestellungen und alternative Verfahren geboten werden.

4. Abgrenzung

Client-Applikationen sowie Logins am Personalcomputer sind nicht Teil dieser Policy. Eine Policy für diese Bereiche wird gesondert ausgearbeitet.

5. In Kraft treten

Diese Policy tritt per 01.02.2012 in Kraft.

6. Begriffserklärung

SAML..... Security Assertion Markup Language