Sicheres Single Sign On ins EJPD SSO Portal

Security / Betreuer: Peter Andres (peter.andres@isc-ejpd.admin.ch)
Projektpartner: Informatik Service Center ISC-EJPD, Bern / Experte: Gerhard Hassenstein

Am Anfang stand eine Vision: Mitarbeiter der Ämter des EJPD verwenden für das Log-in an ihrer Arbeitsstation ihre Smartcard. Nach dem Log-in ist der Benutzer sowohl für die Büroautomatisierungsumgebung als auch im Portal authentisiert (Single Sign On für beide Umgebungen). Die Autorisierung soll wie bis anhin beibehalten werden.

Ausgangslage

Das SSO Portal (Single Sign On Portal) EJPD bildet die zentrale Sicherheitsarchitektur und -infrastruktur des ISC-EJPD. Nach erfolgreicher starker Authentisierung von Fachanwendungsbenutzern stellt es sämtliche erlaubten Anwendungen über das Web zur Verfügung. Im Verlaufe des Jahres 2013 wird die Verwendung von SmartCards zur Authentisierung auch für die Büroautomatisierung eingeführt.

Die Masterthesis untersuchte in einer Studie, wie ein sicherer Single Sign On zwischen Portal und Büroautomatisierung erfolgen kann.

Vorgehen

In 5 Schritten wurde vorgegangen:

1. Anforderungen Festhalten (Pflichtenheft)
2. Lösungsvarianten Entwickeln und Beurteilen
3. Variante mit Proof of Concept (POC) verifizieren
4. Risiken und Massnahmen definieren
5. Ausblick für eine Umsetzung

Lösungsvarianten

Ein Single Sign On zwischen den zwei Umgebungen bedingt einen Trust zwischen ihnen. Grundsätzlich sind dabei beide Trustrichtungen vorstellbar. Insgesamt wurden in der Thesis acht Lösungsvarianten erarbeitet un beurteilt.

Proof of Concept

Für den POC wurde eine Integration über Kerberos gewählt, das SSO Portal traut der Büroautomatisierung. Die Herausforderung an diesem Ansatz war, dass das SSO Portal nur den Authentisierungen trusten darf, die mit der SmartCard durchgeführt wurden. Im Kerberos-Standard ist das nicht vorgesehen, so dass auf Microsoft spezifische Erweiterungen zugegriffen werden mussten. Für den Authentiseirungsservice des Portales wurde ein Plugin in Java entwickelt, das diese Erweiterung in Java auswertet und den Single Sign On nur zulässt, falls mit der SmartCard authentisiert wurde.

Für den POC wurde eine komplette Testumgebung aufgebaut, die aus 8 virtuellen Maschinen bestand:

- Router
- Win2008R2
- Win7 32Bit
- Win7 64 Bit
- Analysesystem mit Wireshark
- Testserver mit spnego.soruceforge.net

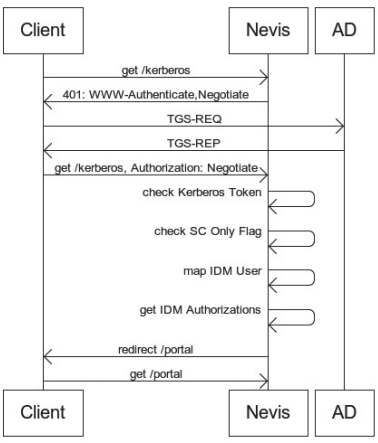
Ergebnis

Die für den POC gewählte Variante konnte erfolgreich verifiziert werden. Der Autor freut sich, dass die in der Studie erarbeiteten Ergebnisse eine gute Chance haben, im nächsten Jahr verwendet zu werden. Für eine produktive Umsetzung wurden inbesondere auch in den Schritten vier (Risiken und Massnahmen definieren) und fünf (Ausblick für eine Umsetzung) aufgezeigt, was für eine produktive Umsetzung zu beachten ist.

Markus Maeder

markus.maeder@oase.ch

Vorgehen in 5 Schritten



Der Kerberos-Trust wird nur akzeptiert, wenn eine starke Authentisierung verwendet wurde (check SC only flag)