Wirtschaftsportalverbund

Risikomanagement für Service Provider

Version 1.16 approbiert am 13.7.2015

Hörbe - Hötzendorfer

Inhalt

Begriffe

Definitionen der in diesem Dokument verwendeten Begriffe siehe unten in Kapitel 1 des Rulebooks „Begriffe und Rollen“.

1 Einführung

Wenn mehrere Organisationen vereinbaren im WPV ihre elektronische Kommunikation vertrauenswürdig zu betreiben, werden die zu Grunde liegenden Regeln als Rulebook bezeichnet[1]. Ein wesentlicher Teilbereich des Rulebooks ist dieses Dokument, welches das Risikomanagement der Service Provider regelt.

Das Ziel des Risikomanagements ist es, die Erfüllung der Qualitäts- und Sicherheitsziele der Serviceprovider durchzusetzen. Da unterschiedliche Benutzergruppen und Dienste verschiedene Anforderungen haben, ist die schwierigste Herausforderung, eine ausreichend spezifische, aber möglichst einheitliche Richtlinie für alle Teilnehmer zu schaffen.

Um diese Regelwerk möglichst einfach zu gestalten, werden im WPV drei wesentliche Konzepte umgesetzt:

- Vereinfachung der explizit vereinbarten Sicherheitsmaßnamen durch Risikotransfer;
- Standardisierung eines Maßnahmenkataloges zur Risikoreduzierung;
- Bündelung der explizit vereinbarten Maßnahmen in drei Sicherheitsklassen.

2 Geltungsbereich des Risikomanagements

Die Sicherheitsklassen regeln wie die Identifikation entfernter Benutzer an den Service Provider zugesichert wird.[2] Dabei wird die Erfüllung der Schutzziele *Vertraulichkeit, Integrität und Nachvollziehbarkeit*, soweit die Identifikation entfernter Benutzer betroffen ist, beachtet. Das Schutzziel *Verfügbarkeit* wird in den Sicherheitsklassen nicht explizit geregelt, so wie die meisten IKT-Dienstleistungen im Internet auf der Basis des „Best Effort“ geliefert werden.

[1] Weitere Begriffe sind u.a.: Trust Framework (Kantara, FICAM), Common Operating Rules (TSCP), Operating Regulations (Visa).

[2] Datenschutz und Interoperabilität werden außerhalb der Sicherheitsklassen geregelt.

3 Risikomanagement für Service Provider

Wenn ein Service Provider die Identifikation von Benutzern in eine Federation auslagert, ist das mit einem Risiko behaftet. Die Bewältigung dieses nicht vermeidbaren Risikos kann generell durch Verminderung, Transfer oder Akzeptanz erfolgen:

- Zur Verminderung werden präventive Sicherheitsmaßnahmen vereinbart.
- Der Transfer ist die Vereinbarung einer Haftung des IdP pro Identifikation.
- Bei der Akzeptanz bleibt das (restliche) Risiko beim Service Provider.

Würden sämtliche Service Provider den IdPs detaillierte Sicherheitsmaßnahmen vorschreiben, dann wäre die Wahrscheinlichkeit groß, dass diese Policy nur für ähnliche Anwendungen verwendbar ist und Abbildung auf andere Anwendungsbereiche schwer machbar oder nicht ökonomisch ist. Die Philosophie des Risikomanagements für Service Provider im WPV ist daher, dass primär Risiko transferiert wird. Zu diesem Zweck werden Haftungen für die korrekte Identifikation der Benutzer vereinbart, wodurch eine radikale Reduktion der Sicherheitsmaßnahmen möglich ist.

Im Zuge der Risikobehandlung wird das Risiko also grundsätzlich auf Haftungen abgebildet. (Beispiel: Für die Richtigkeit der Benutzeridentifikation wird bis max. 100€ pro Login gehaftet.) Nur gesetzlich oder vertraglich vorgegebene Maßnahmen werden an den IdP überbunden. (Beispiel: „Die Identität des Betroffenen muss entsprechend Bankwesengesetz erfolgen“.) Dabei muss darauf geachtet werden, dass die Maßnahmen im Katalog enthalten sind.

4 Risikoübermittlung vom SP zum IdP

Das Prinzip der automatisierten Aushandlung von Vertrauensstellungen gewährt dem Service Provider, dass der Zugriff von Nutzern nur unter (1) den vorgegebenen Haftungsbedingungen und (2) den Maßnahmen der geforderten Sicherheitsklasse erfolgt. Haftungsbedingungen assoziieren jede Transaktion mit einem Risikowert, mit dem IdP und SP ihre Erwartungshaltungen abstimmen. Diese Einstufung wird grundsätzlich pro Attribut angeboten, wobei vereinfachte Verfahren definiert werden können. Explizite Sicherheitsmaßnahmen werden in Form einer Sicherheitsklasse übermittelt.

Wird vom SP die Übermittlung von Haftungsbedingungen und Sicherheitsklasse angefordert, dann sind diese voneinander unabhängig und werden parallel übertragen.

Der Service Broker vermittelt Haftungsbedingungen und Sicherheitsklassen, wobei diese zum Großteil 1:1 auf den IdP überbunden werden.

Pro WPV-Federation ist zu definieren, wie ein Service Broker das übertragene Risiko auf IdP, FO und sich selbst aufteilt.

5 Standardisierung von Sicherheitsmaßnahmen

Es hat sich in der Praxis gezeigt, dass die Sicherheitsanforderungen bei verschiedenen Anwendungsbereichen unterschiedlich sind und ein einheitliches Schema von 3 oder 4 Sicherheitsklassen quer über alle Anwendungsbereiche unzureichend ist. Daher kann jede WPV-Federation ihre Sicherheitsklassen nach ihren Anforderungen definieren.

Damit die Interoperabilität zwischen den verschiedenen WPV-Federations so hoch wie möglich bleibt, werden zwei Konzepte umgesetzt:

1. Elementare Sicherheitsmaßnahmen werden verpflichtend vereinheitlicht und katalogisiert, und
2. eine minimale Anzahl von Maßnahmen ist für alle Federations verpflichtend.

Der Katalog (siehe Kapitel 7) wird im WPV für alle Federations zentral gepflegt und kann in begründeten Fällen geändert und erweitert werden.

Die minimalen Maßnahmen sind im Kapitel 8 definiert.

6 Sicherheitsklassen

Um die Vereinbarung von expliziten Maßnahmen zu vereinfachen, werden die Regeln in drei Sicherheitsklassen zusammengefasst[3]. Jede Sicherheitsklasse fasst ein Bündel von Maßnahmen zusammen, die vom Service Provider in Abhängigkeit von den Risikoklassen angefordert werden. Die Klassen bilden eine Hierarchie, bei der die Regeln einer höherwertigen Klasse die der darunterliegenden einschließen oder ersetzen.

Die Struktur des WPV ist föderal in den Sinn, dass verschiedene Federations ihre Regeln primär nach den Anforderungen ihres Sektors und Geschäftsmodells bestimmen. Dabei sollen aber die Teilnehmer nicht mit einer Federation neue - wenn auch größere - Identitätssilos bilden, sondern die Vernetzung und Interoperabilität zwischen verschiedenen Federations soll möglich sein und gefördert werden.

Das soll durch die Standardisierung der Bewertungskriterien erreicht werden. Aus ihnen sollen die Sicherheitsklassen modular zusammengestellt werden können, wie im Maschinenbau des 19. Jahrhundert genormte Schrauben und Teile Konstruktion und Produktion revolutioniert hatten.

Diese Zerlegung von Sicherheitsklassen in einheitliche Bausteine erzeugt zwar noch keine vollständige Interoperabilität, hat aber folgende Vorteile:

- Unterschiede verschiedener Regelwerke, die auf Grund schwammiger Terminologie, fehlender Ausarbeitung oder Fehlen von Normen entstehen können, werden a priori ausgeräumt.
- Der Normierungsprozess erzeugt ein gemeinsames Interesse den Bausteinkatalog zu pflegen und die Interessen und Anforderungen dabei abzustimmen.
- Identitäts- und Serviceprovider können wesentlich einfacher ihre Dienste in verschiedenen Federations anbieten, weil die Übersetzungsarbeit entfällt.

[3] Beispiele für dieses Konzept in anderen Frameworks sind: Level of Assurance 1-4 (ISO 29115 „Entity Authentication Assurance Framework“); Gewöhnliche, fortgeschrittene und qualifizierte Signatur (Signaturgesetz); Sicherheitsklassen 0-3 (Portalverbundvereinbarung der österr. Verwaltung).

7 Der Kriterienkatalog für IdP

Der Kriterienkatalog ist im Dokument „WPV Kriterienkatalog“ enthalten. Die Kriterien werden wie in der nachstehenden Grafik klassifiziert.

8 Minimale Maßnahmen in Sicherheitsklassen

Als Grundeinteilung sollen 3 Sicherheitsklassen (niedrig – mittel – hoch) definiert werden[4].

Als Minimum müssen in allen Federations folgende Maßnahmen umgesetzt werden:

Bereich „Organisation und Infrastruktur“ („CO“)

> FO und IdP müssen eine IT-Haftpflicht-Versicherung für die den WPV betreffenden Tätigkeiten nachweisen. Damit werden die Maßnahmen der Kategorie „Organisation und Infrastruktur pauschal abgedeckt. Alternativ müssen die Kriterien zur Führung eines ISMS vereinbart und durch den FO für den IdP bzw. FA für den FO überprüft werden.

Bereich „Authentifizierung von Benutzern“ für die mittlere Sicherheitsstufe:

> IdPs müssen eine Zweifaktorauthentifizierung unterstützen (Regel CV-MFA-010)

Bereich „Identifikation und Authentifizierung von Benutzern“ für die hohe Sicherheitsstufe

> Für natürliche Personen sind folgenden Regeln verpflichtend:
>
> - CI-IPV-030(Bürgerkarte) oder CI-IPV-040 (Bankwesengesetz)
> - CV-MFA-040 (qualifizierte Signatur) oder CV-MFA-050 (Recommendation 7 der EZB-Zahlungsverkehrsdirektive[5])

9 Vorgangsweise zur Erstellung der Datensicherheitsvorgaben

Um die Datensicherheitsvorgaben für eine Federation zu erstellen werden folgende Arbeitsschritte empfohlen:

1. Erhebung bestehender Sicherheitsanforderungen die SP an IdPs stellen.
2. Abbildung der Terminologie und der Maßnahmen auf den Kriterienkatalog des WPV.
3. Ergänzung um die minimalen Maßnahmen des WPV.
4. Analyse ob Kriterien des Katalogs zusätzlich empfohlen werden sollen.
5. Zuweisung der Kriterien an FO, IdP und SB.
6. Abstimmung mit den Teilnehmern der Federation.
7. Abstimmung mit der FA.

[4] Soweit möglich wird die Orientierung an der eIDAS-Verordnung empfohlen.

[5] https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf