Anhang 4

Kriterienkatalog für die Anerkennung von alternativen Plattformen

Inhaltsverzeichnis

1 Zweck und Inhalt

Der vorliegende Kriterienkatalog spezifiziert die Anforderungen an Plattformen für alternative Übermittlungsverfahren im Hinblick auf das Anerkennungsverfahren für derartige Plattformen.

2 Begriffe

2.1 Anbieter

Der Anbieter einer Plattform ist diejenige Organisation, die diese Plattform Dritten (Benutzern) zur professionellen Nutzung zur Verfügung stellt. Diese Organisation kann ein Privatunternehmen oder eine Behörde sein.

2.2 Plattform

Eine Plattform besteht aus einer Softwareanwendung sowie allen weiteren Software-, Hardware- und Netzwerkkomponenten, die erforderlich sind, um die Softwareanwendung lauffähig und zugreifbar zu machen.

3 Anforderungen an die Informationssicherheit

3.1 Grundanforderungen für Privatunternehmen

Die Informationssicherheit ist durch eine der folgenden Methoden zu gewährleisten:

a) Durch Einrichtung, Implementierung, Betrieb, Überwachung, Überprüfung, Wartung und Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements). Der Geltungsbereich des ISMS muss alle diejenigen Organisationseinheiten des Anbieters umfassen, die rechtlich, administrativ und betrieblich für das alternative Übermittlungsverfahren verantwortlich sind. Eine Beschränkung des Geltungsbereichs auf den rein technischen Betrieb der Plattform durch einen internen oder externen IT-Dienstleistungserbringer ist nicht zulässig.

Die Wirksamkeit und Angemessenheit des ISMS muss durch die Vorlage des durch eine Zertifizierungsstelle ausgestellten Zertifikats, das die Zertifizierung des ISMS nach ISO/IEC 27001:2005 bescheinigt, nachgewiesen werden. Die Zertifizierungsstelle muss durch die Schweizerische Akkreditierungsstelle (SAS) für die Durchführung von ISO/IEC 27001:2005 Audits akkreditiert sein.

Für die Aufrechterhaltung der Anerkennung sind die Auditberichte der jährlichen Überwachungs- bzw. Rezertifizierungsaudits dem BJ jeweils unaufgefordert vorzulegen. Bei Entzug der Zertifizierung nach ISO/IEC 27001:2005 durch die Zertifizierungsstelle entzieht das EJPD dem Privatunternehmen die Anerkennung, sofern der Nachweis der Informationssicherheit nicht mit der Methode b) erbracht werden kann.

b) Durch die Zertifizierung des ISMS nach einem anderen, zu ISO/IEC 27001:2005 äquivalenten Standard. In diesem Fall müssen die folgenden Bedingungen erfüllt sein:

- **Die unter Buchstabe a) genannten Anforderungen an den Geltungsbereich des ISMS gelten unverändert.**
- **Die Wirksamkeit und Angemessenheit des ISMS nach dem äquivalenten Standard muss durch die Vorlage des durch eine Zertifizierungsstelle ausgestellten Zertifikats**

nachgewiesen werden. Die Zertifizierungsstelle muss durch die SAS, die Eidgenössische Finanzmarktaufsicht (FINMA) oder die Schweizerische Nationalbank (SNB) akkreditiert sein.

- **Die Gleichwertigkeit des äquivalenten Standards mit ISO/IEC 27001:2005 muss durch eine Zertifizierungsstelle bestätigt werden, die durch die SAS für die Durchführung von ISO/IEC 27001:2005 Audits und gleichzeitig durch die FINMA oder die SNB für die Durchführung von Audits nach dem äquivalenten Standard akkreditiert ist.**
- **Die Zertifizierungsstelle, welche die Äquivalenz prüft, wird auf Vorschlag des Anbieters durch das BJ bestimmt. Dieses lehnt den Vorschlag nur aus wichtigen Gründen ab.**
- **Die unter Buchstabe a) genannten Anforderungen an die Aufrechterhaltung der Anerkennung gelten unverändert, wobei der Standard ISO/IEC 27001:2005 durch den äquivalenten Standard zu ersetzen ist.**

3.2 Grundanforderungen für Behörden

Ist der Anbieter der Plattform eine Behörde, kann auf die formale Zertifizierung durch eine akkreditierte Zertifizierungsstelle verzichtet werden, nicht aber auf das ISMS nach ISO/IEC 27001:2005. In einem solchen Fall ist die Wirksamkeit und Angemessenheit des ISMS durch Vorlage des Berichts zum formalen internen ISMS Audit gemäss Klausel 6 von ISO/IEC 27001:2005 nachzuweisen. Der Auditbericht darf keine Befunde enthalten, die eine Zertifizierung ausschliessen. Hinsichtlich der Prinzipien der Auditierung, der Durchführung des Audits sowie der Kompetenzen und Erfahrung des Auditors müssen die Leitlinien von ISO 19011:2011 (Guidelines for auditing management systems) und ISO/IEC 27007:2011 (Information technology – Security techniques – Guidelines for information security management systems auditing) eingehalten werden. Das Audit muss mindestens einmal pro Jahr wiederholt werden. Der jeweilige Auditbericht ist dem BJ unaufgefordert vorzulegen. Kommen die Auditberichte zur Schlussfolgerung, dass das ISMS nach ISO/IEC 27001:2005 kritische Abweichungen besitzt und werden diese nicht in der durch den internen Auditor festgelegten Frist wirksam beseitigt, entzieht das EJPD der Behörde die Anerkennung.

Verwendet eine Behörde einen zu ISO/IEC 27001:2005 äquivalenten Standard, so gelten die Regeln nach Abschnitt 3.1. b), ausser dass eine formale Zertifizierung für Behörden nicht vorgeschrieben ist. Die Wirksamkeit und Angemessenheit des ISMS ist wie oben beschrieben durch Vorlage des Berichts zum formalen internen ISMS Audit gemäss dem zu ISO/IEC 27001:2005 äquivalenten Standard nachzuweisen.

3.3 Zusatzanforderungen für Privatunternehmen und Behörden

Die in den nachfolgenden Buchstaben a), b) und c) beschriebenen Anforderungen sind Ergänzungen der Auditkriterien nach ISO/IEC 27001:2005 oder des dazu äquivalenten Standards gemäss Abschnitt 3.1. b). Massnahmen zur Erfüllung dieser Auditkriterien dürfen bei der Risikobeurteilung im Rahmen der Einrichtung des ISMS nicht ausgeschlossen werden. Das muss bei der Formulierung der Risikoakzeptanzkriterien entsprechend berücksichtigt werden.

a) Management des Betriebs und der Kommunikation

- **Entwicklungs-, Test- und Produktionsplattformen müssen voneinander getrennt werden.**

- **Das Netzwerk muss segmentiert werden. Die Server für den Betrieb von Plattformen müssen entsprechend ihrem Schutzbedarf über die Netzwerksegmente verteilt werden.**
- **Elektronische Nachrichten dürfen grundsätzlich nur in verschlüsselter Form übermittelt und gespeichert werden. Eine End-zu-End Verschlüsselung ist nicht erforderlich. Für die Weiterleitung von elektronischen Nachrichten ist es hinreichend, wenn der Kommunikationskanal gesichert ist. Ist eine Speicherung von elektronischen Nachrichten in verschlüsselter Form nicht möglich, so muss das aus dieser technischen Schwachstelle resultierende Risiko für eine durchgängige Informationssicherheit auf der Basis der Risikobeurteilung im Zentrum des ISMS gemäss Abschnitt 3.1 bzw. 3.2 mit angemessenen und wirksamen organisatorischen Massnahmen (z.B. Regelung der Verantwortlichkeiten, Arbeitsverfahren und Prozesse, Sensibilisierung, Ausbildung und Training der betroffenen Mitarbeitenden) auf ein Restrisiko reduziert werden, das mit den Risikoakzeptanzkriterien des Anbieters konsistent ist.**
- **Bei Verwendung von Passwörtern darf der Anbieter diese nicht auf Dauer speichern oder in Logfiles protokollieren. Ist die Speicherung der Passwörter von technischen Benutzern unvermeidbar, müssen diese Passwörter auf eine andere Weise gleichwertig und nachweislich wirksam geschützt werden.**
- **Die eingesetzten kryptografischen Verfahren und Systeme müssen dem Stand der Technik entsprechen und sich an der aktuellen Bedrohungslage orientieren. Vorzugsweise sind standardisierte Verfahren und Systeme einzusetzen, wie sie etwa in der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 6. Januar 2010 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen empfohlen werden.**
- **Um "Offline Password Guessing'' zu verhindern, ist für die Übertragung eine Nachrichtenverschlüsselung mit Schlüsseln, die von Passwörtern abgeleitet werden, nicht zugelassen.**
- **Die Stärke der eingesetzten kryptografischen Verfahren und Systeme muss im Rahmen einer ganzheitlichen Sicherheitsarchitektur vollständig und nachvollziehbar beschrieben sowie periodisch überprüft und gegebenenfalls angepasst werden.**

b) Zugriffskontrolle

- **Der Zugriff auf elektronische Nachrichten in Übermittlung darf nur über starke Authentifikationsverfahren (z.B. digitale Zertifikate oder persönliche Tokens) erfolgen. Dabei sind starke Authentifikationsverfahren im Sinne der Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 2, Abschnitt 5.3, zu verstehen. Insbesondere darf die Authentifikationsinformation nicht im Klartext übertragen werden, um nicht verwundbar gegenüber Abhorchungs- und Wiedereinspielungsangriffen zu sein.**
- **Werden im Authentifikationsverfahren Passwörter eingesetzt, müssen diese immer über verschlüsselte Verbindungen übertragen werden (z.B. im Rahmen einer SSL/TLS Session). Werden im Authentifikationsverfahren ausschliesslich Passwörter eingesetzt, müssen diese in Bezug auf die Passwortstärke den Anforderungen der Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 1, Abschnitt 2.4, genügen. Auf eine zeitliche Beschränkung der Gültigkeit von Passwörtern kann verzichtet werden.**

c) Beschaffung, Entwicklung und Wartung von Plattformkomponenten

- **Server, die vom Internet her erreichbar sind, müssen bedarfsgerecht gehärtet sein. Dazu sollten Best Practices beigezogen werden, wie sie z.B. das Center for Internet Security (CIS) mit den Security Configuration Benchmarks zur Verfügung stellt.**
- **Die bekannten Angriffe gegen Web-Anwendungen, wie sie z.B. vom Open Web Application Security Project (OWASP) dokumentiert werden, müssen erfolgreich abgewehrt werden können.**

4 Anforderungen an das IT Service Management

4.1 Grundanforderungen

Für den zuverlässigen Betrieb von Plattformen muss nachgewiesen werden, dass die folgenden Betriebsprozesse dokumentiert, eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert werden:

- **Service Lieferprozesse**
  - **Management von Serviceniveaus**
  - **Service Berichtswesen**
  - **Servicekontinuitäts- und -verfügbarkeitsmanagement**
  - **Budgetierung und Verrechnung von Services**
  - **Kapazitätsmanagement**
- **Prozesse zum Beziehungsmanagement**
  - **Pflege der Beziehung zwischen Leistungserbringer und Kunden**
  - **Lieferantenmanagement**
- **Prozesse zur Lösung von Störungen und Problemen**
  - **Behandlung von Störungen (Vorfällen)**
  - **Behebung von Problemen**
- **Steuerungs- und Überwachungsprozesse**
  - **Konfigurationsmanagement**
  - **Veränderungsmanagement**
  - **Freigabe- und Bereitstellungsmanagement**

Die Betriebsprozesse müssen sich an den internationalen Standards ISO/IEC 20000-1:2011 (Information technology – Service management – Part 1: Service management system requirements) und ISO/IEC 20000-2:2005 (Information technology – Service management – Part 2: Code of practice) oder an vergleichbaren Standards orientieren. Eine entsprechende Zertifizierung ist erwünscht aber nicht erforderlich.

Zusätzlich muss ein professioneller Service Desk eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert werden, der sich z.B. an der IT Infrastructure Library (ITIL) orientiert.

4.2 Verfügbarkeit

Die Verfügbarkeit der Plattform orientiert sich an den Öffnungszeiten der Grundbuchämter. Grundsätzlich muss eine Plattform an allen Werktagen durchgängig zwischen 08:00 und 18:00 zur Verfügung stehen. Der maximale Ausfall der Plattform pro Ereignis darf

fünf Minuten nicht überschreiten. Pro Werktag darf die akkumulierte Ausfallzeit fünfzehn Minuten nicht überschreiten. Allfällige Servicefenster sind zwischen 18:00 und 08:00 Uhr nach Schweizer Zeit zu planen. Die Verfügbarkeit einer Plattform muss protokolliert und das Protokoll über die Plattform veröffentlicht werden.

5 Quellenverzeichnis

5.1 Relevante ISO Normen

- **ISO/IEC 20000-1:2011, Information technology – Service management – Part 1: Service management system requirements**
- **ISO/IEC 20000-2:2005, Information technology – Service management – Part 2: Code of practice**
- **ISO/IEC 27000:2009, Information technology – Security techniques – Information security management systems – Overview and vocabulary**
- **ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements**
- **ISO/IEC 27002:2005,Information technology – Security techniques – Code of practice for information security management**
- **ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management**
- **ISO/IEC 27007:2011, Information technology – Security techniques – Guidelines for information security management systems auditing**
- **ISO 19011:2011, Guidelines for auditing management systems**

5.2 Referenzen

- **Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 6. Januar 2010 (www.bundesnetzagentur.de > Sachgebiete > Qualifizierte elektronische Signatur > Veröffentlichungen > Geeignete Algorithmen)**
- **Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 2: Definitionen und Sicherheitsvorgaben für die Netzwerksicherheit (www.isb.admin.ch)**
- **Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 1: Checkliste der minimalen Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf (www.isb.admin.ch)**
- **Open Web Application Security Project (OWASP) (http://www.owasp.org)**
- **Center for Internet Security (CIS) (http://www.cisecurity.org/)**
- **Office of Government Commerce (2001). Service Delivery. IT Infrastructure Library. The Stationery Office. ISBN 0-11-330017-4**